Regulatory Frameworks and Evaluation Methodologies for the Licensing of Commercial Fusion Reactors

By
Robert Patrick White

B.S., Mechanical Engineering, Carnegie Mellon University, 2012
M.S., Mechanical Engineering, Carnegie Mellon University, 2012
M.S., Nuclear Science Engineering, Massachusetts Institute of Technology, 2019

Submitted to the department of Nuclear Science and Engineering
in partial fulfillment of the requirements for the degree of
Doctor of Philosophy in Nuclear Science and Engineering

At the
Massachusetts Institute of Technology
September, 2021

Signature of author: ______________________________
Robert Patrick White
Department of Nuclear Science and Engineering, MIT
August 20, 2021

Certified by: ______________________________
Koroush Shirvan
John Clark Hardwick (1986) Career Development Professor, MIT
Thesis Supervisor

Certified by: ______________________________
Zachary S. Hartwig
Robert N. Noyce Career Development Assistant Professor, MIT
Thesis Supervisor

Certified by: ______________________________
Dennis Whyte
Hitachi America Professor of Engineering, MIT
Thesis Reader

Accepted by: ______________________________
Ju Li
Battelle Energy Alliance Professor of Nuclear Science and Engineering, MIT
Professor of Materials Science and Engineering, MIT
Chairman, Committee on Graduate Students

Regulatory Frameworks and Evaluation Methodologies for the Licensing of Commercial Fusion Reactors

By

Robert Patrick White

Submitted to the department of Nuclear Science and Engineering
on August 20, 2021, in partial fulfillment of the requirements for the degree of
Doctor of Philosophy in Nuclear Science and Engineering

Abstract

Private companies hoping to deploy commercial fusion facilities in the next two decades will encounter a variety of technical, social, and economic challenges. These companies will also need to assess and develop appropriate technology regulation.
The under-regulation, over-regulation, or mis-regulation of a new technology could jeopardize long-term commercial deployment opportunities. Timely assessment and development of appropriate regulatory requirements are critical to the success of commercial fusion technology in the next two decades. The assessment and development of regulatory requirements for new technologies, however, is often based prior on operating experience or regulation of similar technologies. The applicability of these assessment and development methods is restricted for commercial fusion facilities for a variety of factors including the wide variety of fusion technologies currently under development, the preliminary nature of commercial design efforts, and the limited characterization of commercial fusion facility concept of operations.

This work presents an initial comprehensive approach to the assessment and development of appropriate regulatory requirements for commercial fusion technology. Models and methods based on the fundamental hazards of a technology are utilized to help examine the licensing and regulation of novel technologies and provide insights on how to more effectively assess and develop regulatory requirements. The different licensing evaluation methods and regulatory frameworks are developed and presented to provide insights on the impact of these regulatory decisions on the design constraints and regulatory burden for commercial fusion technology.

Specific insights are given on the selection of licensing evaluation methods and regulatory framework from this work. Licensing evaluation related insights include the incompatibility of large tritium inventories with low regulatory burden licensing evaluation methods, the design benefits and regulatory burden drawbacks of crediting engineering safety features in the licensing of fusion facilities, and potential advantages of utilizing System Theoretical Process Analysis (STPA) in the development of operational requirement for novel, complex systems such as commercial fusion. Regulatory framework related insights include the potential applicability of a delegated review regulatory framework (similar to commercial aviation) to commercial fusion, the potential economic costs of a new minimal regulation system based on a new strict liability insurance framework, and the development advantages of a new cooperative operational characterization regulatory framework for novel technologies such as commercial fusion.

The methods and models described in this work are intended to help regulators and industry evaluate the hazards of commercial fusion facilities and select licensing evaluation methods and regulatory frameworks that satisfy the social and economic constraints on commercial fusion facilities. Regulation is often viewed as inhibiting innovation but the proactive development of regulatory requirements using a comprehensive hazard based approach can help maintain social license for fusion technology, facilitate safe operation, and create a stable regulatory environment that will help foster the successful commercial development and deployment of fusion facilities for clean energy production.

Thesis Supervisor: Koroush Shirvan
John Clark Hardwick (1986) Career Development Professor,
MIT Department of Nuclear Science and Engineering

Thesis Supervisor: Zachary Hartwig
Robert N. Noyce Career Development Assistant Professor of Nuclear Science and Engineering, MIT Department of Nuclear Science and Engineering

Thesis Reader: Dennis Whyte
Hitachi America Professor of Engineering,
MIT Department of Nuclear Science and Engineering

Table of Contents

Acknowledgements

While I expected to work on nuclear policy issues during my PhD at MIT, I never expected that I would work on commercial fusion policy issues. The genesis and ultimate successful completion of this project was a result of the right student, at the right time, at the right place, at the right time, with the right resources - financial support from the SPARC Fellowship and the generosity of the MIT alumni donors made this work possible.

Professor Koroush Shirvan has been a great mentor and collaborator throughout this project. He's kept me focused on my thesis work (and taught me that there's a time a place for side projects), provide detailed insights and comments on my technical evaluations and writing, and helped me make sure that my final thesis would be a worth reading.

Professor Zach Hartwig has helped connect my work to the big picture on fusion technology development and commercialization. He has consistently emphasized that my focus would be on developing accurate insights and not to think about if the answers would be favorable for fusion energy commercialization. His focus on academic and research independence and integrity has been a great model for me in technical policy work.

Professor Dennis Whyte has helped me ensure that my work had clear takeaways for the fusion community. As a fission native, he helped explain the basics of fusion and made me realize that there is more to fusion than I could ever hope to learn. These insights helped me focus on developing more technology agonistic approaches to regulation and licensing, and I hope that I can work with the fusion community to apply these insights in the future.

My PhD work and time at MIT would not have been possible without the support of the NSE faculty, staff, and students who I have worked closely with during the last six years. Dr. Marina Dang has been invaluable manager, mentor, and friend, as have all of the other colleagues I've worked closely with in the NSE Communication Lab during my five years as Communication Fellow. Brandy Baker and the other administrators within the department have helped me at every step along the way with their continued support.

My friends from all parts of my life have played a huge role in my success. Meggie helped me get into graduate school and has listened to my stories and complaints throughout process. Allison and Daniel (my PhD support group) were incredible in helping me survive COVID-19 pandemic isolation and continue my work from home. I'm not sure if I would have stayed sane or productive without our morning chats over coffee.

My family (Lori, Bob, and Lindsay) and extended family have always believed in me, and I could not have done this without them. I like to think that I'm following in the footsteps of my nuclear engineering Uncle Jeff and grandfather – the first Dr. Robert White.

And, to Taylor. You've been the best partner I could have imagined throughout graduate school and I simply adore you. I cannot thank you enough for everything you've done for me but I will continue to make it up to you every day we're together.

Regulatory Frameworks and Evaluation Methodologies for the Licensing of Commercial Fusion Reactors

By

Robert Patrick White
August 20, 2021

Executive Summary

Rise of private fusion companies

The past 10 years have seen increasing interest by private companies to develop fusion technology for energy production with substantial investments from venture capital firms, traditional energy companies, and private philanthropists [1]. These private fusion companies seek to accelerate the development of commercially viable fusion technology and help decarbonize electricity production within the next two decades [2]. The development of large experimental devices, specifically the ITER project, has been hampered by physics and engineering limitations that require construction and operation of extremely large machines to achieve net energy gain in a magnetic tokamak confinement configuration using conventional low temperature superconductors [3]. Private fusion companies seek to leverage new enabling technologies and confinement configurations to facilitate the construction of more compact devices capable of net energy gain and energy production. Examples of the enabling technologies and confinement configurations include:

- high temperature, high field superconducting magnets for a tokamak magnetic configuration (Commonwealth Fusion Systems)
- high temperature, high field superconducting magnets for a spherical tokamak magnetic configuration (Tokamak Energy)
- magnetized target fusion confinement (General Fusion)
- field-reversed configuration confinement (TAE Technologies)
- magneto-inertial confinement (Helion Energy)
- inertial confinement (First Light Fusion)

Proponents of these companies believe that use of these technologies and confinement configurations could enable the development of commercially viable fusion technology within the next two decades. Successful near term deployment by these private companies requires development of commercial fusion facilities that are both technically viable and economically competitive.

Challenges of commercial fusion regulation

One of the challenges associated with the deployment of commercially viable fusion energy is assessment and development of appropriate technology regulation [4]. Under-regulation, over-regulation, or mis-regulation of a new technology can jeopardize long-term commercial deployment opportunities. Under-regulation may result loss of social license, legal liability, or harm to stakeholders due to inadequate oversight or requirements on a technology. Over-regulation may result in excessive oversight or requirements that make a technology economically unviable. Mis-regulation of a technology may result in both inappropriate and inadequate oversight or requirements, and result in both the harms of under-regulation and over-regulation. Timely assessment and development of appropriate regulatory requirements are critical to the success of commercial fusion technology in the next two decades.

The assessment and development of regulatory requirements for new technologies is normally based prior on operating experience or regulation of similar technologies. These approaches, however, may not be adequate for some novel technologies such as commercial fusion energy facilities. A net-energy fusion device has not yet been operated and there are many open scientific and engineering questions related to commercial fusion facility design. The unique characteristics of commercial fusion technology results in only tangential similarities to existing technologies such as industrial processing facilities, commercial fission facilities, and particle accelerator systems but strong similarities to none. It is not immediately clear that a compelling and appropriate regulatory precedent exists for commercial fusion technology.

Reliance on prior operating experience or similar industries may not result in appropriate initial regulation for novel technologies, and could slow deployment by private companies or incentivize short term decision-making that ultimately delays technology adoption. The wide variety of fusion technologies currently under development, the preliminary nature of commercial design efforts, and the limited characterization of commercial fusion facility concept of operations further restrict the applicability of the normal methods for the assessment and development of regulatory requirements.

Developing new models and methods for commercial fusion regulation

This work examines how licensing and regulation of novel technologies could be based on the fundamental hazards of the technology to provide insights on how to more effectively assess and develop regulatory requirements. This hazard based approach enables the description and characterization of licensing evaluation methods and regulatory frameworks, and assesses their effects on the design, licensing, and operation of regulated activities. The goal of this work is to provide insights to commercial fusion developers and policymakers on the technical and economic tradeoffs of different licensing evaluation methods and regulatory frameworks for the development and deployment of commercial fusion technology.

System engineering model to characterization of commercial fusion facilities operation

Deployment of commercial fusion technology requires developers to demonstrate the safety of a technology that does not yet exist. Evaluation of safety and development of regulatory requirements after significant research and design efforts have been completed would risk the significant capital and time investment required to commercialize fusion technology. Development of initial safety assessments and regulatory requirements before completion of significant design activities is critical to help frame future regulatory discussions and increase commercial assurance that design efforts and regulatory requirements will converge to a societally acceptable and economically viable technology.

The major challenges associated with pre-design evaluation of safety and development of regulatory requirements include:

- required facility systems, inherent operational hazards, and general concept of operations may be unknown for novel technologies that are immature or do not have significant operating experience,
- difficulty in assessing the hazards of a technology before it is designed,
- costs, time, and technical expertise required to develop detailed regulatory requirements for any complex and high hazard technology, and
- potential development of regulatory requirements that preclude or discourage innovative engineering approaches for novel technologies.

These challenges primarily relate to two topics: defining and assessing hazards for novel technologies, and facilitating innovation for novel technologies. This work addresses both challenges by using system function models.

A systems engineering approach using system function models facilitates the functional analysis of facility requirements into system functions as well as the decomposition and allocation of system functions into multiple lower level system requirements [5]. This process allows for the top down development of system functions from high-level system objectives. Development of system functions, interfaces, and performance requirements can be performed without specification of physical system form [5]. Use of function models for commercial fusion technology helps characterize hazards with a focus on inherent function and not design specific form. Models with increasing level of detail can be used to provide greater specificity for certain hazards or enable quantification of previously qualitative hazards. These systems models are initially developed as technology independent; no specific fusion technology (e.g., confinement method, fuel cycle) is assumed and the models are generally applicable to any fusion technology. This approach enables discussion and development of safety analyses and generalized regulatory requirements in a manner that does not discourage innovation and does not assume or prescribe technology specific solutions.

System engineering models for a technology independent commercial fusion power plant are developed with increasing levels of technical detail on hazards and critical plant characteristics. Initial use of a technology independent model enables insights into regulatory frameworks that may be compatible with a variety of technology approaches to fusion energy and do not require technology specific regulatory requirements. The history of commercial fission regulation demonstrates how development of technology specific, prescriptive regulatory requirements may increase short-term regulatory certainty but can discourage technological innovation due to the additional regulatory barriers. A system engineering model specifically applicable to a deuterium-tritium fueled tokamak commercial fusion facility is ultimately developed as the basis for technology specific hazard analyses in this work. The technology specific system engineering model deuterium-tritium fueled tokamak commercial fusion facility identifies 39 functional systems that are further assessed for system hazards and regulatory significance.

Hazard identification and prioritization based on regulatory significance

Commercial fusion facilities will inherently be complex engineering systems due to the specific and extreme physical conditions required to create and sustain fusion reactions. In addition, the limited operating experience and wide variety of proposed fusion technologies ensure that, at the very least, initial commercial fusion facilities will not be operationally well characterized. Evaluating safety based on analysis of initiating accident events may not be appropriate for commercial fusion facilities. Instead, a hazard-center approach to safety evaluations may be desirable.

In this work, a hazard-centered approach is used as the basis for preliminary safety evaluations and utilizes the following logical progression:

- what are the inherent hazards of a facility?
- what are the potential adverse consequences associated with the inherent hazards, independent of event sequences?
- what are inherent, engineered, or administrative safeguards or controls are in place to prevent the adverse consequences?
- what initiating events and subsequence events can lead to breakdown of these safeguards and controls?

While the difference between an initiating event centered approach and a hazard-centered approach is subtle, a hazard-centered approach focuses on control and mitigation of hazards rather than on prevention of all accident sequences or initiating events. A hazard centered approach enables the insights of preliminary safety evaluations to be incorporated into the design process because the evaluations are based on inherent system characteristics and not specific event sequences. Incorporation of preliminary evaluations into final facility design facilitates designer focus on limiting inherent hazards rather than trying to prevent all accidents. A focus on eliminating hazards by design can help produce a more robust system, especially for complex or poorly characterized systems.

A repeatable hazard characterization method is developed for the identification and prioritization of hazards with highest regulatory significance based on their potential for significant off-site consequences. This enables the characterization of plant systems with hazards that are most relevant to regulators. This process facilitates the identification of hazards significant for the assessment and development of regulatory requirements for commercial fusion facilities.

This work develops a set of hazards of regulatory interest for commercial fusion facilities based on a D-T tokamak specific system engineering model. The major off-site and on-site hazards of regulatory interest identified in this section are:

- radioactive material
- hazardous materials
- radioactive sources
- explosive materials

Certain hazards, such as neutron radiation sources and handling of radioactive tritium fuel, are inherent to a D-T fusion fuel cycle and cannot be eliminated through design and operation choices. Many other hazards, however, may be reduced by design. Hazards associated with activated radioactive materials, hazardous materials, and explosive materials in a commercial fusion facility will depend significantly on design and operational choices made for a commercial facility.

While the presence of these hazards is noted based on the current concept of operations for such a facility, determination of hazard magnitude and forms is a design specific activity. These hazards are discussed within this work to provide context on the development of regulatory requirements, but it is important to note that not all of the hazards are inherent to fusion technology.

Appropriate implementation of process design methods to minimize hazards by design and research into innovative technological or engineering approaches to reduce hazards could significantly reduce the overall risk associated with off-site and on-site hazards without the needs for engineered safeguards. This hazard reduction approach helps lead to safer designs and safer operation.

Hierarchical hazard limit model for comparison of regulatory requirements

Regulatory requirements and oversight are used to protect workers, the public, and the environment from the potential consequences of hazardous activities. Hazardous activities may be regulated using three main methods [6]:

- means based: requirements on how specific activity hazards are controlled
- management based: requirements on how an hazardous activity is managed
- performance based: requirements on presence, release, exposure to hazards

The applicability each of these methods varies depending on the specific regulated activity and factors such as the ability of the regulator the monitor an activity to verify compliance and the similarity of different activities being regulated [6].

Performance based regulatory requirements and performance metrics for the outcomes of management and means based regulatory methods (e.g., harms not prevented by means or management based regulatory frameworks) can be used to compare both regulatory systems and the safety of different regulatory activities. Comparison of these limits and outcomes, however, can be challenging due to significant differences in measurement metrics used by different activities. Radiological material inventory limits, hazardous material emission limits, and car accident fatality rates all characterize hazard consequences of regulated activities but consistent comparison of these hazard consequences is challenging.

A novel hierarchical hazard limit model (Figure 1) is developed that enables the comparison of dissimilar limits on hazards and facilitates development of consequence-consistent regulatory limits for commercial fusion technology. This model provides insights on selection of regulatory requirements that better reflect accepted risks for different activities and seeks to facilitate regulatory requirements for commercial fusion that are consistent with other energy generation activities.

Definition and selection of each hierarchical hazard limit presents advantages and disadvantages in terms of the inherent assumptions and conservatisms associated with the hazard limit, as well as the costs associated with monitoring and verifying regulatory compliance. Developing the hazard limits using a consistent model allows commercial fusion facilities to base regulatory limits on societal hazards and not limits tied to legacy of commercial nuclear fission regulations.

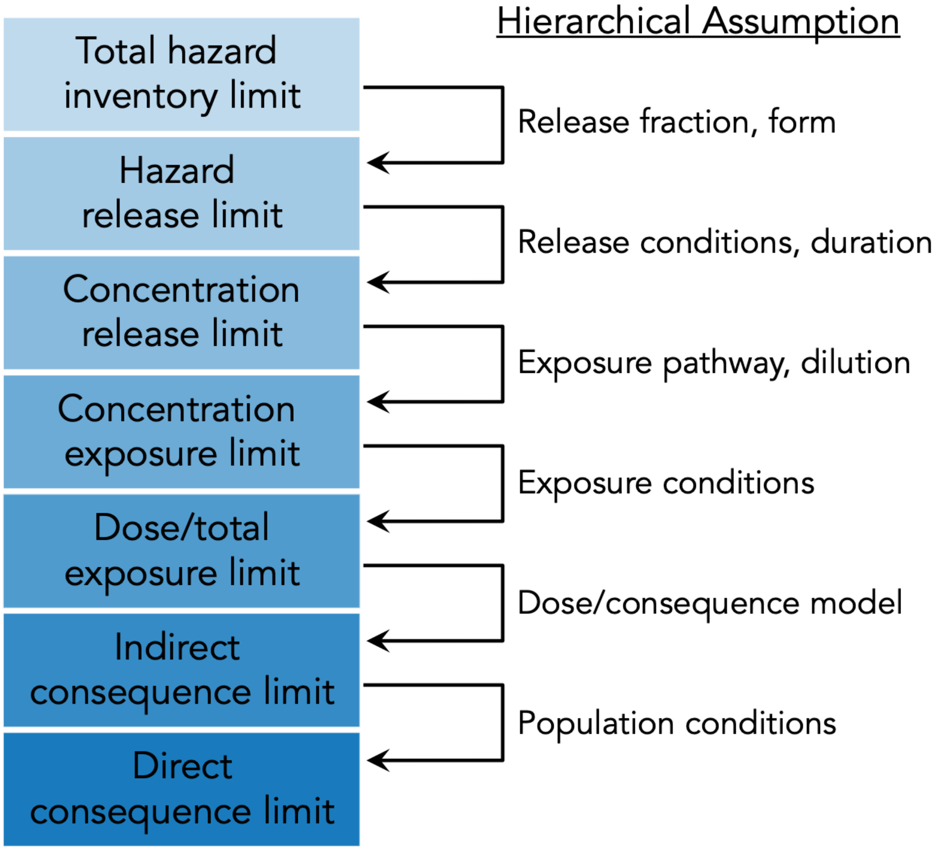

Hierarchical Assumption
Total hazard inventory limit
Release fraction, form
Hazard release limit
Release conditions, duration
Concentration release limit
Exposure pathway, dilution
Concentration exposure limit
Exposure conditions
Dose/total exposure limit
Dose/consequence model
Indirect consequence limit
Population conditions
Direct consequence limit

Figure 1. Hierarchical hazard limits for regulated activities

Licensing evaluation methods for assessment of facility design and operation

Licensing evaluation methods allow the evaluation of facility hazards and demonstrate compliance with regulatory hazard limit requirements. Four licensing evaluation methods widely used for the evaluation of engineered systems are presented. Adaptation of a fifth method, the system theoretical process analysis (STPA) evaluation method, for the regulation of a commercial fusion facility is novel to this work. The technical bases for these evaluation methods are presented, general methodologies are developed and discussed, and a preliminary licensing evaluation of commercial fusion facility or major system is performed for each method. The potential effects of each licensing evaluation method on the design, operation, and regulation of commercial fusion facilities is also reviewed.

Worst-case release evaluation

A worst-case release evaluation determines the maximum possible hazard consequences associated with an activity or facility without regard to event probability. Worst-case analyses for licensing evaluations may be the simplest form of licensing evaluation but can also have the largest inherent conservatisms. This simplified analysis has the potential to minimize the regulatory burden on commercial fusion by eliminating the need to prepare and review detailed regulatory evaluations. A preliminary worst-case release evaluation of tritium hazards D-T tokamak commercial fusion facility suggests that the tritium inventory in some commercial fusion facilities may result in unacceptably high off-site radiation doses. Modifications to facility design (reducing hazard inventory) or updates to facility-specific meteorological and siting characteristics (reducing off-site exposure) would likely be required to demonstrate compliance with relevant regulatory hazard limits for off-site acute exposure to radiological hazards. This licensing evaluation method requires the fewest regulatory resources to complete but will require significant conservatism in design and operation to meet the regulatory limits associated with small hazard inventories.

Maximum credible release evaluation

A maximum credible release evaluation determines the maximum expected hazard consequences associated with an activity or facility based on a qualitative assessment of credible failure mechanisms. Use of maximum credible release analyses for licensing evaluations enables trade offs between decreasing inherent conservatism and increasing regulatory burden. This analysis has the potential to balance inherent hazard design constraints on commercial fusion facilities while still limiting the regulatory burden to those comparable for commercial chemical facilities. A preliminary maximum credible release evaluation of tritium hazards D-T tokamak commercial fusion facility indicates that that major changes would be needed to the facility design or assumptions considered in the analysis to result in acceptable the hazard consequences. Modifications to facility design (reducing inventory), changes to facility operation (reducing inventory at risk), or updates to facility-specific meteorological and siting characteristics (reducing off-site exposure) would likely be required to demonstrate compliance with relevant regulatory hazard limits for off-site acute exposure to radiological hazards. This licensing evaluation method facilitates the use of some engineering principles to reduce facility hazards but will require conservatism in design and operation to meet the regulatory limits associated with controllable hazard inventories.

Deterministic design basis event evaluation

A deterministic design basis evaluation determines the hazard consequences associated with wide range potential initiating events and event sequences that are qualitatively assessed as credible. Use of deterministic design basis analyses for licensing evaluations reduces conservatism from simpler analysis methods and enables the consideration of engineered safety features in hazard consequence analyses. These analyses allow designers and analysts to mitigate significant hazards through the use of active and passive engineered safety features. This approach significantly reduces the calculated hazard consequences for a facility or activity but come at the cost of increased burden of proof and regulatory burden related to systems significant safety and supporting analyses. A preliminary deterministic design basis evaluation of tritium hazards within the tritium storage system at D-T tokamak commercial fusion facility illustrates how use of credited engineered safety features could be used to demonstrate compliance with regulatory requirements. This evaluation method and associated compliance costs would dramatically increases the regulatory costs associated with facility licensing from those associated for industrial chemical facilities to those associated with commercial fission facilities. This licensing evaluation method adds additional regulatory burden and process requirements for commercial fusion facilities but facilitates the credited use of engineering safety features in facility design.

Probabilistic design basis event evaluation

A probabilistic design basis evaluation determines both the hazard probability and consequences associated with sets of initiating events and event sequences. Use of probabilistic design basis analyses for licensing evaluations provides the most detailed analysis of the risk (probability and consequence) of hazardous activities and facilities. This method enables the most realistic modeling of initiating events and evaluation of extremely low probability events without the need to add prescriptive regulatory requirements. The risk insights gained from probabilistic analysis allow applicants to prioritize the SSCs that will contribute greatest to facility risk and safety. This approach significantly further reduces the calculated hazard consequences for a facility or activity but further increases the design, analysis, and regulatory costs associated with facilities. A preliminary probabilistic design basis evaluation of tritium hazards within the tritium storage system at D-T tokamak commercial fusion facility illustrates how use of credited engineered safety feature and fault tree methodologies facilitate compliance with regulatory requirements and reduce the scope of credited safety feature as compared with deterministic analyses. This licensing evaluation method would provide largest degree of design and analysis flexibility based on a realistic assessment of facility design and hazards but also require significant regulatory resources and detailed process requirements for commercial fusion facilities.

System theoretical process analysis evaluation

Use of system theoretical process analysis (STPA) for licensing evaluations is an innovative way to analyze and regulate hazardous activities and facilities. STPA is a paradigm shift for evaluating safety, focusing on the systematic control of hazards rather than identification and mitigation of causal event sequences. STPA enables an extremely comprehensive, system evaluation based on the losses and hazards relevant to all stakeholders. The evaluation method can be used to transparently and robustly develop performance based regulatory requirements for any high hazard activity, scaling both based on the size of the system and the level of design. STPA, when integrated into the design process, enables the analysis of system hazards and development of constraints that highlight potential failure modes of interest. A preliminary STPA evaluation of the tritium storage system at D-T tokamak commercial fusion facility illustrates how operation errors or feedback breakdowns could lead to failure mechanisms not explicitly characterized by other evaluation methods. Certain prescriptive organization safety mechanisms such as quality organizations and change management processes emerge organically as systems important to ensuring long-term safe operation and are traceable to specific hazards and losses of interest to stakeholders. This licensing evaluation method can provide useful insights to the safe design, operation, and maintenance of commercial fusion facilities but it has some unresolved questions related to the high regulatory burden and integration with regulatory requirements.

Summary of licensing evaluation methods

The five licensing evaluation methods presented in this work are all applicable to demonstrate compliance of commercial fusion technology with regulatory hazard limits. Each method balances the level of analysis detail with the use of conservative regulatory assumptions. At their most fundamental level, they answer the following questions:

- “What is the worst that could happen?” – Worst Case Release Evaluation
- “What is the worst that could realistically happen?” – Maximum Credible Release Evaluation
- “What would happen if…?” – Deterministic Design Basis Event Evaluation
- “What is the risk of…?” – Probabilistic Design Basis Event Evaluation
- “How can this facility lose control? – STPA Evaluation

These methods are all intended to help regulators assess whether an activity demonstrates compliance with regulatory requirements. Each method can be used to demonstrate compliance but will have different impacts on the design and licensing process.

More conservative evaluations (Worst Case Release and Maximum Credible Release) require substantially fewer regulatory resources but require significant limitations on design and operation of commercial fusion facilities to minimize the inherent hazards of a system. This work demonstrates that minimizing radiological inventories (tritium and mobile radioactive materials) by design is essential to demonstrating compliance with these evaluation methods.

More realistic evaluations (Deterministic and Probabilistic Design Basis Event Evaluation) require significantly more regulatory resources but provide designers and operators with flexibility in meeting regulatory limits. This works helps demonstrate how engineering safety features and operational controls can be credited for reducing the consequences of accidents. The characteristics would allow commercial fusion facilities to meet regulatory limits without making substantial changes to facility hazards by design.

The STPA evaluation described in this work may present a new method for the evaluation of facility safety. Its integration with existing regulatory frameworks is challenging due to absence quantitative insights currently produced by the standard analysis method. This work helps demonstrate the broad range of operational insights and requirements that can be generated from review of system operation. Application of STPA evaluations on more detailed designs and further development of regulatory metrics that are compatible with regulatory requirements and frameworks may help demonstrate the feasibility of STPA for licensing evaluations. This method may be particularly useful for the evaluation of novel commercial fusion facilities because it can provide insights on operational challenges that are only normally characterized after developing operating experience with a system.

Regulatory framework models for licensing of facility design and operation

Regulatory framework models describe regulatory regimes and can characterize different levels of regulatory oversight and relationships between a regulator and the regulated activity. A model of system operating limits to describe unexpected system failures is developed to facilitate discussion of the impacts of regulatory frameworks on system safety. Development of an insurance requirement based regulatory framework for industrial facilities using a strict liability standard and an operational characterization based regulatory framework for full facility regulation are novel to this work. The theoretical bases for each of these frameworks are presented, the major characteristics of each framework are discussed, and the compatibility of each framework with the licensing evaluation methods is assessed. The potential impact of each framework on the regulation of commercial fusion technology is finally discussed.

Insurance requirement based regulatory framework

The insurance requirement based regulatory framework would enable the development of commercial fusion technology with minimal regulatory requirements related to design and operation safety. Commercial fusion companies instead work with private firms to fully insure against maximum hypothetical releases under a standard of strict liability – accepting full accident liability regardless of fault. Commercial fusion companies would be able to operate without major external design requirements if they could successfully utilize design, operation, siting, and analysis arguments to demonstrate sufficiently low facility risk for private insurance companies. Private insurance companies could, however, impose requirements on commercial fusion companies to control and mitigate maximum and expected risks of commercial fusion facilities.

Negotiation of insurance premiums and imposed requirements from private insurance companies would be conducted on a facility-by-facility basis between private companies. These premiums and requirements could represent a minor or significant impediment to commercial fusion depending on the specific facility and requirements. The formal regulatory and impediments with this regulatory framework are minimal but releases could be extremely costly due to the liability requirements on commercial fusion companies. The insurance requirement based regulatory framework is a wager on the free market viability of commercial fusion technology – a convincing safety case and safe operations results in the lowest possible regulatory costs and minimal regulatory requirements but uncertainty in the safety case and any accidental releases could be extremely costly for the commercial fusion industry.

Permit based regulatory framework

The permit based regulatory framework would enable the development of commercial fusion technology under a similar regulatory regime as other sources of energy and industrial facilities. Commercial fusion companies would work with regulators to develop appropriate regulatory limits that satisfy social requirements on potential hazard consequences. The permit based framework provides commercial fusion companies wide latitude in the design and operation of facilities but would hold them accountable for compliance with relevant regulatory requirements. The challenges associated with managing acute hazards would require facilities to consider the impacts of design and inherent hazards on off-site consequences. Minimizing, substituting, mitigating, and simplifying hazardous processes could significantly reduce risk but may not be technically or commercially feasible in all cases. The permit based regulatory framework is based on decades of successful operation of hazardous facilities in the United States but control of acute catastrophic hazards would be key to successful regulation and maintaining social license for commercial fusion facilities.

Delegated review based regulatory framework

The delegated review based regulatory framework would enable the full regulatory review of commercial fusion facilities while reducing regulatory burden and leveraging the expertise of industry in the regulatory process. This regulatory framework has been extremely effective at enabling the safe and economic development of complex, high hazard, novel technologies such as commercial aviation, and it could provide the same benefits to commercial fusion technology. The delegated review based regulatory framework enables regulatory oversight while minimizing the technical burden on regulators and reducing the need to maintain large, highly specialized regulatory staffs. Regulators can on focus independent reviews of safety critical and novel aspects of commercial fusion facilities and emphasize safe overall operation. Initial development of this regulatory framework would be time consuming due to the administrative process requirements for performing delegated regulatory reviews but maintaining public trust through designee independence is critical to realizing the long-term regulatory benefits of this framework. The delegated review based could help promote the safe and economic development of novel commercial fusion technology.

Independent review based regulatory framework

The independent review based regulatory framework would enable complete regulatory review of commercial fusion facilities and validate compliance with regulatory limits. The independent review based regulatory framework provides full public oversight of hazardous technologies and builds trust through regulatory transparency and rigorous regulatory reviews. This regulatory framework requires substantial technical expertise to adequately operate. Regulators would need to ensure that new regulatory staff is prepared to independently review proposed novel fusion technologies with limited operating experience. These regulatory processes could be costly and time consuming for both regulators and the commercial fusion industry, and could present a substantial regulatory burden for the emerging industry. The precedent set by the regulation of commercial fission facilities using an independent review based regulatory framework may make use of this framework politically favorable, but the regulatory burden associated with developing and performing independent reviews for commercial fusion facilities may make this framework economically unfavorable. The independent review based regulatory framework could minimize regulatory, policy, and safety questions related to the development of commercial fusion technology.

Operational characterization based regulatory framework

The operational characterization based regulatory framework enables the collaborative development of operational experience and understanding of system behavior to better characterize the safe operation of novel commercial fusion facilities. This framework requires operational transparency from industry with the public but enables the more rapid development of operating experience needed to support mature regulatory requirements without excessive conservatisms. Deliberate development of operating experience, identification and reduction of uncertainties, and a continuous focus on incorporation of lessons learned can help commercial fusion technology rapidly mature by leveraging industry wide expertise and experience. The operational characterization based regulatory framework enables more rapid development of novel, high hazard technologies such as commercial fusion by establishing regulatory limits and processes that will evolve with the operational maturity and understanding of the technology.

Summary of regulatory frameworks

The five regulatory frameworks presented or developed in this work are different pathways for the licensing and regulation of commercial fusion technology. Each framework balances the roles of an independent government oversight, industry self-regulation, and third party private audits to ensure the safe operation of commercial fusion facilities. The regulatory frameworks used for industrial facilities (permit-based framework) and fission facilities (independent review based framework) have been largely presumed for the regulation of commercial fusion facilities based on legislative precedent but have inherent limitations related to regulation of a novel technology with significant off-site facility hazards. The remaining three regulatory frameworks presented and developed in this work (insurance requirement based framework, delegated review based framework, and operational characterization based framework) all carry distinct advantages for the development and deployment of fusion technologies. These frameworks attempt to accelerate development and deployment of novel technologies by facilitating regulator focus on safety critical issues or shifting regulatory responsibility to private industry while still ensuring financial liabilities against accidents.

The development of novel insurance requirement based framework and operational characterization based framework in this work present two radically different but theoretically supported approaches to regulation of commercial fusion facilities. The optimal regulatory framework for commercial fusion technology will likely vary depending on specific technology characteristics and business considerations for private fusion developers. Use of hybrid regulatory frameworks (e.g., selection of different regulatory frameworks for different facility hazards) may be effective at ensuring the optimal regulatory framework for the variety of on-site and off-site hazards present at commercial fusion facilities. Stakeholders will need to work to assess which regulatory frameworks are socially, politically, and commercially tenable to support the development of specific fusion technologies

Future work

This work provides initial characterization of fusion facility design, hazards of regulatory interest, and hazard limits for commercial fusion facilities using a repeatable and technology independent process. These processes are used as the basis for assessment of hazard licensing evaluation methods and regulatory framework models for commercial fusion facilities and characterization of their impacts on facility design, operation, and commercial viability. These assessments, however, are largely preliminary and intended to provide initial quantitative insights to commercial fusion developers and policy makers.

Several promising areas of future work related to the development of regulatory requirements for commercial fusion facilities are identified:

- more detailed characterization of fusion system design and system hazards
- quantification and assessment of non-tritium radiological hazards on safety
- quantification and assessment of design constraints based on use of different licensing evaluation methods for commercial fusion facilities
- demonstration of STPA evaluations on more detailed system designs and improved integration of STPA evaluations into regulatory frameworks
- development of more detailed requirement processes and estimation of insurance premiums for insurance requirement based regulatory framework
- development of requirements and methods that can support a operational characterization based regulatory framework for novel technologies

These areas for future work would help better assess the impacts of licensing evaluation methods and regulatory frameworks on the development and deployment of commercial fusion technology.

Summary and impacts of this work

This work presents an initial comprehensive approach to the assessment and development of appropriate regulatory requirements for commercial fusion technology. Methods and models based on the fundamental hazards of a technology are utilized to help examine the licensing and regulation of novel technologies and provide insights on how to more effectively assess and develop regulatory requirements. Existing methods and models are combined with novel methods and models in this work to better characterize commercial fusion facilities despite limitation on design information, operating experience, and related technologies. These methods and models are applied to help characterize proposed commercial fusion facilities. The tools presented and evaluated in this work can provide policymakers and commercial fusion developers with a common set of methods and models to evaluate and discuss when selecting appropriate regulatory pathways and requirements for commercial fusion facilities.

Development and deployment of commercial fusion facilities by private companies in the next two decades will encounter a variety of technical, social, and economic challenges. Early development of appropriate regulatory requirements for novel technologies can help facilitate commercial efforts and not hinder them. Use of existing regulatory methods based on existing operating experience and the regulatory methods used for similar technologies may result in successful regulation but risks the under-regulation, over-regulation, or mis-regulation of commercial fusion facilities. This work presents methods and models that can help regulators and industry evaluate the hazards of commercial fusion facilities and select licensing evaluation methods and regulatory frameworks that satisfy the social and economic constraints on commercial fusion facilities. Regulation is often viewed as inhibiting innovation but the proactive development of regulatory requirements using a comprehensive hazard based approach can help maintain social license for fusion technology, facilitate safe operation, and create a stable regulatory environment that will help foster the successful commercial development and deployment of fusion facilities for clean energy production.

References

[1] J. Deign. Why are oil and gas companies investing in nuclear fusion?

[2] National Academies of Sciences, Engineering, and Medicine. Bringing Fusion to the U.S. Grid. The National Academies Press, 2021.

[3] H. Zohm. On the size of tokamak fusion power plants. Phil. Trans. R. Soc. A, 337:20170437, 2018.

[4] Fusion Industry Association. Igniting the Fusion Revolution in America. June 2020.

[5] U.S. Department of Defense. System Engineering Fundamentals. January 2001.

[6] C. Coglianese. The limits of performance-based regulation. University of Michigan Journal of Law Reform, 50:525, 2017.

Chapter 1 – Introduction to commercial fusion and regulation

This chapter describes the motivation for the development of private commercial fusion companies and the regulatory challenges associated with commercial development. The need to develop new models and methods to support the regulation of commercial fusion is then presented. The licensing evaluation methods and regulatory frameworks developed in this work are briefly discussed and the applicability of this work to inform future discussions on regulatory regimes for commercial fusion technology is highlighted.

1.1. Motivating the private commercialization of fusion energy

Fusion technology has been the "energy of future" for the past seventy years. Regarded as the "holy grail of clean energy", its proponents have promised to capture the energy of stars on earth to produce unlimited clean energy for everyone [1]. Ideally, commercial fusion energy would have all of the advantages of commercial fission energy (dispatchable, high energy density, no particulate emissions) with none of the disadvantages (long-lived wastes, safety concerns, potential for meltdowns, prospect of nuclear non-proliferation and dual use technologies)[2]. These characteristics all contributed to the view of fusion energy as the world's ultimate energy source.

These claims, however, have been tempered by the realized history of fusion energy development. The scientific and engineering challenges associated with studying and developing methods to confine and control extremely high temperature plasmas are immense [3]. Fusion science researchers made steady progress from the early 1970s through the late 1990s and set new records on the fusion power output from experimental fusion facilities (Figure 1.1) [4]. This steady progress in fusion power output, however, has largely stagnated since the early 2000s.

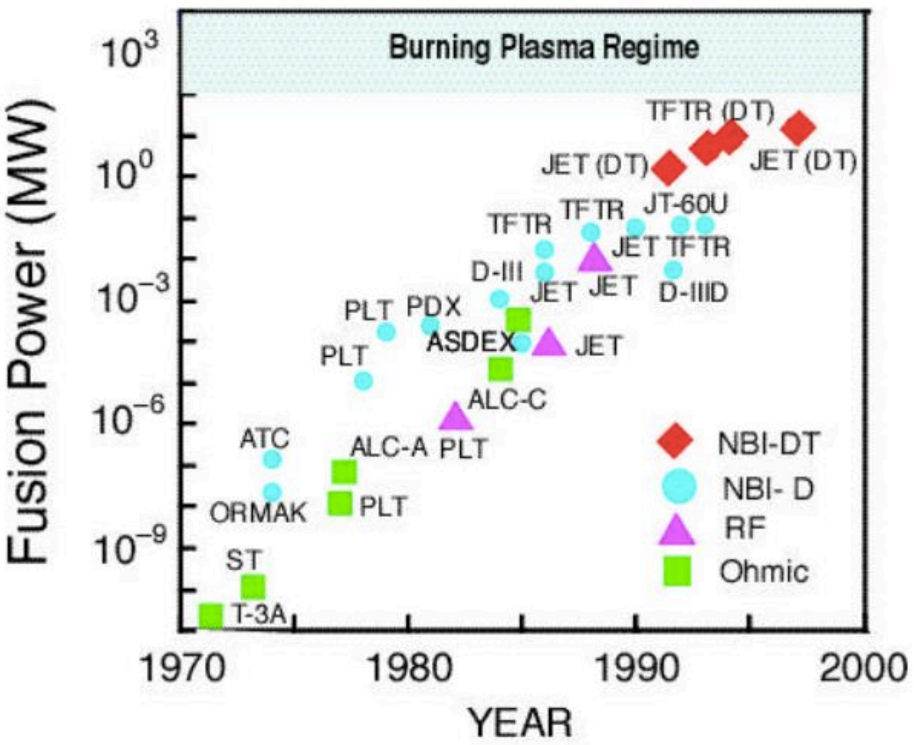


Figure 1.1. Selected fusion device performance [4]. Fusion device power has largely stagnated in the past two decades (not shown).

As experimental fusion facilities grew in power, so did their size, cost, and technical constraints. By the late 1980s, the international community recognized the value in sharing both development costs and research expertise to construct and operate an international experimental fusion facility [4]. The ITER project was intended as the final experimental facility that could demonstrate that fusion technology could produce next energy and be utilized to generate clean energy [5]. The highly complex and international effort encountered scientific, engineering, project management problems with the projected completion data slipping by more than decade [6]. Delays in the successful construction and operation of ITER also pushed back serious international design efforts on commercial fusion technology that relied on scientific and engineering insights gained from ITER operation [7]. The rapid commercial development of other clean energy technologies (including solar, wind, and energy storage) and the push to fully decarbonize electricity production by 2050 raised questions about the commercial viability and social value of a technology that may not be ready for widespread deployment until after 2050 [3].

1.2. Rise of private fusion companies

The past 20 years have seen increasing interest by private companies to develop fusion technology for energy production with substantial investments from venture capital firms, energy companies, and private philanthropists [8]. These private fusion companies seek to accelerate the development of commercially viable fusion technology and compete to help decarbonizing electricity production within the next two decades [9]. The development of ITER has been hampered by physics and engineering limitations that require construction and operation of a large machine to achieve net energy gain in a magnetic tokamak confinement configuration using conventional low temperature superconductors [10]. The new private fusion companies seek to leverage new enabling technologies and confinement configurations to facilitate construction of more compact devices capable of net energy gain. Examples of new enabling technologies and confinement configurations include:

- high temperature, high field superconducting magnets for tokamak magnetic configuration (Commonwealth Fusion Systems)
- high temperature, high field superconducting magnets for spherical tokamak magnetic configuration (Tokamak Energy)
- magnetized target fusion confinement (General Fusion)
- field-reversed configuration confinement (TAE Technologies)
- magneto-inertial confinement (Helion Energy)
- inertial confinement (First Light Fusion)

Private companies and their proponents believe use of these new enabling technologies and confinement configurations could enable the development of commercially viable fusion technology within the next two decades. Successful near term deployment by these private companies requires development of commercial fusion facilities that are technically viable, safe to operate, easily licensable, and economically competitive.

1.3. Challenge of commercial fusion regulation

One of the challenges associated with the commercially successful development of fusion energy is assessment and development of appropriate technology regulation [2]. Under-regulation, over-regulation, or mis-regulation of a new technology can jeopardize long-term commercial deployment. Under-regulation may result loss of social license, legal liability, or harm to stakeholders due to inadequate oversight or requirement on an technology. Over-regulation may result in excessive oversight or requirements that make a technology economically unviable. Mis-regulation of a technology may result in both inappropriate and inadequate oversight or requirements and result in both the harms of under-regulation and over-regulation. Timely assessment and development of appropriate regulatory requirements are critical to the success of commercial fusion technology in the next two decades.

The assessment and development of regulatory requirements for new technologies is normally based insights gained from existing operating experience with a technology and the regulatory methods used for similar technologies. Assessment and development of requirements based on existing operating experience is generally applicable for technologies that have already been operated extensively and are being regulated after commercial deployment (e.g., regulation of industrial facilities by the U.S. Environmental Protection Agency in 1970). Assessment and development based on similar technologies is generally applicable when there are strong functional and technological parallels between the new technology and existing regulated technologies (e.g., regulation of cellular and gene therapy technology by the U.S. Food and Drug Administration). These approaches can assist legislators, regulators, and industry in the assessment and development of appropriate regulatory requirements.

Operating experience with general fusion technologies can first be examined to assess their applicability for commercial fusion facilities. Operating experience with commercial fusion technology is non-existent. No fusion devices have been operated with a net gain of energy or used for the commercial production of energy. There has been, however, significant operation of experimental fusion facilities. The applicability of this prior empirical operating experience may be limited. Commercial fusion facilities will differ significantly from experimental fusion facilities that have been operated around the world over the past seven decades of development:

- operation in a net energy gain or burning plasma regime
- total power produced by fusion reactions will be one to two orders of magnitude higher in the fusion power (tens to thousands of megawatts)
- total production of reaction byproducts will be one to two orders of magnitude larger (scaling with fusion power)
- average thermal loads may be higher due to more compact device and higher total power production
- devices are operated more frequently and for much longer durations than previous experimental facilities and experimental campaigns (steady state, long duration pulses, or long campaigns of high frequency, short duration pulses)
- capture and utilization of fusion power produced by device
- integration of fusion device with balance of plant systems for power production or other industrial energy activities
- steady state or batch production, utilization, processing, and disposal of fuels, working fluids, and other consumables to facilitate on-going operations

These differences will be present for commercial fusion facilities regardless of the specific fusion technology used for the facility. Many fusion reactions planned for use either require radioactive fuel (tritium) or will produce neutrons as a reaction product (e.g., deuterium-deuterium fuel reactions or deuterium-tritium fuel reactions). Experimental fusion facilities have been operated that utilize both radioactive fuel and neutron producing reactions (e.g., the Tokamak Fusion Test Facility (TFTR) at the Princeton Plasma Physics Laboratory) but commercial fusion facilities that utilize these fuels and reactions would have the following additional challenges:

- total neutron radiation production (neutrons per second) will be one to two orders of magnitude larger (scaling with fusion power), impacting radiation dose and shielding requirements
- total secondary gamma radiation production will be one to two orders of magnitude larger (scaling with neutron radiation production and neturon scattering), impacting radiation dose and shielding requirements

- average neutron radiation flux may be higher due to more compact device and higher neutron radiation production, impacting material damage and degradation mechanisms
- total neutron radiation fluence on materials will be much higher (scaling with neutron radiation flux and total duration of operation), impacting material damage and degradation mechanisms
- steady state or batch production, utilization, processing of larger inventory of radioactive fuel (scaling with fusion power and operational parameters), impacting safety characteristics and facility hazards

These differences would result in limited applicability of operational experience from experimental fusion facilities in the assessment and development of regulatory requirements for commercial fusion technology.

Regulatory methods used for technologies and activities similar to fusion can also be examined to assess their applicability for commercial fusion facilities. A commercial fusion facility could be characterized as an industrial energy facility and subject to oversight using methods similar to those utilized by the U.S. Environmental Protection Agency for the regulation of many industrial hazards. A commercial fusion facility could also be characterized as a radiological facility that uses nuclear reactions to produce energy and subject to oversight using methods similar to those utilized by the U.S. Nuclear Regulatory Commission for the regulation of commercial nuclear fission facilities. A commercial fusion facility could still further be characterized as a particle accelerator that utilizes and produces radiological material and subject to oversight using methods similar to those utilized by the U.S. Nuclear Regulatory Commission for the regulation of industrial radioactive material facilities. The unique characteristics of commercial fusion technology result in tangential similarities to many technologies and strong similarities to none.

Reasonable arguments can be made for any of these three characterizations of commercial fusion facilities and it is not immediately clear that a compelling regulatory precedent exists for commercial fusion technology. Hasty assessment and development of regulatory requirements for commercial fusion technology based on tangential similarities to existing technology may facilitate successful regulation but risks the under-regulation, over-regulation, or mis-regulation of commercial fusion facilities.

While assessment and development of regulatory requirements for new technologies is normally based prior operating experience or regulation of similar technologies, these approaches may not be adequate for some novel technologies. These approaches may not result in appropriate initial regulation for novel technologies and could slow deployment by private companies or incentivize short term decision-making that ultimately inhibits technology adoption. The wide variety of fusion technologies currently under development, the preliminary nature of commercial design efforts, and the limited characterization of commercial fusion facility concept of operations further restrict the applicability of normal methods for the assessment and development of regulatory requirements.

1.4. Developing new models and methods for commercial fusion regulation

Examining the licensing and regulation of novel technologies based on the fundamental hazards of the technology could provide insights on how to more effectively assess and develop regulatory requirements. This enables the description and characterization of licensing evaluation methods and regulatory frameworks, and assesses their effects on the design, licensing, and operation of regulated activities. These characterizations can be used to select appropriate regulatory pathways and requirements for commercial fusion. While the licensing evaluation methods and regulatory frameworks are developed in a technology inclusive manner, examples in this work focus on highlighting the regulatory implications for a deuterium-tritium fueled tokamak fusion facility.

This works develops and presents methods and models that can be used to assist in the assessment and development of regulatory requirements for commercial fusion technology. The following methods and models are developed in this work:

1. System engineering method for characterization of commercial fusion facilities operation. This enables the identification of functional systems at varying levels of design without detailed knowledge of plant design. This approach can be completed in a technology agnostic or technology specific manner for commercial fusion facilities.
2. Robust hazard characterization method based on identification and prioritization of hazards with high regulatory significance. This enables the characterization of plant functional systems with hazards most relevant to assessment and development of regulatory requirements. This facilitates the identification of hazards most significant for the assessment and development of regulatory requirements for commercial fusion facilities.
3. A novel hierarchical hazard limit model that enables the comparison of dissimilar limits on hazards, and facilitates development of equivalent regulatory hazard limits. This provides insights on selection of regulatory requirements that better reflect accepted risks for different activities and seeks to facilitate regulatory requirements for commercial fusion that are consistent with other energy generation activities.
4. Licensing evaluation methods that enable the evaluation of facility hazards against hazard limits within regulatory requirements. The five methods evaluated in this work are:
    a. Worst case release evaluation
    b. Maximum credible release evaluation
    c. Deterministic design basis event evaluation
    d. Probabilistic design basis event evaluation
    e. System theoretical process analysis evaluation

    Development of a system theoretical process analysis evaluation method for the regulation of a commercial energy facility is novel to this work. The technical bases for these evaluation methods are presented, a general methodology is developed and discussed, and a preliminary licensing evaluation of commercial fusion facility or major system is performed. The potential effect of each licensing evaluation method on the design, operation, and regulation of commercial fusion facilities is discussed.

5. Regulatory framework models that facilitate the regulation of activities based on different levels of regulatory oversight and relationships between a regulator and the regulated activity. A novel description of system operating limits to describe unexpected system failures is presented to facilitate discussion of the impacts of regulatory frameworks on system safety. The five framework evaluated in this work are:
    a. Insurance requirement based regulatory framework
    b. Permit based regulatory framework
    c. Delegated review based regulatory framework
    d. Independent review based regulatory framework
    e. Operational characterization based regulatory framework

    Development of an insurance requirement based regulatory framework for industrial facilities using a strict liability standard and an operational characterization based regulatory framework for full facility regulation are novel to this work. The theoretical bases for each of these frameworks are presented, the major characteristics of each framework are discussed, and the compatibility of each framework with the licensing evaluation methods is assessed. The potential impact of each framework on the regulation of commercial fusion technology is finally discussed.

Combined, these methods and models provide insights into the assessment and development of appropriate regulatory requirements for commercial fusion technology. Each regulatory approach will have different benefits and risks. Some approaches may facilitate development and deployment with minimal regulatory requirements but would require extremely conservative facility design or industry acceptance of extremely high insurance requirements. Other approaches will allow for significant reduction in design conservatisms but would require costly detailed licensing evaluation methods and lengthy regulatory review processes.

The selection of the optimal regulatory approach for commercial fusion technology will depend on technical, economic, and social limitations on the development and deployment of different fusion technologies. This work does not recommend a specific approach but provides specific insights and bases to support the future selection appropriate regulatory pathways and requirements for commercial fusion facilities by regulators and private companies.

1.5. References

[1] L. Grossman. Inside the quest for fusion, clean energy's holy grail. *Time Magazine*, 2015.

[2] Fusion Industry Association. *Igniting the Fusion Revolution in America*. June 2020.

[3] National Academies of Sciences, Engineering, and Medicine. *Final Report of the Committee on a Strategic Plan for U.S. Burning Plasma Research*. The National Academies Press, Washington, DC, 2019.

[4] M. Zarnstorff, D. Gates, E. Hooper, S. Jardin, H. Ji, S. Luckhardt, J. S. Lyon, T. Simonen, and T. Thorson. Mfe concept integration and performance measures magnetic fusion concept working group.

[5] D. Meade. 50 years of fusion research. *Nuclear Fusion*, 50(1):014004, 2009.

[6] D. Clery. More delays for ITER fusion project, 2015.

[7] H. Fountain. A dream of clean energy at a very high price. *New York Times*, March 27, 2017.

[8] J. Deign. Why are oil and gas companies investing in nuclear fusion? *Greentech Media*, September 18, 2020.

[9] National Academy of Engineering and National Academies of Sciences, Engineering, and Medicine. *Bringing Fusion to the U.S. Grid*. The National Academies Press, Washington, DC, 2021.

[10] H. Zohm. On the size of tokamak fusion power plants. *Phil. Trans. R. Soc. A*, 337:20170437, 2018.

Chapter 2 – Characterizing a Commercial Fusion Facility for Safety and Licensing Evaluations

Assessing the need for licensing and regulatory activities begins with characterization of the operation and hazards associated with an activity, technology, or facility. This chapter outlines a technology-independent, system engineering approach to characterize the operation of a commercial fusion facility for subsequent hazard identification. The need to characterize a commercial fusion facility for safety and licensing evaluations is first presented as the basis for development of system engineering models. System engineering models for a technology independent commercial fusion power plant are then developed with increasing levels of technical detail on hazards and critical plant characteristics. A system-engineering model specifically applicable to a deuterium-tritium fueled tokamak commercial fusion facility is developed as the basis for hazard analyses in this work. Finally, the models developed in this chapter are compared to prior system engineering models for other commercial fusion facilities completed as part of prior national and international design efforts. Differences between these models are discussed and justified. The methods presented in this chapter are a repeatable approach to characterize functional systems for commercial fusion systems for use in hazard identification and other regulatory activities.

2.1 Characterizing technology for safety and regulatory evaluations

Evaluating the safety of any technology first requires an understanding of the technology: form, function, operation, and system interfaces are all critical to assessing overall system safety. Safety evaluations and development of regulatory requirements can be timed in three different ways in relation to design activities: after completion of design activities, concurrent with design activities, and before initiation of design activities. Each of these timing strategies has potential advantages and disadvantages that affect the duration, cost, fidelity, and complexity of the safety evaluation process.

Commercial fusion developers will need to address the challenge of selecting an appropriate strategy for the timing and performance of safety evaluations and developing regulatory requirements. Fusion technology faces two related problems: ensuring safety in the design of a novel technology, and justification of the regulatory requirements and review processes for a novel technology. Ensuring safety in the design of a novel technology can be accomplished by any of the three evaluation of safety strategies, although the cost and effort associated with each strategy may differ significantly. Justification of regulatory requirements and review processes for novel technologies introduces new challenges related to the timing and performance of safety and licensing evaluations.

2.1.1 Strategies for evaluating technology safety

Evaluation of safety after completion of the design process is common in industries where safety is considered largely as an afterthought. The main advantage of post-design safety evaluations is that the design is fully developed, so evaluating safety without significant assumptions on system design or performance is possible. The main disadvantage of post-design safety evaluations is that safety evaluations may reveal significant hazards or potentially unsafe conditions that must be corrected before operation. Major configuration changes made after completion of design activities are resource intensive (schedule delays and emergent engineering effort) or may not be feasible without complete redesign. The effort and time associated with redesign can incentivize designers and other stakeholders to seek engineering solutions to problems (often in the form of additional engineered systems or components) that can satisfy safety evaluations but do not reduce or eliminate the inherent hazard of a technology. Addition of safety after design tends to be costly and resource intensive due to the need to design new safety systems around existing systems and the treatment of safety systems as an "add-on" to an otherwise suitable system design. Configuration changes and redesign can also introduce new system interactions and failure mechanisms. If comprehensive safety evaluations are not repeated following design changes, new unknown failure mechanisms or hazards may be present in the final design. A technology subject to post-design safety evaluations may be made safe, but it is not inherently safe.

Evaluation of safety concurrent with the design process is a preferred approach for development processes that facilitate inherent safety by design and not safety through engineered systems alone. The main advantage of concurrent design and safety evaluation is that safety can be incorporated at all levels of design, from pre-conceptual design through detailed design. System architecture can be fundamental changed to eliminate rather than simply mitigate hazards and produce an overall safer design. Concurrent design and safety evaluation also allows for progressively more detailed safety evaluation based on the increasing design maturity. The main disadvantage of this concurrent design and safety evaluation is that that it can increase upfront development costs and requires more detailed definition of final design safety goals and requirements for the system. Note that the total development costs associated with concurrent design and safety evaluation are likely less than that of post-design safety evaluations due to the costs associated with safety related rework.

Evaluation of safety before the design process can be challenging, primarily due to the lack of detailed design information. This process alone may not ensure development of a safe design but can inform designers of potential hazards that must be eliminated, controlled, or mitigated. For well characterized and standardized mature technologies, these evaluations can be performed based on prior operating experience and previously characterized technology hazards. For example, the general hazards of an automobile are well known based on significant operating experience with the technology. While new automobiles may be designed with features that introduce new potential hazards (e.g., software affecting automated safety controls), many inherent hazards of an automobile (high speed, impacts, rotating components) are already well characterized to facilitate design.

The main limitation of evaluation of safety before the design process occurs for novel technologies that are not well characterized or do not have significant operating experience. Fundamental required systems, inherent operational hazards, or even the general concept of operations for a technology might not yet be known. Determining a safety envelop or informing designers of hazards of concern to include in safety evaluations may be challenging for these technologies. Systems engineering models can be used for these technologies to help define a general concept of operations and minimum required systems to facilitate preliminary safety evaluations. These preliminary evaluations can both inform initial design efforts (including later use of concurrent design and safety evaluations), as well as inform the development of regulatory requirements for a technology that are commensurate with the technology hazards and risk.

For most design activities, safety evaluations will be performed before, during, and after completion of major design activities. The difference between developers' strategies largely relates to the effort and emphasis placed on completing each stage of evaluation. Performing minimal pre-design safety evaluations that fail to facilitate incorporation of safety insights into design activities largely negate the benefits associated with performing the early safety evaluations. Strategic execution of any safety evaluation plan requires understanding of the priority and goals of each state of safety evaluation.

2.1.2 Strategies for development of regulatory requirements

Development of regulatory requirements after completion of the design process is common for technologies where the initial hazards of technology are not known or considered significant by regulators. The advantage of developing regulatory requirements and review processes following design completion is that it enables development of regulatory requirements that accurately reflect the hazards and risks of a technology. The disadvantages of developing regulatory requirement post-design are that the requirement development process may produce regulatory requirements that require substantial redesign of a technology, require design changes or features that render a technology economically infeasible, or requirement substantial development delays that can render the technology economically infeasible.

Development of regulatory requirements following design completion has significant disadvantages related to the potential hazards of deployment of new technology without regulatory oversight and a public perception that imposing regulation following widespread technology deployment is infeasible.

If a new technology is implemented without any regulatory review or oversight, the public, workers, and the environment may be exposed to the inherent hazards of a technology. This could lead to unacceptable harm if the actual operational hazards of a technology exceed the societally acceptable hazard limits. For example, the drug thalidomide was developed in West Germany in the late 1950s and immediately marketed for the treatment of nausea in pregnant women based primarily on animal studies and limited regulatory reviews. The drug was used for several years before it was identified as the cause of severe birth defects for pregnant women and outlawed, but not before affecting approximately 10,000 children in Europe and Asia [1].

Unacceptable harm caused by inappropriate and unregulated early deployment of a technology can also result in public and regulatory backlash that ultimately limits the appropriate long-term deployment of a technology. For example, widespread deployment of modern synthetic insecticides such as DDT began before scientists and regulators understood the severe environmental impacts of heavy (and inappropriate) usage of DDT. Public backlash over demonstrable environmental effects of excessive DDT usage (highlighted by scientists such as Rachel Carson in her book *Silent Spring*) lead to regulatory bans on the manufacture and use of DDT in many countries [2]. These outright bans, however, inhibited the controlled, appropriate, and incredibly effective use of DDT in the fight against mosquito borne malaria which kills more than 500,000 people annually in tropical and subtropical regions [3]. Despite historical bans on DDT usage in many countries, the World Health Organization recommended in 2006 that the controlled use of DDT to prevent malaria citing that "evidence from countries that continued using DDT showed that correct and timely use of indoor spraying can reduce malaria transmission by up to 90%" [4]. The initial inappropriate usage of DDT has arguably contributed to millions of deaths worldwide due to decades of the reactive regulatory bans on usage of DDT that prevented its appropriate use to prevent malaria.

These examples highlight the two potential impacts of deployment of new technology without regulatory oversight or review can have a technology if harm results from previously unidentified technology hazards.

If a technology is deployed and becomes widely adopted before regulatory limits are imposed, imposition of regulatory requirements that could render a technology economically infeasible could be resisted by groups that argue that the societal (and economic) cost of losing the technology outweigh the hazards posed by the technology. For example, environmental controls under the 1970 amendments to the Clean Air Act placed strict restrictions on pollution from new stationary sources but exempted all sources that were currently operating due to the costs associated with plant modifications [5]. This exemption was meant to provide regulatory relief to current operators and enable a gradual transition to cleaner industrial facilities based on typical assessment management or facility modifications that would trigger stricter regulatory requirements. The costs associated with complying with the stricter standards, however, have incentivized operators to exploit the exemption process and find legal ways to operate exempted facilities far beyond their typical operating lifetime with no restrictions on emissions. These exemption methods, while criticized by environmentalists as deviating from regulatory intent, have been upheld as legal and been expanded over time by some administrations [5].

This example highlights how societal and market pressure could limit the ability of regulators to impose regulatory requirements and review processes following design completion.

Development of regulatory requirements concurrent with the design process and technology development is common for technologies where initial development of a technology or previously operated technology indicates potential regulation relevant hazards. Ongoing discussions regarding the development of regulations for genetically modified foods are an example of concurrent development. The advantage of creating regulatory requirements and review processes concurrent with design is that it allows for creation of requirements that accurately reflect the hazards of a technology while providing for the simultaneous iteration of design and regulatory requirements. The processes can enable a collaborative environment where regulatory requirements and techno-economic constraints are negotiated to help create an environment where technology is developed in an economically optimal and socially responsible way. Note that a collaborative process is not necessarily a cooperative process, and that regulatory activities can be performed independently.

The main disadvantages of creating regulatory requirements and review processes concurrent with design are the political challenges with prioritizing regulation of an emerging technology, the inherent uncertainties related to regulatory outcomes, and the competing priorities and pressures from different stakeholders. Concurrent development of regulation at an early stage of design requires creation of initial regulatory infrastructure before it is clear that a social need to regulate a technology exists. Creation of a regulatory infrastructure to concurrently develop regulation takes forethought and requires an investment of both political capital and funding to ensure that the development process is successful and avoid wasted development efforts on a technology that may not reach maturity. A concurrent development process has inherent uncertainties on regulatory outcomes. While an iterative negotiated process may have a higher likelihood of reaching a satisfactory outcome for all stakeholders, it is possible that development of societally acceptable and techno-economic feasible requirements may not be possible – negating the overall purpose of the regulatory development process. Finally, different groups of stakeholders participating in the development will likely be subject to different external pressures and have different priorities. While technology developers may push for rapid rule development to help ensure economic viability, regulators may seek a slower process to ensure fair incorporation and evaluation of all relevant stakeholders.

Development of regulatory requirements before the design process and technology development is common for technologies where public concern over possible technology hazards or previously operated technology indicates significant regulation relevant hazards. Research restrictions on modification of the human embryos using genetic engineering techniques pending development of regulatory requirements are example of preemptive development. The advantages of creating regulatory requirements and review processes before the design process are that it provides technology developers a set of societally imposed requirements for their design (that can be translated into technical requirements) and the ability to assess whether their final design will be societally acceptable. This allows technology developers to make informed design choices that can produce a technology that is ultimately acceptable to society. Technology developers thus have assurance that the time and capital spent on the development and design of a technology can generate returns. For novel technologies that require relatively little time or capital investment (e.g., internet applications and other scalable start-ups), this assurance may not be significant. For novel technologies that require substantial capital for design and development (e.g., pharmaceuticals or heavy industry manufactured products), this assurance can enable market investment in the development of these novel technologies.

The disadvantages of creating regulatory requirements and review processes before the design process is that it can be extremely difficult to assess the hazards of a technology before it is developed, it can be costly to develop regulatory requirements before a technology is known to be economic and socially viable, and overly prescriptive regulatory requirements could preclude or discourage innovative approaches to novel technologies. Assessing the potential hazards of a novel technology before design or development is extremely challenging, especially for technologies without significant technical precedent. For these technologies, the potential to over-regulate or under-regulate is significant, both of which can result in consequences for the technology developer, the public, or other stakeholders. The costs associated with development of regulatory requirements before design and development depend significantly on the level of technology maturity and the availability of technical experts and information to justify requirements. For technology with low or unknown likelihood of future economic viability, justifying these regulatory development costs may be challenging. The final disadvantage is that use of certain regulatory requirements (specifically prescriptive requirements) could preclude or discourage innovation in design. For novel technologies, innovation is key to success and prescriptive requirements can force developers to focus implement known solutions to problems instead of working to design new solutions. For example, advanced fission reactor developers have been repeatedly incentivized to prioritize redevelopment of fission reactor technologies that have been previously operated without widespread commercial adoption (e.g., sodium fast reactors or high temperature gas reactors) due to the existing operating experience base that can be used to support required regulatory compliance activities [6]. While prescriptive requirements can help increase regulatory certainty for technologies, use of prescriptive regulatory requirements for novel technologies before the design process should be avoided.

2.1.3 Selecting evaluation and requirement development approaches for commercial fusion

Deployment of commercial fusion technology requires developers to demonstrate the safety of a technology that does not yet exist, or at most exists partially. Of the three timing strategies discussed above (post-design, concurrent with design, pre-design), the major risk of post-design or concurrent design evaluation of safety and development of regulatory requirements is that it risks the significant capital investment required to develop commercial fusion. Development of the technology for any purpose other than basic scientific research is futile if commercial fusion is not ultimately technically, economic, and socially viable. Creation of an initial safety analysis and regulatory requirements pre-design is critical to help frame future discussions and increase assurance that iterative design efforts and regulatory requirements will result in a societally acceptable and viable technology.

The major challenges associated with pre-design evaluation of safety and development of regulatory requirements are:

- fundamental required systems, inherent operational hazards, and general concept of operations may be unknown for novel technologies that are immature or do not have significant operating experience,
- difficulty in assessing the hazards of a technology before it is designed in detail,
- costs, time, and technical expertise required to develop detailed regulatory requirements,
- potential to develop regulatory requirements could preclude or discourage innovative approaches to novel technologies

These challenges primarily relate to two topics: defining and assessing hazards for novel technologies, and enabling innovation in novel technologies. This work addresses both challenges by using system function models. Systems engineering approaches using system function models facilitate the functional analysis of system requirements into system functions and the decomposition and allocation of system functions into multiple lower level system requirements [7]. This process allows for the top down development of system functions from high level system objectives. Development of system functions, interfaces, and performance requirements without specification of physical form [7]. Use of function models for commercial fusion technology helps clarify and quantify (where possible) hazards with a focus on function, not form. Models with increasing level of detail can be used to provide greater specificity for certain hazards or enable quantification of previously qualitatively described hazards. These systems models are initially developed as technology independent; no specific fusion technology (e.g., confinement method, fuel cycle) is assumed and the models should be generally applicable to any fusion technology. This approach allows discussion of safety analysis and generalized regulatory requirements in a manner that does not discourage innovation (or in fact could encourage innovation) and does not assume or prescribe technology specific solutions.

2.2 Creating function models for commercial fusion facilities

Function models are developed in this section to assist in the definition and assessment of hazards for a commercial fusion facility. The function models developed in the section are separated based on increasing levels of engineering detail. The four levels of detail are:

- Level 0 – Generalized Facility Concept Inputs and Outputs
- Level 1 – Generalized Plant Functions and Interfaces
- Level 2 – High Level System Functions and Interfaces

- Level 3 – Plant System or Component Functions and Interfaces

At each level, function block requirements are defined and a function is assigned to the block. The function is then decomposed and allocated to provide greater detail on the function (and potential underlying hazards) of each function block. These decomposed function blocks are then connected based on their relationships and interfaces, and used to create the next higher level function model. Increasing the model level may not result in decomposition to more detailed functions for some function blocks. In these cases, it is believed that functional decomposition is not practical and that further decomposition would require definition of design specific form. Definition of design specific form is required for the specific hazard identification but premature definition of form can limit the effectiveness of a system engineering approach for facilitating regulatory evaluations of commercial fusion facilities applicable to any technological approach.

Function models consist of a system boundary, system inputs and outputs, function blocks, and relationships between function blocks. The system boundary is represented by a dotted line around the model. This line is a symbolic demarcation between what is analyzed as part of the system model and what is excluded. The system inputs or outputs are represented by solid labeled arrows that cross in and out of the system boundary. These inputs and outputs may be physical (e.g., material) or non-physical (e.g., data) and are required for the operation of the system. The function blocks are represented by solid blocks within the model. Each function block is labeled with a generalized form or description. A supporting data table for each function model provides details on the specified overall function and a decomposition of the function into higher order functions. Relationships between function blocks are represented by solid labeled arrows that described the physical or non-physical relationship between blocks. The direction of the arrow indicates the direction of the relationships, indicating aspects such as control or flow of physical information/material.

2.2.1 Level 0 Function Model for Commercial Fusion

The Level 0 function model, while seemingly trivial, is an important step in the definition of a commercial fusion facility and provides the basis for higher level function models. The Level 0 function model is shown in Figure 2.1.

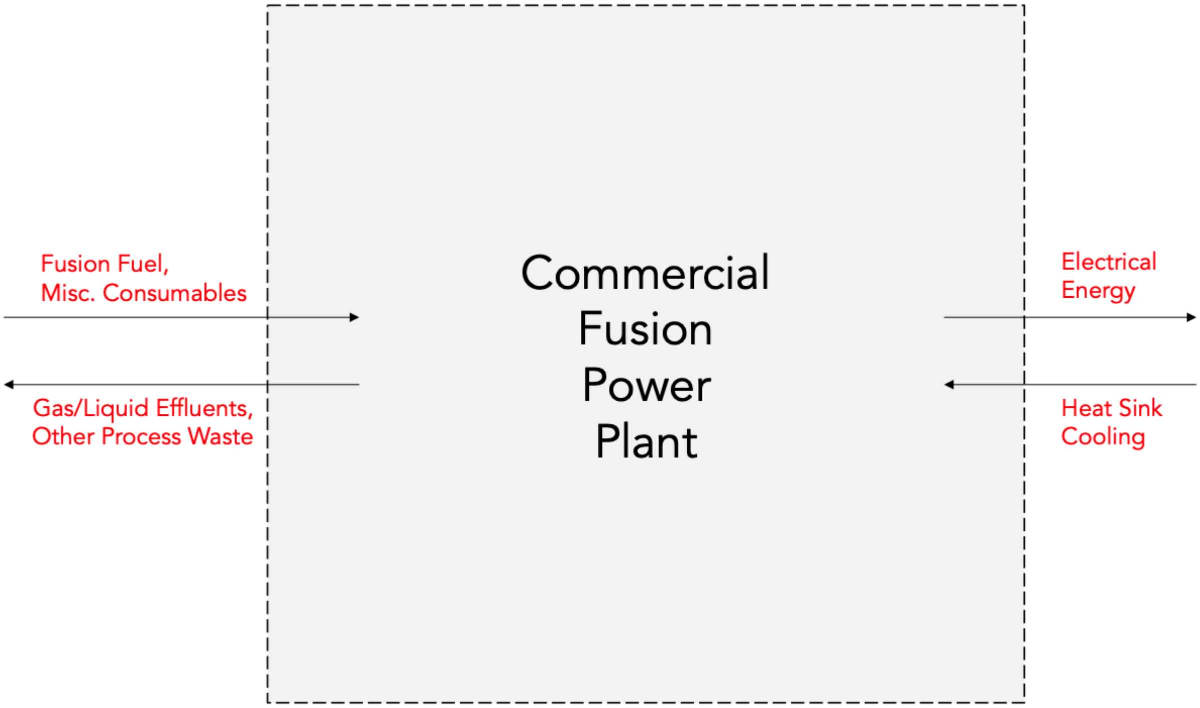


Figure 2.1. Level 0 Commercial Fusion Function Model

This Level 0 model shown in Figure 2.1 does not contain a defined function block. In this case, the entire model is defined as the function block – a commercial fusion power plant. The function of this block is the produce net electricity. While this function is relatively simple, it has several important nuances. The defined objective of the fusion power plant in this model is net electricity production. While this does not preclude the use of fusion energy for applications such as a process heating, the focus of this analysis will be a typical electric generation station. This also sets an initial design parameter that the electric power demand to run the facility must be less than the gross electric output of the facility. While this may be self evident, it will provide constraints or correlations later on the relationships between higher-level function blocks or system inputs and outputs.

Level 0 Function Block Inputs and Outputs

The Level 0 function model provides fundamental inputs and outputs for a commercial fusion facility. These inputs and outputs are listed and justified in Table 2.1. While these inputs and outputs may seem self evident for a fusion facility, they provide the basis for a broad framework for assessing the potential hazards and impacts of a commercial fusion facility on licensing.

Table 2.1. Level 0 Model System Boundary Inputs and Outputs

Inputs	*Function Block*	*Rationale*
Fusion Fuel	Commercial Fusion Power Plant	Required for fusion power generation
Misc. Consumables	Commercial Fusion Power Plant	Required for all functions
Heat Sink Cooling	Commercial Fusion Power Plant	Required for electric power generation

Outputs	*Function Block*	*Rational*
Electrical Energy	Commercial Fusion Power Plant	Produced by electric power generation
Gas/Liquid Effluents	Commercial Fusion Power Plant	Produced by all functions
Other Process Waste	Commercial Fusion Power Plant	Produced by all functions

This Level 0 model is intentionally broad and technology agnostic to enable creation of generalizable model for the analysis of any proposed fusion technology. This broad approach allows the Level 0 model to be applied to any fusion power plant that produces electricity for commercial purposes. These inputs and outputs will be consistent for Level 1, Level 2, and Level 3 models.

For example, the definition of fusion fuel does not specify the fuel needed for fusion or the form of the fuel. The generic definition of the specific fuel allows application of this input model to encompass fuel cycles from the current primary approach proposed for commercial fusion energy production (deuterium-tritium fuel) to less technically mature approaches to commercial fusion energy production (e.g., proton-^{11}B fuel) [8]. In generic definition of the fuel form allows for both open and closed fusion fuel cycles. The fusion fuel brought into the Commercial Fusion Power Plant function block could be a final form fuel produced off-site (e.g., pure tritium gas or tritiated metal hydrides) or an intermediate fuel form that could be converted into fusion fuel via nuclear reactions (e.g., pure lithium, lead-lithium solids, or fluoride-lithium-beryllium salts).

Level 0 Function Block Decomposition

The Level 0 Function Block ("Produce net electricity") is decomposed into three functions that fully encompass the function. Table 2.2 provides the decomposition of the function requirements and the assignment of the decomposed functions to new function blocks for the Level 1 function model.

Table 2.2. Level 0 Function Model Decomposition

Level 0 Function Block	*Function*	*Decomposed Function*	*Level 1 Function Block*
Commercial Fusion Power Plant	Produce net electricity	Produce heat from fusion reactions	Fusion Power System
		Convert heat into electricity	Balance of Plant System
		Support facility operations	Auxiliary Support System

Again, this Level 0 function decomposition is intentionally broad and technology agnostic. The three decomposed function encompass the most general functions required to fulfill the Level 0 function. These function blocks will be decomposed further into more specific functions in the Level 1, Level 2, and Level 3 models.

2.2.2 Level 1 Function Model for Commercial Fusion

The Level 1 function model decomposes the Level 0 Function Block into three Level 1 Function Blocks. The Level 1 function model is shown in Figure 2.2.

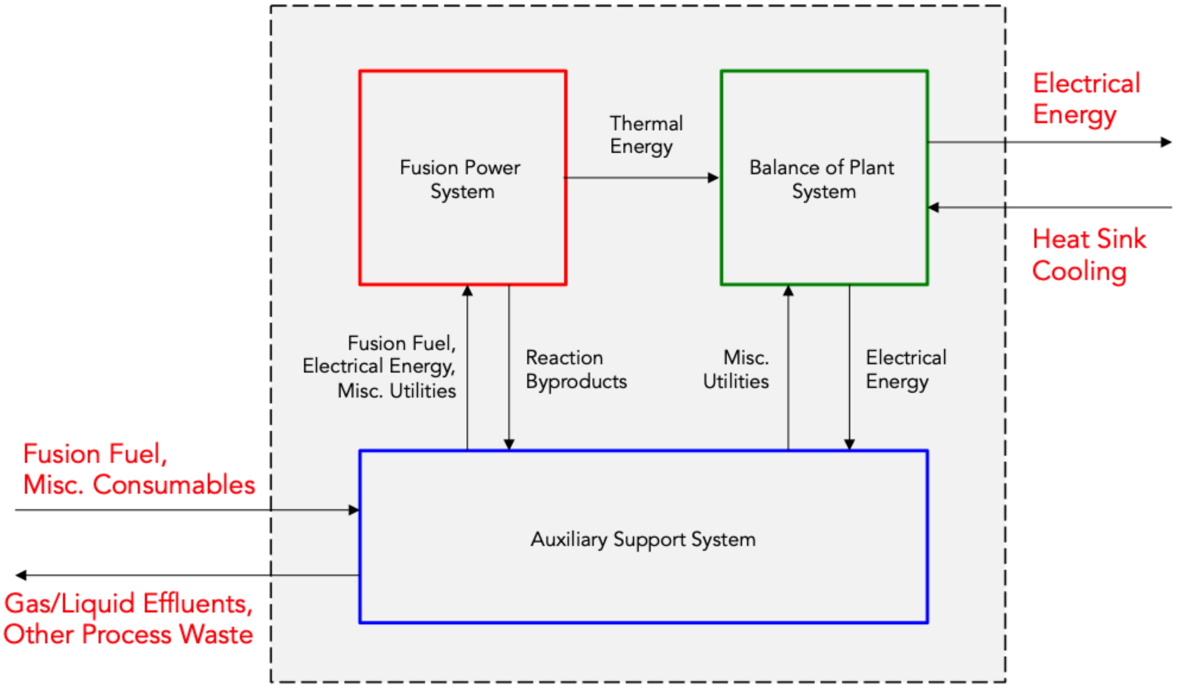


Figure 2.2. Level 1 Commercial Fusion Function Model

This Level 1 model shown in Figure 2.2 consists of three defined function blocks. In this section, detailed descriptions of each Level 2 Function Blocks are provided. Justification for connection of the system inputs and outputs to function blocks is given in Table 2.3, the relationships between function blocks is described in Table 2.4, and the Level 1 model is functionally decomposed in Table 2.5.

Level 1 Function Block Descriptions

Level 1 Function Block: Fusion Power System

Level 1 Function: Produce heat from fusion reactions
Parent Level 0 Function Block: Commercial Fusion Power Plant

This function is the energy source within the fusion power plant. It is directly analogous to the steam supply system found in other thermal power production facilities. This function block consists of all systems, structures, and components needed to obtain thermal energy from fusion reactions. This block is technology agnostic and is applicable to any approach to commercial fusion power production. Further decomposition of this function block at higher levels will provide greater differentiation of the required sub-function for fusion energy production.

Level 1 Function Block: Balance of Plant System

Level 1 Function: Convert heat into electricity
Parent Level 0 Function Block: Commercial Fusion Power Plant

This function is electrical production and thermodynamic functions within the fusion power plant. This function block would likely be identical to standard power production facilities that have thermal electrical energy conversion. This system is separated in order to allow the separation of fusion technology specific analyses from the general power production systems common to other electricity production facilities. This function block will be further decomposed for higher level models but is already fairly well characterized by existing system engineering models for power production facilities.

Level 1 Function Block: Auxiliary Support System

Level 1 Function: Support facility operations
Parent Level 0 Function Block: Commercial Fusion Power Plant

This function encompasses all general facility functions that are required to support the commercial fusion facility functions of producing thermal energy from fusion reactions (Fusion Power System) and converting that thermal energy into electrical energy (Balance of Plant System). This function block consists of systems, structures, components, and organizations needed to facilitate operation. This function block is technology and facility agnostic, and is applicable to any approach to commercial fusion power production. Further decomposition of this function block at higher levels is required to provide actual insight into the required sub-functions of this function block and other relationships.

Level 1 Function Block Inputs and Outputs

These inputs and outputs for the model are consistent between all model levels but may have additional detail provided based on the definition of other function blocks for higher level models. The connection of the inputs and outputs to the Level 1 Function Blocks is described in Table 2.3.

Table 2.3. Level 1 Model System Boundary Inputs and Outputs

Inputs	*Function Block*	*Rationale*
Fusion Fuel	Auxiliary Support System	Interface system for incoming plant consumables
Misc. Consumables	Auxiliary Support System	Interface system for incoming plant consumables
Heat Sink Cooling	Balance of Plant System	Required for electric power generation systems

Outputs	*Function Block*	*Rational*
Electrical Energy	Balance of Plant System	Produced by electric power generation systems
Gas/Liquid Effluents	Auxiliary Support System	Interface system for use of processing waste, effluents
Other Process Waste	Auxiliary Support System	Interface system for use of processing waste, effluents

In the Level 1 Model, the Auxiliary Support System Function Block serves as the primary interface system for inputs and outputs to the model. This function block incorporates all functions not directly related to production of heat from fusion reactions and conversion of fusion heat to electricity.

Level 1 Function Block Relationships

The connection relationships between the function blocks describe the transfer of physical or non-physical entities between systems. Table 2.4 describes the connections between function blocks.

Table 2.4. Level 1 Function Model Relationship

Function Block Producer	*Transfer Relationship*	*Function Block Receiver*	*Rationale*
Fusion Power Systems	Thermal Energy	Balance of Plant Systems	Produced by thermal reactions for electric energy conversion
	Reaction Byproducts	Auxiliary Support Systems	Removal of byproducts for steady state operation
Balance of Plant Systems	Electrical Energy	Auxiliary Support Systems	Electric energy diverted for facility house loads
Auxiliary Support Systems	Fusion Fuel	Fusion Power Systems	Pathway for fusion reaction consumables
	Electrical Energy		Electric energy supplied through support system
	Misc. Utilities		Process gas and water, other needed utilities
Auxiliary Support Systems	Misc. Utilities	Balance of Plant Systems	Process gas and water, other needed utilities

In the Level 1 model, the initial decomposition still shows significant relationships between the three function blocks. This model level is highly interrelated with changes in one system significantly affecting the other two.

Level 1 Function Block Decomposition

The three Level 1 Function Blocks are decomposed into functions that fully encompass the Level 1 functions and allocated to create the Level 2 Function Blocks. Table 2.5 provides the decomposition of the function and the allocation of the decomposed functions to new function blocks for the Level 2 function model.

Table 2.5. Level 1 Function Model Decomposition

Level 1 Function Block	*Function*	*Decomposed Function*	*Level 2 Function Block*
Fusion Power System	Produce heat from fusion reactions	Control, contain, and sustain fusion reactions	Fusion Reactor System
		Provide fuel for fusion reactions	Fusion Reactor Fueling System
		Convert fusion reaction byproducts into heat	Fusion Energy Extraction System
		Process/recycle exhaust/byproducts from fusion reactions	Fusion Exhaust Processing System
Balance of Plant System	Convert heat into electricity	Transfer heat from Fusion Power System to working fluid	BOP Heat Transfer System
		Extract thermal energy from working fluid to spin turbine, generator	BOP Turbine-Generator System
		Close thermodynamic cycle by rejecting waste heat, resetting working fluid state	BOP Thermodynamic System
Auxiliary Support System	Support facility operations	Handle fuel preparation, storage, production, and processing	Fuel Handling System
		Process plant exhaust, working fluids, waste, and effluents	Facility Waste Processing System
		Provide for maintenance, repair, and replacement of plant systems	Facility Maintenance System
		Protect, contain, and provide external environmental and process controls for plant systems	Facility Structural/ Utility System
		Provide for safety, security, and reliable operation of plant systems	Site Control/Operation System

The Level 1 function decomposition is intentionally broad and technology agnostic. Each of the three Level 1 Function Blocks (and underlying functions) are decomposed into between three and five Level 2 function requirements and Level 2 Function Blocks. This decomposition, while still technology agnostic, begins to provide actual insights into the major function blocks that would be present in commercial fusion power plants.

2.2.2 Level 2 Function Model for Commercial Fusion

The Level 2 function model decomposes the Level 1 Function Block into twelve Level 2 Function Blocks. The Level 2 function model is shown in Figure 2.3.

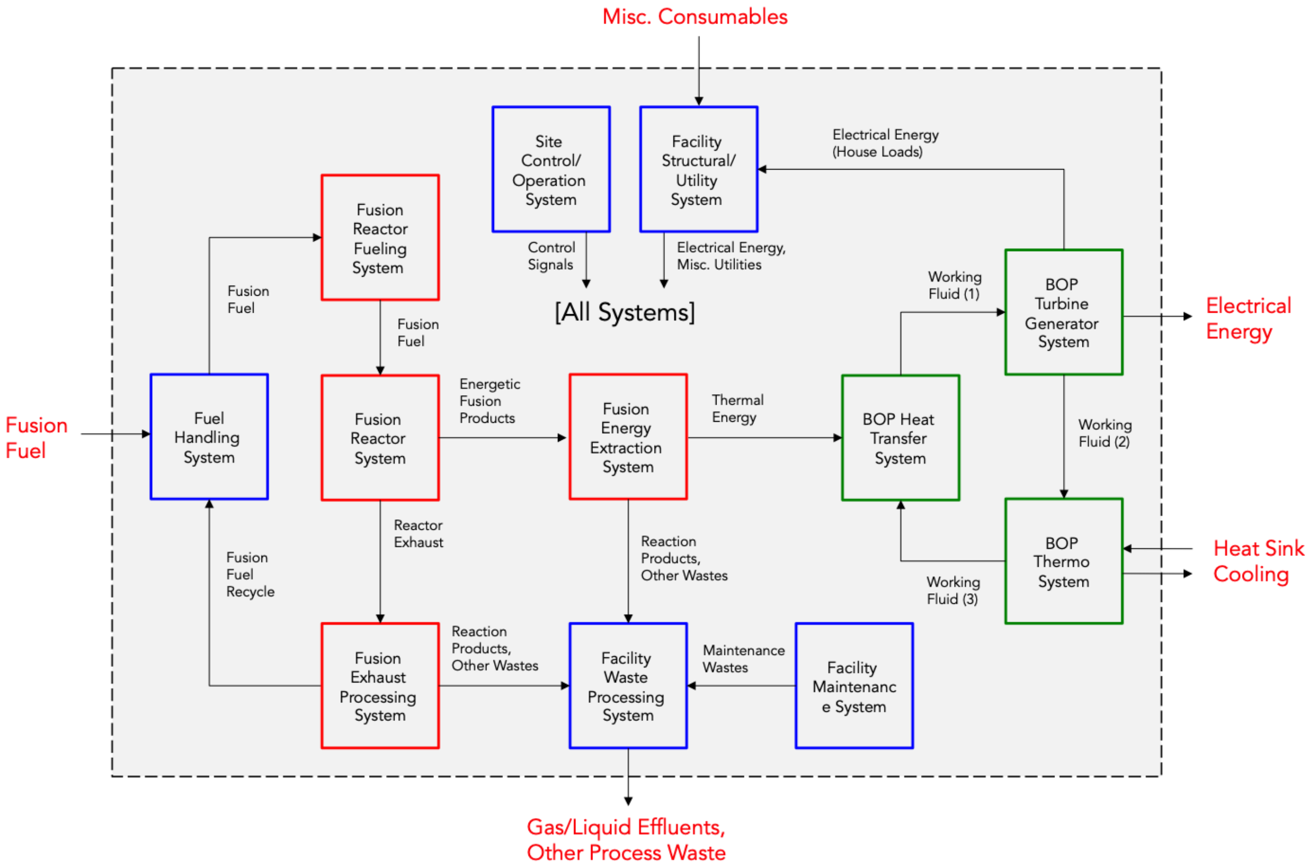

Misc. Consumables
Site Control/ Operation System
Facility Structural/ Utility System
Electrical Energy (House Loads)
Fusion Reactor Fueling System
Control Signals
Electrical Energy, Misc. Utilities
[All Systems]
Working Fluid (1)
BOP Turbine Generator System
Electrical Energy
Fusion Fuel
Fusion Fuel
Fusion Fuel
Fuel Handling System
Fusion Reactor System
Energetic Fusion Products
Fusion Energy Extraction System
Thermal Energy
BOP Heat Transfer System
Working Fluid (2)
BOP Thermo System
Heat Sink Cooling
Reactor Exhaust
Reaction Products, Other Wastes
Fusion Fuel Recycle
Working Fluid (3)
Fusion Exhaust Processing System
Reaction Products, Other Wastes
Facility Waste Processing System
Maintenance Wastes
Facility Maintenanc e System
Gas/Liquid Effluents, Other Process Waste

Figure 2.3. Level 2 Commercial Fusion Function Model

This Level 2 model shown in Figure 2.3 consists of twelve defined function blocks. In this section, detailed descriptions of each Level 2 Function Blocks are provided. Justification for connection of the system inputs and outputs to function blocks is given in Table 2.6, the relationships between function blocks is described in Table 2.7, and the Level 2 model is functionally decomposed in Table 2.8.

Level 2 Function Block Descriptions

Level 2 Function Block: Fusion Reactor System

Level 2 Function: Control, contain, and sustain fusion reactions
Parent Level 1 Function Block: Fusion Power System

This function encompasses the core of the Level 1 function for the Fusion Power System. This function block consists of the systems, structures, and components needed to control, contain, and sustain fusion reactions. This block is technology agnostic and is applicable to any approach to commercial fusion power production. Further decomposition of this function block at higher levels will provide greater differentiation of the required sub-functions to control, contain, and sustain fusion reactions.

Level 2 Function Block: Fusion Reactor Fueling

Level 2 Function: Provide fuel for fusion reactions
Parent Level 1 Function Block: Fusion Power System

This function is separately decomposed from other functions due to known challenges associated with fueling of fusion devices, and the ability to separate the technology approach used for fueling system from the technology approach used in the Fusion Reactor System. This allows the separation of fusion reactor hazard analysis from the general fuel cycle choices made for a specific commercial application. This function block acts as an intermediary between the Level 1 Auxiliary Systems (where fuel is handled) and the Level 2 Fusion Reactor System (where fuel is used).

Level 2 Function Block: Fusion Energy Extraction System

Level 2 Function: Convert fusion reaction byproducts into heat
Parent Level 1 Function Block: Fusion Power System

This function is a key intermediary function that connects the Level 2 Fusion Reactor System (where fusion reactions take place) to the Level 1 Balance of Plant System (where thermal energy is converted into electrical energy). Again, this function block is technology agnostic and does not prescribe form or technology solutions. The fusion reaction byproducts could include neutral particles, charged particles, or photon radiation produced by confined plasma. This function block does, however, assume that a thermodynamic power cycle is used to convert fusion energy into electrical energy via thermal energy, and that direct energy conversion of fusion reaction products is not utilized.

Level 2 Function Block: Fusion Exhaust Processing System

Level 2 Function: Process/recycle exhaust/byproducts from fusion reaction
Parent Level 1 Function Block: Fusion Power System

In any steady state or pulsed commercial fusion facility, byproducts and unused fuel from the Fusion Reactor System must be processed or recycled. This function block is an intermediary that connects the Level 2 Fusion Reactor System (where fusion reactions take place) to the Level 1 Auxiliary System (were fuels and wastes are processed and handled). This function block allows for both open and closed exhaust handling systems, utilizing continuous or batch processing methods.

Level 2 Function Block: BOP Heat Transfer System

Level 2 Function: Transfer heat from Fusion Power System to working fluid
Parent Level 1 Function Block: Balance of Plant System

This function serves as the interface between the Level 2 BOP Turbine-Generator System (where thermal energy is converted into electrical energy) and the Level 1 Fusion Power System (where fusion reactions take place and are converted into thermal energy). This function is technology agnostic, allowing for the analysis of any thermodynamic cycle (e.g., Rankine Cycle, Brayton Cycle, etc.) but does assumes that a working fluid is used energy conversion. The function block may consist of a single system or structure directly coupled with the Level 2 Fusion Energy Extraction System, or consist of multiple system or structures that use intermediate heat transfer loops and heat exchangers to transfer heat to the thermodynamic working fluid.

Level 2 Function Block: BOP Turbine-Generator System

Level 2 Function: Extract thermal energy from working fluid to spin turbine, generator
Parent Level 1 Function Block: Balance of Plant System

This Function Block provides the essential function for the Level 0 Model Function – "Produce net electricity". Mechanical energy is extracted from the working fluid via a turbine, and this mechanical energy is converted to electricity via the generator. This electricity is then provided to power both internal plant systems (e.g., "house loads") and supplied externally directly to users or the grid. The net electrical generation is defined as the total electric power minus the house loads. For the system to satisfy the basic function of "produce net electricity" required house loads must be smaller than total electric power generation. The house loads are served by interface between the Level 2 BOP Turbine-Generator System (where thermal energy is converted into electrical energy) and the Level 1 Auxiliary System (where system support functions and utilities are managed for all other plant systems).

In this model, it is assumed that the BOP Turbine-Generator System is used to power house loads. This allows the plant to operate independently of an external electric grid. For a variety of technical and engineering reasons, some facilities may choose to have house loads powered directly by an external grid and not powered by the BOP Turbine-Generator System. This model of design is still compatible with this system model, but would require an additional external input to the Level 0 Model (and all higher level models of "Electricity") that would then be distributed to the house loads. For the purpose of this system model, it is assumed that external electricity would be routed though the BOP Turbine-Generator System to the Level 1 Auxiliary System for further distribution.

Level 2 Function Block: BOP Thermodynamic System

Level 2 Function: Close thermodynamic cycle by rejecting waste heat, resetting working fluid state
Parent Level 1 Function Block: Balance of Plant System

This function block is a general representation of the systems required to facilitate the remainder of a thermodynamic power cycle. This will include an interface to reject waste heat to the environment and other any systems needed to prepare the working fluid for heat transfer from the Level 2 BOP Heat Transfer System (e.g., working fluid compression before heating). This function block is thermodynamic cycle neutral, allowing any thermodynamic cycles (e.g., Rankine Cycle, Brayton Cycle, etc.) in open and closed thermodynamic cycle configurations.

Level 2 Function Block: Fuel Handling System

Level 2 Function: Handle fuel preparation, storage, production, and processing
Parent Level 1 Function Block: Auxiliary Support System

This function block is the support system that handles the external system input of "fusion fuel" and contains all the necessary functions to handle, prepare, store, and produce fuel for use in the Fusion Power System. This function block is the key input to the Level 1 Fusion Power System (where fuel is used). This function is technology and fuel cycle analysis specific. This block allows for any fuel technology, open or close fuel cycles, and on- or off-site fuel production. Function is separated into the Level 1 Auxiliary Support System to recognize the hazard and process differences between fuel management and fuel utilization.

Level 2 Function Block: Facility Waste Processing System

Level 2 Function: Process plant exhaust, working fluids, waste, and effluents
Parent Level 1 Function Block: Auxiliary Support System

This function block serves as the processing and handling system for all plant systems. This can include gaseous, liquid, and solid waste streams. Processing may include clean-up and recycling of wastes or packaging for disposal. This function block is an interface between all plant systems and the external system output of gas/liquid effluents released by the plant to the environment, and other process wastes.

Level 2 Function Block: Facility Structural/Utility System

Level 2 Function: Protect, contain, and provide external environmental and process controls for plant systems
Parent Level 1 Function Block: Auxiliary Support System

This function block is an intermediary that satisfies common operational requirements for all other plant systems. This Function Block receives external input of Miscellaneous Consumables (e.g., processes gasses, liquids, substances, components) and distributes them (continuously or in batch form) to plant systems. This function block also is responsible for receiving electricity from the Level 1 Balance of Plant System and distributing the electricity to plant systems. Finally, this function block would also incorporate building structures needed to support system and component level operations.

Level 2 Function Block: Facility Maintenance System

Level 2 Function: Provide for maintenance, repair, and replacement of plant systems
Parent Level 1 Function Block: Auxiliary Support System

This function block is a general interface to all systems and provides for the continued plant operation. This function block interfaces with the Level 2 Facility Utility System to receive consumables for use in maintenance activities and send waste streams for processing. The Functions required in this function block are more general than other plant systems and are decomposed generally into common industry functional groups.

Level 2 Function Block: Site Control/Operation System

Level 2 Function: Provide for safety, security, and reliable operation of plant systems
Parent Level 1 Function Block: Auxiliary Support System

This Function Block is a general interface to all systems and provides for the overall plant operations. This Function Block interfaces with all plant systems for control and additionally incorporates larger plant required functions related to security and operator safety. The Functions required in this Function Block are more general than other plant systems and are decomposed generally into common industry functional groups.

Level 2 Function Block Inputs and Outputs

These inputs and outputs for the model are consistent between all model levels. The connection of the inputs and outputs to the Level 2 Function Blocks is described in Table 2.6.

Table 2.6. Level 2 Model System Boundary Inputs and Outputs

Inputs	*Function Block*	*Rationale*
Fusion Fuel	Fuel Handling Systems	Interface system for fuel and fuel production components
Misc. Consumables	Facility Structural / Utility System	Interface system for incoming plant consumables
Heat Sink Cooling	Balance of Plant Thermodynamic System	Required for electric power generation systems

Outputs	*Function Block*	*Rational*
Electrical Energy	Balance of Plant Turbine Generator System	Produced by electric power generation systems
Gas/Liquid Effluents	Facility Waste Processing System	Interface system for use of processing waste, effluents
Other Process Waste	Facility Waste Processing System	Interface system for use of processing waste, effluents

In the Level 2 Model, the model inputs and outputs are assigned accordingly to the decomposed Level 1 systems. The Level 1 Auxiliary Support Systems Function Block has been decomposed into multiple functions and systems, with two larger systems (Facility Structural / Utility System and Facility Waste Processing System) still serving as general interfaces for model inputs and outputs.

Level 2 Function Block Relationships

The connection relationships between the function blocks describe the transfer of physical or non-physical entities between systems. Table 2.7 describes the connections between function blocks.

Table 2.7. Level 2 Function Model Relationship

Function Block Producer	*Transfer Relationship*	*Function Block Receiver*	*Rationale*
Fusion Reactor Fueling System Fusion Reactor System	Fusion Fuel	Fusion Reactor System	Fuel in final form and properly input into the Fusion Reactor System
	Reactor Exhaust	Fusion Exhaust Processing System	Material removed from device to enable steady state operation
	Energetic Fusion Products	Fusion Energy Extraction System	Neutral or charged particles that can be captured to transfer energy
Fusion Energy Extraction System	Thermal Energy	BOP Heat Transfer System	Thermal energy from captured from energetic particles needs to be transferred to thermodynamic cycle
	Reaction Products	Facility Waste Processing System	Useful products of energy extraction that may be used for facility operation (e.g., bred tritium)
	Other Wastes Streams	Facility Waste Processing System	Material removed from system to enable steady state operation
Fusion Exhaust Processing System	Fusion Fuel Recycle	Fuel Handling System	Unburned fusion fuel removed from fusion exhaust and recycled for continuous operation
	Reaction Products	Facility Waste Processing System	Useful reaction products that may be used for facility operation (e.g., He)
	Other Wastes Streams	Facility Waste Processing System	Material removed from system to enable steady state operation
BOP Heat Transfer System	Working Fluid (1)	BOP Turbine-Generator System	Working fluid post heating (energy input) to transfer thermal energy through power cycle
BOP Turbine-Generator System	Working Fluid (2)	BOP Thermodynamic System	Working fluid post mechanical energy extraction (expansion) to cool and close cycle
	Electrical Energy (House Loads)	Facility Structural / Utility System	Electrical energy distributed to run internal facility systems

Table 2.7. Level 2 Function Model Relationship

Function Block Producer	*Transfer Relationship*	*Function Block Receiver*	*Rationale*
BOP Thermodynamic System	Working Fluid (3)	BOP Heat Transfer System	Working fluid post cooling and compression to reset thermodynamic cycle for heating
Fuel Handling System	Fusion Fuel	Fusion Reactor Fueling System	Send fusion fuel in final form to Fusion Reactor Fuel System for fueling
Facility Maintenance System	Maintenance Wastes	Facility Waste Processing System	Radiological or non-radiological wastes produced by maintenance activities
Facility Structural / Utility System	Electrical Energy	All Systems	Electrical energy distributed to all plant structures, systems, and components
	Misc. Utilities	All Systems	Utilities (process fluids, consumables) distributed to all plant structures, systems, and components
Site Control/Operation System	Control Signals	All Systems	Centralized distribution of control signals for all plant activities, structures, systems, and components

In the Level 2 Model, the relationships between function blocks show the emergence of three plant "areas" that differ slightly from three function blocks used in the Level 1 Model. Three of function blocks decomposed from the Level 1 Auxiliary Support System Function Block (Fuel Handling System, Facility Waste Process System, and Facility Maintenance System) show close relationships with the Level 1 Fusion Power System Function Block while the remaining two decomposed Function Blocks (Site Control/Operation System and Facility/Structural Utility System) are largely separated and connected to all plant systems.

Level 2 Function Block Decomposition

The Level 2 Function Blocks are decomposed into functions that fully encompass the Level 2 function and used to create the Level 3 Function Blocks. The Level 2 function decomposition remains technology agnostic but approaches the limit for a System Model without beginning to assign form or technology to different function blocks. Each of the Level 2 Function Blocks (and underlying functions) are decomposed in detail below into between two and five Level 3 functions and function Blocks. Table 2.8 provides the decomposition of the function and the assignment of the decomposed functions to new function blocks for the Level 3 function model. Detailed descriptions of these Level 3 Function Blocks is provided in Section 2.2.4.

Table 2.8. Level 2 Function Model Decomposition

Level 2 Function Block	*Function*	*Decomposed Function*	*Level 3 Function Block*
Fusion Reactor Fueling System	Provide fuel and heating to sustain fusion reactions	Provide fuel to sustain fusion reactions	Plasma Fueling System
		Provide auxiliary heating to start or sustain fusion reactions	Plasma Heating System
		Provide means to defuel or shutdown fusion reactions	Plasma/Fusion Shutdown System
Fusion Reactor System	Control, contain, and confine fusion reactions	Control fusion reactions in the plasma	Plasma Control System
		Actively confine fusion reactions and plasma	Plasma Confinement System
		Passively contain fusion reactions, plasma, and byproducts	Fusion Reactor Vessel System
		Maintain fusion reactor internal conditions	Fusion Reactor Vessel Environmental System
Fusion Energy Extraction System	Convert fusion reaction products into heat	Capture kinetic or radiative energy of fusion reaction products	Fusion Energy Capture System
		Transfer energy into thermal system	Thermal Energy Conversion System
		Capture and contain fusion reaction products or activated materials	Fusion Energy Conversion Containment System
Fusion Exhaust Processing System	Process/recycle exhaust/products from fusion reactions	Remove fusion products and other wastes from fusion reactor system	Fusion Exhaust Removal System
		Separate fusion fuel from other waste streams	Fusion Exhaust Processing System
		Process/purify fusion fuel for individual fusion steam recycling	Fusion Fuel Recycling System
BOP Heat Transfer System	Transfer heat from Fusion Power System to working fluid	Transfer thermal energy into system working fluid	BOP Heat Exchanger System
		Remove excess thermal energy during shutdown	BOP Shutdown Heat Removal System
BOP Turbine-Generator System	Extract thermal energy from working fluid to	Convert thermal energy into mechanical energy	BOP Turbine System
		Convert mechanical energy into	BOP Generator System

Table 2.8. Level 2 Function Model Decomposition

Level 2 Function Block	*Function*	*Decomposed Function*	*Level 3 Function Block*
	spin turbine, generator	electrical energy	
		Distribute electrical energy to grid and plant systems	BOP Electrical Distribution System
BOP Thermodynamic System	Close thermodynamic cycle by rejecting waste heat, resetting working fluid state	Reject waste heat to environment	BOP Ultimate Heat Sink System
		Compress working fluid before heating	BOP Pump Compressor System
		Maintain working fluid chemistry	BOP Chemistry Control System
Fuel Handling System	Handle fuel preparation, storage, production, and processing	Produce or receive fusion fuel	Fusion Fuel Production/Receiving System
		Process or separate fusion fuel into usable form	Fusion Fuel Processing System
		Store reserve or backup separated fusion fuel	Fusion Fuel Storage System
		Prepare fusion fuel into final form for reactor fueling	Fusion Fuel Preparation System
Facility Waste Processing System	Process plant exhaust, working fluids, waste, and effluents	Process and purify process gas and liquid waste streams	Process Fluid Handling System
		Handle non-contaminated waste streams	Waste Handling System
		Handle radiological contaminated waste streams	Radiological Waste Handling System
		Control release of effluents to environment	Effluent Release System
		Prepare waste streams for off-site disposal	Waste Disposal System
Facility Maintenance System	Provide for maintenance, repair, and replacement of plant systems	Maintain and repair plant systems, structures, and components	Plant Maintenance Systems/Org
		Maintain and repair contaminated plant systems, structures, and components	Plant Radiological Maintenance Systems/Org
		Replace plant systems, structures, and components	Plant Infrastructure Replacement System/Org
Facility Utility System	Protect, contain, and provide external environmental and process controls for plant systems	Provide process gas, liquid, electricity for plant systems	Plant Utility Systems
		Contain gas, liquid emissions from plant systems	Plant Emission Control Systems
		Protect plant systems from external threats or conditions	Plant Structural Systems
		Maintain necessary environmental conditions for plant systems	Plant Environmental Control Systems
Site Control/ Operation	Provide for safety, security,	Provide control actions for all plant systems and operations	Plant Operations Control System/Org

Table 2.8. Level 2 Function Model Decomposition

Level 2 Function Block	*Function*	*Decomposed Function*	*Level 3 Function Block*
System	and reliable operation of plant systems	Provide security for operations of plant systems against internal, external threats	Plant Security Systems/Org
		Ensure safe and reliable operation of all plant systems during all conditions	Plant Engineering and Safety System/Org

2.2.4 Level 3 Function Model for Commercial Fusion

The Level 3 function model decomposes the Level 2 Function Block into forty Level 3 Function Blocks. The Level 3 function model is shown in Figure 2.4. Three detailed views of the full Level 3 function model are provided as insets in Figure 2.4a, 2.4b, and 2.4c. Detailed descriptions of each Level 3 Function Blocks are developed and provided in this section. Justification for connection of the system inputs and outputs to Function Blocks is given in Table 2.9 and the relationships between function blocks is described in Table 2.10. Finally, general insights into the characteristics of a commercial fusion power plant based on the Level 3 function model are presented and discussed.

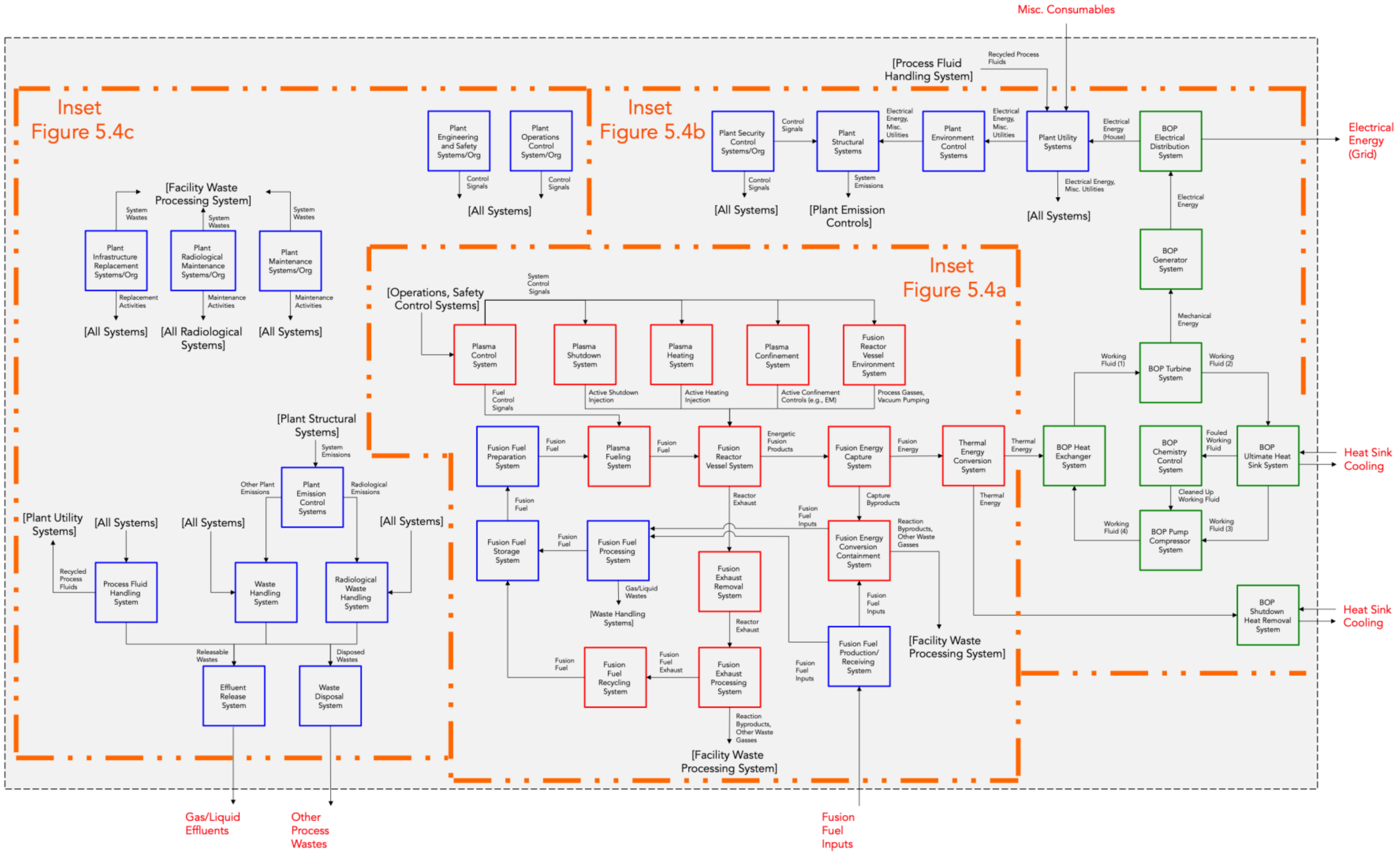

Misc. Consumables
[Process Fluid Handling System]
Recycled Process Fluids
Electrical Energy (Grid)
Inset Figure 5.4c
Inset Figure 5.4b
Inset Figure 5.4a
Plant Engineering and Safety Systems/Org
Plant Operations Control System/Org
Control Signals
Control Signals
[All Systems]
[Facility Waste Processing System]
System Wastes
System Wastes
System Wastes
Plant Infrastructure Replacement Systems/Org
Plant Radiological Maintenance Systems/Org
Plant Maintenance Systems/Org
Replacement Activities
Maintenance Activities
Maintenance Activities
[All Systems]
[All Radiological Systems]
[All Systems]
Plant Security Control Systems/Org
Control Signals
Plant Structural Systems
Electrical Energy, Misc. Utilities
Plant Environment Control Systems
Electrical Energy, Misc. Utilities
Plant Utility Systems
Electrical Energy (House)
BOP Electrical Distribution System
Control Signals
[All Systems]
System Emissions
[Plant Emission Controls]
Electrical Energy, Misc. Utilities
[All Systems]
Electrical Energy
BOP Generator System
Mechanical Energy
[Operations, Safety Control Systems]
System Control Signals
Plasma Control System
Plasma Shutdown System
Plasma Heating System
Plasma Confinement System
Fusion Reactor Vessel Environment System
Fuel Control Signals
Active Shutdown Injection
Active Heating Injection
Active Confinement Controls (e.g., EM)
Process Gasses, Vacuum Pumping
Working Fluid (1)
BOP Turbine System
Working Fluid (2)
[Plant Structural Systems]
System Emissions
Fusion Fuel Preparation System
Fusion Fuel
Plasma Fueling System
Fusion Fuel
Fusion Reactor Vessel System
Energetic Fusion Products
Fusion Energy Capture System
Fusion Energy
Thermal Energy Conversion System
Thermal Energy
BOP Heat Exchanger System
BOP Chemistry Control System
Fouled Working Fluid
BOP Ultimate Heat Sink System
Heat Sink Cooling
Other Plant Emissions
Plant Emission Control Systems
Radiological Emissions
Fusion Fuel
Reactor Exhaust
Capture Byproducts
Thermal Energy
Cleaned Up Working Fluid
Fusion Fuel Inputs
[Plant Utility Systems]
[All Systems]
[All Systems]
[All Systems]
Fusion Fuel Storage System
Fusion Fuel
Fusion Fuel Processing System
Fusion Energy Conversion Containment System
Reaction Byproducts, Other Waste Gasses
Working Fluid (4)
BOP Pump Compressor System
Working Fluid (3)
Recycled Process Fluids
Process Fluid Handling System
Waste Handling System
Radiological Waste Handling System
Gas/Liquid Wastes
[Waste Handling Systems]
Fusion Exhaust Removal System
Fusion Fuel Inputs
BOP Shutdown Heat Removal System
Heat Sink Cooling
Reactor Exhaust
Fusion Fuel Production/ Receiving System
[Facility Waste Processing System]
Releasable Wastes
Disposed Wastes
Fusion Fuel
Fusion Fuel Recycling System
Fusion Fuel Exhaust
Fusion Exhaust Processing System
Fusion Fuel Inputs
Effluent Release System
Waste Disposal System
Reaction Byproducts, Other Waste Gasses
[Facility Waste Processing System]
Gas/Liquid Effluents
Other Process Wastes
Fusion Fuel Inputs

Figure 2.4. Level 3 Commercial Fusion Function Model

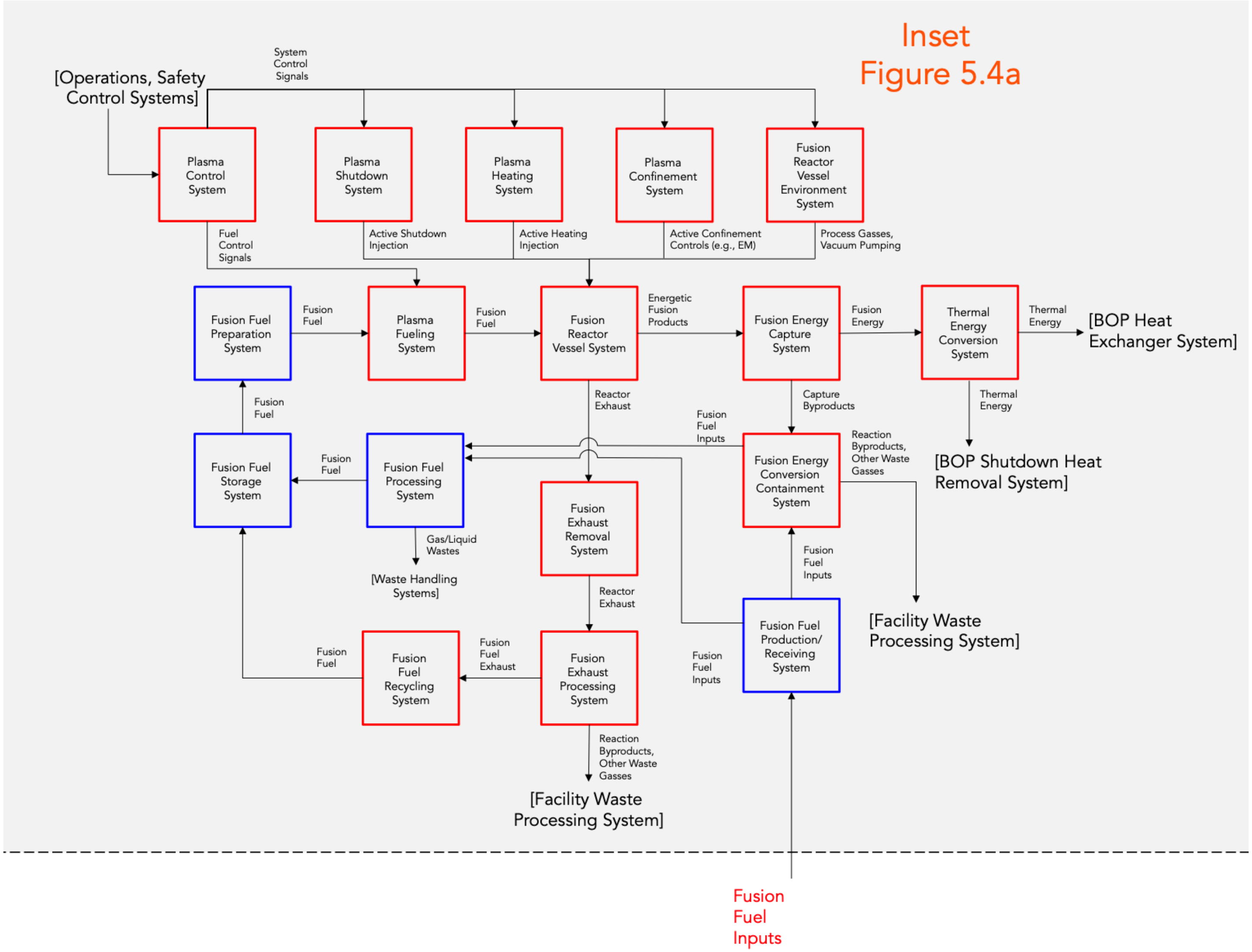

Inset
Figure 5.4a
[Operations, Safety Control Systems]
System Control Signals
Plasma Control System
Plasma Shutdown System
Plasma Heating System
Plasma Confinement System
Fusion Reactor Vessel Environment System
Fuel Control Signals
Active Shutdown Injection
Active Heating Injection
Active Confinement Controls (e.g., EM)
Process Gasses, Vacuum Pumping
Fusion Fuel Preparation System
Fusion Fuel
Plasma Fueling System
Fusion Fuel
Fusion Reactor Vessel System
Energetic Fusion Products
Fusion Energy Capture System
Fusion Energy
Thermal Energy Conversion System
Thermal Energy
[BOP Heat Exchanger System]
Fusion Fuel
Reactor Exhaust
Fusion Fuel Inputs
Capture Byproducts
Thermal Energy
[BOP Shutdown Heat Removal System]
Fusion Fuel Storage System
Fusion Fuel
Fusion Fuel Processing System
Fusion Exhaust Removal System
Fusion Energy Conversion Containment System
Reaction Byproducts, Other Waste Gasses
Gas/Liquid Wastes
[Waste Handling Systems]
Reactor Exhaust
Fusion Fuel Inputs
[Facility Waste Processing System]
Fusion Fuel
Fusion Fuel Recycling System
Fusion Fuel Exhaust
Fusion Exhaust Processing System
Fusion Fuel Inputs
Fusion Fuel Production/ Receiving System
Reaction Byproducts, Other Waste Gasses
[Facility Waste Processing System]
Fusion Fuel Inputs

Figure 2.4a. Level 3 Commercial Fusion Function Model System Part A Inset

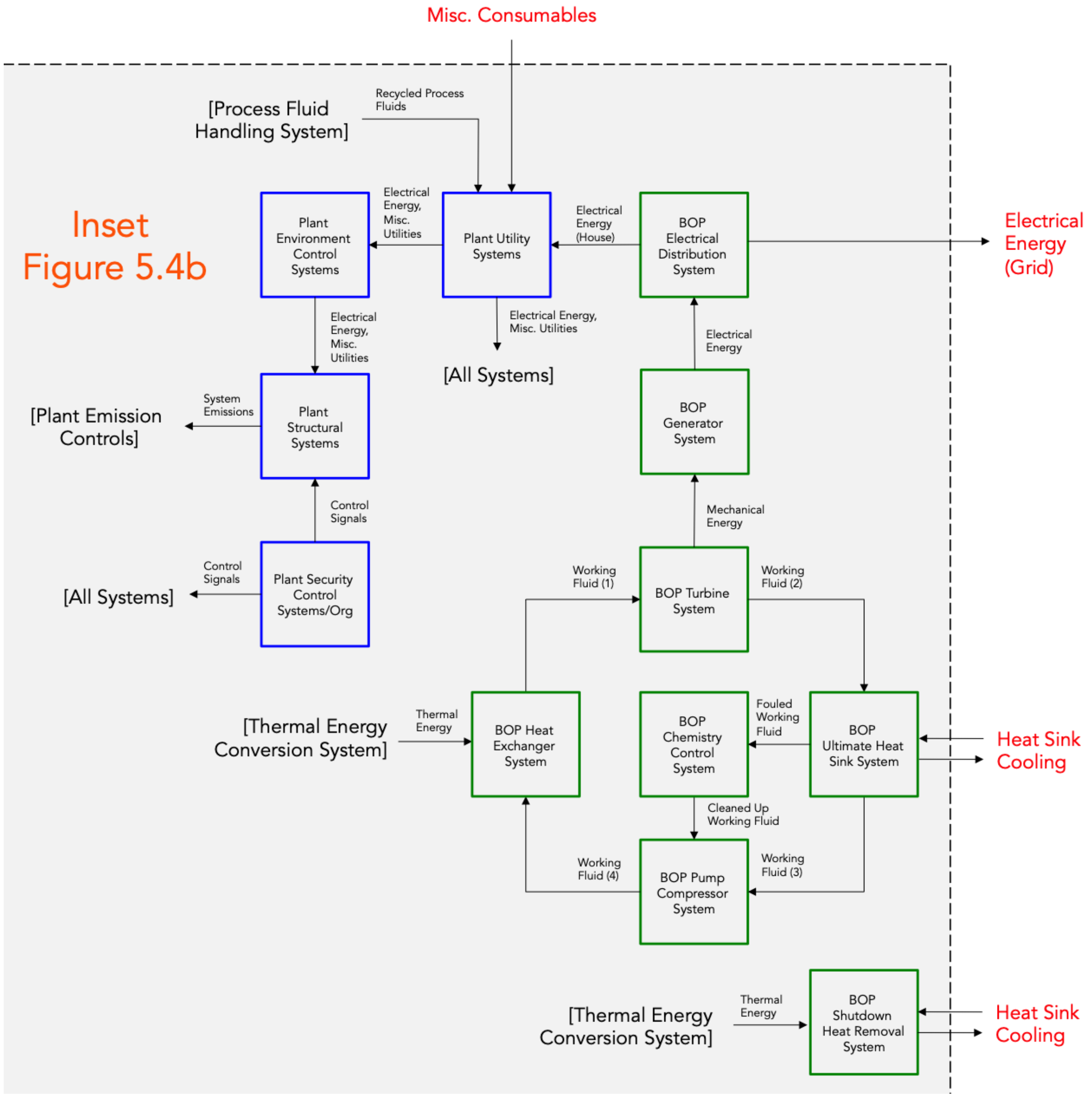

Misc. Consumables
[Process Fluid Handling System]
Recycled Process Fluids
Inset Figure 5.4b
Plant Environment Control Systems
Electrical Energy, Misc. Utilities
Plant Utility Systems
Electrical Energy (House)
BOP Electrical Distribution System
Electrical Energy (Grid)
Electrical Energy, Misc. Utilities
Electrical Energy, Misc. Utilities
[All Systems]
Electrical Energy
[Plant Emission Controls]
System Emissions
Plant Structural Systems
BOP Generator System
Control Signals
Mechanical Energy
Control Signals
[All Systems]
Plant Security Control Systems/Org
Working Fluid (1)
BOP Turbine System
Working Fluid (2)
[Thermal Energy Conversion System]
Thermal Energy
BOP Heat Exchanger System
BOP Chemistry Control System
Fouled Working Fluid
BOP Ultimate Heat Sink System
Heat Sink Cooling
Cleaned Up Working Fluid
Working Fluid (4)
BOP Pump Compressor System
Working Fluid (3)
[Thermal Energy Conversion System]
Thermal Energy
BOP Shutdown Heat Removal System
Heat Sink Cooling

Figure 2.4b. Level 3 Commercial Fusion Function Model System Part B Inset

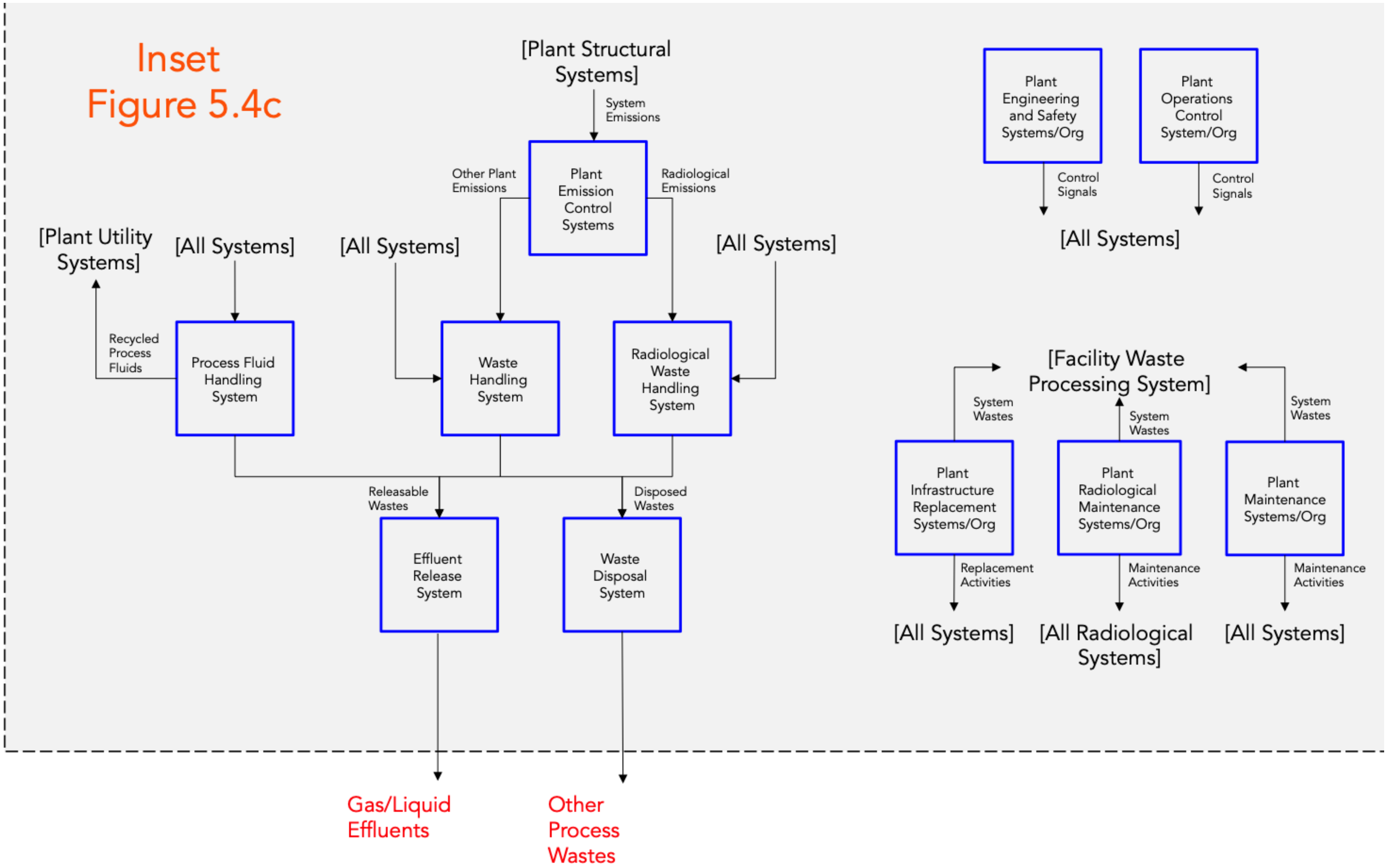


Figure 2.4c. Level 3 Commercial Fusion Function Model System Part C Inset

Level 3 Function Block Descriptions

Level 3 Function Block: Plasma Fueling System

Level 3 Function: Provide fuel to sustain fusion reactions
Parent Level 2 Function Block: Fusion Reactor Fueling System

This function block consists of the physical systems that sustain fusion reactions through continuous or batch fueling systems. This function block is an interface between the Level 2 Fuel Handling System (a Level 1 Auxiliary Support System) and the Fusion Power Systems. This decomposition enables evaluation of the hazards associated with preparation of engineered fusion fuel forms that may be distinctly different from those associated with injection of fuel into the plasma power system. This model assumes that complete fuel forms are provided to the Plasma Fuel System by the Level 3 Fusion Fuel Preparation System.

The Plasma Fueling System is a highly design and technology specific system, varying based on the specific fusion technology used and the fuel cycle configuration. Typical fusion fueling mechanisms could include gas puffing and high speed frozen cylindrical pellet injection for magnetic confinement fusion systems or frozen spherical pellets and hohlraum-target placement for inertial confinement fusion. Other plasma fueling systems may be used, so further decomposition of this function block is limiting in a technology and design agnostic system engineering model.

Level 3 Function Block: Plasma Heating System

Level 3 Function: Provide auxiliary heating to start or sustain fusion reactions
Parent Level 2 Function Block: Fusion Reactor Fueling System

This function block consists of the physical systems that are design to actively heat the fusion plasma. This system may consist of heating to initiate fusion reactions up to point where self-heating from fusion reactions dominate heating (burning plasma conditions) and heating to sustain and control fusion reactions at desired levels (burn control). This function block is decomposed from the Level 2 Fusion Reactor Fueling System Function Block because it provides the necessary inputs to sustain fusion conditions in the plasma.

The Plasma Heating System is a highly design and technology specific system, varying based on the specific fusion technology used and operating configuration. Typical systems for magnetic confinement systems may include current (ohmic) heating, radiofrequency (RF) heating, or neutral beam injection heating. The first two methods are electromagnetic-based while the third method may involve the injection of high energy, neutral fuel particles into the plasma. Typical systems for inertial confinement systems may include pulse laser injection. Other plasma heating systems may be used for different configurations, so further decomposition of this function block is limiting in a technology and design agnostic system engineering model.

Level 3 Function Block: Plasma Shutdown System

Level 3 Function: Provide means to defuel or shutdown fusion reactions
Parent Level 2 Function Block: Fusion Reactor Fueling System

This function block consists of the physical systems that are designed to actively shutdown the fusion reactions within the plasma. This function block is decomposed from the Level 2 Fusion Reactor Fueling System Function Block because of function connection between fueling conditions and plasma shutdown. Multiple methods could be used to passively or actively shutdown a plasma including ceasing fuel injection (passive), ceasing plasma heating (passive for burn controlled plasma or ignited plasma), or injection of impurities into the plasma to disrupt reaction conditions (active). This function block would consist of any active methods used to shutdown fusion reactions within the plasma. A wide variety of active plasma shutdown methods may be used, so further decomposition of this function block is limiting in a technology and design agnostic system engineering model.

Level 3 Function Block: Plasma Control System

Level 3 Function: Control fusion reactions in the plasma
Parent Level 2 Function Block: Fusion Reactor System

This function block consists of the systems that are designed to actively control the plasma conditions within the fusion reactor. Control of fusion plasmas is a multi-dimensional control problem requiring consideration of fueling, heating, confinement, and environmental conditions. This control system does not physically interact with the plasma systems but is the control interface between the Level 2 Site Control/Operation System Function Block (a Level 1 Auxiliary Support System) and the Fusion Power Systems. This function block would provide the necessary coordinated control systems to maintain system operation at desired set points.

Level 3 Function Block: Plasma Confinement System

Level 3 Function: Actively confine fusion reactions and plasma
Parent Level 2 Function Block: Fusion Reactor System

This function block consists of the physical systems that ensure and maintain plasma confinement within the fusion reactor. Plasma confinement is required to both prevent physical interactions between the high temperature plasma and fusion reactor vessels (simultaneously damaging the vessel and degrading the plasma) and to maintain the physical conditions and configurations required for fusion reactions. This function block is decomposed from the Level 2 Fusion Reactor Fueling System Function Block because it enables sustain fusion conditions in the plasma.

The Plasma Confinement System is a highly design and technology specific system, varying based on the confinement approach and machine configuration. For magnetic confinement systems, various high strength magnetic fields produced by electromagnets will be used to ensure plasma confinement and shape or otherwise control the plasma. For inertial confinement systems, the confinement system may be closely coupled with the heating system as the pulsed nature of these devices require simultaneous compression, heating, and confinement of the fusion fuel. Other plasma confinement systems such as electric field confinement may be used for different configurations, so further decomposition of this function block is limiting in a technology and design agnostic system engineering model.

Level 3 Function Block: Fusion Reactor Vessel Environmental System

Level 3 Function: Maintain fusion reactor internal conditions
Parent Level 2 Function Block: Fusion Reactor System

This function block consists of both the physical and control systems required to maintain conditions within the fusion reactor required for fusion reactions. This may include material removal processes such as developing initial vacuum conditions within a plasma vessel or material addition processes such as injection of neutral gasses to mitigate disruptions or otherwise control conditions within the Fusion Reactor Vessel System. In this system engineering model, the process of removing fusion byproducts from the Fusion Reactor Vessel System is separated from the Fusion Reactor Vessel Environmental System. This separation allows more clear delineation of the type and quantity of material processed by different removal systems. The Fusion Reactor Vessel Environmental System will differ significantly based on technology, design, and specific configuration, so further decomposition of this function block is limiting in a technology and design agnostic system engineering model. Further decomposition and specification of subsystems for a technology and specific design system engineering model may be useful at categorizing and assessing particular system hazards.

Level 3 Function Block: Fusion Reactor Vessel System

Level 3 Function: Passively contain fusion reactions, plasma, and byproducts
Parent Level 2 Function Block: Fusion Reactor System

This function block consists of the physical system that contains the plasma during operation and is the "core" of any fusion facility. This function block is a critical system interface between fusion fuel and plasma control related function blocks (system inputs) and reactor exhaust and fusion energy capture related function blocks (system outputs). The decomposition enables evaluation of the hazards associated with the fusion reactions, immediate byproducts, and any material activation or contamination of the reactor vessel system. The Fusion Reactor Vessel System will differ significantly based on technology, design, and specific configuration, so further decomposition of this function block is limiting in a technology and design agnostic system engineering model. Further decomposition and specification of system interfaces for a technology and specific design system engineering model may be useful at categorizing and assessing system hazards.

Level 3 Function Block: Fusion Energy Capture System

Level 3 Function: Capture kinetic or radiative energy of fusion reaction products
Parent Level 2 Function Block: Fusion Energy Extraction System

This function block consists of the physical systems that capture energetic materials emitted by the plasma during operation. Fusion reactions produce a variety of high energy charged and neutral particles, depending primarily on the specific fuel used for the facility. As previously stated for the Level 2 Fusion Energy Extraction System Function Block, this system engineering model assumes that a thermodynamic power cycle is used to convert fusion energy into electrical energy via thermal energy, and that direct energy conversion of fusion reaction products is not utilized. The function block is an important interface converting fusion reaction energy into usable thermal energy. This function block may be integral to the Fusion Reactor Vessel System but is delineated into a separate function due to the system interactions and specific hazards associated with the capture of fusion reaction products. A wide variety of physical mechanisms for the Fusion Energy Capture System are proposed for specific designs (e.g., solid targets, liquid targets) so further decomposition of this function block is limited in a technology and design agnostic system engineering model.

Level 3 Function Block: Thermal Energy Conversion System

Level 3 Function: Transfer energy into thermal system
Parent Level 2 Function Block: Fusion Energy Extraction System

This function block consists of the physical systems that transfer captured thermal energy into a thermal cycle system. This function block is delineated to allow separation and characterization of hazards in a technology agnostic system engineering model. Integration of the Thermal Energy Conversion System functions into either the Fusion Energy Capture System or BOP Heat Exchanger System may occur depending on the specific design and methods used for heat management. Use of intermediate cooling loops or working fluids to transfer energy may result in design specific definition of a Thermal Energy Conversion System while use of direct thermodynamic cycles may result in combination of the Thermal Energy Conversion System and the BOP Heat Exchanger System. Further decomposition of this function block is limited in a technology and design agnostic system engineering model.

Level 3 Function Block: Fusion Energy Conversion Containment System

Level 3 Function: Capture and contain fusion reaction products or activated materials
Parent Level 2 Function Block: Fusion Energy Extraction System

This function block consists of any physical systems required to capture and contain fusion reaction products that leave the Fusion Reactor Vessel System through the Fusion Energy Capture System or byproduct materials resulting from materials interaction, neutron absorption, or secondary reactions. The scope and need for this function block will significantly depend on the specific fusion technology, selection of fusion fuel, fusion fuel cycle, and Fusion Energy Capture System. Fusion facility designs that require the production of fusion fuel via neutron interactions (e.g., tritium production via lithium neutron absorption reactions) may utilize this function block as a primary fuel production system (e.g. in a fuel breeding blanket). The Fusion Energy Conversion Containment System would contain the system systems used to handle fusion fuel inputs, expose fusion fuel inputs to conditions to facilitate nuclear reactions, and separate and output fusion fuel components to other plant systems. This function block is delineated to allow separation and characterization of hazards in a technology agnostic system engineering model. Integration of the Fusion Energy Conversion Containment System function into the Fusion Energy Capture System may occur depending on the specific design and methods used for energetic fusion production management. Further decomposition and specification of system interfaces for a technology and specific design system engineering model may be useful at categorizing and assessing system hazards.

Level 3 Function Block: Fusion Exhaust Removal System

Level 3 Function: Remove fusion products and other wastes from fusion reactor system
Parent Level 2 Function Block: Fusion Exhaust Processing System

This function block consists of the physical systems needed to remove fusion reaction (ash) products, unreacted fusion fuel, or wastes (e.g., processes gasses) from the Fusion Reaction Vessel. The Fusion Exhaust Removal System is responsible for maintaining acceptable conditions in the Fusion Reactor Vessel System through removal of gaseous and mobile impurities that could otherwise disrupt or degrade plasma performance. This system is separated from the Fusion Reactor Vessel Environmental System to allow separate characterization of hazards associated with the handling significant quantities (as compared with residual quantities) of fusion reaction products and unreacted fusion fuel. In many fusion technology configurations, this system will consist of vacuum or other pumping systems but would largely be design specific. Further decomposition of this function block is limited in a technology and design agnostic system engineering model.

Level 3 Function Block: Fusion Exhaust Processing System

Level 3 Function: Separate fusion fuel from other waste streams
Parent Level 2 Function Block: Fusion Exhaust Processing System

This function block consists of the physical systems required to process Fusion Reactor Vessel Exhaust and separate recyclable fusion fuel exhaust from fusion reaction products, process gasses, and other wastes. The design and operation of this function block will differ based on the fusion technology and specific design, resulting in significant differences in terms of characteristics such as exhaust processing methods and throughputs. This function block is limited to the separation of recyclable fusion fuel exhaust from other reactor exhaust products. This delineation allows for the separate analysis of fusion fuel separation processes that may have significant material inventories (e.g., isotopic separation methods). Further decomposition of this function block is limited in a technology and design agnostic system engineering model.

Level 3 Function Block: Fusion Fuel Recycling System

Level 3 Function: Process/purify fusion fuel for individual fusion fuel stream recycling
Parent Level 2 Function Block: Fusion Exhaust Processing System

This function block consists of the physical systems required to process and purify mixed fusion fuel exhaust streams into separated streams usable by the Level 2 Fusion Fuel Handling System (and associated Level 3 systems). This system may consist of isotopic separation systems for elementally identical but isotopically different fusion fuel mixtures (e.g., deuterium and tritium) or chemical separation systems for elementally different fusion fuel mixtures (e.g., deuterium and helium-3). The overall type, required separation fractions, and mass flow rates of separation will vary significantly by design, so further decomposition of this function block is limited in a technology and design agnostic system engineering model. Further decomposition and specification of system interfaces for a technology and specific design system engineering model may be useful at categorizing and assessing system hazards.

Level 3 Function Block: BOP Heat Exchanger System

Level 3 Function: Transfer thermal energy into system working fluid
Parent Level 2 Function Block: BOP Heat Transfer System

This function block consists of physical systems used to transfer thermal energy from fusion energy system to the balance of plant systems via a thermodynamic working fluid. The function block is an important interface between fusion technology specific systems and engineered industrial systems common to other electrical generation technologies. The heat exchangers, working fluids, and other system characteristics will vary significantly by design, so further decomposition of this function block is limited in a technology and design agnostic system engineering model.

Level 3 Function Block: BOP Shutdown Heat Removal System

Level 3 Function: Remove excess thermal energy during shutdown
Parent Level 2 Function Block: BOP Heat Transfer System

This function block consists of physical systems used to transfer residual thermal energy produced during facility shutdown conditions. Thermal energy may be produced in the Level 1 Fusion Power System following plasma shutdown by processes including exothermic chemical reactions or decay of radionuclides. If substantial quantities of thermal energy are released following shutdown of other BOP systems, removal of residual thermal energy would be required to prevent overheating of Fusion Power Systems. This function block is defined as a separate system enabling rejection of residual shutdown thermal energy to the environment. The need, size, and other functional characteristics of this system will vary significantly by design, so further decomposition of this function block is limited in a technology and design agnostic system engineering model.

Level 3 Function Block: BOP Turbine System

Level 3 Function: Convert thermal energy into mechanical energy
Parent Level 2 Function Block: BOP Turbine-Generator System

This function block consists of the physical systems used to convert thermal energy in a working fluid into mechanical energy. This function block is typical of other electrical generation technologies and may consist of a series of gas or steam turbines, as well as other working fluid heat exchanger subsystems used to optimize thermodynamic efficiency of the system. The configuration, sizing, and other specific characteristics will vary significantly by design, so further decomposition of this function block is limited in a technology and design agnostic system engineering model.

Level 3 Function Block: BOP Generator System

Level 3 Function: Convert mechanical energy into electrical energy
Parent Level 2 Function Block: BOP Turbine-Generator System

This function block consists of the physical systems used to convert mechanical energy from the BOP Turbine System into electrical energy. This function block is typical of other electrical generation technologies and may consist of the generator as well as auxiliary cooling and electrical equipment. The configuration, sizing, and other specific characteristics will vary significantly by design, so further decomposition of this function block is limited in a technology and design agnostic system engineering model.

Level 3 Function Block: BOP Electrical Distribution System

Level 3 Function: Distribute electrical energy to grid and plant systems
Parent Level 2 Function Block: BOP Turbine-Generator System

This function block consists of the physical and control systems used to distribute electrical energy from the BOP generator system internally to plant systems and externally to the electrical grid. This function block is typical of other electrical generation technologies and may consist of electrical busses, switchgears, transformers, and other industrial electrical equipment. The configuration, sizing, and other specific characteristics will vary significantly by design, so further decomposition of this function block is limited in a technology and design agnostic system engineering model.

Level 3 Function Block: BOP Ultimate Heat sink System

Level 3 Function: Reject waste heat to environment
Parent Level 2 Function Block: BOP Thermodynamic System

This function block consists of the physical systems used to remove waste heat from the working fluid. This function block is typical of other electrical generation technologies and may consist of heat exchangers or condensers depending on design. This system is the interface to external heat sink cooling and rejection of excess thermal energy to the environment. As a result, it may also include auxiliary pump and flow systems used to transfer heat to the environment. The configuration, sizing, and other specific characteristics will vary significantly by design, so further decomposition of this function block is limited in a technology and design agnostic system engineering model.

Level 3 Function Block: BOP Pump Compressor System

Level 3 Function: Compress working fluid before heating
Parent Level 2 Function Block: BOP Thermodynamic System

This function block consists of the physical systems used to compress and pump the working fluid, completing the thermodynamic cycle. This function block is typical of other electrical generation technologies and may consist of a series of pumps or compressors, as well as other working fluid heat exchanger subsystems used to optimize thermodynamic efficiency of the system. The configuration, sizing, and other specific characteristics will vary significantly by design, so further decomposition of this function block is limited in a technology and design agnostic system engineering model.

Level 3 Function Block: BOP Chemistry Control System

Level 3 Function: Maintain working fluid chemistry
Parent Level 2 Function Block: BOP Thermodynamic System

This function block consists of the physical systems used to maintain the chemistry and purity of the working fluid. Reliable, long term operation of thermodynamic cycles (particularly systems with steam turbines) require highly controlled chemistry to prevent erosion, corrosion, and other degradation mechanisms. This function block is typical of other electrical generation technologies and may consist of a series of pumps, processing subsystems, and storage tanks. The configuration, sizing, and other specific characteristics will vary significantly by design, so further decomposition of this function block is limited in a technology and design agnostic system engineering model.

Level 3 Function Block: Fusion Fuel Production/Receiving System

Level 3 Function: Produce or receive fusion fuel
Parent Level 2 Function Block: Fuel Handling System

This Function Block contains the physical systems used to receive and process external fusion fuel inputs needed for the commercial fusion facility. This system may consist of fusion fuel in a direct usable form, fusion fuel in an unprepared or bulk form, or fusion fuel input materials that need to undergo significant additional processing or nuclear reactions before they are usable in the fusion power plant. This Function Block is auxiliary support system external interface for fusion fuel inputs. Separation of this Function Block enables clarification of external system interfaces separate from chemical or radiological fuel processing systems. Additional interfaces with the Fusion Energy Conversion Containment System or Fusion Fuel Processing System will vary depending on the specific fuel cycle considerations for the facility. Further decomposition of this Function Block is limited in a technology and design agnostic system engineering model.

Level 3 Function Block: Fusion Fuel Processing System

Level 3 Function: Process or separate fusion fuel into usable form
Parent Level 2 Function Block: Fuel Handling System

This function block contains the physical systems used to process fusion fuel inputs into chemical and physical forms suitable for storage or processing by the Level 2 Fusion Reactor Fueling System. This may include external fusion fuel inputs received from the Fusion Fuel Production/Receiving System or internal fusion fuel inputs from the Fusion Energy Conversion Containment System that have undergone additional chemical or nuclear reactions to become usable fusion fuel inputs. This Function Block is the main process system to convert all fusion fuel inputs. The configuration, processes, and other specific characteristics of this system will vary significantly by design and technology, so further decomposition of this function block is limited in a technology and design agnostic system engineering model. Further decomposition and specification of system interfaces for a technology and specific design system engineering model, however, may be useful at categorizing and assessing system hazards.

Level 3 Function Block: Fusion Fuel Storage System

Level 3 Function: Store reserve or backup separated fusion fuel
Parent Level 2 Function Block: Fuel Handling System

This function block contains the physical systems used to store separated and processed fusion fuel before it is prepared for use by the Plasma Fueling System. This may include reserve fuel to account for operational transients in the Fusion Fuel Production/Receiving System or backup fuel to account for operational transients in the Fusion Fuel Recycling System. The design, size, and other specific characteristics of this system will vary significantly by facility design and technology, specifically balancing increased fuel storage requirements with increased robustness against fuel system operational transients. Further decomposition of this function block is limited in a technology and design agnostic system engineering model but analysis technology and specific design system engineering model, however, may be useful at categorizing and assessing specific system hazards.

Level 3 Function Block: Fusion Fuel Preparation System

Level 3 Function: Prepare fusion fuel into final form for reactor fueling
Parent Level 2 Function Block: Fuel Handling System

This function block contains the physical systems used to prepared fuel into the final chemical and physical forms usable by the Plasma Fueling System. This may involve processes such as combining fusion fuels into specific mixtures or manufacturing of solid (i.e., frozen) fuel forms from gaseous fusion fuels. The configuration, processes, and other specific characteristics of this system will vary significantly by design and technology, so further decomposition of this function block is limited in a technology and design agnostic system engineering model. Further decomposition and specification of system interfaces for a technology and specific design system engineering model, however, may be useful at categorizing and assessing system hazards.

Level 3 Function Block: Process Fluid Handling System

Level 3 Function: Process and purify process gas and liquid waste streams
Parent Level 2 Function Block: Facility Waste Processing System

This function block contains the physical systems used to collect and recycle any gas or liquid process fluids used in the facility. For non-consumable or once through fluids, continuous or batch processing may be used to ensure proper fluid characteristics. This system is delineated from other waste handling systems due to the closed system nature typical of process fluid systems. This function block would interface directly (or through intermediate systems) with any facility systems containing process fluids. Separated wastes or non-recoverable fluid streams can be removed from the system and facility through the Effluent Release System or the Waste Disposal System. This function block is typical of industrial facilities but may have technology specific challenges related to process radiologically contaminated process fluids or use of atypical process fluids by plasma control or environmental systems. The configuration, sizing, and other specific characteristics will vary significantly by design, so further decomposition of this function block is limited in a technology and design agnostic system engineering model.

Level 3 Function Block: Radiological Waste Handling System

Level 3 Function: Handle radiological contaminated waste streams
Parent Level 2 Function Block: Facility Waste Processing System

This function block contains the physical systems used to collect and process radiologically contaminated waste streams. Separate consideration of non-radiologically and radiologically waste streams allows separation of the distinct hazards associated with radiological wastes including contamination, worker dose, or production of additional hazards (e.g., radiolytically generated hydrogen gas). This function block would interface directly (or through intermediate systems or organizations) with any facility systems that can produce radiologically contaminated operational or maintenance wastes. Separated wastes would be processed and removed from the facility through the Effluent Release System or the Waste Disposal System. This function block is typical of radiological facilities but may have technology specific challenges related to design specific waste forms or radionuclides. The configuration, sizing, and other specific requirements for this system will vary significantly by facility design, so further decomposition of this function block is limited in a technology and design agnostic system engineering model. Further decomposition and specification of system interfaces for a technology and specific design system engineering model, however, may be useful at categorizing and assessing system hazards.

Level 3 Function Block: Waste Handling System

Level 3 Function: Handle non-contaminated waste streams
Parent Level 2 Function Block: Facility Waste Processing System

This function block contains the physical systems used to collect and process non-radiologically contaminated waste streams. This function block would interface directly (or through intermediate systems or organizations) with any facility systems that can produce operational or maintenance wastes not otherwise handled by facility systems. Separated wastes would be processed and removed from the facility through the Effluent Release System or the Waste Disposal System. This function block is typical of industrial facilities but may have technology specific challenges related to design specific waste streams (e.g., large quantities of beryllium contaminated wastes). The configuration, sizing, and other specific requirements for this system will vary significantly by facility design, so further decomposition of this function block is limited in a technology and design agnostic system engineering model.

Level 3 Function Block: Effluent Release System

Level 3 Function: Control release of effluents to environment
Parent Level 2 Function Block: Facility Waste Processing System

This function block contains the physical systems used to control the release of gaseous and liquid effluents to the environment or sanitary sewers. These effluents may be radiological and non-radiological depending on the emission release limits for the facility.. This function block is the external interface between facility waste systems (Process Fluid Handling System, Waste Handling System, and Radiological Handling System) and off-site effluent sinks. This system controls the release of effluents to ensure that the facility meets the relevant regulatory limits on the concentration and total mass of effluents released by the facility, requiring both process and instrumentation systems. This function block is typical of radiological and industrial facilities but may have technology specific challenges. The configuration, sizing, and other specific requirements for this system will vary significantly by facility design, so further decomposition of this function block is limited in a technology and design agnostic system engineering model.

Level 3 Function Block: Waste Disposal System

Level 3 Function: Prepare waste streams for off-site disposal
Parent Level 2 Function Block: Facility Waste Processing System

This function block contains the physical systems used to prepare releasable waste streams for off-site disposal. This function block is the external interface between facility waste systems (Process Fluid Handling System, Waste Handling System, and Radiological Handling System) and off-site waste facilities. This system would properly package any solid, liquid, or gaseous wastes (both radiological and non-radiological) per regulatory standards for off-site disposal. Some wastes may be packed and stored on site for extended periods up to the duration of facility operation and removed as part of the facility decommissioning process. These operational parameters could decided on a facility by facility or industry wide basis. This function block is typical of radiological and industrial facilities but may have technology specific challenges. The configuration, sizing, and other specific requirements for this system will vary significantly by facility design, so further decomposition of this function block is limited in a technology and design agnostic system engineering model.

Level 3 Function Block: Plant Radiological Maintenance Systems/Org

Level 3 Function: Maintain and repair contaminated plant systems, structures, and components
Parent Level 2 Function Block: Facility Maintenance System

This function block contains the physical systems and organizations needed to maintain and repair plant systems, structures, and components that are radiologically contaminated. Separate consideration of non-radiologically and radiologically maintenance allows separation of the distinct hazards associated with radiological systems including contamination, worker dose, or production of wastes. This function block would interface directly with any radiologically contaminated facility systems and could include separate facilities (e.g., hot cells) for the safe handling, maintenance, or decontamination of radiologically contaminated systems. This function block is typical of radiological and industrial facilities but may have technology specific challenges. The configuration, sizing, and other specific requirements for this system will vary significantly by facility design, so further decomposition of this function block is limited in a technology and design agnostic system engineering model.

Level 3 Function Block: Plant Maintenance Systems/Org

Level 3 Function: Maintain and repair plant systems, structures, and components
Parent Level 2 Function Block: Facility Maintenance System

This function block contains the physical systems and organizations needed to maintain and repair plant systems, structures, and components that are not radiologically contaminated. This function block would interface directly with any non-radiologically contaminated facility systems. This function block is typical of industrial facilities but may have technology specific challenges related to design specific waste streams (e.g., large quantities of beryllium contaminated wastes). The configuration, sizing, and other specific requirements for this system will vary significantly by facility design, so further decomposition of this function block is limited in a technology and design agnostic system engineering model.

Level 3 Function Block: Plant Infrastructure Replacement System/Org

Level 3 Function: Replace plant systems, structures, and components
Parent Level 2 Function Block: Facility Maintenance System

This function block contains the physical systems and organizations needed to replace consumable or life-limited plant systems, structures, and components. This may include interfacing with both non-radiologically and radiologically contaminated facility systems. This function block is typical of radiological and industrial facilities but may have technology specific challenges. The configuration, sizing, and other specific requirements for this system will vary significantly by facility design, so further decomposition of this function block is limited in a technology and design agnostic system engineering model.

Level 3 Function Block: Plant Utility Systems

Level 3 Function: Provide process gas, liquid, electricity for plant systems
Parent Level 2 Function Block: Facility Utility System

This function block consists of the physical systems used to provide operational utilities (process gasses and liquids, and electricity) to all plant systems structures and components. This function block is an interface between the BOP Electrical Distribution System, external facility inputs (e.g., miscellaneous consumables), and all other plant system. The system is typical of industrial facilities but may have design specific requirements based on facility requirements (e.g., large electrical system demands for high-energy systems). The configuration, sizing, and other specific characteristics will vary significantly by design, so further decomposition of this function block is limited in a technology and design agnostic system engineering model.

Level 3 Function Block: Plant Emission Control Systems

Level 3 Function: Contain gas, liquid emissions from plant systems
Parent Level 2 Function Block: Facility Utility System

This function block consists of the physical systems used to contain and collect gas and liquid emissions from plant systems, structures, and components during operation. Uncontrolled release of chemical or radiological materials by operating systems are both a safety and environmental hazard. This function block provides a pathway to appropriate clean up systems for unidentified leakage from system, structures, and components. The system is typical of industrial and radiological facilities but may have design specific requirements based on technology specific challenges related to facility hazards (e.g., high permeability of gaseous tritium through containment barriers). The configuration, sizing, and other specific characteristics will vary significantly by design, so further decomposition of this function block is limited in a technology and design agnostic system engineering model. Further decomposition and specification of system interfaces for a technology and specific design system engineering model, however, may be useful at categorizing and assessing system hazards.

Level 3 Function Block: Plant Structural Systems

Level 3 Function: Protect plant systems from external threats or conditions
Parent Level 2 Function Block: Facility Utility System

This function block consists of the physical systems used to protect facility systems and components from external threats or environmental conditions during operation. The benefits and drawbacks of structural enclosures may vary significantly depending on specific system hazards, system size, and typical or limiting site meteorological conditions. Some industrial production facilities are not structurally enclosed while other facilities may be enclosed by robust structures to prevent damage by external threats or mitigate release of system hazards. The configuration, sizing, and other specific characteristics will vary significantly by design, so further decomposition of this function block is limited in a technology and design agnostic system engineering model. Further decomposition and specification of system interfaces for a technology and specific design system engineering model, however, may be useful at categorizing and assessing interactions with system hazards.

Level 3 Function Block: Plant Environmental Control Systems

Level 3 Function: Maintain necessary environmental conditions for plant systems
Parent Level 2 Function Block: Facility Utility System

This function block consists of the physical systems used to control facility environmental conditions (e.g., temperature, atmosphere, air flow rate) during operations. This system ensures that facility structures operate within design guidelines and ensure an appropriate operational environment for system and component operation. The system is typical of industrial and radiological facilities but may have design specific requirements based on technology specific challenges related to facility hazards. The configuration, sizing, and other specific characteristics will vary significantly by design, so further decomposition of this function block is limited in a technology and design agnostic system engineering model. Further decomposition and specification of system interfaces for a technology and specific design system engineering model, however, may be useful at categorizing and assessing interactions with system hazards.

Level 3 Function Block: Plant Operations Control System/Org

Level 3 Function: Provide control actions for all plant systems and operations
Parent Level 2 Function Block: Site Control/Operation System

This function block contains the control systems and organizations required to ensure operational control of facility systems, structures, and components {I don't quite get distinction between this block and previous…perhaps expand with an example}. This organization is responsible for all operational controls for the facility, maintain operation within acceptable parameters, and coordinating all aspects of facility operation and maintenance. The system is typical of industrial and radiological facilities but may have design specific operational requirements based on technology specific challenges related to facility hazards. The specific organizations characteristics will vary significantly by design, so further decomposition of this function block is limited in a technology and design agnostic system engineering model. Further decomposition and specification of system interfaces for a technology and specific design system engineering model, however, may be useful at categorizing and assessing interactions with system hazards.

Level 3 Function Block: Plant Security Systems/Org

Level 3 Function: Provide security for operations of plant systems against internal, external threats
Parent Level 2 Function Block: Site Control/Operation System

This function block contains the control systems and organizations required to ensure the operational security control of facility systems, structures, and components. This organization coordinates all security activities to prevent or mitigate facility disruption by internal or external threats. This function requires significant coordination with external organizations. The system is typical of industrial and radiological facilities but may have design specific operational requirements based on technology specific challenges related to facility hazards and event scenarios. The specific organizations characteristics will vary significantly by design, so further decomposition of this function block is limited in a technology and design agnostic system engineering model. Further decomposition and specification of system interfaces for a technology and specific design system engineering model, however, may be useful at categorizing and assessing interactions with system hazards.

Level 3 Function Block: Plant Engineering and Safety System/Org

Level 3 Function: Ensure safe and reliable operation of all plant systems during all conditions
Parent Level 2 Function Block: Site Control/Operation System

This function block contains the control systems and organizations required to ensure the safe operation of facility systems, structures, and components. This organization is responsible for emergency controls for the facility, maintain operation that prevent unacceptable operating conditions, with a primary emphasis on operational safety and a secondary emphasis on operational reliability. The system is typical of industrial and radiological facilities but may have design specific operational requirements based on technology specific challenges related to facility hazards. The specific organizations characteristics will vary significantly by design, so further decomposition of this function block is limited in a technology and design agnostic system engineering model. Further decomposition and specification of system interfaces for a technology and specific design system engineering model, however, may be useful at categorizing and assessing interactions with system hazards.

Level 3 Function Block Inputs and Outputs

These inputs and outputs for the model are consistent between all model levels. The connection of the inputs and outputs to the Level 3 Function Blocks is described in Table 2.9.

Table 2.9. Level 3 Model System Boundary Inputs and Outputs

Inputs	*Function Block*	*Rationale*
Fusion Fuel	Fusion Fuel Production / Receiving System	Interface system for different inputs for fusion fuel system
Misc. Consumables	Plant Utility Systems	Interface system for distribution of incoming plant consumables
Heat Sink Cooling	BOP Ultimate Heat Sink System	Interface system for energy removal in thermodynamic cycle
	BOP Shutdown Heat Removal System	Interface system for removal of residual shutdown thermal energy
Outputs	*Function Block*	*Rational*
Electrical Energy	BOP Electrical Distribution System	Interface for electric power generation and distribution
Gas/Liquid Effluents	Effluent Release System	Interface system for use of release of effluents
Other Process Waste	Waste Disposal System	Interface system processing wastes

In the Level 3 Model, the model inputs and outputs are assigned accordingly to the decomposed Level 2 systems. The Level 2 Fuel Handling System Function Block has been decomposed into multiple functions and systems, with the Fusion Fuel Production / Receiving System serving as the external interface for fuel inputs. The Level 2 Facility Waste Processing System Function Block has also been decomposed into multiple functions and systems (Effluent Release System and Waste Disposal System) to enable clarification of environmental releases of effluent wastes and the controlled disposal of waste streams.

Level 3 Function Block Relationships

The connection relationships between the function blocks describe the transfer of physical or non-physical entities between systems. Table 2.10 describes the connections between Function Blocks.

Table 2.10. Level 3 Function Model Relationship

Function Block Producer	*Transfer Relationship*	*Function Block Receiver*	*Rationale*
Plasma Fueling System	Fusion Fuel	Fusion Reactor Vessel System	Fuel input to sustain steady state plasma
Plasma Heating System	Active Heating Injection	Fusion Reactor Vessel System	Heating to control and sustain plasma
Plasma Shutdown System	Active Shutdown Injection	Fusion Reactor Vessel System	Material injection to safely disrupt plasma
Plasma Control System	Fuel Control Signals	Plasma Fueling System	Integrated control of fuel input balance
	System Control Signals	Plasma Shutdown System	Ensure safe plasma operating condition
	System Control Signals	Plasma Heating System	Maintain plasma heating balance
	System Control Signals	Plasma Confinement System	Maintain plasma confinement condition
	System Control Signals	Fusion Reactor Vessel Environmental System	Ensure proper vessel start-up conditions
Plasma Confinement System	Active Confinement Controls (e.g., EM)	Fusion Reactor Vessel System	Active changes to control to maintain steady state plasma
Fusion Reactor Vessel System	Reactor Exhaust	Fusion Exhaust Removal System	Removal of excess in-vessel neutral gasses
	Energetic Fusion Products	Fusion Energy Capture System	Steady state removal of energetic fusion reaction products
Fusion Reactor Vessel Environmental System	Process Gasses	Fusion Reactor Vessel System	Gasses to control plasma conditions, operation parameters
	Vacuum Pumping	Fusion Reactor Vessel System	Develop initial vessel start-up atmosphere
Fusion Energy Capture System	Fusion Energy	Thermal Energy Conversion System	Steady state removal of fusion energy products
	Capture Byproducts	Fusion Energy Conversion Containment	Steady state or batch removal of energetic

Table 2.10. Level 3 Function Model Relationship

Function Block Producer	*Transfer Relationship*	*Function Block Receiver*	*Rationale*
		System	reaction products
Thermal Energy Conversion System	Thermal Energy	BOP Heat Exchanger System	Steady state transfer to thermodynamic cycle
	Thermal Energy	BOP Shutdown Heat Removal System	Transient energy removal when BOP is unavailable
Fusion Energy Conversion Containment System	Fusion Fuel Inputs	Fusion Fuel Processing System	Fuel inputs bred via energetic reactions
	Reaction Byproducts	Waste Handling System, Radiological Waste Handling System, Process Fluid Handling System	Non-fuel reaction byproducts removed to ensure steady state operation
	Other Wastes Streams	Waste Handling System, Radiological Waste Handling System, Process Fluid Handling System	Process fluids, other consumable wastes removed for steady state operation
Fusion Exhaust Removal System	Reactor Exhaust	Fusion Exhaust Processing System	Removal, reprocessing of excess neutral gas
Fusion Exhaust Processing System	Fusion Fuel Exhaust	Fusion Fuel Recycling System	Unconsumed fusion fuel recycled from reactor exhaust
	Reaction Products	Waste Handling System, Radiological Waste Handling System, Process Fluid Handling System	Non-fuel reaction byproducts removed to ensure steady state exhaust processing
	Other Wastes Streams	Waste Handling System, Radiological Waste Handling System, Process Fluid Handling System	Other process wastes removed for steady state exhaust handling
Fusion Fuel Recycling System	Fusion Fuel	Fusion Fuel Storage System	Fully reprocessed, usable fusion fuel
BOP Heat Exchanger System	Working Fluid (1)	BOP Turbine System	High energy state working fluid
BOP Turbine System	Working Fluid (2)	BOP Ultimate Heat Sink System	Low energy state working fluid
	Mechanical Energy	BOP Generator System	Extracted work energy via mechanical cycle
BOP Generator System	Electrical Energy	BOP Electrical Distribution System	Gross electrical output from BOP generator
BOP Electrical Distribution System	Electrical Energy (House)	Plant Utility System	Electrical energy for internal facility loads
BOP Ultimate Heat Sink System	Working Fluid (3)	BOP Pump Compressor System	Minimum energy state working fluid
	Fouled Working Fluid	BOP Chemistry Control System	Working fluid unusable for BOP operation
BOP Pump Compressor	Working Fluid (4)	BOP Heat Exchanger	Compressed working

Table 2.10. Level 3 Function Model Relationship

Function Block Producer	*Transfer Relationship*	*Function Block Receiver*	*Rationale*
System		System	fluid for BOP heating
BOP Chemistry Control System	Cleaned Up Working Fluid	BOP Pump Compressor System	Recycled working fluid usable for BOP cycle
Fusion Fuel Production/Receiving System	Fusion Fuel Inputs	Fusion Energy Conversion Containment System	Fusion fuel inputs requiring energetic reaction for processing
	Fusion Fuel Inputs	Fusion Fuel Processing System	Fusion fuel inputs usable without additional reactions
Fusion Fuel Processing System	Fusion Fuel	Fusion Fuel Storage System	Fully processed, usable fusion fuel
	Other Wastes Streams	Waste Handling System, Radiological Waste Handling System, Process Fluid Handling System	Process fluids, other wastes produced during fuel processing operations
Fusion Fuel Storage System	Fusion Fuel	Fusion Fuel Preparation System	Fusion fuel form usable by preparation system
Fusion Fuel Preparation System	Fusion Fuel	Plasma Fueling System	Final fusion fuel form ready for fuel systems
Process Fluid Handling System	Recycled Process Fluids	Plant Utility System	Reusable process fluids for facility systems
	Releasable Wastes	Effluent Release System	Fluid wastes deemed acceptable for release
	Disposable Wastes	Waste Disposal System	Waste streams requiring controlled off-site disposal
Waste Handling System	Releasable Wastes	Effluent Release System	Fluid wastes deemed acceptable for release
	Disposable Wastes	Waste Disposal System	Waste streams requiring controlled off-site disposal
Radiological Waste Handling System	Releasable Wastes	Effluent Release System	Fluid wastes deemed acceptable for release
	Disposable Wastes	Waste Disposal System	Waste streams requiring controlled off-site disposal
Plant Maintenance Systems/Org	Maintenance Activities	[All Systems]	Organizational activity for all non-radiological facility systems
	System Wastes	Waste Handling System, Process Fluid Handling System	Waste streams produced during maintenance activities
Plant Radiological Maintenance Systems/Org	Maintenance Activities	[All Radiological Systems]	Organizational activity for all radiological facility systems
	System Wastes	Waste Handling System, Radiological Waste Handling System, Process Fluid Handling	Waste streams produced during radiological related maintenance activities

Table 2.10. Level 3 Function Model Relationship

Function Block Producer	*Transfer Relationship*	*Function Block Receiver*	*Rationale*
		System	
Plant Infrastructure Replacement System/Org	Replacement Activities	[All Systems]	Organizational activity for all facility systems
	System Wastes	Waste Handling System, Radiological Waste Handling System, Process Fluid Handling System	Waste streams produced during replacement activities
Plant Utility Systems	Electrical Energy	Plant Environmental Control Systems	Electricity for facility structural systems
	Misc. Utilities	Plant Environmental Control Systems	Utilities (process fluids, etc.) for facility structural systems
	Electrical Energy	[All Systems]	Electricity for facility systems, components
	Misc. Utilities	[All Systems]	Utilities (process fluids, etc.) for facility systems, components
Plant Emission Control Systems	Radiological Emissions	Radiological Waste Handling System	Radiological emissions captured from facility systems, components
	Other Plant Emissions	Waste Handling System	Non-radiological emissions captured from facility systems, components
Plant Structural Systems	System Emissions	Plant Emission Control Systems	Centralized collection of structural system emissions
Plant Environmental Control Systems	Electrical Energy	Plant Structural Systems	Controlled electricity for facility structural systems, components
	Misc. Utilities	Plant Structural Systems	Controlled utilities (process fluids, etc.) for facility structural systems, components
Plant Operations Control System/Org	Control Signals	[All Systems]	Control signals for all plant systems and operations
Plant Security Systems/Org	Control Signals	Plant Structural Systems	Control signals for physical plant security
Plant Engineering and Safety System/Org	Control Signals	[All Systems]	Control signals to ensure safe operation under all conditions
[Any Systems]	Radiological Wastes	Radiological Waste Handling System	Radiological waste streams produced during any operational activities
[Any Systems]	Non-radiological Wastes	Waste Handling System	Non-radiological waste streams produced

Table 2.10. Level 3 Function Model Relationship

Function Block Producer	*Transfer Relationship*	*Function Block Receiver*	*Rationale*
			during any operational activities
[Any Systems]	Fouled Process Fluids	Process Fluid Handling System	Process fluids requiring clean-up for reuse in plant systems

Review of Level 3 Model Insights

In the Level 3 Model, further functional decomposition of function blocks shows further realignment of functional system groups that further differ from the Level 1 and Level 2 models:

- "Fusion Power Area" emerges, combining the decomposed systems from Level 1 Fusion Power System Function Block and fusion fuel related systems from the Level 1 Auxiliary Support System Function Block.
- "Balance of Plant Area" remains fairly intact, consisting of completely of decomposed systems from the Level 1 Balance of Plant Function Block.
- "Utility and Structural Area" emerges based on relationships between utility distribution systems and structural/environmental control systems
- "Waste Processing Area" is the full decomposition of the Level 2 Facility Waste Process Systems Function Block, interfacing internally with all facility systems
- "Physical Operations Area" is the full decomposition of the Level 2 Facility Maintenance System Function Block, interfacing internally with all facility systems
- "Facility Controls Area" is the operational and safety control center of the facility, decomposed with the highest-level system functions derived from decomposition of the Level 2 Site Control/Operation System Function Block

This realignment shows a natural grouping of related function blocks based on functional purpose. This simplistic view of functional alignment is, however, complicated by the number of systems that have connections to "All Systems" including waste related systems, utility systems, control systems, and operational infrastructure systems. This reflects the reality of operation of large industrial facilities but introduces a large number of required interfaces between systems and the need to consider complex system interactions on system behavior.

2.3 Level 3 Tokamak D-T Fueled Function Model for Commercial Fusion

This section presents a modified Level 3 function model to a technology and configuration specific commercial fusion system. Plant functions, requirements, and function blocks are modified from the Level 3 model for a generic fusion facility to fit the specific configuration.

The technology specific commercial fusion facility considered in this section is a compact, high-field tokamak and is based on the ARC conceptual design study developed by researchers at the MIT Plasma and Science Fusion Center [9]. This conceptual design has several key technology specific characteristics:

- Magnetic confinement tokamak plasma configuration
- Deuterium and tritium fuel cycle
- Liquid salt immersion heat transfer and tritium breeding blanket

This design utilizes high temperature superconducting magnetic tapes to produce extremely high strength magnetic fields (on the order of 20 Tesla), enabling improved confinement and smaller core plasma [9]. The use of a deuterium and tritium fuel cycle is typical of first generation fusion devices due to the reactions high cross section at lower energy [10]. The use of a radioactive fuel (tritium) adds some complexity to the processing, storage, and utilization of the fusion fuels.

One unique characteristic of this design is the use of a liquid salt immersion blanket for heat transfer and tritium breeding. Prior conceptual fusion facilities use solid materials to moderate high-energy neutrons produced by fusion reactions and breed tritium through neutron capture reactions. A working fluid (e.g., water, helium) then transfers thermal energy from the solid modules to the balance of plant systems and removes tritium or tritiated materials from the solid modules through diffusion and convection. In this design, the torus and vacuum vessel that contain the fusion reactions are submerged in a tank of liquid fluorine-lithium-beryllium (FLiBe) salts. The liquid salts flow around the torus, moderating energy from high-energy neutrons and breeding tritium through neutron capture reactions [9]. The liquid salt system can interface with other systems for heat transfer to the balance of plant systems, removal of bred tritium, and salt chemistry control. This combines several plant functions normally found in a commercial fusion facility into one integrated plant function.

The technology specific Level 3 function model is shown in Figure 2.5. Three detailed views of the full Level 3 function model are provided as insets in Figure 2.5a, 2.5b, and 2.5c. In this section, the modifications to the system model are discussed and justified in Table 2.11. Detailed descriptions of each modified technology specific Level 3 Function Blocks are provided. Changes to system inputs and outputs to Function Blocks is given in Table 2.12 and the relationships between function blocks is described in Table 2.13.

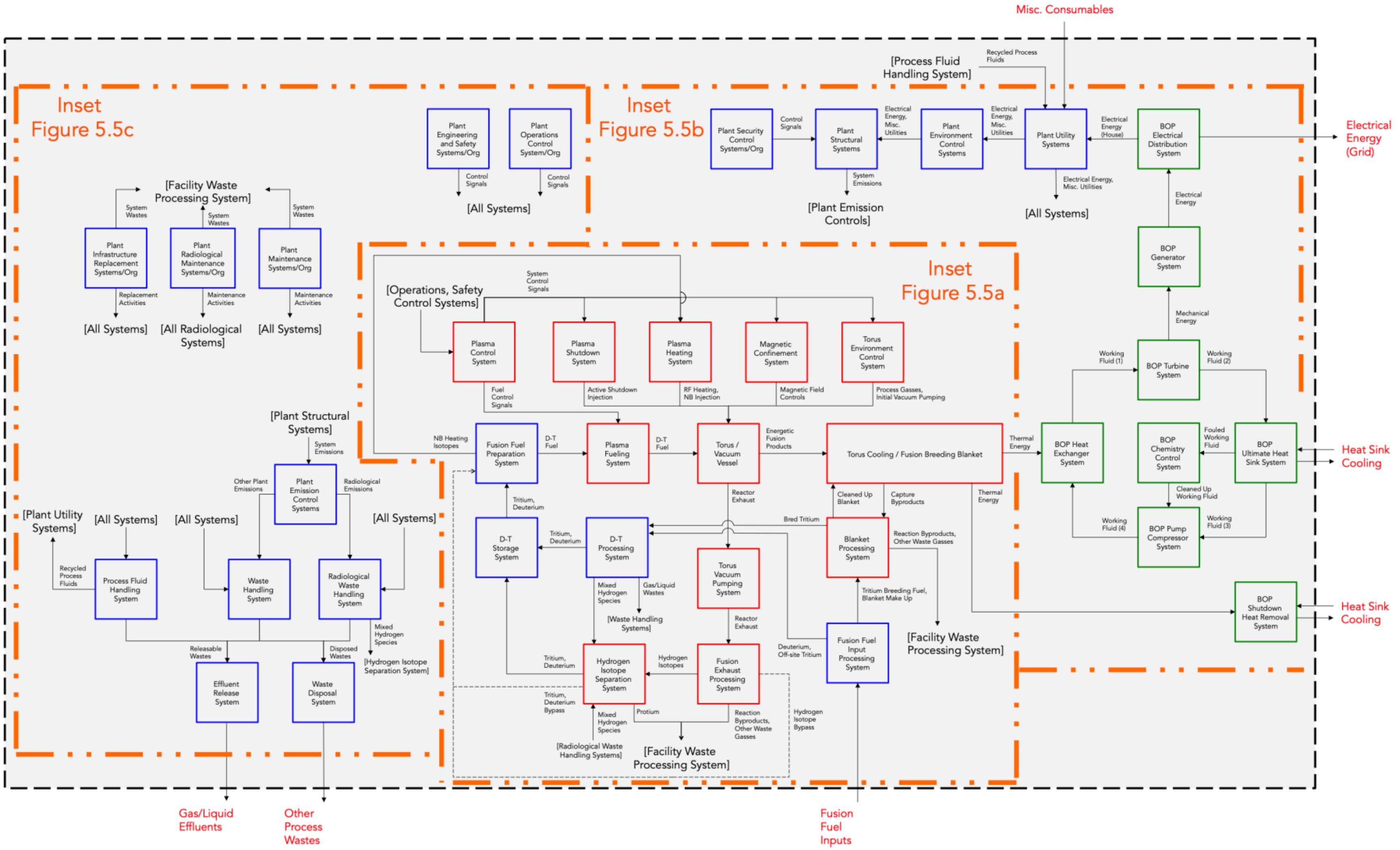

Misc. Consumables
[Process Fluid Handling System]
Recycled Process Fluids
Inset Figure 5.5c
Inset Figure 5.5b
Inset Figure 5.5a
Plant Engineering and Safety Systems/Org
Plant Operations Control System/Org
Control Signals
Control Signals
[All Systems]
Plant Security Control Systems/Org
Control Signals
Plant Structural Systems
Electrical Energy, Misc. Utilities
Plant Environment Control Systems
Electrical Energy, Misc. Utilities
Plant Utility Systems
Electrical Energy (House)
BOP Electrical Distribution System
Electrical Energy (Grid)
System Emissions
[Plant Emission Controls]
Electrical Energy, Misc. Utilities
[All Systems]
Electrical Energy
BOP Generator System
Mechanical Energy
[Facility Waste Processing System]
System Wastes
System Wastes
System Wastes
Plant Infrastructure Replacement Systems/Org
Plant Radiological Maintenance Systems/Org
Plant Maintenance Systems/Org
Replacement Activities
Maintenance Activities
Maintenance Activities
[All Systems]
[All Radiological Systems]
[All Systems]
[Operations, Safety Control Systems]
System Control Signals
Plasma Control System
Plasma Shutdown System
Plasma Heating System
Magnetic Confinement System
Torus Environment Control System
Fuel Control Signals
Active Shutdown Injection
RF Heating, NB Injection
Magnetic Field Controls
Process Gasses, Initial Vacuum Pumping
Working Fluid (1)
BOP Turbine System
Working Fluid (2)
[Plant Structural Systems]
System Emissions
NB Heating Isotopes
Fusion Fuel Preparation System
D-T Fuel
Plasma Fueling System
D-T Fuel
Torus / Vacuum Vessel
Energetic Fusion Products
Torus Cooling / Fusion Breeding Blanket
Thermal Energy
BOP Heat Exchanger System
BOP Chemistry Control System
Fouled Working Fluid
BOP Ultimate Heat Sink System
Heat Sink Cooling
Other Plant Emissions
Plant Emission Control Systems
Radiological Emissions
Tritium, Deuterium
Reactor Exhaust
Cleaned Up Blanket
Capture Byproducts
Thermal Energy
Cleaned Up Working Fluid
[Plant Utility Systems]
[All Systems]
[All Systems]
[All Systems]
D-T Storage System
Tritium, Deuterium
D-T Processing System
Bred Tritium
Blanket Processing System
Reaction Byproducts, Other Waste Gasses
Working Fluid (4)
BOP Pump Compressor System
Working Fluid (3)
Recycled Process Fluids
Process Fluid Handling System
Waste Handling System
Radiological Waste Handling System
Mixed Hydrogen Species
Gas/Liquid Wastes
Torus Vacuum Pumping System
Tritium Breeding Fuel, Blanket Make Up
[Waste Handling Systems]
Reactor Exhaust
[Facility Waste Processing System]
BOP Shutdown Heat Removal System
Heat Sink Cooling
Releasable Wastes
Disposed Wastes
Mixed Hydrogen Species
[Hydrogen Isotope Separation System]
Tritium, Deuterium
Hydrogen Isotope Separation System
Hydrogen Isotopes
Fusion Exhaust Processing System
Deuterium, Off-site Tritium
Fusion Fuel Input Processing System
Effluent Release System
Waste Disposal System
Tritium, Deuterium Bypass
Mixed Hydrogen Species
Protium
Reaction Byproducts, Other Waste Gasses
Hydrogen Isotope Bypass
[Radiological Waste Handling Systems]
[Facility Waste Processing System]
Gas/Liquid Effluents
Other Process Wastes
Fusion Fuel Inputs

Figure 2.5. Technology Specific Level 3 Commercial Fusion Function Model

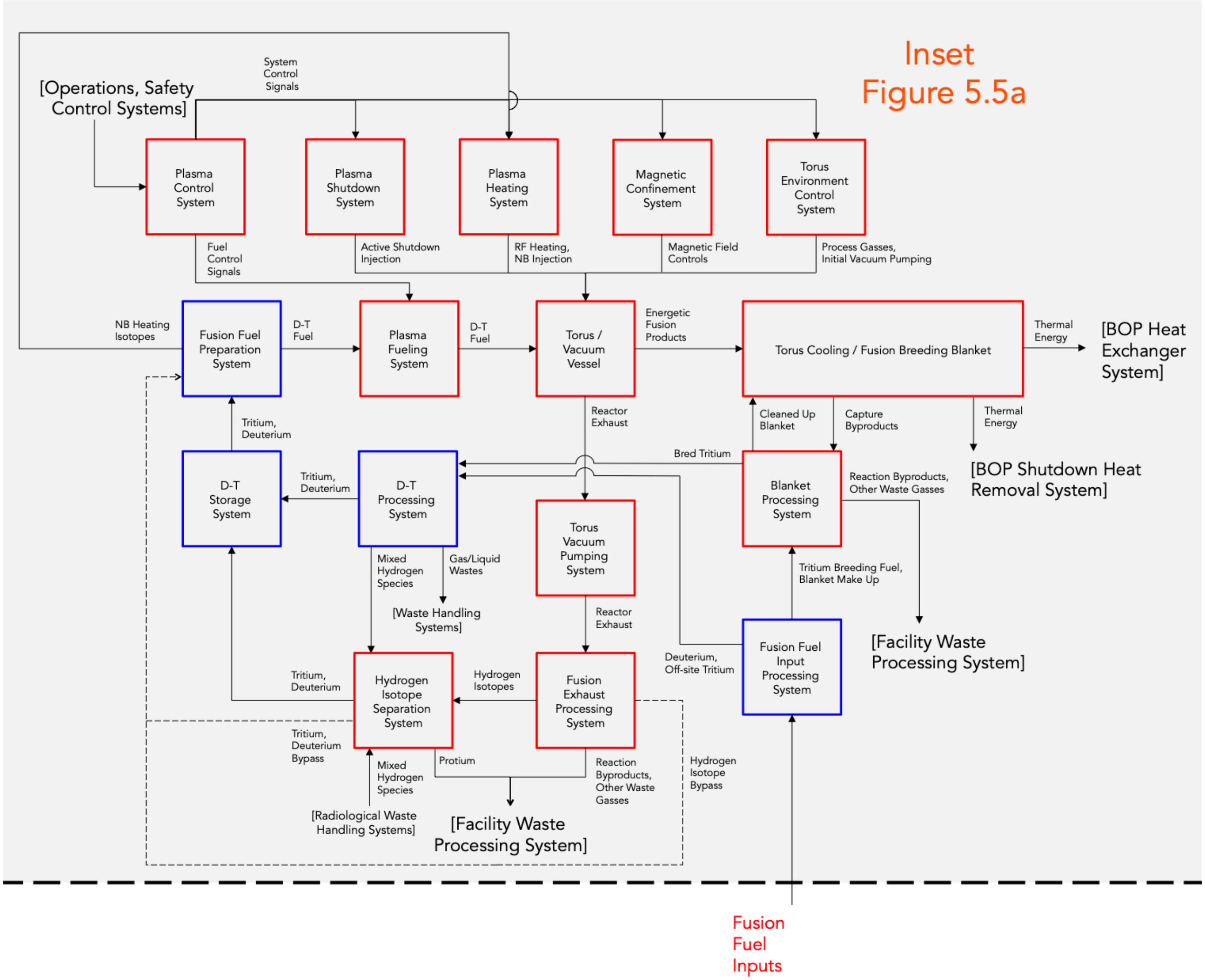

Inset
Figure 5.5a
[Operations, Safety Control Systems]
System Control Signals
Plasma Control System
Plasma Shutdown System
Plasma Heating System
Magnetic Confinement System
Torus Environment Control System
Fuel Control Signals
Active Shutdown Injection
RF Heating, NB Injection
Magnetic Field Controls
Process Gasses, Initial Vacuum Pumping
NB Heating Isotopes
Fusion Fuel Preparation System
D-T Fuel
Plasma Fueling System
D-T Fuel
Torus / Vacuum Vessel
Energetic Fusion Products
Torus Cooling / Fusion Breeding Blanket
Thermal Energy
[BOP Heat Exchanger System]
Tritium, Deuterium
Reactor Exhaust
Cleaned Up Blanket
Capture Byproducts
Thermal Energy
Bred Tritium
[BOP Shutdown Heat Removal System]
D-T Storage System
Tritium, Deuterium
D-T Processing System
Torus Vacuum Pumping System
Blanket Processing System
Reaction Byproducts, Other Waste Gasses
Mixed Hydrogen Species
Gas/Liquid Wastes
[Waste Handling Systems]
Reactor Exhaust
Tritium Breeding Fuel, Blanket Make Up
Deuterium, Off-site Tritium
Fusion Fuel Input Processing System
[Facility Waste Processing System]
Tritium, Deuterium
Hydrogen Isotope Separation System
Hydrogen Isotopes
Fusion Exhaust Processing System
Tritium, Deuterium Bypass
Protium
Mixed Hydrogen Species
Reaction Byproducts, Other Waste Gasses
Hydrogen Isotope Bypass
[Radiological Waste Handling Systems]
[Facility Waste Processing System]
Fusion Fuel Inputs

Figure 2.5a. Technology Specific Level 3 Commercial Fusion Function Model System Part A Inset

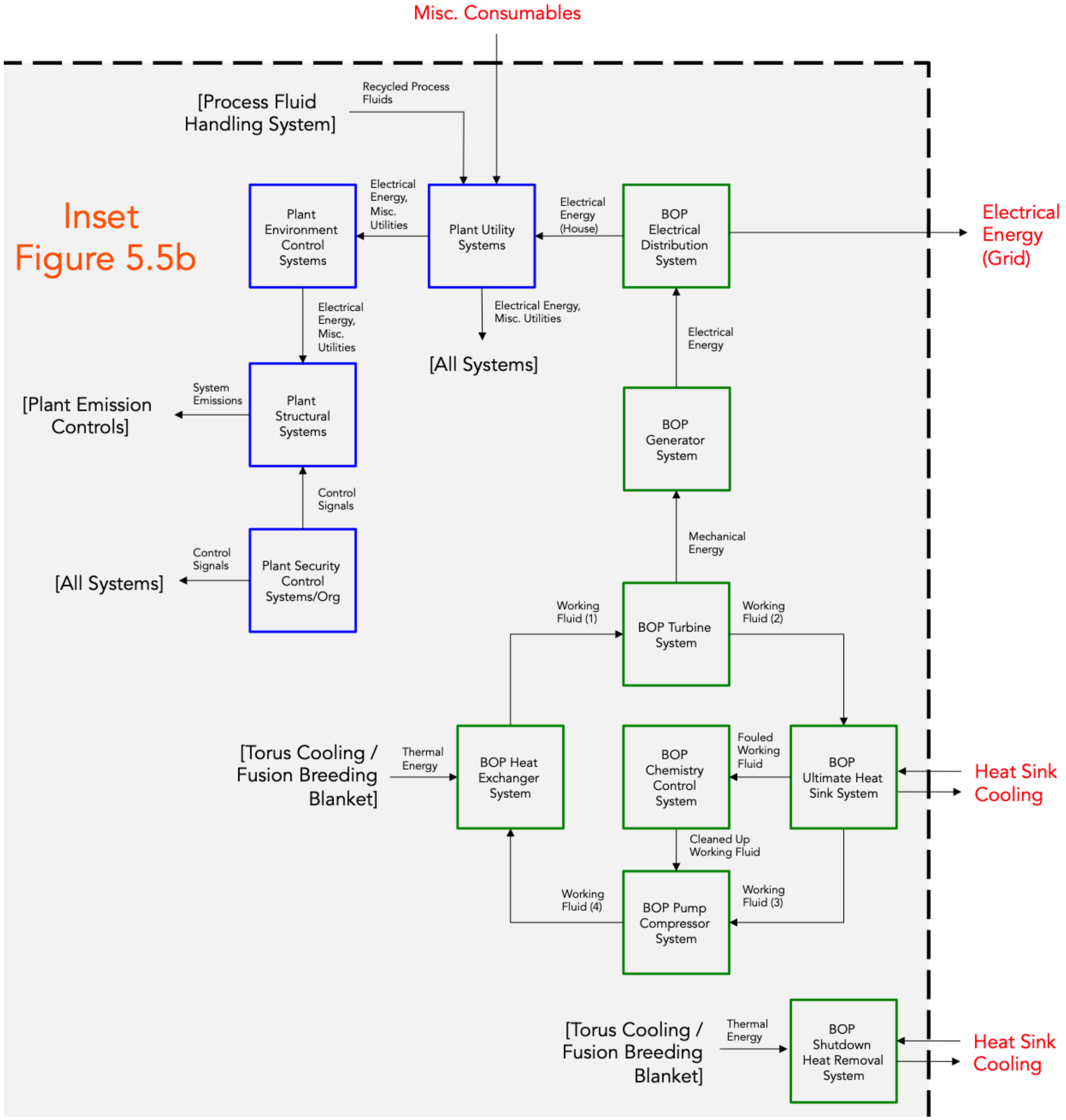

Misc. Consumables
[Process Fluid Handling System]
Recycled Process Fluids
Inset Figure 5.5b
Plant Environment Control Systems
Electrical Energy, Misc. Utilities
Plant Utility Systems
Electrical Energy (House)
BOP Electrical Distribution System
Electrical Energy (Grid)
Electrical Energy, Misc. Utilities
Electrical Energy, Misc. Utilities
[All Systems]
Electrical Energy
[Plant Emission Controls]
System Emissions
Plant Structural Systems
BOP Generator System
Control Signals
Mechanical Energy
[All Systems]
Control Signals
Plant Security Control Systems/Org
Working Fluid (1)
BOP Turbine System
Working Fluid (2)
[Torus Cooling / Fusion Breeding Blanket]
Thermal Energy
BOP Heat Exchanger System
BOP Chemistry Control System
Fouled Working Fluid
BOP Ultimate Heat Sink System
Heat Sink Cooling
Cleaned Up Working Fluid
Working Fluid (4)
BOP Pump Compressor System
Working Fluid (3)
[Torus Cooling / Fusion Breeding Blanket]
Thermal Energy
BOP Shutdown Heat Removal System
Heat Sink Cooling

Figure 2.5b. Technology Specific Level 3 Commercial Fusion Function Model System Part B Inset

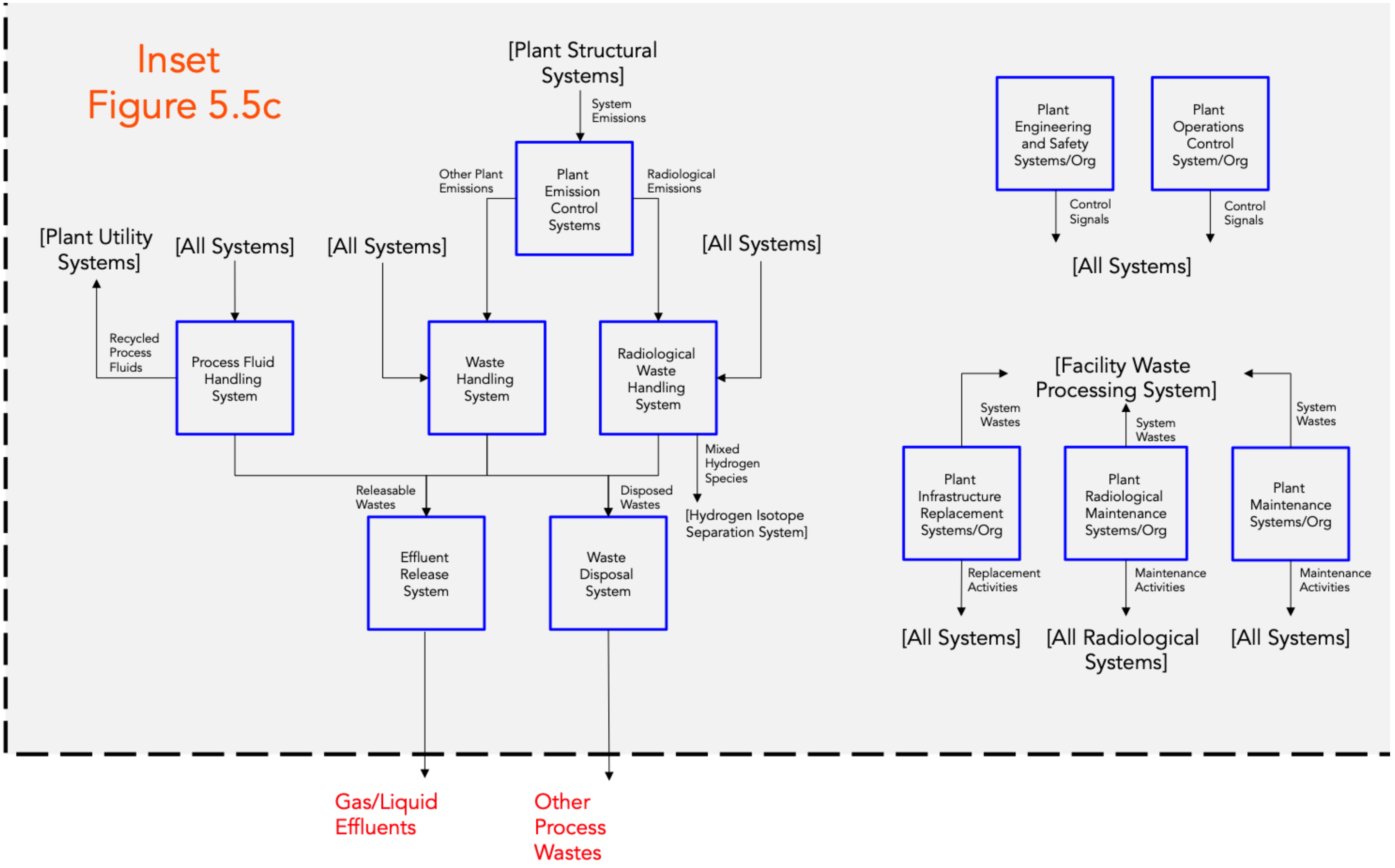


Figure 2.5c. Technology Specific Level 3 Commercial Fusion Function Model System Part C Inset

The Function Blocks modified between the Level 3 Model and the technology specific Level 3 Model are described and justified in Table 2.11.

Table 2.11. Technology Specific Level 3 Model Modifications

Level 3 Function Block	*Technology Specific Level 3 Function Block*	*Rational*
Plasma Confinement System	Magnetic Confinement System	Specification of confinement mechanism and associated inherent system hazards
Fusion Reactor Vessel Environment System	Torus Environment Control System	Specification of environmental controls and processes gasses used for reactor environment
Fusion Reactor Vessel System	Torus / Vacuum Vessel	Specification of physical geometry and interface for systems for plasma vessel
Fusion Exhaust Removal System	Torus Vacuum Pumping System	Specification of method for exhaust removal, indication of possible functional subsystems
Fusion Energy Capture System	Torus Cooling / Fusion Breeding Blanket	Combination of fusion energy capture, thermal energy conversion, and fuel input production via energetic reaction in liquid breeding blanket
Thermal Energy Conversion System		
Fusion Energy Conversion Containment System	Blanket Processing System	Specification of processing system for removal of bred fusion fuel, other capture byproducts from liquid blanket
Fusion Fuel Recycling System	Hydrogen Isotope Separation System	Specification of major processing required in recycling system
Fusion Fuel Processing System	D-T Processing System	Specification of major activity in fuel processing system
Fusion Fuel Storage System	D-T Storage System	Specification of fuel composition in storage system

Modification of the Level 3 System Engineering model for a commercial fusion power plant to a technology specific Level 3 System Engineering model requires a number of changes to the Level 3 Function Blocks. It is important to note, however, that the model modifications are limited to plasma confinement and fuel cycle function blocks within the "Fusion Power Area" described for the Level 3 model. The most significant modification was the combination of the Fusion Energy Capture System and Thermal Energy Conversion System into the Torus Cooling / Fusion Breeding Blanket. This change reflects a design specific functional combination of systems. The associated update of the Fusion Energy Conversion Containment System to the Blanket Processing System also reflects a functional change of the processing requirements for the Conversion Containment system.

The limited scope of the model modifications required for this model suggests that the technology independent system engineering model may be robust enough to characterize different fusion technologies and enable relatively low effort development of subsequent technology specific models.

Technology Specific Level 3 Function Block Descriptions

Technology Specific Level 3 Function Block: Magnetic Confinement System

Technology Specific Level 3 Function: Actively confine fusion reactions and plasma
Parent Level 3 Function Block: Plasma Confinement System

This function block enables the specification of the technology specific confinement method and identification of confinement specific hazards. In the case of magnetic confinement, this allows greater understanding of the high magnetic fields associated with plasma confinement. This technology specific clarification also allows more detailed understanding of high-level failure mechanisms and how the Function Block may interact with other plant function blocks. For example, loss of electrical energy from Level 3 Plant Utility System Function Block the could lead to loss of plasma confinement for this Function Block.

Technology Specific Level 3 Function Block: Torus Environment Control System

Technology Specific Level 3 Function: Maintain torus internal conditions
Parent Level 3 Function Block: Fusion Reactor Vessel Environment System

This function block enables specification of the technology specific conditions required within the torus to facilitate fusion reactions. For a D-T fueled fusion facility, this system would have radioactive material contamination (specifically tritium) related to the operation and maintenance of the torus system. This also specifies the need to pumping and other gas injection systems to maintain proper internal conditions within the torus.

Technology Specific Level 3 Function Block: Torus / Vacuum Vessel

Technology Specific Level 3 Function: Passively contain fusion reactions, plasma, and byproducts
Parent Level 3 Function Block: Fusion Reactor Vessel System

This function block allows for clarification of the physical form and general operation characteristics of the torus and vacuum vessel. This includes the potential for radiological contamination of first wall materials by deposition of radiological materials (e.g., tritium) and neutron activation of materials. The overall function of this function block remains the same in both the technology specific and technology independent system engineering models.

Technology Specific Level 3 Function Block: Torus Vacuum Pumping System

Technology Specific Level 3 Function: Remove fusion products and other wastes from fusion reactor system
Parent Level 3 Function Block: Fusion Exhaust Removal System

This function block enables identification of technology specific hazards. For D-T fueled systems, this exhaust will contain unreacted tritium fuel and could contain a significant radiological inventory depending on the pumping method used. The overall function of this function block remains the same in both the technology specific and technology independent system engineering models.

Technology Specific Level 3 Function Block: Torus Cooling / Fusion Breeding Blanket

Technology Specific Level 3 Function: Capture neutron energy as thermal energy from collisions with liquid blanket and breed tritium from neutron-lithium reactions
Parent Level 3 Function Block: Fusion Energy Capture System, Thermal Energy Conversion System

This function block is one of the most significantly changed in the technology specific model. The function block combines the functions of two technology independent model by utilizing a liquid breeding blanket that captures the energy from neutrons via scattering into a liquid coolant that can be exchanged with Balance of Plant systems and breeds tritium through interaction with lithium. This function block is design specific because of the multiple functions that the liquid blanket fulfills. The combination of function blocks also consolidates hazards into one function block due to the affects of neutron interaction with the blanket materials. This set of characteristics is unique to this technology, so characterization of this function block within the system model is critical. This function block is also a critical interface for the removal of heat from the Fusion Power System.

Technology Specific Level 3 Function Block: Blanket Processing System

Technology Specific Level 3 Function: Capture and contain neutron interaction products from the blanket and maintain blanket chemistry
Parent Level 3 Function Block: Fusion Energy Conversion Containment System

This function block is an important technology specific feature that interfaces between the neutron and energy capture related function blocks with the fuel input and processing function blocks. Constant neutron absorption by the liquid breeding blanket will lead to the depletion of specific isotopes in the blanket and change the rate of tritium production by neutron absorption. This function block must maintain steady-state conditions within the liquid blanket by adding and removing material from the blanket. This includes, at a minimum, addition of lithium and removal of tritium or tritiated compounds to for fueling purposes and would likely include other chemistry control requirements. The hazards and interfaces associated with this system are critical to facility operation and are highly design and technology specific.

Technology Specific Level 3 Function Block: Hydrogen Isotope Separation System

Technology Specific Level 3 Function: Separate hydrogen isotopes for individual fusion fuel steam recycling
Parent Level 3 Function Block: Fusion Fuel Recycling System

This Function Block enables specification of the functional processes and associated hazards required for recycling of fusion fuel in a D-T specific technology. The separation of hydrogen isotopes by the Level 3 Fusion Exhaust Processing System may be easily accomplished by various chemical processing techniques, but additional isotopic separation may be required before returning the fusion fuel to the fuel preparation systems. This Function Block is separated to allow for delineation of the hazards associated with large, hydrogen isotope separation systems and the potential challenges of large inventories of explosive and radioactive fuel forms.

Technology Specific Level 3 Function Block: D-T Processing System

Technology Specific Level 3 Function: Process deuterium and tritium fuel into usable forms
Parent Level 3 Function Block: Fusion Fuel Processing System

This function block interfaces with the Level 3 Fusion Fuel Receiving System and the Level 3 Blanket Processing System to ensure that fusion fuel received from off-site or produced on-site is in a usable form the Fusion Fuel Preparation System. This may require physical or chemical processing of input fuel streams to ensure that is fuel is in an appropriate form. This function block is specified for the technology specific system engineering model due to the hazards associated with the processing of the explosive, radioactive fusion fuel.

Technology Specific Level 3 Function Block: D-T Storage System

Technology Specific Level 3 Function: Store reserve or backup separated deuterium and tritium fuel
Parent Level 3 Function Block: Fusion Fuel Storage System

This function block is defined to allow delineation of the hazards associated with storage of deuterium and tritium fusion fuel. While both of these fuels may be stored in stable, non-volatile form, their processing requires exchange in gaseous forms and may represent a significant process hazard. The specification of this system allows for the specific consideration of the hazards associated with large inventories of deuterium and tritium and the design considerations that may inherently mitigate these hazards.

Technology Specific Level 3 Function Block Inputs and Outputs

The modified inputs and outputs between the Level 3 Model and the technology specific Level 3 Model are described and justified in Table 2.12.

Table 2.12. Technology Specific Level 3 Model Modified Inputs and Outputs

Inputs	*Function Block*	*Rationale*
No changes from Level 3 Model		

Outputs	*Function Block*	*Rationale*
No changes from Level 3 Model		

No changes were needed to model inputs or outputs for the technology specific Level 3 Model. This is due to the concentration of function block changes within the “Fusion Power Area”. While there were no explicit changes to the inputs or outputs, technology specification of the tritium-deuterium fuel cycle with on-site tritium breeding enables additional characterization of several model and outputs.

Under normal operating conditions, the Fusion Fuel Inputs to the Level 3 Fusion Fuel Input Processing System would consist, principally, of deuterium and lithium. The lithium, as previously discussed, would be bred into tritium through the $(n, {}^{3}_{1}H)$ reaction. Therefore, the Fusion Fuel Inputs and the Fusion Fuel Input Processing Systems would not be radiologically inputs or systems.

While the utilization of on-site bred tritium reduces the radiological significance of Fusion Fuel Inputs, it may contribute model outputs with radiological significance. Specifically, both the Gas/Liquid Effluents output and the Other Process Waste outputs may be vulnerable to tritium contamination. Tritium adsorption onto solid surfaces could lead solid tritium contamination of systems, structures, components, and other process equipment. Elemental tritium (T_2), oxidized tritium (T_2O, HTO), or other forms of tritium can lead to the tritium contamination of gaseous or liquid effluent streams. While the effluent release of gaseous tritium can be controlled through existing radiological material handling processes, these processes themselves can produce additional tritium contaminated waste streams. As a result, these outputs will be characteristically different than for a commercial fusion facility that does not utilize tritium as a part of its fuel cycle.

Finally, the high permeability of elemental and oxidized tritium through metallic structures could enable an additional radiological release pathway through the BOP systems. Starting at the Level 3 Torus Cooling / Fusion Breeding Blanket, tritium could diffuse through heat exchangers and other metallic components, ultimately crossing the model boundary through the Heat Sink Cooling output. Consideration of this output as a radiological hazard may require additional controls or treatment of the Heat Sink Cooling output as an additional Gas/Liquid Effluent model output.

Technology Specific Level 3 Function Block Relationships

The connection relationships between the function blocks describe the transfer of physical or non-physical entities between systems. Table 2.13 describes the connections modified between the Level 3 Model and the technology specific Level 3 Model.

Table 2.13. Technology Specific Level 3 Model Modified Relationships

Function Block Producer	*Transfer Relationship*	*Function Block Receiver*	*Rationale*
Magnetic Confinement System	Magnetic Field Controls	Torus / Vacuum Vessel	Active changes to magnetic field configuration to control plasma conditions
Torus Environment Control System	Process Gasses	Torus / Vacuum Vessel	Gasses to control plasma conditions, parameters, surface interactions
	Initial Vacuum Pumping	Torus / Vacuum Vessel	Develop initial vessel start-up vacuum conditions
Torus / Vacuum Vessel	Reactor Exhaust	Torus Vacuum Pumping System	Steady state removal of in-vessel neutral gasses
	Energetic Fusion Products	Torus Cooling / Fusion Breeding Blanket	Steady state removal of neutron / thermal radiation generated by fusion reactions
Torus Vacuum Pumping System	Reactor Exhaust	Fusion Exhaust Processing System	Transfer of steady-state excess neutral gasses for processing, recycling

Table 2.13. Technology Specific Level 3 Model Modified Relationships

Function Block Producer	*Transfer Relationship*	*Function Block Receiver*	*Rationale*
Torus Cooling / Fusion Breeding Blanket	Capture Byproducts	Blanket Processing System	Mobile byproducts from neutron and secondary nuclear reactions
	Thermal Energy	BOP Heat Exchanger System	Steady state transfer to thermodynamic cycle through liquid blanket
	Thermal Energy	BOP Shutdown Heat Removal System	Transient energy removal through liquid blanket when BOP is unavailable
Blanket Processing System	Bred Tritium	D-T Processing System	Separated tritium or tritium compounds from neutron reactions in blanket
	Cleaned Up Blanket	Torus Cooling / Fusion Breeding Blanket	Chemically purified and controlled blanket
	Reaction Byproducts	Waste Handling System, Radiological Waste Handling System, Process Fluid Handling System	Non-tritium reaction byproducts removed from blanket to ensure steady state operation
	Other Waste Gasses	Waste Handling System, Radiological Waste Handling System, Process Fluid Handling System	Process fluids, other consumable wastes removed for steady state operation
Hydrogen Isotope Separation System	Tritium	D-T Storage System	Isotopically separated tritium suitable for short- or long-term storage
	Deuterium	D-T Storage System	Isotopically separated deuterium suitable for short- or long-term storage
	Tritium Bypass	Fusion Fuel Preparation System	Isotopically separated tritium chemically suitable direct to fuel preparation system
	Deuterium Bypass	Fusion Fuel Preparation System	Isotopically separated deuterium chemically suitable direct to fuel preparation system
	Protium	Waste Handling System	Non-fuel waste excess hydrogen isotope
D-T Processing System	Tritium	D-T Storage System	Chemically processed tritium suitable for short- or long-term storage
	Deuterium	D-T Storage System	Chemically processed deuterium suitable for short- or long-term storage
	Gas/Liquid Wastes	Waste Handling System, Radiological Waste Handling	Process wastes created during chemical processing

Table 2.13. Technology Specific Level 3 Model Modified Relationships

Function Block Producer	*Transfer Relationship*	*Function Block Receiver*	*Rationale*
		System, Process Fluid Handling System	
D-T Storage System	Tritium	Fusion Fuel Preparation System	Isotopically and chemically processed tritium suitable for fuel production
	Deuterium	Fusion Fuel Preparation System	Isotopically and chemically processed deuterium suitable for fuel production
Fusion Fuel Input Processing System	Tritium Breeding Fuel	Blanket Processing System	Lithium or lithium containing compounds for tritium breeding in blanket
	Blanket Make Up	Blanket Processing System	Make-up material for blanket from radiation, chemical induced blanket degradation
	Deuterium	D-T Processing System	Elemental or deuterium containing compounds from off-site sources
	Off-site Tritium	D-T Processing System	Elemental or tritium containing compounds from off-site sources (for start-up)
Fusion Exhaust Processing System	Hydrogen Isotopes	Hydrogen Isotope Separation System	Mixed hydrogen isotopes chemically separated from fusion exhaust streams
	Hydrogen Isotope Bypass	Fusion Fuel Preparation System	Mixed hydrogen isotopes suitable for fuel production without separation, processing
	Reaction Byproducts	Waste Handling System, Radiological Waste Handling System, Process Fluid Handling System	Non-hydrogen reaction byproducts removed from fusion exhaust streams
	Other Waste Gasses	Waste Handling System, Radiological Waste Handling System, Process Fluid Handling System	Process fluids, other consumable wastes removed for steady state operation
Fusion Fuel Preparation System	D-T Fuel	Plasma Fueling System	D-T fuel in physical, chemical form for reactor fueling
	NB Heating Isotopes	Plasma Heating System	Fuel isotopes in physical, chemical form for neutral beam heating injection
Plasma Fueling System	D-T Fuel	Torus / Vacuum Vessel	D-T fuel input to sustain steady state plasma
Plasma Heating System	RF Heating	Torus / Vacuum Vessel	Electromagnetic heating of confined plasma to achieve steady state conditions

Table 2.13. Technology Specific Level 3 Model Modified Relationships

Function Block Producer	*Transfer Relationship*	*Function Block Receiver*	*Rationale*
Radiological Waste Handling System	Mixed Hydrogen Species	Hydrogen Isotope Separation System	Mixed hydrogen isotopes collected from other plant waste streams for processing

The technology specific Level 3 System Engineering model did not require substantial realignment of function block relationships from the general Level 3 System Engineering model. The most significant transfer relationship changes relate to the function block fundamentally changed between the general and technology specific model: the Torus Cooling / Fusion Breeding Blanket. Combining the functional requirements of converting energetic particles to thermal energy, transferring thermal energy to the BOP systems, and producing fusion fuel using energetic nuclear reactions results a modification of the relevant system inputs and outputs. Other changes to transfer relationships included specification of the fusion fuel (deuterium and tritium) through the components in the "Fusion Power Area". Finally, an additional set of "bypass" transfer relationships are developed for the technology specific system engineering model. These Hydrogen Isotope, Tritium, and Deuterium Bypass transfer relations highlight the possibility shortening the closed fuel cycle processing time by bypassing the D-T Storage System or even bypassing the Hydrogen Isotope Separation System and directly routing mixed hydrogen species from the Fusion Exhaust Processing System to the Fusion Fuel Preparation System. These bypasses could significantly reduce the required design capacity and hazard inventories associated with these processing systems but could complicate the processing requirements for the Fusion Fuel Preparation System. These operational and design choices require more detailed design to specify but including the bypasses in this model allows general consideration of their effects.

2.4 Comparison to Prior Commercial Fusion Facility Design Studies

The technology specific system engineering model developed in this work can be compared against prior major design studies for power generating demonstration or commercial fusion facilities. The following design studies were reviewed:

- 1980 Starfire Project [11]
- 1982 Argonne National Lab (ANL) DEMO Project [12]
- 1992 ARIES II and ARIES IV Design Study Project [13][14]
- 2004 European DEMO Project [15]

The system engineering model developed in this work was consistent with the plant designs proposed in prior design studies. It is noted, however, that the prior work would often vary in their level of decomposition for certain function blocks. For example, in the 1992 ARIES and 2004 European DEMO studies, there was significantly more detailed design information available for the "Fusion Power Area" systems and much less functional system information was available for other plant systems. For the 1980 Starfire and 1982 ANL DEMO studies, the system information appeared to include two or more additional levels of functional decomposition on the plant function blocks. The functional relationships between systems, however, appeared to align the system engineering model in this work. This initial assessment suggest that the technology specific system engineering model developed in this work is sufficiently accurate to facilitate the identification of hazards for licensing assessments.

This works appears to be the first, standardized and design agnostic system decomposition of a commercial fusion facility. This process enables the general discussion of commercial fusion facility operations without prescription of form or technology. This approach is valuable in assisting in the evaluation of safety and development of regulatory requirements for a novel technology by allowing for the general discussion of hazards. Innovative approaches to design are facilitated by not presuming form. This model could be further generalized to include direct energy capture or non-electricity applications of fusion energy. Changes to the Level 2 function model would likely be required, but these changes would be reflected in the Level 0 and Level 1 concept of operations.

This work aligns with previous design studies and captures many of the general lessons learned but can serve as the basis for future discussions on the identification of major systems and major hazards for commercial fusion facility conceptual designs.

2.5. Summary of Technology Specific System Engineering Model

The technology specific system engineering model developed in this section provides a framework for the systematic identification of hazards. Development of this model from a technology independent model may enable insights into regulatory frameworks that would be compatible with a variety of technology approaches to fusion energy and do not require technology specific regulatory requirements. The history of commercial fission regulation demonstrates how development of technology specific, prescriptive regulatory requirements may increase short-term regulatory certainty but can discourage technological innovation due to the additional regulatory barriers.

The technology specific system engineering model attempts to prevent evaluation of commercial fusion facility design through a physics centered paradigm. Fusion facilities have historically been scientific laboratories, with a focus on the testing and understanding of new physical phenomena. As a result, there has been an design focus on the fusion reactor and associated scientific instrumentation and controls. While a focus on the fusion reactor is important, a commercial fusion facility will be much larger in scope than the fusion reaction occurring at the core of the device. The Level 3 System Engineering model begins to highlight the scope of the facility outside of the reactor torus, vacuum vessel, and magnetic controls that are normally the focus of fusion facility design activities.

This technology specific system engineering model requires significant refinement before it would be useful in most design or regulatory applications. Multiple additional levels of functional decomposition would be required before a more complete evaluation of hazards would be possible. This model starts to demonstrate how a system's engineering approach shows the wider scope of the facility and potential hazardous systems outside of the fusion reactor. Additional decomposition may require implicit or explicit definition of system form but may be possible on a design agnostic level for some function blocks.

The technology specific Level 3 commercial fusion facility is used in the following chapters to enable the preliminary identification of hazards for licensing evaluations and regulatory assessments of proposed facilities.

2.6. References

[1] J. H. Kim and A. R. Scialli. Thalidomide: the tragedy of birth defects and the effective treatment of disease. *Toxicological sciences*, 122(1):1–6, 2011.

[2] Environmental Protection Agency. DDT: A review of scientific and economic aspects of the decision to ban its use as a pesticide. Technical report, Environmental Protection Agency, July 1975.

[3] B. Blankespoor, S. Dasgupta, A. Lagnaoui, and S. Roy. Health costs and benefits of DDT use in malaria control and prevention. *World Bank Policy Research Working Paper*, (6203), 2012.

[4] C. Rehwagen. WHO recommends DDT to control malaria. *Bmj*, 333(7569):622, 2006.

[5] J. R. Nash and R. L. Revesz. Grandfathering and environmental regulation: the law and economics of new source review. *Nw. UL* Rev., 101:1677, 2007.

[6] Department of Energy. Advanced reactor demonstration funding opportunity announcement. Technical Report FOA DE-FOA-0002271, Amendment 000002, Department of Energy, 2020.

[7] *System Engineering Fundamentals*. U.S. Department of Defense, 2001.

[8] R. W. Best. Advanced fusion fuel cycles. Fusion Technology, 17(4):661–665, 1990.

[9] Sorbom, B et al. ARC: A compact, high-field, fusion nuclear science facility and demonstration power plant with demountable magnets. *Fusion Engineering and Design*, 100:378–405, 2015.

[10] National Academies of Sciences, Engineering, and Medicine. *Final Report of the Committee on a Strategic Plan for U.S. Burning Plasma Research*. The National Academies Press, Washington, DC, 2019.

[11] *STARFIRE: A Commercial Tokamak Fusion Power Plant Study*, volume 80. Argonne National Laboratory, 1980.

[12] Abdou, M et al. A demonstration tokamak power plant study (DEMO). *Argonne National Laboratory*, (ANL/FPP-82-1), 1982.

[13] Sharafat, S et al. Design layout and maintenance of the ARIES-IV tokamak fusion power plant. In 15th IEEE/NPSS Symposium. *Fusion Engineering*, volume 1, pages 417–420. IEEE, 1993.

[14] J. S. Herring, K. A. McCarthy, and T. J. Dolan. Safety analyses of the ARIES-II and ARIES-IV tokamak reactor designs. In 15th IEEE/NPSS Symposium. *Fusion Engineering*, volume 2, pages 1033– 1036. IEEE, 1993.

[15] D. Maisonnier, I. Cook, P. Sardain, R. Andreani, L. Di Pace, R. Forrest, et al. A conceptual study of commercial fusion power plants.—final report of the European fusion power plant conceptual study, EFDA (05)-27/4/10, revision 1 April 2005. Technical report, EFDA-RP-RE-5.0, 2005.

Chapter 3 - Assessing the hazards of a commercial fusion facility

The systems engineering models developed in Chapter 2 provide a framework for the determination and assessment of hazards important to licensing. The precise hazards, magnitudes, frequencies, and other characteristics of a commercial fusion facility will be design specific, but creation and evaluation of regulatory approaches for commercial fusion requires a common set of hazards generally applicable to fusion technology.

The focus of this section is on the definition, selection, and characterization of hazards for commercial fusion technology. First, a general hazard evaluation process is used as the basis for identification of hazards relevant to commercial fusion technology. Second, a characterization of hazards is presented based on whether they contribute to on-site adverse consequences or off-site adverse consequences (on-site and off-site hazards). Third, hazards are characterized based on their potential to create on-site or off-site adverse consequences. Finally, hazards for licensing are selected for evaluation in Chapter 4.

3.1 Safety evaluations, consequences, and underlying hazards

The main purpose of any safety evaluation is to determine the possible adverse consequences associated with an activity, or operation of a component, system, or facility. Adverse consequences can encompass a wide variety of physical, psychological, economic, and social harms. In this work, a broad definition of adverse consequences from *Guidelines for Hazard Evaluation Procedures* by the Center for Chemical Process Safety is adapted as the basis for safety evaluations and hazard assessments [1].

Figure 3.1 shows how adverse consequences can be broadly divided into three areas: human impacts, environmental impacts, and economic impacts. Hazards are therefore defined in this work as any state, substance, or situation that can produce an adverse consequence. This definition separates hazards from initiating events. Initiating events are defined as an event or set of events that enable a hazard to produce an adverse consequence.

There is a tendency in preliminary safety evaluations to focus on analysis of initiating events as the basis for evaluations. An initiating event focus follows the following logic:

- What are the possible initiating events for an off-normal condition or accident at a facility?
- What hazards would be affected by the initiating event and subsequent events?
- What are the adverse consequences associated with the proposed event sequences?

This approach works well for well-characterized or simple systems where the initiating event space and subsequent system behavior and interactions are known. For poorly characterized systems (e.g., early in the design cycle, limited operating experience), complex systems, or novel systems, this approach may be much less effective. Limited understanding of initiating events or interacting event sequences that could lead to the adverse consequences can result incomplete or misleading safety evaluations.

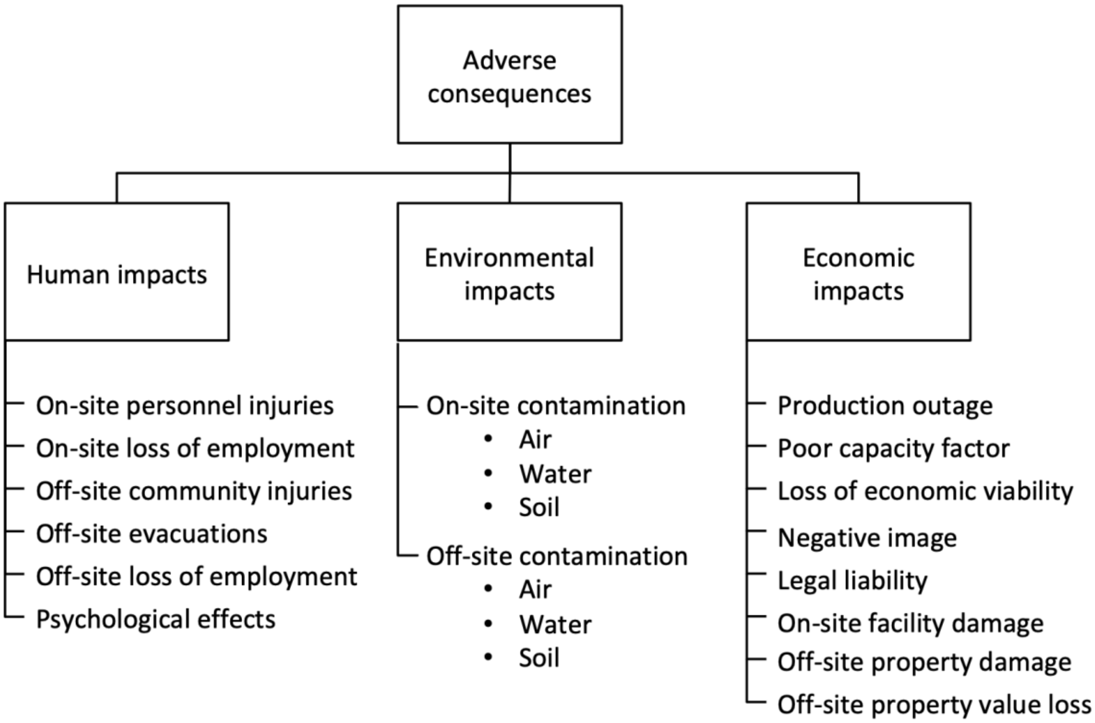


Figure 3.1. Adverse consequence categorization for commercial energy facilities (adapted from Figure 3.1 *Guidelines for Hazard Evaluation Procedures* [1])

Commercial fusion systems will inherently be complex systems due to the specific and extreme physical conditions required to create and sustain fusion reactions. In addition, the limited operating experience and wide variety of proposed fusion technologies ensure that, at the very least, initial commercial fusion systems will not be well characterized. Use of an initiating event based approach to safety evaluations may therefore not be appropriate for commercial fusion facilities. Instead, a hazard-centered approach to safety evaluations may be desired.

In this work, a hazard-centered approach is used as the focus basis for preliminary safety evaluations. A hazard-centered focus follows the following logic:

- What are the inherent hazards of a facility?
- What are the potential adverse consequences associated with the inherent hazards, independent of event sequences?

- What are inherent, engineered, or administrative safeguards or controls are in place to prevent the adverse consequences?
- What initiating events and subsequence events can lead to breakdown of these safeguards and controls?

While the difference between these an initiating event centered approach and a hazard-centered approach is subtle, a hazard-centered approach focuses on control and mitigation of hazards rather than on prevention of accident sequences or initiating events. A hazard centered approach enables the initial conclusions of preliminary safety evaluations to be incorporated into the design process because the evaluations are based on inherent system characteristics and not specific event sequences. Incorporation of preliminary evaluations into final facility design facilitates design focus on limiting inherent hazards rather than trying to prevent all accidents. A focus on eliminating or mitigated hazards can help produce a more robust design for complex or poorly characterized systems.

One limitation of use of a hazard-centered approach for novel systems, however, is the potential for unidentified or unknown hazards that may lead to losses. Robust and detailed characterization of an activity or facility is critical to ensuring that all major hazards are identified and that analyses are updated if operating experience reveal previously uncharacterized or described hazards.

In this work, the hazards associated with commercial fusion are developed based on the system models for commercial fusion presented in Chapter 5 and the hazard analysis method prescribed for use by the U.S. Department of Energy (DOE) in the "Hazard And Accident Analysis Handbook" [2]. While alternative methods can be used to develop a list of hazards for commercial fusion, this method was selected due to its prior use on the analysis of both chemical and radiological hazards at large industrial facilities.

3.2 Identifying possible hazards for industrial facilities

The initial step of any safety evaluation method should be hazard identification. Safety evaluations are ultimately rooted in determining the potential adverse consequences of a facility, system, or process related to the hazards present in a system. Identification of potential hazards (both inherent to a process and created through design choices and engineered design features) should be a first step in performing safety evaluations of engineered processes, systems, and facilities. This work follows the hazard identification process outlined in the DOE "Hazard and Accident Analysis Handbook" [2].

The primary goal of a hazard identification process is to systematically identify all hazards present in a system. It is important to note that the process for identifying hazards is different from the process of identifying possible pathways or scenarios for hazard exposure or release. The Hazard Analysis Handbook notes "(t)he overall quality of hazard scenario definition will be in direct proportion to the accuracy and completeness of the initial hazard information gathered." [2]. Hazard identification started early in the design process can help mitigate or eliminate hazards by design rather than relying on engineering or administrative design to control hazards.

The hazard identification process involves collecting all relevant data for plant, system, or component level operations, recording data to ensure completeness, and evaluating the applicability of the hazard for inclusion or exclusion from subsequent analyses [2]. This hazard identification process works well for systems that are well characterized, already designed, or have significant operating experience (at that facility or related facilities). This process is more challenging for emerging technologies because of limited design data and limited (or no) operating experience with related systems or components. While this may initially appear as a setback for the safety evaluation of commercial fusion technology, it presents a unique opportunity. Early consideration of inherent system hazards and incorporation of safety evaluation into preliminary design enables incorporation of hazard reduction and inherent safety into the design.

Due to the limitations on design data and operating experience for commercial fusion facilities, the hazard identification process normally used for other technologies is reordered. A structured process is first used to facilitate development of a comprehensive list of hazards relevant to regulatory activities. The Level 3 Tokamak System Engineering Model is then evaluated against the comprehensive list of hazards to characterize systems of regulatory interest based on current state of knowledge regarding the design and engineering of tokamak systems. The applicability evaluation will be intentionally broad and lack detailed design information. The goal is to encompass the full design space and highlight areas where additional detail is needed and where designers should focus particular attention to reduction or elimination of inherent hazards by design. Stated another way, this approach emphasizes safety as an inherent function of the design iterations, rather than as a sequential assessment of technical then safety viability.

A generalized hazard checklist provided in the DOE Accident Analysis Handbook (from Table 2-1: "Hazard Identification Checklist Example") is selected as the initial basis for the identification of hazards for commercial fusion [2]. This hazard checklist contains 22 categories of hazards and initiating events for chemical and radiological facilities and each category is further subdivided into specific hazards.

In addition to these hazards, an additional category of "Superconducting Magnets" is added to the initial hazard identification checklist. Not all commercial fusion technology approaches may utilize superconducting magnets as part of a plasma containment strategy. The use of high magnetic fields in a significant number of technologies as well as the unique hazards of superconducting magnets warrant their inclusion in a comprehensive hazard evaluation process. Specific hazards of interest related to superconducting magnets include cryogenic hazards (both thermal and potential pressures hazards from expanding coolants) and electrical hazards (high voltage electrical arcing and other releases of stored electrical energy related with loss of superconductivity). While this hazard is largely covered by other categories, it is included to provide insights into whether superconducting magnets should be considered a significant regulatory risk as part of the licensing process.

Table 3.1 lists the 23 categorical hazards initially considered for the hazard identification process. These 23 categorical hazards are characterized in the following section based on the potential for adverse consequences.

Table 3.1. Initial Hazard Identification Categorizations.

Number	*Hazard Category*	*Number*	*Hazard Category*
1.0	Electrical	13.0	Internal Flooding Sources
2.0	Thermal	14.0	Physical
3.0	Pyrophoric Material	15.0	Radioactive Material
4.0	Spontaneous Combustion	16.0	Hazardous Material (Toxicological, Chemical)
5.0	Open Flame	17.0	Direct Radiation Exposures
6.0	Flammables	18.0	Non-ionizing Radiation
7.0	Combustibles	19.0	Criticality
8.0	Chemical Reactions	20.0	External Man-made Events
9.0	Explosive Material	21.0	Vehicles in Motion
10.0	Kinetic (Linear and Rotational)	22.0	Natural Phenomena
11.0	Potential (Pressure)	23.0	Superconducting Magnets
12.0	Potential (Height/Mass)		

3.3 Characterizing hazards and adverse consequences

One drawback of the generalized hazard identification process discussed in Section 3.2 is that it creates requires consideration of a wide range of hazard categories for a large number functional system blocks highlighted in the Level 3 Technology Specific System Engineering Model for a commercial fusion facility. A screening method is developed and used in to evaluate which hazard categories are of greatest concern for the preliminary safety evaluation of a commercial fusion facility.

The hazard category screening method is based on two assessment metrics:

- Qualitative assessment of adverse consequence regulatory importance (F_{RI})
- Qualitative assessment of the adverse consequence severity (qualitatively assessed based on the adverse consequence category) for each hazard category (F_{CS})

These two qualitative assessments are performed on a zero to three rating scale. The product of the two quantitative factors is used to create a composite hazard category index (HCI) for each pair of hazard adverse and consequence:

$$HCI = F_{RI} \times F_{CS}$$

The HCI scores for each hazard are to prioritize and select hazards important in development of a new licensing and regulatory framework for commercial fusion. The HCI score is not a final evaluation of the importance of a hazard for licensing and regulation;

instead, the HCI provides a metric for prioritizing the review of hazards of commercial fusion facilities. This may ultimately help commercial fusion designer determine which hazards will need to managed and evaluated to meet fusion specific regulatory requirements and which hazards will need to be managed to more general worker safety regulations or business considerations.

3.3.1 Adverse consequences regulatory importance

The first assessment metric in the hazard category screening method is to categorize the adverse consequences shown in Figure 3.1 based on their level of regulatory importance. The level of regulatory importance reflects the level of public interest, regulatory requirements, and regulatory reviews associated with an adverse consequence. Reviewing the types of adverse consequences provide insights into level of regulatory importance for each consequence.

The three broad areas of adverse consequences (human impacts, environmental impacts, and economic impacts) can be subdivided into discrete adverse consequences (shown in Figure 3.1). These subdivided adverse consequences are:

- Human impacts
  - On-site personnel injuries
  - On-site loss of employment
  - Off-site community injuries
  - Off-site evacuations
  - Off-site loss of employment
  - Off-site psychological effects
- Environmental impacts
  - On-site contamination
    - Soil
    - Air
    - Water
  - Off-site contamination
    - Soil
    - Air
    - Water
- Economic impacts
  - Production outage
  - Poor capacity factor for the fusion facility
  - Loss of economic viability
  - On-site facility damage
  - Legal liability
  - Negative corporate image
  - Off-site property damage
  - Off-site property value loss

This list of adverse consequences broadly encompasses the possible adverse consequences associated with the on-going operation of a commercial fusion facility for power production. It is possible to generate adverse consequences associated with other phases of operation (e.g., loss of environmentally sensitive areas due to construction) but these are outside the scope of the safety analyses discussed in this work. Existing environmental laws such as the National Environmental Policy Act would normally cover review of the adverse consequences associated with these other phases. These laws require additional environmental and social reviews of the adverse consequences resulting from federal permitting or regulatory actions.

The listing of adverse consequences separates the human, environmental, and economic impacts for consideration but it important to note that many of the adverse consequences are often coupled but are not inherently coupled. The concept of "machine safety" and "personnel safety", for example, tend to be closely linked due to rational that "personnel safety" can only be assured through "machine safety". While this coupling may be present, it focuses on the machine failure as an initiating event and may not fully address all underlying relevant hazards and system interactions. Errors in design or operation may result in personnel harm without machine failure. Conversely, safety forward design may enable the safe failure of machines that decouples machine safety and failure with personnel safety. As a result, these adverse consequences are evaluated separately to allow for the characterization of designs where the effects are both coupled and decoupled.

There are a variety of ways to characterize these adverse consequences and their regulatory importance. Metrics such as financial impact (based on the assessment of monetary value of human lives and environmental damage) may be obvious to use but do not necessarily reflect the observed relationship between adverse consequences and level of regulatory importance and review. In this work, the effect of adverse consequences both on-site and off-site is used as the main characterizing factor for regulatory impact.

If a technology only has on-site adverse consequences, the risks posed by the technology are limited to those directly involved with operations. On-site adverse consequences may impact areas such as worker safety, operational reliability, and overall asset protection. Risks are not borne by the public but are limited to facility workers, site management, and financial stakeholders. As long as the public perceives workers as adequately protected (e.g., through adequate workplace safety regulations or employer safety programs), imposed regulations will likely be minimal. Owners, operators, and insurers will primarily determine their own level of acceptable risk for on-site adverse consequences, subject to guidance from industry groups (e.g., consensus codes and standards).

If a technology has off-site adverse consequences however, some of the risks posed by the technology are imposed on the community and environment surrounding the facility. Both public health and environmental quality can be impacted by off-site adverse consequences. Potential harm to non-stakeholders (many of whom may not proportionally benefit from the technology) may reduce the socially acceptable level of risk. Reduced tolerance for off-site consequences can drive legislation, regulation, or other government activities to reduce potential consequences, even if the risk is small relative to other societal risks.

Severity of potential off-site adverse consequences for a technology has historically been correlated with the level of regulatory review and oversight imposed on them. Regulatory involvement is largely driven by social demand for accountability and protection from adverse consequences.

On-site facility safety is a key facet of industrial design and development but regulatory review of worker safety in the United States is largely reactive. While there are prescriptive requirements on work place safety, regulatory reviews performed by the U.S. Occupational Health and Safety Administration (OSHA) of compliance with these requirements is prioritized based on reported incidents, worker complaints, and inspection referrals [3]. While worker safety may be important to the public, public and political pressure is rarely significant enough to prevent facility or industry operation due to burdensome regulatory review or requirements.

For industries with the potential for off-site adverse consequences, the level of regulatory review and required documentation may be increased. Three highlighted industries with varying levels of off-site adverse consequences are chemical processing, the commercial aircraft design, and the nuclear fission power plants. While all three have perceived off-site adverse risks, the magnitude of their worst-case adverse consequences varies significantly.

Historically, chemical processing sites have substantial on-site adverse consequences but the off-site adverse consequences are limited. While the 1984 methyl isocyanate release at the Union Carbide facility in Bohpal, India killed thousands and injured hundreds of thousands, most major chemical plant incidents primarily produce on-site adverse consequences [4]. The 2013 West Fertilizer Company explosion destroyed a fertilizer production facility, killing 12 workers on-site and 3 members of the public off-site [5]. These off-site fatalities and over 260 additional injuries, while tragic, are limited off-site consequences relative to the damage produced by the blast. Similarly, while the 2017 Arkema accident (explosion and release of organic peroxides) caused significant off-site concern and some minor health effects, there were few long term or substantial off-site consequences [6]. As a result, while the chemical processing industry has a potential for off-site adverse consequences, these worst-case off-site adverse consequences are normally limited.

The U.S. Environmental Protection Agency (EPA) requires companies that handle sufficient quantities of toxic chemicals or other hazardous materials with potential significant off-site adverse consequences to submit Risk Management Plans (RPM). The RMP details the facility hazards, worst-case release consequences, and the mitigating design and response actions that can reduce the adverse consequences associated with a major accident. While the documents are checked during submission for completeness, submission information is only confirmed by the regulatory during RMP Audits that are conducted periodically or as part of follow-up action based on reported incidents, incidents at similar facilities, or as part of a facility hazard prioritization program [7]. These requirements are primarily designed to help provide workers and the public with information about potentially hazardous processes, and require operators to acknowledge their risk planning processes.

Thus, a low level of regulatory concern correlates with a potential for limited off-site adverse consequences.

Commercial aviation safety has evolved over the past century due, in large part, to public pressure over the off-site adverse consequences associated with the technology. In this specific case, loss of passenger life during a commercial aircraft accident is considered an off-site adverse consequence due to the modern perception that commercial aviation travel should not present an undue risk to the public. The off-site adverse consequences of accidents involving commercial aircraft can be significant and result in hundreds of fatalities in a single incident. Two high profile crashes related to suspected design flaws in the Boeing 737 Max aircraft in 2018 and 2019 resulted in 333 public fatalities and caused regulators around the world to suspend flights of the Boeing 737 Max aircraft [8]. Public concern over the safety of commercial aircraft and demands for reduced off-site adverse consequences has resulted in a greater level of regulatory review and required documentation.

The U.S. Federal Aviation Administration (FAA) has jurisdiction over all phases of commercial aviation including design, manufacturing, and operation. The increased potential for off-site adverse consequences has resulted in a higher level of regulatory review and scrutiny for the design of commercial aircraft. Despite the potential for off-site (public) adverse consequences, however, the FAA and predecessor organizations have recognized the need to focus oversight and review efforts for commercial aviation to balance both the "safety and efficiency" [9]. While the FAA requires that substantial regulatory documentation be produced to support the development, design, and deployment of commercial aircraft, the level of regulatory review may differ. The FAA's use of "delegated authority" and "design organization certificates" enable the FAA to authorize companies to self-certify that portions of designs meet all appropriate regulatory requirements [10]. While the off-site adverse consequences are serious for commercial aviation, these consequences are not severe enough to require full regulatory review of all regulatory documents, enabling a targeted and delegated regulatory review process.

For commercial nuclear fission technology, understanding of the off-site adverse consequences has evolved parallel to the development of plants in terms of both reactor size and engineering design. The potential for off-site adverse consequences was recognized by the scientists and engineers that created the first experimental and plutonium production reactors during the Manhattan Project [11]. Remote siting of reactors served to provide secrecy, security, and safety for the new facilities.

Scientists and engineers at the Hanford plutonium production reactors site did not know the specific off-site consequences of a nuclear reactor accident, but recommended an exclusion zone of 0.01 $\sqrt{P_r}$ miles around the reactor where P_r was the reactor power in kilowatts [12]. This was a clear recognition of the potential for off-site adverse consequences – although the exact magnitude was unknown.

As reactors grew in power from kilowatts to tens and hundreds of megawatts, regulators at the U.S. Atomic Energy Commission (AEC) sought to quantify these adverse consequences. The 1957 WASH-740 report "Theoretical possibilities and consequences of major accidents in large nuclear power plants" analyzed the full off-site adverse consequences of different major accidents at a 500 MW thermal fission power plant [13]. The report finds that in the unlikely (but theoretically possible) case of release of 50% of the reactor core inventory, under worst case conditions the off-site adverse consequences could include [13]:

- 3,400 public fatalities,
- 43,000 injuries,
- 460,000 evacuated,
- 1,500,000 living in contaminated areas, and
- 150,000 square miles unusable for farming

The report authors stressed that these off-site adverse consequences were highly unlikely but an emphasized the potential severity of nuclear reactor accidents. Reactors continued to increase their thermal power through the thousands of megawatts and the AEC sought to have Brookhaven National Lab update the WASH-740 report in 1964 [14]. The AEC had expected better system characterization and engineered safety features to have reduced off-site adverse consequences but the increased reactor size and better characterization of accident dynamics instead dramatically increased the calculated consequences [15]. The updates to the WASH-740 report were never published but AEC memos regarding the report stated it presented an "inescapable calculation [that] damages would result possibly 100 times as large as those calculated in the previous study"[15].

While the consequences would likely scale linearly with reactor power and radioactive fission product inventory, these early calculations demonstrated that catastrophic off-site adverse consequences were mechanistically possible, if not highly improbably, for large commercial fission facilities.

The U.S. Nuclear Regulatory Commission (NRC) has jurisdiction over commercial nuclear power plants and civilian uses of radiological material. The potential catastrophic severity of large fission power plant accident off-site adverse consequences has resulted in a high level of regulatory review and scrutiny for commercial nuclear power. The NRC's mission is to "protect public health and safety" and does not require the agency to balance the benefits of nuclear technology against the hazards [16]. For new commercial nuclear reactors, detailed regulatory documentation covering a wide range of design conditions are prepared and submitted as part of the licensing process. NRC technical staff performs independent confirmatory calculations to ensure the completeness and accuracy of regulatory documentation [17]. Technical advisory panels independent of both the NRC and the commercial nuclear industry review and must approve license application [18]. Public hearings on both administrative matters and technical subjects are required to ensure that citizens groups may comment on or challenge the pending licenses [18]. For this industry, the potential for severe off-site adverse consequences warrant full regulatory review of all regulatory documents and a high level regulatory burden.

Historical experience from these three industries with the potential for off-site adverse consequences demonstrates that the level of regulatory review and required documentation correlates with the presence and severity of off-site consequences. All three industries (chemical processing, the commercial aircraft design, and the nuclear fission power plants) have perceived off-site adverse risks but the magnitude of their worst-case adverse consequences varies significantly. All three industries are regulated and the actual level of regulatory review and associated regulatory burden differs based on the severity of the off-site adverse consequences.

The potential regulatory importance of adverse consequences is useful when screening the importance of different hazard categories. A simple qualitative ranking assessment is used to create adverse consequence regulatory importance factor, F_{RI}. An adverse consequence regulatory importance factor is assigned based on the following simple ranking in Table 3.2 for each of the adverse consequences listed in Figure 3.1.

Table 3.2. Regulatory importance factors

F_{RI}	*Factor Criteria*
3	High regulatory importance (Off-site adverse consequences)
2	Medium regulatory importance (On-site adverse consequences)
1	Low regulatory importance or only economic importance
0	No regulatory or economic importance

These regulatory importance factors are based solely on the adverse consequences, so they can be assigned independent of the hazards in Table 3.1. A regulatory importance factors is assigned to each of the adverse consequences in Table 3.3.

Table 3.3. Consequence specific importance factors.

Adverse consequence	*Consequence importance factor (F_{CS})*
Off-site community injuries	3
Off-site evacuations	3
Off-site property damage	3
Off-site property value loss	3
Off-site loss of employment	3
Off-site psychological effects	3
Off-site contamination	3
On-site personnel injuries	2
On-site loss of employment	2
On-site contamination	2
On-site facility damage	2
Legal liability	2

Table 3.3. Consequence specific importance factors.

Production outage	1
Poor capacity factor	1
Loss of economic viability	1
Negative corporate image	1

This importance factor ranking process allows for consistent categorization and discussion of hazard importance based on the regulatory and social impact of different potential adverse consequences.

3.3.2 Adverse consequence severity magnitude

The second part of the hazard category screening method is to assess the potential severity of adverse consequences (Figure 3.1) that could be caused by each of the hazard categories (Table 3.1). A simple qualitative assessment is used to create adverse consequence magnitude factor, F_{CM}, for each pair of hazard category and adverse consequence. The factor is based on the potential maximum severity of an adverse consequence directly caused by a hazard category. The qualitative severity factors are defined in Table 3.4.

Table 3.4. Adverse consequence magnitude factors

F_{CM}	*Factor criteria*
3	High severity potential
2	Moderate severity potential
1	Low severity potential
0	No potential for consequence
N/A – IE	Not Applicable – Initiating Event external to facility hazards
N/A – NP	Not Applicable – Not Present hazard in any future fusion facility

Two additional exclusion categories (N/A – IE and N/A – NP) are added to the numeric scale to allow for the exclusion of hazard categories not relevant to an initial assessment of inherent facility hazards.

Note that the adverse consequence magnitude factor specifically relates to the adverse consequence severity directly attributable to category and not related to any events simply initiated by the hazard (e.g., while an open flame can initiate a fire or explosion that causes off-site community injuries, it would not cause off-site community injuries directly).

An adverse consequence magnitude factor is assigned for each hazard category and each adverse consequence pair. The factor were assigned base on a qualitative assessment of the potential maximum severity of an adverse consequence directly caused the hazard category. These factors are listed for all pairs in Table 3.5.

Table 3.5. Hazard category specific adverse consequence magnitude factors

		Human							*Environmental*			*Economic*								
No.	*Hazard Category*	*Category Max*	*On-site personnel injuries*	*On-site loss of employment/facility*	*Off-site community injuries*	*Off-site evacuations*	*Off-site loss of employment*	*Off-site psycological effects*	*Category Max*	*On-site Air, Water, Soil Contamination*	*Off-site Air, Water, Soil Contamination*	*Category Max*	*Production outage*	*Poor capacity factor*	*Loss of economic viability*	*On-site facility damage*	*Legal liability*	*Negative image*	*Off-site property damage*	*Off-site property value loss*
1.0	*Electrical*	3	3	0	0	0	0	1	0	0	0	3	3	3	2	2	1	1	0	0
2.0	*Thermal*	3	3	0	0	0	0	1	0	0	0	3	3	3	2	2	1	1	0	0
3.0	*Pyrophoric Material*	3	3	1	1	1	0	2	1	1	1	3	3	3	2	2	1	2	1	1
4.0	*Spontaneous Combustion*	3	3	1	1	1	0	2	1	1	1	3	3	3	2	2	1	2	1	1
5.0	*Open Flame*	3	3	1	0	0	0	1	0	0	0	3	2	2	1	1	1	1	0	0
6.0	*Flammables*	3	3	2	2	1	0	1	2	2	2	3	3	2	3	3	2	2	2	1
7.0	*Combustibles*	3	3	1	1	1	0	1	1	1	1	3	2	1	1	1	1	1	1	1
8.0	*Chemical Reactions*	3	3	2	2	2	0	2	1	1	1	3	3	3	2	2	2	2	1	1
9.0	*Explosive Material*	3	3	3	3	2	1	2	2	2	2	3	3	3	3	3	2	3	3	1
10.0	*Kinetic (Linear and Rotational)*	3	3	1	0	0	0	0	0	0	0	3	2	3	2	3	1	1	0	0
11.0	*Potential (Pressure)*	3	3	2	1	0	0	1	0	0	0	3	3	3	3	3	1	2	1	0
12.0	*Potential (Height/Mass)*	3	3	1	0	0	0	0	0	0	0	3	2	1	3	3	1	1	0	0
13.0	*Internal Flooding Sources*	2	2	2	0	0	0	0	1	1	1	3	3	3	2	3	1	1	0	1
14.0	*Physical*	2	2	0	0	0	0	1	0	0	0	3	1	0	1	0	2	1	0	0
15.0	*Radioactive Material*	3	3	2	3	3	3	3	3	3	3	3	3	3	3	1	3	3	3	3
16.0	*Hazardous Material (Toxic, Chemical, Biological)*	3	3	2	3	3	3	3	3	3	3	3	3	3	3	2	3	3	3	3
17.0	*Direct Radiation Exposures*	3	3	0	2	1	1	3	1	1	1	3	2	2	3	1	3	3	2	1
18.0	*Non-ionizing Radiation*	3	3	0	1	0	0	2	0	0	0	3	1	3	2	1	3	3	1	0
19.0	*Criticality*	N/A - NP							N/A - NP			N/A - NP								
20.0	*External Man-made Events*	N/A - IE							N/A - IE			N/A - IE								
21.0	*Vehicles in Motion*	N/A - IE							N/A - IE			N/A - IE								
22.0	*Natural Phenomena*	N/A - IE							N/A - IE			N/A - IE								
23.0	*Superconducting Magnets*	3	3	3	1	0	0	0	0	0	0	3	3	3	3	3	2	3	1	0

3.4 Identifying relevant hazards for commercial fusion

The relevant hazards for commercial fusion licensing are identified in a multi-step down select process.

1. Composite hazard category index (HCI) scores are calculated for each pair of hazard category and adverse consequences based on the inputs in Section 3.3 and Section 3.4.
2. Hazard categories are sorted based on the maximum HCI across all adverse consequences.
3. Hazard categories with an HCI of 9 (highest possible score) are selected for detailed evaluation and down selection to specific hazards (detailed in DOE Accident Analysis Handbook) that are relevant to a commercial fusion facility regulation and licensing based on a Level 0 system engineering model.

This down selection process produces a list of general hazards of regulatory interest applicable to any commercial fusion facility. Regulatory assessment of the specific hazards of interest for a particular commercial fusion technology or facility requires evaluation of a higher level, technology specific system engineering model. The following steps of the down select process are then completed to produce technology or facility specific regulatory hazards.

4. The list of functional system forms from a technology or facility specific higher level system engineering model (Level 3 or higher) is evaluated and systems with the greatest number of relevant hazards are further selected for hazard evaluation.
5. The selected system engineering functional systems are evaluated. The presence, form, and characteristics of each of the relevant hazards for the system are documented to support licensing assessments.

This final down select process can be completed for any particular commercial fusion technology or facility to generate the specific hazards of regulatory interest. For this work, the Level 3 D-T fueled tokamak specific system engineering model is selected. This process results in the identification, down selection, and evaluation of the major hazards relevant for D-T fueled tokamak based commercial fusion facilities. These hazards are summarized and discussed in detail in Section 3.6.

3.4.1 Calculating and sorting technology independent composite HCI

The calculated HCI scores are presented in Table 3.6 based on the adverse consequence regulatory importance factors (F_{RI}) provided in Table 3.3 and the adverse consequence magnitude factor (F_{CM}) provided in Table 3.5.

The HCI scores are calculated and sorted based on the maximum HCIs for each of the three classes of adverse consequences (human, environmental, and economic impacts) and the overall maximum HCI score. The sorting priority used was (from highest to lowest) overall, human, economic, and environmental. The calculated and sorted HCI scores are provided in Table 3.6.

Table 3.6. Composite hazard category index scores for hazards

No.	Hazard Category	**Overall HCI**	**Human**							**Environmental**			**Economic**								
			Category Max	On-site personnel injuries	On-site loss of employment/facility	Off-site community injuries	Off-site evacuations	Off-site loss of employment	Psychological effects	Category Max	On-site Air, Water, Soil Contamination	Off-site Air, Water, Soil Contamination	Category Max	Production outage	Poor capacity factor	Loss of economic viability	On-site facility damage	Legal liability	Negative image	Off-site property damage	Off-site property value loss
15.0	Radioactive Material	**9**	9	6	4	9	9	9	9	9	6	9	9	3	3	3	3	2	6	9	9
16.0	Hazardous Material (Toxic, Chemical, Biological)	**9**	9	6	4	9	9	9	9	9	6	9	9	3	3	3	3	4	6	9	9
9.0	Explosive Material	**9**	9	6	6	9	6	3	6	6	4	6	9	3	3	3	3	6	4	9	3
17.0	Direct Radiation Exposures	**9**	9	6	0	6	3	3	9	3	2	3	6	2	2	3	3	2	6	6	3
6.0	Flammables	**6**	6	6	4	6	3	0	3	6	4	6	6	3	2	3	2	6	4	6	3
10.0	Kinetic (Linear and Rotational)	**6**	6	6	2	0	0	0	0	0	0	0	6	2	3	2	1	6	2	0	0
11.0	Potential (Pressure)	**6**	6	6	4	3	0	0	3	0	0	0	6	3	3	3	2	6	2	3	0
12.0	Potential (Height/Mass)	**6**	6	6	2	0	0	0	0	0	0	0	6	2	1	3	1	6	2	0	0
18.0	Non-ionizing Radiation	**6**	6	6	0	3	0	0	6	0	0	0	6	1	3	2	3	2	6	3	0
23.0	Superconducting Magnets	**6**	6	6	6	3	0	0	6	0	0	0	6	3	3	3	3	6	4	3	0
3.0	Pyrophoric Material	**6**	6	6	2	3	3	0	6	3	2	3	4	3	3	2	2	4	2	3	3
4.0	Spontaneous Combustion	**6**	6	6	2	3	3	0	6	3	2	3	4	3	3	2	2	4	2	3	3
8.0	Chemical Reactions	**6**	6	6	4	6	6	0	6	3	2	3	4	3	3	2	2	4	4	3	3
1.0	Electrical	**6**	6	6	0	0	0	0	3	0	0	0	4	3	3	2	1	4	2	0	0
2.0	Thermal	**6**	6	6	0	0	0	0	3	0	0	0	4	3	3	2	1	4	2	0	0
7.0	Combustibles	**6**	6	6	2	3	3	0	3	3	2	3	3	2	1	1	1	2	2	3	3
5.0	Open Flame	**6**	6	6	2	0	0	0	3	0	0	0	2	2	2	1	1	2	2	0	0
13.0	Internal Flooding Sources	**6**	4	4	4	0	0	0	0	3	2	3	6	3	3	2	1	6	2	0	3
14.0	Physical	**4**	4	4	0	0	0	0	3	0	0	0	4	1	0	1	1	0	4	0	0
19.0	Criticality		N/A - NP							N/A - NP			N/A - NP								
20.0	External Man-made Events		N/A - IE							N/A - IE			N/A - IE								
21.0	Vehicles in Motion		N/A - IE							N/A - IE			N/A - IE								
22.0	Natural Phenomena		N/A - IE							N/A - IE			N/A - IE								

3.3.2 Technology independent composite HCI down-selection

Calculation and sorting of the HCI scores reveals four hazard categories with HCI scores of 9 – representing hazard categories with both high regulatory importance and a potential for high severity adverse consequences. The four HCI score 9 hazard categories are:

- Radioactive Material
- Hazardous Material (Toxicological, Chemical, Biological)
- Explosive Material
- Direct Radiation Exposures

These four hazard categories are the hazard categories of greatest interest for regulatory evaluation. The importance of these hazard categories for regulatory evaluations is not surprising given historical precedent from other industries but the formal down selection process confirms the need to evaluate these hazards. This analysis indicates that these hazard categories would be the hazards with the highest regulatory importance regardless of the specific industry or activity.

These four hazard categories are expanded based on the full hazard identification checklists provided in the DOE Accident Analysis Handbook [2]. The four hazard categories each consist of between one and fifteen specific identified hazard types. Each of these categories is expanded and evaluated for against the Level 0 system engineering model in Chapter 5 to determine what specific hazards would be relevant for commercial fusion facility licensing.

The Level 0 system model was selected because it provides the most general applicability to any potential commercial fusion system. Each expanded hazard is categorized as "Present", "May be present", or "Not present" a Level 0 system model. The expanded hazards rated as "Present" or "May be present" are the basis the detailed model hazard identification. The expanded hazard down selection is detailed in Table 3.7. Ultimately, 27 hazards from the four hazard categories are selected for detailed hazard identification and evaluation. This is the last technology or facility independent step of the hazard identification process. The subsequent steps to identify, characterize, and quantify hazards must be performed on a specific technology, design, or facility.

Table 3.7. Consequence specific importance factors

Hazard Number	Hazard	Present in Level 0 System Model
15.1	Radioactive material	Present
16.1	Asphyxiants	Present
16.2	Bacteria/viruses	Not present
16.3	Beryllium and compounds	May be present
16.4	Biologicals/Biotoxins	Not present
16.5	Carcinogens	Present
16.6	Chlorine and compounds	May be present
16.7	Corrosives	Present
16.8	Decontamination solutions	Present
16.9	Dusts and particles	Present
16.10	Fluorides	Present
16.11	Hydrides	Present
16.12	Lead	Present
16.13	Oxidizers	May be present
16.14	Poisons (herbicides, insecticides, fungicides)	Not present
16.15	Other Hazardous Material	May be present
9.1	Caps	Not present
9.2	Dusts	Present
9.3	Dynamite	Not present
9.4	Electric squibs	May be present
9.5	Explosive chemicals	May be present
9.6	Explosive gases	May be present
9.7	Hydrogen	Present
9.8	Hydrogen (batteries)	Not present
9.9	Nitrates	Not present
9.10	Peroxides	May be present
9.11	Primer cord	Not present
9.12	Propane	Not present
9.13	Other Explosive Materials (e.g., NiCd batteries)	Present
17.1	Radiation Contamination	Present
17.2	Electron (or ion) beams	Present
17.3	Radioactive material	Present
17.4	Radioactive sources	Present
17.5	Radiography equipment	May be present
17.6	X-ray machines	May be present
17.7	Other Direct Radiation Exposures	Present

3.5 Separating technology specific hazards for commercial fusion facilities

Fusion reactions may be harnessed on a commercial scale using a variety of different specific technological approaches. Each of these different approaches will have different inherent hazards based on the reactions, byproducts, and conditions needed to sustain fusion reactions. These technological approaches can be generally categorized and separated based on their fusion fuel, fuel cycle, and specific plasma confinement technology design choices. Major categories for each characteristic include:

- Fusion fuel
    - Deuterium-deuterium
    - Deuterium-tritium
    - Deuterium-helium-3
    - Protium-boron-11
- Fuel cycle
    - On-site production and processing
    - On-site production, off-site processing
    - Off-site production and processing
- Plasma confinement
    - Magnetic confinement
    - Inertial confinement
    - Magneto-inertial confinement

Each combination of the fusion fuel, fuel cycle, and plasma confinement will introduce different technology specific hazards. Selection of a particular fusion fuel combination can introduce radioactive material into the fueling process or exhaust handling, and the resulting reaction products may activate surrounding materials from neutron irradiation. Selection of fuel cycle production and processing can present significantly different chemical and radiological hazards depending on the fuel inputs and outputs, the breeding method, and the processing methods. On-site production and processing eliminate transportation risks but concentrate and collocate these industrial processes with energy production facilities. Finally, the plasma confinement method introduces significantly different physical system requirements and results in a wider variety of hazards. Magnetic confinement requires high strength magnetic fields, inertial confinement requires extremely high energy lasers, and magneto-inertial confinement requires operation of high energy, high mass inertial systems. Each of these confinement approaches introduces different hazards into the facility and would require different methods to control, mitigate, and evaluate.

These significant hazard differences make more detailed regulatory evaluation of a technology independent commercial fusion facility largely infeasible based on the regulatory hazards of interest discussed in Section 3.4. The radioactive material, hazardous material, explosive material, and direct radiation exposure hazards will primarily be dominated by systems in the “Fusion Power Area” that vary on a technology specific basis. Some technology independent systems (e.g., Balance of Plant systems) could be characterized but will not likely have significant hazards of off-site concern. As a result, definition and evaluation of a technology specific commercial fusion facility is needed to provide meaningful insights into relevant hazards for commercial fusion facilities. This insight also suggests that generalized commercial fusion facility regulatory requirements should be developed in a performance based manner to enable the appropriate evaluation of design and technology specific hazards rather than relying on prescriptive requirements with significant exemptions.

3.6 Hazards for D-T tokamak commercial fusion facilities

The list of functional system forms for a specific technology or facility must be evaluated to enable the final identification of hazard. The Level 3 technology specific system engineering model for a deuterium-tritium fueled tokamak commercial fusion facility developed in Chapter 5 is analyzed in this work. The Level 3 model is reviewed and the system forms with the greatest number of relevant hazards are further selected for hazard evaluation. The model down-selection process identifies that 17 of the 39 system forms have inherent hazards in all four hazard categories.

This list of system forms is the basis for detailed hazard identification using the 27 down selected specific hazards of regulatory interest.

Table 3.8. Level 3 D-T Tokamak Specific System Engineering Model Hazard Identification

System Form	15.0 - Radioactive Material	16.0 - Hazardou s Material	9.0 Explosive Material	17.0 Direct Radiation Exposure	Hazard Categories Present
Blanket Processing System	Y	Y	Y	Y	4
D-T Processing System	Y	Y	Y	Y	4
D-T Storage System	Y	Y	Y	Y	4
Effluent Release System	Y	Y	Y	Y	4
Fusion Exhaust Processing System	Y	Y	Y	Y	4
Fusion Fuel Preparation System	Y	Y	Y	Y	4
Hydrogen Isotope Separation System	Y	Y	Y	Y	4
Plant Emission Control Systems	Y	Y	Y	Y	4
Plant Radiological Maintenance Org	Y	Y	Y	Y	4
Plasma Fueling System	Y	Y	Y	Y	4
Plasma Heating System	Y	Y	Y	Y	4
Process Fluid Handling System	Y	Y	Y	Y	4
Radiological Waste Handling System	Y	Y	Y	Y	4
Torus / Vacuum Vessel	Y	Y	Y	Y	4
Torus Cooling / Fusion Breeding Blanket	Y	Y	Y	Y	4
Torus Vacuum Pumping System	Y	Y	Y	Y	4
Waste Disposal System	Y	Y	Y	Y	4
Plant Infrastructure Replacement Org	N	Y	Y	Y	3
Plant Structural Systems	N	Y	Y	Y	3
BOP Heat Exchanger System	Y	Y	N	N	2
BOP Shutdown Heat Removal System	Y	Y	N	N	2
BOP Electrical Distribution System	N	Y	Y	N	2
Fusion Fuel Input Processing System	N	Y	Y	N	2
Plant Maintenance Systems/Org	N	Y	Y	N	2
Plasma Shutdown System	N	Y	Y	N	2
Torus Environmental Control System	M	Y	Y	N	2
Waste Handling System	N	Y	Y	N	2
BOP Chemistry Control System	M	Y	N	N	1
BOP Generator System	N	N	Y	N	1
BOP Turbine System	M	N	N	N	0
BOP Pump Compressor System	N	N	N	N	0
BOP Ultimate Heat Sink System	N	N	N	N	0
Magnetic Confinement System	N	N	N	N	0
Plant Engineering and Safety System/Org	N	N	N	N	0
Plant Environmental Control Systems	N	N	N	N	0
Plant Operations Control System/Org	N	N	N	N	0
Plant Security Systems/Org	N	N	N	N	0
Plant Utility Systems	N	N	N	N	0
Plasma Control System	N	N	N	N	0

3.6.1 System engineering model hazard identification

The selected system engineering model system forms from the D-T tokamak specific system engineering model are evaluated. For each system form, the presence, form, and characteristics of each of the relevant hazards for the system are documented to support licensing assessments. This produces a list of hazards that must be evaluated to support licensing and other regulatory activities.

After the hazards for all selected system engineering model system forms have been identified, a final categorization is performed to assess whether the hazard is relevant to only on-site adverse consequences or on-site and off-site adverse consequences.

One way to characterize these adverse consequences is whether the hazard has the potential for on-site adverse consequences (fully contained within a site boundary or localized around a device) or off-site adverse consequences (extended beyond a site boundary or outside of a device). As previously discussed, presence of hazards with on-site consequences or off-site consequences can have very different regulatory implications. Technology design, licensing, and operation are all impacted by the regulatory requirements and limits associated with on on-site and off-site hazards.

This final assessment was primarily based on the nature of the hazard and expected "order of magnitude" of the hazard in a commercial fusion facility. The summary of the identified hazards is provided in Table 3.9 (off-site hazards) and Table 3.10 (on-site hazards). These hazards are discussed in Section 3.7 for on-site and off-site relevant hazards and Section 3.8 for on-site only relevant hazards.

The detailed assessment of system forms and identification of relevant hazards are documented in Appendix 3A. Note that in some cases, the hazards may be inherent to the system form; in other cases, the hazards may be dependent on specific design or technology choices made during the design process. Assumptions regarding these hazards are noted where appropriate.

Table 3.9. Off-site and on-site D-T Tokamak Specific Hazard Identification

Hazard Category	Description	Blanket Processing System	D-T Processing System	D-T Storage System	Effluent Release System	Fusion Exhaust Processing System	Fusion Fuel Preparation System	Hydrogen Isotope Separation System	Plant Emission Control Systems	Plasma Fueling System	Plasma Heating System	Radiological Waste Handling System	Torus / Vacuum Vessel	Torus Cooling / Fusion Breeding Blanket	Torus Vacuum Pumping System	Waste Disposal System	Plant Radiological Maintenance Systems/Org	Process Fluid Handling System
15.1 - Radioactive Material	Gaseous - activated air and process gasses				x				x			x		x		x		x
	Gaseous - activated control gasses				x	x			x			x	x		x	x		x
	Gaseous blanket/structural activation products (e.g., C-14, F-18 based on blanket composition)	x			x				x			x		x		x		
	Gaseous tritium and tritiated compounds	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
	Liquid activation product (e.g., Be-10 based on blanket composition)	x										x		x		x		
	Liquid aqueous radioactive products (water with dissolved activated materials, HTO)				x				x			x				x		x
	Solid activated products - mobile (erosion/corrosion products)	x				x						x	x	x	x	x	x	
	Solid contaminated (including T) products - mobile (erosion/corrosion products)					x						x	x		x	x	x	
	Solid tritium metallic compounds (e.g., uranium titride, titanium titride)			x														
	Solid (frozen) tritium compounds						x			x	x							
16.6 - Chlorine	Chlorine (based on blanket chemistry, reducing)	x	x		x				x					x		x	x	
16.10 - Fluorine	Fluorine (based on blanket chemistry, reducing)	x	x		x				x					x		x	x	
17.1 - Radioactive Contamination, 17.4 - Radioactive Sources	Beta radiation (T) - radioactive contamination (tritiated materials)	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
	Gamma/x-ray, beta, alpha radiation - radioactive contamination (activated materials)	x			x	x			x			x	x	x	x	x	x	x
17.4 - Radioactive Sources	Neutron radiation												x	x				
	Gamma radiation												x	x				
9.7 - Explosive Material	Hydrogen gas	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x		x
9.5 - Explosive Material	Salt components based on blanket chemistry (e.g., Li, Na, K)	x												x		x	x	

Table 3.10. On-site D-T Tokamak Specific Hazard Identification

Hazard Category	*Description*	*Blanket Processing System*	*D-T Processing System*	*D-T Storage System*	*Effluent Release System*	*Fusion Exhaust Processing System*	*Fusion Fuel Preparation System*	*Hydrogen Isotope Separation System*	*Plant Emission Control Systems*	*Plasma Fueling System*	*Plasma Heating System*	*Radiological Waste Handling System*	*Torus / Vacuum Vessel*	*Torus Cooling / Fusion Breeding Blanket*	*Torus Vacuum Pumping System*	*Waste Disposal System*	*Plant Radiological Maintenance Systems/Org*	*Process Fluid Handling System*
15.1 - Radioactive Material	*Plasma radioactive products (tritium, activated control gasses)*												x					
	Plasma tritium										x		x					
	Solid activated products - fixed (structural materials)											x	x	x		x	x	
	Solid contaminated (including T) products - fixed (structural materials)						x				x	x	x		x	x	x	
16.1 - Asphyxiants	*Asphyxiants - helium, cryogenic coolants*			x			x	x		x	x							
16.3 - Beryllium	*Beryllium and beryllium compounds (based on blanket composition, structural layers)*	x	x						x			x	x	x		x	x	x
16.5 - Carcinogens	*Carcinogens (based on processing methods, design choices)*	x			x				x			x	x	x		x	x	x
16.7 - Corrosives	*Corrosives (based on processing methods)*	x			x				x			x		x		x	x	x
16.9 - Dusts	*Dusts and particles*					x							x		x	x	x	
16.12 - Lead	*Lead/heavy metals (structural, shielding, particle)*		x										x			x	x	
16.13 - Oxidizers	*Oxidizers (based on processing methods)*		x										x					
17.2 - Electron or ion beam	*Ion and neutral heating beams*										x		x					
9.2 - Dust	*Dust and particles*					x						x	x		x	x	x	

3.6.2 On-site and off-site hazards for D-T tokamak commercial fusion facilities

Off-site hazards for commercial fusion are the primary hazards that must be evaluated during a licensing as part of a regulatory regime. The hazards listed in Table 3.9 are significant hazards for both on-site and off-site adverse consequences. These hazards are grouped based on general hazard characteristics, and discussed in detail in this section. Full details on these hazards and system specific discussion of the hazards can be found in Appendix 3A.

Radioactive gasses

Radioactive gasses present a significant on-site and off-site hazard but the magnitude of the inherent hazard will depend on the radionuclide, form, and inventory. Review of plant system forms reveal two major types of radioactive gas hazards – activated gasses / gasses produced via neutron activation and tritiated gasses.

Activated gasses or gasses produced via neutron activation are a concern due to their mobility and continuous production during operation. Sources include:

- Air and process gasses exposed to neutron radiation
    - Example: N-16 produced via (n, p) reactions or neutron absorption, C-14 produced via neutron absorption
- Control gasses injected into the torus to control fusion reactions
    - Example: Ar-41 produced via neutron absorption
- Blanket/structural activation products
    - Example: F-18 produced via neutron absorption

The gasses may be produced in any plant systems that are subject to neutron radiation produced directly by fusion reactions or neutron producing secondary reactions (e.g., $(n, 2n)$ reactions with beryllium). The inventory and production rate of these gasses is a function of a number of factors including:

- Neutron flux
- Neutron spectrum
- Mass and density of exposed materials
- Isotopic composition of exposed materials
- Isotope processing and removal system capabilities

The resulting gaseous activation products have different hazard characteristics depending on their physical form and biological availability. Gaseous isotopes of are particular concern as an off-site hazard due to their high mobility. Some normally gaseous activation products may be retained in stable forms (e.g., F-18 in an fluoride-lithium-beryllium ionic salt) but can mobilized if subject to certain environmental conditions such as a high temperatures (citation:FLiBe_hazards).

The potential forms and quantities of these activated gasses must be assessed based on design choices (e.g., material selection and exposure to neutron radiation fields) and operational choices (e.g., use of clean-up systems to limit steady state or maximum free gaseous radionuclide inventories). While the presence of this off-site hazard is noted, determination of hazard magnitude and forms is a design specific activity.

Gaseous tritium and tritiated compounds are present in a large number of plant system forms due to the use of tritium as a primary fuel for a commercial D-T tokamak fusion facility. Sources include:

- Tritiated diatomic hydrogen species
    - Example: HT, DT, T_2 present in production, processing, utilization, recovery, storage, and environmental off-gas systems
- Tritiated compounds
    - Example: TF formed due to radiolytic decomposition of tritium breeding salts, HTO and other tritiated water compounds

Tritiated species and compounds will be present in any plant system forms that handle fusion fuel. A facility tritium breeding ratio (TBR) greater than unity is required by design to ensure that a commercial facility can sustain operations without external sources of tritium fuel. This techno-economic requirement on the TBR results in a need to minimize releases of tritium for commercial and not environmental reasons.

The high permeability of tritium and tritiated species will challenge containment of these gaseous tritium compounds. All maintenance and environmental systems must be designed to capture and reprocess tritiated species. This may result in the presence of significant quantities of gaseous tritium and tritiated compounds in a large number of plant system forms.

The inventory and production rate of tritium is a function of a number of factors including:

- Reactor fusion power
- Fuel handling, storage, and reprocessing system design
- Tritium production and separation system design
- Environmental control system design

The tritium and tritiated compounds have different hazard characteristics due to the biologic availability of oxidized tritium. The radiological hazard of oxidized tritium is 10,000 greater than the radiological hazard of elemental tritium [19]. Hydrogen is easily combusted and oxidized so it is commonly assumed that any available tritium is oxidized upon release. The biological availability of oxidized tritium presents a significant hazard, and the mobility of gaseous tritium and oxidized tritium present significant off-site hazard.

The potential forms and quantities of tritium must be assessed based on design choices including system power, technology choices, materials choices, and overall system design. While the presence of this off-site hazard is known for a commercial D-T tokamak system, determination of hazard magnitude and forms is a design specific activity.

Radioactive liquids

Radioactive liquids present a significant on-site and off-site hazard but the magnitude of the inherent hazard will depend on the radionuclide, form, and inventory. Review of plant system forms reveals two major types of radioactive liquid hazards – activated liquids produced via neutron activation and liquids contaminated with aqueous or dissolved radioactive products.

Radioactive liquids produced via neutron activation are a concern due to their continuous production during operation. Sources include:

- Water exposed to neutron radiation
    - Example: N-16 produced via (n, p) reactions with O-16, H-3 produced via single or double neutron absorption by H-1 or H-2, respectively
- Liquid blanket materials exposed to neutron radiation
    - Example: Be-10 produced via neutron absorption

Activated liquids be produced in any plant systems that are subject to neutron radiation produced directly by fusion reactions or neutron producing secondary reactions (e.g., $(n, 2n)$ reactions with beryllium). The inventory and production rate of these liquids is a function of a number of factors including:

- Neutron flux
- Neutron spectrum
- Mass flow rate and density of exposed liquids
- Isotopic composition of exposed liquids
- Isotope processing and removal system capabilities

The resulting liquid activation products have different hazard characteristics depending on their physical form and biological availability.

Liquids contaminated with aqueous or dissolved radioactive products are a concern due to the ability to mobilize and transport otherwise stationary radionuclides. Source include:

- Liquids contaminated with activated materials
    - Example: liquid coolants with neutron activated corrosion products such as Co-60 produced via double neutron absorption with Ni-58
- Liquid contaminated with tritium or tritiated materials
    - Example: water contaminated with HTO

These liquids may be generated through surface interactions with irradiated materials or by diffusion of radioactive materials through structural materials. Radioactive liquids are concern as an off-site hazard due to their mobility but still require a flow release pathway or an energy source to enable vaporization and high mobilization as a gas.

The potential forms and quantities of these radioactive liquids must be assessed based on design choices (e.g., material selection, corrosion control, and exposure to neutron radiation fields) and operational choices (e.g., use of clean-up systems to limit steady state or maximum free contamination levels). While the presence of this off-site hazard is noted, determination of hazard magnitude and forms is a design specific activity.

Mobile radioactive solids

Mobile or easily mobilized radioactive solids are a significant on-site and off-site hazard for commercial fusion facilities. The magnitude of the inherent hazard will depend on the radionuclide, form, inventory, and operational characteristics of the facility. Review of plant system forms reveals two general types of relevant radioactive solid hazards – activated or contaminated solids mobilized by erosion or corrosion processes and solid tritiated storage or fueling materials.

Mobile radioactive solids produced via neutron activation are a concern due to their continuous production during operation. Sources include:

- Plasma facing components exposed to neutron radiation
    - Example: W-187 produced via neutron absorption reactions with tungsten first wall materials and eroded into mobile dust via plasma-material surface interactions
- Tritium contaminated mobile solid materials
    - Example: Tritium adsorption by tungsten first wall materials and eroded into mobile dust via plasma material surface interactions
- Materials with trace actinides exposed to neutron radiation
    - Example: Trace naturally occurring actinides (thorium, uranium) present in various plant materials (alloys, concretes) that may produce radioactive activation products or fission products when exposed to neutron radiation

Mobile activated solids are produced in plant systems that are subject to neutron irradiation or tritium contamination and material surface degradation mechanisms. The inventory, production rate, and hazards of these mobile materials will depend on a number of factors including:

- Neutron flux and neutron spectrum
- Tritium exposure conditions
- Isotopic composition of solids
- Solid surface conditions
- Surface degradation rates and mechanisms
- Particle clean-up and removal system capabilities
- Detritiation system capabilities

Radioactive mobile radioactive solids are concern as an off-site hazard due to their mobility but still require a flow release pathway and an energy source to enable transport. The resulting mobile radioactive solids will have different hazard characteristics depending on their physical form (e.g., particulate size) and biological availability.

The potential forms and quantities of these radioactive solids must be assessed based on design choices (e.g., material selection, erosion control, and exposure to neutron radiation fields) and operational choices (e.g., use of clean-up systems or maintenance activities to limit steady state or maximum inventory). While the presence of this off-site hazard is noted, determination of hazard magnitude and forms is a design specific activity.

Solid tritiated storage or fueling materials are a concern due to the ability to mobilize stored tritium into a liquid or gaseous form under specific conditions. Sources include:

- Solid tritium metallic storage forms
    - Example: solid uranium titride storage beds for the short- or long-term solid-state storage of tritium gas
- Solid tritium fuel forms
    - Example: frozen tritium or deuterium-tritium pellets used in tokamak fueling systems

Both of these tritiated solids are a concern because they can release retained tritiated materials at elevated temperatures. Solid tritium fuel forms may melt or sublimate and release tritium at temperatures above the freezing point of hydrogen gas (11 Kelvin) while solid tritium metallic compounds may require temperatures in excess of 400 to 500 degrees Celsius to release significant fractions of stored tritium. This means that these hazards still require energy sources and release pathways to produce on-site or off-site consequences.

The potential forms and quantities of these materials must be assessed based on design choices (e.g., fuel storage forms and inventories) and operational choices (e.g., use of active, passive, or inherent safety mechanisms to prevent release). While the presence of this off-site hazard is noted, determination of hazard magnitude and forms is a design specific activity.

Radiation sources

Radiation sources present a significant on-site hazard and may present as an off-site hazard depending on facility design parameters. Review of plant system forms reveals three major types of radiation sources – radiation (beta) from radioactive contamination by tritium and tritiated materials, radiation (alpha, beta, and gamma) from radioactive contamination by activated materials or secondary reactions, and neutron and gamma radiation from fusion and secondary reactions.

Radiation from alpha and beta emitting radionuclides (tritiated materials and some activated materials) are primarily onsite hazards due to the short range of charged particle radiation and the ease of employing practical physical shielding to significantly reduce dose exposure. The major concern for these nuclides is to prevent mobilization and ingestion or inhalation during any onsite activities.

Radiation from gamma emitting radionuclides are significant onsite due to the challenge associated with operating and maintenance activities in proximity to significant gamma radiation sources. Standard radiological safety practices and as-low-as-reasonably-achievable (ALARA) principles could be implemented to help reduce potential on-site hazards associated with gamma emitting activated materials. Gamma emitting radionuclide sources may present an off-site hazard if they are not sufficiently shielded or if there is a small distance between the source and off-site receptors.

Gamma radiation will also be produced during operation by neutron scattering interactions (n, γ) with structural materials and breeding blanket materials. This specific gamma radiation source is only present during power operation because it is driven by neutron radiation interactions. The magnitude and energy spectrum of this gamma radiation source will vary depending on the neutron radiation characteristics and the material selection with in the structural materials and breeding blanket. This gamma radiation sources presents an on-site hazard for workers around the device during operation and may present an off-site hazard if the neutron exposed structural materials and breeding blanket are not sufficiently shielded or if there is a small distance between the source and off-site receptors.

The neutron radiation from a fusion facility is characteristically different from other radiation sources and other radiological facilities. The characteristic high energy of fusion produced neutrons (14.1 MeV) and their function as primary energetic reaction product result in facility designs with high neutron radiation fluxes. Efficient, controlled slow down and capture of these neutrons is critical for both system efficiency and fuel breeding, so there is a design requirement to minimize neutron radiation leakage. Neutron radiation from fusion reactions or secondary reactions (e.g., $(n, 2n)$ reactions with beryllium) is both an on-site and off-site hazard if areas are not sufficiently shielded or if there is a small distance between the source and off-site receptors during operation.

Hazardous materials

Chemically and reactively hazardous materials may present on-site and off-site hazards depending on their form and inventory. Review of plant systems suggests significant hazardous material source is liquid breeding blanket chemical components.

Several of the component materials in proposed breeding blankets for commercial fusion facilities are chemically hazardous. Specific components of concern include:

- Chlorine
    - Example: component in chloride salt breeding blankets
- Fluorine
    - Example: component in fluoride salt breeding blankets

In their elemental form or specific chemical forms, both of these materials can present significant on-site and off-site hazards to human health. Both materials, however, can also be stored and processed in safe and inert forms. Facility design and operational usage of these materials should be considered to minimize the inventory of both chlorine and fluorine in hazardous chemical forms. While the presence of this off-site hazard is noted, determination of hazard magnitude and forms is a design specific activity

Explosive materials

Explosive materials present a significant on-site hazard and may present as an off-site hazard depending on quantity and design controls on the materials. Review of plant system forms reveals two major types of explosive materials – hydrogen gases and highly reactive materials.

Hydrogen gasses are a concern due to the potential for fires or explosions given sufficient concentrations of oxygen. Hydrogen explosions are an on-site hazard concern and may be on off-site hazard concern in sufficient quantities.

The main sources of hydrogen gas are the hydrogen isotopes (deuterium and tritium) used to fuel the fusion reactions. Hydrogen gas may be found in a wide number of plant systems including all fuel and fusion reaction related systems, the breeding blanket processing systems, and plant systems that contain and collect gaseous leakage from systems, structures, and components. This hydrogen gas may be found in gaseous form or solid form (e.g., metal hydride or frozen state) that can be released at elevated temperatures. A secondary source of hydrogen gas is as a process gas for cooling of some industrial components such including turbine generators.

The potential forms and quantities of these explosive materials must be assessed based on process design choices (e.g., available gaseous inventories) and operational design choices (e.g., use of active or passive systems to prevent explosive conditions during releases). While the presence of this off-site hazard is noted, determination of hazard magnitude and forms is a design specific activity.

Highly reactive materials are a concern due to the potential for spontaneous, exothermic explosion reactions. Several elemental species of particular concern are alkali metals that may be used in the breeding blanket salts, including:

- Lithium
- Sodium
- Potassium

These materials may react explosively in their elemental form or specific chemical forms, and present significant on-site and off-site hazards. These elements, however, can also be stored and processed in safe and inert forms. Facility design and operational usage of these materials should be considered to minimize the process and storage inventory of reactive materials in reactive forms. While the presence of this off-site hazard is noted, determination of hazard magnitude and forms is a design specific activity.

3.6.3 On-site hazards for D-T tokamak commercial fusion facilities

On-site hazards with potentially significant consequences must be evaluated during a licensing as part of a regulatory regime for commercial fusion. The hazards listed in Table 3.10 are significant hazards for on-site adverse consequences. These hazards are grouped based on general hazard characteristics, and discussed in detail in this section. Full details on these hazards and system specific discussion of the hazards can be found in Appendix 3A.

Fuel/vacuum vessel hazards

Fusion plasma presents several significant on-site hazards, primarily related to radioactive materials present in the plasma. While the plasma operates at extremely high temperatures, the low density of the plasma and the tendency of plasma to quench during disruptions will limit significant damage to the Torus Vacuum Vessel. The plasma does not present a significant on-site hazard to personnel due the to relatively low stored energy of the plasma relative to other systems. Additionally, requirements shielding of personnel from the radiation hazards (i.e., gamma and neutron radiation) would likely protect personnel from any direct exposure to plasma hazards. The radioactive material within the plasma, however, presents a challenge due to the potential for on-site contamination, shutdowns, and worker exposure. Sources of radioactive material in the plasma include:

- Tritium fuel ions within the plasma
- Neutral tritium gas and activated control gasses at the plasma edge

These materials are a concern during operation if loss of Torus Vacuum Vessel integrity permits the release of these radioactive materials during loss of plasma confinement events. While these events may not pose significant off-site hazards, the physical damage from such an event could require significant downtime for repairs or may result in complete loss of commercial fusion facility due to economically irrecoverable repair costs. The inventories of these radioactive materials will vary based on design choices (e.g., plasma volume, density) and operational choices (e.g., use of clean-up systems to limit steady state or maximum free gaseous radionuclide inventories). While the presence of this off-site hazard is noted, determination of hazard magnitude and forms is a design specific activity. Due to the low density of the plasma, the actual radiological inventory will likely be minimal.

Fixed radioactive solids

Fixed radioactive solids are a significant on-site hazard for commercial fusion facilities but represent a minimal off-site hazard. The magnitude of the inherent hazard will depend on the radionuclide, form, inventory, and operational characteristics of the facility. Fixed radioactive solids may be produced via neutron activation or via contamination of structural materials by mobile radiological materials. Fixed radioactive solids include:

- Component and structural materials exposed neutron radiation
  - Example: Co-60 produced via neutron absorption reactions with Co-59 present in structural and component alloy materials
  - Example: Co-60, Mn-54, Ba-131 produced via neutron absorption reactions with naturally occur isotopes in structural concrete materials [20]
- Component and structural materials contaminated by tritium
  - Example: Tritium adsorption by the vacuum vessel and other fuel facing components and systems

  - Example: Tritium adsorption by components and systems exposed to non-fuel tritium contaminated materials [21]
  - Example: Tritium adsorption by structural concrete materials [21]

These materials are a concern for operational, maintenance, and replacement activities. All materials exposed to neutron radiation may become activated including structures, systems, and components. Neutron activation is not limited to mechanical systems but electrical systems, magnet systems, and control and diagnostic systems that not fully shielded against neutron radiation. Material activation or contamination with gamma emitting radionuclides can limit operational activities due to the resulting high radiation fields that may degrade unshielded systems and components. Maintenance and replacement activities on or near activated or contaminated fixed solids structures, systems, and components can require operation in high radiation field environments. Minimizing worker dose may require additional shielding, remote handling methods, or a cool-down period to allow for the decay of short-lived radionuclides. Safe storage and ultimate disposal of radioactive materials is an operational challenge to minimize worker doses.

The inventory and hazards of these fixed radioactive solid materials will depend on a number of factors including:

- Neutron flux and neutron spectrum
- Tritium exposure conditions
- Isotopic composition of solids
- Solid surface conditions

Fixed radioactive solids are not concern as an off-site hazard due to the fact that sufficient energy required for mobilization and release are not present. Sufficiently high energy releases that lead to the vaporization or pulverization of fixed radioactive material could facilitate the release and their inclusion in regulatory evaluations as an off-site hazard. The quantities of these radioactive solids must be assessed based on design choices (e.g., material selection, erosion control, and exposure to neutron radiation fields) and operational choices (e.g., tritium and other permeable radioactive material presence). Determination of hazard magnitude and forms for this hazard is a design specific activity.

Asphyxiants

Asphyxiants present a significant on-site hazard depending on quantity and location of materials. Review of plant system forms reveals two major asphyxiants of concern – helium gases and cryogenic coolants used in plant systems, structures, and components.

The major sources of helium gas produced on-site include He-4 used for the gaseous cooling of internal fusion components, produced in the D-T fusion reactions and He-3 produced via the radioactive decay of tritium. The rate of helium gas produced via fusion reactions will vary based on facility fusion power and the rate of helium gas produced via tritium decay will depend largely on the steady state tritium inventory on-site. Both production rates would be less than tens of kilograms per year while the quantity of helium gas for cooling is design dependent.

The larger source of potential asphyxiants are cryogenic coolants used in plant systems, structures, and components. Extremely low temperatures are needed for many plant systems including freezing hydrogen isotopes for solid fuel forms (11 K), certain vacuum pump systems (15 K), cryogenic hydrogen isotope separation (20 K), and high temperature superconducting magnet operation (25 K). These systems may require large quantities of coolants to ensure safe and reliable operation. The quantity of these cryogenic coolants would depend on design choices and technology selection.

These asphyxiants, specifically the cryogenic coolants, are a concern as an on-site hazard due to potential human health effects. Exposure at sufficiently high concentrations can lead to incapacitation or death, so leakage or releases of cryogenic coolants must be controlled. Minimizing operator risk may require reducing releasable inventories of cryogenic coolants, ensuring sufficient environmental system performance to prevent development of hazardous conditions, and limiting operator access to areas where hazardous conditions may occur during leaks or releases.

Asphyxiants are not concern as an off-site hazard due to their limited inventories in these facilities (i.e., non-industrial production quantities) and their rapid dissipation in open areas. The quantities of these asphyxiants must be assessed based on design choices (e.g., use of cryogenic coolants and storage of produced helium) and operational choices (e.g., in process versus stored quantities of cryogenic coolants). Determination of hazard magnitude and forms for this hazard is a design specific activity.

Beryllium and beryllium compounds

Beryllium and beryllium compounds present a significant on-site hazard depending on quantity, form, and location of these materials. Review of plant system forms reveals two major sources of beryllium – structural materials and breeding blankets.

The first use of beryllium is in structural materials, specifically in plasma facing components. Beryllium has several unique characteristics that make it a candidate material for these applications:

- Intermediate melting point in metallic form or when alloyed with other metals
- Moderate surface retention of tritium and deuterium
- Low atomic mass that minimizes plasma contamination if ionized
- Limited material activation by neutron radiation

These characteristics make beryllium a possible choice for a first wall or plasma facing material.

The second use of beryllium is in breeding blankets for the production of tritium. The unique neutron interaction characteristics of beryllium, specifically Be-9 neutron multiplication reactions $(n, 2n)$ with high energy neutrons, make it an ideal material for nuclear applications. Beryllium may be used as a solid structural neutron multiplier to increase the total neutron flux outside of the torus or it may be used as a major component in a molten salt breeding blanket such as a FLiBe (Fluorine-Lithium-Beryllium). This application may lead to significant masses of beryllium salts in the breeding blanket and processing system.

The technical advantages of beryllium in a commercial fusion facility may incentivize use of beryllium metal, beryllium alloys, and beryllium salts throughout the facility. Beryllium, however, is a significant on-site hazard of concern due to the significant human health effects of inhalation of beryllium dusts and particles. While beryllium is a known industrial hazard, significant usage could complicate worker safety and operational maintenance activities related to beryllium containing systems, structures, and components.

Beryllium is not a significant concern as an off-site hazard since transport of beryllium dusts in significant concentrations off-site is limited. The quantities and forms of beryllium must be assessed based on design choices (e.g., structural and blanket materials) and operational choices (e.g., processing and maintenance activities). Determination of hazard magnitude and forms for this hazard is a design specific activity.

Carcinogens, Corrosives, Oxidizers

Carcinogens, corrosives, and oxidizers may present a significant on-site hazard depending on quantity, form, and location of materials. These materials may be present in a variety of plant systems responsible for physical, chemical, or isotopic processing of fusion fuels, breeding blankets, process fluids, wastes, and other materials. These materials may pose a hazard to human health or could damage physical systems, structures, and components if not properly handled. These hazards are routine managed in other industrial facilities and could be managed according to industry best practices or guidance.

Carcinogens, corrosives, and oxidizers are not expected to be a significant concern as an off-site hazard due to the total inventories of materials that would likely be present at commercial fusion facility. The exact quantities and forms of these materials must be assessed based on design choices (e.g., use of hazardous materials in processes, process capacity) and operational choices (e.g., handling requirements, inventory fraction in a hazard form). Determination of hazard magnitude and forms for this hazard is a design specific activity and could become sufficiently large to affect off-site receptors.

Dusts and particles

Dust and particles may present an on-site hazard depending on physical and chemical characteristics of the materials. These materials are a concern for two main reasons – explosions result from high surface area releases and transport of toxic, radiologic, or otherwise hazardous contaminated materials. Sources of dusts and particles include:

- Torus / vacuum vessel dusts
    - Example: Tungsten or other plasma facing material dust produced via plasma-material surface interactions and surface sputtering

- Process dusts
    - Example: Lithium compound dusts produced during processing of fusion fuel input material for the breeding blanket

The inventory and hazards of these dusts and particle will depend on a number of factors including:

- Isotopic composition
- Chemical composition
- Particle size and size distribution
- Surface production rates
- Particle clean-up and removal system capabilities

These materials are not likely an off-site hazard concern from explosions due to relatively small quantities expected in a commercial fusion facility but specific dusts (e.g., radioactive or toxic contaminated dusts) may pose an off-site concern, even in small quantities. These secondary hazards are covered by previously discussed hazard categories. The exact quantities and forms of the dusts must be assessed based on design choices (e.g., material selection, rate of particle formation) and operational choices (e.g., dust clean-up and containment processes). Determination of hazard magnitude and forms for this hazard is a design specific activity.

Lead/heavy metals (structural, shielding, particle)

Lead and other heavy metals may present an on-site hazard depending on the chemical and physical forms of the materials. These materials are primarily a concern due to the potential for human health effects from acute and chronic exposure to heavy metals. Sources of lead and heavy metals may include radiation shielding or structural systems and components, as well as the use of lead as a neutron multiplier in the blanket. These materials may pose a hazard to human health or could damage physical systems, structures, and components if not properly handled. These hazards are routine managed in other industrial facilities and could be managed according to industry best practices or guidance.

Lead and heavy metals are not expected to be a significant concern as an off-site hazard because it is not expected that the materials will be a mobile or easily mobilizable form. Environmental contamination of lead on-site or off-site may be a concern if waste materials are not properly handled. The exact quantities and forms of these materials must be assessed based on design choices (e.g., material selection, form, and placement of radiation shielding) and operational choices (e.g., handling requirements, worker interactions with hazardous systems). Determination of hazard magnitude and forms for this hazard is a design specific activity.

Ion and neutral heating beams

High energy ion and neutral particle beams are a unique on-site hazard at a commercial fusion facility. These systems are a concern due to the potential consequences of human exposure and the potential for damage to systems, structures, and components inadvertently exposed to the beam lines. The main source of these high energy beams is the systems used to heat the fusion plasma in the torus and vacuum vessel. These hazards are largely fixed in place due to the size of the systems, structures, and components used to generate high energy ion and neutral particle beams.

These beams are not a significant concern as an off-site hazard because of the attenuation of these beams and the fixed or limited positioning of the beam lines. The exact hazard characteristics of these beam lines should be assessed based on design choices (e.g., beam energy, physical configuration, safety interlocks) and operational choices (e.g., operational practices, physical checks on hazards). Determination of hazard magnitude and forms for this hazard is a design specific activity.

3.7 Hazards selected for licensing D-T commercial fusion facilities

Regulation of any industrial hazard in the United States is largely performed on a jurisdictional basis. This includes geographic jurisdictions (federal, state, and local), affected group jurisdictions (workers, members of the public, ecological populations), and individual hazard jurisdictions (chemical hazards, radiological hazards). These jurisdictions are defined by overlapping pieces of legislation (e.g., Emergency Planning and Community Right-To-Know Act, Clean Air Act, Occupational Safety and Health Act) and regulation (e.g., EPA and OSHA promulgated regulation) that define legal requirements for different industries, activities, and hazards. Prior DOE reviews of state and federal hazard jurisdictions have identified legislation relevant to the regulation of commercial fusion facilities [22].

This work identifies four hazard categories with both high regulatory importance and a potential for high severity adverse consequences:

- Radioactive material
- Hazardous material (toxicological, chemical, biological)
- Explosive material
- Direct radiation exposures

Two of the four hazard categories (hazardous materials and explosive materials) are already subject to technology independent regulatory requirements. Federal and state legislation and regulatory requirements are already promulgated federally by the Environmental Protection Agency, Department of Homeland Security, and Occupational Safety and Health Administration [22]. Review of the technology specific D-T tokamak commercial fusion facilities hazards also suggest that the expected hazardous and explosive material inventories will be comparable to or less than industrial facilities already regulated by state and federal agencies. This work will, therefore, not address the licensing challenges associated with hazardous and explosive materials because existing regulatory requirements and processes are expected to be appropriate and adequate for commercial fusion facilities.

The remaining two hazard categories (radioactive material and direct radiation exposure) are unique to nuclear facilities but are still regulated across a variety of jurisdictions. Regulatory requirements are imposed by both states and the federal government depending on the specific location and activity, with differing relevant regulators and requirements on exposures for workers and members of public. Direct radiation exposure is a significant on-site hazard and may be an off-site hazard depending on the magnitude of the radiation source, the radioisotopes, and the physical design of the system and facility. The hazards associated with direct radiation exposures for the technology specific D-T tokamak commercial fusion facilities are limited to the combination of these factors.

Neutron radiation and secondary gamma radiation sources are physically limited to the torus/vacuum vessel and breeding blanket. Near perfect utilization of reaction neutrons for tritium fuel breeding is required for fuel self-sufficiency, providing additional engineering and economic incentive for effective shielding of neutron radiation sources. Use of appropriate additional physical shielding, limited worker interactions with relevant plant systems during operation, and controlling public access to the facility during operation would limit the hazard posed by the neutron and secondary gamma radiation sources.

Significant gamma radiation sources from neutron activated materials are primarily limited to activated system, structure, and component materials. These activated materials are normally fixed during operation with limited movement during maintenance and replacement activities. While these materials present a significant hazard to on-site workers, use of standard radiation protection principles could control on-site and off-site hazards. Similar to the neutron radiation sources, the use of appropriate additional physical shielding, limited worker interactions with relevant plant systems during operation, and controlling public access to the facility during operation would limit the hazard posed by gamma radiation sources.

Direct radiation exposure to charged particle radiation (alpha and beta) is not a significant concern due to the short effective distance of each radiation type. Internal dose exposure from alpha and beta radiation is a significant concern but is more closely tied to release of radiological materials. Radiological precautions sufficient for gamma direct radiation exposure in a commercial fusion power plant will be sufficient to protect against charted particle direct radiation exposure.

Direct radiation exposure hazards are primarily under the jurisdiction of the NRC and OSHA. Both agencies have established regulatory requirements for radiation exposure limits for workers and members of the public and recommended protection actions that are largely independent of the specific facility, technology, or activity. This work will, therefore, not address the licensing challenges associated with direct radiation exposure because existing regulatory requirements and processes are appropriate and adequate for commercial fusion facilities.

The remaining hazard category with both high regulatory importance and a potential for high severity adverse consequences is radioactive material. This hazard has both on-site and off-site consequences and would contain radiological hazard characteristics (radioisotopes, forms, and inventories) not previously present in any industrial system. As a result, this hazard represents a unique hazard of particular regulatory interest for commercial fusion facilities.

3.8 Innovative elimination or reduction of hazards

This section has developed a set of hazards of regulatory interest for commercial fusion facilities based on a D-T tokamak specific system engineering model for a commercial fusion facility. While the presence of these hazards is noted based on the current concept of operations for such a facility, the description and discussions for the hazards stated that "determination of hazard magnitude and forms is a design specific activity". These hazards are discussed within this work to provide context on the development of regulatory requirements, but it is important to note that not all of the hazards are inherent to fusion technology. Some hazards will change based on use of different fusion technologies and fuel cycles, but many hazards may be reduced through design changes with a fixed fusion technology and fusion cycle. Innovative approaches to the design, engineering, and operation of systems have the potential to reduce, mitigate, or even eliminate a number of the regulatory hazards of interest presented in this section.

The major off-site and on-site hazards of regulatory interest identified in this section were:

- radioactive material
- hazardous materials
- radioactive sources
- explosive materials

Certain hazards, such as neutron radiation, are inherent to a D-T fusion fuel cycle and cannot be eliminated through design and operation choices. Many other hazards, however, may be reduced. Hazards associated with radioactive materials in a commercial fusion facility will depend significantly on design and operational choices made for a commercial facility. Use of low activation materials for plasma facing components and other materials exposed to neutron radiation could significantly reduce the radioactive material inventory from activated materials. Reducing the processing time associated with D-T fuel cycle could reduce the radiological inventory of mobilized, in process radioactive tritium. Development of new barrier materials to prevent the diffusion of radioactive tritium or development of new sink materials that can readily absorb tritium could significant reduce the radiological inventory of mobile radioactive materials. Appropriate implementation of process design methods to minimize hazards by design and research into innovative technological or engineering approaches to reduce hazards could significantly reduce the overall risk associated with off-site and on-site hazards without the needs for engineered safeguards. This hazard reduction approach helps lead to safer designs and safer operation.

The remainder of this work will focus on the licensing evaluations of radiological material hazards associated with commercial fusion facilities. These hazards may fall under the jurisdiction of multiple regulatory organizations and is it not clear if the unique combination of radioisotopes, forms, and inventories would be adequately controlled by existing regulatory frameworks. This work will seek to identify how to adequately characterize and evaluate this hazard category for commercial fusion facilities.

Finally, it is important to note that regulation and licensing of a commercial fusion facility would require evaluation of all hazard categories. Compliance with or exemption from all relevant statues, regulations, and rules would be required. For hazards not explicitly described in this work, it is assumed that existing frameworks would enable the adequate handling of hazards.

3.9 References

[1] Center for Chemical Process Safety (CCPS). Guidelines for hazard evaluation procedures. Wiley, 2011.

[2] Department of Energy. Hazard and accident analysis handbook. Technical Report DOE-HDBK-1224-2018, Department of Energy, 2018.

[3] Occupational Safety and Health Administration. OSHA Fact Sheet: Occupational Safety and Health Administration (OSHA) Inspections. Technical Report DEP FS-3783, Occupational Safety and Health Administration, 2016.

[4] E. Broughton. The Bhopal disaster and its aftermath: a review. Environmental Health, 4(1):1–6, 2005.

[5] US Chemical Safety and Hazard Investigation Board. Investigation Report: West Fertilizer Company fire and explosion. Technical Report 2013-02-I-TX, US Chemical Safety and Hazard Investigation Board, 2013.

[6] U.S. Chemical Safety and Hazard Investigation Board. Investigation Report: Organic Peroxide Decomposition, Release, and Fire at Arkema Crosby Following Hurricane Harvey Flooding. Technical Report 2017-08-I-TX, U.S. Chemical Safety and Hazard Investigation Board, May 2018.

[7] Environmental Protection Agency. Risk Management Program (RMP) Audit Program, 2013.

[8] Federal Aviation Administration. Emergency Order of Prohibition to Owners of Boeing Company, 2019.

[9] Federal Aviation Administration. FAA Strategic Plan FY 2019-2022. Technical report, Federal Aviation Administration, 2019.

[10] B. Elias. Delegation of Federal Aviation Administration Certification Authorities to Aviation Manufacturers. Technical report, Congressional Research Service, 2019.

[11] R. Rhodes. The Making of the Atomic Bomb. Simon and Schuster, 1986.[19

[12] G. T. Mazuzan and J. S. Walker. Controlling the Atom: the Beginnings of Nuclear Regulation, 1946- 1962. University of California Press, Berkeley, 1985.

[13] Atomic Energy Commission. Theoretical possibilities and consequences of major accidents in large nuclear power plants. Technical Report WASH-740, 1957.

[14] J. S. Walker and G. T. Mazuzan. Containing the Atom: Nuclear Regulation in a Changing Environment, 1963-1971. University of California Press and U. S. Nuclear Regulatory Commission, Berkeley, 1992.

[15] B. L. Welch. Nuclear power risks: challenge to the credibility of science. International Journal of Health Services, 10(1):5–36, 1980.

[16] Nuclear Regulatory Commission. NRC Strategic Plan FY 2019-2022. Technical Report NUREG-1614, Vol. 7, Nuclear Regulatory Commission, 2018.

[17] Nuclear Regulatory Commission. Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition. Technical Report NUREG-0800, Nuclear Regulatory Commission.

[18] Domestic Licensing of Production and Utilization Facilities. 10 CFR Part 50, 2007.

[19] K. Eckerman, J. Harrison, H. Menzel, C. Clement, et al. ICRP publication 119: compendium of dose coefficients based on ICRP publication 60. Annals of the International Committee on Radiation Protection, 41:1–130, 2012.

[20] T. Zagar and M. Ravnik. Measurement of neutron activation in concrete samples. 2000.

[21] G. Eichholz, W. Park, and C. Hazin. Tritium penetration through concrete. Waste Management, 9(1):27–36, 1989.

[22] Department of Energy. DOE Standard: Safety of Magnetic Fusion Facilities: Guidance. Technical Report DOE-STD-6003-96, Department of Energy, May 1996.

Appendix 3A – Detailed hazard identification

This appendix documents the detailed hazard identification performed in Section 3.4 for the D-T tokamak specific Level 3 system engineering model. The hazards were down selected using the following multi-step process:

1. Composite hazard category index (HCI) scores are calculated for each pair of hazard category and adverse consequences based on the inputs in Section 3.2 and Section 3.3.
2. Hazard categories are sorted based on the maximum HCI across all adverse consequences.
3. Hazard categories with an HCI of 9 (highest possible score) are selected for detailed evaluation and down selection to specific hazards (detailed in DOE Accident Analysis Handbook) that are relevant to a commercial fusion facility regulation and licensing based on a Level 0 system engineering model.
4. The list of functional system forms from the D-T tokamak specific Level 3 system engineering model is evaluated and systems with the greatest number of relevant hazards are further selected for hazard evaluation.
5. The selected system engineering functional systems are evaluated. The presence, form, and characteristics of each of the relevant hazards for the system are documented to support licensing assessments.

This appendix provides the results of the system form evaluations. For each system, each of the four hazard categories are discussed and the specific hazards and forms are identified. In some cases, the hazards may be inherent to the system form; in other cases, the hazards may be dependent on specific design or technology choices made during the design process. This appendix documents hazards from both categories to inform regulatory and licensing assessments.

Table 3A.1. Full Hazard Description for Licensing Significant Systems and Hazards

System	*Hazard Category*	*Specific Forms and Hazards*	*Discussion*
Torus Cooling / Fusion Breeding Blanket	15.0 - Radioactive Material	Solid activation products - fixed (structural materials)	Radioactive material is both fixed (activated structural materials) and mobile (liquid, gas, and solid corrosion products). Holdup or absorption of mobile radioactive materials could lead to additional contamination of surfaces and structures. Removal of mobile radioactive material could be conducted on a continuous or batch process. Batch may be simpler operationally but would result in larger inventories due to the build-up of radioactive material. Assume a TBR => 1, where the minimum tritium production rate is equal to the tritium burn rate
		Solid activation products - mobile (corrosion products)	
		Liquid activation product (based on blanket composition) Typical isotopes for FLiBe are Be-10, compounds	
		Gaseous activation products (based on blanket chemistry) Typical isotopes for FLiBe are H-3, C-14, F-18. Activated air/process gasses.	

Table 3A.1. Full Hazard Description for Licensing Significant Systems and Hazards

System	*Hazard Category*	*Specific Forms and Hazards*	*Discussion*
	16.0 - Hazardous Material	Beryllium and beryllium compounds, coolant components based on blanket chemistry (e.g., Pb, F, Cl) carcinogens, corrosives	Beryllium is the most significant hazard if used in salts. Other coolant components could present hazards such as fluoride in the form for fluoride gas or hydrogen fluoride gas. Chloride salts or metallic lead could also present hazards. Some materials and their compounds are carcinogenic and corrosive in a radioactive environment.
	9.0 Explosive Material	Salt components based on blanket chemistry (e.g., Li, Na, K), hydrogen gas	While salt components are flammable/explosive, the alkali metal components are stable in ionic salts and free reactive alkali metals are not expected in the breeding blanket.
	17.0 Direct Radiation Exposure	Neutron radiation, gamma/x-ray radiation, beta radiation, alpha radiation, radioactive contamination	All types of radiation are present in and around the blanket. This includes neutron radiation (from torus, (n,2n) reactions with beryllium), gamma/x-ray radiation from neutron scattering/activation, beta radiation from activated materials, alpha particles from (n,a) reactions, and radioactive contamination from mobile radioactive materials in the breeding blanket.
Blanket Processing System	15.0 - Radioactive Material	Solid activation products - mobile (corrosion products)	Mobile radioactive materials will be present in the blanket due to neutron activation (activation of blanket, corrosion of activated structural materials) and tritium breeding. Design designs will dictate if these products are left in the salt to build up to steady states, are removed continuously, or are removed in batch processes. Gaseous activation products will likely need to be actively removed.
		Liquid activation product (based on blanket composition) Typical isotopes for FLiBe are Be-10, compounds	
		Gaseous activation products (based on blanket chemistry) Typical isotopes for FLiBe are H-3, C-14, F-18	
	16.0 - Hazardous Material	Beryllium and beryllium compounds, coolant components based on blanket chemistry (e.g., Pb, F, Cl) carcinogens, corrosives	Beryllium is the most significant hazard if used in salts. Other coolant components could present hazards such as fluoride in the form for fluoride gas or hydrogen fluoride gas. Chloride salts or metallic lead could also present hazards. Some materials and their compounds are carcinogenic and corrosive in a radioactive environment. Systems for clean up and replenishment of degraded salts (transmutated salts, disassociated salts, corrosion products) may result in presence of concentrated or free salt components.

Table 3A.1. Full Hazard Description for Licensing Significant Systems and Hazards

System	*Hazard Category*	*Specific Forms and Hazards*	*Discussion*
	9.0 Explosive Material	Salt components based on blanket chemistry (e.g., Li, Na, K), hydrogen gas	While salt components are flammable/explosive, the alkali metal components are stable in ionic salts and free reactive alkali metals are not expected in the breeding blanket. Systems for clean up and replenishment of degraded salts (transmutated salts, disassociated salts, corrosion products) may result in presence of concentrated or free salt components.
	17.0 Direct Radiation Exposure	Gamma radiation, beta radiation, radioactive contamination	Gamma and beta radiation from activation, and radioactive contamination from mobile radioactive materials in the breeding blanket will be present in the processing system.
D-T Processing System	15.0 - Radioactive Material	Gaseous tritiated compounds (based on blanket chemistry). Typical compounds (based on blanket chemistry) could include be TF, T2, HT, or DT.	Tritiated compounds extracted from the blanket processing system are radioactive Depending on blanket chemistry and chemistry control, could include various tritium compounds including TF and mixed diatomic hydrogen species (T2, DT, HT). Additionally, activation of fluorine (F-18) is another radioactive source. Goal of DT processing system is to separate into hydrogen species for processing.
	16.0 - Hazardous Material	Beryllium or other alkali earth metals (if used as a reducing agents), gaseous coolant components based on blanket chemistry (e.g., F if separated from salt as TF)	Separation of hydrogen species from fluorine species has been proposed using alkali metal catalysts. Presence of beryllium and associated compounds would constitute a hazardous material. Separated fluorine would also represent a hazardous material.
	9.0 Explosive Material	Hydrogen gas	Gaseous hydrogen would be present from tritium and deuterium, likely as D2 and as various tritium species depending on system design (T2, DT, HT).
	17.0 Direct Radiation Exposure	Beta radiation (F-18, T), radioactive contamination	Both tritium and F-18 are beta emitting nuclides. Radioactive contamination by material uptake or formation of compounds could lead to residual contamination.
D-T Storage System	15.0 - Radioactive Material	Gaseous tritium (T2)	The storage system will contain gaseous tritium (T2) as part of routine loading and unloading of storage vessels. Some tritium may also be stored in the gaseous form.

Table 3A.1. Full Hazard Description for Licensing Significant Systems and Hazards

System	*Hazard Category*	*Specific Forms and Hazards*	*Discussion*
		Solid tritium compounds based on storage method (e.g., uranium titride, titanium titride)	The storage system will contain solid tritiated compounds as part of the storage medium. Current engineering practice is to store tritium on metallic hydrides. These metallic tritrides are solid radioactive substances that can also liberate tritium under certain conditions.
	16.0 - Hazardous Material	Storage materials (heavy metals), helium off gas, oxidizers	Storage of tritium and deuterium may involve use of heavy metal storage medium (e.g., uranium). Helium-3 off gassing from tritium decay is an asphyxiant hazard. Other oxidizers may be present as part of storage processing.
	9.0 Explosive Material	Hydrogen gas	Gaseous hydrogen would be present from tritium and deuterium, likely as D2 and T2.
	17.0 Direct Radiation Exposure	Beta radiation (T), radioactive contamination (tritiated materials)	Tritium is a beta emitting nuclide. Radioactive contamination by material uptake or formation of compounds could lead to residual contamination.
Fusion Fuel Preparation System	15.0 - Radioactive Material	Gaseous tritium (T2)	The fuel preparation system will include both gaseous tritium (for injection via neutral beams, fuel gas puffing, and as the source fuel for frozen pellets) and solid form tritium (frozen pellets of D-T). Holdup or absorption of tritium could lead to additional contamination of surfaces and structures.
		Solid tritium or deuterium-tritium (frozen pellet), contaminated tritium systems	
	16.0 - Hazardous Material	Asphyxiants - cryogenic coolants	Liquid helium or other cryogenic coolants will be needed for the pellet production and other fuel handling systems.
	9.0 Explosive Material	Hydrogen gas	Gaseous hydrogen would be present from tritium and deuterium, likely as D2 and T2. Some mixed DT hydrogen may be found in certain systems
	17.0 Direct Radiation Exposure	Beta radiation (T), radioactive contamination (tritiated materials)	Tritium is a beta emitting nuclide. Radioactive contamination by material uptake or formation of compounds could lead to residual contamination.
Plasma Heating System	15.0 - Radioactive Material	Gaseous tritium (T2)	The plasma heating system may include tritium for neutral beam injector (NIB) heating of he plasma This system would include gaseous tritium fuel, plasma generated for the neutral beam injector, solid (frozen) tritium deposited on NBI collection surfaces, and tritium absorbed by surfaces.
		Plasma tritium	
		Solid tritium, tritiated systems	

Table 3A.1. Full Hazard Description for Licensing Significant Systems and Hazards

System	*Hazard Category*	*Specific Forms and Hazards*	*Discussion*
	16.0 - Hazardous Material	Asphyxiants - cryogenic coolants	Liquid helium or other cryogenic coolants will be needed for the NBI
	9.0 Explosive Material	Hydrogen gas	Gaseous hydrogen would be present from tritium and deuterium, likely as D2 and T2. Some mixed DT hydrogen may be found in certain systems
	17.0 Direct Radiation Exposure	Beta radiation (T), ion beam, radioactive contamination (tritiated materials, activated materials)	Tritium is a beta emitting nuclide. Radioactive contamination by material uptake or formation of compounds could lead to residual contamination. The NBI contains an ion beam that is neutralized before injection and is a high energy particle beam source.
Plasma Fueling System	15.0 - Radioactive Material	Gaseous tritium (T2)	The plasma fueling system will include both gaseous tritium (for fuel gas puffing) and solid form tritium (frozen pellets of D-T). Holdup or absorption of tritium could lead to additional contamination of surfaces and structures.
		Solid tritium or deuterium-tritium (frozen pellet)	
	16.0 - Hazardous Material	Asphyxiants - cryogenic coolants	Liquid helium or other cryogenic coolants may be needed for the pellet production and other fuel handling systems.
	9.0 Explosive Material	Hydrogen gas	Gaseous hydrogen would be present from tritium and deuterium, likely as D2 and T2. Some mixed DT hydrogen may be found in certain systems
	17.0 Direct Radiation Exposure	Beta radiation (T), radioactive contamination (tritiated materials, activated materials)	Tritium is a beta emitting nuclide. Radioactive contamination by material uptake or formation of compounds could lead to residual contamination.
Torus / Vacuum Vessel	15.0 - Radioactive Material	Solid activated and tritium contaminated products - fixed (structural materials)	The torus will contain radioactive material in every form of matter. Plasma will contain tritium and neutron activated control gasses. As the plasma cools and neutralizes, they will reconvert to gaseous tritium and activated control gasses. D-T fusion reactions within the plasma will produce high energy (14.1 MeV) neutron fluxes. This radiation will activate structural materials inside the torus. The structural materials will also absorb free tritium and form tritated solid compounds. Erosion of structural materials by plasma wall interactions will produce mobile solid radioactive materials (tritiated materials and activated materials).
		Solid activated and tritium contaminated products - mobile (erosion products)	
		Gaseous radioactive products (tritium, activated control gasses)	
		Plasma radioactive products (tritium, activated control gasses)	

Table 3A.1. Full Hazard Description for Licensing Significant Systems and Hazards

System	*Hazard Category*	*Specific Forms and Hazards*	*Discussion*
	16.0 - Hazardous Material	Dusts and particles; lead, beryllium or carcinogenic materials (based on first wall choices), strong oxidizing conditions (based on first wall choices)	Erosion products within the torus are a source of fine dusts and particles. Some proposed structural materials such as lead or beryllium are significant carcinogenic materials and health concerns. At elevated temperatures, some proposed structural materials are strongly oxidizing.
	9.0 Explosive Material	Dusts and particles, hydrogen	Fine dusts and particles; gaseous hydrogen would be present from tritium and deuterium fuel
	17.0 Direct Radiation Exposure	Neutron radiation, gamma/x-ray radiation, beta radiation, alpha radiation, radioactive contamination	The torus will have significant neutron radiation, gamma/x-ray radiation (activation, (n,y) reactions), beta radiation (activation, tritiated materials), alpha radiation, radioactive contamination from tritiated materials and neutron activated materials.
Torus Vacuum Pumping System	15.0 - Radioactive Material	Solid activated and tritium contaminated products - mobile (erosion products)	The primary radioactive material in the torus vacuum pumping system is gaseous tritium and activated control gasses pumped from the torus to maintain proper atmospheric conditions. Depending on torus conditions, solid activated or tritiated contaminated erosion products could be pumped into this system if mobilized.
		Gaseous radioactive products (tritium, activated control gasses)	
	16.0 - Hazardous Material	Dusts and particles	Any mobile dusts and particles removed from the torus via vacuum pumping
	9.0 Explosive Material	Dusts and particles, hydrogen	Any mobile dusts and particles removed from the torus via vacuum pumping; gaseous hydrogen would be present from tritium and deuterium
	17.0 Direct Radiation Exposure	Gamma/x-ray radiation, beta radiation, alpha radiation, radioactive contamination	Gamma/x-ray, beta, and alpha radiation (activated materials), beta radiation (tritium and tritiated materials), radioactive contamination from tritiated materials and neutron activated materials.
Fusion Exhaust Processing System	15.0 - Radioactive Material	Solid activated and tritium contaminated products - mobile (erosion products)	The primary radioactive material in the torus vacuum pumping system is gaseous tritium and activated control gasses pumped from the torus to maintain proper atmospheric conditions. Depending on torus conditions, solid activated or tritiated contaminated erosion products could be pumped into this system if mobilized.
		Gaseous radioactive products (tritium, activated control gasses)	

Table 3A.1. Full Hazard Description for Licensing Significant Systems and Hazards

System	*Hazard Category*	*Specific Forms and Hazards*	*Discussion*
	16.0 - Hazardous Material	Dusts and particles	Any mobile dusts and particles removed from the torus via vacuum pumping
	9.0 Explosive Material	Dusts and particles, hydrogen	Any mobile dusts and particles removed from the torus via vacuum pumping; gaseous hydrogen would be present from tritium and deuterium
	17.0 Direct Radiation Exposure	Gamma/x-ray radiation, beta radiation, alpha radiation, radioactive contamination	Gamma/x-ray, beta, and alpha radiation (activated materials), beta radiation (tritium and tritiated materials), radioactive contamination from tritiated materials and neutron activated materials.
Hydrogen Isotope Separation System	15.0 - Radioactive Material	Gaseous tritium (T2, DT, HT)	Mixed diatomic hydrogen species (H, D, T)
	16.0 - Hazardous Material	Asphyxiants - cryogenic coolants	Large quantities of cryogenic materials (e.g., He) to reach 20K separation temperatures for hydrogen
	9.0 Explosive Material	Hydrogen gas	Large cryo-columns of hydrogen for isotopic separation
	17.0 Direct Radiation Exposure	Beta radiation, radioactive contamination	Tritium is a beta emitting nuclide. Radioactive contamination by material uptake or formation of compounds could lead to residual contamination.
Plant Emission Control Systems	15.0 - Radioactive Material	Gaseous radioactive products (tritium, activated control gasses, gaseous activation products)	Radiological emissions from plant systems, structures, and components during normal operation include radioactive gasses and liquid streams. These emissions may be due to leaks or diffusion through structures, systems, and components.
		Liquid radioactive products (water with dissolved activated materials or solid activation products, HTO)	
	16.0 - Hazardous Material	Off-gas coolant components based on blanket chemistry (e.g., F, Cl), process gasses, carcinogenic compounds in water (decontamination solutions), beryllium contaminated materials	Hazardous emissions from plant systems, structures, and components during normal operation include toxic and carcinogenic gasses and contaminated liquids. These emissions may be due to leaks or diffusion through structures, systems, and components.
	9.0 Explosive Material	Hydrogen gas	Leaks of hydrogen gas will be captured by this system and processed before release
	17.0 Direct Radiation Exposure	Gamma/x-ray radiation, beta radiation, alpha radiation, radioactive contamination	This system may contain mobile radioactive contaminants and radiation present in any plant system.
Radiological Waste Handling System	15.0 - Radioactive Material	Solid activation and tritium contaiminated products - fixed (structural materials)	The radiological waste handling system will process any and all radiological waste streams from plant systems. This includes solid, liquid, and gaseous waste streams. This can include process and maintenance wastes.
		Solid activation and tritium contaiminated products - mobile (corrosion products)	

Table 3A.1. Full Hazard Description for Licensing Significant Systems and Hazards

System	*Hazard Category*	*Specific Forms and Hazards*	*Discussion*
		Liquid activation product (based on blanket composition) Typical isotopes for FLiBe are Be-10, compounds, liquid radioactive products (water with dissolved activated materials, HTO)	Hydrogen and tritiated wastes are separated for isotopic separation.
		Gaseous activation products (based on blanket chemistry) Typical isotopes for FLiBe are C-14, F-18. Gaseous tritium and tritiated compounds. Activated air and process gas products	
	16.0 - Hazardous Material	Contaminated corrosive, carcinogenic, beryllium compounds	Any hazardous wastes from plant systems contaminated with radiological materials (e.g., tritiated materials or activated hazardous materials)
	9.0 Explosive Material	Hydrogen gas, dusts	Both radiological hydrogen gas and tritiated/activated dusts
	17.0 Direct Radiation Exposure	Gamma/x-ray radiation, beta radiation, alpha radiation, radioactive contamination	This system may contain mobile radioactive contaminants and radiation present in any plant system.
Waste Disposal System	15.0 - Radioactive Material	Solid activation products (mobile and fixed), contaminated solid materials. Absorbed or stabilized liquid and gaseous radioactive materials.	This system contains radiological wastes that are processed for off-site controlled disposal and not effluent releases. This can include packaged solids, free or stabilized liquids, and free or solidified gases. Any radioactive material found in the plant may be found in this system.
		Liquid activation product (based on blanket composition) Typical isotopes for FLiBe are Be-10, compounds, liquid radioactive products (water with dissolved activated materials, HTO)	
		Gaseous activation products (based on blanket chemistry) Typical isotopes for FLiBe are C-14, F-18. Gaseous tritium and tritiated compounds. Activated air and process gas products	
	16.0 - Hazardous Material	Beryllium and beryllium compounds, coolant components based on blanket chemistry (e.g., Pb, F, Cl) carcinogens, corrosives, dusts, lead	Any hazardous wastes from plant systems that cannot be recycled on site will be found in this system for off-site disposal.
	9.0 Explosive Material	Hydrogen gas, dusts, salt components based on blanket chemistry (e.g., Li, Na, K),	Hydrogen gas not designated for effluent release, dusts, and any separated salt components may be found in this system for disposal.

Table 3A.1. Full Hazard Description for Licensing Significant Systems and Hazards

System	*Hazard Category*	*Specific Forms and Hazards*	*Discussion*
	17.0 Direct Radiation Exposure	Gamma/x-ray radiation, beta radiation, alpha radiation, radioactive contamination	This system may contain mobile radioactive contaminants and radiation present in any plant system.
Effluent Release System	15.0 - Radioactive Material	Gaseous radioactive products (tritium, activated control gasses, gaseous activation products)	Radioactive release of effluents is permitted for specific isotopes per national regulatory requirements. This system would contain both the gaseous and liquid radiological wastes for release, monitoring and controlling the total releases.
		Liquid radioactive products (water with dissolved activated materials, HTO)	
	16.0 - Hazardous Material	Off-gas coolant components based on blanket chemistry (e.g., F, Cl), process gasses	Release of specific hazardous effluents is permitted for specific chemicals per national regulatory requirements. This system would contain both the gaseous and liquid wastes for release, monitoring and controlling the total releases.
		Carcinogenic compounds in water (decontamination solutions)	
	9.0 Explosive Material	Hydrogen gas	Hydrogen gas could be released or flared per design
	17.0 Direct Radiation Exposure	Gamma/x-ray radiation, beta radiation, alpha radiation, radioactive contamination	This system may contain mobile radioactive contaminants and radiation present in any released radioactive effluent stream.

Chapter 4 – Hazard limits for commercial fusion hazards

Optimal regulation of a new technology requires that hazards and hazard consequences associated with all phases of the technology lifecycle are limited to below acceptable limits. Technology hazard limits generally include hazards relevant to both short-term (acute) hazard consequences and long-term (chronic) hazard consequences. These limits may be provided by a wide variety of groups, each with different focuses and priorities. Potential groups that provide hazard limits include:

- Individual companies and developers
- Insurance companies
- Industry trade groups
- Professional societies
- Public interest groups
- Governmental regulators
- Legislative bodies
- Executive bodies

These limits may be recommended (public interest groups, industry trade groups), voluntarily adopted (insurance companies, individual companies, professional societies), or required by contract or law (insurance companies, governmental groups). The limits will inform both the design and operation of facilities.

This chapter reviews the types of limits that can be developed and set for both hazards and hazard consequences. Generally, hazard limits can be categorized into five groups:

- Consequence limits (direct and indirect)
- Dose/total exposure limits
- Concentration exposure limits
- Release limits (concentration and total emission)
- Total inventory limits

These limits are used by different industries to control the hazard consequences and risks of technologies. Each limit has different advantages and limitations that impact its effectiveness as a regulatory benchmark.

In this chapter, the five limit types are discussed in detail, and the advantages and disadvantages of each are highlighted. A process for creating each type of hazard limit is then presented for major hazards associated with commercial fusion (Chapter 3). When applicable, limits based existing regulatory precedent are proposed and justified. Finally, the hazard limits are compared and their impacts on licensing and regulatory activities are discussed.

4.1 Basis for hierarchical hazard limits

Hazard limits are defined in this work as any specified limit for a hazard (e.g., a material that may result in a loss) or consequnce. Hazard limits are generally characterized based on hazard itself (e.g., quantity or concentration of the hazard) or the potential consequences of the hazard, either directly (e.g., excess cancers) or indirectly (e.g., radiation dose that increases cancer risk).

Different stakeholders may implicitly or explicitly set hazard limits for different activities. Business owners, workers, and members of the public may set different levels of acceptable hazards for the same activity. Regulatory hazard limits are intended to represent a socially acceptable limit for the consequences of a particular hazard.

Hazard limits can be challenging to compare between activities because different types of hazard limits are used for different activities. Consider specific hazard limits for different industries:

- Coal power plant operation: missions must not exceed a maximum filterable particulate limit of 9.0E-2 lb/MWh [1]
- Natural gas pipeline operation: required design margin for pipelines vary based on the proximity of homes and other structures [2]
- Nuclear power plants: members of the public must not exceed a total effective dose equivalent of 1 rem annually [3]

These hazard limits all relate to the safety of energy infrastructure but it is not clear from these limits if all energy coal, natural gas, and nuclear fission are held to the same level of safety for operations. The challenge of comparing hazard limits can lead to different levels of safety for different activities that are based, in part, on the perceived hazards and not on the actual hazards. While use of different hazard limits for different activities is the prerogative of stakeholders, understanding the actual relationship between different hazard limits is useful when developing limits for new technologies.

Comparing seemingly dissimilar hazard limits is possible through the hierarchical characterization of hazard limits. All hazards are, ultimately, expressions of the socially acceptable direct consequence of a particular hazard. While no major regulatory organizations explicitly state the number of people who may be killed or injured each year by a technology (direct consequence limit), regulatory assumptions used in the creation and calculation of all other hazard limits inherently link to a direct consequence limit. Characterizing the different hazard limit levels and determining appropriate regulatory assumptions that can be used to compare different hazard limits and develop equivalent and self-consistent hazard limits for direct comparison.

For example, air concentration exposure hazard limits are commonly used by regulatory agencies such as the Occupational Health and Safety Administration (OSHA) to define regulatory limits for hazardous substances. These limits can be given in time based average concentrations (such as $\frac{\mu g}{m^3}$of air averaged over an eight-hour period). This hazard limit, while measurable, does not correspond to a socially relevant hazard consequence. Instead, regulatory assumptions are used by agencies to connect this limit to direct and indirect consequence limits.

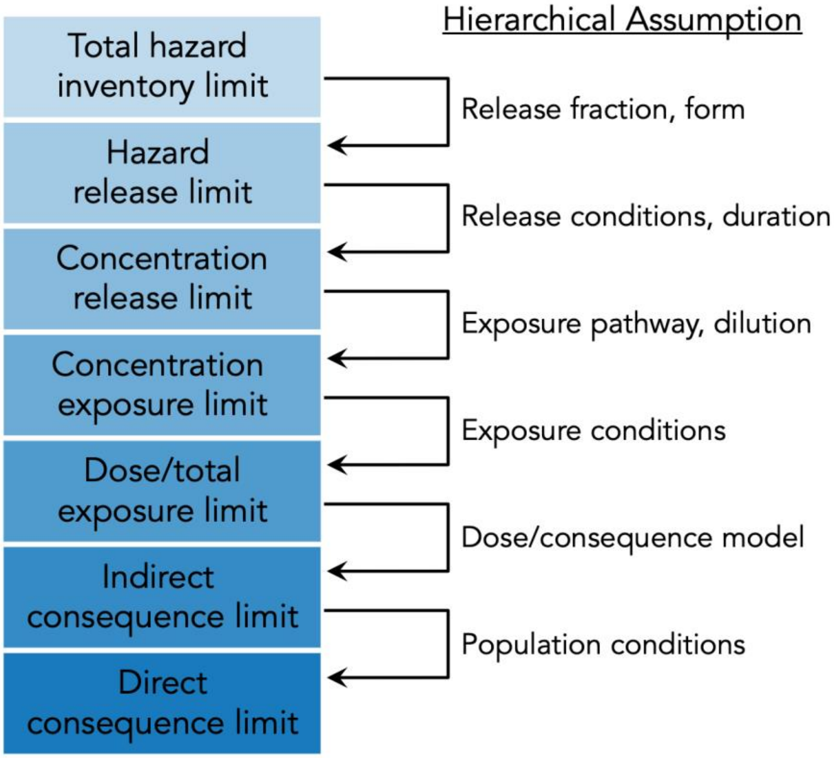

Hierarchical Assumption
Total hazard inventory limit
Release fraction, form
Hazard release limit
Release conditions, duration
Concentration release limit
Exposure pathway, dilution
Concentration exposure limit
Exposure conditions
Dose/total exposure limit
Dose/consequence model
Indirect consequence limit
Population conditions
Direct consequence limit

Figure 7-1. Hierarchical hazard limits

The following example regulatory assumptions could be used to correlate the concentration exposure hazard limits (higher hierarchical level hazard limit) to a socially relevant direct hazard consequence (lower hierarchical level hazard limit):

- Concentration exposure to total exposure:
    - The expected bounding exposure of an individual is assumed to occur at the maximum allowable concentration (e.g., individual is continuously exposed to air at the maximum allowable concentration for 8 hours per day, 250 days per year, for a 45 year career). This calculation produces a total exposure characterized in terms of a cumulative exposure or lifetime average exposure based on the concentration exposure
- Total exposure to indirect consequence limit:
    - A scientific correlation between total exposure and increased incidence of some indirect consequence (e.g., increase incidence of illness, cancer, or fatality) is developed based on existing scientific literature or experience. Absent adequate scientific literature, other data sources may be used to derive the relationship. This is a scientific model representing best understanding of the exposure/consequence relationship. This calculation produces a risk of incidence or fatality based on the total exposure

- Indirect consequence limit to direct consequence limit:
    - The total number of individuals potentially exposed to the hazard is multiplied by the indirect consequence limit to produce an expected direct consequence on society. This is the calculated socially relevant consequence of setting the air concentration exposure hazard limit at a specific level.

Description and understanding of hierarchical limits facilitates the development of more consistent regulatory limits. First, it forces clarification of the underlying assumptions behind different hazard limits and can provide clear justification for limits. Second, it allows comparison of different hazards or calculation of cumulative consequence limits for multiple hazards using indirect or direct consequence limits. Third, if new types of limits are proposed for a technology to ease licensing (e.g., total inventory limit for technology traditionally subject to dose/total exposure limits), this hierarchy can be used to help demonstrate equivalent safety or justify the change in consequence.

Depending on the application, the direct or indirect consequences of hazards may be of societal interest, but the cumulative direct consequence represents the total societal cost of a hazard consequence and the corresponding regulatory limit. In some cases, this cost can be converted into an economic cost using a conversion metric such as cost per human life or cost per year of life.

Hierarchical hazard limits are important to understanding the potential impacts of hazard limits on licensing and regulatory activities, as well as understanding underlying connections between different hazard limits. This chapter reviews each type of hazard limit and describes the hierarchical connections between limits from direct consequence limits (lowest hierarchical level hazard limit) to total inventory limits (highest hierarchical level hazard limit).

4.2 Characterizing hazard limits and performance based limits

In this work, hazard limits are defined as regulatory limits that are independent of technology instead relating limits directly to the hazard and potential consequences of the hazard. These regulatory limits are commonly characterized in regulatory literature as "performance based" limits because they specify the performance characteristics of the activity and not the means or methods used satisfy the regulatory intent. These limits differ from technology based limits and requirements, commonly described as "prescriptive" or "design standard" regulations [4]. These prescriptive and performance based limits are compatible and comparable using hierarchical hazard limits. Section 4.8 describes the relationship and compatibility between these limit types.

A hazard limit type can be characterized based on its impact on important types of factors including:

- Inherent assumptions and uncertainty
    - Number of embedded regulatory assumptions in hazard limit
    - Level of residual uncertainty (producing excess risk or conservatism)

- Effects on regulatory evaluations
    - Initial analytic work or effort required by regulator
    - Analytic work or effort required by licensee
    - Effort required for review and approval by regulator
    - Flexibility for exemptions to hazard limits
    - Overall usability of limit for regulatory evaluation
- Effects on regulatory enforcement and operations
    - Ability for regulator to monitor or enforce limits
    - Ability to enforce/correct operation before consequence occurs
    - Overall usability of limit for regulatory operations

These factors affect the overall regulatory burden of complying with (and demonstrating compliance with) hazard limits for both regulatory evaluations and operations. The appropriate hazard limit type will depend on the specific hazard, the licensing evaluation method (Chapter 5), and the regulatory framework (Chapter 6). This section discusses the impact of each hazard limit type on listed factors.

4.3 Consequence based hazard limits

Consequence based hazard limits are the simplest (conceptually) type of regulation of technology or activity for public health and safety. These limits explicitly limit the effect of a hazard and require applicants to demonstrate by analysis (and performance) that they do not exceed acceptable limits. The consequences limits can be characterized as either direct (e.g., excess cancers) or indirect (e.g., excess increases in risk of developing cancer). For any regulated activity, the ultimate goal of regulation is to limit the consequences (physical, psychological, social, financial) of the activity to a socially acceptable level. There are no assumptions made between the hazard limit and the consequence.

4.3.1 Direct consequence based hazard limits

Explicit direct consequence based hazard limits are not used for regulatory applications in the United States. Consequence based limits are normally set based on the social acceptability of a hazard, an industry, and a consequence. Explicit discussion of acceptable number of injuries or fatalities for routine commercial applications can be seen as permitting companies to put operations and profit over worker safety. As a result, no major industries are regulated based on the principle that operation is permitted if the number of accidents, illnesses, injuries, or fatalities remains below a specified threshold level.

For example, the U.S. Occupational Health and Safety Administration (OSHA) does not regulate solely based on the number of incidents that a company has – there is not a legally acceptable number of annual fatalities for companies in the United States. Company incidents or incidents rates exceeding threshold rates may trigger additional interventions or inspections by OSHA [5], but this does not indicate that any incidents below the threshold are wholly acceptable.

Inherent assumptions and uncertainty

Direct consequence based hazard limits have no inherent assumptions but may be subject to significant uncertainty. Direct consequence based hazard limits are attractive because of their perceived simplicity: the hazard limit is based solely on the actual consequence of the hazard. The elimination of regulatory assumptions also allows for the direct comparison of the consequences of different technologies or societal choices. The impact of any decision related to hazards (e.g., selection of different electricity generation source) can be compared on consequence to consequence basis (e.g., deaths per kW-hr of electrical energy produced including all known technology externalities). There are no requirements on design or tracking plant performance, as long as it can be demonstrated that the facility does not exceed the socially accepted consequence limits. This advantage is, ironically, also a major weakness for the use direct consequence based hazard limits for operational regulatory purposes.

Despite this simplicity related to inherent assumptions related to the actual consequence, this limit can be subject to significant uncertainty especially for controlling the potential impacts of industries with catastrophic or extremely high consequence individual events. For industries where a single event or product can impact tens, hundreds, or thousands of people, use of an annual direct consequence limit may not result in the socially desirable level of safety. Would an activity or industry be permitted to operate until it has an accident that exceeds the direct consequence limit, at which point it is no longer permitted? If so, could bounds be placed on the catastrophic consequence? In this case, industries would be assumed to be safe until they demonstrate otherwise – a potentially socially unfavorable proposition.

An alternative approach for low probability, high consequence events would be to base a direct consequence limit on an averaged basis. For example, an industry may not have more than an average of 10 fatalities per year over any 10 year period. Using this limit, a catastrophic event resulting in 100 fatalities could be permitted once every 10 years. This raises the question as to whether such a consequence would be socially acceptable, even though it thought it meets an averaged annual consequence limit. Studies in the field of risk perception suggest a lower societal tolerance for catastrophic risk than chronic or routine risks [6]. As a result, while an annual averaged direct consequence limit may produce a numerically acceptable level of safety, the realized safety performance may be socially unacceptable for activities or events with potentially catastrophic events.

While eliminating regulatory assumptions can simplify the use of direct consequence based hazard limits, the uncertainty related to application of these limits for events with severe consequences may be limited.

Effects on regulatory evaluations

Use of direct consequence based hazard limits creates a regulatory system where initial creation requires substantial societal discussion and decision making, but the technical regulatory burden is shifter to later in the process.

One major challenge of direct consequence based hazard limits is that initial determination of the hazard limit is subject to a social process of selecting a socially acceptable consequence limit. This social process for agreeing upon the limit can be challenging and even taboo. It requires a wide variety of stakeholders to evaluate a hazard collectively, balance competing or conflicting priorities, and arrive at a compromise limit. The idea of explicitly and directly stating acceptable number of injuries or deaths associated with a commercial activity challenges basic social norms on topics such as the value of an individual human life against economic profit or larger societal goals. The death or injury of an individual to better society may be acceptable in an abstract sense, but socially unacceptable when put into practice.

Additionally, issues of equality and social justice are likely major factors when selecting who would be the "acceptable" victims of a hazard limit; are all people subject to the same consequence likelihood or would people from historically disadvantaged groups have a higher consequence likelihood due to political or economic factors? While direct consequence based hazard limits are (conceptually) simple and fair, these practical limitations of demonstrating compliance with direct consequence limits and social selection of consequence renders these limits largely ineffective for regulatory purposes. This process is socially challenging but does not require substantial initial analytic work by a regulator.

Following determination of direct consequence based hazard limits, subsequent regulatory evaluations may provide a wide degree of flexibility in design and analysis (given no regulatory assumptions inherent in a direct consequence based hazard limit) but require substantial effort to prepare and review. Calculation of the direct consequences of any activity require a substantial number of assumptions, each of which could have substantial uncertainties or be subject to challenge from regulators or members of the public. This could result in extremely lengthy calculations that are difficult and costly to prepare and review.

Use of direct consequence based hazard limits are fairly compatible with a flexible, exemption based regulatory process. If an applicant does not meet the direct consequence hazard limit, they could apply for an exemption and allow operation. The absence of regulatory assumptions with direct consequence hazard limits may allow for simpler exemptions because the potential societal implication of the exemption will be demonstrated based on the regulatory evaluation. This is ultimately also a challenge facing exemptions for direct consequence based hazard limits: the potential societal impacts of the exemption will be extremely clear and may face social barriers. For example, stating that an activity should be allowed to statistically cause ten excess cancer cases per year to eliminate the need for additional safety equipment many not be a socially viable argument in some cases.

Direct consequence based hazard limits may be an effective regulatory evaluation metric because they allow for complete flexibility in how an applicant proposes and evaluates safety. This flexibility, however, comes at a cost as the effort required to prepare and review these evaluations may be high. The societal decision making process associated with initial creation and justification of the direct consequence based hazard limits could also present additional challenges.

Effects on regulatory enforcement and operations

While direct consequence based hazard limits can be effective for regulatory evaluations, they can be difficult in practice for regulatory enforcement and monitoring during operations.

Demonstration that a hazard is directly responsible for or related to a consequence can be extremely difficult, especially for consequences with multiple causes. For example, if a consequence limit for a hazard is based on number of excess cancers caused by the hazard, demonstrating the direct link between the hazard and the consequence can be subject to significant uncertainties. For certain hazards that may cause extremely rare cancers, statistical proof between the expected number of cancers (near zero) and observed number of cancers may constitute proof that a direct consequence limit is met (e.g., chronic beryllium diseases caused primarily by exposure to airborne beryllium dust [7]). For most hazards, however, their consequences can be hard to distinguish from consequences related to other environmental, industrial, or genetic related causes (e.g., general increase in whole body cancer incidence expected based on ingestion of tritium [8]. As a result, proving that the limit has been met may be extremely challenging, subject to significant uncertainty, and vulnerable to challenge.

The use of a direct consequence based hazard limit for regulatory operation also means that the limit has not been violated until after the consequence has actually occurred. Preemptive correction of an activity is impossible with use of direct consequences alone. One strategy for partial operational enforcement of direct consequence limits is to enforce that all evaluation assumptions used to demonstrate compliance with the direct hazard consequence limit are met.

4.3.2 Indirect consequence based hazard limits

Explicit indirect consequence based hazard limits relate a hazard to a consequence indirectly, often through a calculation of a statistical increase in risk of the consequence occurring. This may include injuries (e.g., risk of system failure resulting in worker injury), illnesses (e.g., risk of excess cancers), or fatalities (e.g., risk of fatal injury) resulting from a hazard. An example of an explicit indirect consequence based hazard limit is given the U.S. Nuclear Regulatory Commission's *Reactor Safety Goal Policy Statement*:

> The risk to an average individual in the vicinity of a nuclear power plant of prompt fatalities that might result from reactor accidents should not exceed one-tenth of one percent (0.1 percent) of the sum of prompt fatality risks resulting from other accidents to which members of the U.S. population are generally exposed [9]

This limit indirectly links a potential hazard source (reactor accidents) to a hazard consequence (prompt fatality risks) via a socially acceptable risk level.

Inherent assumptions and uncertainty

Indirect consequence based hazard limits has no inherent assumptions although it may require an implicit assumption depending on specific societal priorities on hazard consequences.

The lack of inherent assumptions for indirect consequence based hazard limits enables the comparison of consequences to other societally acceptable activities or "background" risk to justify acceptability. This type of limit also allows for the direct comparison of the safety of disparate activities or industries that otherwise may not be comparable. It attempts to provides a quantitative technical basis for "how safe is safe enough" rather than solely relying on expert judgment or social decision making enacted through legislation or court judgments.

Implicit assumptions may be used to allow comparison between direct and indirect hazard limits. The indirect consequence hazard limit (e.g., rate or change of occurrence) and the direct consequence hazard limit (total occurrence) can be specifying the exposed group (e.g., population) and total time during which the hazard occurs. In some cases, the indirect consequence based hazard limits may be used as a method to reframe societal discussion or avoid explicit statement of the actual societal consequences of a hazard.

In the example given above, the indirect hazard limit for commercial nuclear power plants is given as 0.1 percent of all other causes. This number may appear exceedingly low, but if one considers that 3.8 million people live within 10 miles of a nuclear power plant [10] and approximately 50 people per 100,000 are killed each year from all other accidents [11], than the total statistical direct consequence would be:

$$3{,}800{,}000\ people \cdot \frac{50\ deaths}{100{,}000\ people} \cdot 0.001 = 1.9\ people$$

This number may not be useful for regulatory discussions, but it is possible to compare direct and indirect consequence based hazard limits based on the implicit assumption of exposed groups. This number may be subject to uncertainty depending on the level of information available regarding the exposed group.

Indirect consequence limits can provide value as a backstop or technical justification for other hazard limits. Selection of dose or concentration based limits require justification, so indirect consequence analysis of criteria such as increase in cancer rates or mortality can be used to justify these exposures. For example, OSHA has historically based permissive exposure levels (PEL) based on the threshold for excess risk of one death or serious illness per 1000 workers exposed to a hazard over a 45-year working life [12]. This indirect consequence limit constitutes a "significant risk" it relates to protection of workers specified in the Occupational Health and Safety Act and is part of the underlying regulatory basis to the concentration based PEL set by OSHA. This role for indirect consequence limits can be extremely effective at creating uniform standards for acceptable consequences, especially for similar hazards

Effects on regulatory evaluations

Use of indirect consequence based hazard limits requires significant societal discussion and decision making to initially develop, but the technical burden of implementation is shifted to later in the regulatory process. Similar to direct consequence based hazard limits, indirect consequence limits do not require substantial initial technical analysis by a regulator, but the initial determination of a hazard limit requires selection a socially acceptable consequence limit.

Creation of an indirect consequence based hazard limits can be socially challenging because it is a public admission of the residual risk of a technology or activity. For example, while it is a factually true that commercial aircraft crash, aircraft manufacturers and commercial airlines would not want customers to focus on the fact their plane could be the outlier. Instead, limits are set in a manner that "ensure safety" and not "limit risk".

For some activities or technologies, limits can be created based on regulatory precedent set by related activities or other societal risks. For example, the one-tenth of one percent limit selected by the NRC for risks associated with commercial nuclear power plants was derived based on the rational that "the 0.1 percent ration to other risks is low enough that people living or working near nuclear power plants would have no special concern due to the plant's proximity" [13]. Alternatively, courts and regulatory agencies have relied on more colloquial measurements of hazard when determining acceptable societal risk. In a 1980 Supreme Court ruling regarding OSHA air quality standards, the Court notes:

> Some risks are plainly acceptable, and others are plainly unacceptable. If, for example, the odds are one in a billion that a person will die from cancer by taking a drink of chlorinated water, the risk clearly could not be considered significant. On the other hand, if the odds are one in a thousand that regular inhalation of gasoline vapors that are 2% benzene will be fatal, a reasonable person might well consider the risk significant and take appropriate steps to decrease or eliminate it. Although the Agency has no duty to calculate the exact probability of harm, it does have an obligation to find that a significant risk is present before it can characterize a place of employment as "unsafe." [14]

While the indirect risk metric of one in one thousand risk was created without any formal social decision making process, it has become a "general policy" for OSHA to use this metric when creating hazard limits for materials [12].

Similar to direct consequence based hazard limits, subsequent regulatory evaluations to demonstrate compliance with indirect consequence based hazard limits can provide a wide degree of flexibility in design and analysis but require substantial effort to prepare and review. While indirect consequences do not require knowledge of specific populations or areas, calculation of an indirect consequence requires a substantial number of assumptions, each of which could have substantial uncertainties or be subject to challenge from regulators or members of the public. This could again result in extremely lengthy calculations that are difficult and costly to prepare and review.

Indirect consequence based hazard limits are also fairly compatible with a flexible exemption based regulatory process. The absence of regulatory assumptions may allow for simpler exemptions because the potential societal implication of the exemption will be demonstrated based on the regulatory evaluation. The main challenges of exemptions with an indirect consequence based hazard limit are social challenges associated with explicit justification of higher societal consequences.

Indirect consequence based hazard limits have been demonstrated as an effective backstop regulatory evaluation metric because they allow for comparison with other societal risks. While indirect consequence based hazard limits have not been used widely as the primary hazard limit, the flexibility in how an applicant proposes and evaluates safety could allow for innovation in design and analysis. Similar to direct consequence based hazard limits, this flexibility can increase the effort required to prepare and review these evaluations. The societal decision making process associated with initial creation and justification of the indirect consequence based hazard limits could also present additional challenges.

Effects on regulatory enforcement and operations

Similar to direct consequence based hazard limits, indirect consequence based hazard limits can be difficult in practice for regulatory enforcement and monitoring during operations.

Demonstration that a hazard is directly responsible for or related to a consequence can be extremely difficult, especially for consequences with multiple causes or consequences that occur naturally with low or high frequency. Much like the challenge faced by direct consequence based hazard limits, the proving that limits are met is challenging when multiple environmental, industrial, or genetic related causes can increase the incidence of illnesses or fatalities. Demonstrating small statistical changes can be extremely challenging due to the large number of observations required to gain statistical significant certainty. Proving that the indirect consequence limit has been met may therefore be extremely challenging, subject to significant uncertainty, and vulnerable to challenge if extensive monitoring of exposed populations is not monitored before, during, and after operation.

The use of an indirect consequence based hazard limit for regulatory operation also means that the limit has not been violated until after the consequence has actually occurred or evidence suggests that the indirect limit will be exceeded based on observable trends. Preemptive correction of an activity is impossible with use of indirect consequences alone. Similar to a direct hazard limit, one strategy for partial operational enforcement of indirect consequence limits is to enforce that all evaluation assumptions used to demonstrate compliance with the indirect hazard consequence limit are met.

4.3.3 Creating consequence based hazard limit for commercial fusion facilities

Developing direct and indirect consequence based hazard limit for commercial fusion facilities is challenging due to the impact of social factors on the development process and the cultural taboo against accepting public injury or death as an unavoidable consequence of economic output. While a no-consequence hazard limit is desirable for all activities, meeting this hazard limit may be not technologically feasible, cost-effective, or allow for net societal benefit from a hazardous activity. Definitions of direct and indirect consequence based hazard limits is critical for assessing the acceptability of probabilistic consequences and for the consistent definition of higher hierarchical hazard limits from lower hierarchical hazard limits.

In this work, direct and indirect consequence based hazard limits are proposed to enable consistent development of higher hierarchical hazard limits and facilitate discussion on the impacts of direct and indirect consequence based hazard limit assumptions on the regulatory process. These limits are not intended as recommendations and should not be construed to supplant the social decision making processes necessary when defining direct and indirect consequence based hazard limits.

Table 4.1. Direct consequences from energy generation technologies

		500 MWe facility, 90% capacity factor	
Power Source	Observed average fatalities per TWh	Annual average fatalities	80-year average fatalities
Coal	24.62[1]	97.05	7764.16
Oil	18.43[1]	72.65	5812.08
Biomass	4.63[1]	18.25	1460.12
Gas	2.82[1]	11.12	889.32
Nuclear	0.07[1]	0.28	22.08
Wind	0.04[2]	0.16	12.61
Hydropower	0.02[2]	0.08	6.31
Solar	0.02[2]	0.08	6.31

Notes: 1. Data from [15]
2. Data from [16]

A direct hazard limit for commercial fusion is defined based on the number of serious injuries or deaths associated with the lifetime operation of a commercial fusion facility. A lifetime averaged direct consequence hazard limit is selected because it allows for the combination of chronic and acute hazard consequences that may affect the public. This allows a balanced evaluation approach between facilities such as a coal power plants which have severe chronic hazard consequences and minimal acute hazard consequences and nuclear fission power plants that have minimal chronic hazard consequences but severe acute hazard consequences.

A direct hazard consequence based hazard limit for commercial fusion facilities is developed based on a comparison of the direct hazard consequences for other electrical generation sources. Table 4.1 provides the combined observed acute and chronic fatality relate per generated terawatt-hour of electrical energy. These fatality rates can be converted into a direct hazard consequence by assuming the energy output of a facility. Equivalent direct hazard consequences are calculated for each technology assuming a facility with a net electrical output of 500 MW and a capacity factor of 90%. These consequences are calculated on an annual average basis and for an 80 year operational average basis.

Review of the average direct consequences in Table 4.1 show that the production of electricity from combustion sources (coal, oil, biomass, and gas) result in significantly higher average fatalities, largely associated with the chronic impacts of air emissions. The average direct consequences of non-emitting sources of electricity (nuclear, wind, hydropower, and solar) are one to two order of magnitude lower. A direct hazard consequence based limit between these two sets of socially accepted electricity generation sources would ensure that commercial fusion facilities are a significant safety improvement from existing electrical energy sources but do not overly constrain their design and operation.

In this work, a direct hazard consequence limit of 0.3 fatalities per TWh of electrical output is selected as the hazard limit for commercial fusion facilities. This value is arbitrary but is selected to represent an approximately 90% reduction as compared with natural gas power plants when reviewing the direct human health effects associated with production of electricity on per TWh basis. Determining this value in real regulatory applications is extremely difficult for many of the technical and societal reasons previously discussed.

Table 4.2 summarizes the related direct hazard limits for commercial fusion facility with a net electrical output of 500 MW and a capacity factor of 90%. The direct hazard limit for commercial fusion means that the expect public fatalities from chronic and acute operation must be less than 1.18 fatalities per year and less than 94.61 fatalities over the lifetime of the facility operation. In this manner, the maximum direct consequence associated with the facility (excess fatalities) is directly correlated with the benefit associated with the facility (electrical energy production).

Table 4.2. Direct consequences limit for commercial fusion technology

		500 MWe facility, 90% capacity factor	
Power Source	Maximum average fatalities per TWh	Annual average fatalities	80-year average fatalities
Fusion	0.30	1.18	94.61

An indirect hazard consequence limit can be developed for commercial fusion facilities by including assumptions regarding the population exposed to a hazard. The population can be roughly estimated based an area of concern around a facility and the average population density of the area. This process is incredibly site specific, but general assumptions are required for the development of an indirect hazard consequence limit.

In this work, the area of concern around a commercial fusion facility is assumed to a ten-mile radius zone around the facility. A ten-mile radius area was selected based on prior policy decisions by the NRC on the area of concern around commercial fission power plants for "population generally considered subject to significant risk" [9]. It is expected that the hazards of a commercial fusion facility will bound a commercial fission facility, so consideration of the population in the ten-mile surrounding area is likely conservative.

The population density in this area is assumed based on the average population density within the state of Massachusetts. The average population density of Massachusetts is estimated at 860 people per square mile [17]. This population density assumption estimate for a commercial fusion power plant is high because of the relatively high population density of Massachusetts nationally (third highest among US states) and the tendency to site large industrial facilities in less populated areas. It is expected that this population density, so consideration of the population in the ten-mile surrounding area is likely conservative.

This averaged area and population density results in an averaged population of 270,000 people surrounding the plant. Table 4.3 provides the populations within 10 miles of various proposed, research, and operating commercial nuclear facilities [18]. An averaged population of 270,000 is smaller than those surrounding academic research reactors but is larger than the population surrounding proposed or operating commercial facilities.

Table 4.3. Direct consequences limit for commercial fusion technology

Facility Site	10 Mile Radius Population
Seabrook Nuclear Power Plant	127,635
Devens, MA – Proposed Fusion Prototype Site	200,580
Commercial Fusion Average	270,000
TFTR Research Fusion Reactor	390,490
MIT Research Fission Reactor	1,796,273

The average population around the facility is used to develop the indirect hazard consequence limit for commercial fusion facility. The number of excess fatalities around the facility must not exceed an average if 1.18 fatalities per year (direct consequence limit), so the population averaged increase on a yearly or lifetime basis:

$$\frac{1.18\, fatality/year}{270{,}000\, people} = 4.38 \times 10^{-6} \frac{fatality}{person - year}$$

$$\frac{94.61 fatality/facility}{270{,}000\, people} = \frac{35.04\, fatalities}{100{,}000\, person}$$

These averaged fatality rates are the indirect hazard consequence limit for commercial fusion facility. Maintaining facility operations at or below the annual average rate will result in compliance with the direct hazard consequence limit among the general population around the facility. The varying populations for real facilities in Table 4.2 highlights how different assumed populations could result in an order of magnitude or larger change in the indirect consequence based hazard limits for a facility. The larger the assumed population, the lower the indirect hazard consequence based limit must be to meet the correlating direct hazard limit.

This indirect hazard consequence can be compared with the indirect hazard consequence limits for other industries. The NRC Quantitative Heath Objectives (QHOs) state that the excess annual risk to an average annual member of the public should not exceed one-tenth of one percent (0.1 percent) of the risk of other accidental causes [19]. The US Death rate due to accidents was 49.4 per 100,000 in 2018 [11] so the corresponding acceptability accident rate would be 1000 times smaller or 4.94×10^{-7} fatalities per person-year. Thus, this indirect hazard consequence limit is approximately an order of magnitude higher than that currently used by the NRC QHOs.

The higher indirect hazard limit for commercial fusion is largely expected given the higher direct hazard limit selected in this work for fusion power as compared with the operational safety record of fission power (0.30 fatalities per TWh limit for fusion versus 0.07 fatalities per TWh observed for fission power).

These two hazard consequence based hazard limits are a foundation for all other hierarchical hazard limits. These assumed hazard limits will be used to derive higher order hazard limits based on the correlation assumptions for each limit.

4.4 Dose or total exposure based hazard limits

Dose or total exposure based hazard limits are the second simplest of regulation of technology or activity for public health and safety. These limits set a maximum amount of exposure to a hazard, normally based on the known or predicted exposure that would result in consequence. This type of limit requires use of a regulatory assumption that connects specific levels of dose or exposure (e.g., exposure to lead as measured via blood concentration) to a socially unacceptable consequence (e.g., damage to brain and central nervous system) [20]. In this way, the dose or total exposure based hazard limits could be related to direct or indirect consequence hazard limits.

An example of a dose based hazard limit is given by the U.S. Department of Energy's *Occupational Radiation Protection Limits* (Title 10 of the Code of Federal Regulation, Part 835):

> §835.204 Planned special exposures.
> (a) Except for planned special exposures conducted consistent with §835.204 and emergency exposures authorized in accordance with §835.1302, the occupational dose received by general employees shall be controlled such that the following limits are not exceeded in a year:
>
> (1) A total effective dose of 5 rems (0.05 Sv);
> (2) The sum of the equivalent dose to the whole body for external exposures and the committed equivalent dose to any organ or tissue other than the skin or the lens of the eye of 50 rems (0.5 Sv);
> (3) An equivalent dose to the lens of the eye of 15 rems (0.15 Sv); and
> (4) The sum of the equivalent dose to the skin or to any extremity for external exposures and the committed equivalent dose to the skin or to any extremity of 50 rems (0.5 Sv) [21]

This limit implicitly links a dose (exposure to a dose of ionizing radiation) to a hazard consequence (increases in cancer incidence and other health affects due to chronic exposure to radiation).

An example of a total exposure based hazard limit is the OSHA limit on worker blood lead concentration levels that trigger medical removal (Title 1910 of the Code of Federal Regulation, Part 1025 Appendix C). Appendix C states that workers are to be removed when [22]:

- A confirmed blood lead level of 60 ug/100 g or greater is obtained, or
- A six month average blood level of equals or exceeds 50 ug/100 g is observed

This limit implicitly correlates a total exposure (based on the measured blood lead levels) to a hazard consequence (damage to neurological, hematopoietic, and reproductive systems).

Inherent assumptions and uncertainty

Dose or total exposure based hazard limits has require significant regulatory assumptions that allow for correlation between doses or total exposures to societally significant consequence. These assumptions may carry significant uncertainty that underlie the importance and effectiveness of these limits.

These types of limit are always based on two major sets of assumptions: scientific correlation assumptions and societal policy assumptions. The main scientific assumption is about the relationship between the exposure and the socially unacceptable consequence. While the correlation between exposure and consequences is most often based on scientific data, many correlations are subject inherent uncertainties related to data collection, dose measurement, or impact of other contributing factors that can skew correlation. For this reason, it can be considered a policy assumption. These dose-consequence relationships can vary in both time and consequence severity. In time, this can include both acute or one-time exposures as well as chronic exposures. Additionally, the rate of exposure can affect consequences for certain hazards. In severity, the assumed dose-consequence relationship for a hazard plays a significant role. The assumed slope of the relationship and the existence of thresholds or cliff-edge effects can have significant impacts on selected concentration exposure based hazard. This relationship must be assumed for dose or total exposure based hazard limits.

In general, these correlations have highest certainty for well-studied hazards at high doses and lowest certainty for new or under-studied hazards at low doses. As a high certainty example, the biologic consequences of extremely high blood concentrations of lead are well understood and the correlation between high blood levels and acute health effects is well characterized (citation needed). As a low certainty example, the long-term consequences of acute exposures to very low levels of ionizing radiation are not well understood, and the correlation low dose radiation and health effects is a subject of robust scientific (and policy) debate (citation needed). For new hazards or potential hazards exposures at previously unseen levels, there is likely to be substantial uncertainty in the scientific assumptions underlying exposure or dose and consequences. Use of bounding or best-estimate models may likely be required if more precise scientific correlation information is not available.

The main policy assumption relates to the level of societally acceptable consequences for a hazard. For dose or total exposure based hazard limits, this consequence level may not always be explicitly stated but still lies at the heart of the limit. Many of the challenges associated with the creation of direct or indirect consequence based hazard limits reemerge when attempting to set the societally acceptable consequences. Determining the socially acceptable consequence of any activity still requires consideration of a wide variety of stakeholders to evaluate a hazard collectively, balance competing or conflicting priorities, and arrive at a compromise limit. This assumption can complicate the initial creation of limits due to debate over the regulatory limit and leave the limit vulnerable to social, legislative, or legal challenges to limit based on underlying hazard consequence limit assumptions.

With these two assumptions, dose or total exposure based hazard limits may be derived. In most regulatory applications, the policy assumption of societally acceptable consequence will drive the hazard limit. Once an acceptable level of consequence is determined, scientific correlation of exposure to consequence will be used to derive the hazard limit. In some cases, the societally acceptable consequence level cannot be achieved due to technological limitations (e.g., it is not possible using existing technology to meet the limit) or economic limitations (e.g., it is not possible to meet the limit using existing technology in an economically viable manner). When these limitations occur, society may consider the benefits and drawbacks of the technology to determine if the activity should be allowed, and assess the limitations that should be put on the activity. [Good example here?]

One major disadvantage of dose or total exposure based limits is the scientific correlations underlying the exposure-consequence relationship. Dose or total exposure based limits are largely surrogate limits that couple a measurable or calculable quantity of exposure to a negative consequence. This correlation between limit and consequence requires scientific models with varying types of assumptions. These assumptions may include characteristics like expected consequences of concern related to exposure, existence (and level) of a threshold dose or exposure at which different consequences occur, and the observed or predicted relationship between dose and consequences (i.e., dose response curve).

For some hazards, these assumptions are fairly well characterized, and current scientific models are accepted by most as adequate. For other hazards, however, these assumptions can be the subject to significant scientific debate. The dose-response curve for ionizing radiation is heavily debated in the scientific community, especially at very low levels of total exposure, due the limited scientific data on human low dose response and the long latency between exposure and observed consequences (e.g., excess cancers). Dose response may also vary significantly for different groups of the population based on individual sensitivities to specific hazards (e.g., sensitivity to aerosolized beryllium).

For new hazards or exposure to hazards previously unrecognized quantities, this exposure-consequence relationship may be unknown. Absent adequate human data on exposure-consequence relationships, comparison to similar hazards, use of theoretical consequence or underlying physiological effect models, use of animal test data, or extrapolation of models may be used. These methods may introduce significant uncertainties into dose or total exposure based limits. Given limited data sets and the potential latency between exposure and observed consequences, these uncertainties may result in dose relationships that either over-predict or under-predict overall consequences, violating the social assumptions about the socially acceptable level of consequence for a hazard.

While conservative dose relationships may be used, (e.g., erring towards minimized consequences) this may be result in overly conservative limits that render new technologies infeasible. Conversely, if there is a significant latency in observed consequences or if initial dose relationships are created based on limited populations (e.g., size, group characteristics, or observation for only specific consequences), these limits may actually under-predict consequences and result in socially unacceptable exposures.

For specific hazards, the uncertainties, assumptions, and scientific questions about the dose consequence relationship can significantly complicate the use of dose or total exposure based limits. Debate about these scientific correlation assumptions can slow or complicate the limit creation process and introduce social or political challenges.

Effects on regulatory evaluations

Dose or total exposure based regulatory limits are used widely for regulatory evaluations. Use of these hazard limits creates regulatory system where initial creation balances regulatory effort between initial limit creation and specific activity justification and analysis.

Use of dose or total exposure based regulatory limits requires initial work by a regulator to establish limits that aligns with societal expectations. This requires determination of the socially acceptable consequences for a hazard, and then assessment of dose or total exposure limits that correspond to those consequences. Determination of the corresponding dose or total exposure limits requires selection of the dose-consequence relationships and inclusion of "safety factors" to account for uncertainty in the models or consequences. This limit process can be controversial for hazards, as different stakeholders may disagree on the dose-consequence models used, as well as the socially acceptability of different consequences. For well-characterized hazards, limit recommendations from professional societies, non-governmental organizations, or other regulators may be used as the basis for selected limits. For other hazards, regulatory limits for comparable hazards or industries may be used to create new limits

Once a dose or total exposure limit has been determined, regulatory evaluations to demonstrate compliance with the hazard limits can provide flexibility in design and analysis but may require effort to prepare and review. Depending on the level of analytic detail needed by the applicant to meet the hazard limits or supplemental regulatory requirements, evaluations could use bounding inputs or best-estimate inputs, the latter of which would require more effort to gather, prepare, and review. While this limit does not require an applicant to submit and justify dose-consequence relationships, it requires them to adhere to the set regulatory assumptions even if other models would be more favorable. Calculation of dose or total exposure limits could vary from very simple to very complex (and costly) to prepare and review depending on the level of detail chosen by an applicant.

Dose or total exposure based hazard limits are also fairly compatible with a flexible exemption based regulatory process. Exemptions could be sought based on factors such as use of an alternative dose-consequence relationship or changes to the set hazard limits. The main challenges of exemptions with dose or total exposure based limit are the technical challenge associated with justification of different regulatory assumptions and the social challenges associated with justification of greater consequences. The main advantages of exemptions process for dose or total exposure limits over lower hierarchical hazard limits is that the consequence is abstracted (e.g., no explicit description of consequence), so the social justification may be more readily obtained.

Dose or total exposure based hazard limits have also been demonstrated as an effective backstop regulatory evaluation metric because the explicit regulatory assumptions (dose-consequence relationship) can be used to compare limits as indirect or direct consequences.

Dose or total exposure based hazard limits are used as the primary hazard limit in industries where hazards consequences can be collapsed into a single limit. For example, use of ionizing radiation dose limits for nuclear activities allows for the holistic evaluation of the cumulative effects of multiple separate radionuclide hazards. In certain regulatory frameworks, the flexibility in how an applicant proposes and evaluates safety could allow for innovation in design and analysis. Similar to lower hierarchical hazard limits, this flexibility can increase the effort required to prepare and review these evaluations. This hazard limit can balance regulatory effort between initial limit creation and specific activity justification and regulatory analysis.

Effects on regulatory enforcement and operations

Use of dose or total exposure based limits has several distinct advantages related to regulatory enforcement and operational regulation over the lower hierarchical consequence-based hazard limits. The main advantages of this limit relate to the potential to assess hazard effects and prevent significant consequences, and the ability to more easily monitor and assess compliance with dose limits.

The first advantage is that total exposure based limits can be set in a manner that triggers intervention or reassessment of an activity before a consequence occurs. For example, in the annual worker radiation exposure limit example (10 CFR Part 835) the whole body total effective dose limit is set at 5 rem. An acute exposure to 5 rem of ionizing radiation is sufficiently low that it will not result in any detectable acute health effects – an acute whole body dose of 25 rem to 50 rem is needed to product medically detectable symptoms of acute radiation syndrome. The acute dose of 5 rem would increase the individual's lifetime risk of cancer, but the risk is quite small – increasing the average lifetime cancer incidence from 41.91% to 42.34% [23]. Use of sufficiently low dose based limit allows workers and regulators to assess and mitigate hazards before a societally unacceptable consequence (e.g., acute radiation poisoning) occurs. This depends heavily on the hazard, the limit set, and any potential remediation that can occur after a dose or exposure occurs. Exposures to ionizing radiation cannot be effectively reversed, so treatment focuses on mitigation of symptoms and avoiding medical complications. For exposures to certain chemical agents, treatment can occur to remove or neutralize the agent, thereby preventing further biologic consequences. This is societally preferable to a consequence limit where the indication of limit exceedance would be the actual consequence (e.g., excess fatalities above the set limit).

The second advantage of dose or total exposure based limits is that they can be more easily monitored than indirect consequence based limits. For indirect consequence limits (e.g., increased probability of developing cancer or dying), demonstrating compliance with the limit can be difficult due to the challenge of assessing statistical significance for low probability events. Use of dose or total exposure based limits allow for the monitoring or testing of potentially exposed individuals, particularly if the exposure is expected. This can help simplify the process of assessing compliance with regulatory limits. For certain types of doses or exposures, however, real-time monitoring or sensing may not be feasible so the time delay in taking and analyzing dose or exposure data must be considered when setting limits.

The main operational disadvantages dose or total exposure based limits relate to isolation of specific hazards and contributions from multiple sources and the need to monitor and test to assess compliance.

The first disadvantage of dose or total exposure based limits is that regulatory application of the limit requires either the ability for separate measurement of the hazard of interest from background levels or other activities, or acceptance of all hazards into one limit. For some hazards (e.g., exposure to aerosolized beryllium), a single regulated activity may be the only possible point of exposure. In these cases, measurement of a dose or total exposure correlates to the operation and safety of the regulated activity.

For many hazards however (e.g., exposure of ionizing radiation), multiple naturally occurring and man-made hazards may exist. For these cases, measurement of an individual's dose or total exposure may include contributions from both the regulated activity as well other sources and may not correlate to the operation and safety of the regulated activity if the other contributions are significant. It may be possible to isolate measurement of some dose or total exposures if the sources are relatively localized or known. For example, worker use of an ionizing radiation dosimeter while at a nuclear facility allows for the measurement of worker doses from to the regulated activities due to the controlled nature of the facility and ability to account for natural occurring background radiation. If a member of the public who lived near a nuclear facility used a similar dosimeter continuously to measure dose, it may be difficult to correlate measurements to nuclear facility operation and safety. Factors such as exposure to variable naturally occurring radiation sources (e.g., home radon levels, elevation), different common manmade radiation sources (e.g., medical procedures, aircraft flights), as well as other nearby nuclear facilities could result in higher than expected doses that cannot be correlated to an individual nuclear facility operation and safety. For acute exposures that are significantly larger than background or other expected routine exposures, the contribution from regulated activities may be clear but it may be difficult to adequately determine separate dose contributions for low-level releases that are similar to other hazards.

The second major disadvantage of dose or total exposure based limits is the need to monitor and test to assess compliance. Total dose or exposure to some hazards (e.g., magnetic fields) cannot be measured biologically, but can be measured and recorded using standard instrumentation. Exposure to other hazards (e.g., lead) can be monitored using established scientific tests for determining absorbed chemical levels but may require invasive medical procedures such as a blood draw. The effects of other common industrial hazards (e.g., explosion) may not be easily measured and instead may use surrogate characteristics that can be more easily measured but relate directly to the consequences of the hazard (e.g., blast pressure, fire temperature, thermal radiation flux).

For certain populations (e.g., workers), monitoring and testing can be conducted as part of the standard industrial health and safety processes, but this monitoring comes additional cost and complexity. Accurate measurement of all exposures and robust record keeping are required to ensure that regulatory limits are met and that accountability for exposures is maintained. For members of the public or environmental concerns, monitoring or testing may be more complicated due to more limited control over behavior and the potentially larger geographic space monitored. Deployment, calibration, and maintenance of large numbers of instruments may be logistically and financially challenging. Requirements for additional medical tests for members of the public related to monitoring and testing may affect public support for the technology both due to the inconvenience and intrusive nature of the testing.

Monitoring of all public places and populations that may be potentially exposed may be infeasible, so a hypothetical exposed individual or location may be used for calculation analyses. This representative “person” may not actually exist but is used as a stand in for regulatory analysis and bounds the maximum possible dose or total exposure of all other populations. While use of this maximum exposed offsite individual (MOI) can be useful for regulatory analyses, it is impossible to use for actual monitoring and testing purposes. Additional monitoring and testing of calculation assumptions (e.g., hazard concentrations or releases) used for the MOI must be conducted to ensure that the dose or total exposure limit is met.

Additionally, physical and temporal limits of dose monitoring and testing must be considered. Physically, monitoring and testing may take place on an individual basis, a random sampling of a population, fixed locations, or varying locations. Temporally, monitoring and testing may be one-time, intermittent, routine, or continuous. The exact type of physical and temporal monitoring required will depend on factors including the characteristics of the specific hazard and consequences, the exposure or release characteristics, and the regulatory limits with allowable uncertainties. Temporally continuous monitoring of all physical locations and populations may be technically or financially infeasible, so use of certain dose or total exposure based limits may not be possible. This can significantly complicate the use of dose or total exposure based limits.

Overall, dose or total exposure based limits are an effective method for operational regulation of activities. These limits may be more effective for worker or fixed environmental populations as compared with public or general environmental areas due to the monitoring and testing requirements associated with verifying dose or total exposure based limits.

4.4.1 Creating dose or total exposure hazard limit for commercial fusion facilities

Dose or total exposure based limits are developed on a hazard-by-hazard basis due to the different correlations between exposure and indirect or direct hazard consequences. The evaluation of commercial fusion facilities hazards is limited to radiological material hazards in this work (Chapter 3). Therefore, dose or total exposure hazard limits are only developed in this section are limited to radiological hazards. Dose or total exposure hazard limits for the other hazards of highest regulatory significance (hazardous materials, explosive materials, and direct radiation exposures) are not developed in this work but would be required to support commercial fusion facility regulation. These limits would likely be based on existing guidance for commercial fission and other industrial facilities.

Two different approaches may be used to develop the dose or total exposure based limits for radiological hazards for commercial fusion facility. The first is definition of a limit consistent with the lower level hierarchical hazard limit (indirect and direct consequence based hazard limits) using dose-consequence model relationships. The second is a consensus-based approach where the limit is defined using best practices and limits from other regulatory organizations and professional societies. In this work, the dose and total exposure based limits defined are the radiation dose equivalents. This dose equivalent includes all factors that characterize the biological effects of ionizing radiation exposure.

The first approach uses the indirect and direct consequence based hazard limits for commercial fusion developed in Section 4.3.3 and dose-consequence model relationships to define a dose or total exposure based limits. The indirect consequence based hazard limit developed in Section 4.3.3 are:

- annualized indirect consequence of $4.38 \times 10^{-6} \frac{fatality}{person-year}$
- facility lifetime indirect consequence of $3.50 \times 10^{-4} \frac{fatality}{person}$.

These indirect consequence limits are converted to fatality rates per 100,000 people:

- annualized indirect consequence of $0.44 \frac{fatality}{100{,}000\ persons}$ and
- facility lifetime indirect consequence of $35 \frac{fatality}{100{,}000\ persons}$

These dose-consequence model relationship for exposures to ionization radiation is extremely complex and is not fully described by existing scientific models. Factors including total exposure, exposure rate, exposure duration, exposure pathway, and specific radionuclides are all known to affect the observed health effects of exposure to ionizing radiation [24]. Quantifying and separating the health effects from small specific exposures to ionizing radiation from the health effects from other ionizing radiation sources, environmental, and genetic factors is challenging due to the stochastic nature of ionizing radiation damage.

The indirect and direct consequence based hazard limits for commercial fusion developed in this work were focused on excess off-site fatalities associated with facility operation. Therefore, the dose-consequence model relationships reviewed in this work focus on the relationship between dose and fatalities. It is important to note that other types of dose-consequence models could be selected if different types of indirect and direct consequence based hazard limits were defined. General health effects, excess cancers, or financial costs could all be utilized as indirect and direct consequence based hazard limits. Selection of these different types of limits would require different dose-consequence model relationships to calculate dose or total exposure based limits.

The dose-consequence model relationship for exposures to ionization radiation selected for this work is the linear no-threshold (LNT) dose model. This model is largely based on high-dose, acute exposure epidemiological data but is considered the most appropriate model for regulatory assessments of ionizing radiation health effects [23]. Validity of the LNT model for low-dose and low-dose rate exposures is unclear based on limited data and high uncertainties but is generally considered conservatively bounding. Therefore, the LNT model is the dose-consequence model selected for applicability at all dose levels in this work.

The following dose-consequence model relationship for excess fatalities from acute and continuous exposure to ionizing radiation are utilized based on a review of existing guidance on radiation health effects [23][24]:

- 418 excess cancer fatalities per 100,000 people for annual exposure to 1 mSv per year during lifetime
- 5.7 excess cancer fatalities per 100,000 people for acute exposure to 1 mSv

Using these dose-consequence model relationships, it is possible to calculate equivalent chronic and acute exposure limits for the commercial fusion facilities that meet the indirect consequence limits developed in Section 4.3.3. The annual acute exposure dose limit is:

$$\frac{Excess\ Fatalities\ Limit}{Dose - Consequence\ Relationship} = \frac{\frac{0.44\, fatality}{100{,}000\, persons}}{\frac{5.7\, fatality}{100{,}000\, persons - 1\, mSv}} = 0.077\, mSv$$

The lifetime acute and chronic exposure dose limits are:

$$\frac{Excess\ Fatalities\ Limit}{Chronic\ Dose - Consequence\ Model} = \frac{\frac{35\, fatality}{100{,}000\, persons}}{\frac{418\, fatality}{100{,}000\, persons - 1\, mSv}} = 0.084\, mSv$$

$$\frac{Excess\ Fatalities\ Limit}{Actue\ Dose - Consequence\ Model} = \frac{\frac{35\, fatality}{100{,}000\, persons}}{\frac{5.7\, fatality}{100{,}000\, persons - 1\, mSv}} = 6.14\, mSv$$

Thus, exposure dose limits for the facility are 0.077 or 0.084 mSv for exposures that may happen on an annual basis (acute and chronic respectively) throughout the lifetime of the facility and 6.14 mSv for acute exposures that occur once during the lifetime of the facility. Note carefully that this formulation could result in a total effective indirect consequence double the intended limit if exposures at both the annual and lifetime levels occurred. Halving each of these limits would result in a conservative dose exposure limit but may be overly conservative if the principle of “As Low As Reasonably Achievable” (ALARA) is applied to exposures. Using ALARA, activities seek to reasonably minimize the exposures and not simply meet the regulatory limit. As a result, adherence to the ALARA principle would likely result in total exposures that meet the indirect consequence limit. The final two exposure limits using the hierarchical hazard method for commercial fusion facilities are rounded 0.08 mSv for routine or annual exposures and 6 mSv for one-time acute exposures.

The second approach is a consensus-based approach where the limit is defined using best practices and limits from other regulatory organizations and professional societies. This relies on the understanding the technical rational and underlying analytic assumptions of regulators and experts responsible for developing and setting dose and total exposure limits. The dose limits recommended by the International Committee on Radiation Protection (ICRP) are generally considered independent and reliable recommendations, and are used as a benchmark for regulatory limits set by the Nuclear Regulatory

Commission [25]. Dose guidance compiled from several ICRP technical recommendations are summarized in Table 4.4. Technical annexes published with the ICRP technical recommendations provide insights on the scientific, epidemiological, and policy basis for the dose guidance in Table 4.4.

Table 4.4. ICRP Dose Exposure Guidance [24], [26]

Limit Type	Effective Dose	
	(mSv)	(rem)
Intervention / Mitigation Should Be Performed	100	10
Intervention Threshold	20	2
Intervention / Mitigation May Be Needed	10	1
Practical Public Dose Limit	1	0.1
Dose Limit On-going Exposure	0.1	0.01
Dose Limit Exemption Threshold	0.01	0.001

Review of the ICRP dose limit guidance in Table 4.4 reveal two general types of limits – upper dose limits for acute exposure and intervention, and lower dose limits for limiting chronic exposure. The upper dose limits relate to the need for intervention and mitigation of acute exposures that present an undue risk to members of the public. These doses are all below the threshold of statistically and epidemiologically observed ionizing radiation health effects at 100 mSv but represent the current best practices on avoiding unnecessary increases in risk [23]. The lower dose limits relate to the need to limit on-going exposures that may, over a lifetime of repeated or continuous exposure, lead to statistically significant health effects. These lower doses are a fraction of the naturally occurring background radiation (typically 3 mSv or 0.3 rem) but an abundance of caution suggest that the exposures may be significant over time. There is limited epidemiological and mechanistic scientific evidence for these extremely low doses health effects but use of limits consist with the LNT model are generally considered conservative.

The ICRP dose guidance can be used to benchmark dose limits for commercial fusion facilities. For public exposures that could be routinely expected, a dose limit of 1 mSv would be appropriate with a goal of achieving observed doses of below 0.1 mSv for actual chronic exposures. For larger acute exposures, a dose limits of 10 mSv would enable exposure without the need for additional intervention or dose mitigation such as evacuation, shelter-in-place, or other activity restrictions. Doses between 20 mSv and 100 mSv would warrant intervention and mitigation due to the increased likelihood of health effects from acute exposures.

Review of the two different approaches (hierarchical development and review of consensus standards) used to develop the dose or total exposure based limits for radiological hazards for commercial fusion facility shows general alignment between the developed dose limits. Table 4.5 provides both sets of dose limits. The dose limits derived hierarchically based on the indirect consequence limits are lower than the dose limits developed based on consensus recommendations. This difference can be traced, in part, back to the population assumptions used in the calculation of the direct consequence limits. Changing the assumed population density from that of Massachusetts (860 persons per square mile), the third highest state population density, to the state with the median population density (Washington with a population density of 105 persons per square mile) results in indirect hazard consequences limits that are eight times higher.

Table 4.5. Dose or Total Exposure Limits for Commercial Fusion

Exposure Limit Type	Hierarchical Derived Dose Limits (mSv) [rem]	Consensus Derived Dose Limits (mSv) [rem]
Acute Dose Exposure	6 [0.6]	10 [1]
Maximum Chronic Exposure	0.08 [0.008]	1 [0.1]
Routine Chronic Exposure		0.1 [0.01]

This change in the exposed population assumption has a significant impact on the hierarchical derived dose. This observation also reveals a potential limitation of the hierarchical derived dose limit method where doses limits can vary significantly based on population assumptions and potentially lead to different dose limits (and subsequent risks) based on the population and location. This relates directly to concerns related to equitable distribution of risk previously discussed for direct hazard consequences. This discrepancy also helps illustrate the importance of using uniform assumptions and methods to calculate acceptable risk and consequences, and prevent inequitable distribution of hazards and risks. While further discussion is important to the development of appropriate hazard consequence limits, the implications are largely outside of the scope of this work and are not considered further.

In this work, the 6 mSv and 0.08 mSv derived dose limits will be used as the basis for development of higher order hierarchical hazard limits. This limits is comparable to the consensus based limits and are consistent with existing regulatory guidance, allowing for consistent comparison with higher order hazards limits.

4.5 Concentration exposure based hazard limits

Concentration exposure based hazard limits are the most common limit used for the regulation of technology or activity that impact public health and safety. These limits or control exposure to substances or materials to specific concentrations for different specified conditions. This type of limit requires use of a regulatory assumption that correlates acute or chronic exposure or ingestion, inhalation, or deposition of material at specific concentrations to a socially unacceptable consequence (e.g., human health effects or negative environmental effects).

Concentration exposure based hazard limits relate to the specific concentration of a hazardous material a worker, member of the public, or the environmental may be exposed to. A workplace example of a concentration exposure hazard limit is given by the U.S.

Occupational Health and Safety Administration's regulation on *Toxic and Hazardous Substances* (Title 29 of the Code of Federal Regulation, Part 1910):

> §1910.1024 Beryllium
>
> (c) Permissible Exposure Limits (PELs)—
>
> (1) Time-weighted average (TWA) PEL. The employer must ensure that no employee is exposed to an airborne concentration of beryllium in excess of 0.2 μg/m^3 calculated as an 8-hour TWA. (2) Short-term exposure limit (STEL). The employer must ensure that no employee is exposed to an airborne concentration of beryllium in excess of 2.0 μg/m^3 as determined over a sampling period of 15 minutes.

This limit implicitly links concentration exposure (continuous inhalation of beryllium at concentrations greater than 0.2 μg/m^3) to a hazard consequence (long term socially unacceptable potential for the development of chronic beryllium disease given constant exposure) [27].

A public example of a concentration exposure hazard limit is given by the U.S. Environmental Protection Agency's regulation on *National Primary Drinking Water Regulation* (Title 40 of the Code of Federal Regulation, Part 141). Title 40 CFR Part 141.62 sets the maximum contaminant level for beryllium in drinking water at 0.004 mg/L (0.004 PPM) [28]. The "Mandatory health effects language" provided in Title 40 CFR Part 141.32 for beryllium provides the rational for the regulatory limit [29]:

> §141.32(e)(54)
>
> (54) Beryllium. The United States Environmental Protection Agency (EPA) sets drinking water standards and has determined that beryllium is a health concern at certain levels of exposure… Beryllium compounds have been associated with damage to the bones and lungs and induction of cancer in laboratory animals such as rats and mice when the animals are exposed at high levels over their lifetimes. There is limited evidence to suggest that beryllium may pose a cancer risk via drinking water exposure. Therefore, EPA based the health assessment on noncancer effects with an extra uncertainty factor to account for possible carcinogenicity. Chemicals that cause cancer in laboratory animals also may increase the risk of cancer in humans who are exposed over long periods of time. EPA has set the drinking water standard for beryllium at 0.004 part per million (ppm) to protect against the risk of these adverse health effects. Drinking water which meets the EPA standard is associated with little to none of this risk and should be considered safe with respect to beryllium.

This describes the regulatory rational correlating the exposure concentration (continued ingestion of water contaminated with beryllium at concentrations greater than 0.004 ppm) to a hazard consequence (long-term socially unacceptable potential for the development of cancer given constant exposure) [29].

Inherent assumptions and uncertainty

Concentration exposure based hazard limits add two significant regulatory assumptions to assumptions used in the preceding hierarchical limit (dose or total exposure based hazard limits). These additional assumptions allow for correlation between exposures to hazards (at specific concentrations and durations) to lower hierarchical limits (i.e., dose or total exposures levels or societally significant consequences). These assumptions may carry significant uncertainty that add inherent conservatism or limitations to the limits.

The two major embedded regulatory assumptions of concentration exposure based hazard limits are how exposure to a hazard correlates to societally significant consequences (either directly or via dose or total exposures levels) and under what specific conditions the exposure is assumed to occur.

The first regulatory assumption inherent in concentration exposure based hazard limits is how exposure to a hazard can ultimately lead to societally significant consequences. Consequences can occur from a number of pathways including external exposure (e.g., skin exposure) and internal exposure (e.g., ingestion or inhalation). For each hazard, a concentration exposure limit requires an assumption of how the exposure level correlates to the consequence. This assumed correlation is related to the dose-consequence models used in the lower hierarchical hazard limits such as dose or total exposure limits but includes assumptions regarding how exposure translates into dose, total exposure, or consequence. For example, if a worker ingests water contaminated with lead at a specific level, the scientific correlation that estimates the amount of lead absorbed and retained by the body that can cause a total exposure or consequence is a necessary assumption.

The second regulatory assumption inherent in concentration exposure based hazard limits is under what specific conditions the exposure is assumed to occur. Depending on the specific hazard, different consequences may only occur if exposure depending on the time of exposure and level of exposure. In many cases, exposure levels will not be constant with time and could vary significantly. As a result, unless there is an available method to capture and measure total exposure (which could be compared to a dose or total exposure hazard limit) it can be difficult or impossible to quantify the time integrated hazard exposure. Thus, specific condition exposure assumptions are often made for concentration exposure based hazards so that the limit can be justified based on the predicted consequence from the estimated exposure.

For example, when calculating time weighted average (TWA) allowable workplace exposure limits for air contamination, OSHA normally assumes "standard occupational exposure conditions of eight hours a day/five days a week and/or respiratory volume during work activity" [15]. OSHA will then compare the hazards of such exposure for a typical 45 year working career and determine if the resulting consequence exceeds their indirect hazard consequence limit of an excess one in one thousand risk [15]

OSHA also may establish additional concentration based exposure limits that reflect allowable short-term exposures to higher hazard concentrations. Short term exposure limits (STELs) and Ceiling limits can be used to bound short temporary exposures and no greater exposures to certain materials. For example, OSHA regulations on air exposure to benzene limit exposure to 1 ppm in air for the TWA (over an 8 hour averaged work day) but allow exposure of up to 5 ppm in air for the STEL (no greater than a 15 minute period)[30]. Assumptions on the duration and consequence of exposure must vary for different hazards.

These two regulatory assumptions can introduce large uncertainties into the regulatory process. For existing hazards that have been well characterized, selection of an exposure-consequence or exposure-dose relationship may be fairly simple due to scientific consensus on the underlying scientific or epidemiologic models. For new hazards or hazards without significant prior study, there may be substantial uncertainty in this assumption. Limits may be set based on limit data or experience with related hazards, with the understanding that the limits may be revised based on further information. These limits may be overly conservative or under conservative depending on the specific hazard and the data available to inform limits. For both cases, scientific data and limits may be skewed based on the collection sets and may not capture potential consequences on underrepresented or vulnerable groups and populations (e.g., pregnant women, under studied plant and animal species).

Assumptions on specific exposure conditions for hazards are a necessary assumption that invariably introduces uncertainty into the regulatory process. Specific exposure conditions that maximize dose, total exposure, or consequences that bound predicted exposures cases can be selected to help generate a conservative case where no individual exceeds the set societally acceptable limits. This approach can be effective (and is routinely used) but can result in unrealistic condition (e.g., an individual drinks nothing but 2.5 liters per day of water at the maximum allowable hazard exposure concentration). This type of assumption may bound many cases but could be overly conservative and result in an unnecessarily low hazard limit. Conversely, if actual exposure conditions are not bounded by the assumed conditions, the hazard limit may be non-conservative and under-predict maximum consequences. In cases where exposures can be more carefully controlled or monitored, more realistic exposure conditions may be justifiable.

For both assumptions, if the resulting hazard limit is under conservative, societal consequences larger than the societally acceptable limit may occur and could lead to social backlash against the technology. If a hazard limit is overly conservative, the limit could negatively impact the economic or technical viability of the technology. Additionally, excess conservatisms can lead to the misallocation of limited safety resources and reduce overall protection of the public.

Overall, the assumptions inherent in concentration exposure based hazard limits are generally conservative but will introduce uncertainty into the process. While these uncertainties may be significant, these limits can be conservatively selected so that they bound the potential consequences of a hazard to below acceptable levels.

Effects on regulatory evaluations

Concentration exposure based regulatory limits are used widely for regulatory evaluations. Use of these hazard limits creates regulatory system that requires regulatory effort for the creation and justification of regulatory limits, but can reduce the regulatory effort needed to prepare and review regulatory documents for specific activities.

These concentration exposure limits has several distinct advantages related to regulatory enforcement and operational regulation over the lower hierarchical consequence-based hazard limits. The main advantages of this limit relate to the ability to prevent significant chronic consequences and simplify regulatory analyses for applicant. The main disadvantages of the limit are the increased initial regulation preparation effort and increased regulatory assumptions (and decreased regulatory flexibility).

The main advantage of concentration exposure limits is the ability to track and prevent chronic consequences. Setting a sufficiently low concentration exposure limit allows a regulator to reduce doses or total exposures to below threshold levels for consequence (if these exist) or reduce the likelihood of consequence occurrence to socially acceptable levels. While lower level hierarchical hazard limits limit consequence or the total dose/exposure, concentration exposure limits allow for the quantification and control over the hazard itself. Setting a concentration exposure limit allows for the monitoring and control the hazard before harm occurs.

The primary disadvantage of concentration exposure limits are the initial effort required to create these limits. Use of concentration exposure based regulatory limits requires initial work and justification by a regulator to establish limits that aligns with societal expectations. Similar to lower level hierarchical hazard limits (consequence limits, dose/total exposure limits), this process requires determination of the socially acceptable consequences for a hazard, selection of an appropriate dose-consequence model for the hazard, and assessment of dose or total exposure limits that correspond to those consequences (while accounting for uncertainties in scientific assumptions). In addition, the assumptions inherent in concentration exposure based hazard limits require justification of an exposure-dose relationship and a bounding or typical set of exposure conditions.

In addition to the regulatory evaluation work required to prepare dose/total exposure limits, use of a concentration exposure based limit selection of the exposure-dose relationships and inclusion of additional “safety factors” to account for uncertainty in the models or consequences. This limit process can be controversial for hazards, as different stakeholders may disagree on the exposure-dose models used, as well as the acceptability under different exposure conditions. For well-characterized hazards, limit recommendations from professional societies, non-governmental organizations, or other regulators may be used as the basis for selected limits. For other hazards, regulatory limits for comparable hazards or industries may be used to create new limits, with an understanding that limits may be updated based on operational experience or updated evidence of the dose-consequence relationship. This process can require substantial regulatory effort to review scientific evidence, incorporate stakeholder input and feedback, and select an exposure-dose relationship. These initial limits may not always be based on a technical basis (e.g., excessively restrictive to conservatively bound possible consequences) and could be challenging to revise once additional data is available due to the perceived reduction of safety associated with change.

The second major assumption required by regulators when establishing concentration exposure based regulatory limits is the selection of the assumed exposure conditions. As previously discussed, the assumed exposure conditions can lead to the under or over prediction of actual doses based on exposures. Selection of exposure conditions requires understanding of all possible exposure scenarios and what set of conditions lead to a "safe" outcome. This process can also require substantial regulatory effort to review scientific evidence, incorporate stakeholder input and feedback, and select a set of assumed exposure conditions.

Once a regulator has made (and justified) the inherent regulatory assumptions of the acceptable consequences, dose-consequence relationship, exposure-dose relationship, and exposure conditions, a concentration exposure limit can be derived. For established hazards, this process may be simplified to incorporating (by rule or by reference) existing regulatory limits. For new hazards or new use cases, this process could take substantial regulatory resources.

Conversely, one of the major advantages of concentration exposure based limits is the reduced applicant effort associated with concentration exposure based limits. Following creation of an exposure-based regulatory limit, licensees may be asked to show by analysis and or by operation that activities do not exceed the regulatory limits. Depending on factors such as the severity of the consequence and whether the consequence is related to acute or chronic exposure, a regulatory system may require analytic justification that limits are meet or may require one-time, repeated, or evening on-going demonstration that limits are met. In general, movement of regulatory assumptions from the applicant to the regulator will reduce applicant effort due to reduce need to justify analytic assumptions.

This reduction in applicant effort contributes secondary disadvantage of concentration exposure based limits: reduced regulatory flexibility. The larger number of embedded regulatory assumptions contributes may contain a substantial number of conservatisms that applicants may wish to eliminate to increase design flexibility. If assumptions or methods used in an applicants to demonstrate safety, additional analysis and review would be needed to justify and confirm the deviation is allowable. Allowing deviations from concentration exposure regulatory limits can spark claims of regulatory bias and reduce applicant flexibility. Use of exemptions may require more substantial effort that lower level hierarchical hazard limits because the analytic and review infrastructure to review the deviations from the larger number of inherent regulatory assumptions is not normally present.

Concentration exposure based limits are extremely common as the primary hazard limit in industries where control and monitoring of individual hazards is possible and desirable. In certain regulatory frameworks, the flexibility in how an applicant meets the emissions limits could allow for innovation in design and analysis, but concentration exposure based limits reduce overall regulatory flexibility. This reduction in flexibility, however, can substantially the effort required to prepare and review these evaluations depending on the type of justification required (analytic or by demonstration). This hazard limit shifts regulatory effort towards initial limit creation and reduces regulatory burden on specific activity justification and regulatory analysis.

Effects on regulatory enforcement and operations

Use of concentration exposure based limits has several distinct advantages related to regulatory enforcement and operational regulation over the lower hierarchical hazard limits. The main advantages of this limit relate to the potential to monitor and mitigate conditions that could produce consequences, and the ability to more easily monitor and assess compliance with exposure limits. The main disadvantages of concentration exposure based limits are the cost of sufficiently wide monitoring and an inability to monitor for certain hazards.

Concentration exposure based limits have an advantage of enabling the monitoring and mitigation of hazards before consequences occur. Unlike the lower hierarchical consequence or dose/total exposure hazard limits, concentration exposure limits relate to a measurable quantity with limits that can be set to prevent or mitigate consequences. Detecting short periods of hazard limit non-compliance can indicate underlying problems with activities that could result in consequences. In this way, harm need not occur before regulatory action can be taken to stop a potentially harmful activity. One-time, repeated, or continuous monitoring of exposure conditions in fixed or variable areas can allow for varying levels of assurance that the public and the environment are not exposed to unacceptable hazard levels.

These of concentration exposure limits are also easier to monitor than lower hierarchical limits. For many air and water pollutants, standard industrial equipment can be used to test for the presence and concentration of hazards. Unlike dose or total exposure monitoring, these tests are not individual specific and do not require any type of invasive activity – they are based solely on external exposure. Unlike consequence monitoring, population statistics and epidemiological data are not needed to ensure that limits are being met. This process can simplify assurance that an activity complies with regulatory limits.

The main disadvantage of concentration exposure based hazard limits for regulatory enforcement is the need to monitoring equipment or testing to ensure compliance. For hazards and specific situations where exposure is controlled and infrequent (e.g., non-routine use of hazardous material in a controlled workplace environment), one-time testing or monitoring may be useful in ensuring compliance with regulatory limits. For hazards that may vary with time and could extend into larger environments, repeated or continuous monitoring of exposure concentrations in many independent locations or of many samples may be required. The level of monitoring should be commensurate with the hazard, specific exposure conditions, and the level of assurance needed to ensure compliance with limits. Depending on the resulting monitoring requirements, the economic costs associated with ensuring compliance could be very high.

The second major disadvantage of concentration exposure based hazard limits is the difficulty of testing and monitoring some hazards. These difficulties can include both technical difficulties (e.g., no robust or reliable way to test for specific hazards) and economic difficulties (e.g., no cost effective way to test for a specific hazard). These limits may affect the viability of using concentration exposure based hazard limits for specific hazards or creating a high level of assurance of compliance.

Overall, concentration exposure based hazard limits are a very effective method for operational regulation of activities where measurement and monitoring of concentration can be made in real time. These limits are particularly effective for worker or fixed environmental populations as compared with public or general environmental areas due to the monitoring and testing requirements but can be implement in a wide variety of situations. These limits would be less effective for some radiological hazards due to the challenges associated with real time monitoring.

4.5.1 Creating concentration exposure based hazard limit for tritium hazards

Development of concentration exposure based hazard limits for ionizing radiation hazards require detailed knowledge and characterization of specific hazards. Hazard forms, isotopes, exposure pathways, and duration of exposure all have significant impacts on the consequences associated with exposure to a hazard. In this work, the concentration exposure based hazard limits (and higher order hierarchical hazard limits) are only developed for tritium hazards. Development of concentration exposure based hazard limits for a specific radionuclide requires significant evaluation effort.

The purpose of this section is to illustrate the connection between hierarchical hazard limits for commercial fusion and not to provide a comprehensive set of concentration exposure based hazard limits for all commercial fusion hazards. As a result, the development of concentration exposure based hazard limits is limited to tritium radiological hazards in this work. The processes used in this section to develop a concentration exposure based hazard limit for tritium and tritiated materials could be repeated to develop concentration exposure based limits for a wide variety of radiologic hazards.

Similar to the development of dose and total exposure limits for ionizing radiation, two different approaches may be used to develop exposure based hazard limits for tritium hazards for commercial fusion facility. The first is definition of a limit consistent with the lower level hierarchical hazard limit (dose or total exposure) using exposure-dose model relationships and assumptions on exposure conditions. The second is a consensus-based approach where exposure limit is defined using best practices and limits from other regulatory organizations and professional societies.

The first approach uses dose and total exposure hazard limits for commercial fusion developed in Section 4.4.1, exposure-dose model relationships, and assumptions on exposure conditions to define concentration exposure based hazard limits.

The first input, dose and total exposure hazard limits, were developed in Section 4.4.1 and were set 6 mSv for acute doses and 0.08 mSv for chronic / routine acute doses. The higher dose limits developed in Section 4.4.1 based on consensus guidance (10 mSv and 0.1 mSv for acute and chronic exposures, respectively) could also be used to derive exposure limits.

The second input, exposure-dose model relationships, are based on the different potential exposure pathways and biological interactions between radiological hazards and the human body. Potential exposure pathways for radioactive material include [31]:

- Direct radiation exposure
    - Cloud shine
    - Sky shine
    - Ground shine
- Skin deposition
- Inhalation
- Ingestion

Each of these pathways may be a major source of exposure for radioactive material depending on the radionuclide, the form, and the release type. In this work, development of concentration exposure based hazard limits are only developed for tritium hazards. As a result, the direct radiation exposure pathways (cloud shine, sky shine, and ground shine) are no relevant and considered due to negligible external shine radiation dose contribution from the low energy beta radiation decay from tritium. This reduces the concentration exposure based hazard limits of interest in this work to skin deposition, inhalation, and ingestion pathways.

The exposure-dose model relationships are compiled by expert organizations such as the ICRP based on mechanistic and epidemiological scientific data. For radiological materials, the exposure-dose model is given in terms of the effective dose (Sv) per activity of exposure (Bq). This exposure-dose model relationship already accounts for the biological uptake and biological half-life of the radionuclide exposure. The selected exposure-dose model relationships for tritium and tritiated material exposure pathways are [32]:

- Ingestion of oxidized tritium (HTO): $1.8 \times 10^{-11}\ Sv/Bq$
- Inhalation of oxidized tritium (HTO): $1.8 \times 10^{-11}\ Sv/Bq$
- Inhalation of elemental tritium (HT): $1.8 \times 10^{-15}\ Sv/Bq$
- Skin deposition dose assumed to be 50% of inhalation dose

These dose coefficients provide the exposure-dose model relationships required to develop exposure concentration limits.

The third input is the most challenging for development of concentration exposure limits - assumptions on exposure conditions. Specific material exposure limits can be developed based on the dose coefficients and the total dose limits. Table 4.6 provides calculated material exposure limits for ingested and inhaled tritium.

Table 4.6. Material Exposure Limits for Commercial Fusion

Exposure Type	Dose Limit (mSv)	Equivalent Total Exposure to Meet Dose Limit (Bq)		
		HTO Ingestion and Inhalation	HTO Skin Deposition Only	HT Inhalation
Acute	6	3.37E+08	6.74E+08	3.37E+12
Chronic	0.08	4.44E+06	8.89E+06	4.44E+10

The challenge associated with use of material exposure limits based on total dose or exposure limits is that simultaneously meeting all material exposure limits would result in over exposure. Developing concentration based limits, especially for ingestion pathways, requires a detailed understanding of the exposure conditions and individual behaviors. If this understanding is not available, conservative assumptions must be made (e.g., 100% of ingested food and water from tritium contaminated sources). This can result in extremely low concentration exposure limits that may result in unnecessarily conservative restrictions on exposure. Systematic analysis and development of concentration based exposure limits are important to the regulatory evaluation of chronic exposures but are outside the scope of this work. The development of concentration based exposure limits is limited to the inhalation and skin deposition as the immediate acute exposure pathways for tritium and tritiated materials.

Further assumptions regarding exposure conditions allows correlation of the calculated material exposure limits in Table 4.6 with concentration based exposure limits. Material exposure through inhalation can be described using the following time averaged expression:

$$M_{expose} = F_{inhale} R_{rate} C_{expose} T_{expose}$$

Where M_{expose} is the total material exposure (Bq), F_{inhale} is the respirable fraction, R_{rate} is the breathing rate (m^3/s), C_{expose} is the average exposure concentration (Bq/m^3), and T_{expose} is the total time of exposure. Note that a robust form of this expression would be a time integrated exposure. Assumptions may be made about each of the exposure conditions to back calculate acceptable exposure concentrations. Respirable fractions for different materials are available from the ICRP based on mechanistic and epidemiological scientific data, varying depending on the radionuclide and specific form [32]. Breathing rates can vary significantly based on person and activity, but typical breath rates have been measured by different studies and recommended rates are available in regulatory guidance documents. Typical breathing rates are [31]:

- Chronic activity: $2.66 \times 10^{-4}\ m^3/s$
- Light activity: $3.33 \times 10^{-4}\ m^3/s$
- Heavy activity: $3.47 \times 10^{-4}\ m^3/s$

A breathing rate corresponding with light activity ($3.33 \times 10^{-4}\ m^3/s$) is used in this work.

Finally, the time of exposure must be assumed to calculate the limiting exposure concentration. An exposure time of one hour is assumed for acute exposures. This time is intended to reflect both a reasonable duration for a large acute release and the amount of time that may be required to take mitigating actions such as shelter-in-place or evacuation. Note that this assumed time has a significant (linear) impact on the calculated limiting exposure concentration and the selection of this assumption should be carefully considered when calculating these limits.

Using these assumed conditions, the limiting exposure concentration is calculate for acute exposure via inhalation and skin absorption (HTO only) for both oxidized tritium (HTO) and elemental tritium (HT):

- Acute oxidized tritium exposure: $1.88 \times 10^{8}\ Bq/m^{3}$
- Acute elemental tritium exposure: $2.74 \times 10^{12}\ Bq/m^{3}$

These exposure concentrations limits could be used as public exposure limits during acute release, as exposure under the assumed conditions would result in exposures that satisfy the total dose or exposure limits.

The second approach is a consensus-based approach where the exposure concentration based limit is defined using best practices and limits from other regulatory organizations and professional societies. This again relies on the understanding the technical rational and underlying analytic assumptions of regulators and experts responsible for developing and setting exposure concentration limits. In this work, exposure limits are taken from NRC guidance used by the NRC, OSHA, and EPA on worker inhalation doses from tritium and tritiated materials. The workplace exposure limit, assuming 40 hours of acute exposure to oxidized tritium, is [3]:

- Tritium exposure concentration limit: $2 \times 10^{-5}\ \mu Ci/ml$ or $7.4 \times 10^{5}\ Bq/m^{3}$

Acute exposure at this concentration for 40 hours with inhalation and skin absorption would result in a total dose of approximately 1 mSv – equal to the practical dose limit given by the ICRP in Table 4.4 for public or on-going worker exposure. Thus, this limit is consistent with the methodology developed in this work for constraining the total dose exposure. In this work, the derived exposure concentrations limits based on hierarchical hazard limits are used due to their consistency with the expected acute release conditions.

4.6 Release based hazard limits

Release based hazard limits are another common limit used for the regulation of technology or activity that impact public health and safety. These limits or control the release of substances or materials to specific concentrations or total release amounts. This type of limit requires use of a regulatory assumption that correlates releases to a socially unacceptable consequence (e.g., human health effects or negative environmental effects).

The first type of release based hazard limits are release concentration based hazard limits. These limits relate to the specific concentration of a hazardous material that may be released by a regulated activity. An example of a release concentration hazard limit is given by the U.S. Environmental Protection Agency's air program requirements on *Standards of Performance for Stationary Gas Turbines* (Title 40 of the Code of Federal Regulation, Part 60):

> §60.333 Standard for sulfur dioxide
>
> (a) No owner or operator subject to the provisions of this subpart shall cause to be discharged into the atmosphere from any stationary gas turbine any gases which contain sulfur dioxide in excess of 0.015 percent by volume at 15 percent oxygen and on a dry basis.

This limit implicitly links a release concentration (continuous release of sulfur dioxide) to a hazard consequence (socially unacceptable increases in respiratory illnesses as well as causing environmentally damaging acid rain) [33].

The second type of release based hazard limits is total emission release based hazard limits. These limits relate to the amount of hazardous materials that may be released by a regulated activity. These limits may be given on a mass per activity basis (e.g., grams per kilowatt hour of electricity produced) or on a facility total basis (e.g., grams per site).

An example of a release hazard limit given in a mass per activity basis are the U.S. Environmental Protection Agency's air program requirements on *Standards of Performance for Electric Utility Steam Generating Units* (Title 40 of the Code of Federal Regulation, Part 60)[34]:

> § 60.43Da Standards for sulfur dioxide (SO2).
>
> (a) …[N]o owner or operator subject to the provisions of this subpart shall cause to be discharged into the atmosphere from any affected facility which combusts solid fuel or solid-derived fuel… any gases that contain SO2 in excess of:…
>
> (1) 520 ng/J (1.20 lb/MMBtu) heat input and 10 percent of the potential combustion concentration (90 percent reduction);
>
> (2) 30 percent of the potential combustion concentration (70 percent reduction), when emissions are less than 260 ng/J (0.60 lb/MMBtu) heat input;
>
> (3) 180 ng/J (1.4 lb/MWh) gross energy output; or
>
> (4) 65 ng/J (0.15 lb/MMBtu) heat input.

This limit implicitly links the amount of material released per unit of activity (pounds of sulfur dioxide per million BTU of heat input) to a hazard consequence (socially unacceptable increases in respiratory illnesses as well as causing environmentally damaging acid rain) [34]. In this way, the limit connects a potential benefit of an activity (production of electricity) to an acceptable level of hazard (release of sulfur dioxide).

An example of a release hazard limit given in a total mass basis is the U.S. Environmental Protection Agency's requirements on the applicability of Section 112 of the Clean Air Act for regulation of “major sources” of hazardous air pollution. Major sources of air pollution subject to additional permit and regulatory requirements are defined as (Title 40 of the Code of Federal Regulation, Part 63) [1]:

> § 63.2 Definitions.
>
> *Major source* means any stationary source or group of stationary sources located within a contiguous area and under common control that emits or has the potential to emit considering controls, in the aggregate, 10 tons per year or more of any hazardous air pollutant or 25 tons per year or more of any combination of hazardous air pollutants, unless the Administrator establishes a lesser quantity, or in the case of radionuclides, different criteria from those specified in this sentence.

This limit implicitly links the amount of material released per facility (tons of hazardous air pollutant) to a socially unacceptable consequence (significant individual contribution to human or environmental consequences) [1]. This use of a regulatory cutoff helps clarify when a source becomes sufficiently impactful that the contributions of the source should be monitored and regulated.

Inherent assumptions and uncertainty

Release based hazard limits add two significant regulatory assumptions to assumptions used in the preceding hierarchical limit (exposure concentration hazard limits). These additional assumptions allow for correlation between releases of hazards (at specific concentration levels, controlled quantities, or total amounts to lower hierarchical limits (i.e., exposure concentration hazard limits, dose or total exposures levels or societally significant consequences). These assumptions may carry significant uncertainty that add inherent conservatism or limitations to the limits.

The two major embedded regulatory assumptions of release based hazard limits are how a release of a hazard correlates to societally significant consequences (either by total exposure or accumulation) and under what specific conditions the release is assumed to occur.

The first assumption inherent in release based hazard limits is how a release of hazard correlates to a societally significant consequence. The two primary routes of consequences are by exposure (and uptake) or by accumulation of hazardous materials. For each hazard, a release limit requires an assumption of how the release correlates to the lower level hierarchical limits (exposure concentrations, doses, or consequences). This assumed correlation is related to the generalized hazard-effect models used in the lower hierarchical hazard limits but includes more generalized assumptions regarding release, dispersion, and ecological characteristics of hazards. For example, regulatory assumptions on release and dispersion are needed to assess the societal and environmental consequences (or other hazard limits) of the release of 10 tons of sulfur dioxide from a combined cycle natural gas power plant. Use a particular release dispersal models could result produce accurate or inaccurate results under a wide range of conditions.

The second assumption inherent in release based hazard limits is the conditions under which a release occurs. The potential consequences of a release can vary based on number of factors including activity or design specific characteristics, site specific characteristics, release conditions, and meteorological conditions that can vary on time scales from seconds to years. As a result, assumptions are required that enable the evaluation of releases under analyzable conditions. These results could have significant impacts on societal or environmental conditions correlated with a release based hazard limit, so selection or guidance on the release conditions is extremely important to regulatory evaluations.

These two inherent assumptions are subject to significant uncertainty. Modeling releases and environmental transport of hazards is extremely complex and depends significantly on the input parameters and models used. Use of a particular model or set of release conditions may be accurate in some cases, but under or over conservative in others. As seen for other hazard limits, if the resulting limit is under conservative, societal consequences larger than the societally acceptable limit may occur and could lead to social backlash against the technology. If a hazard limit is overly conservative, the limit could negatively impact the economic or technical viability of the technology. Additionally, excess conservatisms can lead to the misallocation of limited safety resources and reduce overall protection of the public.

Overall, the assumptions inherent in release based hazard limits are generally conservative but will introduce uncertainty into the process. The additional inherent assumption and resulting uncertainties reduce both the number regulatory justifications an applicant is required to justify for regulation, but increases the potential uncertainty and conservatism inherent in the limits.

Effects on regulatory evaluations

Release based regulatory limits are not widely used for regulatory evaluations but are commonly used as a backstop or requirement in operations and regulatory enforcement. Use of these hazard limits creates regulatory system that requires significant regulatory effort for the creation and justification of regulatory limits, but can significantly reduce the regulatory effort needed to prepare and review regulatory documents for specific activities.

These release limits have several distinct advantages related to regulatory evaluations over the lower hierarchical hazard limits. The main advantages of this limit include the ability to more simply characterize quantify (or limit) hazards instead of consequences, and simplified regulatory evaluations for applicants. The main disadvantages of the limit are the increased initial regulation preparation effort and increased regulatory assumptions (and decreased regulatory flexibility).

The main advantage of release based regulatory limits is the ability to quantify hazards instead of consequences. For lower level hierarchical limits, the quantification of the limit relates to the harm caused by the hazard or potential for harm via exposure to the hazard.

Quantification, tracking, and limitation on total hazards are largely absent. While this may not be significant for acute or chronic exposures in humans, understanding the cumulative environmental effect of released hazards may be critical predicting ecological impacts. For these hazards (e.g., hazards that do not degrade or naturally biologically cycle over time), quantification and tracking of the hazard release may be as important as limiting exposures, doses, or consequences.

An example of quantification of cumulative hazards is atmospheric carbon emissions that will contribute to global warming. While it is difficult to quantify the exposures, doses, or consequences associated with individual releases, the cumulative affects of release of carbon into the atmosphere will be significant so quantifying and controlling these release is of significant regulatory interest [35].

The second advantage of release based regulatory limits is simplified regulatory evaluations for applicants. Instead of performing detailed atmospheric modeling or consequence calculations, applicants simply need to show that their activities will not exceed the set regulatory limits. Common methods for regulatory evaluations include citing manufacturer emissions data for commercially available equipment, performing testing to determine activity specific emissions, or performing calculations to determine bounding emissions. The regulatory evaluations required for release based regulatory limits become will more closely resemble permits rather licenses, where an applicant states that they will comply with limits but do not have to demonstrate *a priori* compliance. Instead, the regulatory evaluation simply shows that limits will likely be met, and the operation will depend on continued compliance with limits. In this way, the effort required by applicants is small compared with other lower hierarchical hazard limits.

The main disadvantages of the limit are similar to those of higher hierarchical limits including the increased initial regulation preparation effort and increased regulatory assumptions (and decreased regulatory flexibility). These higher hierarchical limits (with greater inherent regulatory assumptions) shift analytic burden to regulators for the preparation of hazard limits. In addition the assumptions required for lower level hierarchical limits including dose-consequence models, exposure-dose models, use of release based regulatory limits requires definition of release-exposure models which can be subject to significant uncertainty. Development and justification of assumptions also required on release conditions can add additional regulatory burden to limit preparation.

Similar to other relationship models for well-characterized hazards, recommended release-exposure models from professional societies, non-governmental organizations, or other regulators may be used as the basis for selected limits. For other hazards, models for comparable hazards or industries may be used to create new models, with an understanding that the models may be updated based on operational experience or updated scientific observation and modeling. This process can require substantial regulatory effort to review scientific evidence, incorporate stakeholder input and feedback, and select release-exposure models and release conditions.

Similar to concentration exposure hazard limits, a reduction in applicant effort contributes to the second major disadvantage of release limits: reduced regulatory flexibility. The larger number of embedded regulatory assumptions contributes may contain a substantial number of conservatisms that applicants may wish to eliminate to increase design or operational flexibility. Allowing deviations from release regulatory limits can spark claims of regulatory bias and claims that undue harm is occurring due to the regulatory relief. The inherent assumptions and separation from the lowest hierarchical limit of direct and indirect consequences can complicate public discussion of the potential impacts of exemption to release limits. Use of exemptions may require more substantial effort that lower level hierarchical hazard limits because the analytic and review infrastructure to review the deviations from the larger number of inherent regulatory assumptions is not normally present.

Release based limits are extremely common as the primary hazard limit in industries where control and monitoring of individual hazards are possible and desirable. In certain regulatory frameworks, the flexibility in how an applicant meets the release limits could allow for innovation in design and analysis, but total release based limits reduce overall regulatory flexibility and exemptions. This reduction in flexibility, however, can substantially the effort required to prepare and review these evaluations depending on the type of justification required (analytic or by demonstration). This hazard limit shifts regulatory effort towards initial limit creation and reduces regulatory burden on specific activity justification and regulatory analysis.

Effects on regulatory enforcement and operations

Use of release based hazard limits has several distinct advantages related to regulatory enforcement and operational regulation over the lower hierarchical hazard limits. The main advantages of this limit are the ability to easily monitor and assess compliance with release limits. The main disadvantages of this limit are limitations on control and mitigation for acute release limits.

Release based limits have an advantage of much simpler monitoring and testing to ensure compliance with regulatory limits. Unlike the lower hierarchical concentration exposure limits, release limits relate to a measurable quantity that is normally under the control of the applicant. For hazard point sources or small area sources, tools such as of stationary instrumentation or system mass accountancy could be used to determine the release rate, total release, or time averaged release rate. Unlike exposure concentrations that can occur over wide areas, release concentrations or total releases can normally be tracked to a small, fixed number of sources. For mobile source pollution, this may be a smaller advantage but the source location is often known. For release concentration limits, short periods of limit non-compliance can help indicate underlying problems with activities that would result in consequences if not controlled. In this way, release concentration limits can be set sufficiently low that consequences need not occur before regulatory action can be taken to stop a potentially harmful activity. One-time, repeated, or continuous monitoring of releases can allow for varying levels of assurance that the public and the environment are not exposed to unacceptable hazard levels.

While the release based hazard limits are advantageous for monitoring chronic releases, they can be a significant disadvantage for certain total acute release situations. Depending on the hazard, it may not be possible to contain, confine, or eliminate a hazard after it has been release into the environment. If a release hazard limit is based on a total acute release and the limit may be exceeded during operation. If the hazard limit is set sufficiently high, harm may occur if a release occurs and it is not possible to mitigate the harm. As a result, enforcement of acute release limit violations may lead to punitive results and operational improvement but may not be able to undue consequences that have occurred or prevent future consequences related to the release. As a result, waiting for a total release based hazard limit to be exceeded may not be an effective regulatory method depending on the potential consequences associated with the release.

Overall, release based hazard limits are an established method for operational regulation of activities. These limits are particularly effective for fixed source hazards or known mobile hazards that can be monitored. Hazard limits are also generally more applicable for chronic hazards rather than acute hazards but the effectiveness depends heavily on the specific hazard and selected limit.

4.6.1 Creating release based hazard limits for tritium

Release based hazards limits can be separated into two general classes: release concentration based hazard limits and total inventory release based hazard limits. Each of these limits can be related to lower hierarchical hazard limits based on assumptions correlating release concentration or total release to other hazard limits. Similar to the development of exposure concentration based hazard limits, development of release concentration based hazard limits also requires detailed knowledge and characterization of specific hazards.

As previously discussed for exposure concentration based hazard limits, release concentration based hazard limits are only developed in this work for tritium related hazards. Development of release concentration based hazard limits for a specific radionuclide requires significant evaluation effort.

The purpose of this section is to illustrate the connection between hierarchical hazard limits for commercial fusion and not to provide a comprehensive set of release based hazard limits for all commercial fusion hazards. Note that the release based hazard limits in this section are defined with respect to human health effects for acute hazard exposures. There may be additional environment or economic concerns related to acute or chronic releases of tritium that are not bounded by the limits discussed and developed in this section. These considerations would need to be included when setting hazard limits for regulatory purposes.

Tritium and other radiological hazards are accumulating consequence hazards. The cumulative exposure and uptake of tritium will correspond to the hazard consequences. As a result, use of release concentration based hazard limits for tritium hazards would not be useful at limiting the lower hierarchical hazard consequences without also specifying the mass release rate or total material release. Release concentration based hazard are not further defined in this work for acute tritium and tritium related hazards.

For chronic releases, definition of extremely low allowable release concentrations enables reasonable assurance that the total dose exposure or other hazard consequences associated with the release would be socially acceptable. While not discussed further in this work, the NRC guidance used by the NRC, OSHA, and EPA for effluent air release concentration of tritium and tritiated materials can be used to illustrate the conservatism associated with these release limits. The effluent concentration release limit is $1 \times 10^{-7}\ \mu Ci/ml$, a factor of 200 reduction in acceptable concentration compared with the acceptable worker dose [3]. This significantly reduced concentration release limit assures that if the maximum exposed individual were continuously exposed to gaseous tritium effluent at the limit, their total annual exposure would be approximately equal to the 1 mSv annual total dose exposure goal. This represents a conservative method for setting exposure concentration limits needed in regulatory frameworks.

Total inventory release based hazard limits or time averaged release based hazard limits can be defined for an accumulating consequence hazard limit to ensure compliance with lower hierarchical hazard limits for concentration based exposure or total exposure. A standard dispersion model can be used to describe the relationship between the release rate and the downstream exposure conditions [31]:

$$\dot{m}_{release} = C_{expose}\left(\frac{\chi}{Q}\right)^{-1}$$

Where $\dot{m}_{release}$ is the material release rate (Bq/s), C_{expose} is the concentration exposure (Bq/m^3), and χ/Q is the atmospheric dispersion coefficient (s/m^3). Similarly, the standard dispersion model can relate the total exposure to the total released quantity:

$$M_{release} = M_{expose}\left(\frac{\chi}{Q}R_{rate}\right)^{-1}$$

Where $M_{release}$ is the total material release (Bq), M_{expose} is the total material exposure (Bq), χ/Q is the atmospheric dispersion coefficient (s/m^3), and R_{rate} is the breathing rate (m^3/s). These two expressions can be used to develop rate and total release based hazard limits that directly relate to lower hierarchical hazard limits.

The main input assumption required to develop these release based hazard limits is the atmospheric dispersion coefficient (χ/Q) that describes the downstream dispersion of release material. The atmospheric dispersion coefficient is affected by a large number of release characteristics including:

- Distance from release point
- Type of release (continuous or intermittent)
- Release conditions (high velocity or stagnant release)
- Wind speed and direction (constant or variable)
- Meteorological conditions (stable or unstable atmospheric layers)

- Local geography (flat or hilly)
- Local obstructions (no other buildings or significant obstructions)
- Buoyancy of released material (rising, neutral, or falling release)
- Deposition of release material (dry, wet, or no deposition of release)

Development of atmospheric dispersion coefficients can be challenging due to the wide range of possible conditions. Assumption of the atmospheric dispersion coefficient for development of release based hazard limits requires collapse of all variables to a set of consistent release assumptions. Selection of appropriate release assumptions is critical to ensuring that the release based hazard limits are adequate for regulatory evaluations. The following release conditions are assumed based on NRC regulatory guidance for development of atmospheric dispersion coefficients [36]:

- 100 meter distance from release point
- Continuous, low velocity material release
- 1 m/s constant wind speed directed toward receptor
- Stable meteorological conditions (Class F atmospheric stability)
- Local flat geography with no obstructions besides release building
- Neutrally buoyant released material with no deposition

Using these specific release conditions, use of Gaussian Plume dispersion models predict an atmospheric dispersion coefficient of [36]:

$$\frac{\chi}{Q} = 3.3 \times 10^{-3}\ s/m^3$$

With this assumed release condition, material release rate hazard limits and total released quantity hazard limits can be calculated using the lower hierarchical hazard limits developed for acute release of oxidized tritium. The two calculated release based hazard limits are:

- Oxidized tritium release rate limit ($\dot{m}_{release}$): $5.68 \times 10^{10}\ Bq/s$ [$1.59 \times 10^{-4}\ g/s$]
- Oxidized tritium total release limit ($M_{release}$): $2.04 \times 10^{14}\ Bq$ [$0.57\ g$]

Note that the acute oxidized tritium release rate limit is simply a time averaged release rate that, if integrated over a 60 minute release, will equal the total release limit. Changing assumptions regarding the release duration for the acute release would result in changes to the oxidized tritium release rate limit (as well as the lower hierarchical limit of the concentration exposure based hazard limit) but would not change the total release limit or the dose / total exposure based hazard limits.

Comparing the tritium total release limit to the annual tritium releases from PWRs and CANDU reactors can help better contextualize release limit. Both PWRs and CANDU reactors generate tritium during operation due to neutron interactions. In PWRs, tritium is created via neutron interactions with the lithium hydroxide added to PWR primary reactor coolant to control coolant pH. In CANDU reactors, tritium is created via neutron absorption by the deuterium atoms in the heavy water moderator. Table 4.7 presents the tritium total release limit to highest annual tritium releases from a US PWR and Canadian CANDU.

Table 4.7. Comparison of tritium release limits for different technologies

Limit or Release	*Value (Bq)*	*Reference*
Tritium total release limit	2.04×10^{14}	n/a
PWR typical large annual release	6.21×10^{13}	[44]
CANDU typical large annual release	4.10×10^{14}	[45]

Review of the values in Table 4.7 reveal that the actual emissions from large PWR and CANDU facilities are within an order of magnitude of the actual emissions from both the PWR and the CANDU facilities. While annual routine tritium releases are a concern for many facilities, the observed tritium releases from the operating PWR and CANDU plants did not result in violation of other regulatory limits. This apparent inconsistency is due, in large part, to the regulatory assumptions that were made when calculating this release hazard limit and the proceeding hazard limits. Specific conservative assumptions related to exposure pathway (distance, time of exposure, dispersion) and form (assuming fully oxidize releases) result in significantly higher calculated doses than may be realistic for a routine tritium release. While the total release limit calculated in this section are conservative, the impact of these conservatisms on design and operation should be characterized to help determine what hazard limits are appropriate and what regulatory assumptions should be reviewed and revised.

4.7 Total inventory based hazard limits

Total inventory hazard limits are the highest hierarchical hazard limit typically used for the regulation of technology or activity that impact public health and safety. These limits or control the total amount of material or hazard that activity may possess or use. This type of limit requires use of a regulatory assumption that correlates any potential hazard to a socially unacceptable consequence (e.g., human health effects or negative environmental effects).

An example of a total inventory hazard limit for hydrogen chloride (hydrochloric acid) is given by the U.S. Environmental Protection Agency's air program requirements on *Regulated Substances for Accident Release Prevention* (Title 40 of the Code of Federal Regulation, Part 68) [37]:

§68.130 List of substances

(a) Regulated toxic and flammable substances under section 112(r) of the Clean Air Act are the substances listed in Tables 1, 2, 3, and 4. Threshold quantities for listed toxic and flammable substances are specified in the tables.

Table 1 to § 68.130 - List of Regulated Toxic Substances and Threshold Quantities for Accidental Release Prevention

Chemical name	CAS No.	Threshold quantity (lbs)	Basis for listing
...	...	...	...
Hydrogen chloride (anhydrous) [Hydrochloric acid]	7647-01-0	5,000	Mandated for listing by Congress
...	...	...	...

This limit implicitly links a total inventory (mass of hydrochloric acid) to a hazard consequence (socially unacceptable human or environmental consequences released) [37]. As a result, this requirement delineates when a facility inventory has a sufficiently large potential hazard consequence that additional requirements on accident release prevention and risk management are required by the Environmental Protection Agency. This specific requirement was mandated by law by Section 112(r) of the Clean Air Act Amendments of 1990 [38].

Inherent assumptions and uncertainty

Total inventory based hazard limits add one final significant regulatory assumptions to assumptions used in the preceding hierarchical limit (release based hazard limits). This additional assumptions allow for correlation between releases of hazards (at specific concentration levels, controlled quantities, or total amounts to lower hierarchical limits (i.e., releases, exposure concentration hazard limits, dose or total exposures levels, or societally significant consequences). This assumption may carry significant uncertainty that add inherent conservatism or limitations to the limits.

The major embedded regulatory assumptions of concentration exposure based hazard limits are how a hazard inventory correlates to societally significant consequences (via releases or exposures).

The first assumption inherent in total inventory based hazard limits is how the total inventory correlates to societally significant consequences. For each hazard, an inventory limit requires an assumption of how the total inventory could correlate to lower level hierarchical hazard limits (releases, exposure concentrations, doses, or consequences). This assumed correlation is related to the generalized hazard-effect models used in the lower hierarchical hazard limits but includes more generalized assumptions regarding mechanisms, pathways, and scenarios that could lead to release. For example, regulatory assumptions on release and dispersion are needed to assess the societal and environmental consequences (or other hazard limits) of the release of 5,000 pounds of hydrogen chloride from a chemical processing facility. Assumptions and models that relate to the amount of releasable material, the form of the release, the rate of release, and mechanics of the release and related systems could have significant impacts on the assessed release and resulting down steam conditions and consequences.

This inherent assumption is subject to significant uncertainty. Modeling inventories, systems interactions, and events that could produce consequences is extremely complex and depends significantly on specific facilities and system models used. Creation of specific activity agnostic model relating inventory to releases or consequences is challenging. Use of a particular model or scenario may be accurate for some cases, but under or over conservative in others. As seen for other hazard limits, if the resulting limit is under conservative, societal consequences larger than the societally acceptable limit may occur and could lead to social backlash against the technology. If a hazard limit is overly conservative, the limit could negatively impact the economic or technical viability of the technology. Additionally, excess conservatisms can lead to the misallocation of limited safety resources and reduce overall protection of the public. Due to the potential for consequences (as well as societally significant backlash), most inventory limits will tend to be conservatively bounding for all activities.

Overall, the assumptions inherent in total inventory based hazard limits are generally conservative but introduce uncertainty into the process. The additional inherent assumption and resulting uncertainties completely largely eliminate any regulatory justifications an applicant is required to justify for regulation, but increases the potential uncertainty and conservatism inherent in the limits.

Effects on regulatory evaluations

Total inventory based regulatory limits are not widely used for regulatory evaluations but are commonly used as a cutoffs for implementation of more stringent regulatory requirements. Use of these hazard limits creates regulatory system that requires the most significant regulatory effort for the creation and justification of regulatory limits, but can effectively eliminate the regulatory effort needed to prepare and review regulatory documents for specific activities.

These inventory limits have several distinct advantages related to regulatory evaluations over the lower hierarchical hazard limits. The main advantage of this limit is that is greatly simplified regulatory evaluations for applicants and regulators. The main disadvantages of the limit are that it requires the highest level of regulation preparation effort to create regulations and the complete set of regulatory assumptions significantly decreases regulatory flexibility.

The main advantage of inventory based regulatory limits is their simplicity. Unlike other regulatory limits that can require applicants to preparation and regulators to review detailed technical analyses, inventory limits are much simpler to implement. Design calculations and analyses would be required to demonstrate that inventory limits are not exceeded, but calculations of releases, exposures, and consequences are not required for applicants. This could significantly reduce time and cost associated with regulatory applications, reviews, and approvals; if an applicant meets a simple inventory limit, their activity would be allowed.

This simplicity for applicants is also the source for major disadvantages for total inventory limits: increased initial regulation preparation effort and increased regulatory assumptions (and decreased regulatory flexibility). Total inventory based regulatory limits shift the analytic burden of proof from the applicant to the regulator. In addition the assumptions required for lower level hierarchical limits including dose-consequence models, exposure-dose models, and release-exposure models, use of total inventory based regulatory limits requires definition inventory-release models which quantify potential releases based on inventory.

Similar to other relationship models for well-characterized hazards, recommended inventory-release models or assumptions from professional societies, non-governmental organizations, or other regulators may be used as the basis for selected limits. For other hazards, models for comparable hazards or industries may be used to create new models, with an understanding that the models may be updated based on operational experience or design requirements. This process can require substantial regulatory effort to review scientific evidence, incorporate stakeholder input and feedback, and select release-exposure models and release conditions.

Creation of total inventory limits require regulators to development and justification all assumptions down to the lowest minimum socially acceptable hierarchical hazard limit. For some hazards, demonstrating that an inventory limit corresponds to a maximum release hazard limit or exposure concentration limit may be sufficient. For other hazards, demonstration that an inventory limit meets indirect or direct consequence may be required. Depending on the scope of evaluation required, the challenges associated with regulatory preparation and justification of lower level hierarchical hazard will be relevant in addition to the challenges associated with defining and justifying an inventory-release model. This limit creation process could be extremely costly and time consuming to perform.

The increase in number of inherent regulatory assumptions for total inventory limits has the secondary disadvantage of decreasing regulatory flexibility. Total inventory limits are the highest hierarchical hazard limit and, through regulatory assumptions, do not consider activity specific choices or actions that could reduce consequences (e.g., design, operation, siting) and allow operation. Unless an exemption process is available and used, the applicant has no flexibility in how they will achieve sufficiently safe operation: the magnitude of the hazard is the only criteria.

The larger number of embedded regulatory assumptions contributes may contain a substantial number of conservatisms that applicants may wish to eliminate to increase design or operational flexibility. Allowing deviations from total inventory regulatory limits can spark claims of regulatory bias and claims that undue harm is occurring due to the regulatory relief. The inherent assumptions and separation from the lowest hierarchical limit of direct and indirect consequences can complicate public discussion of the potential impacts of exemption to release limits. Use of exemptions may require more substantial effort that lower level hierarchical hazard limits because the analytic and review infrastructure to review the deviations from the larger number of inherent regulatory assumptions is not normally present.

Total inventory based limits are used most commonly as either primary hazard limits or as regulatory cut-offs for activities where large inventories of hazards are required. These limits allow for very little regulatory flexibility as the hazard itself is fixed. This reduction in flexibility, however, is balanced by the minimal applicant effort required to meet regulatory limits. This hazard limit fully shifts regulatory effort towards initial limit creation and minimizes regulatory burden on specific activity justification and regulatory analysis.

Effects on regulatory enforcement and operations

Use of total inventory based hazard limits has several distinct advantages related to regulatory enforcement and operational regulation over the lower hierarchical hazard limits. The main advantages of this limit are the ability is minimized requirements on monitoring and testing of hazard conditions or consequences, and the ability to mitigate and correct limit exceedance before consequences occur. The main disadvantages of this limit is the challenge of externally validating compliance with total inventory limits.

Total inventory based limits are the simplest hazard limit to conceptually measure and ensure compliance with regulatory limits. Unlike the lower hierarchical limits, total inventory should be under full control of the applicant. Based on design and operation of a facility, the total hazard inventory should be fully characterized at all times, with some known or bounded uncertainties. Unlike release or concentrations exposure limits that require monitoring in a variety of locations, or dose or consequence limits that require tracking or testing of large areas or populations, total inventory limits are normally quantities in a limited number of locations that can be more easily monitored. In this way, confirmation that total inventory limits is may be a simple regulatory process.

In addition to simpler measurement to assure regulatory compliance during operation, total inventory limits allow for mitigation and correction of limit violations before consequences occur. Unlike all lower hierarchical limits, inventory limits control the quantity of hazard and not a released quantity or societally significant consequence. If a violation of a total inventory limit occurs, the regulator would have an opportunity to correct the violation and underlying problems before a release or subsequence consequence could occur. This process, however, requires that the regulator or applicant accurately monitor or record total inventory and that correction action occurs in a timely fashion; inaccurate tracking of total inventory or long delays between violation and correction could invalidate the inherent regulatory assumptions associated with total inventory limit and could allow societally unacceptable consequences (should a release occur).

One potential disadvantage of total inventory limits is the challenge of external validation of compliance with total inventory limits. Depending on the hazard and activity, the total inventory related to an activity may be spread among multiple facilities, systems, components, or processes. The hazard may exist in multiple forms and calculating the total inventory could require accountancy of system inputs and outputs. As a result, it may be difficult for a regulator to ensure that total inventory limits are met without detailed knowledge and history of operations if a simple metric (e.g., tank volume, pressure, and temperature or measurable mass balance) is not available for review and operation. While detailed operational oversight is possible, the effort associated with the oversight and complications related to proprietary design information could be significant. Public accountability of compliance with total inventory limits could be challenging, especially if high levels of transparency are required.

Overall, total inventory based hazard limits are a known method for operational regulation of activities. These limits are particularly effective for activities with relatively fixed, constant or well-characterized hazard inventories. Hazard limits are may be simple to monitor operationally but regulatory independence and monitoring can be challenging depending on process and activity transparency.

4.7.1 Creating total inventory based hazard limit for tritium

Development of total inventory based hazard limits requires knowledge of the physical form and usage of specific hazards. These characteristics are needed to assess the potential for releases that would correspond to the lower hierarchical total release hazard limit. A total inventory based hazard limit is only developed in this work for tritium hazards.

Similar to the development of lower hierarchical hazard limits, two different approaches may be used to develop total inventory based hazard limits for tritium hazards for commercial fusion facility. The first is definition of a limit consistent with the lower level hierarchical hazard limit (total release) using assumptions on release conditions. The second is a consensus-based approach where exposure limit is defined using best practices and limits from other regulatory organizations and professional societies.

The first approach uses total release based hazard limits for commercial fusion developed in Section 4.6.1 and assumptions on release conditions to define total inventory based hazard limits. The total release based hazard limit for acute release of oxidized tritium was $2.04 \times 10^{14}\ Bq\ [0.57\ g]$, corresponding to lower hierarchical hazard limits. The assumptions on release conditions can have significant impact on the development of total inventory based hazard limits. There are thee specific release conditions of interest for tritium:

- Release fraction of tritiated material, $F_{release}$
- Oxidation fraction of tritiated material, $F_{oxidized}$
- Amount of tritiated material at risk for release, $M_{vulnerable}$

These assumptions are used in this work to justify the release condition inputs for the development total release based hazard limits for tritium. They are related to the total material release hazard limit developed in Section 4.6.1 by the expression:

$$M_{release} = M_{vulnerable}F_{oxidized}F_{release}$$

Note that these release conditions are not comprehensive for all hazards and that other conditions may be relevant for other hazards or even other tritium hazards in different forms.

The first assumption, release fraction, relates to the physical form of the tritiated material and different failure methods that result in mobilization and release. Two bounding assumptions, full release of material (100% release) or no release from sufficiently robust forms (0% release), must be weighed to assess what releases are mechanistically possible. Discussion of likelihood of release, what constitutes a credible release mechanism, and what level of assurance of meeting lower hierarchical hazard limits may all arise when determining release fractions. Detailed study of the specific hazard may be needed to provide quantitative details to support development of an appropriate release fraction for total release hazard limit development. A release fraction of 1 (100% release) is assumed in this work due to the volatility of tritium in gaseous form and off-gassing of tritium from solid form at temperatures that may be experienced during fires. This release fraction is also conservatively bounding for all physical conditions.

The second assumption, oxidation fraction, relates to the fraction of tritiated material that is released in an oxidized form or oxidizes before reaching an exposed member of the public. This assumption is critical due to the factor of 10,000 difference between the exposure-dose model relationships for elemental tritium ($1.8 \times 10^{-15}\ Sv/Bq$) and for oxidized tritium ($1.8 \times 10^{-11}\ Sv/Bq$) [32]. Assessing the oxidation fraction in a controlled setting may be possible based on controlled release and environmental conditions, but it is challenging for general regulatory evaluations due to both passive oxidation (e.g., environmental exchange) and active oxidation (e.g., combustion) pathways possible for hydrogen release. For these reasons, a lower bound realistic oxidation factor has not been readily identified for releases where combustion is mechanistically possible [39]. An oxidation fraction of 1 is assumed in this work for any acute tritium releases. This oxidation fraction is conservatively bounding for all physical conditions.

The third assumption, amount of tritiated material at risk, describes how much tritiated material is vulnerable for the full release fraction, fully oxidized release. This assumption relates specifically to the distribution and protection of tritiated materials that may be excluded or separated from the evaluation of the total tritiated material on-site. Again, two bounding assumptions, full site release of any present material or full independence of any sufficiently separated and protected inventories, must be evaluated to determine which assumptions are appropriate for both the specific hazard and the regulatory application of the hazard limit.

In this work, tritiated material stored or processed in gaseous, frozen elemental solid, or metal hydride form at any location on the site are considered to be 100% at risk. This tritiated material risk factor is based on the potential for energetic release reactions with both tritium material sources. Oxidized tritium in sufficiently low concentration liquid form is excluded due to the energy input required to rapidly mobilize and disperse the radiological material. Physical separation and protection of tritiated material is also not credited in this work due to limited knowledge of failure modes that could lead to multiple, protected inventories being released simultaneously. More detailed analysis or evaluation could ultimately be used to exclude inventories from the material at risk accountancy but are outside the scope of limit development and this work.

The total inventory limit for the tritium material at risk can be evaluated as a function of the total release based hazard limit, the material release fraction, and the oxidation fraction:

$$M_{vulnerable} = \frac{M_{release}}{F_{release}F_{oxidized}}$$

In this specific case, the total site inventory based hazard limits for tritium in frozen elemental form, gasses, or metallic hydrides is equal to the material release hazard limit of $2.04 \times 10^{14}\ Bq$ [$0.57\ g$] due to the conservatively assumed release and oxidation fractions. While this result appears trivial, this process of explicitly quantifying release assumptions is critical in connecting the total site inventory and total release based hierarchical hazard limits.

This total site inventory based hazard limit is the limit, which exceeded, would result in exceeding the lower hierarchical hazard limits based on the assumptions made in the development of each hazard limit. Use of this hazard limit would vary depending on the regulatory context but could be used as a threshold requiring additional analysis to demonstrate activity or facility compliance with lower hierarchical hazard limits. This helps demonstrate the flexible use of higher order hierarchical hazard limits, enabling vary levels of regulatory burden and conservatism to meet applicant specific needs.

The second approach is a consensus based approach where the total inventory limit is defined using best practices and limits from other regulatory organizations and professional societies. This again relies on the understanding the technical rational and underlying analytic assumptions of regulators and experts responsible for developing and setting site limits. In this work, total inventory limits are taken from NRC requirements on thresholds for developing emergency response plans for facility handling tritium and tritiated materials. The NRC tritium possession limit is $7.4 \times 10^{14}\ Bq$ ($2.07\ g$) with an oxidation fraction of 100% and a release fraction of 50% [40]. These total inventory limits were developed to correspond with an off-site total exposure limit of 1 rem (10 mSv) [41].

These total inventory limits from the NRC for development of additional regulatory analysis align with the dose limits developed for commercial fusion based on the hierarchical hazard limits. The factor of four difference between the derived and consensus total inventory hazard limits are primarily attributable to the different assumptions in the total inventory release fraction (factor of 2) and the difference in the total dose hazard limits (factor of 1.67). This converging result may initially suggest that a hierarchical method for development is redundant with existing regulatory efforts. A hierarchical hazard development method, however, allows for direct consideration and comparison of different hazards and changes to higher hierarchical hazard limits based on explicit changes to lower hierarchical hazard limits or assumptions made between hazard limit levels. This enables direct identification of conservatisms that may normally be unapparent when utilizing higher hierarchical hazard limits.

4.8 Summary of performance based hierarchical hazard limits for commercial fusion acute tritium releases

This work develops hierarchical hazard limits for acute tritium releases from commercial fusion facilities. Table 4.7 summarizes the hierarchical hazard limits developed within this section. These hazard limits are self-consistent, allowing for clear comparison with hazards from other activities or facilities at every hierarchical hazard level. The limits are generally lower than those allowed commercial fission facilities due to the conservatisms used to develop the direct consequence limits and the development of these limits on an individual facility basis that does not explicitly the likelihood of acute facility releases. In the remainder of this work, both the derived and consensus based hazard limits may be used to evaluate the hazards associated with commercial fusion facilities. The selection of these limits for particular evaluations is based on which limit enables the greatest insights into the potential effects of regulatory evaluations on design and licensing burden.

Table 4.7. Derived hierarchical hazard limits for commercial fusion

Hierarchical Hazard Limit	*Value*
Direct consequence limit	0.3 fatalities / TWh
Indirect consequence limit	4.38×10^{-6} fatalities / person-year near facility
	35.04 fatalities / 100,000 persons for acute release
Dose / total exposure limit	6 mSv
	3.37×10^{8} Bq
Concentration exposure limit	1.88×10^{8} Bq/m^3
Hazard release limit	2.04×10^{14} Bq, 0.57 g
Total hazard inventory limit	2.04×10^{14} Bq, 0.57 g

Further development of regulatory frameworks for commercial fusion facilities could, however, incorporate derived hierarchical hazard limits to enable a holistic evaluation of fusion safety as compared with other industrial facilities. This process, including the refinement of hierarchical hazard limits and regulatory assumptions used to correlate limits, may be resource intensive or require extended rulemaking to be incorporated into new or existing regulatory frameworks. This includes the use of hierarchical hazard limits with the different classes of hazards described in Section 6. Full development of hierarchical hazard limits for commercial fusion facilities may be limited to hazards where hierarchical hazard limits either increase regulatory margin or can be used to more appropriately characterize (and differentiate) the inherent hazards associated the commercial fusion technology. The hierarchical hazard limit development process ultimately enables the clear and self-consistent regulation of hazards across technologies, facilities, and industries.

4.9 Reconciling performance based and prescriptive hazard limits

For some regulated technologies, an explicit hazard limit may not be given. Instead, regulatory guidance and requirements on the performance of generic safety systems may be provided with the understanding that adequate implementation of all prescribed safety systems will result in a sufficiently safe system. These requirements and limits are characterized as "prescriptive" or "technology-based" regulations because they prescribe a specific design approach or technology that must be used to satisfy regulatory requirements.

At their most basic level, every prescriptive design or technology requirement relates to a hazard and a relevant hazard limit. The requirements are based, fundamentally, on a regulator's understanding that meeting the requirement will result in overall system characteristics that meet societal expectations for safety. These requirements may relate to performance of individual components or to the need to design and operate systems with types of components.

For an example of a prescriptive design requirement on an individual component, OSHA regulations require that for all liquefied petroleum (LP) gas (e.g., propane) systems used in the construction industry (Title 29 of the Code of Federal Regulation, Part 1926):

> §1926.153(c)(1) Valves, fittings, and accessories connected directly to the container, including primary shut off valves, shall have a rated working pressure of at least 250 p.s.i.g. and shall be of material and design suitable for LP-Gas service

In this way, a technology performance requirement is related to the potential hazard associated with failure. Under design and overpressure of an LP gas system could lead to a release of hazardous gas, fire, or explosion – all of which could produce direct or indirect societal consequences. The technology performance requirement attempts to reduce the likelihood of these consequences by excluding (by design) certain initiating events (e.g., pressurization events up to 250 p.s.i.g.) and resulting accidents. While this does not prevent all possible consequences related to over pressurization, it is intended to limit consequences related to these events to societally acceptable levels.

For an example of a prescriptive design requirement on the need to design an operate systems with certain components, U.S. Department of Transportation (DOT) regulations provide the Federal Motor Vehicle Safety Standards for use with all motor vehicles and motor vehicle equipment (Title 49 of the Code of Federal Regulation, Part 571 [43]). This collection of standards provides requirements on the presence (and in some cases minimum performance of) systems in legal motor vehicles. Systems include:

- Controls and displays (Standard No. 101)
- Rear visibility (Standard No. 111)
- Accelerator control systems (Standard No. 124)
- Minimum Sound Requirements for Hybrid and Electric Vehicles (Standard No. 141)
- Interior trunk release (Standard No. 401)

These requirements related to design characteristics of a system that could contribute to or worsen hazard consequences. While none of these individual requirements alone ensure safety, the simultaneous satisfaction of all prescriptive requirements should produce a safe design. It will not does not prevent all possible consequences related to motor vehicle design and operation, it is intended to limit consequences related to the device to societally acceptable levels.

For both component performance or system design requirements, prescriptive and technology based requirements are ultimately surrogates for societally acceptable consequences. The assurance of safety is assurance of a specific level of safety, as set by the regulator and public. Both propane tanks and motor vehicles could be designed in a more conservative manner and reduce the societal consequences associated with each technology but doing so may have other negative societal consequences such as increased cost, decreased availability, or impacts on usability. As a result, these prescriptive regulations represent a societal balance between the benefits and costs associated with hazard related activities and can be correlated to a hierarchical hazard limit.

Prescriptive and technology based requirements can be correlated to hierarchical hazard limits by determining what aspect of an activity or hazard are they controlling or mitigating. Some requirements are straightforward: prescriptive requirements on use of “best available control technology” (BACT) for controlling air emissions clearly correlate to concentration release limits or total emission limits [42]. Other requirements require a deeper understanding of the system and consequences: prescriptive requirements on design of automobiles will produce vehicles that are socially acceptable, i.e., do not have unacceptably high accident or fatality rates (indirect consequences) or total number of fatalities (direct consequences). This correlation level will depend significantly on the specific requirement.

Creating or reviewing prescriptive and technology based requirements, understanding the underlying correlation to hierarchical hazard limits are critical for uniform discussion of the potential societal impacts or costs of different technologies. Depending on the corresponding hierarchical hazard limit, significant portions of discussion in the above sections may be generally applicable.

Creation and use of prescriptive and technology based requirements works well for established industries where general concept of operations for facilities or products is standardized. These requirements help reduce the burden associated with preparation and review of regulatory documents, and ensure uniformity across an industry. This can be especially useful in industries where a single technology is known and widely accepted to ensure safety. This approach may reduce the time, effort, and cost associated with some regulatory actions. A major downside of this approach, however, is that it requires significant regulatory effort and industry acceptance to implement. Prescriptive requirements can limit innovation by requiring an industry to follow a specific approach and discourage companies from pursuing potentially more effective (but not yet developed) options. Balancing prescriptive and performance based requirements and hazard limits is a challenge for the development of any new regulatory system.

For the initial development and commercialization of commercial fusion technology, generic safety system performance requirements may not be appropriate. Commercial fusion technology is a relatively immature technology, with multiple proposed approaches used to generate fusion reactions. Each technological approach will have different hazards that must be controlled, mitigated, or eliminated to ensure public safety. As a result, use of generic safety system performance requirements may not adequately address the hazards of proposed commercial fusion plants: some hazards may be subject to excessive requirements while other hazards are subject to no requirements. Initial regulation of fusion technology should focus on a broad, hazard limit based approach that allow for the regulation of a wide variety of technologies. As the industry matures, technology standardization between vendors and increased operational experience may allow for development of generic safety system performance requirements that reduces regulatory burden for industry while still ensuring safety.

In this work, the nascent nature of commercial fusion technology does not support the development and implementation of prescriptive and technology based requirements. As a result, the safety analyses and frameworks described in later sections will focus on evaluating safety based on hierarchical, performance based hazard limits. Future work on the topic of commercial fusion licensing could review potential impacts of prescriptive and technology based requirements on the regulation and economic viability of commercial fusion technology.

4.10 References

[1] National Emission Standards for Hazardous Air Pollutants for Source Categories. 40 CFR Part 63,1992.

[2] Transportation Of Natural And Other Gas By Pipeline: Minimum Federal Safety Standards. 49 CFR Part 192, 2006.

[3] Standards for Protection Against Radiation. 10 CFR Part 20, 2015.

[4] National Academies of Sciences, Engineering, and Medicine and others. Designing safety regulations for high-hazard industries. Washington: The National Academies Press. doi, 10:24907, 2018.

[5] K. M. Marios Michaelides, Scott Davis. Implementation and Random Assignment Evaluation of the OSHA SST11 Program. Technical report, U.S. Department of Labor, September 2014.

[6] P. Slovic, B. Fischhoff, and S. Lichtenstein. Facts and fears: Societal perception of risk. ACR North American Advances, 1981.

[7] Occupational Safety and Health Administration. OSHA Fact Sheet: Medical Surveillance for Beryllium- exposed Workers. Technical Report DSG FS-3822, Occupational Safety and Health Administration, 2018.

[8] Health Physics Society. Tritium fact sheet. Technical report, Health Physics Society, March 2011.

[9] Nuclear Regulatory Commission. Modified Reactor Safety Goal Policy Statement. Number SECY-01-0009. 2001.

[10] D. Kyne and B. Bolin. Emerging environmental justice issues in nuclear power and radioactive contamination. International journal of environmental research and public health, 13(7):700, 2016.

[11] Kochanek, K et al. National Vital Statistics Reports: Deaths: Final Data for 2017. Technical report, U.S. Department of Health and Human Services, June 2019.

[12] Occupational Safety and Health Administration. Chemical Management and Permissible Exposure Limits (PELs). (79 FR 61383), 2014.

[13] Nuclear Regulatory Commission. Safety Goals for the Operation of Nuclear Power Plants; Policy Statement; Correction and Republication. (51 FR 30028), 1986.

[14] U.S. Supreme Court. Industrial Union Department, AFL-CIO v. American Petroleum Institute. (448 U.S. 607), 1980.

[15] A. Markandya and P. Wilkinson. Electricity generation and health. The lancet, 370(9591):979–990, 2007.

[16] B. K. Sovacool, R. Andersen, S. Sorensen, K. Sorensen, V. Tienda, A. Vainorius, O. M. Schirach, and F. Bjørn-Thygesen. Balancing safety with sustainability: assessing the risk of accidents for modern low-carbon energy systems. Journal of cleaner production, 112:3952–3965, 2016.

[17] U.S. Census Bureau. US Census Population Estimates Program.

[18] Center for International Earth Science Information Network, Columbia Univeristy. Socioeconomic Data and Applications Center.

[19] Nuclear Regulatory Commission. History of the use and consideration of the large release frequency metric by the U.S. Nuclear Regulatory Commission. Number SECY-13-0029. 2019.

[20] Occupational Safety and Health Administration. Lead in Construction. Technical Report OSHA 3142- 12R, Occupational Safety and Health Administration, 2004.

[21] Occupational Radiation Protection. 10 CFR Part 835, 1993.

[22] Lead. 1910 CFR Part 1025, 2020.

[23] Committee to Assess Health Risks from Exposure to Low Levels of Ionizing Radiation, National Research Council. Health risks from exposure to low levels of ionizing radiation: BEIR VII phase 2. National Research Council (US), 2006.

[24] ICRP. ICRP Publication 82: Protection of the Public in Situations of Prolonged Radiation Exposure, volume 82. Elsevier Health Sciences, 2000.

[25] Nuclear Regulatory Commission. Options to Revise Radiation Protection Regulations and Guidance with Respect to the 2007 Recommendations of the ICRP. Number SECY-08-0197. 2008.

[26] R. Clarke, J. Valentin, et al. ICRP Publication 109. application of the Commission's recommendations for the protection of people in emergency exposure situations. Annals of the ICRP, 39(1):1–110, 2009.

[27] Beryllium. 29 CFR Part 1910.1024, 2020.

[28] Maximum contaminant levels for in-organic contaminants. 40 CFR Part 141.62, 2003.

[29] Mandatory health effects language. 40 CFR Part 141.32(e), 1998.

[30] Benzene. 29 CFR Part 1910.1028, 2019.

[31] Department of Energy. MACCS2 computer code application guidance for documented safety analysis final report. Technical Report DOE-EH-4.2. 1.4, 2004.

[32] K. Eckerman, J. Harrison, H. Menzel, C. Clement, et al. ICRP publication 119: compendium of dose coefficients based on ICRP publication 60. Annals of the International Committee on Radiation Protection, 41:1–130, 2012.

[33] US Department of Health and Human Services and others. Toxicological profile for sulfur dioxide. Public Health Service, Agency for Toxic Substances and Disease Registry, 1998.

[34] Standards of Performance for Electric Utility Steam Generating Units. 40 CFR Part 60, 1971.

[35] Allen, Myles R et al. Warming caused by cumulative carbon emissions towards the trillionth tonne. Nature, 458(7242):1163–1166, 2009.

[36] Nuclear Regulatory Commission. A Regulatory Analysis on Emergency Preparedness for Fuel Cycle and Other Radioactive Material Licensees. Technical Report NUREG-1140, Nuclear Regulatory Commission, 1988.

[37] Chemical Accident Prevention Provisions. 40 CFR Part 68, 1994.

[38] Environmental Protection Agency. Clean Air Act Section 112(r): Accidental Release Prevention / Risk Management Plan Rule. Technical Report EPA 550-R-09-002, Environmental Protection Agency, March 2009.

[39] Department of Energy. DOE Standard: Tritium Handling and Safe Storage. Technical Report DOE- STD-1129-2015, Department of Energy, September 2015.

[40] Rules of General Applicability to Domestic Licensing of Byproduct Material. 10 CFR Part 30, 2007.

[41] Nuclear Regulatory Commission. Emergency Preparedness for Fuel Cycle and Other Radioactive Material Licensees. (54 FR 14061), 1989.

[42] U.S. Code. Clean Air - Definitions. (42 USC 7479), 1990.

[43] Federal Motor Vehicle Safety Standards. 49 CFR Part 571, 2004.

[44] Nuclear Regulatory Commission. Radioactive Effluents From Nuclear Power Plants: Annual Report 2014. Technical Report NUREG-2907, 2018.

[45] Canadian Nuclear Safety Commission and others. Tritium releases and dose consequences in Canada in 2006. 2014.

Chapter 5 – Licensing evaluation methods for commercial fusion

All regulatory frameworks used for oversight of technologies and activities are based, at some level, on licensing evaluation methods. A licensing evaluation method is defined in this work as any formal calculation that evaluates a hazard and produces a result that can be compared to a hazard limit. This chapter focuses on the use of licensing evaluation methods to assess the potential acute catastrophic hazards of commercial fusion facilities. The scope of the licensing evaluations is limited to acute catastrophic evaluations for two major reasons. First, established frameworks for both chronic and non-catastrophic acute hazards are likely adequate for previously characterized commercial fusion hazards. Second, historic experience with commercial fission facility regulation illustrates the challenges and potential impacts of licensing evaluations on the design, operation, regulation, and social acceptance of new technology. Selection of different licensing evaluation methods for acute catastrophic hazards for commercial fusion facilities will significantly impact the commercial viability of the new technology.

This chapter presents the use of five different licensing evaluations that can be used to quantify the acute severe hazard consequences for commercial fusion facilities. Four of the licensing evaluation methods presented are established in existing regulatory frameworks to quantify hazard consequences. These four licensing evaluation methods are:

- Worst case event evaluation
- Maximum credible event evaluation
- Deterministic design basis event evaluation
- Probabilistic design basis event evaluation

These methods illustrate a historical evolution of safety related licensing evaluations in the United States for acute severe hazards. The final licensing evaluation method, probabilistic design basis event evaluation, represents the current "state of the art" for licensing evaluations in the United States for advanced nuclear fission but still has limitations related to regulatory complexity, evaluation uncertainty, and applicability for new technologies. An alternative licensing evaluation method is developed and presented that addresses the challenges associated with probabilistic design basis event evaluation. The alternative evaluation is a hazard control based evaluation and is based on the System-Theoretic Process Analysis (STPA) methodology.

For each of the five licensing evaluations methods discussed in this work, the following information is developed and presented:

- Theoretical basis and major historic regulatory uses of the licensing evaluation method
- Process for applying the specific licensing evaluation method as part of the licensing basis for a commercial fusion facility.

- Preliminary licensing evaluation for a typical commercial fusion facility is then described – the level of detail and completion for each licensing evaluation varying based on the complexity of licensing evaluation method.
- Advantages and disadvantages of the licensing evaluation method
- Potential regulatory implications of the licensing evaluation method on the design, operation, and regulation of commercial fusion facilities

This discussion provides details on the implementation on the licensing evaluations, insights on the licensability of commercial fusion facilities, and information on design, operation, and regulation tradeoffs for different licensing evaluation methods. This information may be useful for developers, regulators, and policymakers when determining appropriate licensing evaluation methods for commercial fusion facilities.

5.1 Generalized model for hazard consequence evaluations

The complexity and detail of different licensing evaluation methods can vary dramatically due to the wide variety of hazard limits. For example, determining a site hazard inventory for comparison to a total inventory hazard limit could simply require documentation of the maximum possible hazard inventory of all plant systems, structures, and components (SSCs). Conversely, determining a facility's overall contribution to public cancer and mortality rates for comparison to probabilistic indirect health consequence limits could requires substantially more documentation and analysis including justification of inventory, release probabilities, exposure pathways, population patterns, and exposure-consequence correlations.

A generalized model for evaluating hazard consequences is based on the hierarchical hazard consequence framework presented in Chapter 4. Hazard consequences can be conceptually described using three separate categories: hazards, exposures, and impacts (Figure 5.1).

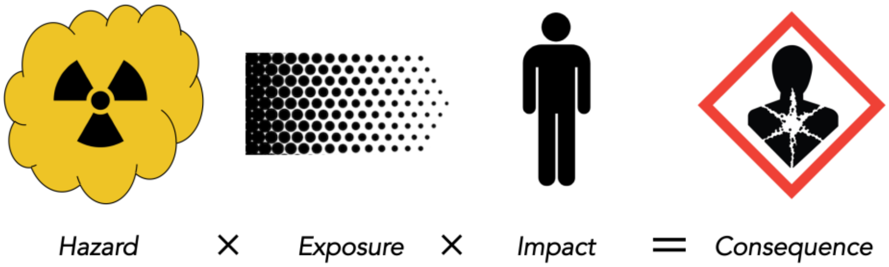


Figure 5.1. Hazard consequence characterization

Each of the three high level categories helps answer a basic question regarding the severity of an accident:

- Hazard: How much hazardous material was released/what was the hazard?
- Exposure: How much hazardous material/hazard affected people/property?
- Impact: What is the correlation of the final exposure to consequences?

Understanding each of these three categories helps characterize the relationship between a hazardous material, activity, or situation and the potential consequences associated with it. The three categories can be further subdivided into seven factors that relate hazards to hazard consequences. Table 5.1 lists the seven factors present in the generalized model across three categories.

Table 5.1. Generalized hazard consequence evaluation model factors

Category	*Specific factor*	*Example factors*
Hazard	Hazard inventory	Material vulnerable to release
	Hazard inventory released	Fraction of material released
	Hazard inventory release conditions	Time, location, form of the release
Exposure	Dispersion conditions	Meteorological, geographic, location factors that control dispersion
	Exposure-dose conditions	Duration of exposure, physiological factors that affect total exposure
Impact	Exposure-consequence relationships	Correlations between exposure and exposure consequences
	Exposed population characteristics	Population distribution and characteristics that affect consequences from a release

These factors are useful to explicitly describe because they can be used to correlate hazards to different hazard limits. This seven factor model characterizing hazard releases is most applicable to acute dispersal hazards (e.g., acute chemical or radiological releases) but is easily adapted to other hazards by combining different factors based on the categories of hazard, exposure, and impact. For each of the hierarchical hazard consequence limits discussed in Chapter 4, different factors of generalized hazard consequence evaluation model factors are applicable. The applicability of each model factor to the analysis of a hierarchical hazard limit is presented in Figure 5.2.

		Hazard Consequence Model Factors						
		Hazard inventory	Hazard inventory released	Hazard release conditions	Dispersion conditions	Exposure conditions	Exposure - consequence relationship	Exposed population characteristics
Hierarchical hazard limits	Total inventory limits	Applicable						
	Release limits (total emission)	Applicable	🟩					
	Release limits (concentration)	Applicable	🟩	🟩				
	Concentration exposure limits	Applicable	🟩	🟩	🟩			
	Total exposure/ dose limits	Applicable	🟩	🟩	🟩	🟩		
	Consequence limits (indirect)	Applicable	🟩	🟩	🟩	🟩	🟩	
	Consequence limits (direct)	Applicable	🟩	🟩	🟩	🟩	🟩	🟩

Figure 5.2. Evaluation model factor applicability for hierarchical hazard limits

Figure 5.2 illustrates two important relationships between the hierarchical hazard limits and the model factors. First, the figure allows for a clear delineation of which model factors relate to different hierarchical hazard limits. For example, evaluation of compliance with total inventory hazard limits only requires consideration of the hazard inventory while evaluation of compliance with concentration exposure hazard limits requires consideration of hazard inventory, hazard inventory release, hazard release conditions, dispersion conditions, and maximum off-site individual conditions. Second, the figure shows how converting between different hierarchical hazard limits can enable expanded flexibility in the analyses of hazard limits (high level limit to lower level limit) by allowing analysis of case-specific factors or enable simplified but more conservative analyses of hazard limits (lower level limit to higher level limit) by requiring standardized assumption of hazard consequence models for all analyses.

Licensing evaluations often serve as the basis for regulatory decisions and processes. In some regulatory frameworks licensing evaluations may be required to demonstrate compliance with existing hazard limits or to determine applicability of additional regulatory requirements. For example, the U.S. Environmental Protection Agency (EPA) Chemical Accident Prevention Program (CAPP) are required to submit a “worst case scenario analysis” that documents the consequences associated with a hazardous material release [1]. These licensing analyses calculate the distance from the release site to a safe location for major accidents. The EPA CAPP requires additional regulatory process controls and emergency planning actions if members of the public may be exposed based on these worst case analysis [1][2].

In other frameworks, a regulator may perform licensing evaluation as a basis for a general permit or regulatory limit on an activity. For example, the Occupational Safety and Health Administration’s Process Management Rule has threshold quantities (TQs) of specific toxic chemicals, exceeding which trigger Process Safety Management regulatory requirements.

These threshold values are based on simplified chemical release calculations of the minimum material quantity required to produce toxic air level or unacceptable blast effects at a specific distance from the release point [3]. These licensing evaluations are used as the basis for a regulatory framework or regulatory limits.

A single licensing evaluation rarely constitutes the entire regulatory basis for an activity or a facility. A complete regulatory basis for an activity or a facility will consist of multiple permits or licenses that govern how it can affect workers, the public, and the environment. In the United States, a regulatory basis for all power plants may consist of regulatory review of and permitting related [4] on topics such as:

- Air pollution emissions (CAA)
- Waste water emissions (CWA)
- Drinking water and ground water usage
- Surface water, waterway, and wetland usage
- Solid waste management
- Land usage and local siting requirements
- Environmental impacts (NEPA)

The form and content of these permits depend on the hazards, the regulatory framework used, and the activity or facility specific hazard. These permits and the relevant requirements can be applied with activities with potential chronic hazard consequences and acute hazard consequences.

For activities with potential chronic hazard consequences (e.g., air emissions), total emission release limits or concentration release limits are commonly specified as part of the regulatory basis. The regulatory basis for these chronic hazards (and their connection to lower level hierarchical hazard consequences) are well characterized and documented based on existing environmental regulations [5][6]. This basis is commonly either prescriptive use of specific hazard reduction, control, or mitigation technologies or specification, monitoring, and documentation of performance based emission limits. In either case, this portion of the regulatory basis can be characterized as general permits [7], with the regulatory bases and licensing evaluation burden shifted to the regulator. Similar regulatory bases may be developed for potential non-catastrophic hazard consequences such as standard industrial hazards for workers [8]. Successful regulation of activities with potential chronic hazard consequences and non-catastrophic hazard consequences is important to deployment of commercial fusion facilities but the challenges associated with regulating these hazards it is not unique to commercial fusion and would likely not present significant new challenges to licensing and regulation.

For activities with potential acute catastrophic hazards, licensing evaluations may be used to quantify the potential consequences associated with an activity or facility. Catastrophic hazards are the residual risk produced by various factors including economic and engineering design considerations, and inherent technological hazards. Quantifying the hazard through licensing evaluations enables comparison to socially accepted limits. A worst-case accident analysis is the simplest form of a licensing evaluation for acute catastrophic hazards.

The design, operational, or other assumptions used in licensing evaluations to demonstrate compliance with regulatory limits may become additional regulatory requirements on an activity or facility. For example, hazardous material quantities used in licensing evaluations may become design or administrative requirements to ensure that the initial hazard quantity inventory assumptions are not violated during facility operation. Licensing evaluations submitted to a regulator become part of a public record and are a check on the activities that may endanger workers, the public, or the environment.

Different licensing evaluations can be used to quantify the hazard consequences associated with an activity or facility. Each licensing evaluation has different levels of inherent conservatism and requires different amounts of resources to prepare (applicant) and review (regulator). Selecting the appropriate licensing evaluation for a technology, activity, or facility requires an understanding of how the licensing evaluation will affect the overall regulatory framework and burden for that activity.

5.2 Licensing evaluation facility parameters and design assumptions

The five preliminary licensing evaluations performed in this chapter are based on analysis of a hypothetical commercial fusion facility or specific systems within the facility for more detailed licensing evaluation methods. This section describes high-level facility design parameters, characteristics, and assumptions that are used as inputs to the preliminary licensing evaluations. The basis for the parameters, characteristics, and any additional assumptions are provided and justified (where appropriate). In some cases, more detailed design information may be required to support evaluations and is provided in the appendices to this work.

5.2.1 General facility parameters

The commercial fusion facility considered in this work is based on the technology specific Level 3 System Engineering Model for a deuterium and tritium fueled, magnetic confinement tokamak commercial fusion facility with a liquid blanket. The general system model is described in Chapter 2 but the design parameters and performance characteristics of the model are not specified. This section provides and justifies general design parameters needed to support preliminary licensing evaluations.

A deuterium and tritium fueled, magnetic confinement tokamak commercial fusion facility with a liquid blanket is selected for analysis in this work for several reasons.

First, a deuterium – tritium fuel mixture is presently regarded as the most technically feasible fusion fuel due to a fusion power density that is two orders of magnitude higher than other fuels at relatively low plasma pressures and temperatures [9]. While the fuel mixture has potential drawbacks (specifically the radioactive tritium and high energy neutrons produced by the reaction), it will likely be used by the first commercial fusion facilities. The general hazards of a deuterium and tritium fueled facility will be comparable between facilities with different confinement methods but the magnitude of the hazards may vary.

Second, a magnetic confinement tokamak has the most operating experience of large fusion experiments including both the TFTR and JET facilities (both also fueled with deuterium – tritium). The ITER facility selected a magnetic confinement tokamak confinement configuration based on the technical readiness of the design and most well characterized physics basis. While the confinement method is specified in this work for completeness, many of the hazards and analyses are comparable for different confinement methods. Analyses of a magnetic confinement tokamak would be very similar to other magnetic confinement configurations such as the spheromak or stellerator. Other confinement configurations would have different hazards but specific differences would depend, in part, on the licensing evaluation method and the level of detailed in the analyses.

Third, a liquid breeding blanket is selected due to the unique hazards associated with the technology as compared with other tritium breeding methods (such as solid breeding modules). This method is also simpler compared with other separated breeding concepts (e.g., solid breeding modules) and simplifies the preliminary safety analysis process. The integration of the tritium breeding and heat removal functions also results in different hazard characterization than other tritium breeding configurations. While the hazards associated a liquid breeding blanket are not explicitly discussed in this work due to the scope limitations of the preliminary licensing evaluations, they would present regulatory challenges due to the radiological and chemical hazards of a molten salt tritium breeding blanket. These hazards would need to be considered by subsequent licensing evaluations.

While this work focuses on deuterium and tritium fueled, magnetic confinement tokamak commercial fusion facility with a liquid blanket, the analyses could be repeated for any proposed fusion facility. Some conservative licensing analyses (e.g., worst-case release analyses) would require minimal effort to repeat for other facilities while more detailed licensing analyses (e.g., deterministic design basis analyses) would require significant design information and effort to complete. The licensing evaluations methods presented in this work are generalizable and applicable to any future commercial fusion facility.

Table 5.2. Facility design input parameters

Facility Parameter	*Variable*	*Value*	*Justification*
Fusion power	P_{fusion}	525 MW	[10]
Plasma volume	V_{plasma}	141 m^3	[11]
Tritium breeding ratio	TBR	1.1	[10]
Fuel injection efficiency	η_{eff}	0.9	Assumption
Fuel burn efficiency	f_b	0.026	Assumption
Net fueling efficiency	$\eta_{eff} f_b$	0.025	Assumption
Fuel Storage (breed based)	τ_{fs}	24 h	Assumption - Need to store 24 hour of burn/breed for T extraction maintenance
Fuel Reserve (input based)	τ_{fr}	8 h	Assumption - Need to store 8 hour input for exhaust processing
Blanket Extraction Time	τ_{be}	12 h	Assumption - Average time to extract tritium from blanket. Steady state.
Exhaust Process Time	τ_{ep}	4 h	Assumption - Average time to process tritium exhaust

Table 5.3. Plasma physics input parameters

Plasma Parameter	*Variable*	*Value*	*Justification*
Average electron density	$< n_e >$	1.3E+20 a/m^3	[11]
Peak electron density	n_0	1.8E+20 a/m^3	[11]
Average ion temperature	$< T_i >$	14 keV	[11]
Peak ion temperature	T_0	27 keV	[11]
Confinement time	τ_c	0.64 s	[11]
Recycle coefficient	R	0.5	Assumption
Fusion reactivity integral	I	1.5E-19	Based on S_n/S_t integral table [12]

Table 5.4. Facility design output parameters

Facility Parameter	*Variable*	*Value*	*Justification*
Tritium consumption rate	$\dot{m}_{T_{burn}}$	$9.3 \times 10^{-4} g/s$	Appendix 5A
Tritium breeding rate	$\dot{m}_{T_{breed}}$	$1.03 \times 10^{-3} g/s$	Appendix 5A
Reactor fueling rate	$\dot{m}_{T_{fuel}}$	$3.9 \times 10^{-2}\ g/s$	Appendix 5A
Plasma Inventory	I_p	$4.6 \times 10^{-2} g$	Appendix 5A
Blanket Inventory	I_b	44 g	Appendix 5A
Exhaust Inventory	I_{ex}	562 g	Appendix 5A
Hold Up Inventory	I_{hu}	958 g	Appendix 5A
Auxiliary System Inventory	I_{as}	1.3 g	Appendix 5A
Fuel Storage (breed based)	I_{fs}	235g	Appendix 5A
Fuel Reserve (input based)	I_{fr}	1123 g	Appendix 5A

5.3 Worst case release licensing evaluation

The first licensing evaluation method proposed for commercial fusion technology is the worst-case release analysis. The worst-case analysis, also termed the "maximum hypothetical accident" [13], is the conceptually simplest form of a hazard analysis. A worst-case analysis is the answer that a worker, regulator, insurer, or member of the public is seeking when they ask the question "What's the worst that could happen?".

A worst-case analysis has several characteristics:

- The analysis should use bounding combinations of input values and assumptions that produce the most severe hazard consequences
- The analysis should calculate hazard consequences independent of probability of occurrence of different hazard consequences
- The analysis should not consider hazard consequence reduction mechanisms (e.g., any engineered safety features) that have plausible failure mechanisms
- The analysis should calculate hazard consequences that can compared against appropriate hazard consequence limits
- The analysis should bound (e.g., predict more severe hazard consequence) any other theoretically possible hazard consequences

This simplicity, however, masks the underlying challenge of performing worst-case analyses: the role and impact of the analyst on analysis results. The cases considered in a worst-case analysis reflect the technical understanding, experience, biases (conscious and unconscious), and imagination of the analyst. These factors include:

- Technical understanding of what constitutes the bounding combination of input values and assumptions
- Consideration of all contributing internal and external factors that could result in more severe hazard consequences (i.e., scenario completeness)
- Assessment of what inputs or assumptions are "theoretically possible" or feasible for the scope of the analysis
- Selection of analysis boundaries (spatially, temporally, stakeholders) and appropriate hazard consequence limits for comparison

These factors can complicate the creation and usage of worst-case analyses for licensing evaluations. Use of structured or repeatable process for conducting worst-case analyses can help ensure consistency and fidelity of licensing analyses and limit analyst bias. These analysis processes may include guidance on analysis methodologies and boundaries, selection of inputs and analysis scenarios, and selection of analysis assumptions. This type of process can result in a consistent worst-case analysis usable for licensing evaluations.

5.3.1 Worst case release evaluation types

Worst-case analyses can be used for licensing evaluations in two distinct ways: analyses performed by a regulator as a basis for regulatory hazard limits (backward analyses) or analyses performed by applicants as the basis for showing compliance with regulatory hazard limits (forward analyses). Backward analyses use a worst-case analysis to justify a hazard quantity or other analysis input limiting condition based on a set hazard consequence limit. Forward analyses use a worst-case analysis to show that an activity or facility with hazards satisfies set hazard consequence limit. These analysis types are characterized based on the visualization of hazard analysis (Figure 5.3). These two types of analyses are both used to justify the licensing and regulation of an activity or facility.

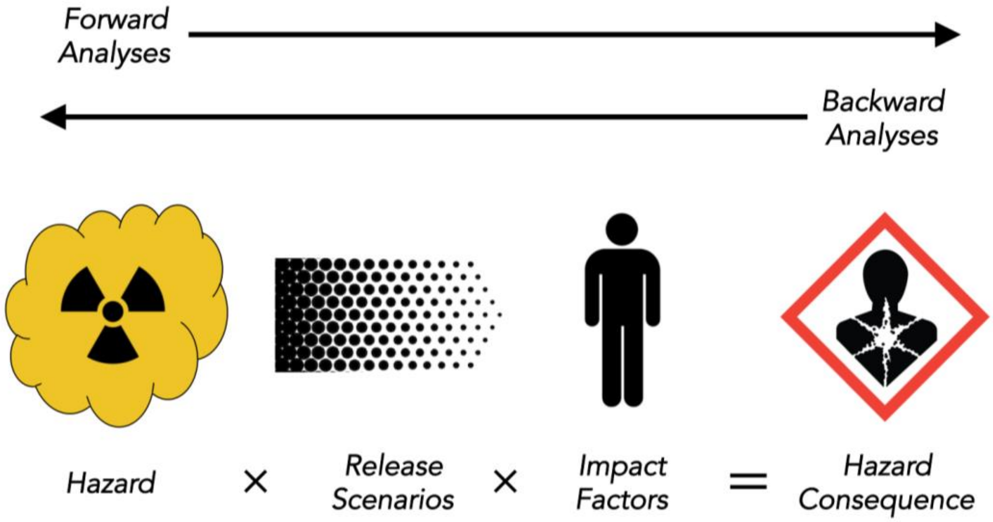


Figure 5.3. “Backward” and “forward” analyses for worst case release analyses

Regulator performed backward worst-case analyses can be used as part of the technical basis for regulatory hazard limits. These analyses provide justification for hazard limits and anchor point for discussion on the adequacy of the hazard limits. Regulators can start with lower order hierarchical hazard limit and determine the bounding hazards or input conditions that will satisfy the hierarchical hazard limit. These analyses are generally performed as part of the rulemaking process for regulatory hazard limits and are used to support higher order hierarchical hazard limits or prescriptive based limits.

One example of a regulator performed worst-case analyses are the inventory limits for toxic materials in the Occupational Safety and Health Administration’s (OSHA) Process Management Rule. OSHA has threshold quantities (TQs) of specific toxic chemicals, exceeding which trigger Process Safety Management regulatory requirements. These threshold values were based on worst-case chemical release calculations of the minimum material quantity required to produce toxic air level or unacceptable blast effects at a specific distance from the release point [3].

OSHA staff conducted the “backward” worst-case analysis to determine the mass of a toxic chemical would result in lethal exposure conditions at a distance of 100 meters. The analysis consists of a simplified Gaussian plume dispersion model of a ground level chemical release for one hour with typical, conservative geographic and meteorological conditions (4.3 m/s wind speed, D-class stability, and urban dispersion coefficients)[1] [14]. It is important to note that these conditions do not necessarily result in the maximum hazard consequence; theoretically more conservative geographic, meteorological, and release conditions could be assumed. Nevertheless, agency staff analysts selected this set of analysis conditions as appropriately representative of the theoretically worst-case release. Use of a worst-case analysis is particularly useful as part of the regulatory basis because the calculated hazard limits should bound all possible facility conditions. This process allows regulators to have a simple and technically transparent inventory based hazard limit that should be simple for applicants to comply with regulatory limits.

Applicant performed forward worst-case analyses can be used as part of the technical basis for showing compliance with regulatory hazard limits. These analyses provide justification how a facility or activity meets hazard limits and are performed as part of a license preparation process. Specific characteristics of a facility or activity are analyzed used bounding inputs and assumptions to assess or demonstrate compliance with a hazard limit.

One example of applicant performed forward worst-case analyses are Off-site Consequence Analyses (OCA) performed for toxic or explosive materials as part of the Environmental Protection Agency's (EPA) Risk Management Program (RMP). The RMP mandates that applicants create and maintain safety and risk management programs for facilities with hazardous substances. The regulatory requirements for the facility vary based, in part, on the results of a worst-case analysis of a bounding plant accident. The OCA is a forward worst-case analysis that determines the maximum distance from the facility to the toxic or flammable end point where a member of the public would be exposed to fatal or permanently disabling conditions [15]. The EPA does not prescribe the method for performing a worst case analysis, but provides guidance on recommended worst case assumptions, available methods, and provides a free tool for applicants to use that satisfy the regulatory requirements for the worst case analysis [16].

The recommended EPA worst-case analysis consists of a simplified Gaussian plume dispersion model of a ground level chemical release of the largest chemical inventory for 10 minutes with typical, conservative geographic and meteorological conditions (1.5 m/s wind speed, F-class stability, and urban or rural dispersion coefficients as appropriate) [15]. This calculation is repeated for all chemicals or mixtures of chemicals that are covered by the RMP rule [2].

[1] Note that Class D atmospheric stability is defined as the neutral class for overcast conditions for day or night with no direct sunlight. Urban dispersion coefficients were selected by OSHA for the PSM rulemaking based on the general assumption that chemical plants would contain numerous buildings and structures and would more appropriately resemble urban conditions than open-country conditions [14]

The distance to toxic endpoint calculated for the EPA RMP worst-case analyses are compared to population data for the area surrounding a facility. If there are "public receptors" located closer than the distance to toxic endpoint, then the facility is subject to additional regulatory requirements related to hazard assessment, hazard management, and emergency planning [2]. The EPA RMP worst-case analyses are a simple regulatory assessment that help assess the need for additional requirements based on the potential significant off-site consequences.

Table 5.5. Comparison of worst-case model parameters

Model	*Wind Speed (m/s)*	*Atmospheric Stability*	*Dispersion Coefficient*	*Release Duration (min)*
OSHA PSM	4.3	D	Urban	60
EPA RMP	1.5	F	Urban or Rural	10

Table 5.5 summarizes the worst-case analysis model parameters used in the OSHA PSM rulemaking and specified by the EPA RMP regulations. While the EPA RMP conditions are more conservative than the OSHA PSM conditions (resulting in higher calculated consequences), these EPA conditions still do not necessarily result in the maximum hazard consequence. More conservative geographic, meteorological, and release conditions could be assumed that would result in more severe hazard consequences. Again, EPA staff selected this set of analysis conditions as appropriately representative of the theoretically worst-case release and allow for regulatory analysis using these conditions.

These worst-case analyses are a simple but efficient regulatory tool to help determine the potential off-site hazard consequences of facilities, trigger different levels of regulatory requirements and reviews, and provide information to regulators and the public on the hazards present in facilities. The availability of free and simplified computational tools to prepare these regulatory analyses (e.g., RMP*Comp) helps enable straightforward regulatory compliance [17].

5.3.2 Proposed worst case release method

The following method is proposed for a worst-case release licensing evaluation for a commercial fusion facility. The following steps are recommended for a worst-case release method analysis:

1. Define analysis boundary (hazards of interest, geographic boundary, temporal boundary)

Defining the analysis boundary requires setting as initial assumptions boundaries such as the specific hazards considered in the analysis, the geographic boundary of the release analysis, and the temporal boundary considered. Depending on the hazards and licensing framework used, worst-case analysis of a single hazard may be sufficient or analysis of multiple hazards in a single or multiple analyses may be required. Geographic and temporal boundaries should be clearly defined to ensure that the analysis accurately models the worst-case hazard consequences. The worst-case release scenario for an acute release (short time scales) into areas immediately surrounding a facility may differ from the worst-case release scenario for a chronic release on a regional basis.

2. Define hazard level of interest (analysis endpoint or calculation product)

Defining the hazard limit level of interest specifies the factors that should be considered in the analysis and the end point of the analysis. The hazard consequence level end point should be based on either the desired regulatory hazard limit level ("backward" analyses) or the mandated hazard limit level ("forward" analyses). The hazard limits selected are most often based on larger political, social, and technical decision-making process that reflect societal acceptance of different hazards and risks within a regulatory framework.

3. Select bounding inputs or assumptions for each of the model factors

Selecting bounding inputs and assumptions for each of the model factors generally requires the greatest level of technical understanding of the facility or activity to complete. Two approaches (with different levels of conservatism) are normally used to complete this step. The first approach is use of generic, worst-case bounding inputs. This approach allows an analyst to select generic inputs that are not physically related to the facility or activity. For example, the EPA's recommendation (40 CFR 68.22(b)) of 1.5 m/s wind speed and F-class stability as generic, worst-case bounding inputs for analysis of off-site hazard consequence [18]. These are assumptions based largely on expert judgment or precedent, but do not require facility or site specific technical information.

The second approach is use of facility of site-specific worst-case inputs. In the prior example, the EPA also permits (40 CFR 68.22(b)) use of site-specific meteorological conditions in worst-case analyses if "the owner or operator can demonstrate that local meteorological data applicable to the stationary source show a higher minimum wind speed or less stable atmosphere at all times during the previous three years" [18]. For each of the model factors needed to perform the analysis, selection of these bounding inputs and assumptions must be made and justified. Independent technical reviews, professional or standard society recommendations, and regulator guidance can all be extremely useful in selecting and justifying appropriate bounding inputs and assumptions.

4. Perform backward or forward analysis to determine bounding hazards based on hazard limits or assess compliance with hazard limits

Appropriate processes for conducting these analyses will vary based on the hazards and hazard limit level of interest. Professional organizations, consensus standards organizations, and regulator guidance can all be useful in selecting the specific analysis process used to calculate the quantities of interest. The technical basis for the analysis should be presented and justified.

5. Review model factors and analysis to confirm linear/expected model behavior or confirm selected factors result in maximum hazard consequences

Reviewing the analysis to confirm that the calculated quantities are actually bounding is important to ensure the safety basis for the calculation. For simple analyses with linear behavior, selection of the maximum or minimum values for each analysis factor will likely result in an overall bounding worst-case analysis. For more complex phenomena with non-linear behavior, a non-obvious combination of factors may produce more severe consequences. The analysis process and inputs should be reviewed to verify and justify that the analysis results in worst case hazard consequences.

This general method for conducting worst-case release analyses is a robust and repeatable process intended to produce consistent, transparent, and technically justifiable results. If performed correctly, a worst-case analysis is the simplest and most robust licensing evaluation for a facility or activity.

5.3.3 "Backward" worst case release analysis for a commercial fusion facility

A "backward" worst-case release analysis is conducted for hypothetical commercial fusion facility. Based on the discussion of hazards of regulatory significance in Chapter 3, the boundaries of this analysis are limited to the catastrophic, acute, local geographic releases of tritium or tritiated materials from a commercial fusion facility. Deposition of tritium into the biosphere and chronic impacts of tritium contamination are not considered.

For this "backward" analysis, the starting hazard consequence limit of interest is an off-site effective radiation dose that requires evacuation of the public based on existing regulatory guidance from the U.S. Department of Homeland Security (DHS) and U.S. EPA [19][2]. Based on the DHS and EPA guidance, a dose limit of 1 rem (10 mSv) is selected.

The worst-case analysis end point is a total inventory limit for tritium and tritium containing materials at a commercial fusion facility. Atmospheric release of tritium and tritiated material will result in the most severe off-site consequence and it is known for atmospheric dispersion modeling that distance to the maximum exposed off-site individual (MOI) has a significant impact on the calculated hazard consequence. It is assumed (based on conservative DOE guidance [20]) that MOI will occur at the site boundary, but for a generic site the distance to site boundary is not know. Instead, this analysis will determine a simplified relationship that describes the inventory-distance factors that result in the

[2] Note that this starting point is a significant assumption in this calculation and will have a significant effect on final calculated hazard inventory limits. Selection and justification of a higher off-site effective radiation dose limit or use of lower hierarchical hazard limits such as indirect or direct consequences could have significant impacts on the calculated acceptable hazard.

hazard consequence limit of interest. This relationship cannot be described using simple numeric equations due to the correlations and models used to calculate off-site hazard consequences, so the results are given as points along an inventory-distance curve.

The following inputs and assumptions are used to support the corresponding model factors in this "backward" worst-case analysis:

- Hazard inventory (vulnerable to release): 100% of the onsite inventory is vulnerable to release. Complete destruction of the commercial fusion facility during a worst-case release. Release of all tritium and tritiated materials is assumed. The inventory limits resulting from the "backward" analysis will correspond to a site inventory limit.
- Hazard inventory released (fraction released): 100% of the onsite inventory is released during the worst-case release. No credit for mitigating design or engineering features to reduce the release fraction is assumed.
- Hazard inventory release conditions (time, location, form): A release time of 2 hours is assumed on DOE and NRC regulatory guidance for acute release [20] [21]. The release location is conservatively assumed as a ground level release to produce the highest concentrations closest to the release point[3]. All tritium is assumed to be released in the oxidized form (HTO, DTO, or T_2O) in a neutrally buoyant plume. This assumption is conservative and will result in the maximum off-site dose if the oxidation fraction cannot be otherwise quantified and assured.
- Dispersion conditions (meteorological, geographic, location): Conservative meteorological and geographic dispersion conditions are assumed in accordance with DOE and NRC regulatory guidance for acute release [20] [21]. These include Pasquill stability class F, 1 m/s wind speeds, countryside dispersion coefficients, and Gifford plume meander. The location of the calculated dose will vary to provide the distance – inventory relationship.
- Exposure/dose conditions (physiological, duration): It is conservatively assumed that an MOI is exposed for the entirety of the release. A typical breathing rate of $3.33 \times 10^{-4}\ \mathrm{m}^3/\mathrm{s}$ for an adult is assumed [20]. Based on existing guidance for exposure to tritiated water vapor, it is conservatively assumed that the MOI has two major exposure pathways: inhalation and skin absorption. For skin absorption of HTO, the dose is assumed to be 50% of the inhalation dose [22]. A dose exposure coefficient for HTO from the ICRP recommendation of $1.8 \times 10^{-11}\ Sv/Bq$ is used [23].

[3] For elevated release conditions, plume effects may produce higher concentrations at the touchdown point – potentially offsite. In all cases, however, the dose-distance relationship for a ground level release will bound doses for any elevated releases. Therefore, the ground level release condition is conservative and bounding.

Using these model factors, the off-site acute radiation dose is calculated using a Gaussian plume model. This model is based on DOE and NRC regulatory guidance for analysis of acute radiation releases [24]. Using the backward analysis, a hazard inventory factor (site inventory of tritium) corresponding to a 1 rem (10 mSv) dose is calculated for different distances from the release to the site boundary. The results of these calculations are presented in Figure 5.3 and Table 5.6.

In the selection of the individual conservative model factors appears to produce a conservative, worst-case result. Off-site dose modeling of neutrally buoyant plumes to model the release of radiological material has been fairly standardized, so use of established model techniques provides confidence in the bounding results of the calculation. The model factors considered for this worst-case analysis results in a dilution factor (χ/Q) of 9.97×10^{-3} at a distance of 100 meters. This dilution factor conservatively bounds DOE analysis guidance for releases which recommend a dilution factor (χ/Q) of 3.5×10^{-3} (where a lower dilution factor results in lower calculated hazard consequences) [20]. This set of model factors appears to conservatively calculate the worst-case acute, off-site consequences for a tritium release.

This “backward” worst-case release licensing evaluation results in bounding inventory limits for a commercial fusion facility. For a specified distance from the release point to the site boundary (or edge of an owner’s controlled exclusion zone), a site inventory limit can be determined. In this case, if a site’s tritium inventory were at or below the specified total inventory hazard limit, a worst-case release analysis would demonstrate the maximum off-site consequence would be at or below the 1 rem dose limit for emergency evacuations. To meet an effective regulatory hazard limit on dose/total exposure, the applicant would simply need to submit evidence to the regulator that they will meet the total inventory limit.

These inventory limits can be compared to inventory limits in federal rules on domestic licensing of byproduct material (including tritium) in the United States (10 CFR 30). The NRC has established inventory limits for byproduct materials, above which emergency response plans are required. The NRC (working in conjunction with the EPA) based these limits to ensure that “the maximum dose to a person offsite due to a release of radioactive materials would not exceed 1 rem effective dose equivalent” [25]. The inventory limit for tritium listed in 10 CFR 30.72 is 20,000 Curies (2.072 g) of tritium with a release fraction of 0.5. This dose limit was set based on a set of similar (but not identical) conservative meteorological conditions that produced slighter higher atmospheric dispersion, producing the limiting dose at a distance of 100 meters [26] [27]. This compares with a dose of 1 rem at a distance of 200 meters for a release of 10,000 Curies (20,000 Curies with a 0.5 release fraction or 1.036 grams) with the standard worst-case release conditions described in this section. The increased dispersion in the 10 CFR 30.72 calculations is largely related to the inclusion of building wake effects help increase turbulence near the release point [27]. This reduces the distance to the 1-rem dose limit and effectively increases the acceptable inventory limit for a given worst case analysis.

The comparison of the “backward” worst-case release analysis conducted in this work to the inventory-based limit and analysis conducted by the NRC to support 10 CFR 30 inventory limits reveals the potential impacts of different worst-case assumptions. The including building wake effects in the analysis but excluding plume meander and assuming a shorter release time results in a lower dose. Is the worst-case analysis always the analysis assumptions that produce the highest possible doses? Are worst case analyses still useful for regulatory purposes even if the combination of bounding assumptions are not realistic or reasonable. These advantages and disadvantages of worst case analyses are discussed in Section 5.2.5.

Table 5.6. Worst-case tritium inventory and site boundary limits for 1 rem dose

Distance (m)	Inventory Limit (g)	Inventory Limit (Ci)
50	0.10	9.17E+02
75	0.19	1.84E+03
100	0.31	3.01E+03
125	0.46	4.45E+03
150	0.63	6.10E+03
175	0.82	7.95E+03
200	1.03	9.99E+03
225	1.27	1.22E+04
250	1.51	1.46E+04
300	2.06	1.99E+04
350	2.67	2.58E+04
400	3.35	3.23E+04
450	4.08	3.94E+04
500	4.87	4.70E+04
600	6.60	6.37E+04
700	8.54	8.24E+04
800	10.67	1.03E+05
900	12.97	1.25E+05
1000	15.53	1.50E+05
1250	22.48	2.17E+05
1500	29.98	2.89E+05
1750	37.95	3.66E+05
2000	46.31	4.47E+05
2250	55.02	5.31E+05
2500	64.03	6.18E+05
3000	82.86	8.00E+05
3500	102.63	9.90E+05
4000	123.19	1.19E+06
4500	144.45	1.39E+06
5000	166.33	1.61E+06

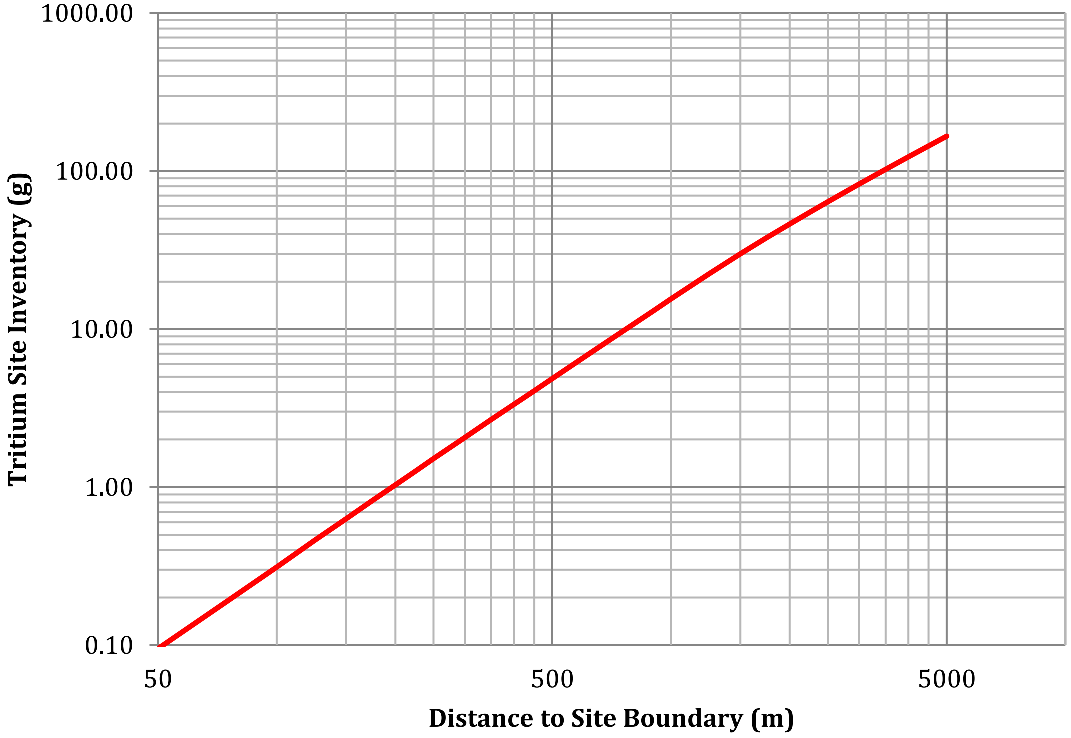


Figure 5.3. Worst-case tritium inventory and site boundary limits

5.3.4 "Forward" worst case release analysis for a commercial fusion facility

A "forward" worst-case release analysis is conducted for hypothetical commercial fusion facility. Based on the discussion of hazards of regulatory significance in Chapter 3, the boundaries of this analysis are limited to the catastrophic, acute, local geographic releases of tritium or tritiated materials from a commercial fusion facility. Deposition of tritium into the biosphere and chronic impacts of tritium contamination are not considered.

The worst-case analysis end point for this worst-case release limit is the off-site dose or total exposure. The dose or total exposure limit is selected by process of elimination of the two lower hierarchical hazard limits. First, this analysis considers a generic commercial fusion facility without specific consideration of the facility location. As a result, the population model information needed to determine the direct consequence limits would be unavailable or would require use of a generic population model. While this model could create licensing envelope if the generic population model bounds a future site-specific population model, it considered outside the scope of this analysis. Second, while an indirect consequence limit could be utilized for this analysis, regulatory guidance for licensing evaluations of most chemical and radiological hazards is based on dose or total exposure limits. For ease of comparison to existing regulatory hazard limits, a dose or total exposure limits is selected.

The following inputs and assumptions are used to support the corresponding model factors in this "forward" worst-case analysis:

- Hazard inventory (vulnerable to release): Complete destruction of the commercial fusion facility is assumed for a worst-case release. Release of all tritium and tritiated materials is assumed possible. Based on the facility design parameters in Table 5.4, this inventory is 1565 grams of tritium circulating and held up in active processing/handling systems, and 1358 grams of tritium in storage systems. The worst-case analysis considers the full site inventory of tritium including tritium in plant systems, tritium storage, and tritium retained in structural materials (2923 grams). The second worst-case analysis excludes the tritium inventory stored in tritium storage systems (1565 grams). While this appears to be a mitigating factor, it is important to separate and contextualize the dose contributions from these two major sources.
- Hazard inventory released (fraction released): In both cases, 100% of the analyzed hazard inventory is released. No credit for mitigating design or engineering features to reduce the release fraction is assumed.
- Hazard inventory release conditions (time, location, form): A release time of 2 hours is assumed on DOE and NRC regulatory guidance for acute release [20] [21]. The release location is conservatively assumed as a ground level release to produce the highest concentrations closest to the release point[4]. All tritium is assumed to be released in the oxidized form (HTO, DTO, or T_2O) in a neutrally buoyant plume. This assumption is conservative and will result in the maximum off-site dose if the oxidation fraction cannot be otherwise quantified and assured.
- Dispersion conditions (meteorological, geographic, location): Meteorological and geographic dispersion conditions are assumed in accordance with DOE and NRC regulatory guidance for acute release [20] [21]. These include Pasquill stability class F, 1 m/s wind speeds, countryside dispersion coefficients, and Gifford plume meander. Site specific meteorological conditions could likely be used but are not assumed for this specific analysis. It is assumed that the facility site boundary (and the maximum exposed off-site individual) is located 160 meters from the release point. This distance is based on the average distance from existing power plants to property boundaries for 200 – 500 MW power plants in Massachusetts.
- Exposure/dose conditions (physiological, duration): It is conservatively assumed that an MOI is exposed for the entirety of the release. A typical breathing rate of 3.33×10^{-4} m^3/s for an adult is assumed [20]. Based on existing guidance for exposure to tritiated water vapor, it is conservatively assumed that the MOI has two major exposure pathways: inhalation and skin absorption. For skin absorption of

[4] For elevated release conditions, plume effects may produce higher concentrations at the touchdown point – potentially offsite. In all cases, however, the dose-distance relationship for a ground level release will bound doses for any elevated releases. Therefore, the ground level release condition is conservative and bounding.

HTO, the dose is assumed to be 50% of the inhalation dose [22]. A dose exposure coefficient for HTO from the ICRP recommendation of $1.8 \times 10^{-11}\ Sv/Bq$ is used [23].

Using these model factors, the off-site acute radiation dose is calculated using a Gaussian plume model. This model is based on DOE and NRC regulatory guidance for analysis of acute radiation releases [24]. Using the forward analysis, two values are calculated for each release case: the acute dose at the site boundary (160 meters) and the distance to evacuation boundary with a 1 rem (10 mSv) dose. The results of these calculations are presented in Table 5.7

Table 5.7. Worst-case site boundary doses and evacuation distances for analyzed commercial fusion facility

Case Number	Tritium Inventory	Dose at 160 m Site Boundary	Distance to 1 rem Evacuation Boundary
Case 1 – Full Site Inventory	2923 g	4140 rem (41.4 Sv)	49.4 km
Case 2 – Active Circulating/ Hold-up Inventory	1565 g	2220 rem (22.2 Sv)	29.4 km

This "forward" worst-case release licensing evaluation for a commercial fusion facility results in both high site boundary doses and large distances to the 1 rem evacuation boundary. A site boundary dose of more than 2000 rem could be expected to cause acute fatalities in nearly 100% of the population exposed[5]. The calculated evacuation distances of 30 km to 50 km are two to three times further than the NRC emergency evacuation planning distance for large light water reactors (10 miles or 16.1 km) [28]. This licensing evaluation (given the specified worst-case assumptions) would likely be unacceptable for a commercial facility. The evaluation (absent changes to methodology assumptions) would likely require significant changes the tritium inventory, siting (e.g., larger site boundary or remote siting), or evaluation limits to meet reasonable regulatory limits.

While these initial worst case results may appear alarming and even imply that the worst-case radiological hazards of commercial fusion may be greater than commercial fission, comparison to the fission worst-case analysis is needed. The Atomic Energy Commission's (AEC) Safeguard Committee developed a conservative "rule of thumb" by 1948 for "postulated worst possible uncontained reactor accident" [29]. The rule of thumb provided

[5] Approximately 50% of people exposed to whole body radiation doses of 600 rem (6 Sv) are expected to die of acute radiation sickness, even with medical treatment. At doses of over 1000 rem, the fatality rates would exceed 90% although there is limited human data on these doses effects [30]

for creation of a controlled exclusion area around the reactor facility calculated using the following formula:

$$d_{exclusion} = 0.01\sqrt{P_{reactor(kW)}}$$

where $d_{exclusion}$ is the distance from the reactor to the edge of the exclusion area in miles and $P_{reactor(kW)}$ is the thermal power of the reactor in kilowatts [29]. For a 525 MW thermal power fission reactor, the controlled exclusion area is:

$$d_{exclusion} = 0.01\sqrt{525{,}000\ kW} = 7.25\ miles = 11.7\ km$$

This formula assumed a release of 50 percent of the reactor fission product inventory and a maximum exposed individual whole body exposure dose of 300 roentgens[6] (approximately 300 rem for whole body tissue exposure). Using this dose limit, we can recalculate the exclusion distance for the two different tritium release cases. The calculated exclusion distance for the forward worst case analysis to the 300 rem exposure boundary for a commercial fusion reactor are presented in Table 5.8.

Table 5.8. Worst-case site exclusion distances for 300 rem exposure for analyzed commercial fusion facility

Case Number	Tritium Inventory	Distance to 300 rem Exclusion Area Boundary
Case 1 – Full Site Inventory	2923 g	0.76 km
Case 2 – Active Circulating/ Hold-up Inventory	1565 g	0.52 km

These recalculated worst-case exclusion boundary distances suggest that there may a one to two order of magnitude difference in radiological hazard between the worst-case release analyses for commercial fission and commercial fusion facilities. Consideration of other radionuclides in the worst-case analysis may increase the distance to the 300 rem exclusion area boundary, causing the worst-case release for a commercial fusion facility to be more similar to those of fission. While these worst-case licensing evaluation for commercial fusion may result in high doses and long distances to the evacuation boundary, it should be recognized that these calculations are extremely conservative and that

[6] The 300-rem dose limit used in the AEC appears high, but it does correlate to an exposure that will produce significant and immediate harm. For a 300 rem whole body dose, most people (75%) would experience acute radiation sickness, a significant fraction (15%-30%) would die even with medical case, and survivors could expect a 25% lifetime increase in fatal cancer risk [30].

substantial reductions in calculated doses can be gained by basing inputs on site or project specific conditions.

5.3.5 Advantages and challenges for worst case release analyses

The main advantage of worst-case analyses for licensing evaluations is also its main disadvantage: simplicity.

Reduction of safety to a single calculation with bounding inputs produces an evaluation method that is simple for both applicants to prepare and for regulators to review. This ideally results in a simple, standardized review methodology that enables transparency for applicants, regulators, and the public. Depending on hazard, simplified evaluation methodologies (e.g., simplified correlations like the AEC exclusion area “rule of thumb” [29]) or computational tools (i.e., EPA off-site consequence analysis with RPM-Comp [17]) can be used to demonstrate compliance with regulatory hazard limits. These tools can significantly reduce regulatory burden on industries and, ideally, increase public trust in the regulatory conclusions.

This simplicity, however, requires significant conservatisms to ensure that it bounds all possible conditions. These excess conservatisms can produce unrealistic results that do not represent any physical scenarios or conditions. These results can constrain the design or operation of a facility to the point of technical or economic infeasibility. A worst-case release licensing evaluation may not produce favorable results if the inherent hazards of the technology are sufficiently high. An activity may be licensable using a worst-case release analysis but the applicant may be unable to meet the regulatory hazard limits using this licensing evaluation.

The main challenge with the simplicity of worst-case analyses for licensing evaluations is that the low number of degrees of freedom in the evaluation can limit pathways to meeting regulatory limits. The limited degrees of freedom relate to the inputs and assumptions used in the analysis. Conservative bounding values must be used for the hazard, exposure, and impact factors. Each of these factors has potential limitations related to the design and evaluation of regulated activities and facilities. In all cases, the exercise of professional judgment is required to determine that constitutes an appropriate “worst-case” for licensing.

Determining the “worst-case” hazard factor associated with an activity or facility often results in evaluation of inherent process hazards without consideration of active or passive design or operational constraints that reduce hazards. In a worst-case analysis, it is commonly assumed that any SSC or operation that can fail will fail. Selection of the bounding hazard factor for a worst-case licensing evaluation requires consideration of the full inherent hazards of a process. Thus, reductions in the hazard factor for a worst-case analysis cannot be accomplished through traditional engineering design methods of increased reliability, redundancy, and resiliency; instead the inherent hazard of an activity must be reduced or eliminated by design (physical reduction of inherent hazard) or by analysis that demonstrates that release is physically impossible under all bounding conditions (analytic reduction of inherent hazard). While this approach to hazard reduction leads to an inherently safer design, the elimination or significant reduction inherent hazards to below acceptable levels may be technically or economically infeasible using existing technology. Consideration of activity specific hazards and resulting worst-case hazard factors is necessary when assessing the viability of utilizing worst-case licensing evaluations.

The selection of bounding inputs and assumptions for hazard, exposure, and impact factors all require the use of professional judgment and can complicate the "simple" process of a worst-case evaluation. Selection of these "worst-case" can be difficult due to exercise of professional judgment in selecting inputs and social acceptance of residual risk of events beyond the "worst-case". While the assumptions and inputs can be sometimes be clearly stated (e.g., the timing of a exposure, the location of a maximum exposed individual, etc.), the agreement on the "worst-case" and excessive conservatism in these assumptions can complicate the analysis process.

For example, bounding "worst-case" meteorological inputs were selected based on guidance of from the DOE and NRC for the licensing evaluations performed in Section 5.3.3 and 5.3.4. A wind speed of 1 m/s, plume meander, and countryside roughness coefficients are used as bounding "worst-case" input conditions. Review of the Gaussian plume model, however, shows that use of a lower wind speed, constant wind direction (no meander), and assuming no contributing surface roughness would result in less plume dilution and higher doses. Changing these three parameters together would result in a factor of 5.9 increase in calculated doses at the 160 m site boundary. While this is revised calculation is more conservative (a worse "worst case"), the question for the analyst, regulator, and public becomes the value in excess conservatism. Ultimately, selection of the bounding inputs and justification of any assumptions depends on the how the licensing analysis is used in the context of the social process of licensing a particular activity or facility and the larger licensing framework.

One way to reduce excess conservatism in these bounding inputs and assumptions (conditions) is to use facility and activity specific bounding conditions worst case analysis instead of generic bounding conditions. Use of generic bounding conditions is intended to bound all expected evaluated activities or provide a pre-evaluated design envelope for facilities or activities. This may result in excess conservatisms if the generic bounding conditions exceed the facility or activity specific bounding conditions. The "backward" worst-case analysis completed in Section 5.3.3 used generic bounding conditions for all model factors, producing results that were applicable to any activity but were extremely conservative. For the "forward" worst-case analysis completed in Section 5.3.4, facility and activity specific bounding conditions were selected for the hazard while generic bounding conditions for the exposure and impact factors, producing results specific to the activity but generally applicable to any site. In either case, use of facility and activity specific bounding conditions for exposure or impact would likely produce less conservative results but would limit the evaluation applicability to the specific site envelope.

Choice of the bounding condition can come at the cost of simplicity, as well as the time and money associated with collection of site-specific data. Use of site-specific meteorological data as part of the EPA RMP rule requires at least three year of measurements for use in OCA. Use of either facility and activity specific bounding conditions or generic bounding conditions are another example of the simplicity versus excess conservatisms tradeoff that must be considered when performing worst-case analyses for licensing evaluations.

5.3.6. Summary of worst case release analyses

Worst-case analyses for licensing evaluations can be the simplest form of licensing evaluation but also may have the largest inherent excess conservatisms. This simplified analysis has the potential to minimize the regulatory burden on commercial fusion. The results of the benchmark worst-case analyses in this section for the tritium hazards from a D-T fusion facility, however, suggest that unless significant changes are made to the hazard, exposure, or impact factors considered in the analysis, the calculated hazard consequences may be unacceptable given the large tritium inventories expected in commercial fusion facilities. Revised or refined facility design characteristics (hazard factor) or updates to facility-specific meteorological and siting characteristics (exposure factors) would likely be required to demonstrate compliance with the stated regulatory hazard limits. Additional analyses would be needed to evaluate the significance of other radiological hazards. The conclusions in this section may change for commercial fusion facilities that utilize non D-T fuel cycles or significantly smaller radiological inventories. The general tradeoffs between design and analysis constraints and regulatory burden should be considered when determining if this analysis method is appropriate for specific commercial fusion facilities.

5.4 Maximum credible release licensing evaluation

The second licensing evaluation method proposed for commercial fusion technology is the maximum credible release analysis. The maximum credible release analysis is closely related to worst-case analysis but seeks to reduce excessive conservatisms in the inputs and assumptions. While the worst-case analysis answers the question “what’s the worst that could happen?”, the maximum credible release instead answers “what’s the worst that could realistically happen?”. The purpose of the maximum credible release analysis for licensing is to provide a realistic evaluation of hazard consequences for a facility or activity while still acknowledge the potential residual risk related to highly unlikely events.

A maximum credible release analysis has several characteristics:

- The analysis should use realistic combinations of bounding input values and assumptions that produce the most severe (but still credible) hazard consequences
- The analysis should calculate hazard consequences with implicit consideration of the probability of different hazard consequences
- The analysis may consider passive hazard consequence reduction mechanisms (e.g., engineered safety features). Failure mechanisms of these passive engineered safety

features relevant to release scenarios (e.g., common cause, correlated, or non-independent failures) should be considered.
- The analysis should calculate hazard consequences that can compared against appropriate hazard consequence limits
- The analysis should bound (e.g., predict more severe hazard consequence) any other credible possible hazard consequences

The maximum credible release intends to provide a more realistic assessment of the hazard consequences that the worst-case release. This conservatism reduction process in a maximum credible release analysis results in two inherent challenges: defining what constitutes credible events and how to account for residual risk from events not considered. Similar to worst-case release analyses, the process for determining the scope, inputs, and assumptions for a maximum credible release reflects the technical understanding, experience, biases, and imagination of the analyst, the regulator, and the public. Understanding the context and purpose of maximum credible release analyses can be critical to creating licensing evaluations that contribute to a successful regulatory process.

5.4.1 Assessing credibility for a maximum credible release analysis

Effective use of maximum credible release analyses as licensing evaluations requires explicit discussion of how analysts can classify release scenarios as either "credible" or "non-credible" and consideration of how handle residual high consequence, low probability events. Credibility is inherently a subjective quality. While the probability of events can be defined, estimated, or quantified, describing event credibility includes subjective interpretation of the estimated probability, quantified uncertainties, and unquantifiable uncertainties of the event. Maximum credible release analyses enable hazard consequences quantification while reducing the excess conservatisms associated with worst-case release analyses, but structured decision making on event consideration and handling of "non-credible" events is important to ensuring transparency and consistency in the regulatory process.

The first challenging question to consider when performing a maximum credible release analysis is whether a particular event being analyzed is "credible" or "non-credible". This assessment may be based on a number of methods including:

- Physical and mechanistic constraints events
- Operational experience
- Expert judgment
- Qualitative design rules
- Quantitative assessment of event probability

These methods exist across a spectrum and have different advantages and disadvantages. Some events may be classified as "credible" or "non-credible" based on the understanding of the underlying physics and mechanistic constraints on a system. For example, while commercial fission reactors contain large quantities of fissile material, their physical configuration and presence of other non-fissionable materials make it impossible for a fission reactor to explode like a nuclear weapon. Instantaneous explosion of fission reactor and release of 100% of the core inventory can thus be classified as a "non-credible" event.

For facilities or activities with significant operational experience, review of operational records is an excellent indicator of possible events [31]. While engineering judgment should also be used to help assess if additional (more severe) accidents are possible, they are a baseline for known possible (and therefore credible) events. Operational experience, however, can bias analysts against more severe accident, particularly for lower probability events that may not have yet been observed but are possible. Additional, for facilities or activities without significant operating experience, assessment of a maximum credible event may be difficult even if operating histories from similar industries are considered.

Historically, expert judgment was the main method of assessing credibility. The AEC Reactor Safeguard Committee used the "maximum credible accident" as the basis for reactor siting evaluations for the first commercial nuclear fission reactors in the Untied States [29]. This evaluation was based on a combination of expert judgment and qualitative design rules. Members of the Reactor Safeguard Committee and AEC staff would develop and evaluate credible accidents until the credible postulated accident with the most severe consequences was identified. This expert judgment was paired with a qualitative design rule that the maximum credible accident was defined by a "single equipment failure or operational error" that resulted in release [29].

These AEC evaluation processes ultimately lead to the designation of the large break loss of coolant accident (LOCA) as the maximum credible accident for light water reactors. This maximum credible accident became the basis for design and safety cases in the United States in commercial fission reactors. While this combination of methods was fairly effective at establishing a design basis, expert judgment suffers implicit bias of experts. The completeness of their assessment or the creation of qualitative design rules created using their expert judgment is based on their technical understanding of system behaviors and possible initiating events. It is important to note that historical operating experience has proven that the large break LOCA does not bound all accident cases. Events such as the 1979 meltdown at Three Mile Island and the 2011 meltdown at Fukushima Daiichi illustrated how multiple concurrent system failures and operator errors can lead to releases.

The fourth method, quantitative assessment of event probability, can be useful to eliminate sufficiently low probability events as "non-credible". This method is intended to reduce some of the biases related to event assessment by assessing credibility based on probability [32]. This approach is useful in theory, but has drawbacks related to both the high time and cost associated with creating event sequence probabilities and the uncertainties related the event probabilities or events assessed. Use of quantitative assessment of event probability to determine the maximum credible accident is valid but engineering effort associated with assessing the probabilities could negate the low regulatory complexity and cost associated with maximum credible accidents as the licensing basis evaluation.

In this work, operational experience and engineering judgment are used to build a case for the maximum credible accident. The justification for the maximum credible accident is a technical argument based on appeals to technical evidence. Development of a set of technical arguments to support licensing is similar to the concept of a "safety case" used by some nuclear regulators in the justification for licensing of nuclear facilities [33].

The second challenging question related to maximum credible releases is how to handle residual postulated high consequence, low probability events. These events are characterized as "non-credible" based on historical experience or other methods, but they are still theoretically possible events. These types of events are natural extensions of "what if" style analyses. In this type of analysis, one can examine any model factors (hazard, exposure, impact) and ask "what if it failed or a more severe condition occurred?" [34]. Ultimately, this type of methodology should converge you to the worst-case analysis. Once a maximum credible release event is selected based on the different methods discussed in Section 5.4.1, the challenge is how to handle the physically possible but characterized "non-credible" events. Facilities and regulators must address non-credible events with catastrophic consequences but exceedingly low probability.

These residual non-credible but catastrophic events should considered in the design and analysis to identify design and operational features with "cliff edge" effects in hazard consequences. Additional efforts to eliminate, mitigate, or control hazards can contribute to a robust facility design and operation. These efforts may not be required by regulators to fully address non-credible events but designing systems to further reduce the probability or consequences of non-credible event can help ensure public safety for rare events. The U.S. implementation of diverse and flexible mitigation strategies (FLEX) following the 2011 Fukushima nuclear accident was designed to provide additional response and mitigation capabilities for unexpected events and reduce the probability and consequences of rare events [35].

For example, the EPA Risk Management Plan requires that facilities or activities conduct "alternative release analyses" that provide for more credible release conditions than a worst-case release analysis. Based on the results of this "alternative release analysis", an owner must have site accident prevention programs and emergency response programs that reduce the likelihood and mitigate the consequences of potential severe accidents [2]. Different design or operational contingencies should be specified for a facility as a part of the maximum credible licensing analysis based on the specific facility, hazards, and the credible and non-credible release analyses to help mitigate these residual high consequence, low probability events.

5.4.2 Proposed maximum credible release method

The following method is proposed for a maximum credible release licensing evaluation for a commercial fusion facility. Seven steps are recommended for a maximum credible release method analysis:

1. Define analysis boundary (hazards of interest, geographic boundary, temporal boundary)

Defining the boundary of the maximum credible release analysis provides a basis for subsequent analysis activities. Specific hazards considered in the analysis, the geographic boundary of the release analysis, and the temporal boundary considered may all be specified. A maximum credible release analysis of a single hazard may be sufficient or analysis of multiple hazards in a single or multiple analyses may be required depending on the hazards and licensing framework used.

2. Define hazard level of interest (analysis endpoint or calculation product)

Defining the hazard limit level of interest specifies the factors that should be considered in the analysis and the calculation end point of the analysis. Again, the hazard consequence level end point should be based on either the desired regulatory hazard limit level ("backward" analyses) or the mandated hazard limit level ("forward" analyses). Use of "backward" maximum credible accident analyses may be limited due to the facility and activity specific hazards that are normally considered as part of the reduction of excess conservatisms associated with maximum credible accident analyses.

3. Develop bounding credible release scenarios (including hazard, exposure, impact factors) based on operational experience and engineering judgment.

The two recommended methods for development of bounding credible release scenarios are operational experience and engineering judgment. Operational experience relies of review of similar hazards, activities, facilities, or industry to identify loss events or precursor events (e.g., "near-miss"). These events (and subsequent investigations) can be used as the basis to develop credible release scenarios. Engineering judgment relies on consultation with subject matter experts to develop credible events. This method is more challenging to categorically describe because it experts may use a combination of operational experience, bounding analyses, engineering "rules of thumb", or other methods to help develop their methods. As a result, differing expert opinions may be anticipated when developing credible release scenarios. Use of multiple independent experts to develop scenarios and justification of engineering judgment can be useful to help provide transparency for the development and selection of the maximum credible release scenario.

Part of developing and selecting bounding credible release scenarios is determining whether to use generic or site specific information to develop these factors. In parallel to the worst-case analyses, the EPA "alternative release analyses" recommends 3 m/s wind speed and D-class stability for generic dispersion factor modeling of off-site consequence analyses or use of "typical" meteorological conditions for the specific site [31]. This change in generic meteorological conditions (1.5 m/s and F-class stability to 3 m/s and D-class stability) results in a factor of 7 or greater reduction in calculated off-site consequences depending on distance. The reduction in conservatism related these and other factors has significant impacts on the calculated consequences. For any model factors needed to perform the analysis, selection of non-bounding factors should be justified. In some cases, justification of some factors may require additional assurances or qualifications that systems, structures, components, or operations will function as intended during the maximum credible event. Generally, mitigating features with credible failure mechanisms (e.g., active and some passive safety systems) should not be relied upon to reduce off-site consequences in the maximum credible analyses.

4. Perform analysis to demonstrate facility compliance with relevant hazard limits

Appropriate processes for conducting these analyses will vary based on the hazards and hazard limit level of interest. Professional organizations, consensus standards organizations, and regulator guidance can all be extremely useful in selecting the specific analysis process used to calculate the quantities of interest. The technical basis for the analysis should be presented and justified.

5. Review calculated model and results to verify that no more severe, credible events can be developed based on operational experience and engineering judgment

Reviewing analyzed release scenarios is important to ensuring that no other credible event could produce more severe consequences. The analysis process and inputs should be reviewed to verify and justify that the analyses produce the maximum credible release hazard consequences.

6. Identify design or operational assumptions present in analytic basis and determine additional assurances or qualifications required to support assumptions.

The sixth and final step is identifying additional assurances and qualifications that are needed to support analysis assumptions, and to identify control and mitigation actions that could be used to reduce the likelihood or consequences of residual “non-credible” but still phenomenological possible events. This step helps ensure the validity of the maximum credible release scenarios and to reduce the risk (probability and consequence) of events deemed “non-credible” based on prior operations or expert experience. If systems, structures, components, or operations were credited in step 3 to reduce conservatism in model factors, additional assurances and qualifications should be identified to ensure that they function as intended under all credible events. The level of assurances needed will likely vary based on the hazards, consequences, and impact of the factor variations on the event consequences. An example of this type of additional assurances for these analyses are OSHA PSM requirements on written operation procedures and qualify assurance programs for hazardous process related equipment [36].

7. Identify additional prevention or mitigation actions that can be used to reduce the probability or consequences of “non-credible” but mechanistically possible events that exceed hazard limits.

If “non-credible” but phenomenological possible events exist that exceed the maximum credible event, additional control and mitigation actions should be identified could be used to reduce the likelihood or consequences of a “non-credible” event. Catastrophic industrial events are rarely unforeseen; their root cause is often described as the tragic intersection of multiple, highly unlikely events that regulators previously dismissed as statistically impossible. The inherent complexity of modern engineered systems limits the ability of engineers to provide high assurance that certain “non-credible” but phenomenological possible events will never occur. If the maximum credible event is used as the licensing evaluation for an activity or a facility, additional control and mitigation actions should be identified that could reduce the likelihood or consequences of a “non-credible” events. These may include actions such as design and siting considerations, operational constraints, or emergency response planning that can used to flexibly respond to low probability events. These controls would not be relied upon to meet hazard limits but help contribute to a robustly safe facility. An example of this type of additional assurances for these analyses is EPA RMP requirements on emergency response program for hazardous facilities [36]. The EPA requirements on emergency response programs are flexible, allowing facilities to vary the scope of the program based on the hazards and interactions with local communities. Identification of these additional qualification and control methods help enable applicants to reduce the inherent conservatisms in licensing evaluations while still ensuring safety.

This general method for conducting maximum credible release analyses is a consistent process intended to produce a technically justifiable result and robust safety case. The maximum credible release enables a reduction in the calculation conservatisms associated with the worst-case release analysis while controlling increases in the licensing application burden and regulatory requirements on the design, manufacturing, and operation of facilities.

5.4.3 Maximum credible release analysis for a commercial fusion facility

A maximum credible release analysis is conducted for hypothetical commercial fusion facility. Based on the discussion of hazards of regulatory significance in Chapter 3, the boundaries of this analysis are limited to the catastrophic, acute, local geographic releases of tritium or tritiated materials from a commercial fusion facility. Deposition of tritium into the biosphere and chronic impacts of tritium contamination are not considered.

The maximum credible release analysis end point for this worst-case release limit is the off-site dose or total exposure. The dose or total exposure limit is selected by process of elimination of the two lower hierarchical hazard limits. First, this analysis considers a generic commercial fusion facility without specific consideration of the facility location. As a result, the population model information needed to determine the direct consequence limits would be unavailable or would require use of a generic population model. While this model could create licensing envelope if the generic population model bounds a future site-specific population model, it considered outside the scope of this analysis. Second, while an indirect consequence limit could be utilized for this analysis, regulatory guidance for licensing evaluations of most chemical and radiological hazards is based on dose or total exposure limits. For ease of comparison to existing regulatory hazard limits, a dose or total exposure limits is selected.

In this analysis, the maximum credible release is characterized as catastrophic destruction of active tritium processing/handling systems, resulting in the oxidized and ground level release of system tritium under typical meteorological conditions. This scenario balances excess conservatism by assuming full system release and oxidation but typical meteorological conditions. The following conservative inputs and assumptions are used to support the corresponding model factors in this maximum credible release analysis:

- Hazard inventory (vulnerable to release): Physical separation of active processing/handling systems and tritium storage systems is assumed. Use of a robust, external hazard resilient storage facility for tritium on metal titride beds is assumed, enabling separation of active process/handling and storage system failure modes. Based on the facility design parameters in Table 5.4, inventory is 1565 grams of tritium circulating and held up in active processing/handling systems is considered as the hazard inventory vulnerable to release.
- Hazard inventory released (fraction released): 100% release of the analyzed hazard inventory is assumed due to the engineering challenges of containing hydrogen gas. No credit for mitigating design or engineering features to reduce the release fraction is taken.
- Hazard inventory release conditions (time, location, form): A release time of 2 hours is assumed on DOE and NRC regulatory guidance for acute release [20] [21]. The release location is conservatively assumed as a ground level release to produce the highest concentrations closest to the release point[7]. All tritium is assumed to be released in the oxidized form (HTO, DTO, or T_2O) in a neutrally buoyant plume. This assumption is conservative and will result in the maximum off-site dose if the oxidation fraction cannot be otherwise quantified and assured.
- Dispersion conditions (meteorological, geographic, location): Alternative meteorological and geographic dispersion conditions are assumed in accordance with EPA regulatory guidance for alternative release off-site consequence analyses [31]. This include Pasquill stability class D, 4.5 m/s wind speeds, countryside dispersion coefficients, and Gifford plume meander. Site specific meteorological conditions could likely be used but are not assumed for this specific analysis. It is assumed that the facility site boundary (and the maximum exposed off-site individual) is located 160 meters from the release point. This distance is based on the average distance from existing power plants to property boundaries for 200 – 500 MW power plants in Massachusetts. A second distance will be evaluated to determine a limiting boundary for emergency response purposes.
- Exposure/dose conditions (physiological, duration): It is conservatively assumed that an MOI is exposed for the entirety of the release. A typical breathing rate of

[7] For elevated release conditions, plume effects may produce higher concentrations at the touchdown point – potentially offsite. In all cases, however, the dose-distance relationship for a ground level release will bound doses for any elevated releases. Therefore, the ground level release condition is conservative and bounding.

3.33×10^{-4} m^3/s for an adult is assumed [20]. Based on existing guidance for exposure to tritiated water vapor, it is conservatively assumed that the MOI has two major exposure pathways: inhalation and skin absorption. For skin absorption of HTO, the dose is assumed to be 50% of the inhalation dose [22]. A dose exposure coefficient for HTO from the ICRP recommendation of $1.8 \times 10^{-11}\ Sv/Bq$ is used [23].

Using these model factors, the off-site acute radiation dose is calculated using a Gaussian plume model. This model is based on DOE and NRC regulatory guidance for analysis of acute radiation releases [24]. Three values are calculated for this maximum credible release case:

- acute dose at the site boundary (160 meters),
- distance to an exclusion boundary with a 25 rem (0.25 Sv) dose, and
- distance to an evacuation boundary with a 1 rem (10 mSv) dose.

The results of these calculations are presented in Table 5.9.

Table 5.9. Maximum Credible Release Analysis

Licensing Evaluation	Tritium Inventory	Dose at 160 m Site Boundary	Distance to 25 rem Exclusion Boundary	Distance to 1 rem Evacuation Boundary
Maximum Credible Analysis	1565 g	117 rem (1.2 Sv)	387 m	2.8 km

This maximum credible licensing evaluation for a commercial fusion facility reduces the excess conservatisms found in the worst-case release analysis but still results in both high site boundary doses and large distances to the 1 rem evacuation boundary. The calculated site boundary dose is reduced by a factor of 20 (as compared with the worst-case release analyses) but would still result in doses 4 to 5 times greater than the 25 rem dose limit for exclusion boundary surrounding a facility in 10 CFR 100.11 [37]. The distance to the edge of this exclusion boundary is calculated using the maximum credible release model factors as 387 meters. The calculated evacuation distances to the 1 rem dose limit of 2.8 km is smaller than the NRC emergency evacuation planning zone for large light water reactors (10 miles or 16.1 km) but still significantly outside of the site boundary [28].

This licensing evaluation (given the specified maximum credible assumptions) would likely be unacceptable for a commercial facility. The evaluation (absent changes to methodology assumptions) would likely require significant changes to the vulnerable tritium inventory (e.g., reducing credible release inventory) or siting (e.g., larger site boundary or remote siting) to meet regulatory limits.

If this maximum credible release were used as a licensing evaluation, several important analysis assumptions would need to be considered for additional assurances and qualifications, or control and mitigation actions. These include:

- Vulnerable hazard inventory limited to active tritium processing/handling systems

- Alternative meteorological release conditions
- Existence of higher consequence non-credible but still phenomenological possible release scenarios

The first assumption relates directly to the vulnerable hazard inventory. In this maximum credible analysis, it is assumed that the active tritium processing/handling systems are physical separated from the tritium storage facility, thus making them independent for the purposes for failure analysis. This assumption requires that there is no credible common cause initiating event or scenario that could lead to the catastrophic release of both inventories. Design considerations such as sufficient physical separation or engineered hardening and qualification of the storage facility against credible release scenarios could be used to support this assumption. If this assumption cannot be credibly supported, the vulnerable hazard inventory would need to be increased.

The second assumption relates to the release conditions for the maximum credible release. In this maximum credible release analysis, the generic alternative release conditions from the EPA RMP were used as the basis for the off-site consequence analysis. These generic conditions may not be appropriate credible release conditions for all sites, particularly for sites that may have lower wind speeds or calmer meteorological conditions (e.g., Class E or Class F). If expert judgment suggests that a more conservative release condition are credible based on local meteorological conditions, the maximum credible analysis inputs may need to be changed.

The release conditions used for the maximum credible release analysis result in calculated dispersion parameters similar to those used for the licensing evaluation of commercial fission facilities. The specified release conditions and 160 meter distance to the exclusion boundary result in a calculated release dispersion factor (χ/Q) of $4.33 \times 10^{-4}\ s/\mathrm{m}^3$. This value is comparable with the dispersion factor considered in the Westinghouse AP1000 licensing documents ($5.1 \times 10^{-4}\ s/m^3$ [38]), AP1000 Vogtle site license documents ($3.49 \times 10^{-4}\ s/m^3$ [39]), and the NuScale license documents ($6.22 \times 10^{-4}\ s/m^3$ [40]). While these three licensing values consider different specific meteorological conditions, release conditions, and exclusion boundary distances, the similar values in the licensing documents suggest that the release conditions used in this analysis are credible and in-line with accepted calculation methods.

The third limiting factor for this analysis is the existence of higher consequence non-credible but still phenomenological possible release scenarios. In this maximum credible analysis, the release of the full inventory under worst-case meteorological conditions was deemed non-credible but it is phenomenological possible. As a result consideration of potentially greater consequence events should be considered to increase facility robustness. Mitigating steps could include quality assurance programs (similar to OSHA PSM requirements) to reduce the likelihood of high consequence events or additional emergency response programs (similar to EPA RPM requirements) that could help mitigate off-site consequences and coordinate emergency response during events that exceed the maximum credible release.

5.4.4 Advantages and disadvantages for maximum credible release analyses

Maximum credible release analyses seek to calculation more realistic hazard consequences while still bounding expected operational situations.

The major advantage of maximum credible release analyses is the trade off between reduced conservatism and increased regulatory burden. The analysis allows an applicant to take regulatory credit for design factors or engineering analyses that reduce the inherent hazards of a facility. Common safety engineering design principles such as a physical separation can be relied upon to reduce hazard inventory if it can be demonstrated (qualitatively) that the physical separation results in independent failure mechanisms for all credible events. Allowing credit for this type of inherent safety and help significantly reduce hazard consequences through reasonable design practices.

The trade-off for this decreased conservatism is an increase in the regulatory burden, but this increase is inherently limited. This type of analysis avoids crediting mitigating features with credible failure mechanisms in conservatism reductions, eliminating the need for more complex analysis methods that demonstrate system performance under a wide range of event sequences and initiating conditions. Instead, a limited number of analysis are needed to justify assumptions related to credible releases and inherent safety, with applicants choosing which conservatisms they would like to reduce based on their business considerations. This trade-off helps facilitate a more realistic (while still semi-transparent) licensing evaluation process.

An acknowledgement of the potential for events beyond the maximum credible release analysis enables licenses to demonstrate that their facilities have some robustness against the “unknown unknowns” events that both operational experience and expert judgment suggest are non-credible. While design considerations and programs that are developed to prevent or mitigate these “non-credible” events may not be relied upon to prevent all off-site consequences, appropriate implementation by applicants can provide both regulators and the public with increased assurance that “non-credible” events will not result in catastrophic off-site losses. The level of company compliance with (and regulatory review of) these additional prevention and mitigation program can produce varying levels of assurance and regulatory burden.

The maximum credible release analysis ultimately seeks to have a similar low regulatory burden as the worst-case release analysis while reducing the excess conservatisms that may make regulatory compliance using worst-case release analyses infeasible. Limited use of engineered systems to reduce consequences can limit the increases in regulatory burden associated with these analyses. The use of additional analysis or qualifications to support these analyses can help increase both regulator and public confidence in the robustness of activities and facilities against rare, catastrophic events.

The main disadvantage of these analyses is the need to define and defend the limiting bounds for what is “credible” in a maximum credible analysis. Each of the four major methods to define credibility (operational experience, expert judgment, qualitative design rules, and quantitative assessment of event probability) has limitations, inherent bias, unquantifiable uncertainties, and may require significant resources to develop. For qualitative definitions of credibility, differing prospective on acceptable risk (based on the risk triplet of what can go wrong, probability, consequences)[41] can lead to differing opinions on credible events. For quantitative definitions of credibility, the calculation of (and uncertainties inherent in) sufficiently low probability events that could be characterized at the threshold of "credible" and "non-credible" events is extremely challenging and may be resource intensive.

Either of these "credible" definitions would be up for debate between stakeholders during review of maximum credible release analyses as a licensing evaluation. Reintroduction of excess conservatisms initially removed (either appropriately or inappropriately) would be a challenge during regulatory reviews. If sufficient conservatisms were reintroduced during the regulatory review process, the maximum credible release analysis would converge with the worst case release analysis, eliminating trade off benefits of utilizing a maximum credible release analysis. The definition of "credible" is, indeed, a regulatory challenge that would need to be addressed before, during, and after the licensing process that requires buy-in from applicants, regulators, and the public to gain social acceptance for the technology.

The second main disadvantage of maximum credible release analyses is the varying level of regulatory burden that may be required to support conservatism reductions made in the analyses or supplemental prevention or mitigation programs. For example, quality assurance programs are a common practice in many industries that help ensure that activities, systems, and components meet the specified performance requirements. What may differ, however, is the level of documentation, review, and regulatory oversight associated with different programs that may (or may not) achieve different levels of quality and performance [42]. Depending on the level of assurance needed to support these reductions, the regulatory burden could be significant. This varying level of regulatory burden is a potential weakness of maximum credible releases because it could fully offset the benefits of conservatism reductions if not properly controlled.

5.4.5 Maximum credible release analysis summary

Use of maximum credible release analyses for licensing evaluations enables trade offs between decreasing inherent conservatism and increasing regulatory burden. This analysis has the potential to balance inherent hazard design constraints on commercial fusion facilities while still limiting the regulatory burden to those comparable for commercial chemical facilities. The results of the benchmark maximum credible release analyses in this section, however, suggest that major changes would be needed to the hazard, exposure, or impact factors considered in the analysis to result in acceptable the hazard consequences. Revised or refined facility design characteristics (hazard factor) or additional updates to facility-specific meteorological and siting characteristics (exposure factors) would likely be required to demonstrate compliance with the stated regulatory hazard limits. The tradeoffs between these design and analysis constraints should be considered when determining if this analysis method is appropriate for specific commercial fusion facilities.

5.5 Deterministic design basis evaluation

The third licensing evaluation method proposed for commercial fusion technology is the deterministic design basis method. The deterministic design basis analysis is a natural extension of the maximum credible release analysis but analyzes system behavior to a wide range potential initiating events that could result in hazard consequences. While the maximum credible release analysis answers the question "what's the worst that could realistically happen?", the deterministic design basis instead answers the question "what would happen if…?". The purpose of the deterministic design basis analysis is to provide assurances that for all explicitly analyzed conditions and design basis events, the facility meets the regulatory hazard limits. These analyses are deterministic because they do not explicitly include the probability of event sequences when evaluating the acceptability of hazard consequences.

A deterministic design basis analysis has several characteristics:

- A design basis for the facility that describes all limiting internal and external conditions for which the plant is design to withstand while meeting regulatory limits
- Event sequences that bound all design basis conditions are analyzed to demonstrate compliance with regulatory limits
- Explicit assumptions are made regarding event sequences including assuming the failure of any single system, structure, or component (SSC)
- Analyses do not explicitly consider the risk of event sequences when assessing whether hazard consequences meet regulatory hazard limits
- Conservative, bounding input values are used for all licensing analyses
- Engineering safety features credited to prevent or mitigate hazard consequences in design basis analyses must have additional assurance that they will function under all design basis conditions
- Events outside of the design basis are analyzed to assess potential weaknesses for non-credible but catastrophically consequential events

The deterministic design basis analysis is intended to further provide a more realistic assessment of the hazard consequences of events and allow facilities to credit passive and active safety systems that can prevent or mitigate hazards. While this conservatism reduction allows for incorporation of engineering safety features into the licensing basis, this process dramatically increases the regulatory burden associated with licensing. Analyses documenting both bounding event sequences and the performance of credited SSCs for all design basis conditions must be performed to support the deterministic design basis. These analyses can be extensive, requiring substantial time and resources to both prepare and review. Understanding the context and purpose of deterministic design basis analyses can be critical to creating licensing evaluations that contribute to a successful regulatory process.

5.5.1 Developing deterministic design bases

In this work, a facility design basis is the set of events, conditions, parameters, and assumptions that a facility is designed and analyzed against to ensure safe operation. These parameters may relate to internal or external events, be unique to a site or uniform across a design or technology, or may be quantitative or qualitative. Note that discussion of this term is complicated by the use of the varying usages of "design-basis" in differing contexts for nuclear fission facility regulation in the United States [43].

This simplified definition of design basis allows for the logical derivation of "design-basis" related requirements including:

- "design-basis event": an initiating event that a facility is designed and analyzed against to ensure safe operation
- "design-basis accident": an accident event sequence that a facility is designed and analyzed against to ensure safe end state
- "design-basis assumptions": assumptions that are explicitly included in the evaluations of other design basis requirements
- "design-basis issues": topical areas or conditions that a facility is design and analyzed against to ensure safe operation
- "design-basis phenomena": an external meteorological condition that a facility is designed and analyzed against to ensure safe operation
- "design-basis threat": an adversarial scenario that a facility is designed and analyzed for to safeguard against radiological sabotage or theft of special nuclear material

In a deterministic design basis, all of these requirements would need to be defined to help ensure that the facility would safely operate through all expected conditions.

There are two main challenges with developing a deterministic design basis for a facility: developing an exhaustive set of parameters needed to ensure safe operation and reaching consensus on quantitative values for unknown, uncertain, or unboundable parameters.

The first challenge relates to assessing what sets of parameters are adequate or expected to assure safe operation. Initial design-basis events and design-basis accidents for commercial fission facilities were derived from the maximum credible accident evaluations performed for early reactors [43]. These sets of parameters were primarily based on operational experience from the early commercial fission industry and other high-hazard industries. By the late 1950s, increased operational experience with fission facilities and more detailed studies of reactor safety suggested that explicit consideration of external events and phenomena (e.g., flooding) and special issues (e.g., anticipated transient without scram) were needed in the design basis to ensure safe operation [43].

The scope of design basis requirements for facilities has grown over time via lessons learned or more detailed engineering study, or as new vulnerabilities are introduced (e.g., cyber-threats related to digital systems). These have lead to an evolving set of requirements, often requiring additional evaluations or even physical backfits to bring facilities into compliance with new requirements [43]. Many of these changes only arise after accidents or near-misses have occurred, such as the fire protection design basis requirements after the 1975 Browns Ferry fire, operator training requirements and design basis event response assumptions after the 1979 Three Mile Island accident, and off-site power reliability requirements and outage event sequence assumptions after the 1990 Vogtle refueling loss of off-site power event [44][45]. Changes to design-basis assumptions (e.g., the single failure-criterion) based on lessons learned or more detailed engineering study have also significantly changed the design and analysis of engineered systems over time [46].

The challenge of developing an exhaustive set of parameters needed to ensure safe operation requires technology developers, regulators, experts, and other stakeholders to determine what events, conditions, parameters, and assumptions that a facility should be designed and analyzed against. This development process can be challenging, especially for novel technologies with little or no operational experience. Use of existing design bases from related technologies is common, but over-constraining a design can both limit innovation and potentially increase costs. Similarly, under-constraining a design may allow unsafe operating conditions (or even accidents) or result in costly backfits that endanger that economic viability of operating facilities. An additional complicating factor for development of design basis parameter sets is the competing priorities between stakeholders involved in the development process. Developers, for instance, may be interested in at maximizing profitability and thus would resist attempts to add additional design basis requirements that they do not believe are necessary to achieve safe operation. Public advocates, on the other hand, may be interested in maximizing safety regardless of profitability and would those push for any additional design basis requirements that they believe would increase safety. Determining the final set of design basis parameters is a simultaneous technical and social negotiation process and could be a significant challenge under different regulatory frameworks (e.g. different countries).

The second challenge is an extension of the technical and social negotiation process for developing the set of parameters: reaching consensus on quantitative values for unknown, uncertain, or physical unboundable parameters. Many design basis parameters are unknown (e.g., system behavior in untestable conditions such as full core melt in fission reactors), uncertain (e.g., true failure behavior of SSCs), or mechanistically unbounded (e.g., maximum tsunami height).

For example, design basis tornado wind speeds for commercial nuclear reactors in the United States are defined as the wind speeds "so that the probability that a tornado exceeding the design basis would occur was on the order of 10^{-7} per year per nuclear power plant" [47]. Given the limited data on tornado wind speeds, this exceedance basis of one time in 10 million years is clearly a somewhat arbitrary value. Original regulatory guidance (WASH-1300) on design basis tornados states [48]:

> In order to adequately protect: public health and safety. The determination of the design basis tornado is based on the premise that the probability of occurrence of a tornado that exceeds the Design Basis Tornado (DBT) should be on the order of 10^{-7} per year per nuclear power plant.

Selecting a DBT exceedance probability of 5×10^{-8} or 2×10^{-7} (half or twice as frequent exceedance) could be equally valid using this logic. Using a DBT exceedance probability of 5×10^{-8} or 2×10^{-7} could increase or decrease the DBT wind speed by approximately 20 MPH given the data provided in the WASH-1300 for a 340 MPH DBT wind speed. This change would affect the structural design basis of nuclear power plant facilities by increasing or decreasing wind loading by approximately 13%. This change could have impact on facility design depending on the loading combinations used in the design and analysis of facility structures. The process for selecting these values can have real impacts on the both the design and cost of regulated activities or facilities. For some design basis parameters, changes in quantitative limits may have minor affect on facility design and operation while others (e.g., post-Fukushima seismic and flooding design basis reevaluations) could require extensive reanalysis or facility modifications [49].

Another example of design basis event selection would be the selection of the design basis tsunami height for coastal nuclear power plants. Tsunami height is mechanistically unbounded, so an assessment must be made when designing protective measures for coastal power plants. Tsunami hazard curves relating tsunami height and annual probability of exceedance developed by regulators and experts are used to estimate appropriate protective measures based on an acceptable exceedance probability.

The challenge of setting these design basis tsunami heights was highlighted by the 2011 Fukushima nuclear accident when the plant sea walls (originally set at 3.1 meters and later raised to 5.7 meters) were overwhelmed by a 10-meter tsunami [50]. The root cause of this under design could be attributed to a number of factors:

- Inadequate, incomplete, or incorrect tsunami hazard curves
- Inappropriately low annual probability of exceedance limit
- A true observed “rare” event with extremely low recurrence probability

Selecting annual probability of exceedance 10 times lower than used for Fukushima could have increased the design basis tsunami height by several meters (based on the tsunami hazard curves) but it is unlikely that it would have resulted in a design basis tsunami heights of greater than 10 meters [51]. Regulators would be challenged to specify adequate method for selection of design basis tsunami height. While the design basis tsunami height could always be set higher to reduce the likelihood of exceedance, there would significant capital costs associated with higher tsunami protection and safety benefit from mitigating extremely unlikely events may never be observed.

Stakeholders (e.g., technology developers, owners, regulators, experts, the public, etc.) must reach agreement on acceptable quantitative values or methods for all of these quantitative design basis parameters based on any available information, design parameter significance, and qualitative or quantitative estimates of acceptable residual risk. This process must be conducted, in some form, for all design basis parameters. As previously highlighted, design basis parameters may have a significant impact on technical and economic viability as additional safety, and so conflicts between different stakeholders could occur. Reaching agreement between stakeholders may vary significantly on the regulatory framework used and the role of different stakeholders in the quantitative design basis parameters selection process. These potential complications should be considered when formulating the development of a deterministic design basis for a facility. Again, the final values of design basis parameters are the result of a simultaneous technical and social negotiation process.

These processes for developing deterministic design bases and the potential challenges associated with the development process are outside the scope of this work but should be considered when assessing the use of deterministic design basis analysis methods for the licensing evaluation of commercial fusion facilities.

5.5.2 Proposed deterministic design basis analysis method

In this work, a simplified framework for performing deterministic design basis analyses is described to highlight the potential regulatory and impacts of this licensing evaluation type on a commercial fusion facility The following general method is based on a review of deterministic analyses conducted for other regulated industries [52]:

1. Define analysis boundary (hazards of interest, geographic boundary, temporal boundary) and what is inside and outside of the analysis scope
2. Establish design basis: what conditions must the facility be able to withstand while still ensuring that it meets public health and safety goals. Establish regulatory hazard consequence limits for different classes of design basis events based on qualitative likelihood of occurrence.
3. Determine and group licensing basis events: can be based on historic operating experience, engineering judgment, PRA indications of high risk events. These events will be considered for their hazard consequences
4. Rank events based on their likelihood of occurrence: normal operation (on-going), anticipated operational occurrences (annual), infrequent events (once-in-plant lifetime), and limiting events (once-in-fleet lifetime). Initiating events with very low probability may be evaluated separately as special events or beyond design basis events.
5. Develop event sequences for initiating events based on plant design. Use of event sequences can be useful at organizing outcomes. Consider the single failure criterion when determining bounding limiting event sequences.
6. Perform design basis safety analysis to demonstrate plant satisfies regulatory requirements for the event type. These analyses should be performed using conservative, bounding values. Events with different likelihoods of occurrence will have different regulatory requirements.
7. Perform qualification design analyses for any systems, structures, or components that are required to ensure that the facility demonstrates compliance regulatory

hazard limits and guidance. These analyses must show that systems can perform their safety function for all design basis events with appropriate margin and support the conclusions of the design basis safety analyses.

8. Develop special events and beyond design basis events: these are event sequences requiring common cause failures, multiple independent failures, or initiating events that are considered exceedingly rare (below once-in-fleet lifetime occurrences). Also identify event sequences that may have defense-in-depth considerations.
9. Perform design basis safety analysis to quantify hazard consequences for special events and beyond design basis events. These analyses should be performed using best estimate values and less restrictive regulatory requirements. These events highlight potential design changes or operational improvements that can reduce the risk of catastrophic accidents.

Similar to prior analysis types, the first step is defining the boundary of the deterministic design basis analysis. This requires setting as initial assumptions boundaries such as the specific hazards considered in the analysis, the geographic boundary of the release analysis, and the considered temporal boundary. A clear definition of scope will result in adequate regulatory treatment of hazards and demonstrate compliance with relevant regulatory limits.

The second step in the deterministic design basis analysis methodology is definition of the plant design basis. The plant design basis consists of the limiting design conditions from internal and external events for SSCs credited in safety analyses. These design basis conditions may be prescribed by a regulator or developed by an applicant on a design specific basis. Certain design basis conditions may also be developed for a generic site or a specific site (e.g., geologic or meteorological conditions). Similar to inputs for other analysis methods, use of a site specific design basis can reduce excess conservatism but can require substantial time and resources to develop.

The third step in the deterministic design basis analysis methodology outlined in Section 5.4.2 is definition of the plant design basis initiating events. Definition of plant design basis events initially appears as an unbounded problem, requiring the analyst to posit the possible space of all events – many of which will not be relevant to facility safety case. Instead, a guided process based on facility safety case can be used to develop the list of initiating events. The concept of the fundamental safety function (based on IAEA Guidance) developed for fission reactor regulation is used to develop plant design basis events. In IAEA guidance for fission reactor safety, the following fundamental safety functions are defined [53]:

1. control of reactivity (rate of fission reactions in the core);
2. removal of heat from the reactor and from the fuel store; and
3. confinement of radioactive material, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases

In fission power plants, fulfilling the three fundamental safety functions help ensure worker and public safety against radiological hazards. Engineered safety features in fission facilities are designed to ensure that these three fundamental safety functions are fulfilled.

The underlying logic of these fundamental safety functions is to control maintain control and confinement of hazards. Reactivity control and removal of heat are both means for ensuring stable configuration of radiologically hazardous material and ensuring confinement.

These fundamental safety functions may be generalized for any hazards to help develop design basis initiating events. For example, a high level list of fundamental safety functions for commercial fusion could be written as:

1. control of energetic hazards sources;
2. control of retained and residual energy in systems; and
3. control and confinement of hazardous material, protection against hazards and control of planned hazardous releases, as well as limitation of accidental hazard releases

These high level fundamental safety functions are similar to the list developed in the DOE Magnetic Fusion Safety Standard [54]. The DOE Magnetic Fusion Safety Standard was developed to provide regulatory guidance for the development of large experimental magnetic confinement fusion devices. The standard provides a fundamental safety function approach for magnetic confinement fusion devices but these fundamental safety functions represent a more technology agnostic approach.

From these fundamental safety functions, classes of initiating events can be developed based on a mechanistic understanding of the system. For typical fission power plants, the NRC has developed seven design basis event groups for development of fission reactor design basis events [52]:

1. Increase in heat removal by the secondary system
2. Decrease in heat removal by the secondary system
3. Decrease in RCS flow rate
4. Reactivity and power distribution anomalies
5. Increase in reactor coolant inventory
6. Decrease in reactor coolant inventory
7. Radioactive release from a subsystem or component

For well-characterized systems with uniform hazards, this level of detail in development of initiating events class can be used to help ensure uniformity and completeness across licensing applications. Based on the relatively early state of technological development for commercial fusion and the wide range of technology specific approaches, development of these design basis event groups for commercial fusion would not likely be useful. Instead, fundamental safety functions should be used to help guide the development of design basis initiating events, with each event tied directly to a fundamental safety function.

As fusion technology matures, development of design basis event groups for commercial fusion may be appropriate to help increase consistency and completeness in the regulatory process.

The fourth step in the deterministic design basis analysis methodology is assigning a qualitative event frequency class to each of the initiating events. These five event frequency classes, based in part on definitions in ANS-51.1-1983 [54] and NUREG-0800 Chapter 15 [52] are:

- Normal operation (NO) – an event or fault that can occur and be sustained during nominal facility operations
- Anticipated operational occurrence (AOO) – an event or fault that can occur during operations (e.g., annually) and is controlled without propagating to more serious conditions.
- Infrequent Event or Fault (IE) – an event or fault that may occur once during facility operations (e.g., once in facility lifetime) and does not have off-site consequences
- Limiting Events or Faults (LE) – an event that may occur once during fleet operations (e.g., once in the complete operations of all related facilities) and limits off-site consequences to acceptable levels
- Beyond Design Basis Accidents or Events (BDBA) – low probability events that are not expected during fleet operations but are phenomenologically possible. These events are not included in the design basis but are reviewed to identify opportunities to increase facility resiliency against low probability, high consequence event sequences.

In a deterministic design basis, the facility must be designed meet relevant regulatory requirements for NO, AOO, IE, and LE design basis events. For events that are characterized as BDBA, facilities should review event sequences and possible consequences. The goal of reviewing BDBAs is to better understand the potential implications of these events, and how design and operational choices could increase facility resiliency to rare, potentially catastrophic events. These event frequencies are primarily based on engineering judgment and observed operating experience.

These event frequency classes are important because they determine the regulatory acceptance criteria for different design basis events. In NUREG-0800, the NRC recommends a mix of technology specific performance criteria (e.g., maximum system temperature and pressure) and technology neutral performance criteria (e.g., off-site doses) for different design basis events [52]. Technology specific performance criteria can be useful for establishing regulatory limits prior to off-site consequences. These criteria, however, also require either general standardization of technology and design prior to development of regulatory requirements or agreement on appropriate performance requirements for individual applicants. Based on the discussion of hazard limits in Chapter 9, different hazard limits (e.g., hazard inventory limits, direct consequence limits) may be selected for use with these licensing evaluations but will have impacts on the possibility of crediting different engineering safety features to meet the limits.

The fifth step in the deterministic design basis analysis methodology is to develop event sequences for bounding event sequences based on plant design. The goal of this step is to comprehensively develop event sequences that describe event progression from a single initiating event to a set of final event state. Development of event sequences is largely an inductive process that involves sequentially evaluating engineered safety features that can prevent or mitigate hazard consequences [55]. For each relevant engineered safety feature in the event sequence, two paths are developed: one if the safety function is performed and a second if the safety function is not performed. Through this process of branching, all significant event sequences should be developed for an initiating event.

The level of design detail and the expertise of analysts developing the event sequences may have a significant impact on the final event sequences [56]. Methodical analysis and use of formal evaluation procedures are useful in ensuring the accuracy and completeness of these analyses [57].

The event sequences should then categorized based on the number of SSC failures that occur in the event sequence. For event sequences with no SSC failures (beyond the initiating event), the event sequence will be part of the design basis. For all other event sequences, the single failure criterion should be applied to determine whether the event sequence and failures are considered design basis event sequences or beyond design basis event sequences. The single failure criterion states that any system relied upon to meet the DBA acceptance criteria must remain functional during design basis events given [58]:

> "(a) any single detectable failure within the safety systems concurrent with
> all identifiable but non-detectable failures,
> (b) all failures caused by the single failure, and
> (c) all failures and spurious system actions that cause or are caused by the
> design basis event requiring the safety function"

Thus, in the review of event sequences, all events involving the failure of non-credited SSCs and up to one credited SSC are considered design basis event sequences while all events requiring multiple, independent credited SSC failures are considered beyond design basis events.

Minimizing the number of SSCs with credited safety functions reduces the regulatory burden associated with a licensing evaluation by limiting the number of SSCs with additional design and performance review requirements. During initial development of the deterministic design basis accident, an applicant may attempt to meet regulatory acceptance limits without crediting any SSCs – an analysis that may resemble worst case or maximum credible release analyses. If preliminary scoping analyses indicate that event sequences do not meet the regulatory acceptance limits, an applicant should review which engineered safety features could be credited with performing safety functions or if changes to system design (and development of new event sequences) are needed to meet regulatory limits. When determining which SSCs should be credited, engineering best practices such diversity of safety features, SSC functional independence, and defense in depth should be considered to produce a more robust design.

Based on the designation of SSCs with credited safety functions and the number of credited SSC failures in each event sequence, the event sequences can either be designated as design basis event sequences (zero or one credited SSC failure) or beyond design basis event sequences (two or greater credited SSC failures).

The sixth step in the deterministic design basis analysis methodology outlined is analyzing event sequences for bounding event sequences. Formal calculations should be prepared for the design basis event sequences to determine if the hazard consequences meet the regulatory acceptance criteria using conservative assumptions. If it can be shown using qualitative and quantitative arguments that one event sequence bounds all other event sequences (i.e., results in the lowest margin to regulatory acceptance criteria), then a formal calculation may only be required for the bounding event sequence.

Uncertainties in analysis methods must be considered and appropriately handled in formal calculations. Uncertainties will exist in all parts of the analyses including input values, boundary conditions, system interactions, analysis models and correlations, and the applicability of analysis results. These uncertainties may be handled explicitly by calculating uncertainty and error propagation or they may be handled implicitly by using bounding parameters. For some analyses, selection of a bounding parameter may not be possible due to the non-linear nature of the system behavior. These non-bounded uncertainties must be carefully handled to make sure that the analysis results appropriately inform the overall deterministic design basis analysis. Quantification of uncertainties in analyses and use of adequate engineering margin to account for them is a critical activity when developing and performing deterministic design basis analyses [59].

The seventh step in the deterministic design basis analysis methodology is to perform qualification design analyses for any SSCs that are credited with safety functions. These analyses must demonstrate that these systems can perform their safety function for all design basis conditions (Section 5.4.3.1) with appropriate margin and support the conclusions of the design basis safety analyses. These analyses can be based on guidance from professional organizations or engineering consensus codes and standards (e.g., ASME, ASCE) can help standardize these calculations and provide justification for assumptions and methods.

It is important to note that for high level or complex SSCs with credited safety functions, detailed assessments of possible failure mechanisms and further credited subsystems may be required. For example, NRC staff guidance on General Design Criteria 17 from 10 CFR Part 50 NRC requires if an SSC requires electric power to fulfill the credited safety function, those electric power systems may also need to be credited as fulfilling a safety function [52]. Additional deterministic design basis analyses may be required to demonstrate that the SSCs can be relied upon for all design basis conditions and that the system meets qualitative design criteria such as the “single failure criterion” [58].

This process of performing qualification design analyses for safety credited SSCs would is repeated for all bounding design basis event sequences identified in prior steps of the deterministic design basis analysis methodology. For systems that rely on a large number of safety credited SSCs, this may require a substantial number of qualification design analyses and can present a substantial regulatory burden. For example, crediting an emergency diesel generator with providing back-up AC power a U.S. commercial nuclear power plant requires analyses substantiating the design and performance, procurement, and operation under 10 CFR 50 Appendix B as a safety related SSC [60] and additional regulatory guidance from the NRC on frequent testing to ensure operability [61]. These requirements are in addition to the normal quality assurance requirements used by private firms when producing commercial grade SSCs. Reviews of safety credited SSCs have indicated that significant cost increases may be expected from the nuclear quality assurance requirements associated with safety credited SSCs [42].

The eighth step in the deterministic design basis analysis methodology is to develop special events and beyond design basis events and event sequences for plant systems. Beyond design basis events include events or event sequences that involve common cause failures, multiple independent failures, or initiating events that are considered exceedingly rare (below once-in-fleet lifetime occurrences). Special events include events that are of particular regulatory concern or have unique regulatory challenges. An example of special events considered in the deterministic design basis analysis regulation of fission reactors is the anticipated transient without SCRAM (ATWS) event [60][62]. This special event is of particular regulatory concern due to the potential severe consequences associated with an ATWS in a fission reactor.

Regulators will normally add of special events to licensing requirements on a hazard-by-hazard basis. These additions are normally based on engineering judgment, expert opinion, or operational experience. No special events are identified in this work for commercial fusion but it is possible that certain operational transients such as plasma disruptions or magnet quenches could be added later as regulatory special events. Regulators and applicants should be cautious about adding special events to the regulatory basis for a facility or activity. Adding extraneous regulatory requirements, especially for highly improbable events, can add significant (and largely undue) regulatory burden with a commensurate increase in public safety. The rational for any adding special events should be clearly documented as part of any new regulatory rulemaking process.

In addition to the events and event sequences identified above, it is common practice to review event sequences that may have defense-in-depth implications. Defense-in-depth is an imprecise (and inconsistent) term in many regulatory applications [63] but is generally refers to the use of multiple, independent layers of protection that are intended to protect the public from releases of radioactivity. These layers include both physical layers (plant capacity defense-in-depth based on design and SSCs) and operational layers (programmatic defense-in-depth based on on-going operator activities) [64]. The goal of defense-in-depth is to increase system resiliency during beyond design basis events and provide additional margin to compensate for both known uncertainties (and unknown uncertainties) in the design and analysis of facilities with significant worst-case hazard consequences.

The ninth step in the deterministic design basis analysis methodology is to perform safety analyses to quantify hazard consequences for the selected beyond design basis event sequences. These analyses are performed using best estimate values (i.e., realistic and non-conservative values) and are intended to highlight potential design or operational improvements to reduce the risk of catastrophic accidents. These results of the analyses provide insights into the safety characteristics of the facility and to examine potential cliff-edge effects relate to certain engineering safety features or common-cause failure mechanisms. If these safety analysis analyses suggest that selected BDBE sequences could have catastrophic consequences, that failure of specific systems could lead to dramatic increases in hazard consequences, or that there is a potential for significant common-cause failure mechanisms, facilities should reexamine plant capacity and programmatic defense-in-depth to determine if changes to plant design could prevent or mitigate these event sequences. Depending on regulator framework, additional SSCs or operator actions may not be required to meet the same regulatory requirements as SSCs with credited safety functions but are intended to increase the overall robustness of the facility.

5.5.3 Deterministic design basis analysis for a commercial fusion facility

A deterministic design basis analysis is outlined in this section for a hypothetical commercial fusion facility. The regulatory burden associated with development of a full deterministic design basis can be significant and is outside the scope of this work. As a result, the high level program parameters for the deterministic design basis are considered, and representative examples of supporting analyses for the deterministic design basis are presented and discussed. The goal of this section is to illustrate the design and regulatory burden trade-offs associated with use of deterministic design basis analyses for licensing evaluations.

Based on the discussion of hazards of regulatory significance in Chapter 3, the boundaries of this analysis are limited to the catastrophic, acute, local geographic releases of tritium or tritiated materials from a commercial fusion facility. Deposition of tritium into the biosphere and chronic impacts of tritium contamination are not considered. On-site or worker protection considerations are not considered in this analysis.

The scope of this deterministic design basis analysis in this work is also limited to the review of the deuterium-tritium storage system discussed in the Level 3 System Engineering Model in Chapter 2. This analysis is limited for two major reasons. First, the facility parameters and design assumptions presented in Section 5.1 show that the fusion fuel reserve storage system would contain the largest single system inventory of tritium. While the tritium stored in this system is likely in a stabilized form (e.g., metallic hydride), it can be mobilized into gaseous form at high temperatures [65]. Thus, analysis of the D-T storage system may be representative of reductions in hazard consequences that may be gained from use of deterministic design basis analyses.

Second, limited design information is available for many proposed systems in a commercial fusion reactor due to the pre-conceptual nature of the facility and technology. Performing a deterministic design basis analysis requires some design information to enable creation of event sequences and identification of initiating events, failure mechanisms, and mitigating SSCs. While the design of a commercial fusion facility is novel, design and safety analysis of a large tritium storage facility has precedent – specifically at both the Darlington Tritium Removal Facility for CANDU reactors [66] and the Tritium Extraction Facility [67]. As a result, general design practices for tritium storage facilities can be used to develop a simplified tritium storage facility design for a commercial fusion facility. This allows for the identification of basic systems that could be credited to prevent or mitigate the consequences of initiating events.

The simplified storage system is presented and discussed in Appendix 5B. The extension of this partial analysis to a complete commercial fusion facility and the implications of the deterministic design basis analysis performed in this section are discussed in Section 5.5.4.

5.5.3.1 Establishing analysis design basis

For the purpose of this analysis, a general plant design basis is described to enable discussion of supporting analyses that would be required for any SSCs credited for prevention or mitigation in design basis event analyses [68]. In this work, a set of typical conditions included in a design basis are taken from existing regulatory guidance as described by the General Design Criteria (GDC) in 10 CFR 50 Appendix A [60]. Particular GDC of interest would include:

- *Criterion 2—Design bases for protection against natural phenomena*: SSC are designed to perform safety function during "natural phenomena such as earthquakes, tornadoes, hurricanes, floods, tsunami, and seiches"
- *Criterion 3—Fire protection*: SSC are "designed and located to minimize, consistent with other safety requirements, the probability and effect of fires and explosions"
- *Criterion 4—Environmental and dynamic effects design bases*: SSC are "designed to accommodate the effects of and to be compatible with the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents... [and] be appropriately protected against dynamic effects, including the effects of missiles, pipe whipping, and discharging fluids"

For an actual facility design basis, significant engineering analysis would need to be conducted to determine the bounding natural phenomena conditions, fire/explosion loads, and environmental and dynamic effects that SSCs would need to be designed against. For any SSC credited in the deterministic design basis analysis to prevent or mitigate hazard consequences, analyses would be required to demonstrate compliance with these conditions by either demonstrating that they are fully protected against (based on other credited SSCs) or can withstand the specified design basis conditions. This requires more detailed engineering design information as well as more specific information on the specific site or bounding design envelope and is outside the scope of this analysis.

5.5.3.2 Defining design basis events

The third step in the deterministic design basis analysis methodology outlined in Section 5.5.2 is definition of the plant design basis events. In this work, the fundamental safety function from IAEA Guidance is used to define plant design basis events: "confinement of radioactive material, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases"[53]. Based on this fundamental safety function and the system description in Appendix 5B, the initiating events are developed for the deuterium-tritium storage system for a commercial fusion facility in Table 5.10.

Table 5.10. Deterministic design basis events for D-T Storage System

FSF/Event Group	*Event No.*	*Initiating Events*	*Frequency*
Loss of radioactive material confinement	1	Loss of glove box clean up – loss of ability to remove mobilized tritium from glove box	NO
	2	Loss of process pipe integrity – loss of in-process mobilized tritium inventory flow	AOO
	3	Loss of glove box integrity – loss of tritium inventory leakage from storage tanks	AOO
	4	Loss of storage bed integrity – loss of mobilized tritium inventory	IE
	5	Loss of storage bed inventory – loss of full component tritium inventory	LE
	6	Loss of multiple storage bed inventory	BDBA
	7	Simultaneous loss of storage bed inventory and glove box integrity	BDBA

These deterministic design basis events represent the initial development of events that directly contribute to loss of radioactive material confinement. This list of events would likely be expanded and consolidated through the design and licensing process. As the facility design progress from pre-pre-conceptual design to detailed design, other methods such as expert review, operational experience, or insights from other hazard analysis methods such as PRA may be used to expand the list of design basis events of interest. As the list of events expands, some events may be selected as bounding and representative of a class of events and allow consolidation of the deterministic design basis event list.

5.5.3.3 Ranking initiating events

The fourth step in the deterministic design basis analysis methodology is assigning a qualitative event frequency class to each of the initiating events. Each of the initiating events in Table 5.10 is assigned a qualitative event frequency class based on historic operations at tritium storage facilities and engineering judgment.

In this work, the limited design information available for the facility largely limits acceptance criteria to technology neutral performance criteria. A regulatory hazard limit of total exposure or dose limits is selected as the analytic end point for this deterministic design basis analysis. This limit allows for incorporation of dispersion mitigation SSCs in analyses and alignment with prior regulatory guidance related to the safe handling of radioactive materials. It also eliminates the need to have more detailed site-specific information for lower hierarchical hazard limits. Note that other hazard consequence limits (e.g., inventory hazard limits) could be used with this type of analysis but would inherently exclude crediting SSCs that enable mitigation of releases. The regulatory limits (given in in Table 5.11 are proposed for this analysis based on precedent and guidance from the NRC and DOE on the design basis of nuclear and tritium facilities.

Table 5.11. Offsite hazard consequence acceptance limits at exclusion area boundary for design basis event frequency classes

Event Frequency	*Dose (rem)*	*Acceptance Limit Basis*
NO	< 0.1	Total dose limit for any license activities from 10 CFR 20.1301(a)(1)
AOO		
IE	2.5	Reduced dose limit defined as "small fraction" of 10 CFR 100 off-site dose limit of 25 rem [(1)]
LE	25	Total off-site dose limit from 10 CFR 100

Notes:
1. Limit based on precedent from Chapter 15 Design Specific Review Standard for NuScale SMR Design [69]

5.5.3.4 Developing event sequences

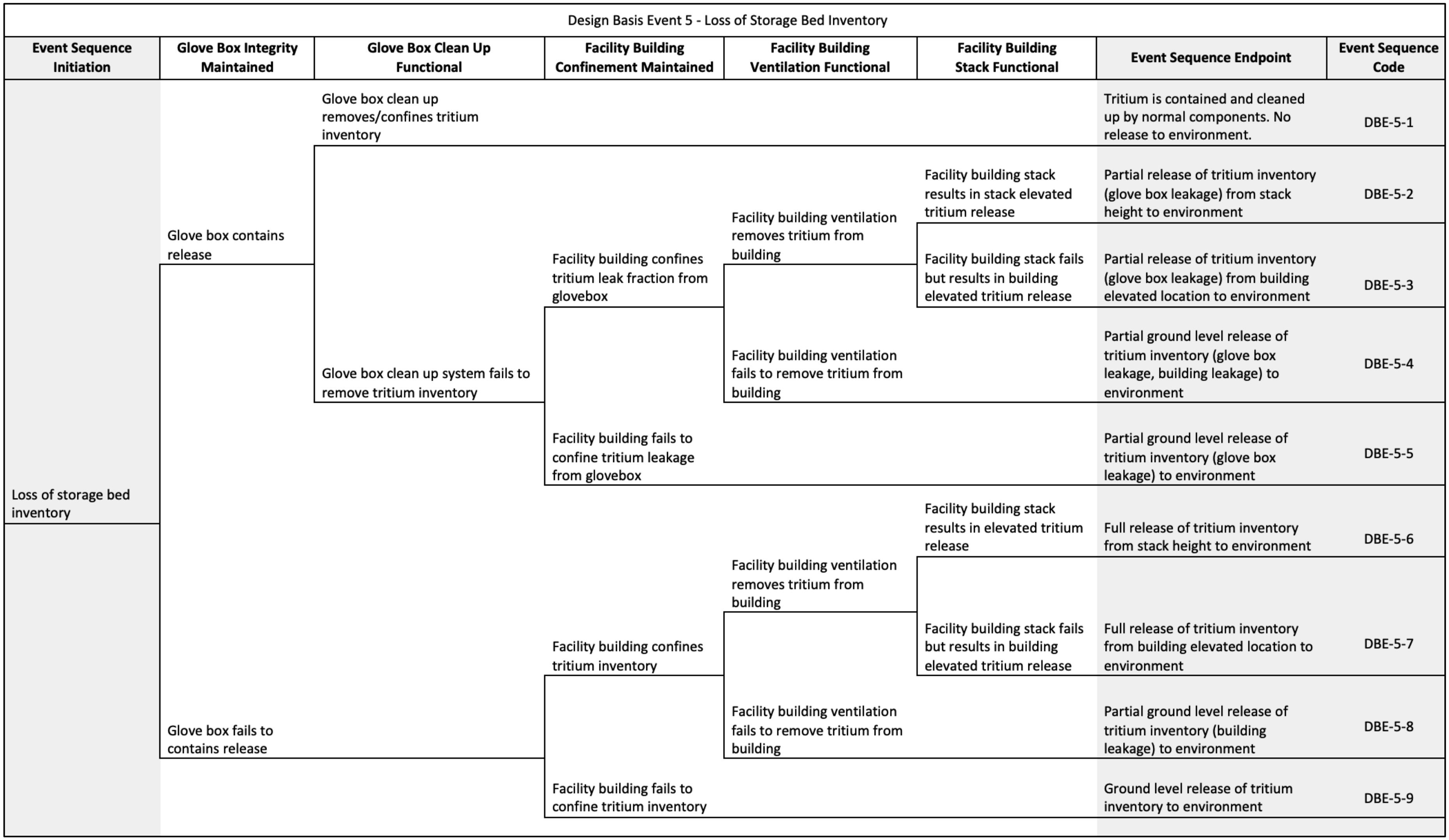
The fifth step in the deterministic design basis analysis methodology outlined in Section 5.5.2 is to develop event sequences for bounding event sequences based on plant design. In this work, the event sequences are limited to the deuterium tritium storage system described in Appendix 5B and the design basis events listed in Table 5.10. In a complete deterministic design basis analysis of this system, event sequences for the five non-BDBA design basis events would need to developed and analyzed to ensure compliance with the appropriate acceptance limits in Table 5.11, unless it could be shown that a licensing of an event could be used to bound other licensing basis events under all conditions.

In this work, event sequences are developed for the most severe design basis event. Design Basis Event 5, ("Loss of storage bed inventory") is classified as the only design basis LE for the D-T storage system. This event is selected as the most severe design basis event for this system, and an event sequence is developed to identify event sequences for this design basis event. Figure 5.4 shows the simplified event sequence for Design Basis Event 5 (DBE-5). Note that in this simplified analysis, only subsystem level events affecting systems or components discussed in Appendix 8B are discussed. With additional design information, event sequences could be developed for individual sequence events (e.g., "Glove box clean up systems fails to remove tritium inventory") to identify more specific system or component dependencies in event sequences.

The development of event sequences for DBE-5 resulted in nine event sequences. Recommendations on crediting SSC safety functions were conducted based on a review of the event sequences and preliminary estimates of off-site consequences. Preliminary scoping analyses were conducted for the nine event sequences developed in Figure 5.4 using best estimates of release fractions and release locations with the same conservative meteorological release conditions assumed for the worst-case analysis (1 m/s wind speed, Class F atmospheric stability, 2 hour Gifford plume meander, and countryside surface roughness). Table 8.12 summarizes the results of each of these preliminary estimates of off-site consequences.

Of the nine events, three events sequences (DBE-5-1, DBE-5-2, and DBE-5-6) are automatically considered design basis event sequences because the event sequences involve the failure of zero or one SSC, regardless of whether SSCs were credited with safety functions. The off-site consequences of these three event sequences meet the regulatory acceptance limits in Table 5.10 for limiting events (25 rem). With the exception of DBE-5-6, the resulting doses are sufficiently low that they would meet the regulatory acceptance limit for normal operation (0.1 rem). Of the remaining six event sequences, the off-site consequences for three event sequences (DBE-5-3, DBE-5-4, and DBE-5-5) are small enough that they meet the regulatory acceptance limit for both limiting events and normal operation.

Three event sequences (DBE-5-7, DBE-5-8, and DBE-5-9) have off-site consequences that challenge or exceed the limiting event regulatory acceptance limit of 25 rem. In these three event sequences, failure of the glove box confinement system results in release of the full radiological inventory to the facility building and a secondary failure of the failure the facility building stack, ventilation, or building confinement allows a large ground or near ground level release. Note that ground level release of the full storage bed inventory (DBE-5-9) represents the worst-case release analysis for this system.



Design Basis Event 5 - Loss of Storage Bed Inventory

Event Sequence Initiation	Glove Box Integrity Maintained	Glove Box Clean Up Functional	Facility Building Confinement Maintained	Facility Building Ventilation Functional	Facility Building Stack Functional	Event Sequence Endpoint	Event Sequence Code
Loss of storage bed inventory	Glove box contains release	Glove box clean up removes/confines tritium inventory				Tritium is contained and cleaned up by normal components. No release to environment.	DBE-5-1
		Glove box clean up system fails to remove tritium inventory	Facility building confines tritium leak fraction from glovebox	Facility building ventilation removes tritium from building	Facility building stack results in stack elevated tritium release	Partial release of tritium inventory (glove box leakage) from stack height to environment	DBE-5-2
					Facility building stack fails but results in building elevated tritium release	Partial release of tritium inventory (glove box leakage) from building elevated location to environment	DBE-5-3
				Facility building ventilation fails to remove tritium from building		Partial ground level release of tritium inventory (glove box leakage, building leakage) to environment	DBE-5-4
			Facility building fails to confine tritium leakage from glovebox			Partial ground level release of tritium inventory (glove box leakage) to environment	DBE-5-5
	Glove box fails to contains release		Facility building confines tritium inventory	Facility building ventilation removes tritium from building	Facility building stack results in elevated tritium release	Full release of tritium inventory from stack height to environment	DBE-5-6
					Facility building stack fails but results in building elevated tritium release	Full release of tritium inventory from building elevated location to environment	DBE-5-7
				Facility building ventilation fails to remove tritium from building		Partial ground level release of tritium inventory (building leakage) to environment	DBE-5-8
			Facility building fails to confine tritium inventory			Ground level release of tritium inventory to environment	DBE-5-9

Figure 5.4. Event sequences for D-T Storage System for Design Basis Event 5

Table 5.12. Preliminary offsite consequences scoping analyses for D-T Storage System Design Basis Event 5

Event Sequence	*Failed SSCs*	*Failed SSCs*	*Peak off-site dose (rem)*	*25 rem dose distance (m)*	*1 rem dose distance (m)*
DBE-5-1	0	None	N/A	N/A	N/A
DBE-5-2	1	Glove Box Clean Up	1.6E-05	N/A	N/A
DBE-5-6	1	Glove Box Confinement	0.167	N/A	N/A
DBE-5-3 (Note 1)	2	Glove Box Clean Up, Facility Building Stack	7.3E-4	N/A	N/A
DBE-5-4	2	Glove Box Clean Up, Facility Building Ventilation	4.5E-3	N/A	6.9
DBE-5-5	2	Glove Box Clean Up, Facility Building Confinement	2.9E-2	N/A	10.9
DBE-5-7 (Note 1)	2	Glove Box Confinement, Facility Building Stack	7.31	N/A	2520
DBE-5-8	2	Glove Box Confinement, Facility Building Ventilation	44.6	224	1549
DBE-5-9	2	Glove Box Confinement, Facility Building Confinement	99.11	360	2662

Note 1: These event sequences model an elevated release from a building based on a elevated release source but does not include building wake effects which may be significant depending on the building. Dose calculations near the release point (e.g., within 500 m) may be significantly higher [24].

In order to meet the regulatory limits without changing overall system architecture or analysis assumptions (e.g., use of conservative site specific meteorological data to reduce excess conservatisms), the different systems can be designated as having credited safety functions. As previous discussed, the simultaneous failure of two or mote independent, safety credited SSCs is highly unlikely; event sequences containing two or more safety credited are considered beyond design basis events.

In this analysis, four systems are designated as safety credited SSCs:

- Glove Box Confinement
- Facility Building Confinement
- Facility Building Ventilation
- Facility Building Stack

Designating these four systems as safety credited SCCs allows DBE-5-4, DBE-5-5, and DBE-5-7 to be classified as beyond design basis event sequences because the event sequences require the simultaneous failure of two or more safety credited systems. As a result, the design basis event sequences for D-T Storage System for Design Basis Event 5 are limited to DBE-5-1 through DBE-5-6.

This process for designation of safety credited SSCs eliminated the need for crediting the Glove Box Clean Up System with an important safety function due to it's relatively small impact on event sequence consequences. While this may be a minor system, reducing the regulatory burden associated with a safety credited SSC can reduce the regulatory, design, construction, and operational costs associated with the system and cumulatively impact overall system economics and operations.

It is important to note that in this analysis, the Facility Building Stack was designated as a safety credited SSC. While the event sequence that assumed its failure (DBE-5-7) still met the regulatory acceptance criteria, the calculated off-site dose of 7.31 rem was significantly higher than the doses associated with the next most severe event sequence (DBE-5-6: Glove Box Confinement Failure) with a calculated off-site of 0.167 rem, below the regulatory guideline for off-site evacuation. Due to this cliff edge effect in dose and the ability to provide significant regulatory margin with the designation of a single safety related SSC, the Facility Building Stack was designated as a safety credited SSC. One drawback of this designation may be cost associated with design, construction, and operation (as well as it's impact on surrounding SSCs) of the Facility Building Stack as a safety credited SSC. Later evaluation by an applicant may suggest that the potential regulatory and social license issues associated with higher design basis event sequence consequences may outweigh the costs associated with designating the Facility Building Stack with a credited safety function.

This process of developing event sequences for initiating events, designating SSCs with safety credited functions, and classifying the events as design basis or beyond design basis events would need to be repeated for each of the initiating events classified as NO, AOO, IE, or LE in Table 5.10. Events classified as NO are not normally considered as part of the accident analysis but would be included in the operational regulatory requirements for the facility. Events classified as BDBA are not considered as part of the accident analysis but would be included in the extended BDBA scoping analyses.

5.5.3.5 Evaluate bounding event sequences

The sixth step in the deterministic design basis analysis methodology outlined in Section 5.5.2 is analyzing event sequences for bounding event sequences. Table 5.13 summarizes the nine event sequences, whether they are classified as design basis or beyond design basis events. For the six design basis event sequences, formal calculations would need to be prepared to demonstrate that the sequence consequences meet the regulatory acceptance criteria using conservative assumptions. If it can be shown using qualitative and quantitative arguments that one event sequence (e.g., DBE-5-6) bounds all other event sequences (i.e., results in the lowest margin to regulatory acceptance criteria), then a formal calculation may only be required for that event sequence.

Table 5.13. Classification of D-T Storage System Design Basis Event 5

Event Sequence	*Event Sequence Classification*	*Peak off-site dose (rem)*	*25 rem dose distance (m)*	*1 rem dose distance (m)*
DBE-5-1	Design Basis Event	N/A	N/A	N/A
DBE-5-2	Design Basis Event	1.6E-5	N/A	N/A
DBE-5-6	Design Basis Event	0.167	N/A	N/A
DBE-5-3	Design Basis Event	7.3E-4	N/A	N/A
DBE-5-4	Design Basis Event	4.5E-3	N/A	6.9
DBE-5-5	Design Basis Event	2.9E-2	N/A	10.9
DBE-5-7	Beyond Design Basis Event			
DBE-5-8	Beyond Design Basis Event			
DBE-5-9	Beyond Design Basis Event			

A formal engineering analysis documenting the evaluation of DBE-5-6 is outside the scope of this work but would need to be performed for a full deterministic design basis analysis. This calculation would document the conservative assumptions, inputs, and methods used to determine the hazard consequences for the particular event sequence. Use of engineering consensus codes and standards can help standardize these calculations and provide additional justification for assumptions and methods. The engineering analysis documenting the hazard consequences of DBE-5-6 would be performed to confirm that the peak off-site dose meets the relevant regulatory acceptance criteria. In this work, it is assumed that the formal engineering analysis would confirm the conservative off-site dose of 0.167 rem previously calculated for DBE-5-6 is the bounding hazard consequence and satisfies regulatory requirements for LE.

5.5.3.5 Qualifying safety credited systems

The seventh step in the deterministic design basis analysis methodology outlined in Section 5.5.2 is to perform qualification design analyses for any SSCs that are credited with safety functions. Based on the design basis event sequences discussed in Section 5.5.3.4 for DBE-5, supporting qualification analyses would need to be prepared for the following systems:

- Glove Box Confinement
- Facility Building Confinement
- Facility Building Ventilation
- Facility Building Stack

These analyses must demonstrate that these systems can perform their safety function for all design basis conditions (Section 5.5.3.1) with appropriate margin and support the conclusions of the design basis safety analyses. These analyses can be based on guidance from professional organizations or engineering consensus codes and standards (e.g., ASME, ASCE) can help standardize these calculations and provide justification for assumptions and methods.

Performing these calculations is outside of the scope of this work. These calculations are fairly standard in the design and analysis of components in commercial nuclear industry but may require substantial effort or engineering expertise to complete. Due to these limitations, these qualification design analyses will not be conducted for the credited SSCs discussed above. This process would need to be repeated for an SSC in the facility with credited with performing a safety function.

5.5.3.7 Developing special events and beyond design basis events

The eighth step in the deterministic design basis analysis methodology outlined in Section 5.5.2 is to develop special events and beyond design basis events and event sequences for plant systems. In this work, beyond design basis events and special events are reviewed for the D-T Storage System. In Section 5.5.3.2, two beyond design basis events were identified that challenged the confinement of radiological material critical safety function: "loss of multiple storage bed inventory" and "simultaneous loss of storage bed inventory and glove box integrity".

These two events were classified as beyond design basis because they are not expected to occur during the operational lifetime of any fusion facilities (based, in part, on operating experience from large tritium storage facilities) but are phenomenologically possible. The first event involves the simultaneous release of the radiological inventory from more than one tritium storage bed (up to the release of all storage bed inventories). The second event involves the simultaneous failure release of the radiological inventory a tritium storage bed and the failure of the glove box confinement, resulting in the full tritium inventory releasing into the surrounding facility building. These two events require common cause failures (e.g., internal fire or seismic events) or multiple independent failures to occur but would result in significant radiological inventories bypassing several engineering safety features. Additional beyond design basis events may be identified and considered for this system if the list of possible initiating events were expanded based on new fundamental safety function or revised system design.

In Section 5.5.3.4, three beyond design basis event sequences were identified for DBE-5 (loss of storage bed inventory):

- DBE-5-7: failure of glove box confinement and facility building stack
- DBE-5-8: failure of glove box confinement and facility building ventilation
- DBE-5-9: failure of glove box confinement and facility building confinement

Designation of the failed SSCs with safety functions (and the associated quality requirements for the SCCs to ensure safety function performance under design basis conditions) results in a beyond design basis event sequence designation for each of these three event sequences. These event sequences, similar to the beyond design basis events previously discussed, all possible given a common cause failure mechanism or multiple independent failures of the safety credited SSCs. In a complete deterministic design basis analysis, additional beyond design basis event sequences would likely be identified based on development of event sequences for the other design basis initiating events listed in Table 5.10.

Based on the pre-conceptual system design described in Appendix 5B and the published experience with large tritium storage facilities at the Darlington Tritium Removal Facility for CANDU reactors [66] and the Tritium Extraction Facility [67], no special events are identified for inclusion in the deterministic design basis analysis for the D-T Storage System. Future regulatory reviews or operational experience may introduce new special events for consideration with the beyond design basis events.

Event sequences were also reviewed for defense-in-depth considerations. In this work, the design of the facility has multiple, diverse, and independent physical barriers to the release of radiological material (storage bed, glove box, facility building) and multiple diverse methods to mitigating initiating events (glove box clean-up and building ventilation to stack release). Event sequences with common cause failure mechanisms that could lead to the failure of multiple, independent safety function credited SSCs are already discussed as part of the beyond design basis event sequences discussed above.

While the multiple, diverse, and independent physical barriers to the release of radiological material constitute, in part, plant capacity defense-in-depth, additional plant capacity against common cause failure mechanisms (e.g., internal fire) could be useful at increasing facility robustness. The identification and evaluation of these needs is outside of the scope of this work but should be considered in a full deterministic design basis analysis. Additionally, programmatic defense-in-depth attributes related to SSC reliability, operation, and performance (both SSC and human) are not discussed in this work due to the pre-conceptual nature of both design and the concept of operations but should be considered in a full deterministic design basis analysis.

In this work, two beyond design basis initiating events and three types of event sequences are reduced to four bounding event sequences for analysis and review.

- Single storage bed inventory, with unmitigated ground level release
- Double bed inventory, with building mitigated ground release
- Half system inventory, with elevated release
- Full system inventory, with design basis stack release

These four beyond design basis event sequences are intended to provide insights into the order of magnitude of accident consequences, and trade-offs between the effects of different engineered safety features and radiological inventories. It is clear that the limiting BDBA would converge on to the worst-case release event – a ground level release of the full system inventory with no mitigation. While this event may be fully bounding, the number of failures required to produce it is considered outside the scope of the analysis and does not result in useful regulatory safety insights.

This work only addresses these four beyond design basis event sequences based on the limited scope of the deterministic design basis analysis work performed. In a complete deterministic design basis analysis, a larger set of beyond design basis events would need to be considered and be down selected to determine the bounding event sequences most relevant and to the facility.

5.5.3.8 Quantifying beyond design basis events

The ninth step in the deterministic design basis analysis methodology outlined in Section 5.5.2 is to perform safety analyses to quantify hazard consequences for the selected beyond design basis event sequences. Table 5.14 summarizes the four beyond design basis event sequences considered as a part of this work. In the four cases, realistic release conditions were used to calculate the dose consequences (4.5 m/s wind speed, atmospheric stability Class D, countryside surface roughness, and 2 hour Gifford meander). These inputs are intended to provide insights into the facility safety profile and to examine potential cliff-edge effects relate to certain engineering safety features or common-cause failure mechanisms. In reviewing the four analyzed BDBA event sequences, it is important to note that the 25 rem dose limit is a recommended off-site maximum dose for any radiological incidents [37] while the 1 rem dose limit is the lower protective action guide (PAG) for shelter in place or evacuations during radiological incidents [19].

Table 5.14. Beyond Design Basis Event Consequence Summary

Event Sequence	*Tritium Source Term (g)*	*Tritium Release Fraction*	*Release Height (m)*	*Peak off-site dose (rem)*	*25 rem dose distance (m)*	*1 rem dose distance (m)*
BDBE-1	70	1	0	5.239	N/A	413
BDBE-2	140	0.45	0	4.715	N/A	388
BDBE-3 (Note 1)	700	1	10	19.43	N/A	1637
BDBE-4	1400	1	50	1.29	N/A	1823

Note 1: This sequence models an elevated release from a building based on an elevated release source but does not include the building wake effects which may be significant depending on the building. Dose calculations near the release point (e.g., within 500 m) may be significantly higher [24].

Review of these four beyond design basis event sequences reveals several important features about the overall safety of the system as assessed using a deterministic design basis analysis.

First, the calculated dose consequences of BDBE-1 can be compared with the calculated dose consequences of DBE-5-9 in Table 5.12. The event sequence DBE-5-9 also described the ground level release (0 m) of a full storage bed inventory (70 g) but assumed worst-case meteorological conditions. Table 5.14 compares the two event sequence release conditions and calculated dose consequences. The difference between these two cases highlights the impact of local meteorological release conditions on off-site consequences. While additional mitigating factors are not likely needed for this system, this difference in dose consequence highlights the need to have assurance of the low likelihood of simultaneous occurrence of the initiating event (storage bed inventory loss), system failures (glove box confinement, facility building), and worst case weather conditions (uncontrollable). This assessment points towards the importance of programmatic defense-in-depth considerations when it comes to preventing beyond design basis accidents.

Table 5.14. Beyond Design Basis Event Consequence Summary

Event Sequence	*Release Conditions*		*Calculated Dose Consequences*		
	Wind speed (m/s)	*Atmospheric stability class*	*Peak off-site dose (rem)*	*25 rem dose distance (m)*	*1 rem dose distance (m)*
BDBE-1	4.5	D	5.239	N/A	413
DBE-5-9	1	F	99.1	360	2662

Second, review of BDBE-2 illustrates the potential benefits of mitigating safety in the reduction of off-site consequences for beyond design basis event sequences. The BDBE-2 sequence postulated the simultaneous initiating failure of two tritium storage beds, as well the failure of the glove box confinement and building ventilation and exhaust systems. In this sequence, the facility building is able to confine and slow the release of tritium into the environment both reducing the total source term released (accounted for the analysis) and could provide a time delay to allow for other mitigating actions (such as off-site evacuations or shelter in place). In the case of BDBE-2, off-site doses (4.7 rem) do not exceed the 25 rem dose limit but do exceed the 1 rem PAG. In this case, consideration of emergency planning (either formal or informal) may be warranted to help ensure public health and safety even during extremely low probability, catastrophic events. For this event sequence, the doses are sufficiently low and the 1 rem dose distance is sufficiently close (388 m) that major off-site emergency planning programs may not be needed.

Third, comparison and review of BDBE-3 and BDBE-4 illustrate the importance of common-cause catastrophic events and engineered safety features that can effectively mitigate catastrophic releases. Both BDBE sequences involve the failure of a large numbers of tritium storage beds (50% and 100% of total storage inventory, respectively). BDBE-3 additionally assumes failures of the glovebox confinement and the facility building stack resulting in an elevated release (top of facility building) of the 50% of the tritium inventory. BDBE-4 assumes failures of the glovebox confinement but successful release of 100% of the tritium inventory through the facility building stack.

In these two cases, the massive tritium source terms are due to the simultaneous (or rapidly sequential) failure of a large number of tritium storage beds. This is likely a function of a common cause failure mechanism that can cause significant facility damage and exceed the thermo-mechanical capacity of the storage beds and HIVES. Review of the design characteristics of the tritium storage beds and the flammable nature of the hydrogen suggests that large internal fire event would be most likely common cause failure mechanism for a large number of tritium storage beds. Thus, additional plant capability defense in depth and programmatic controls may be implemented to prevent and mitigate internal fire events both inside and outside of the glove boxes that could lead to common cause failure of multiple beds. Controls such as limiting presence of flammable materials, inerting the glove box environment with nitrogen, or implementation of additional fire detection and suppression systems would strengthen the overall defense in depth characteristics of the facility. Note that these systems are not credited in the analysis with a safety function, so they would not be subject to the additional regulatory burden associated with safety credited SSCs thus providing additional safety at reduced cost. Review of system design and associated failure mechanisms could indicate which additional safety features could be most effective at reducing common cause failure mechanisms.

The second major takeaway from comparison of BDBE-3 and BDBE-4 is the significant impact of the elevated stack release on the calculated near-field dose consequences but the limited impact of this engineered safety feature on far-field dose consequences. The maximum off-site dose consequences (primarily near-field consequences) calculated for BDBE-4 are less than one twentieth the maximum off-site dose consequences for BDBE-3 (1.3 rem vs 19.4 rem) despite a doubling of the total released radiological inventory (1400 g vs 700 g). Crediting the 50 meter facility building stack and the facility building ventilation system enables the wide range dispersion of the radiological source term. These features minimize the maximum off-site consequences to below the regulatory consequence limits for LE (25 rem) and comparable to the regulatory consequence limits for IE (2.5 rem) in Table 5.11. This highlights the importance of these engineered SSC in mitigating the releases associated with large inventories. This analysis suggests that prioritizing the programmatic DID associated with the facility building stack and the facility building ventilation could have a large impact on BDBA where large inventories cannot fully confined and reduce near-field off-site consequences to acceptable levels.

While these engineered safety features create significant dispersion of the source term and minimize maximum acute exposures, they still result in the release of large quantities of radionuclides over wide areas. While the near field doses for BDBE-4 are significantly lower than for BDBE-3, the distance to the 1 rem dose boundary is larger for BDBE-4. Figure 5.5 illustrates the dose-distance relationship for different release elevations, all other release conditions held constant. While the near field effects differ significantly for different release heights due to the initial elevation of the plume centerline, the off-site consequences converge the plume disperses and touches down off-site. For sufficiently large releases of radiological releases, elevated plume dispersion may reduce the off-site site consequences associated with release but will not eliminate them. This highlights that for BDBAs with large radiological inventories, use of safety credited SSCs to disperse are not a panacea. Plant capacity and programmatic defense in depth that reduce vulnerable radiological inventories should be implemented to improve facility but may not be required as part of the licensing basis of a facility.

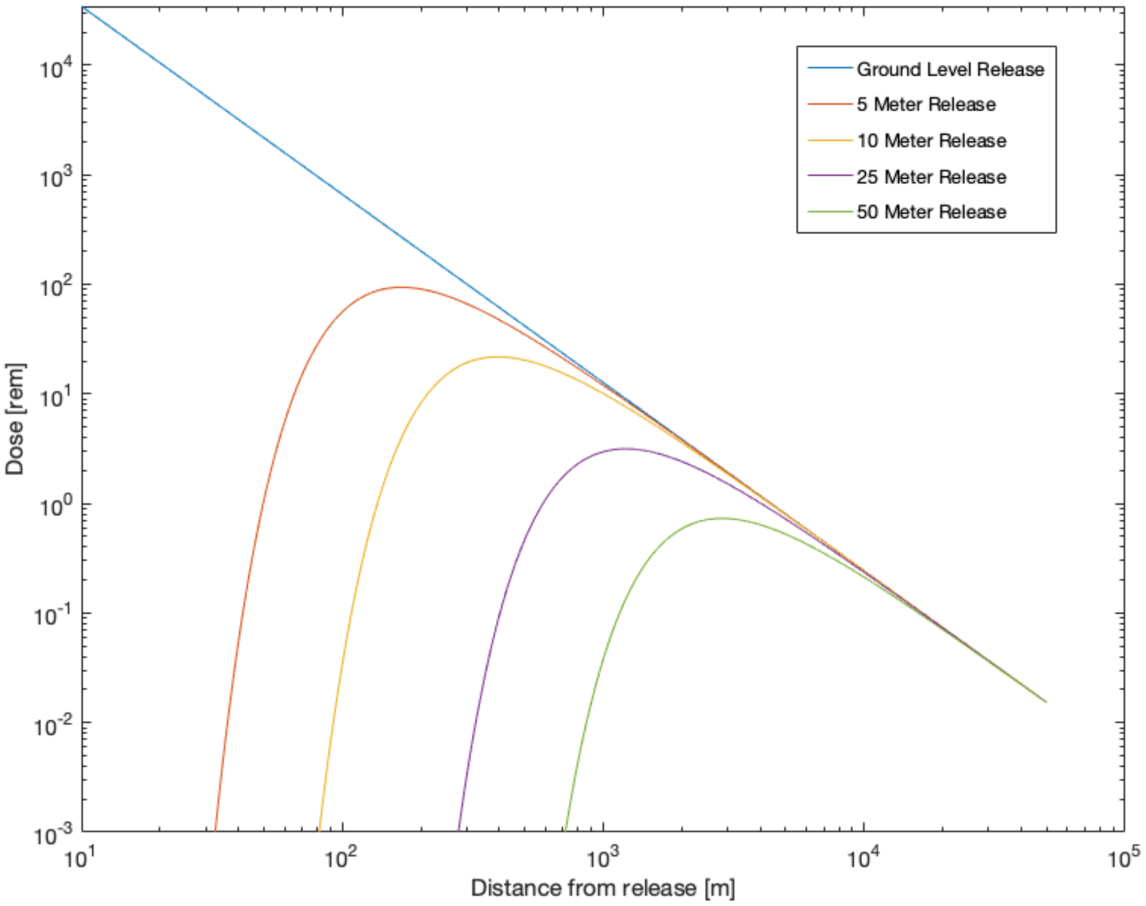


Figure 5.5. Off-site dose consequences as a function of distance from release and initial plume release height.

5.5.3.9 Summary of deterministic design basis analysis results

The deterministic design basis analysis performed in this work for the D-T storage system provided preliminary assurance that the system could meet relevant regulatory limits for acute, off-site release of radiological material. To meet relevant regulatory limits using the preliminary design in Appendix 5B, five SSCs were designated as performing safety-credited functions:

- Tritium Storage Bed with HIVES
- Glove Box Confinement
- Facility Building Confinement
- Facility Building Ventilation
- Facility Building Stack

These safety credited SSCs would have additional requirements on design, manufacturing, and operation to ensure that they can perform their safety credited function under all design basis conditions.

For the limited set of initiating events analyzed in this work, the limiting design basis event sequence resulted in an off-site dose of 0.167 rem using conservative calculation assumptions and did not require any additional off-site emergency response actions to meet existing regulatory guidelines. Formal documentation and review of this bounding safety analysis would be required to ensure that the regulatory limits are met under all design basis conditions and postulated initiating events.

Beyond design basis events were also evaluated for the systems and events considered as part of the deterministic design basis analysis. These analyses highlighted several important defense-in-depth considerations including:

- impact of internal fire prevention, detection, and mitigation to reduce the likelihood of common-cause tritium storage bed failure mechanisms
- importance of programmatic defense-in-depth considerations to ensure high reliability of the facility building ventilation and stack for severe accidents
- potential benefits of some off-site emergency planning to enable consequence mitigation during some beyond design basis event sequences

These considerations should not necessarily be translated directly into regulatory requirements for the facility but should be considered by the designer to increase overall facility robustness against initiating events, account for uncertainties, and increase overall facility safety.

5.5.4 Advantages and challenges of deterministic design basis analysis

Deterministic design basis analyses enable consideration of engineered safety features in safety analysis, reducing excess conservatism present in worst-case and maximum credible release analyses and incorporating the importance of engineering design in the safety of systems and facilities.

The major advantage of deterministic design basis safety analyses is that they enable the use of engineering safety systems in the control of hazards and the prevention and mitigation of hazard consequences. Unlike worst-case analyses or maximum credible release analyses, engineered safety feature that prevent events or mitigate the consequences of events can credited in safety analyses to reduce the hazard consequences. It may be possible to demonstrate that some systems with a sufficient number of diverse, independent engineered safety features do not have design basis events that result in releases of radiological material. This ability to credit engineered safety features is complimented by a review of the defense-in-depth considerations for facilities to identify possible common-cause failure modes and identify changes to the design, construction, or operational basis of a facility to increase robustness against low probability, catastrophic events.

An additional advantage of deterministic design basis safety analyses is a standardized method to exclude events that are qualitatively judged to be sufficiently low probability. Use of the single failure criterion and characterization of events requiring multiple, independent failures as beyond design basis help to focus the safety analysis to events that will credibly occur during facility or fleet operations. Use of a graded regulatory hazard consequence acceptance criteria reflects this more rational approach to events and hazard consequences.

Overall, deterministic design basis analyses provide conservative evaluation of facility safety while still enabling a realistic evaluation of the impacts of engineered safety features on the hazard consequences associated with facility hazards.

The major challenges of deterministic design basis safety analyses are the definition of the design basis for a facility, the burden of proof required for SSCs with credited safety functions, the level of regulatory burden associated with the analyses, and the potential for non-bounding analyses and event sequences.

The first challenge of deterministic design basis safety analyses is defining an appropriate design basis for an activity or a facility. As part of the first step in a deterministic design basis safety analysis as outlined in Section 5.4.2 is to define the design basis for the facility, specifically the limiting design conditions from internal and external events that SSCs with credited safety functions must be designed for. The challenge of defining the design basis is determining what level of conservatism is needed when establishing these limits.

The underlying issue is a risk of exceedance (both the probability of exceedance and the consequence of exceedance) for the design basis. For example, GDC-2 in Appendix A of 10 CFR Part 50 on the design of fission facilities for natural phenomena design basis states that the design basis of the SSCs should include [60]:

> "(1) appropriate consideration of the most severe of the natural phenomena that have been historically reported for the site and surrounding area, with sufficient margin for the limited accuracy, quantity, and period of time in which the historical data have been accumulated,
> (2) appropriate combinations of the effects of normal and accident conditions with the effects of the natural phenomena and
> (3) the importance of the safety functions to be performed."

The process of determining the site appropriate parameters can be resource intensive if data sets are not already available and the definition of "sufficient margin" present regulatory challenges. The process of developing, selecting, and providing an acceptable regulatory justification for all possible design basis condition could present a significant regulatory burden for applicants.

Standardized sets of design basis requirements can simplify the process for applicants and regulators. NRC Regulatory Guide 1.221 provides design basis conditions for hurricanes for U.S. fission plants based on a combination of historical data and simulations that is intended to provide conditions with a 1e-7 (1 in 10 million year) annual probability of exceedance [70]. This standardized approach can be extremely useful for reducing the applicant's regulatory burden associated with design basis events but can require significant regulatory infrastructure or support from professional standards organizations to develop design basis requirements for a new type of facility.

The second major challenge of deterministic design basis analyses is the burden of proof required for SSCs with credited safety functions. Based on existing practices for SSCs with credited safety functions in nuclear applications this burden of proof (Appendix B of 10 CFR Part 50) may consist of additional assurances and documentation, calculations, and procedures related to "designing, purchasing, fabricating, handling, shipping, storing, cleaning, erecting, installing, inspecting, testing, operating, maintaining, repairing, refueling, and modifying" SSCs [60]. This practice of "nuclear quality assurance" can present a substantial regulatory burden and extend from SSCs with credited safety functions to supporting auxiliary systems such as Plant Utility Systems for electricity or other common utilities. For SSCs with credited safety functions, this additional regulatory burden can come at a significant cost increase if not properly managed. Review of standard quality assurance practices related to SSCs with credited safety functions at nuclear power plants suggest that process is subject to significant regulatory judgment and can introduce large uncertainties into the regulatory process [42]. Minimizing the number of SSCs with credited safety functions required to meet applicable regulatory limits is advisable both in terms of inherent plant safety and economic viability.

The third major challenge of deterministic design basis analyses is the level of regulatory burden associated with the analyses. A deterministic design basis analysis consists of roughly three sets of evaluations, analyses, and calculations: design basis event selection and evaluation, beyond design basis event evaluation, and safety credited SSC evaluation. The first two analyses (event selection and evaluation) require full review of plant hazards and plant design details to identify possible failure sequences. These analyses require detailed information on the physical and operational design of SSCs to identify system and component level interactions, and to determine system behavior given off-normal conditions. Given sufficiently complex systems, the number of events and event sequences can grow exponentially. While the final regulatory analysis may be condensed to a bounding set of event sequences requiring full documentation, development of this bounding set requires consideration and review of all events within the design basis. The final analysis (safety credited SSC evaluation) require a comprehensive analysis of SSCs for all design basis conditions. This may involve both physical qualification of SSCs to determine performance parameters and analytic qualification of SSCs under thermo, mechanical, radiation, or electrical conditions. The analytic evaluation of SSCs that rely on computational models, simulations, or correlations may require additional qualification processes to verify and validate the applicability and results of these analytical tools [71]. The cumulative regulatory burden from all of these analyses, qualifications, and documentations can be extremely resource intensive, especially for complex SSCs comprised of any active subsystems.

In this work, a simplified deterministic design basis analysis was outlined for a single simple passive storage system for a single initiating event. Completing the licensing evaluations just included in the scope of this work using deterministic design basis analysis method would require:

- formal completion of the design basis condition design basis event sequence selection evaluations,

- justification and evaluation of the limiting design basis event sequences,
- evaluation of the beyond design basis event sequences and
- development of mitigating actions to prevent or mitigate consequences, and
- documentation of design basis calculations for the five SSCs with credited safety functions (including at least one active engineered safety feature with multiple additional failure mechanisms – facility building ventilation).

The D-T storage system is one of 17 systems from the Level 3 System Engineering model with all four significant off-site hazards identified in Chapter 7. Expansion of the deterministic design basis analysis facility wide (especially for more complex engineering systems) would create a significant regulatory burden for the facility.

The fourth major challenge of deterministic design basis analyses is ensuring that the documented analyses bound all possible event sequences. The process of developing a design basis and determining which events sequences are included in or beyond the design basis inherently reduces the hazard space considered for safety analysis. This reduction is intended to focus analyses on events that are physically possible but the reduction process relies on assumptions related to SSC performance, initiating events, and the ability of analysts to correctly identify bounding event sequences.

One significant challenge with this hazard space reduction process is that for complex engineered systems, it may be difficult (or impossible) to characterize all possible system interactions that may lead to an accident or loss [72]. On paper, the Union Carbide facility in Bohpal had redundant, independent safety systems but breakdowns in programmatic defense-in-depth during operation invalidated assumptions related to independence and ultimately enabled progression of the 1984 accident [73].

The other significant challenge with the hazard space reduction process is that the process may exclude design basis conditions, initiating events, or event sequences that are considered exceedingly unlikely and beyond the design basis. While this process is effective at limiting the scope of the licensing process to credible events, it is based on expert understanding of event likelihood and acceptable risk. For example, the tsunamis associated with the 2011 Fukushima Diachii nuclear disaster exceeded the design basis tsunamis height of the facility; plant owners and regulators had considered such an event improbable and thought that the facility would not be compromised event if the event occurred [74]. Performing beyond design basis event analyses and consideration of additions to plant capability and programmatic defense-in-depth can be help mitigate the risks posed by these excluded events and increase the robustness of the facility to non-bounded events and event sequences.

5.5.5 Deterministic design basis analysis summary

Use of deterministic design basis analyses for licensing evaluations reduces conservatism from simpler analysis methods and enables the consideration of engineered safety features in hazard consequence analyses. These analyses allow analysts to control significant hazards through the use of active and passive engineered safety features. This approach significantly reduces the calculated hazard consequences for a facility or activity but come at the cost of increased burden of proof and regulatory burden related to SSCs significant safety and supporting analyses. This would dramatically increases the regulatory costs associated with facility licensing to beyond those currently implemented for chemical industries to those comparable for commercial fission. The tradeoffs between these design and analysis flexibility versus additional regulatory burden and process requirements should be considered when determining if this analysis method is appropriate for specific commercial fusion facilities.

5.6 Probabilistic design basis licensing evaluation

The fourth licensing evaluation method proposed for commercial fusion technology is the probabilistic design basis method. The probabilistic design basis analysis is an extension of the deterministic analysis that seeks to formally quantify the importance of different events and events sequences based on the likelihood and consequence of the event. While the deterministic design basis analysis uses qualitative principles to include or exclude events from the design basis of a facility, the probabilistic design basis analyses uses risk insights to determine the importance of different aspects in licensing. Risk is defined in this work based on the "risk-triplet": what can go wrong, what is the probability of occurrence, and what are the consequences of occurrence 41.

The purpose of the probabilistic design basis analysis is to utilize risk information to better inform event sequence based safety analysis methods and focus safety activities on those with the highest risk (probability and consequence). These analyses are probabilistic because they explicitly include the probability of event sequences when evaluating the acceptability of hazard consequences.

A probabilistic design basis analysis has several characteristics:

- Quantification of the probability of different event sequences for both internal and external events
- Explicit analysis of a set of internal and external initiating events that are considered as part of the licensing basis for the facility
- Event sequences that describe plant response to initiating events
- Fault trees that describe and quantify the probability of intermediate events
- Quantified probability distributions and uncertainties for relevant inputs and results from the analysis
- Use of explicit risk insights to include, exclude, limit, or bound events and SSCs into the design basis of the facility

It is important to note that this work will describe a risk-informed probabilistic design basis analysis method and not a risk-based method. In a risk-based regulatory method, compliance with regulatory requirements is based solely on the results of risk calculations 41. This type of method relies on the completeness and accuracy of risk calculations; for sufficiently complex engineering systems or risk events with low probability and high consequences, the accuracy and uncertainties in these calculations can be impossible to quantify.

In a risk-informed regulatory method, insights from risk calculations are used to provide insights into system safety and provide rational for regulatory requirements and limits. This enables more effective allocation of both applicant and regulator resources to ensure safety. It also allows explicit discussion and handling of low probability, high consequence events that would have otherwise been arbitrarily included or included in licensing analysis based on general engineering judgment that did not reflect the specific facility or activity. In some cases, risk information and results from risk analyses will be used to demonstrate compliance with regulatory limits (e.g., probabilities of projected dose consequences) but in a risk informed approach these analysis will always be supplemented by additional regulatory requirements commonly used in deterministic design basis analyses (e.g., defense-in-depth).

The probabilistic design basis analysis utilizing risk insights continues to develop a more realistic assessment of both the probability and consequences of events. Overall, the goal of probabilistic design basis analysis is to apply risk insights (such as the significance of particular SSCs) and allow facilities to focus safety on the areas that matter most. Incorporation of probability quantification into the licensing basis can more effectively ensure public health and safety. The main drawback of this process, however, is that it dramatically increases the regulatory burden associated with licensing. In addition to analysis of event sequences performed to support the deterministic design basis analyses, risk assessments must also be developed to quantify the probability of events and event sequences. These risk analyses are extensive, requiring substantial time and resources to both prepare and review. Understanding the potential additional benefits and drawbacks of probabilistic design basis analyses are critical in selecting appropriate regulatory methods.

5.6.1 Developing initiating events and failure probabilities

A major part of the probabilistic design basis analysis is the definition and quantification of different initiating events, hazard groups, and failure mechanisms for SSCs and facilities. These events and associated data is key to the qualitative and quantitative insights gained probabilistic methods. While challenges of the definition of events and interactions is common to both deterministic and probabilistic analyses, unique challenges of probabilistic analyses is the development of probabilities of these events and failures. Selection of these values may have significant effects on calculated risk for different event sequences and subsequent impacts on design, engineering, and operational choices for a facility. Appropriate data is therefore critical to ensuring effectiveness of probabilistic methods.

The main process for generating data for initiating event and failure probabilities is analysis of historic operating data [75]. This data (subject to considerations regarding applicability, data quality, and potential other sources of variability) is the highest quality source of information to predict future performance. Performance databases from manufacturers, industry groups, research organizations, or regulators can be extremely valuable in assigning probability values for many SSCs or internal and external initiating events [76][77][78].

Data for some events or failures may be sparse, questionable, or otherwise unavailable for use in probabilistic assessments. In these cases, expert elicitation may be useful at generating approximate values for use in analyses. This process has become formalized by U.S. nuclear regulators but can have significant (and normally unquantifiable) uncertainties as the underlying distribution are not known [79]. The process is also commonly used by other regulatory organizations and is an accepted technique for use with probabilistic analyses given appropriate constraints [79].

One particular challenge of utilizing probabilistic methods with novel technologies, especially technologies that require the use of innovative SSCs, is developing the failure modes and failure probabilities. Components designed for high reliability may have failure rates sufficiently low that failure would not be expected for thousands of years of continuous operation, making operational test of failure probabilities infeasible. Development of reliability estimates using various approximation methods is possible but providing operating margin and enabling the updating of probability information based on operational data of novel components [80] may be useful if utilizing probabilistic design basis analysis methods for the licensing evaluations of commercial fusion facilities.

5.6.2 Proposed probabilistic design basis analysis method

In this work, the general framework for the probabilistic design basis analysis is composed of phases or levels based on existing guidance from professional organizations and regulators on the development of risk assessment methods for commercial nuclear facilities [81]. Each of these levels will contribute risk insights for consideration in the probabilistic design basis analysis and enable demonstration of compliance with relevant regulatory requirements. The three levels of analysis discussed in this work based on conventional work scopes for probabilistic risk assessments (PRAs) are:

- Level 1: Loss of control and primary confinement of hazard (e.g., mobilization and loss of containment of radiological material)
- Level 2: Release of hazard to the facility or environment
- Level 3: Exposure to and consequences of hazards released

These different levels of analyses can be correlated to the hazard limit types discussed in Chapter 9. Table 5.14 shows the relationship between the hazard limit types of the three levels of PRA. Depending on the intended use of risk insights from the PRA analysis and the need for different types of risk information, different Level PRA analyses may be required. In some probabilistic design basis analyses, the risk insights may be mixed with other analysis types. For example, a Level 1 or Level 2 PRA model may be used to produce inputs for use in deterministic design basis analyses to determine the bounding hazard exposure or consequences associated with an analytically reduced hazard inventory, release, or release probability.

Table 5.14. PRA model level applicability for hierarchical hazard limits

Hazard Limit Type	*Applicable PRA Model Level*
Total inventory limits	Level 1 PRA
Release limits (total emission)	Level 2 PRA
Release limits (concentration)	
Concentration exposure limits	Level 3 PRA
Total exposure/ dose limits	
Consequence limits (indirect)	
Consequence limits (direct)	

In this work, a simplified methodology for describing and performing probabilistic design basis analyses is presented to illustrate the potential regulatory and design impacts of this analysis on commercial fusion facilities. Performing formal probabilistic risk assessments is a detailed and mature field, requiring specialized knowledge and substantial resources to complete. The following joint standards from ASME and ANS represent currently accepted guidance on performing PRA:

- ASME/ANS RA-S-2008, Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications
- ASME/ANS RA-S-1.2-2014, Severe Accident Progression and Radiological Release (Level 2) PRA Standard for Nuclear Power Plant Applications for Light Water Reactors (LWRs)
- ASME/ANS RA-S-1.3-2017, Standard for Radiological Accident Offsite Consequence Analysis (Level 3 PRA) to Support Nuclear Installation Applications
- ASME/ANS RA-S-1.4-2013, Probabilistic Risk Assessment Standard for Advanced Non-LWR Nuclear Power Plants

Those seeking detailed formal guidance on performing probabilistic design basis analyses for commercial fusion applications should refer to the above standards. Additional guidance on hazard specific probabilistic analyses (e.g., external flooding, fires, seismic hazards) should also be utilized depending on the specific analysis.

In this work, a simplified framework for performing probabilistic design basis analyses is described to highlight the potential regulatory and impacts of this licensing evaluation type on commercial fusion facilities. The following general method (based, in part, on recent prior documents PRAs [82]) are recommended for a probabilistic design basis analysis in the form of a probabilistic risk analysis calculation:

1. Define the analysis boundary including relevant hazards, initiating event classes, geographic boundary, temporal boundary, and PRA scope (level)
2. Identify internal and external initiating events and hazards to be modeled. Quantify the probability distribution and uncertainties of the events and hazards.

3. Determine the evaluation criteria used to determine end states for the analysis and safety functions performed to reach safe end states
4. Determine the SSCs or operator actions needed to accomplish the safety functions, and the success criteria for those systems and actions
5. Develop event sequences for initiating events that lead to event end points based on plant design and the identified SSCs and operator actions
6. For each SSCs or operator actions, develop a fault tree to identify possible failure modes, identify underlying dependencies, and quantify conditional failure probability of each safety function
7. For each event sequence, quantify the probability of the sequence and calculate the evaluation criteria of interest based on the joint probability of all sequence events based on the underlying fault trees and accounting for dependent probabilities
8. Develop assurances (e.g., calculations, programs, testing, defense-in-depth) that demonstrate SSC compliance with the technical basis of the analysis

This process can be generally repeated for any level PRA. For Level 1 analyses, the inputs would consist of initial system states and the analysis end state would be sequences that result in loss of system control and loss of primary confinement of hazards. For Level 2 analyses, the inputs would be Level 1 analyses outputs or conservative inputs from deterministic analyses that describe the loss of hazard confinement and the outputs would be sequences that result in the release of hazards. For Level 3 analyses, the inputs would be Level 2 analyses outputs or conservative inputs from deterministic analyses that describe the hazard releases and the outputs would be sequences that result in hazard consequences.

The first step in probabilistic design basis analyses is defining the overall scope of the analysis. This largely depends on the ultimately intended use of the PRA risk insights. Several uses of risk insights include:

- Determination of credible or significant event sequences for use in deterministic design basis analysis calculations. This enables quantifiable selection of credible, bounding event sequences rather than selecting generally bounding and overly conservative event sequences.
- Determination of SSCs that are significant contributors to the overall risk of the facility. This enables development of component specific design and performance requirements to ensure adequate safety for individual systems and prevents use of overly burdensome regulatory requirements on all SSCs.
- Assessment of design adequacy in combination with defense-in-depth considerations. This provides designers with insights on vulnerable portions of design where independence, physical separation, or additional redundancy may be needed to ensure safety or where it is not needed due to low relative risk.
- Assessment of design adequacy for catastrophic but low probability event sequences. Quantification of probability and consequence through risk calculations can enable determination of when design changes would or would not be needed to further prevent or mitigate these events

For some cases such as SSC classification, risk insights from a Level 1 PRA that only considers internal events may be sufficient. This analysis would be limited to analyzing the risk associated with reliability and design capacity related failures of SSCs that can result in a loss of control and primary confinement of hazardous materials. In other cases such as design adequacy for BDBAs, risk insights from a Level 3 PRA considering both internal and external events may be needed due to the risk contribution of different initiating event classes.

Based on US DOE guidance for development of PRAs, the scope of the analysis should include [83]:

- Intended use of risk information and insights
- Physical boundaries of the analysis and facility SSCs included in analysis
- Classes of internal hazards and events included in analysis
- Classes of external hazards and events (e.g., seismic, fire, flooding, wind, malicious acts) included in the analysis
- Level of probabilistic analysis performed (Level 1, Level 2, Level 3)
- Relationship of the probabilistic risk analysis to other licensing analyses (e.g., direct input to other analyses, using other analyses as inputs, informing assumptions on other analysis, etc.)
- Risk metric of interest for the analysis (e.g., probabilities, indirect consequences, direct consequences, probability-consequence composites)

This scope defines what should be included in the probabilistic design basis analyses and what will constitute a completed analysis.

The second step in the probabilistic design basis analyses is identification of internal and external initiating events and hazards to be modeled. This step of the analysis can vary significantly depending on the particular scope of the analysis.

The logic for developing the list of internal events is similar to that used for the development of design basis events for deterministic design basis analysis. These events include those that can contribute to the failure of fundamental safety functions for a facility, events that are identified through expert review of the engineering design of a facility, or events identified by prior operating experience. In the case of probabilistic design basis analysis, risk significant events from preliminary probabilistic risk assessment may also be included in analyses.

The logic for developing the list of external events is similar to the process used for the development of the general design basis for a facility in a deterministic design basis analysis. This includes events identified by prior operating experience of similar facilities or industries, or through review by field experts. Guidance from regulators [52] or industry [57] can also guide development of external events for analysis. Common external events for analysis include seismic, fire, flooding, high wind, and accidental or malicious offsite events.

For each of the internal and external events developed for the probabilistic design basis analyses, a technical basis is required that quantifies the probability distribution and uncertainties related to the event. This may include the magnitude of the event (e.g., probability of different strength earthquakes), the frequency of the event (e.g., recurrence frequency of different strength earthquakes), and the uncertainties related to these values (e.g., percentile bounds on likelihood of occurrence). Industry and regulatory guidance can be extremely valuable in developing the technical basis for this input data [56]. This technical information is likely gathered from a variety of sources (historical records, testing, expert judgment), so the data sources and data quality should be explicitly included as part of the analysis to enable validation of analysis completeness and technical adequacy.

The third step in the probabilistic design basis analyses is determining the evaluation criteria used to determine end states for the analysis and safety functions performed to reach safe end states. The scope of the analysis (specifically the probabilistic analysis level, relationships to other licensing documents, and the risk metrics) all help define the end state criteria for the analysis. For Level 1 analyses, characterizing risk (quantity and probability) of the uncontrolled and unconfined hazards may be sufficient as an analysis end state. For Level 3 analyses, risk metrics including probability related total exposure and dose limits, and direct and indirect consequence limits may be required. Assessing the end point of the analysis is important to determining the scope of the event sequences developed as part of the probabilistic design basis analyses. For an individual analysis, the end point should also be determined based on whether the sequence reaches an analysis boundary condition (spatially, temporally) or the threshold for another analysis.

The fourth step and fifth steps in the probabilistic design basis analyses are identifying the SSCs and operator actions necessarily to fulfill plant safety functions and developing event sequences that consider the success and failure of these SSCs and operator actions. Similar to the deterministic design basis analysis method, the goal of this step is to comprehensively develop event sequences that describe event progression from initiating event to a final event state. Development of event sequences is largely an inductive process [55]. The level of design detail and the expertise of analysts developing the event sequences may have a significant impact on the final event sequences [56]. Methodical analysis and use of formal evaluation procedures are useful in ensuring the accuracy and completeness of these analyses [57]. Event sequences should be developed for each initiating event (or group of initiating events if a bounding event can be determined).

The sixth step in the probabilistic design basis analyses is developing probabilistic fault trees for each SSC or operator action included in the event sequences for the initiating events. This step marks a divergence in the analysis processes for probabilistic and deterministic design basis analyses. In deterministic methodologies, the success or failure of SSCs is determined based on assumptions such as the single failure criterion and crediting the performance of SSCs and operator actions. This approach can both overestimate the failure of simpler systems (over emphasizing the significance of single failure of highly reliable component) and underestimate the failure of more complex systems (under emphasizing the potential for multiple, simultaneous unrelated failures due to unforeseen or discounted system interactions).

In a probabilistic design basis analysis method, the fault tree technique is used to systematically describe and quantify the failure probability of SSCs or operator actions in event sequences with a credited safety function. In a fault tree analysis, a “top level” event is selected (conventionally the failure of the SSC in the event sequence), and the system is then analyzed to determine all of the credible ways the top level event can occur [55]. The different failure modes of system are repeatedly decomposed using logical operators (e.g., “and”, “or”, “not”) until the fault tree consists of either phenomenologically simple “basic events” not requiring further decomposition or more complex intermediate events that exit the analysis scoped boundaries, requiring separate analysis or other additional assumptions. SSC or operator action dependencies on other systems or conditions should be noted as part of the fault tree. Completed fault trees thus characterize the logical basis for the top level event – most commonly the failure of the SSC to perform its credited safety function.

It is important to note that in fault trees, the top level event should be a clearly defined binary event based on the event sequence. In nearly every engineering system, performance is rarely binary. In real applications, a pump does not simply operate or fail to operate; a pump may produce more or less than the desired flow rate with a pressure differential that is above or below the desired set point. Timing of operation (e.g., starting too early or late, shutting off too early or too late) or temporal changes to pump performance (e.g., changing flow during operation) may all occur during operation. Any of these variations in performance may occur for a pump and some conditions may prevent the SSC from fulfilling its credited safety functions while others may have acceptable or negligible impact. Analysis of all these factors individually would over complicate the fault tree structure; instead top level events should be developed with specific parameters directly related to the ability of the SSC to perform its credited safety function. Thus construction of the subsequent fault tree will focus analysis on conditions that prevent SSC success.

Once a fault tree has been developed for a top level event, the probabilities of the individual basic events or intermediate events can be used with the logical operators between events and the principles of Bayesian probability to determine the overall probability of the top level event occurring [55]. In many cases, dependencies between different basic events may exist (e.g., probability of failure given failure of a common support system). In these cases, conditional probabilities should be included to more accurately describe the probability of the top level event. For extremely simple systems with few basic events, these analyses may be conducted by hand. For more complex systems, however, various analytic and numerical tools can be used to calculate the probability of top level events.

Depending on the top level event, limited information may be available about the probabilities of individual basic events. Novel or FOAK systems developed for commercial applications, for example, may not have significant prior operating experience that can be used as a basis for development of failure probabilities. For other events, there may be a range of values based on operational experience or expert judgment. In cases, use of best estimate as well as upper and lower bound values can be useful at providing insights into the affect of different events and systems on the overall failure of the SSC or operator action and, ultimately, on the event sequence.

It is important to characterize and assess the performance of both physical and digital SSCs, as well as human operators. The success or failure of human operator action is, in some ways, more complicated than a physical SSC. Human operators may be required to perform a safety function (e.g., start the correct pump or close a valve) or contribute to the safety function of an SSC (e.g., correctly maintaining an SSC in an operable condition). Human operators are potentially invaluable to complex systems because they can provide flexibility in response for non-typical event sequences or facility conditions.

The role of human operators in these processes, however, also presents possible new failure mechanisms. Human operators fail to perform their safety function (e.g., fail to close a valve), may introduce additional failure mechanisms (e.g., close the wrong valve), interfere with other SSCs (e.g., incorrectly open a safety related valve that had already closed), or introduce additional failure mechanisms to other SSCs (e.g., perform inappropriate maintenance that creates new valve failure mechanisms). Both the Three Mile Island nuclear accident and the Chernobyl nuclear accident highlighted how human operator error can contribute to significant accidents [84]. The flexibility of human operators means that characterizing all possible human operator related failure mechanisms is extremely challenging.

Human factors engineering (HFE) and human reliability analysis (HRA) are useful methods to help improve and assess the reliability of human operators. HFE facilitates the design of facilities, systems, and procedures to minimize errors produced by human operators [84]. HRA is a structured approach to help identify human operator related failure mechanisms based on design and contributing factors, and quantify the success and failure probabilities for use in probabilistic analyses [84]. These two disciplines are important to the accurate modeling of safety credited human operator action and interaction with SSCs in probabilistic assessments.

The probabilistic information from the fault trees should be calculated and documented to provide a success and failure probability for each SSC or operator action credited with a safety function in the event sequences. These probabilities, subject to assumptions and bounding conditions of the particular event and fault tree analysis, are valid for assessing the overall probability of the event sequence.

The seventh step in the probabilistic design basis analyses is quantifying the probability of event sequences and calculating the evaluation criteria of interest. The probability of an event sequence is based on the joint probability of all sequence events based on the underlying fault trees and accounting for dependent probabilities. For simple event trees with independent events, the probability of the event sequence is simply the product of probabilities of each event in the sequence:

$$P_{seq} = \prod_{i=1}^{j} P_i$$

$$C_{seq} = I_{int} \prod_{i=1}^{j} DRF_i$$

For more complex event trees with dependent event probabilities or other interactions, more detailed hand calculations or software can be utilized to calculate the probability of each event sequence.

Calculating the evaluation criteria of interest for the sequence requires mechanistic understanding of the event sequence and how initial conditions, assumptions, and individual events will affect the progression of the event. For a Level 1 PRA, the analysis may focus on quantifying the degree of mobilization and loss of confinement for hazards (e.g., determining vulnerable source term inventory). For a Level 2 PRA, the analysis may focus on quantifying how engineered safety features can mitigate (or prevent) the release of hazardous material into areas that may cause worker or public harm (e.g., determining released source term inventory). For a Level 3 PRA, the analysis may focus on quantifying the biologic or economic consequences of a hazard release (e.g., off-site radiation dose or land contamination). Calculating evaluation criteria can require substantially different levels of engineering effort depending on the depth of the analysis and required inputs, so clear definition of scope at the beginning of the analysis is critical to avoiding unnecessary calculations.

Classification of risk results (including probability and hazard consequences for each event) can be challenging due to interrelation between the two characteristics. A frequency consequence (F-C) curve is commonly used by risk analysts to classify and visualize acceptable risk limits [85]. These can be constructed using a variety of different assumptions regarding acceptable regulatory risk and hazard consequence limits but all enable risk classification. This process allows use of any type of hazard consequence limit (Chapter 4) for various PRA levels and classification of acceptable probabilities for different consequence levels.

The final step in the evaluation process is to provide assurances that SSCs or operator actions credited in the analysis can meet or exceed the technical assumptions made in the analysis. This can include assumptions related to SSC performance for different initiating events, SSC reliability during operation, reserved design margin, or interactions between SSCs during normal and off-normal operation. These assurances will take a number of different forms including SSC design requirements and analyses, operation and maintenance programs, operational and surveillance testing, and defense-in-depth considerations. The appropriate assurance method will vary on an application-by-application basis depending on the SSC and the importance of the SSC in the overall risk profile of the plant. The applicant should develop assurance methods that best validate the assumptions made the analysis and support the conclusions of the analysis.

5.6.3 Probabilistic design basis analysis for a commercial fusion facility

A probabilistic design basis analysis is outlined in this section for a hypothetical commercial fusion facility. The regulatory burden associated with development of a full probabilistic design basis licensing analysis is significant and far outside the scope of this work. As a result, the high level characteristics for the probabilistic design basis are considered, and representative examples of supporting analyses for the probabilistic design basis are presented and discussed. The goal of this section is to illustrate the design and regulatory burden trade-offs associated with use of probabilistic design basis analyses for licensing evaluations.

Based on the discussion of hazards of regulatory significance in Chapter 3, the boundaries of this analysis are limited to the catastrophic, acute, local geographic releases of tritium or tritiated materials from a commercial fusion facility. Deposition of tritium into the biosphere and chronic impacts of tritium contamination are not considered. On-site or worker protection considerations are not considered in this analysis.

The scope of this probabilistic design basis analysis in this work is also limited to the review of the deuterium-tritium storage system discussed in the Level 3 System Engineering Model in Chapter 2. This specific system is selected to allow comparison to the deterministic design basis analysis of the same system in Section 5.4.3. Analysis of this system provides prospective on the regulatory burden associated with probabilistic analyses and enables comparison of reductions in hazard consequences that may be gained from use of probabilistic design basis analyses versus deterministic design basis analyses. The rational for selection of the deuterium-tritium storage system for this demonstration analysis provided in Section 5.4.3 also applies to this section.

The simplified storage system is presented and discussed in Appendix 5B. The extension of this partial analysis to a complete commercial fusion facility and the implications of the deterministic design basis analysis performed in this section are discussed in Section 5.6.4.

This work will provide a high level outline of the processes for Level 2 PRA of the deuterium-tritium storage system. This analysis cannot be completed in detail due to the limited information regarding system designs but will be outlined to provide insights into the required inputs, regulatory burden, design constraints, and regulatory outputs of the analyses. The criterion of interest in this specific analysis is environmental release of radiological material, as quantified by both the total inventory of the release and release conditions. In this scope of this work, the release conditions are characterized by the elevation of the release (e.g., ground level release or elevated release conditions), as these conditions would directly affect calculated hazard consequences associated with the release in a Level 3 PRA or deterministic analysis.

The scope of the PRA is limited to Level 2 due to availability of input information in this model example. Completing a Level 1 PRA analysis requires detailed design information regarding source terms and SSCs, as well as mechanistic understanding of system behavior.

This level of design information and detail on system behavior is not available, so it is not practicable to perform a preliminary Level 1 PRA. Instead of using the results of Level 1 PRA as inputs to a Level 2 PRA, deterministic source terms and probabilities will be used based on review of published literature, fault trees, and other engineering assumptions and calculations. Opportunities to reduce conservatism in inputs through future use of a Level 1 PRA will be highlighted.

Similarly, completing a Level 3 PRA analysis requires detailed information regarding site-specific building layout, and regional meteorology, geography, ecology, economic bases, and population distribution statistics. This level of detailed information is not available for this analysis of a generic, pre-conceptual design facility, so it is not practicable to perform a preliminary Level 3 PRA. Instead of using the results of Level 2 PRA in a Level 3 PRA, the results from the Level 2 PRA will be used with deterministic release calculations or a set of bounding value calculations to determine different release conditions. Opportunities to further characterize the release consequences using a Level 3 PRA will be highlighted.

This analysis does not have a specific intended risk goal but instead is intended to demonstrate how different risk insights may be obtained using probabilistic analyses. The types of risk insights and their uses in the licensing process will be highlighted.

5.6.3.1 Identifying initiating events and hazards

The second step in the probabilistic design basis analysis is the definition of initiating events, the hazard modeled, and probability distribution of this data. A full PRA of the D-T storage system should include modeling of both internal and external events. In this work, the scope of the analysis is limited to analysis of Level 2 PRA internal events. The rational to limit analysis to internal initiating events is similar to that developed in Section 5.5.3 for the deterministic design basis event analysis. The generalized fundamental safety functions of interest (Section 5.4.2) is:

- control and confinement of hazardous material, protection against hazards and control of planned hazardous releases, as well as limitation of accidental hazard releases

The D-T storage system contains both energetic hazard sources (less than ten kilograms of flammable and explosive hydrogen in gaseous process or solidified hydride form) and residual energy forms (0.324 W/g for tritium [86]) but these hazards are minor compared with the primary radiological hazard posed by the tritium. The hazards posed by flammable and explosive hydrogen gas will be bounded by other analyzed external events.

Internal initiating events are developed for the deuterium-tritium storage system for a commercial fusion facility in Table 5.16 based on the relevant fundamental safety function and the system description in Appendix 5B. These events are similar to the initiating events developed for the deterministic design basis analysis but do not include the simultaneous loss of multiple storage bed inventories or the loss of both the storage bed inventory and glove box integrity. These events are captured by event sequence that initiates with loss of storage bed inventory (independent failure) or external common cause failure modes (correlated failure), and thus are captured by other event sequences and external analyses.

Published literature on tritium handling systems was reviewed to determine the probability of occurrence for each of the internal initiating events. A failure probability is most often given as an occurrence rate that can be used in a Binomial or Poisson distribution to calculate an annual likelihood of occurrence [56]. If published initiating event probabilities were not available, event probabilities were assumed based on engineering judgment. In this work, the probability information is limited to point failure estimation and uncertainty bounds were not included due to the limited scope of the project.

Review of published operational experience with metal hydride tritium storage beds revealed that loss of full component tritium is not a recognized failure mode [87]. A fault tree was developed for the tritium storage beds to determine a probability of loss of full component tritium inventory. The developed fault tree was incomplete and only included internal events, so it likely represents a non-conservative low failure probability. The fault tree for the storage bed and the other engineered safety features related to the deuterium-tritium storage system are presented in Section 5.5.3.5. In a formal probabilistic analysis, additional testing or data would be required to support these engineering assumptions, calculations and inputs.

Table 5.16. Internal events for probabilistic design basis analysis for the deuterium-tritium storage system

Event No.	*Initiating Events*	*Probability (1/year)*	*Data Source*	*Radiological Source Term (g Tritium)*
INT-1	Loss of glove box clean up – loss of ability to remove mobilized tritium from glove box	1.00E-02	Bruske & Holland, 1983 [105]	0.7
INT-2	Loss of process pipe integrity – loss of in-process mobilized tritium inventory flow	3.00E-01	Bruske & Holland, 1983 [105]	7
INT-3	Loss of glove box integrity – loss of tritium inventory leakage from storage tanks	4.00E-02	Cadwallader & Sanchez, 1992 [88]	0.7
INT-4	Loss of storage bed integrity – loss of mobilized	4.00E-02	Cadwallader & Sanchez, 1992 [88]	7

	tritium inventory			
INT-5	Loss of storage bed inventory – loss of full component tritium inventory	8.24E-04	Tritium storage bed fault tree	70

Table 5.16 also provides the radiological source term associated with each of the internal events. In this work, the lack of detailed design information regarding processing and handling of tritium during storage operation required simplifying assumption with regards to the source terms. For events involving the loss of a full storage bed inventory (INT-5), it was assumed that 100% of total storage bed inventory would be released (total of 70 grams of tritium). For events involving the release of the mobilized tritium inventory (INT-2, INT-4), it was assumed that 10% of the total storage bed inventory would be released before the leakage was detected, isolated, and stopped using other engineered systems (total of 7 grams of tritium). For events involving the release of the routine leakage from storage beds (INT-1, INT-3), it was assumed that 1% of the total storage bed inventory would be released before the leakage was detected, isolated, and stopped using other engineered systems (total of 0.7 grams of tritium).

These assumptions allow for the quantification of the hazard consequences associated with these internal events but are rough approximations. More substantial engineering justification, analysis, or experimental data would be needed to justify these radiological source terms in a complete probabilistic design basis analysis. In many cases, the radiological source terms may not be point estimates but instead would be a probabilistic distribution of a range of possible radiological release source terms. For the Level 2 PRA, these probabilistic source term and event probability inputs could be generated by completion of a Level 1 PRA.

Similar to the deterministic design basis analysis, this list of events would likely be expanded and consolidated through the design and licensing process. As the facility design progress from pre-pre-conceptual design to detailed design, other methods such as expert review, operational experience, or insights from other hazard analysis methods. As the list of events expands, some events may be selected as bounding and representative of a class of events and allow consolidation of the probabilistic design basis event list.

For a Level 1 PRA, internal initiating events would be identified that can lead to the initiating internal events identified in the Table 5.16 for the Level 2 PRA. These could include the failure of electromechanical components or subsystems that ultimately lead to a loss of confinement of radiological material. These events would be based on the specific design of the deuterium-tritium storage system. For a Level 3 PRA, the initiating events would be the end states, radiological inventories, and a probability related to the event trees developed as part of the completed Level 2 PRA.

5.6.3.2 Determine end state evaluation criteria

The third step in the probabilistic design basis analysis is to develop the evaluation criteria used to determine end states for the analysis and safety functions performed to reach safe end states. In the Level 2 PRA of internal events developed in this work, the end state is based on the release of radiological material to the environment. A safe end state occurs when an event sequence does not result in the unplanned or uncontrolled release of radiological material to the environment. An unsafe end state occurs when an event sequence results in any unplanned or uncontrolled release of radiological material to the environment. This may be a static, single release of radiological material or a dynamic, time varying release of radiological material.

For the deuterium-tritium storage system for a commercial fusion facility described in Appendix 5B and Section 5.6.3.1, the primary safety function is confinement and control of unplanned radiological releases. The secondary safety function for the system is the mitigation of hazard consequences for unplanned radiological releases. If a release cannot be prevented by engineered safety systems, then the goal is to minimize the hazard consequences associated with the release.

5.6.3.3 Determining safety significant features

The fourth step in the probabilistic design basis analysis is determine the SSCs or operator actions needed to accomplish the safety functions, and the success criteria for those systems and actions. For the deuterium-tritium storage system for a commercial fusion facility described in Appendix 8B and the 5.5.3.1, there are three SSCs that perform the primary safety function of confinement and control of unplanned radiological releases:

- Tritium Storage Bed with HIVES (SSC-1)
- Glove Box Confinement (SSC-2)
- Glove Box Clean Up System (SSC-3)

In the Level 2 PRA analysis, it is assumed that the Tritium Storage Bed with HIVES has failed and resulted in the complete release of the radiological inventory from its primary confinement. The success criteria for the two remaining SSCs are given in Table 5.17. In both cases, the success criteria are given as qualitative criteria and not quantitative criteria. Due to limited design information available for the system in this work, quantitative criteria were not feasible to develop or evaluate. In a final probabilistic design basis evaluation, the success criteria should be both quantifiable and measurable. This allows for the calculation of event sequence consequences, development of fault trees quantifying success and failure probabilities, and the verification of SSC performance during design, construction, and operation.

Table 5.17. Primary safety function SSC success criteria

SSC	*Success Criteria*	*Rational*
Glove Box Confinement	System external leakage at or below design basis level	Control material release during high concentration transients
Glove Box Clean Up System	System is able to return glove box atmosphere to within design parameters in set time	Material retention and capture following in-box hazardous material releases

There are three SSCs that perform the second safety function of mitigation of hazard consequences for unplanned radiological release:

- Facility Building Confinement (SSC-4)
- Facility Building Ventilation (SSC-5)
- Facility Building Stack (SSC-6)

The success criteria for these SSCs are given in Table 5.18. Again, the success criteria in this work are generally characterized based on qualitative criteria and not quantitative criteria. In a final probabilistic design basis evaluation, the success criteria should be both quantifiable and measurable.

Table 5.18. Secondary safety function SSC success criteria

SSC	*Success Criteria*	*Rational*
Facility Building Confinement	Facility external leakage at or below design basis level	Control material leakage during high concentration transients
Facility Building Ventilation	System is able to remove all contaminated facility atmosphere within set time	Timely removal of contaminated atmosphere from worker spaces and facility
Facility Building Stack	System is able to discharge contaminated gas at specific flow conditions and location	Enable adequate dispersion of hazardous material to acceptable concentrations for release

In addition to the SSCs described in Table 5.17 and Table 5.18, automated control systems, instrumentation, and operator actions may be required to ensure that the SSCs fulfill their intended safety function. Due to the limited design information available in this work, these subsystems and actions were not accounted for in the PRA. In a final probabilistic design basis evaluation, these considerations would need to be included as possible failure modes or dependencies for the SSCs.

5.6.3.4 Developing event sequences

The fifth step in the probabilistic design basis analysis is developing event sequences for initiating events that lead to event end points based on plant design and the identified SSCs and operator actions. In this work, the event sequences developed for the Level 2 PRA are limited to the deuterium tritium storage system described in Appendix 5B and the internal initiating events listed in Table 5.16. In a complete deterministic design basis analysis of this system, event sequences for all five internal initiating events would need to developed, unless it could be shown that an event could be used to fully bound others licensing basis events under all conditions.

In this work, event sequences are developed for the two internal events: INT-2 (Loss of process pipe integrity – loss of in-process mobilized tritium inventory flow) and INT-5 (Loss of storage bed inventory – loss of full component tritium inventory). These two events are selected for further analysis in this work because they are internal initiating events with highest likelihood of occurrence and largest released inventory, respectively. Note that in a full deterministic design basis analysis of this system, event sequences would need to be developed for all internal initiating events. Figure 5.6 shows the simplified event sequence for INT-2 and Figure 5.7 shows the simplified event sequence for INT-5. The end states in the event sequences are either the confinement and clean up of radiological material (safe end state) or the release of radiological material to the environment (unsafe end state)

Again, note that in this simplified analysis, only subsystem level events affecting systems or components discussed in Appendix 5B are discussed. With additional design information, event sequences could be developed for individual sequence events (e.g., “Glove box clean up systems fails to remove tritium inventory”) to identify more specific system or component dependencies in event sequences.

Due to the presence of the same SSCs and the similarity of the initiating event (release of radiological material in the D-T Storage System glove box), the event sequences presented in Figure 5.4, 5.6, and 5.7 are nearly identical. This is a function of the initiating event, safety functions, and system design, and would not be the case for other systems and events. They are provided in this work for completeness and to highlight the potential range of end states for the Level 2 PRA.

Each SSC with a possible system safety function (Tables 5.17 and 5.18) are listed as top level events in the event trees. For each top level event, a fault tree is developed to characterize the possible failure of the SSC to perform its safety function.

Internal Event 2 - Loss of Process Pipe Integrity

Event Sequence Initiation	SSC-2: Glove Box Integrity Maintained	SSC-3: Glove Box Clean Up Functional	SSC-4: Facility Building Confinement Maintained	SSC-5: Facility Building Ventilation Functional	SSC-6: Facility Building Stack Functional	Event Sequence Endpoint	Event Sequence Code
Loss of process pipe inventory	Glove box contains release	Glove box clean up removes/ confines tritium inventory				Tritium is contained and cleaned up by normal components. No release to environment.	INT-2-1
		Glove box clean up system fails to remove tritium inventory	Facility building confines tritium leak fraction from glovebox	Facility building ventilation removes tritium from building	Facility building stack results in stack elevated tritium release	Partial release of tritium inventory (glove box leakage) from stack height to environment	INT-2-2
					Facility building stack fails but results in building elevated tritium release	Partial release of tritium inventory (glove box leakage) from building elevated location to environment	INT-2-3
				Facility building ventilation fails to remove tritium from building		Partial ground level release of tritium inventory (glove box leakage, building leakage) to environment	INT-2-4
			Facility building fails to confine tritium leakage from glovebox			Partial ground level release of tritium inventory (glove box leakage) to environment	INT-2-5
	Glove box fails to contains release		Facility building confines tritium inventory	Facility building ventilation removes tritium from building	Facility building stack results in elevated tritium release	Full release of tritium inventory from stack height to environment	INT-2-6
					Facility building stack fails but results in building elevated tritium release	Full release of tritium inventory from building elevated location to environment	INT-2-7
				Facility building ventilation fails to remove tritium from building		Partial ground level release of tritium inventory (building leakage) to environment	INT-2-8
			Facility building fails to confine tritium inventory			Ground level release of tritium inventory to environment	INT-2-9

Figure 5.6. Event sequences for D-T Storage System for Internal Event 2 (INT-2)

Internal Event 5 - Loss of Storage Bed Inventory

Event Sequence Initiation	SSC-2: Glove Box Integrity Maintained	SSC-3: Glove Box Clean Up Functional	SSC-4: Facility Building Confinement Maintained	SSC-5: Facility Building Ventilation Functional	SSC-6: Facility Building Stack Functional	Event Sequence Endpoint	Event Sequence Code
Loss of storage bed inventory	Glove box contains release	Glove box clean up removes/confines tritium inventory				Tritium is contained and cleaned up by normal components. No release to environment.	INT-5-1
		Glove box clean up system fails to remove tritium inventory	Facility building confines tritium leak fraction from glovebox	Facility building ventilation removes tritium from building	Facility building stack results in stack elevated tritium release	Partial release of tritium inventory (glove box leakage) from stack height to environment	INT-5-2
					Facility building stack fails but results in building elevated tritium release	Partial release of tritium inventory (glove box leakage) from building elevated location to environment	INT-5-3
				Facility building ventilation fails to remove tritium from building		Partial ground level release of tritium inventory (glove box leakage, building leakage) to environment	INT-5-4
			Facility building fails to confine tritium leakage from glovebox			Partial ground level release of tritium inventory (glove box leakage) to environment	INT-5-5
	Glove box fails to contains release		Facility building confines tritium inventory	Facility building ventilation removes tritium from building	Facility building stack results in elevated tritium release	Full release of tritium inventory from stack height to environment	INT-5-6
					Facility building stack results in elevated tritium release	Full release of tritium inventory from building elevated location to environment	INT-5-7
				Facility building ventilation fails to remove tritium from building		Partial ground level release of tritium inventory (building leakage) to environment	INT-5-8
			Facility building fails to confine tritium inventory			Ground level release of tritium inventory to environment	INT-5-9

Figure 5.7. Event sequences for D-T Storage System for Internal Event 5 (INT-5)

5.6.3.5 Developing fault frees

The sixth step in the probabilistic design basis analysis is to develop a fault tree to identify possible failure modes, identify underlying dependencies, and quantify conditional failure probability of each safety function. Preliminary fault trees were developed for all six SSCs in the D-T Storage System. Each fault tree identifies possible failure modes for each SSC based on the safety functions identified in Tables 5.17 and 5.18. A best estimate probability of failure to complete the safety function is calculated for each SSC based on the failure modes developed in the fault trees. This calculated probability is a preliminary quantification of the probability of failure for each SSCs.

The fault trees for the six SSCs are shown in Figures 5.8 through 5.13. The fault trees were developed based on guidance for fault trees in NUREG-0492 [55]. In all SSC fault trees, the tree is developed to either a basic event (an initiating event requiring no further development) or an undeveloped event (an initiating event is that outside of the scope of this work).

The probability of failure for each SSC in this work was calculated using the methods prescribed in NUREG-0492 [55] based on the joint or intersectional probability of basic and intermediate events. Table 5.19 summaries the calculated annual failure probability for each of the SSCs. The numerical models and assumptions for each of the fault trees are presented in Appendix 5C. These failure probabilities can be used in the PRA to determine the likelihood of different analyzed event sequences.

Table 5.19. D-T Storage System SSC Fault Tree Failure Probabilities

System, Structure, or Component	*Failure Probability* (yr^{-1})
SSC-1: Storage bed inventory lost	8.24E-04
SSC-2: Glove box integrity not maintained	1.20E-02
SSC-3: Glove box clean up not functional	6.21E-01
SSC-4: Facility building confinement not maintained	3.20E-02
SSC-5: Facility building ventilation not functional	1.20E-02
SSC-6: Facility building stack not functional	1.98E-03

The fault trees developed in this work are limited for three primary reasons: limitation on analyzed initiating events, availability of design information on the D-T storage system, and limited information on the failure rates and modes of SSCs.

First, due to the limitation on the quantification and analysis of initiating events to internal events, potential failure modes related to external events (including fires, seismic, and flooding) and operator errors (including actions taken or not taken) are not included in the fault trees. In some places, these are marked as “undeveloped events” and are given a placeholder probability of zero to enable calculation of the overall fault tree failure probability. In this way, the fault trees represent lower bound failure probability for the SSC probability.

Second, due to the limited design information regarding the D-T Storage System described in Appendix 5B and the treatment of design at a pre-conceptual system level. The fault trees, therefore, do not have significant detail regarding subsystem and component level failure mechanisms, details on control and instrumentation systems, information on operational failure mechanisms, or information on common cause failure mechanisms related to shared systems or co-location of SSCs. As a result, both the intermediate and basic events in the fault tree are very generic and provide limited insights into the actual performance of SSCs. In a complete probabilistic design basis analysis, these fault trees would need to updated to better reflect the actual design and operation of the SSCs.

Third, the basic events used in these fault trees no not necessarily represent the expected failure rates of the SSCs. There is limited public information on the failure rates of many systems due to the small amount of operating experience with many of these systems (e.g., fewer than 10 facilities worldwide with greater than 50 gram tritium inventories). There has also been limited publication of prior PRAs that could be used to help characterize the failure mechanisms and rates of comparable systems. Relevant information from design studies on ITER and other fusion devices and other DOE facilities were used as a basis for basic event probabilities [78][80][88]. More accurate estimation of specific failure mechanisms and failure rates would be needed for a complete probabilistic design basis analysis.

The development of complete fault trees that accurately characterize and quantify the probability of SSC failure is a key input to the calculation of probabilistic design basis analyses.

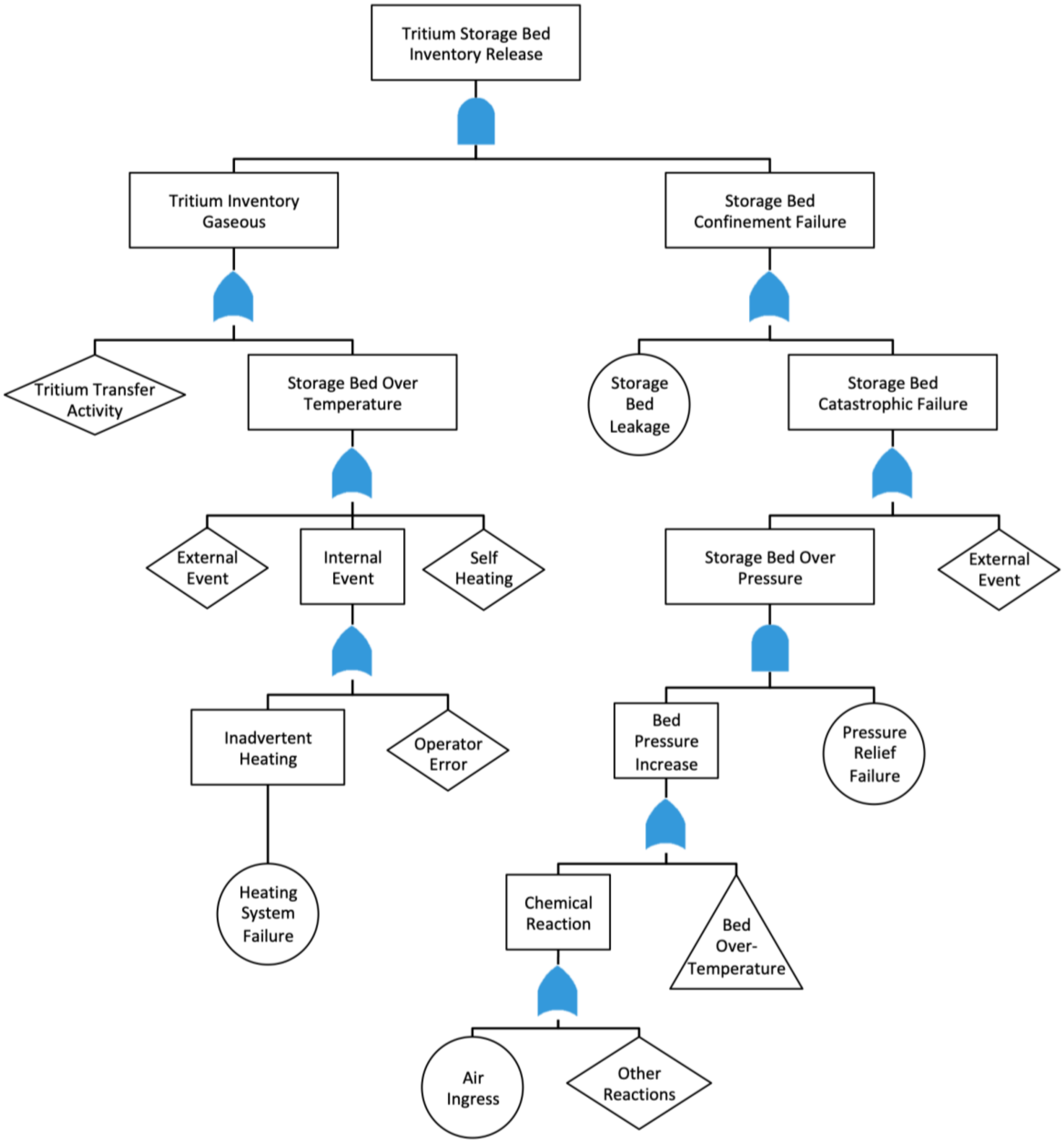


Figure 5.8. Fault Tree for SSC-1: Tritium Storage Bed

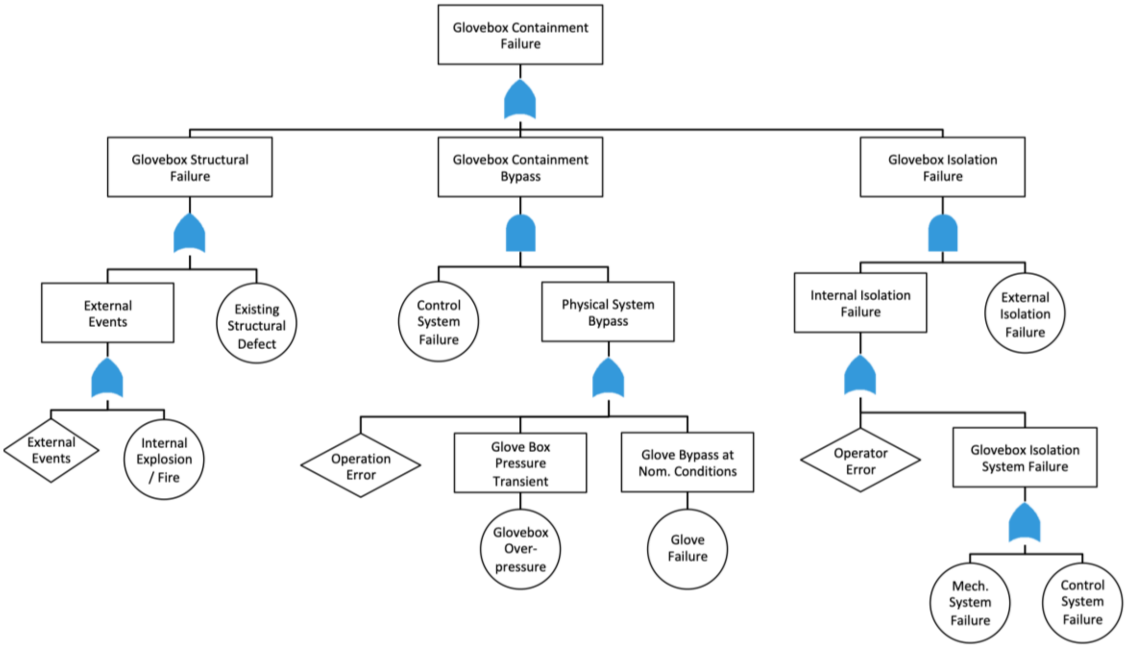

Glovebox Containment Failure
Glovebox Structural Failure
Glovebox Containment Bypass
Glovebox Isolation Failure
External Events
Existing Structural Defect
Control System Failure
Physical System Bypass
Internal Isolation Failure
External Isolation Failure
External Events
Internal Explosion / Fire
Operation Error
Glove Box Pressure Transient
Glove Bypass at Nom. Conditions
Operator Error
Glovebox Isolation System Failure
Glovebox Over-pressure
Glove Failure
Mech. System Failure
Control System Failure

Figure 5.9. Fault Tree for SSC-2: Glove Box Confinement

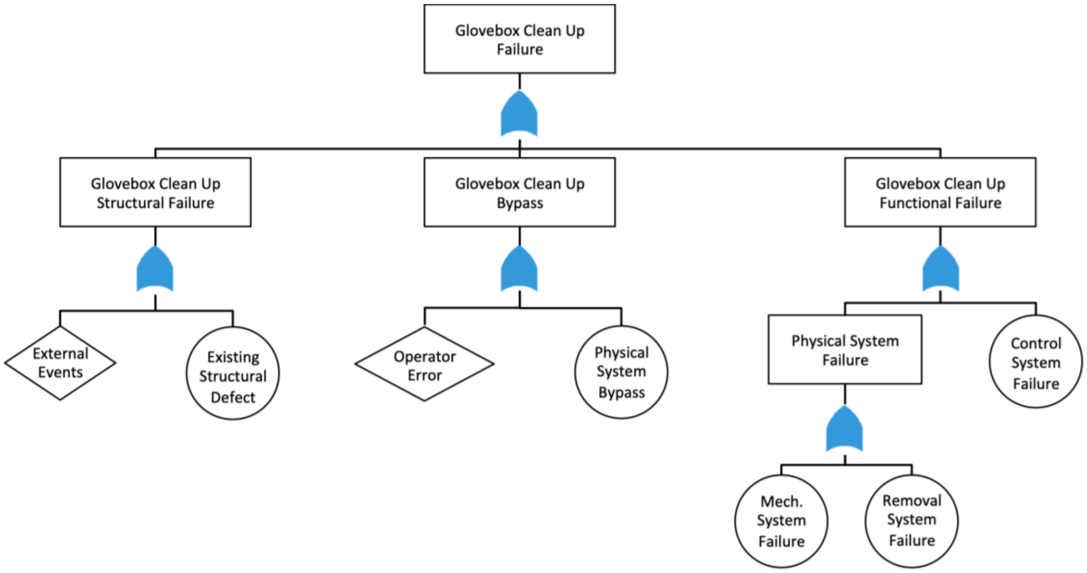


Figure 5.10. Fault Tree for SSC-3: Glove Box Clean Up System

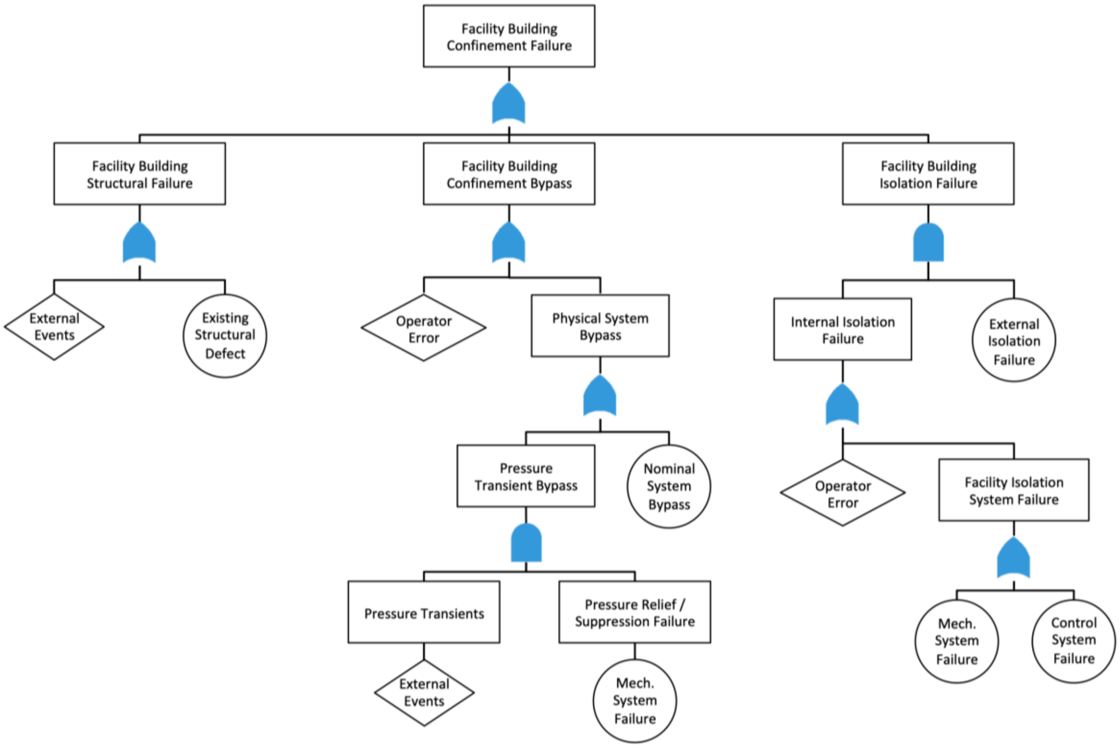

Facility Building Confinement Failure
Facility Building Structural Failure
Facility Building Confinement Bypass
Facility Building Isolation Failure
External Events
Existing Structural Defect
Operator Error
Physical System Bypass
Internal Isolation Failure
External Isolation Failure
Pressure Transient Bypass
Nominal System Bypass
Operator Error
Facility Isolation System Failure
Pressure Transients
Pressure Relief / Suppression Failure
Mech. System Failure
Control System Failure
External Events
Mech. System Failure

Figure 5.11. Fault Tree for SSC-4: Facility Building Confinement

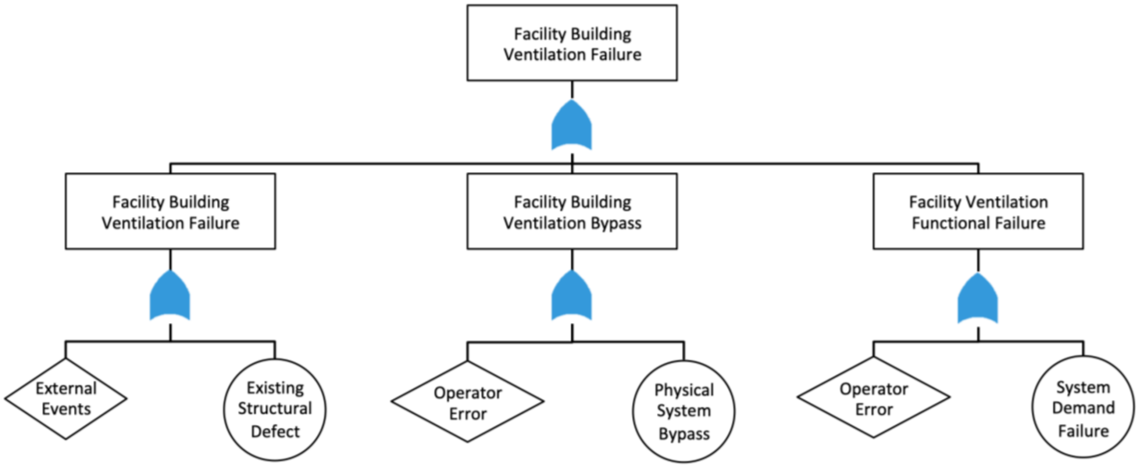

Facility Building Ventilation Failure
Facility Building Ventilation Failure
Facility Building Ventilation Bypass
Facility Ventilation Functional Failure
External Events
Existing Structural Defect
Operator Error
Physical System Bypass
Operator Error
System Demand Failure

Figure 5.12. Fault Tree for SSC-5: Facility Building Ventilation

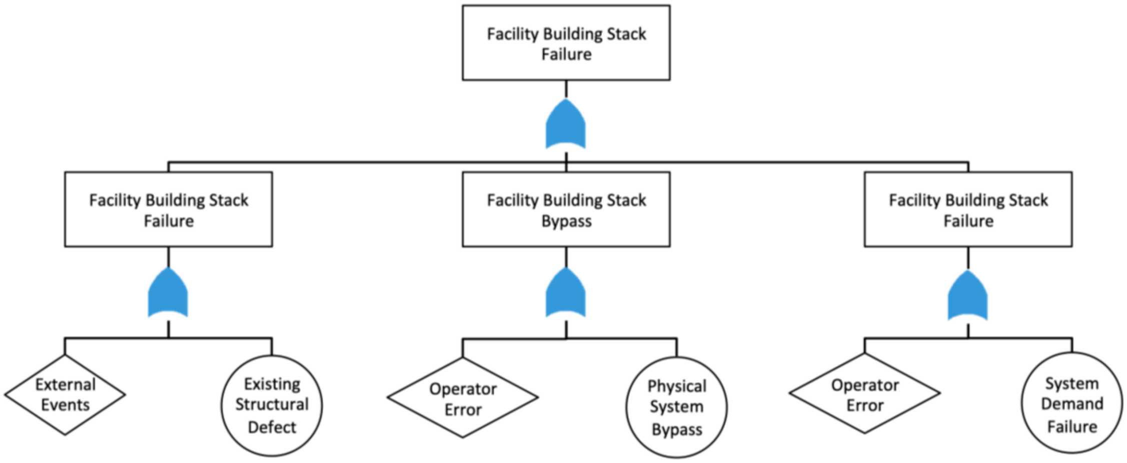

Facility Building Stack Failure
Facility Building Stack Failure
Facility Building Stack Bypass
Facility Building Stack Failure
External Events
Existing Structural Defect
Operator Error
Physical System Bypass
Operator Error
System Demand Failure

Figure 5.13. Fault Tree for SSC-6: Facility Building Stack

5.6.3.6 Quantifying failure probabilities

The seventh step in the probabilistic design basis analysis is to quantify the probability occurrence and calculate the evaluation criteria of interest for each developed event sequence. These calculations are based on the underlying fault trees and accounting for dependent probabilities in the different sequences.

In total, there were 18 event sequences identified for the two initiating events developed in Section 5.6.3.4. The probability of occurrence for each event sequence was calculated by combining the probability of the initiating and intermediate events. The evaluation criteria of interest for each event sequence (tritium inventory release and release elevation) were also calculated for each event sequence based on the assumed confinement or leakage of different systems. Table 5.20 and Table 5.21 provide the calculated probabilities and evaluation criteria of interest for INT-2 (tritium pipe break) and INT-5 (storage bed release), respectively.

Table 5.20. INT-2 (Tritium Pipe Break) Level 2 PRA Results

Event Sequence	*Probability (yr^{-1})*	*Event Risk Contribution*	*Released Inventory (g T)*	*Release Height (m)*
INT-2-2	1.76E-01	58.67%	0.0007	50
INT-2-1	1.12E-01	37.33%	0	0
INT-2-5	5.89E-03	1.96%	0.0007	0
INT-2-6	3.44E-03	1.15%	7	50
INT-2-4	2.14E-03	0.71%	0.000315	0
INT-2-3	3.48E-04	0.12%	0.0007	10
INT-2-9	1.15E-04	0.04%	7	0
INT-2-8	4.19E-05	0.01%	3.15	0
INT-2-7	6.81E-06	0.002%	7	10

Table 5.21. INT-5 (Storage Bed Failure) Level 2 PRA Results

Event Sequence	*Probability (yr^{-1})*	*Event Risk Contribution*	*Released Inventory (g T)*	*Release Height (m)*
INT-5-2	4.83E-04	58.56%	0.007	50
INT-5-1	3.09E-04	37.44%	0	0
INT-5-5	1.62E-05	1.96%	0.007	0
INT-5-6	9.46E-06	1.15%	70	50
INT-5-4	5.88E-06	0.71%	0.00315	0
INT-5-3	9.56E-07	0.12%	0.007	10
INT-5-9	3.17E-07	0.04%	70	0
INT-5-8	1.15E-07	0.01%	31.5	0
INT-5-7	1.87E-08	0.002%	70	10

The result tables provide both the annual probability of occurrence for each event sequence as well as the relative probability contribution of each sequence for the overall initiating event. The two initiating events analyzed had identical fault trees following the initiating event, the per relative probability contributions for each sequence is the same in both analyses but the overall probability of the specific event sequence differs.

The results from Table 5.21 can provide additional insights into the deterministic design basis evaluations performed in Section 5.5.3.4. In the deterministic design basis evaluations, all event sequences were initially evaluated. Use of safety credited systems and a single failure criterion assumption were used to classify event sequences as design basis event sequences and beyond design basis event sequences. This process classification was largely qualitative and did not explicitly consider probability of different sequences. The results in Table 5.21 for the same event sequences highlight that several event sequences of concern (INT-5-3, INT-5-9, INT-5-8, and INT-5-7) have event probabilities that are extremely small. The results from the probabilistic evaluations in this section could be used to justify the inclusion or exclusion of event sequences from a deterministic design basis evaluation. This process is generally referred to as a risk-informed regulatory process as probabilistic information is used to support deterministic regulatory decision making [89].

These Level 2 PRA results show that for 96% of analyzed event sequences, the internal initiating events either result in no release (INT-2-1, INT-5-1) or an elevated release of an extremely small tritium inventory (INT-2-2, INT-5-2). Review of the two fault trees suggest that the glove box confinement (SSC-2) is a critical safety component, dividing the releases into significantly different classes of environmental tritium releases.

While these results were the goal of the Level 2 PRA performed in this work, conceptualizing the meaning of these results can be difficult for those without prior intuitive understanding of the significance of the event probabilities, tritium inventories, and release heights. In formalized probabilistic design basis analysis that ended with a Level 2 PRA, regulatory acceptance criteria would be developed to enable acceptance or rejection of the PRA results in Table 5.20 and 5.21. Additional metrics such as limiting the risk significance of any individual SSC could also be utilized.

The results from this Level 2 PRA were used as the inputs into a deterministic hazard consequence evaluation model (identical to the model used for the worst-case release analysis) and used to estimate off-site hazard consequences associated with the different event sequences. This work appears similar to a Level 3 PRA (hazard consequence analysis) but is distinctly different because it does not consider site-specific meteorological or population conditions that could significantly affect the hazard consequences. Combining probabilistic analyses and conservative deterministic analysis can be problematic because it skews the focus on results but in this case enables better understand of the results of the difference between different Level 2 PRA results.

Off-site hazard consequences (acute radiation doses) for each of the event sequences in Table 5.20 and Table 5.21) were calculated using a simplified Gaussian plume model (described in Section 5.3) using very conservative meteorological release conditions (1 m/s wind speed, Class F atmospheric stability, no plume meander, and no surface roughness). For each event sequence, the maximum offsite dose and location were calculated (location at or past the site boundary at 160 m) and the distance to the 1 rem dose boundary was calculated, if applicable. The results of these analyses are provided in Table 5.22.

The event sequences in Table 5.22 are plotted on two separate limit F-C curves: an NRC proposed F-C curve for a risk informed licensing framework [85] and an NEI proposed F-C curve for risk-informed licensing framework [64]. Details on the probability and hazard consequence limits shown on the two F-C plots are provided in the original documentation. The event sequences analyzed in this work are plotted on Figure 5.14 and Figure 5.15.

Table 5.22. Offsite Hazard Consequence Estimations for Level 2 PRA Results

Event Sequence	*Probability (y^{-1})*	*Max Dose (Rem)*	*Max Dose Location (m)*	*1 rem dose boundary (m)*
INT-5-9	3.17E-07	292.32	160	5887
INT-5-8	1.15E-07	131.55	160	3257
INT-2-9	1.15E-04	29.23	160	1186
INT-5-7	1.87E-08	21.56	393	5727
INT-2-8	4.19E-05	13.15	160	736
INT-2-7	6.81E-06	2.15	393	1022
INT-5-6	9.46E-06	0.49	3399	N/A
INT-2-6	3.44E-03	4.90E-02	3399	N/A
INT-5-5	1.62E-05	2.92E-02	160	N/A
INT-2-5	5.89E-03	2.92E-03	160	N/A
INT-5-3	9.56E-07	2.16E-03	393	N/A
INT-2-4	2.14E-03	1.31E-03	160	N/A
INT-5-4	5.88E-06	1.31E-03	160	N/A
INT-2-3	3.48E-04	2.16E-04	393	N/A
INT-5-2	4.83E-04	4.93E-05	3399	N/A
INT-2-2	1.76E-01	4.94E-06	3399	N/A
INT-2-1	1.12E-01	0	0	N/A
INT-5-1	3.09E-04	0	0	N/A

Review of the two F-C curves based on the probabilistic design basis analysis provides several important insights into the safety of the D-T storage system.

The first insight is that there is one event sequence (INT-2-9) that would be unacceptable under both sets of proposed regulatory limits using the analysis assumptions in this work. This event may not be traditionally expected as a limiting case because it only involves the release of a relatively small quantity of tritium (7 grams) based on the failure of a process pipe. Review of the event reveals that the high assumed failure rate of processing piping results in a (relatively) high probability for an unmitigated, ground level tritium release.

The potential dose consequence from a related event (INT-5-9) is much higher, but the high reliability of the tritium storage bed contributes to a much lower overall risk for INT-5-9.

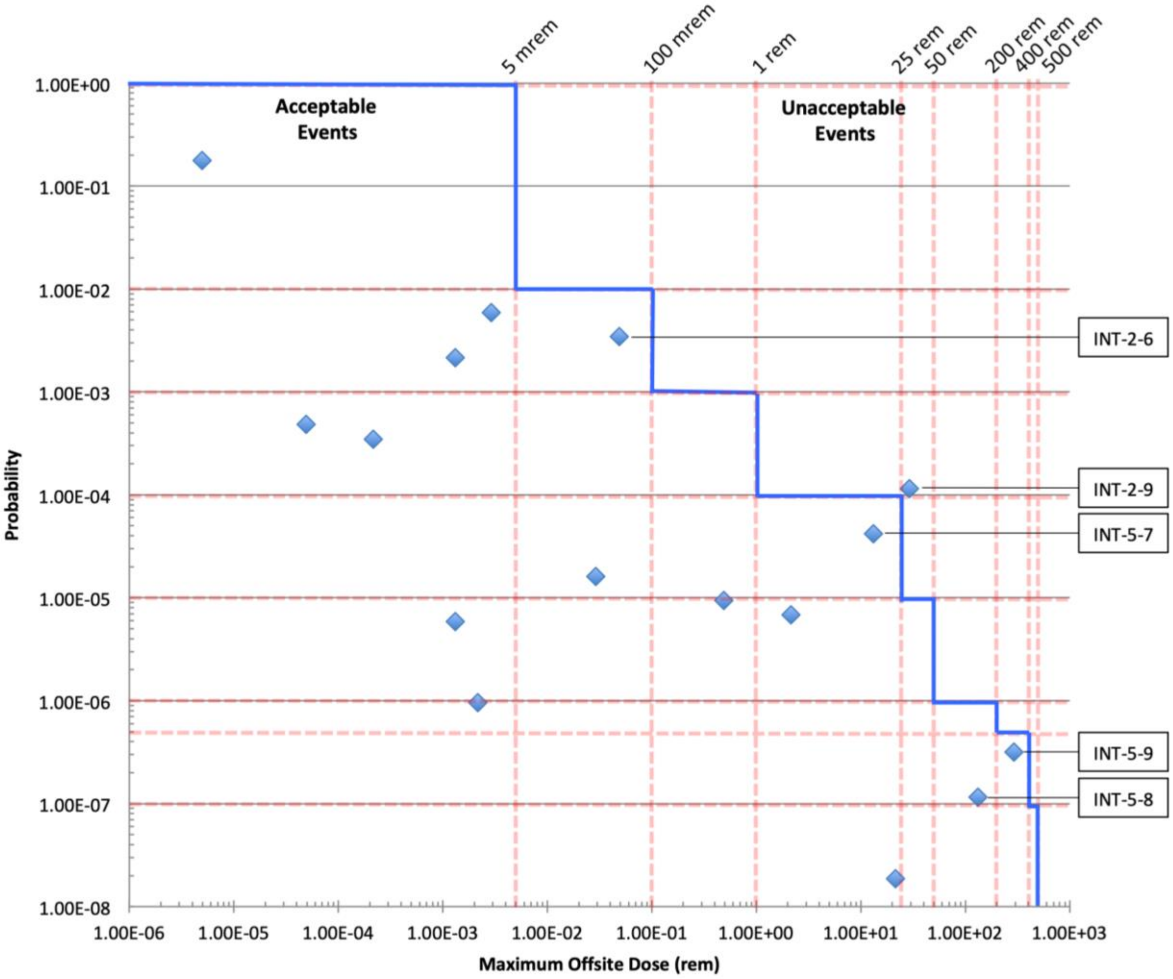


Figure 5.14. Preliminary PRA Results Plotted Against NRC Proposed F-C Curve

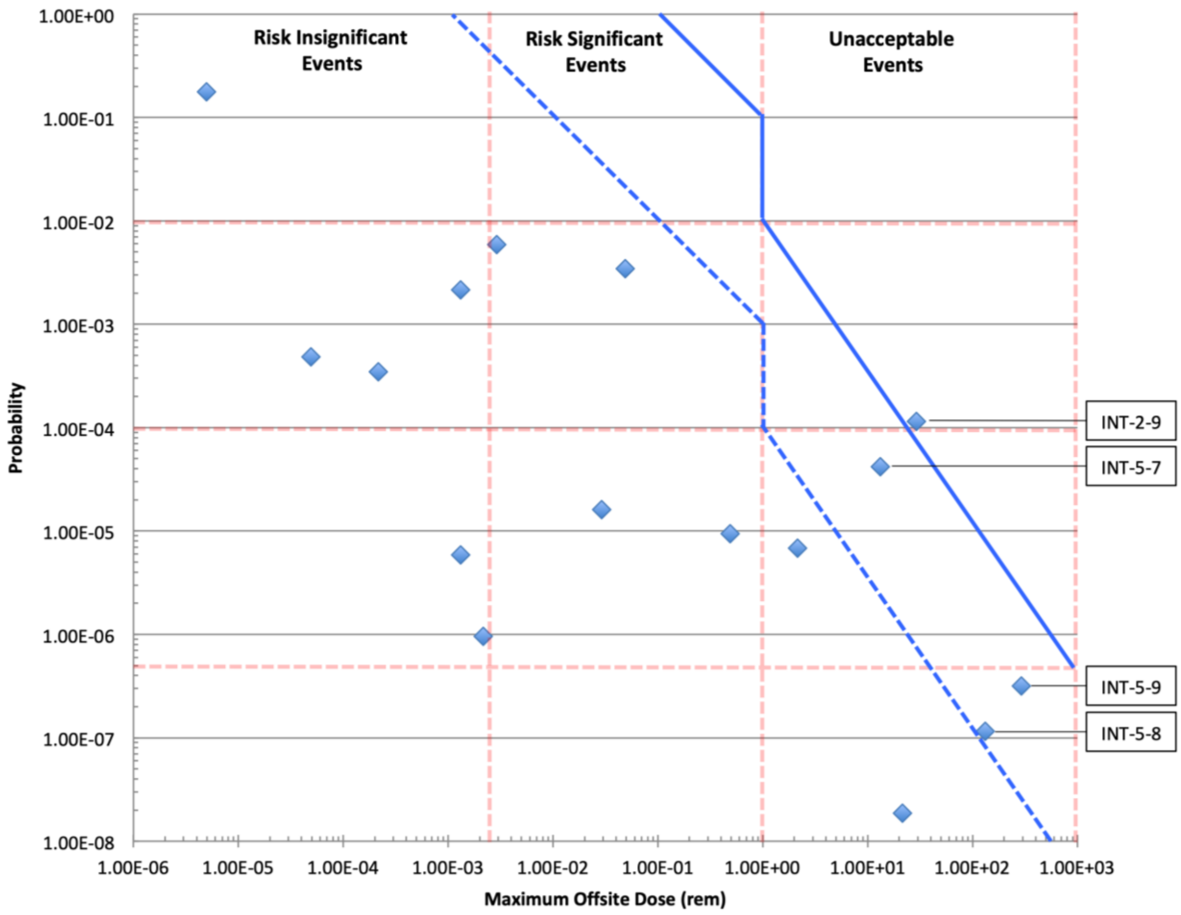


Figure 5.15. Preliminary PRA Results Plotted Against NEI Proposed F-C Curve

The calculated risk for this event sequence would need to be reduced to meet the regulatory limits under both frameworks. The risk could be reduced a combination of radiological inventory decrease and event probability decrease. Many physical or analytic options are available for designer to mitigate the risk such as:

- Additional SSCs that can reduce the likelihood or magnitude of a process pipe release (e.g., use of double walled pipes for tritiated systems)
- Changes to process implementation, instrumentation, and control to decrease the quantity of tritium released following a pipe failure
- Improved process pipe qualification to reduce the likelihood of pipe failure
- Improved glovebox or building confinement qualification to reduce the likelihood of confinement failure during a process pipe release
- Design/application specific quantification of expected failure rates (rather than use of generic benchmarks) for SSCs to reduce event probability

Each of these changes would impact the overall safety characteristics of the facility but the designer would have the flexibility to select the options that made sense on a project specific basis.

In addition to the physical changes to the system, the deterministic analysis performed to calculate the hazard consequences used a simplistic modeling technique and extremely conservative metrological conditions. Justification and use of less conservative inputs would reduce the calculated hazard consequences or a more complete Level 3 PRA could be performed that accurately accounts for the likelihood of different release and exposure conditions. These models could be used to reduce the risk associated with the event to below regulatory limits.

The second insight is that event sequences INT-5-7, INT-5-8, and INT-5-9 have the highest risk significance for both sets of internal initiating events. While this is not surprising from a mechanistic perspective (i.e., they result in the largest tritium releases), they highlight the risk significance of the SSCs that must function to prevent or mitigate these event sequences. While different strategies and metrics have been proposed for classification of SSC risk significance based on PRA results and F-C plots [64][85][90], a simplistic review of the event sequences show that the SSCs with greatest risk significance are:

- Tritium Storage Bed with HIVES (SSC-1)
- Glove Box Confinement (SSC-2)
- Facility Building Confinement (SSC-4)

This result may appear trivial upon review as these three SSCs provide the primary, secondary, and tertiary confinement barriers to the release of large quantities of radiological material. The result, however, confirms the importance of these barriers and the need to ensure that these SSCs can perform their safety function and meet the performance conditions assumed in the PRA calculations.

This result also justifies the prioritized allocation of resources in the design and operation of a facility. While the facility building stack is a highly visible engineered safety feature, its overall contribution to the risk reduction of the D-T storage system is minimal. In the pre-conceptual design phase, applicants could review the cost-benefit (i.e., cost-risk reduction) associated with this SSC and determine if it is the optimal strategy to reducing risk and ensuring safety, or if an alternative approach (e.g., additional confinement layers or mitigation of internal events) would be a more effective approach.

The ability to enable a risk informed decision-making process is ultimately the biggest benefit of probabilistic design basis analysis. While the D-T storage system analyzed in this work is relatively simple, this method still enables the calculation of hazard consequence risk and the quantification of different risk contributors. This process can formalize and provide greater transparency for engineering decision-making and regulatory decisions. This ideally results in a more efficient allocation of engineering resources and helps maximize the overall facility safety. This risk informed decision-making process can support and improve the efficiency of other licensing evaluation methods discussed this work.

5.6.3.7 Developing assurances for system performance

The eighth step in the probabilistic design basis analysis process is to develop assurances that demonstrate SSC compliance with the technical basis of the analysis. One challenge associated with probabilistic design basis analyses is that they require a large number of SSC performance characteristics to quantify the probability and consequences of different event sequences. These analyses are only accurate if the actual SSCs meet or exceed the performance characteristics assumed in the analyses. As a result, technical assurances are needed to ensure that the SSCs meet or exceed the design basis conditions used in the probabilistic design basis analysis.

In this work, technical assurances would be required for each of the six SSCs considered in the analyses, as well as any connecting systems (e.g., process piping, valves, pumps, instrumentation) that are required for processing and represent potential failure points. The technical assurances would likely include:

- SSC requirements for all design basis events and analyses to demonstrate that the components will perform as analyzed during the events,
- quality assurance on the design, manufacturing/fabrication, construction, and installation of SSCs,
- programmatic controls on the operation and maintenance of SSCs,
- operational and surveillance testing

Development of these assurances in the scope of this work is difficult due to the pre-conceptual design information available, limited evaluation scope, and the scoping nature of the failure data used in the analysis. Each SSC would need a technical specification document that outlines the key performance parameters and design conditions for the SSC, along with any design standards or codes that are used to ensure adequate performance. These design requirements, calculations, and programmatic controls would support the conclusions of the probabilistic design basis analysis and ensure that the project satisfies regulatory requirements.

5.6.3.8 Summary of probabilistic design basis analysis results

The probabilistic design basis analysis performed in this work for the D-T storage system provided preliminary assurance that the system could meet relevant regulatory limits for acute, off-site release of radiological material based on the results of a Level 2 PRA for internal events and a conservative off-site release consequence analysis. Six SSCs were analyzed as having safety functions the facility:

- Tritium Storage Bed with HIVES (SSC-1)
- Glove Box Confinement (SSC-2)
- Glove Box Clean Up (SSC-3)
- Facility Building Confinement (SSC-4)
- Facility Building Ventilation (SSC-5)
- Facility Building Stack (SSC-6)

These safety credited SSCs would have additional requirements on design, analysis, manufacturing, and operation to ensure that they can meet the performance characteristics assumed in the Level 2 PRA. Further analysis could enable elimination of the Glove Box Clean Up system from the list of SSCs with safety functions due to it's limited impact on event sequence risk.

Of the six analyzed SSCs, three were identified as risk significant due to their function or failure in the highest risk event sequences as evaluated on an F-C plot:

- Tritium Storage Bed with HIVES (SSC-1)
- Glove Box Confinement (SSC-2)
- Facility Building Confinement (SSC-4)

While a numeric risk metric was not developed for risk significance in this work, these SSC were qualitatively identified and would merit additional assurance requirements on performance or design modifications to reduce risk significance.

In addition to these three risk significant SSCs, the tritium processing piping system was identified as a potential risk significant system. The high failure rate and large working tritium inventory assumed in the Level 2 PRA resulted in unacceptable highly risk for event INT-2-9. As a result, modifications to the system such as decreasing pipe failure rates, design modification to mitigate releases, or decreases in working inventory are needed to decrease event sequence risk to below regulatory limits.

This work was limited in both breadth and depth but could be expanded to provide both more detailed assessment of facility risk. The analysis consisted of a Level 2 PRA that only modeled internal events. The Level 2 PRA could be expanded to include additional significant external events including fire, flooding, wind, and seismic events. The analysis could also be expanded to include both Level 1 and Level 3 PRA analysis rather than simply relying on deterministic analyses to provide the inputs and assess outputs of the Level 2 PRA analysis.

5.6.4 Advantages and challenges of probabilistic design basis analysis

Probabilistic design basis analyses enable the most realistic evaluation of engineered safety features in safety analysis without considering arbitrary failures of engineering safety features used in deterministic, maximum credible, and worst-case release analyses. These analyses evaluate risk based on both the probability and consequence of event and enable use of risk insights in the design, operation, maintenance, and regulation of hazardous systems.

The major advantages of probabilistic design basis analyses are the ability to incorporate risk insights into regulatory analyses, a more accurately evaluation of low probability events and uncertainty, the ability to credit highly reliable engineered SSCs in safety analyses, and the ability to explicitly quantify and communicate risk.

The primary advantage of probabilistic design basis analyses is the incorporation of risk information into regulatory analyses. Use of deterministic, maximum credible, and worst-case release analyses cannot capture the impact of event or sequence probability on the risk posed by different potential events. Qualitative criteria (e.g., the single failure criteria) or engineering judgment is used to separate credible from non-credible events but this method can result in opaque and inconsistent process. Explicit handling of probability allows for a more transparent quantification of safety significance of SSCs and event sequences. This also enables designers to reduce the regulatory requirements on SSCs that actually have limited risk significance to the overall facility, reducing the costs associated with the SSC.

These risk insights can help inform design and operational decisions to minimize risk and highlight potential lower consequence but higher probability events that can produce unacceptable consequences. This process can help avoid requirements for costly engineered safety features that primarily prevent or mitigate high visibility events.

Use of probabilistic design basis analyses also enables the more explicit handling of low probability initiating events and event sequences. In deterministic and maximum-credible event analyses, low probability events are either excluded or addressed indirectly through defense in depth considerations. In both cases, the consequence may only be included through use of engineering judgment but is not explicitly handled. Probabilistic design basis analyses allow consideration of any conceivable event or event sequence, limited primarily by the scope provided by the analyst.

Use of probability distributions for event and sequence probability also enables explicit handling of uncertainties in evaluations. In deterministic methods, use of conservative bounding values or bounding cases can limit the analysis of parameters that realistically may take a variety of possible values. This forces analysts to either analyzed large numbers of point estimates for different input ranges or determine the bounding set of inputs. Probabilistic design basis analyses can be done in greater detail in handling of uncertainties and provide insights into the likelihood of different event end states.

The fourth advantage of probabilistic design basis safety analyses is the ability to more accurately credit highly reliable engineered SSCs in safety analyses. In deterministic, maximum credible, and worst-case release analyses, assumptions such as the single failure criterion prevent designers from taking credit of highly reliable engineered SSCs in safety analyses. In a probabilistic design basis analysis, the prevention or mitigation effects of highly reliable engineered SSCs can be captured by the risk of different event sequences. While the recognizing principles of defense-in-depth and calculating risk significance of SSCs are still useful to help ensuring that a single SSC isn't relied upon for safety, probabilistic methods provide another way to explicitly credit additional design margin in safety analysis not recognized other methods.

The final advantage of probabilistic design basis safety analyses is the ability to explicitly quantify and discuss risk associated with an activity. Facilities or activities with the potential for high consequence events may have challenges related to social license and public discourse. If a catastrophic event is mechanistically possible and not precluded by design, it is natural for the public to inquire the likelihood of the event. Deterministic analyses must rely on design philosophies (e.g., defense-in-depth or redundancy) to qualitatively demonstrate that the probability of these events is sufficiently low. Probabilistic analyses, however, provide quantitative information on different event sequences and allow for explicit comparison between events sequences within an analysis. This quantitative analysis can facilitate communication of risk if performed correctly but the context and level of detail must be carefully managed to ensure effective messaging.

The major challenges of probabilistic design basis safety analyses are the regulatory burden associated development of probabilistic analyses, the need for additional assurances for SSCs credited in the analyses, the potential for non-bounding event sequences, and the potential misuse of probabilistic analysis results.

The first challenge of probabilistic design basis safety analyses is the regulatory burden associated with development, review, and maintenance of the analyses. Detailed design information for system and mechanistic understanding of system behavior is needed to develop initiating events, prepare event sequences, analyze fault trees, calculate probabilities, and identify possible system interactions. Some estimates for fission system PRA reports that it many of 75 man-years of effort to create a Level 1, Level 2, and Level 3 PRA for a new facility once all design information and calculations are available [56]. A regulator may be required to independently review the inputs, assumptions, and results of the PRA may then be reviewed, adding time and cost to the regulatory process. Finally, it is important to note that a PRA is not a static analysis – the failure rates, system configurations, and system interactions must reflect the current as-built facility. The risk insights and conclusions from the PRA are only valid if the PRA is maintained during operation to reflect the operation, maintenance, and changes to the facility. Maintenance of the facility safety basis is a task required for all safety analyses, the level of detail in the PRA can dramatically increase the costs associated with maintaining the analysis.

The second challenge of probabilistic design basis safety analyses is the need for additional assurance for SSCs credited in the analyses and documentation on the failure mechanisms for SSCs. The analyses conducted for the SSCs for deterministic design basis safety analyses must demonstrate that the SSC can perform its safety credited function during all design basis events; the analyses for the probabilistic analyses, however, must assure the failure probability and modes of the SSC for specific events or conditions. These technical assurances may require substantial time, cost, and effort to develop and maintain for SSC. This is the major drawback of use of SSC as engineered safety features. The inclusion of probabilistic information again increases the detail of the analysis, reducing conservatism but increasing costs.

The third challenge of probabilistic design basis safety analyses is the potential for unevaluated event sequence and uncertainties and errors in probabilistic calculations. Similar to the discussion provided for deterministic design basis analyses, the insights from probabilistic analyses are ultimately limited by the analyst and understanding of the system and its interactions. Incorrect or limited knowledge of failure modes and interactions can dramatically change the calculated probability of different events or event sequences. For SSCs or events with limited operational experience (e.g., novel technologies) and significant uncertainities, it is likely that failure rate data would be unavailable. Conservatively high failure rates would need to be assumed until testing and operational data could become available for the SSC. This excess conservatism could dramatically change the initial results a probabilistic analysis and result in an analysis that does not reflect the actual event risk..

System interactions (such as operator actions, external events, and common cause failure modes) may also result in event sequences that were not modeled in a facility PRA. This may result in non-bounding event sequences and unacceptable hazard consequences. Processes such as HRE and HRA attempt to identify and minimize the potential for these system interactions, may not identify all possible interactions. It is impossible based on current methods to analytically assess the completeness or accuracy of a PRA, so expert judgment, peer review, and procedural methods must be used to ensure repeatable of analyses. This residual risk is a continuing challenge for probabilistic methods.

The fourth challenge of probabilistic methods is the potential misinterpretation of probabilistic analysis results in regulatory processes. Probabilistic analyses are the most detailed licensing analysis considered in this work and a full probabilistic licensing analysis considers failure mechanisms, probabilities, uncertainties, and interactions between SSCs. The results of these analyses, especially full analyses consisting of Level 1, Level 2, and Level 3 analyses can provide detailed risk insights into the safety characteristics of a facility. These results can also be misconstrued, however, into an assessment of the total risk posed by a facility or activity and not an informed measure of relative risk. It is important to note the limitation on the assumptions of PRA and that low probability, high consequence events can occur and will occur given sufficient time. The results of probabilistic methods should not be used as the sole basis for facility safety but should be used to provide insights into facility risk (e.g., relevant design basis events or safety significant SSCs) in conjunction with other safety analyses such as deterministic safety basis analysis and defense-in-depth principles.

5.6.5 Probabilistic design basis analysis summary

Use of probabilistic design basis analyses for licensing evaluations provides the most detailed analysis of the risk (probability and consequence) of hazardous activities and facilities. This method enables the most realistic modeling of initiating events and evaluation of extremely low probability events without adding prescriptive regulatory requirements. The risk insights gained from probabilistic analysis allow applicants to prioritize the SSCs that will contribute greatest to facility risk and safety. This approach significantly further reduces the calculated hazard consequences for a facility or activity but further increases the design, analysis, and regulatory costs associated with facilities. In a refined probabilistic analysis, it may be possible to reduce regulatory costs by eliminating excess conservatisms and reducing scope of SSCs related to safety but this process would require additional initial analysis. The probabilistic analyses performed in this work was highly limited (both in terms of PRA Level, scope, and events considered), the results of the analyses in this section demonstrate how a commercial fusion facility could meet existing regulatory limits using this analysis method. The tradeoffs between these largest degree of design and analysis flexibility versus the significant regulatory burden and process requirements should be considered when determining if this analysis method is appropriate for specific commercial fusion facilities.

5.7 Hazard control based evaluation

The fifth licensing evaluation method proposed for commercial fusion technology is the hazard control based method. A hazard control based method is a departure from the traditional accident models previously developed for both deterministic and probabilistic design basis analysis. These traditional accident models are based on a direct causality model [72]. This mental model treats accidents as chains of directly related (but largely random) events that result in a hazard consequence or loss. The focus on safety with this model becomes either lengthening the chain of events to prevent a loss (e.g., defense-in-depth through multiple safety systems) or strengthening the links in the chain (e.g., increased reliability of safety systems). This model, however, fails to recognize that events are rarely linear in reality and that interactions between systems, components, and operators often dominate observe accidents. This perceived linear nature of event sequences is primarily based on the investigations that were performed following events to identify a citable "root cause" [72]. Highly engineered systems may have complex system interactions that make development of comprehensive and fully bounding event trees infeasible or impossible. Analysis of these systems may require use of a different accident model.

A system theory based accident model resolves the primary weaknesses of the direct causality model by focusing analysis on the interactions between hazards and the physical and operational controls on them [72]. System-Theoretic Process Analysis (STPA) is a safety analysis process that focuses on the control and elimination of inherent system hazards rather than the identification and prevention of all bounding initiating events. STPA is based on use of control theory for the analysis of complex system interactions that could result in accidents or losses (including human injury or death, damage to facilities, offsite contamination, or unplanned outages). STPA was initially developed for use with complex systems (including software and commercial aerospace) but the methodology has expanded and is inherently technology agnostic [72]. STPA may enable safety analysis of highly complex software and digital instrumentation and control (I&C) systems not currently possible using deterministic or probabilistic methodologies.

In a system theory based analysis approach, safety is considered an emergent property that arises from interactions between system components (both physical components and operational actions). Imposing constraints on these interactions allows for the control of emergent properties. These constraints may be imposed through the physical design of components and systems, processes that effect system behavior (maintenance and operation processes), and social controls (organizational, regulatory, cultural systems). System safety is based on controlling the interactions that cause unsafe conditions and not just the individual events that cause specific accidents.

The purpose of a hazard control based analysis is to provide a structured method for the analysis of system interactions and analysis of control adequacy for system hazards. These analyses are different from the previously discussed licensing analyses; the focus of the hazard control based analysis is on ensuring system safety rather than on the acceptability of hazard consequences. The results of a hazard control based analysis are paired with deterministic hazard consequence analyses when quantifying the outcomes of different identified accidents or losses.

The hazard control based analysis is distinctly different from the event sequence based method previously developed. Overall, the goal of hazard control based analysis is to develop safer systems through incorporation of system engineering interaction insights throughout the design process. Safety is not a quantifiable characteristic but rather the emergent property of a well-designed system. The main drawback of this method, however, is that it does not necessarily align with the hazard consequence based regulatory limits normally used for licensing. In addition, eschewing the direct casualty model is a significant departure from currently recognized methods for safety and risk assessment. As a result, adapting both analyst and regulator thinking to this model may take significantly more resources than use of already accepted analysis technique. These analyses are also extensive, requiring substantial time and resources to both prepare and review. Understanding the potential additional benefits and drawbacks of hazard control based analyses are critical in selecting appropriate regulatory methods.

5.7.1 Basis for STPA based evaluations

The current safety paradigm for safety analysis of high-hazard activities and facilities in the United States is based on a direct causality model of accidents; safety is determined based the plant's resiliency to a set of initiating events through analysis of the linear set of events that occur after sequence initiation. The deterministic and probabilistic design basis event evaluations previously discussed in this chapter are based on a direct causality model of accidents.

Activities or facilities designed and regulated using this model of accidents are required to specifically address and mitigate a large number of highly unlikely initiating events and combinations of initiating events. These initiating events often lead to the prescription of specific mitigating design features that prevent or interrupt event sequences with unacceptable consequences. While this process may result in a system designed for a wide range of initiating events, it does so at an extremely high cost. Existing commercial nuclear fission plants were design and regulated within this safety paradigm and their engineered safety features reflect this.

The historic performance of nuclear fission facilities reveals two major insights about the impacts of direct causality model of accidents paradigm:

- The current system produces very safe reactors at very high costs
- Major accidents still happen despite the high safety costs and normally occur outside the established design basis for the plant.

These two insights present a significant economic and social risk to new technologies, and should be resolved by the organizations that are seeking to develop and deploy new technologies.

The current safety paradigm for nuclear fission power plants was developed largely on historic lessons learned on initiating events. Several 'fundamental' principles of nuclear safety were not developed and included in the design basis of nuclear fission power plants until near misses or accidents highlighted the importance of the event:

- Physical separation and common cause failure of redundant systems, importance of internal fire as a initiating event, – Browns Ferry Unit 1 (1975) [44]
- Operator action as an initiating event, selection of bounding initiating events, severe accident system behavior – Three Mile Island Unit 2 (1979) [44]
- Plant risk profile during shutdown conditions, loss of offsite power as a significant initiating event – Vogtle Unit 1 (1990) [91]
- Common cause failure of physically separated and independent systems, importance of BDBA in plant safety evaluations – Fukushima Daiichi (2011) [92]

Each of these major incidents highlighted the importance of previously unknown initiating events or system interactions that lead to either a near-miss or a nuclear accident and loss.

The direct causality paradigm has become extremely effective at preventing or mitigating known initiating events because the industry has taken lessons learned from near misses and accidents seriously. The paradigm, however, is susceptible to accidents that result from previously unrecognized (or ignored) initiating events or conditions. If a specific event or set of conditions has not been considered (or bounded) in the design basis of the plant, the plant safety for that initiating event is not explicitly evaluated.

While use of a direct causality accident model for evaluating nuclear power plants safety has been fairly effective for existing nuclear fission facilities based on significant operating experience and lessons learned, it has done so at very high cost and complexity. For the novel activities and facilities, significant prior operating experience may not be available. While many initiating events considered for commercial nuclear fission facilities may applicable to commercial fusion or other activities and facilities, the importance of these events and subsequent system interactions may be significantly different. Reduced public tolerance for accidents (and even near-misses) with off-site consequences means that future hazardous activities and facilities will not be able to capture lessons learned in the same manner as current commercial nuclear fission facilities: a major accident (even an accident that does not result in an significant offsite consequence) could be extremely detrimental to the development and deployment of novel technologies.

Review of the current nuclear safety paradigm reveals the potential for vulnerabilities, especially for technologies with limited operating experience. Specifically, current analyses are subject to make several important assumptions regarding safety and accidents [72]:

- Safety is increased by increasing system or component reliability; if components do not fail, then accidents will not occur
- Accidents are caused by chains of directly related events; we can understand accidents and assess risk by looking at the chains of events leading to a loss
- Major accidents occur from the chance simultaneous occurrence of random events.

- Probabilistic risk analysis based on event chains is the best way to assess and communicate safety and risk information.

These assumptions are all inherent in the fault tree methodology that underlies the current nuclear safety paradigm; these assumptions have also all been challenged by operational events in the nuclear industry. Table 5.22 provides examples of major operational events for each of these assumptions.

Table 5.22. Revised Safety Assumptions Based on Operational Events

Current Safety Assumption	*Nuclear Fission Industry Operational Event*	*New Safety Assumption*
Safety is increased by increasing system or component reliability; if components do not fail, then accidents will not occur	1975 Browns Ferry Unit 1 Fire Event – System reliability was high due to redundant and independent reactor shutdown cable systems. System was highly susceptible to common-cause fire failure mechanism not previously considered [44]	High reliability is neither necessary nor sufficient for safety
Accidents are caused by chains of directly related events; we can understand accidents and assess risk by looking at the chains of events leading to a loss	2002 Davis Besse RPV Head Corrosion – Nuclear accident near-miss was a function of design, manufacturing, operational, and maintenance errors, none of which were directly related in sequence [44]	Accidents are complex processes involving entire sociotechnical systems. Traditional event-chain models cannot describe this process adequately.
Major accidents occur when multiple rare, random events occur simultaneously	1979 Three Mile Island Unit 2 Core Melt Event – Initiating event (stuck open pressurizer pilot operated relief valve) can be considered random; subsequent operator actions that directly contributed to fuel melt were intentional but incorrect [44]	Systems will tend to migrate toward states of higher risk. Such migration is predicable and can be prevented by appropriate system design or detected during operation using leading indicator of increasing risk.
Probabilistic risk analysis based on event chains is the best way to assess and communicate safety and risk information.	1990 Vogtle Unit 1 Refueling Loss of Offsite Power Event – Initiating event and sequence not identified in existing PRAs. Probability and risk of shutdown conditions were considered bounded by full power operation. [91]	Risk and safety may be best understood and communicated in ways other than probabilistic risk analysis.

These assumptions also carry significant design and operational consequences for the commercial nuclear fission and other high-hazard industries. Use of system and component reliability as a surrogate metric for safety has both increased costs for design and manufacturing of nuclear systems. Use of high reliability components and redundant systems can increase reliability but are still subject to common cause failures and are extremely costly to manufacture, install, and maintain. Safety analyses based on fault trees focus design efforts on preventing against previously identified initiating events and event sequences. While this makes plants resilient against previously identified events, it may leave them vulnerable for unknown events or events which were believed to be sufficiently unlikely to occur.

This direct causality model also encourages the potentially extremely costly process of safety design or backfitting for newly identified initiating events. Assuming that accidents are truly random events ignores the organizational factors that can often contribute to accidents. Nuclear accidents or near miss events are rarely due to simultaneous, truly independent random failures. Finally, PRA and event trees can be counterproductive when assessing and communicating risk. They encourage focus on hypothetical individual initiating events ("what if…") and require acceptance of an unquantifiable residual risk based on events not considered or known and uncertainty related to modeled data. While PRA is valuable for decision making in absence of complete information, use of it for communicating safety and risk information obscures the uncertainties and assumptions present in the data, methodology, and results.

Resolving these assumptions in a different methodology could result in a more efficient and effective safety evaluation of nuclear reactors and may result in reduced cost due to less reliance on expensive high reliability and redundant systems for safety. System-Theoretic Process Analysis (STPA) attempts to resolve these assumptions (and other assumptions related to direct causality based accident models) by focusing safety analysis on the identification of control actions related to hazardous conditions and enforcement of safety constraints on these actions through design choices or operations requirements.

STPA is based on use of control theory for the analysis of the complex system interactions that can result in accidents or losses. In STPA, an accident is broadly defined as any "unplanned and undesirable loss" of any type [72]. This can include death or injury of those on or off site, damage or destruction of material, contamination and loss of use of land, or loss of system functionality (e.g., unplanned system shutdowns). In this way, reliability or system performance is not a metric for safety. Instead, system reliability is one of several different losses that can be analyzed and explicitly included when making decisions about engineering tradeoffs related to design, operation, and other losses.

In a system theory based analysis approach, safety is considered an emergent property that arises from interactions between system components (both physical components and operational actions). Imposing constraints on these interactions allows for the control of emergent properties. A system control based approach to safety focuses on the "control and enforcement of safety-related constraints on the development, design, and operation of the system" [72]. These controls may be imposed through the physical design of components and systems, processes that effect system behavior (manufacturing, maintenance, and operation processes), and social controls (organizational, regulatory, cultural systems). Using control actions, system interactions, and safety-related constraints as the basis for safety analysis eliminates the need for a direct-causality model of accident analysis; safety can be analyzed based on the system interactions that cause unsafe conditions and not just the individual events that cause specific accidents. There is no longer a need to develop an exhaustive or fully bounding list of all possible initiating event sequences to ensure safety.

One defining feature of STPA is a de-emphasis on probability and numerical calculations of risk and safety. Fault tree based methodologies implicitly or explicitly rely on probability estimations to determine which initiating events and sequences are considered for design basis or maximum credible events. This process is requires use of significant assumptions (e.g., event independence) and may have substantial uncertainties depending on the event sequences considered (e.g., natural event occurrences). STPA focuses instead on the elimination or control of system hazards through safety constraints. Analysis and communication of safety with STPA is based external evaluation of the identified accidents, hazards, system control actions, constraints, and requirements that ensure safe design. Engineering evaluations are still required to ensure that component and system performance satisfies the safety requirements developed through the STPA process. Safety is not treated as a number in STPA but as system property that emerges with sufficient control of hazards.

STPA may be able to resolve many of the current weaknesses associated with the use of fault tree based methods for the safety evaluation of nuclear power plants. STPA can be used for to both evaluate existing designs to identify control action vulnerabilities that should be resolved through backfit or operational changes or to guide design development and reduce reliance on operational constraints to prevent unsafe control actions. STPA does not inherently result in a numeric calculation of safety or accident probability but instead produces a consistent and traceable set of analyses and constraints that can be used to evaluate whether the system is designed and operated in a safe manner. This is a significant change from existing analysis methods: safety is evaluated based on the presence of mitigating and elimination of unsafe control actions instead of the absence of fault trees that result in unacceptable losses.

One particular advantage of STPA for licensing is the ability to explicitly include operational, organizational, and software behavior in safety analyses. STPA can be applied recursively to systems starting with component control and interactions and extended up through the impacts of organizational interactions (e.g., plant management, operators, maintenance staff, regulators) on plant safety and control of hazardous states. Additionally, as future reactors become increasing reliant on digital controls and automation, STPA will allow for safety analysis of software and digital systems in a way that is not currently possible using fault tree methodologies.

While STPA has not been formally adopted by any regulatory agencies for licensing, STPA has been studied for use in safety analysis of a wide range of high-risk systems including automobile safety, aerospace, and commercial medical devices [93]. The use of STPA for evaluation of digital nuclear safety systems has been highlighted in reports prepared under contract by the NRC, Sandia National Lab, and the Electric Power Research Institute (EPRI) ([94], [95], [96]).

While STPA was found in these studies as a promising method for the safety analysis of complex systems, there is currently no research on how STPA could be applied to the safety analysis of nuclear reactor systems as a whole. Two of the major concerns cited by reviewers related to further nuclear applications of STPA were a lack of technique maturity and documentation of previous successful applications of STPA to nuclear systems.

Most recently, NuScale Power has incorporated STPA into the licensing of their digital instrumentation and control systems. While STPA was not explicitly used for licensing, system design requirements generated using STPA were used as the basis for licensing using current safety methodologies [97][98][99]. EPRI also has recognized potential benefits of a hazard control methodology for analysis and licensing of advanced reactors. An industry/university joint project was initiated by EPRI in 2017 to study the feasibility and benefits of incorporating general hazard analysis methods into the safety analysis of conceptual nuclear fission reactor designs [100]. Use of hazard control based evaluation methods and moving away from the direct causality model safety paradigm could have significant advantages in licensing of complex and highly engineered high-hazard systems with limited regulatory or operational precedent and experience.

5.7.2 Proposed hazard control based analysis method

In this work, a simplified framework for performing hazard control based analyses is described to highlight the potential regulatory and impacts of this licensing evaluation type on commercial fusion facilities. The following general method is based on the System-Theoretic Process Analysis (STPA) [93]:

1. Define analysis boundary (systems of interest, geographic boundary, temporal boundary) and what is inside and outside of the analysis scope
2. Define accidents or losses of concern for the system
3. Identify system hazards can produce the accidents or losses of concern
4. Define safety constraints and functional requirements that prevent hazards from developing into losses
5. Develop a functional control diagram for the system that describes interactions between actors or components
6. Identify how hazardous states may occur from inadequate control or enforcement of safety constraints

7. Develop causal scenarios that identify how unsafe control actions may occur
8. Develop design changes, requirements, analyses, or recommendations that mitigate or prevent unsafe control actions
9. Identify potential control degradation mechanisms and develop additional controls to mitigate or prevent loss of protection

The first step is defining the boundary of the analysis. This requires setting as initial assumptions boundaries such as the specific facility or activity considered in the analysis, the geographic boundary of the analysis, and the temporal boundary considered. The boundaries help constrain the development of hazards, losses, constraints, and requirements on the system in later stages of the hazard control based analysis. The scope of the analysis, including the level of design detail needed in final analysis (e.g., facility versus component level analysis) to support licensing analyses should also be specified. This will help detail the level of detail needed in developing the system engineering models.

The main analysis steps for the hazard control based analysis method are based on the STPA methodology. Further background and detailed guidance on these analysis steps is available in both Engineering A Safer World [72] and the STPA Handbook [93].

The second step in the analysis is defining accidents or losses of concern for the system and identifying hazards that can produce these losses. The STPA handbook defines losses as any event or condition that involves loss of value to stakeholders. This may include loss of human life or injury, environmental contamination, loss of plant production, loss of SSCs operability, loss of reputation or public trust, or any other loss of concern for stakeholders [93].

The third step in the analysis to identify system level hazards that can result in these losses. Unlike prior definitions of hazards in this work, a hazard in the context of a hazard based analysis is "is a system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to a loss" [93]. This focus places emphasis on the actual states of particular interest to stakeholders and not on materials that are conventionally hazardous (e.g., stored energy) but could not lead to a loss. Each hazard should be traceable to one or more of the identified losses. If an identified hazard does not have a corresponding loss, it should be excluded or the list of losses should re-evaluated. Note that hazards are distinctly different from failures, initiating events, or external factors – they are specifically the system state that leads to a loss.

As part of this process, analysts should review hazards and determine if it is possible to eliminate hazards by design. Minimizing number of hazards increases the inherent safety of a facility of activity by actively removing loss pathways. If hazards cannot be eliminated, the goal of the designer to should be to reduce hazards and minimize the potential losses associated with the hazard. These remaining hazards must be controlled through both design and operations.

The fourth step in the analysis is developing safety constraints and functional requirements that prevent hazards from developing into losses. The safety constraints specify the system behavior that is required to prevent the hazard and ultimately to prevent losses [93]. Functional requirements may include technical, operational, or organization requirements that must be satisfied to prevent hazards.

The fifth step in the analysis is to develop a functional system control structure for the system that describes interactions between different stakeholders, systems, and components. A hierarchical system-engineering model may be used in this step to provide a framework for modeling interrelationships between different systems, structures, and stakeholders. This model should include physical, digital, information, or operational controls, feedbacks, and exchanges between any components in the control structure model [93]. This model should fully encompass the analysis scope detailed in the first step of this analysis.

The use of traditional system engineering techniques may be useful in decomposing the system design to its functional components. Decomposition and allocation of functional requirements of higher order system models to lower level system, subsystem, or component level models is useful for ensuring that all top level requirements are fulfilled for the analysis [72]. A system engineering approach is particularly useful if STPA is being applied early in the design process, before substantial detailed design work has been completed. This iterative process enables the inclusion of safety starting at the pre-conceptual design stage. This system engineering approach may also be employed recursively with additional functional system control structure developed for model components. This enables the decomposition of functions from high level, system characteristic to the subsystem and component levels.

Following the development of the functional system control structure, the hazards, constraints, and requirements for the analysis should be refined to ensure that they correspond to specific model components depending on the level of engineering detail available. Refinement of these hazards, constraints, and requirements reduces the inductive challenge associated with identification of unsafe control actions in the analysis [93].

The sixth step in the analysis is to identify how hazardous states may occur from inadequate control or enforcement of safety constraints. Off-normal control actions are developed for each control action or interaction between model components in the functional system control structure. Four general unsafe control action modes are used to guide analysis in STPA [93]:

- Not providing the control action leads to a hazard.
- Providing the control action leads to a hazard.
- Providing a potentially safe control action but too early, too late, or in the wrong order
- The control action lasts too long or is stopped too soon (for continuous control actions, not discrete ones)

The impact of each of the four unsafe control action modes is documented and evaluated for each control action and interaction. The evaluation should determine if the resulting unsafe control action (UCA) produces a hazard or if it does not have a negative effect on the system. If an unsafe control action produces the hazard, the unsafe control action is documented as a combination of the controller, action mode, control action, and context [93]. Figure 5.16 provides an example of this unsafe control action methodology. The corresponding hazard for each unsafe control action should also be noted to ensure traceability of hazards and UCAs.

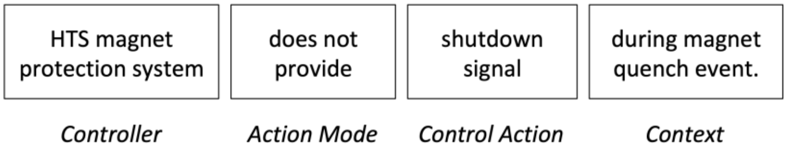


Figure 5.16. Unsafe Control Action Formulation

This step in the STPA analysis produces a list of UCAs that could produce the hazards and losses for the system that were previously identified. All UCAs should correspond to one or more hazards and all hazards should have at least one identified UCA [93]. If a hazard does not have a corresponding UCA, both the analysis scope and the functional system control structure development should be reviewed to determine if the hazard is not actually possible given the system, is outside the scope of the analysis and should be excluded, or if a UCA corresponding to the hazard has not been fully developed.

Following UCA identification, a controller constraint is developed for each UCA. A controller constraint is defined as a set of conditions or constraints that, if satisfied, prevents the UCA [93]. For the example UCA shown in Figure 5.16, a corresponding controller constraint would be:

> "HTS magnet protection system must provide the system shutdown signal during a magnet quench event."

This controller constraint is a binary constraint; quantifiable technical characteristics should be specified where appropriate for other controller constraints derived from UCAs (e.g., "provided within a 1 second"). A corresponding controller constraint is developed for each UCA.

The seventh step in the analysis is developing causal scenarios for each UCA that identify how unsafe control actions may occur. These scenarios consist of two major classes of events:

- Unsafe control actions occurring
- Control actions being improperly executed or not executed

The first class of control actions relates directly to the controllers while the second class of control actions relates to the controlled processes or components. Common types of unsafe control action scenarios for the first class of events include:

- Unsafe controller behavior
- Inadequate or incorrect controller feedback

Unsafe controller behavior may occur due to a number of conditions including physical controller failures, inadequate control algorithms, unsafe controller inputs, and inadequate process models. Inadequate process models include many operator error scenarios where an operator believes they are making the correct decision but do not correctly interpret the system state. Inadequate or incorrect controller feedback can result from physical failure of feedback systems, incomplete feedback, or misinterpretation of received feedback.

Common types of scenarios for the second class of events include:

- Control actions not executed or improperly executed due to physical component failures
- Control actions not executed or improperly executed due to control command pathway failures (physical, digital, operational)
- Control actions applied but desired system state is not achieved due to other system conditions

These different scenarios characterize events where the physical system fails to prevent hazards. This includes both the failure modes normally characterized in event tree analyses (physical and control failures) and failure modes in which the component functions correctly but the existing system conditions prevent ultimate fulfillment of the safety function.

Developing these causal scenarios guide the analyst in developing events where unsafe control actions produce a hazard and loss. The goal is to develop as many scenarios that produce the unsafe control action within the scope of the analysis. Peer review can be useful at ensuring that casual scenarios have been captured for the identified UCAs. Additional details and guidance on the creation of causal scenarios is found in the STPA Handbook [93].

The eighth step in the analysis is developing design changes, requirements, analyses, or recommendations that mitigate or prevent unsafe control actions. The purpose of this step is to review casual scenarios and identify methods to increase the robustness of design by reducing the potential for unsafe control actions. Each casual scenario is reviewed and assessed to determine if there are adequate controls to prevent the unsafe control action [72]. This may include changes to design (modification to existing design or additional SSCs), changes to requirements to ensure that unsafe control actions do not develop, additional analyses or testing to validate performance of SSCs, or recommendations on operations to mitigate or prevent unsafe control actions.

This part of the analysis contributes to development of comprehensive defense-in-depth for the facility or activity. A hazard control based analysis method includes both the physical and operational controllers for a system that can create unsafe conditions and lead to losses. Developing plant capability defense-in-depth using a direct causality accident model results in relatively static design of plant capability defense in depth that may be subject to bypass based on the initiating events. Development and justification of comprehensive defense-in-depth for the facility or activity using the STPA analysis helps create a more robust design by focusing primarily on hazards that lead to losses and not on discrete initiating event.

These design changes, requirements, analyses, and recommendations should be documented as a significant part of the licensing basis of the plant. If these conditions are met, then the facility or activity should be sufficiently robust against hazards that can lead to losses. Discussions with regulators and other stakeholders may be required as part of this process to develop appropriate requirements.
The ninth step in the analysis is to identify potential control degradation mechanisms and develop additional controls to mitigate or prevent loss of protection. This can include physical degradation of SSCs, changes in analytical assumption and design bases, changes in the physical configuration of facility that invalidate existing analyses, or degradation in the operational capabilities [72]. A facility may have adequate controls when first constructed but during operation, both physical equipment and operator actions to control hazards may degrade and result in facility deviation from initial licensing assumptions. This degradation increases the potential for significant loss events. Contributing factors for nearly all major industrial accidents (e.g., 2010 Deep Water Horizon oil rig explosion, 1984 Bhopal chemical disaster, 1988 Piper Alpha gas platform disaster) can all be tied to degradation of either physical or operational safety controls [101] [73] [102].

Development of additional controls to mitigate or prevent degradation of hazard control mechanisms is as important as the development of the controls themselves because it contributes to the long-term safety of the facility or activity. Use of inspections, audits, trainings, and change management plans are all common tools that can be used to prevent degradation [72]. Relevant best practices from each discipline should be used when developing these additional controls. Finally, these controls should be documented as a significant part of the licensing basis of the plant.

It is important to note that the STPA method does not result in a quantitative assessment of safety. The STPA method is, in fact, antithetical to quantitative methods, as safety is defined as an emergent behavior of a system and not a numerical characteristic. This approach works conceptually with the non-causal model of accidents in STPA but does not align well with conventional regulatory methods that focus on demonstrating compliance with quantitative hazard consequence limits. A regulatory framework could be utilized that does not require demonstrated compliance with quantitative hazard consequence limits but for other frameworks, a quantitative consequence analysis is required. In these cases, an STPA evaluation could be paired with another licensing evaluation method (e.g., worst-case release analysis or a maximum credible release analysis) to provide quantitative insights.

The documentation developed during this hazard control analysis can be used to support reduction of the analyzed maximum credible release. Development and documentation of comprehensive defense-in-depth within the STPA analysis may enable reduction in the credible material at risk within the maximum credible release analysis. This can result in an overall reduced hazard consequence as compared with a normal maximum credible release analysis. The quantitative consequence analysis may be performed to meet any hazard consequence limit. This process, however, is done in parallel to the STPA analysis and is not part of the STPA assumptions related to the safe design and operation of systems.

A quantitative hazard consequence analysis may not be required in all regulatory frameworks. For these frameworks, documentation of the STPA analysis and formal commitment to the requirements, analyses, or recommendations to prevent unsafe control actions, along with the processes to mitigate degradation of control mechanisms, may constitute the licensing basis for the facility. This process of submitting licensing documentation demonstrating qualitative safety through design is more similar to a prescriptive process based regulatory framework than a performance based licensing framework.

5.7.3 STPA evaluation for a commercial fusion facility

An STPA evaluation is outlined in this section for a hypothetical commercial fusion facility. The regulatory burden associated with development of a hazard control licensing analysis for a full facility is significant and far outside the scope of this work. As a result, the general processes and insights for an STPA based method are considered, and STPA analyses on select systems are performed and discussed as examples. The goal of this section is to illustrate the design and regulatory burden trade-offs associated with use of STPA for licensing evaluations.

The scope of the STPA evaluations in this work is limited to the review of the deuterium-tritium storage system discussed in the Level 3 System Engineering Model in Chapter 2. This specific system is selected to allow comparison to the probabilistic and deterministic design basis analysis of the same system in Sections 5.5.3 and 5.6.3. Analysis of this system provides prospective on the regulatory burden associated with STPA evaluations and enables comparison of licensing insights that may be gained from use of STPA evaluations as compared with deterministic or probabilistic design basis analyses. The rational for selection of the deuterium-tritium storage system for this demonstration analysis provided in Section 5.5.3 also applies to this section.

The mechanical design of the simplified storage system analyzed in this analysis is presented and discussed in Appendix 5B. One unique aspect of STPA evaluations is a focus elimination, constraint, or control of system interactions that result in both desirable and undesirable emergent behaviors. As a result, this evaluation also requires definition of the control structures that detail system interactions outside the scope of traditional hazard analyses. Discussion of the control structure assumed and analyzed in this work documented in Appendix 5D and is briefly presented in this section to inform the STPA evaluation. These control structures are based on the functional decomposition performed in the Level 3 System Engineering Model in Chapter 2.

This work performs an STPA evaluation on the Tritium Storage Bed system within the deuterium-tritium storage system. The STPA methodology starts by identifying system level losses and hazards (Step 2 and Step 3) relevant to the deuterium storage system, and then develop safety constraints, controller constraints, and additional requirements based on a structured analysis of system interactions. Performing an STPA evaluation of the Level 3 Function Block for the Deuterium-Tritium Storage System outside of an active design process is challenging due to the limited assignment of functions to specific systems. The Level 3 Function Block for the Deuterium-Tritium Storage System is further decomposed into partial Level 4 and Level 5 functional blocks to enable more concise description and evaluation of system interactions. This process approximately follows the same decomposition performed in Chapter 2. Table 5.23 summarizes the function blocks used in this model.

Table 5.23. Functional Decomposition for STPA Evaluation

Level 3 Model Function Block	*Decomposed Level 4 Function Blocks*	*Decomposed Level 5 Function Blocks*
Plant Engineering and Safety Systems/Org	N/A – No Further Decomposition	
Plant Operations Control System/Org	N/A – No Further Decomposition	
Plant Environment Control Systems	N/A – No Further Decomposition	
Plant Utility Systems	N/A – No Further Decomposition	
D-T Storage System	D-T Clean Up / Removal Systems	Glove Box Clean-up System
		D-T Storage System Building Ventilation
		D-T Storage System Building Stack
	D-T Structural Confinement Barriers	Tritium Glove Box
		D-T Storage System Building
	Hydrogen Storage/ Handling System	Tritium Storage Bed
		Tritium Processing Piping
		Deuterium Storage System
		Deuterium Processing Piping

In this work, a full STPA evaluation is only outlined and demonstrated for the Tritium Storage Bed. The project scope was limited for the following reasons:

- Tritium Storage Bed is the largest single contributor to potential system losses and hazards based on radiological and explosive hazards
- Analysis of Tritium Storage Bed is representative of insights that may be gained through the detailed evaluations of other systems
- Engineering effort is required to complete a full STPA evaluation for all systems is outside the scope of this work and was not expected to significantly change insights gain on STPA evaluations

Safety constraints, controller constraints, and unsafe control actions are developed for all systems and interactions but detailed causal scenarios and additional requirements are only developed for the Tritium Storage Bed. This analysis demonstrates how different insights may be obtained using STPA and how the methodology may be used to transparently generate performance based requirements for engineered systems.

5.7.3.1 Defining analysis boundaries

The first step in the STPA evaluation is the definition of analysis boundary (systems of interest, geographic boundary, temporal boundary) and what is inside and outside of the analysis scope. This analysis is limited to the D-T Storage System and the interfacing control systems presented in Table 5.23. Potential upstream or downstream system interactions are not considered in this analysis. In the STPA evaluation, any geographic or temporally relevant losses of concern for the system are considered. In the final step of the analysis, a deterministic maximum credible release analysis is considered to enable comparison to quantitative design limits. The boundaries of this deterministic analysis are limited to the catastrophic, acute, local geographic releases of tritium or tritiated materials from a commercial fusion facility. Deposition of tritium into the biosphere and chronic impacts of tritium contamination are not considered. On-site or worker protection considerations are not also considered in the analysis due to the ability to control worker exposure through administrative controls.

5.7.3.2 Defining losses of concern

The second step in the STPA evaluation is to define accidents or losses of concern for the system. The losses of concern are based on general discussion in Chapter 3 on the hazards and accidents of concern for major industrial facilities. Table 5.24 lists the losses defined for this evaluation. These losses are applicable to all facilities as well as all system in a commercial fusion facility. Justification for these losses is provided in Chapter 3. These losses are the basis for the definition of all hazards, constraints, and requirements in an STPA evaluation and are intended to be encompassing of possible facility hazards.

Table 5.24. Losses of Concern for Commercial Fusion Facility

Loss Number	Defined Losses
L-1	On-site personnel injury or death
L-2	Off-site community injury or death
L-3	Environmental contamination
L-3.1	On-site environmental contamination
L-3.2	Off-site environmental contamination
L-4	On-site economic impacts
L-4.1	On-site loss of employment
L-4.2	On-site facility damage
L-4.3	Poor capacity factor
L-4.4	Loss of economic viability
L-4.5	Negative image
L-4.6	Legal liability
L-5	Production outage
L-6	Off-site socioeconomic impacts
L-6.1	Off-site evacuation
L-6.2	Off-site loss of employment
L-6.3	Psychological effects
L-6.4	Off-site property damage
L-6.5	Off-site property value

5.7.3.3 Identifying system hazards

The third step in the STPA evaluation is to identify system hazards can produce the accidents or losses of concern for this system. The hazard identification process performed in Chapter 3 identified several licensing significant hazards:

- Radioactive material: gaseous tritium and tritiated compounds
- Radioactive material: solid tritium metallic compounds
- Explosive material: hydrogen gas
- Hazardous material: asphyxiants – helium, cryogenic coolants
- Direct radiation exposure: β radiation and tritium contaminated materials

Hazardous materials including asphyxiants (e.g., helium, cryogenic coolants) are not considered in this section due to small quantities likely present in the D-T Storage System. These hazardous materials would need to be considered in a larger analysis that included maintenance activities as work in confined spaces could present a significant risk for on-site personnel even in relatively small quantities.

In other parts of this thesis, hazards are generally described as any material or process that may cause harm or a loss. Recall that in this section of the thesis, a hazard within an STPA evaluation “is a system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to a loss” [93]. As result, the licensing significant hazards described in Chapter 4 are adapted to an STPA defined hazard by not just the material or process but providing context on the conditions that could lead to a loss. The relevant high-level loss for each defined hazard is specified to ensure traceability between derived requirements and the losses of interest.

Seven high-level hazards are identified for the D-T Storage System based on decomposition to the system to Level 4 Function Blocks. These seven high-level hazards are further refined into the STPA evaluation relevant hazards by defining hazards to Level 5 Function Blocks described in Table 5.23. Table 5.25 summarizes the hazards identified for the D-T Storage System.

Review of the hazards identified in the Table 5.25 reveal that the loss of confinement of radiological material is the primary hazard. The robust D-T storage system design with multiple barriers to radiological material release to the environment results in identification of four hazards relevant to worker safety and operational reliability (H-1, H-2, H-4, H-5) and only one hazard relevant to public safety (H-6). These hazards also reflect the known failure mechanisms for a simple and fairly well characterized system. The STPA process of hazard identification based on losses of interest could be particularly valuable for novel systems or systems early in the design process where non-trivial hazards could impacts on-site, off-site, or economic stakeholders.

Table 5.25. D-T Storage System Identified Hazards

STPA Defined Hazards	*Hazard Number*	*Relevant Losses*
Tritium release from processing systems	H-1	L-4, L-5
Unplanned release of tritium from Tritium Storage Bed	H-1.1	
Release of tritium from Tritium Storage Bed into Tritium Glove Box	H-1.2	
Release of tritium from Tritium Process Piping into Tritium Glove Box	H-1.3	
Tritium release into worker areas	H-2	L-1, L-4, L-5
Release of tritium from Tritium Process Piping into D-T Storage System Building	H-2.1	
Release of tritiated material from Tritium Glove Box	H-2.2	
Release of tritium from Glove Box Clean Up into D-T Storage System Building	H-2.3	
Deuterium release into worker areas	H-3	L-1, L-4, L-5
Release of deuterium from Deuterium Storage System into D-T Storage Building	H-3.1	
Release of deuterium from Deuterium Process Piping into D-T Storage Building	H-3.2	
Hydrogen fire or explosion	H-4	L-1, L-4, L-5
Hydrogen fire or explosion in Tritium Storage Bed	H-4.1	
Hydrogen fire or explosion in Tritium Glove Box	H-4.2	
Hydrogen fire or explosion in D-T Storage System Building	H-4.3	
Released tritium not cleaned up or removed	H-5	L-1, L-4, L-5
Tritiated material is not cleaned up from Tritium Glove Box	H-5.1	
Tritiated material is not removed from D-T Storage System Building	H-5.2	
Unmitigated release from D-T Storage System Building	H-6	L-1, L-2, L-3, L-4, L-6
Release of tritiated material from D-T Storage System Building	H-6.1	
Release of tritiated material from Building Ventilation System	H-6.2	
Release of tritiated material from Building Stack	H-6.3	
Facility shutdown or production reduced during normal operations	H-7	L-4, L-5
Facility operation disruption - capacity factor/production reduced	H-7.1	
Facility shutdown by safety systems	H-7.2	

5.7.3.4 Defining safety constraints

The fourth step in the STPA evaluation is to define safety constraints and functional requirements that prevent hazards from developing into losses. The hazard decomposition performed in Table 5.25 reveals the wide scope of hazards in the D-T Storage System relevant to losses of interest for a variety of stakeholders. Development of safety constraints, functional requirements, unsafe control actions, and causal scenarios for all Level 5 Function Blocks function blocks defined for the D-T Storage System would require effort outside of the scope of this analysis. In this work, the full STPA evaluation is performed for the Tritium Storage Bed and interfaced control systems. Preliminary analysis of other Level 5 Function Blocks suggested that completing the full STPA evaluation would produce a significant number of design requirements but would not likely produce significant additional insights into the applicability, strengths, or weaknesses of the STPA method for the licensing of fusion facilities.

In this work, safety constraints and functional requirements were developed for all system hazards identified in Step 3 of the STPA evaluation. The full set of safety constraints and functional requirements is documented in Appendix 5D. Table 5.26 lists the safety constraints and functional requirements relevant to the Tritium Storage Bed.

High-level safety constraints are provided for the Level 4 Function Blocks (H-1, H-4, H-7) while definition of the Level 5 Function Blocks enables definition of the functional requirements for the Tritium Storage Bed. These high-level safety constraints (e.g., "SC-1: Tritium release must be controlled or prevented from all processing systems") are not readily enforceable by design or operation but represent larger design goals for a system. In contrast, the functional requirements (e.g., "SC-1.1.1: Tritium Storage Bed must be kept under [TBD] °C unless part of a planned tritium off-loading process.") are quantifiable requirements on system performance based on design and operation. In this work, the limited design information inhibits specification of many of these functional requirements, which is why some quantified requirements are left as "[TBD]" in this work and in Table 5.26. This step, however, demonstrates how this evaluation method could integrate with design to provide quantifiable functional requirements on a system based on system hazards and losses of interest.

Table 5.26. Tritium Storage Bed Safety Constraints

Hazard Number	*STPA Hazards*	*Safety Constraint*	*Safety Constraint Functional Requirement*
H-1	Tritium release from processing systems	SC-1	Tritium release must be controlled or prevented from all processing systems.
H-1.1	Unplanned release of tritium from Tritium Storage Bed	SC-1.1.1	Tritium Storage Bed must be kept under [TBD(1)] °C unless part of a planned tritium off-loading process.
		SC-1.1.2	Tritium Storage Bed must be isolated from process piping when not on- or off-loading tritium.
		SC-1.2.3	Tritium Storage Bed must be purged to below [TBD(1)] MBq/m^3 before opening for maintenance activities.
H-1.2	Release of tritium from Tritium Storage Bed into Tritium Glove Box	SC-1.2.1	Tritium Storage Bed must have a leakage rate of less than [TBD(1)] under all possible conditions.
		SC-1.2.2	Tritium Storage Bed connections must have a leakage rate of less than [TBD(1)] under all possible conditions.
		SC-1.2.3	Tritium Storage Bed must kept under [TBD(1) pressure, temperature, mass] at all times.
H-4	Hydrogen fire or explosion	SC-4	Hydrogen gas concentration must be kept below the lower flammability limit (LFL) or above the upper flammability limit (UFL) in all configurations.

Table 5.26. Tritium Storage Bed Safety Constraints

Hazard Number	*STPA Hazards*	*Safety Constraint*	*Safety Constraint Functional Requirement*
H-4.1	Hydrogen fire or explosion in Tritium Storage Bed	SC-4.1.1	Tritium Storage Bed hydrogen gas concentration must kept below the LFL or above the UFL in all configurations
H-7	Facility shutdown or production/ capability reduction during normal operations	SC-7	Facility operations must be designed to meet minimum safety requirements while maximizing capacity factor.
H-7.1	Facility operation disruption - capacity factor/production reduced	SC-7.1.1	Facility must have a capacity factor of greater than [TBD$^{(1)}$] averaged over a period of [TBD$^{(1)}$].
H-7.2	Facility shutdown by safety systems	SC-7.2.1	Facility must have a spurious shutdown rate and related downtime of less than [TBD$^{(1)}$] averaged over a period of [TBD$^{(1)}$].
		SC-7.2.2	Facility design must prioritize and enable preemptive shutdowns that prevent have a credible probability of resulting in catastrophic damage to a facility.

Notes: (1) Many system specific functional requirements are left as "to be determined" (TBD) and would need to be specified based on the final system design characteristics.

5.6.3.5 Developing functional control diagram

The fifth step in the STPA evaluation is to develop a functional control diagram for the system that describes interactions between systems and components. In this work, the system configuration for the Deuterium Tritium Storage System presented in Appendix 5B is expanded to include additional systems and components responsible for the control of subsystems within the Deuterium Tritium Storage System.

A functional control diagram is composed of function blocks and details Control signals and set points provided by controllers and feedback provided by actuator systems. A functional control diagram is developed for the Deuterium Tritium Storage System by analyzing the relationship between the Level 3 controller function blocks and the Level 5 actuator function blocks specified in Table 5.23. A simplified functional control diagram showing the relationship between Level 3 controller function blocks and the Level 4 actuator function blocks is presented in Figure 5.16. The full complexity functional control diagram showing the relationship between Level 3 controller function blocks and the Level 5 actuator function blocks is presented in Figure 5.17.

These functional control diagrams begin to highlight the operational complexity of modern engineering systems. Even for a relatively simple system, there are numerous overlapping control, feedback, and operational decision-making loops. As the design is further decomposed to the subsystem or component level (e.g., instrumentation or electromechanical actuators), the number of functional controls could be expected to grow exponentially. This is a potential challenge associated with use of STPA evaluations, as the analysis can become extremely large and require significant resources to complete. Gradually increasing detail in an iterative fashion may enable the analyst to determine what level of detail is needed to fully characterize the behavior of the system and assess whether specific systems need further decomposition to accurately describe their functional interactions.

Note that in Figures 5.16 and 5.17, arrows are used to connect the different functional boxes and provide information regarding physical interactions, control interactions, and feedback interactions. The standard method for completing STPA evaluations use vertical likes to indicate the hierarchical relationship (from controller to actuator) between systems [93]. In this work, this convention is not followed to allow for the simpler visualization of system structure. The relationship of controller to actuator is indicated by a solid arrow ("control interaction") and the relationship of actuator to controller is indicated by a dotted arrow ("feedback interaction"). These marked arrows should be used to characterize the hierarchical control relationship in the work and not the position of the system boxes.

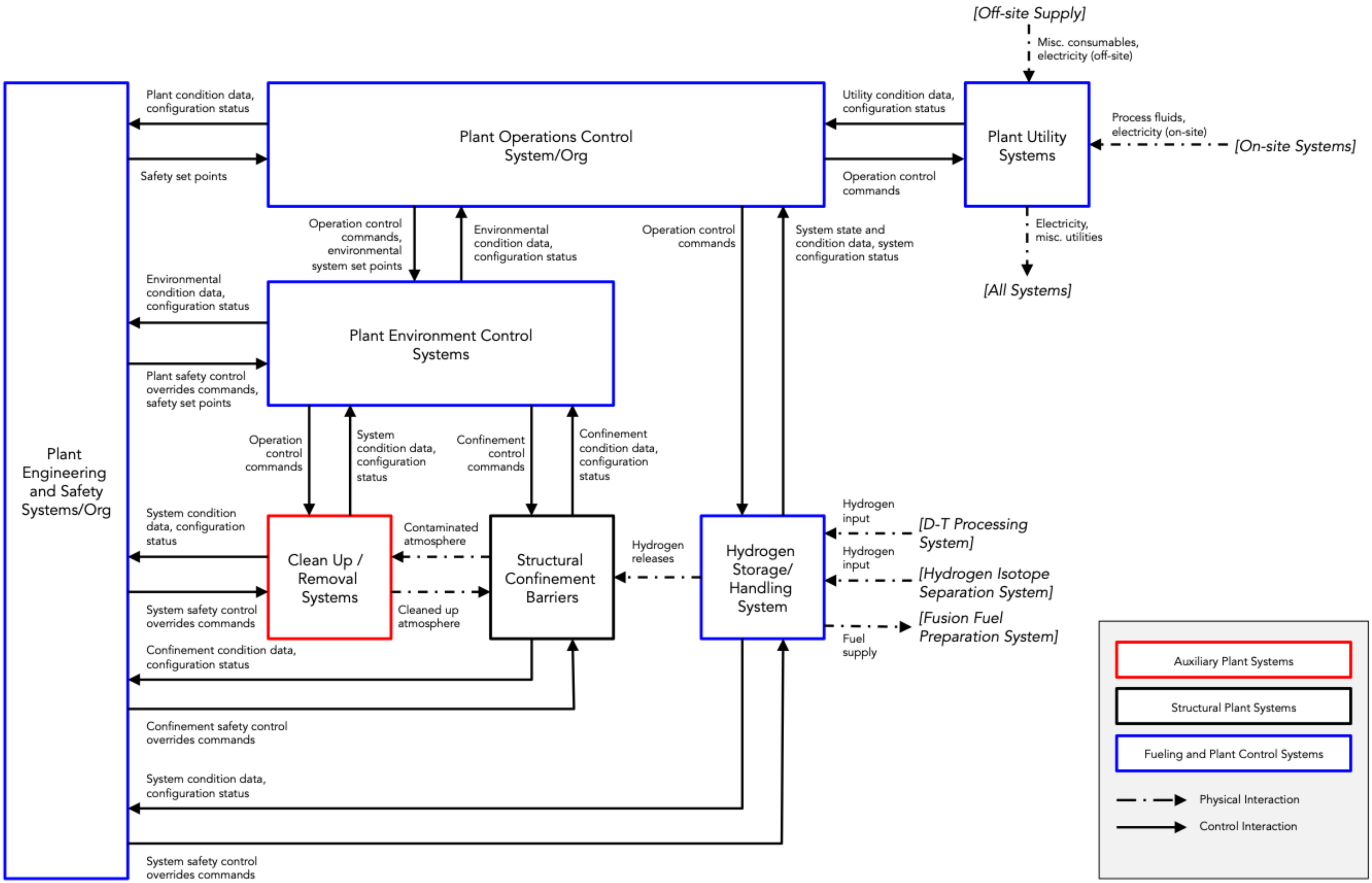

[Off-site Supply]
Misc. consumables, electricity (off-site)
Plant condition data, configuration status
Plant Operations Control System/Org
Utility condition data, configuration status
Plant Utility Systems
Process fluids, electricity (on-site)
[On-site Systems]
Safety set points
Operation control commands
Operation control commands, environmental system set points
Environmental condition data, configuration status
Operation control commands
System state and condition data, system configuration status
Electricity, misc. utilities
[All Systems]
Environmental condition data, configuration status
Plant Environment Control Systems
Plant safety control overrides commands, safety set points
Plant Engineering and Safety Systems/Org
Operation control commands
System condition data, configuration status
Confinement control commands
Confinement condition data, configuration status
System condition data, configuration status
Clean Up / Removal Systems
Contaminated atmosphere
Structural Confinement Barriers
Hydrogen releases
Hydrogen Storage/ Handling System
Hydrogen input
[D-T Processing System]
Hydrogen input
[Hydrogen Isotope Separation System]
[Fusion Fuel Preparation System]
Fuel supply
System safety control overrides commands
Cleaned up atmosphere
Confinement condition data, configuration status
Confinement safety control overrides commands
System condition data, configuration status
System safety control overrides commands
Auxiliary Plant Systems
Structural Plant Systems
Fueling and Plant Control Systems
Physical Interaction
Control Interaction

Figure 5.16. Simplified functional control diagram for Deuterium Tritium Storage System

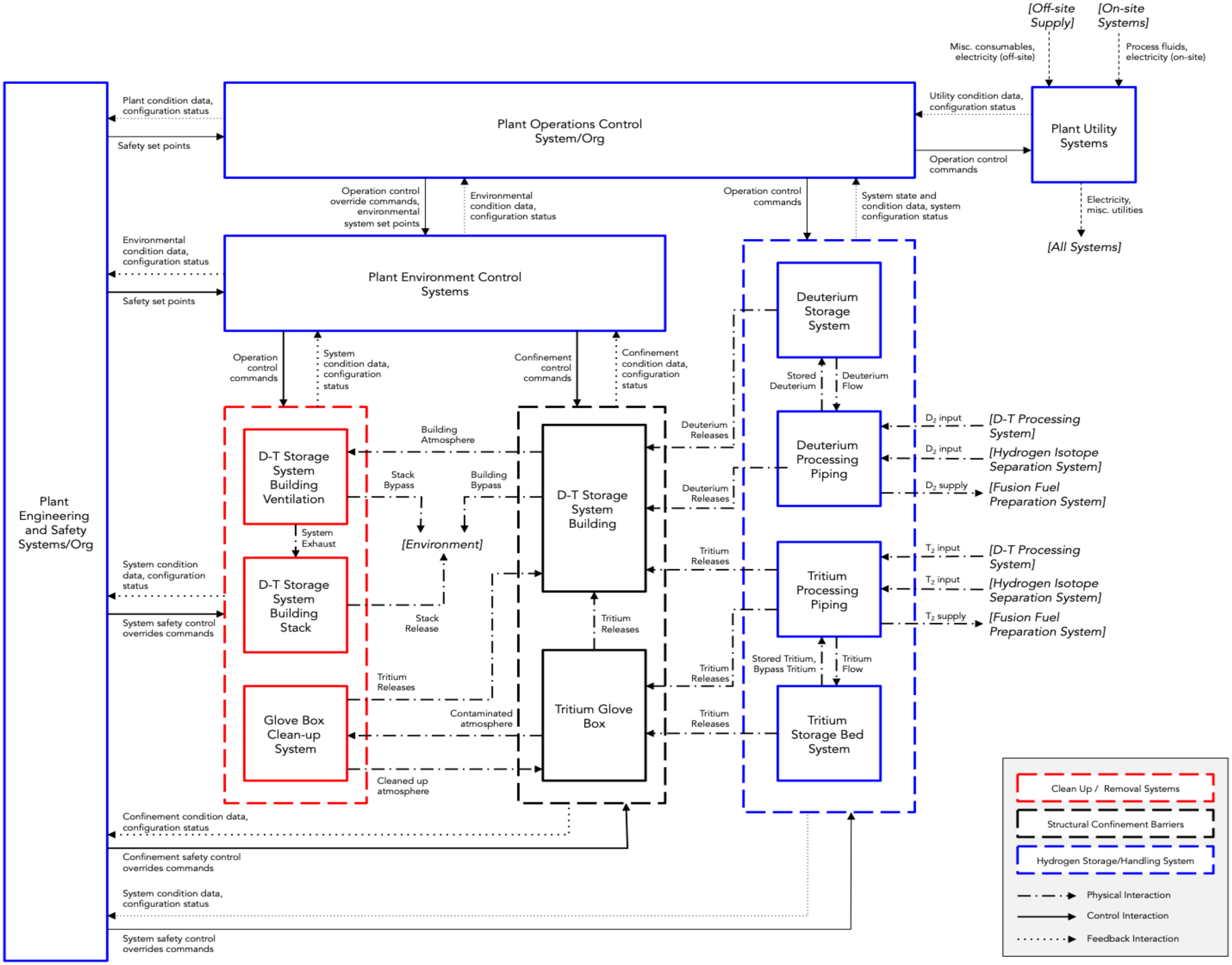

[Off-site Supply]
[On-site Systems]
Misc. consumables, electricity (off-site)
Process fluids, electricity (on-site)
Plant condition data, configuration status
Safety set points
Plant Operations Control System/Org
Utility condition data, configuration status
Plant Utility Systems
Operation control commands
Electricity, misc. utilities
[All Systems]
Operation control override commands, environmental system set points
Environmental condition data, configuration status
Operation control commands
System state and condition data, system configuration status
Environmental condition data, configuration status
Safety set points
Plant Environment Control Systems
Operation control commands
System condition data, configuration status
Confinement control commands
Confinement condition data, configuration status
Deuterium Storage System
Stored Deuterium
Deuterium Flow
Deuterium Processing Piping
D_2 input
[D-T Processing System]
D_2 input
[Hydrogen Isotope Separation System]
D_2 supply
[Fusion Fuel Preparation System]
Deuterium Releases
Deuterium Releases
Building Atmosphere
D-T Storage System Building Ventilation
Stack Bypass
Building Bypass
D-T Storage System Building
System Exhaust
[Environment]
Plant Engineering and Safety Systems/Org
System condition data, configuration status
System safety control overrides commands
D-T Storage System Building Stack
Stack Release
Tritium Releases
Tritium Processing Piping
T_2 input
[D-T Processing System]
T_2 input
[Hydrogen Isotope Separation System]
T_2 supply
[Fusion Fuel Preparation System]
Tritium Releases
Stored Tritium, Bypass Tritium
Tritium Flow
Tritium Releases
Tritium Releases
Glove Box Clean-up System
Contaminated atmosphere
Tritium Glove Box
Tritium Releases
Tritium Storage Bed System
Cleaned up atmosphere
Confinement condition data, configuration status
Confinement safety control overrides commands
System condition data, configuration status
System safety control overrides commands
Clean Up / Removal Systems
Structural Confinement Barriers
Hydrogen Storage/Handling System
Physical Interaction
Control Interaction
Feedback Interaction

Figure 5.17. Functional control diagram for Deuterium Tritium Storage System

5.7.3.6 Identifying hazardous states

The sixth step in the STPA evaluation is to identify how hazardous states may occur from inadequate control or enforcement of safety constraints. The functional control diagrams for the Deuterium Tritium Storage System describe the control actions between different function blocks. Unsafe control actions and controller constraints are developed and defined for each control action. The structured process of defining unsafe control actions and constraints is illustrated below for an example control action.

Figure 5.17 shows that the Plant Operational Control System provides operational control commands to the Hydrogen Storage and Handling System (which includes the Tritium Storage Bed). In the case of the Tritium Storage Bed, the operational control commands consist of storage bed temperature and valve alignment commands. For this control action, four types unsafe control actions are considered in the STPA methodology:

- Not providing operational control commands leads to a hazard
- Providing the operational control commands leads to a hazard
- Providing a potentially safe operational control command too early, too late, or in the wrong order
- The operational control commands lasts too long or is stopped too soon

Each control action is reviewed for each type of unsafe control action to determine whether the situation would lead to a hazard or whether it does not present a hazard. Table 5.27 lists the unsafe control actions that are reviewed for the Plant Operational Control System and Tritium Storage Bed interactions. The process for developing the unsafe control actions and control constraints is described below.

The four unsafe control action types are first used to develop unsafe general unsafe control actions according the STPA methodology. Each unsafe control action is then reviewed to determine whether it will lead to a hazard or will not produce a hazard. If it will lead to a hazard, the relevant hazard is specified to ensure to traceability in requirements. A corresponding controller constraint is then developed for each unsafe control action that, if satisfied, would prevent the unsafe control action from occurring. Due to the level of design detail, these constraints are a mix of design constraints (operational actions must occur) and performance constraints (certain conditions must be achieved or maintained). At more detailed stages of design, these constraints could be iteratively developed into design criteria or design performance requirements.

This process of identifying unsafe control actions and developing controller constraints is repeated for the thirty control actions between the Level 3 controller function blocks and the Level 4 actuator function blocks (Figure 5.16) and the Level 5 actuator function blocks (Figure 5.17). The full list of identified unsafe control actions is provided in Appendix 5D.

Table 5.27. Example Tritium Storage Bed Unsafe Control Actions

Control Action (CA)	*CA-8.2: POC provides bed temperature and valve configuration commands to Tritium Storage Bed*		
Control Deviation	*Unsafe Control Action (UCA)*	*Relevant Hazards*	*Controller Constraint (CC)*
Not providing causes hazard	UCA-39.2: POC does not provide bed temperature and valve configuration commands to Tritium Storage Bed to control operation in a safe, operable state	H-1.1, H-1.2, H-4.1	CC-54: POC must provide bed temperature and valve configuration commands to the Tritium Storage Beds to maintain SC-1.1.# and SC-1.2.#, and meet all operational and safety set points
Providing (or providing incorrectly) causes hazard	UCA-40.2: POC provides incorrect bed temperature and valve configuration commands to Tritium Storage Bed when systems are operating in a safe state	H-1.1, H-1.2, H-4.1, H-7.1	CC-58: POC bed temperature and valve configuration commands must be verified before being provided to the Tritium Storage Beds
Too early, too late, out of order causes hazard	UCA-41.2: POC provides bed temperature and valve configuration commands to Tritium Storage Bed after systems have been in an unsafe or inoperable state (too late)	H-1.1, H-1.2, H-4.1	CC-62: POC must provide bed temperature and valve configuration commands to the Tritium Storage Bed within [TBD](Note 1) seconds of violations of SC-1.1.#, SC-1.2.#, or operational or safety set points
Too long or stopped too soon causes hazard	UCA-42.2: POC stops providing bed temperature and valve configuration commands to Tritium Storage Bed before systems are returned to safe, operating state (stopped too soon)	H-1.1, H-1.2, H-4.1	CC-66: POC must continue to provide bed temperature and valve configuration commands to the Tritium Storage Bed until the system satisfies operational and safety set points

Notes: (1) Many controller constraints are left as “to be determined” (TBD) and would need to be specified based on the final system design characteristics.

5.7.3.7 Developing causal scenarios

The seventh step in the STPA evaluation is to develop causal scenarios that identify how unsafe control actions may occur. For each unsafe control action, the analyst develops scenarios that describe different mechanisms that enable the unsafe control action. As previously discussed two separate classes of scenarios are initially considered [93]:

- Unsafe control actions occurring
    - Unsafe controller behavior
    - Inadequate or incorrect controller feedback
- Control actions being improperly executed or not executed

  - Control actions not executed or improperly executed due to physical component failures
  - Control actions not executed or improperly executed due to control command pathway failures (physical, digital, operational)
  - Control actions applied but desired system state is not achieved due to other system conditions

Scenarios are developed for each unsafe control action should include all mechanistically possible scenarios regardless of probability. As a result, care must be taken in the analyst to ensure that the developed scenarios are appropriately broad so that a large number of overlapping scenarios are developed. The level of detail in these scenarios will also vary significantly depending on the level of design information available. Guidance on performing STPA evaluations provide additional details on developing causal scenarios.

In this work, causal scenarios are developed for the eleven unsafe control actions related to the Tritium Storage Bed. Each unsafe control action in this work is characterized with between two and six causal scenarios. As an example, the causal scenarios for UCA-39.2 (described in Table 5.27) that characterizes interactions between the Plant Operation Control (POC) System and the Tritium Storage Bed are developed and presented in Table 5.28. The full list of causal scenarios developed for the Tritium Storage Bed is provided in Appendix 5D.

Review of the scenarios in Table 5.28 illustrates that only development of high level scenarios related to function failure of systems is possible in this example due to the level of design information available. If an STPA evaluation is performed on a system with a greater degree of design information available, more specific causal scenarios could be developed.

These scenarios also highlight the failure mechanisms that are not normally considered in other evaluation methods. For example, Casual Scenario UCA-39.2:CS-5 demonstrates how a system can operate correctly and meet all performance requirements but fail to fulfill the design basis function if system conditions deviate in a way that cannot be detected and compensated for by operational systems. This scenario could develop if an exothermic reaction caused by air ingress to a Tritium Storage Bed [103] caused bed temperature to increase independent of commands to Tritium Storage Bed heaters. While air ingress is a known failure mechanism for Tritium Storage Beds, the STPA process helps identify the failure mechanism in an operational context and enables analysts to identify possible design or operational requirements to address the casual scenario.

Note that the UCA causal scenarios and UCA CS derived constraints in Table 5.28 are incomplete based on the limited design information and concept of operations for the Tritium Storage Beds. More specific causal scenarios could be developed that provide specific insights on conflicting feedback related to the unsafe control actions in Table 5.27 based on the design configuration and operation. These improved scenarios would facilitate development of more specific design constraints in Table 5.28.

Table 5.28. Example Tritium Storage Bed Causal Scenario and Derived Constraints

CC-54	*The POC must provide bed temperature and valve configuration commands to the Tritium Storage Beds to maintain SC-1.1.# and SC-1.2.#, and meet all operational and safety set points.*		
UCA-39.2	*POC does not provide bed temperature and valve configuration commands to Tritium Storage Bed System to control operation in a safe, operable state*		
UCA Number	*UCA Causal Scenario*	*Constraint Number*	*UCA CS Derived Constraint* (Note 1)
UCA-39.2:CS-1	POC receives incomplete or incorrect feedback indicating Tritium Storage Bed in safe state when unsafe state actually exists and does not provide correct operational commands (heating, valve configuration) to return system to safe state	CC-54:UCA-39.2:CS-1.1	Tritium Storage Bed conditions provided to POC must be accurate within [TBD - Accuracy Measure] with a reliability greater than [TBD - Reliability Measure]
UCA-39.2:CS-2	POC receives feedback indicating Tritium Storage Bed in unsafe state but incorrectly interprets it as a safe state and does not provide correct operational commands (heating, valve configuration)	CC-54:UCA-39.2:CS-2.1	POC must provide operational commands (heating, valve configuration) to Tritium Storage Bed with accuracy of [TBD - Accuracy Measure] and a reliability of [TBD - Reliability Measure]
UCA-39.2:CS-3	POC correctly provides operational commands based on Tritium Storage Bed feedback but operational commands (heating, valve configuration) is not received and actuated by D-T systems	CC-54:UCA-39.2:CS-3.1	POC-Tritium Storage Bed control interface must transmit commands with a reliability of [TBD - Reliability Measure]
UCA-39.2:CS-4	POC correctly provides operational commands to Tritium Storage Bed and command is received, but system does not actuate (physical controller failure)	CC-54:UCA-39.2:CS-4.1	Tritium Storage Bed must have an on-demand operational reliability of [TBD - Reliability Measure]
UCA-39.2:CS-5	POC correctly provides operational commands to Tritium Storage Bed, command is received, system actuates, but the commands do not maintain a safe and operable state (other system conditions)	CC-54:UCA-39.2:CS-5.1	Tritium Storage Bed must provide feedback if POC operational commands do not produce expected system behavior within [TBD] seconds of actuation and a reliability of [TBD - Reliability Measure]

Notes: (1) Many UCA CS derived constraints are left as "to be determined" (TBD) and would need to be specified based on the final system design characteristics.

5.7.3.8 Mitigating unsafe control actions

The eighth step in the STPA evaluation is to develop design changes, requirements, analyses, or recommendations that mitigate or prevent unsafe control actions. Each of the unsafe control action causal scenarios should be addressed with one or more design or operational features that prevent, mitigate, or relieve the unsafe control action. The proposed response to the unsafe control action causal scenario will vary drastically on a range of factors in including the system, the controllers, and the level of design detail available.

In this work, design changes, requirements, analyses, or recommendations are developed for each of the unsafe control action causal scenarios developed for the Tritium Storage Bed in step seven. As an example, derived constraints for the UCA-39.2 causal scenarios (Table 5.28) are developed and presented in Table 5.28 for each scenario. Table 5.28 demonstrates how each derived constraint can be traced through a casual scenario and, ultimately, to unsafe control actions, hazards, and losses. This traceability helps eliminate unnecessary design requirements from the regulatory basis and ensure that design constraints considered for licensing purposes are needed to ensure safe operation. The full list of derived constraints developed for the Tritium Storage Bed is provided in Table 5.29 and is sorted by constraint type (actuator requirement, controller requirement, design constraint, design requirement, and interface requirement).

Table 5.29. Tritium Storage Bed Design Constraints and Requirements

Constraint Number	*Constraint Requirement* (Note 1)	*Constraint Type*
CC-28:UCA-22.2:CS-1.1	Tritium Storage Bed conditions provided to PES must be accurate within [TBD - Accuracy Measure] with a reliability greater than [TBD - Reliability Measure]	Actuator Requirement
CC-28:UCA-22.2:CS-5.1	Tritium Storage Bed must have an on-demand emergency actuation reliability of [TBD - Reliability Measure]	Actuator Requirement
CC-28:UCA-22.2:CS-6.1	Tritium Storage Bed must provide feedback on whether PES emergency actuation returned system to safe state within [TBD] seconds of actuation and a reliability of [TBD - Reliability Measure]	Actuator Requirement
CC-28:UCA-26.2:CS-3.1	Tritium Storage Bed must receive command actuation signal within [TBD] seconds of being issued by PES	Actuator Requirement
CC-28:UCA-26.2:CS-4.1	Tritium Storage Bed must actuate within [TBD] seconds of receiving an emergency actuation command from PES	Actuator Requirement
CC-32:UCA-23.2:CS-5.1	Tritium Storage Bed must have a spurious operation rate of less than [TBD - Reliability Measure]	Actuator Requirement
CC-36:UCA-24.2:CS-3.1	Tritium Storage Bed must default to safe clean up actuation command if incomplete/conflicting feedback is suspected from PES	Actuator Requirement
CC-36:UCA-24.2:CS-4.1	Tritium Storage Bed must be designed to fail into safe state	Actuator Requirement
CC-40:UCA-27.2:CS-4.1	Tritium Storage Bed must remain in safe state (emergency actuation) until all safety constraints and set points are verified	Actuator Requirement
CC-54:UCA-39.2:CS-1.1	Tritium Storage Bed conditions provided to POC must be accurate within [TBD - Accuracy Measure] with a reliability greater than [TBD - Reliability Measure]	Actuator Requirement
CC-54:UCA-39.2:CS-4.1	Tritium Storage Bed must have an on-demand operational reliability of [TBD - Reliability Measure]	Actuator Requirement

Table 5.29. Tritium Storage Bed Design Constraints and Requirements

Constraint Number	*Constraint Requirement* (Note 1)	*Constraint Type*
CC-54:UCA-39.2:CS-5.1	Tritium Storage Bed must provide feedback if POC operational commands do not produce expected system behavior within [TBD] seconds of actuation and a reliability of [TBD - Reliability Measure]	Actuator Requirement
CC-62:UCA-41.2:CS-3.1	Tritium Storage Bed must receive operational command signal within [TBD] seconds of being issued by POC	Actuator Requirement
CC-62:UCA-41.2:CS-4.1	Tritium Storage Bed must actuate within [TBD] seconds of receiving an operational command from POC	Actuator Requirement
CC-28:UCA-22.2:CS-2.1	PES up be must resilient against single point failure for feedback from Tritium Storage Bed	Controller Requirement
CC-28:UCA-22.2:CS-3.1	PES operation must provide emergency actuation commands to Tritium Storage Bed with accuracy of [TBD - Accuracy Measure] and a reliability of [TBD - Reliability Measure]	Controller Requirement
CC-28:UCA-26.2:CS-2.1	PES must provide emergency actuation command on feedback signal within [TBD] seconds of receiving the feedback	Controller Requirement
CC-32:UCA-23.2:CS-3.1	PES must have spurious emergency actuation command rate to Tritium Storage Bed of less than [TBD - Frequency Measure]	Controller Requirement
CC-36:UCA-24.2:CS-1.1	PES must default to a safe state emergency actuation command to Tritium Storage Bed on incomplete, conflicting, or loss of all feedback from Tritium Storage Bed	Controller Requirement
CC-40:UCA-27.2:CS-1.1	PES must not allow stop of emergency actuation command to Tritium Storage Bed until satisfaction of all safety constraints and set points is verified	Controller Requirement
CC-44:UCA-28.2:CS-1.1	PES must stop emergency actuation command within [TBD] seconds of verification of satisfaction of all safety constraints and set points	Controller Requirement
CC-54:UCA-39.2:CS-2.1	POC must provide operational commands (heating, valve configuration) to Tritium Storage Bed with accuracy of [TBD - Accuracy Measure] and a reliability of [TBD - Reliability Measure]	Controller Requirement
CC-58:UCA-40.2:CS-1.1	POC must not be able to provide operational commands to Tritium Storage Bed that produce an unsafe condition	Controller Requirement
CC-58:UCA-40.2:CS-3.1	POC must have spurious actuation command rate to Tritium Storage Bed of less than [TBD - Frequency Measure]	Controller Requirement
CC-62:UCA-41.2:CS-2.1	POC must provide operational command on feedback signal within [TBD] seconds of receiving the feedback	Controller Requirement
CC-66:UCA-42.2:CS-1.1	POC up be must resilient against single point failure for feedback from Tritium Storage Bed	Controller Requirement
SC-1.1.1	Tritium Storage Bed must be kept under [TBD] °C unless part of a planned tritium off-loading process.	Design Constraint
SC-1.1.2	Tritium Storage Bed must be isolated from process piping when not on- or off-loading tritium.	Design Constraint
SC-1.2.1	Tritium Storage Bed must have a leakage rate of less than [TBD] under all possible conditions.	Design Constraint
SC-1.2.2	Tritium Storage Bed connections must have a leakage rate of less than [TBD] under all possible conditions.	Design Constraint
SC-1.2.3	Tritium Storage Bed must be purged to below [TBD] MBq/m^3 before opening for maintenance activities.	Design Constraint
SC-1.2.3	Tritium Storage Bed must be kept under [TBD pressure, temperature, mass] at all times.	Design Constraint
SC-4.1.1	Tritium Storage Bed hydrogen gas concentration must be kept below the LFL or above the UFL in all configurations	Design Constraint

Table 5.29. Tritium Storage Bed Design Constraints and Requirements

Constraint Number	*Constraint Requirement* (Note 1)	*Constraint Type*
CC-28	The PES must provide emergency actuation command to the tritium storage bed for shutdown and isolation within [TBD] seconds if the tritium storage bed shutdown and isolation is not actuated within [TBD] seconds of detecting a glove box tritium concentration of greater than [TBD - Set Point] MBq/m^3, exceeding SC-1.1.# or SC-1.2.#, or receiving full system shutdown command	Design Requirement
CC-32	PES must not provide emergency actuation commands to the tritium storage bed if all safety constraints and set points are satisfied	Design Requirement
CC-36	PES emergency actuation command to the tritium storage bed must result in design basis emergency shutdown and isolation of the tritium storage bed	Design Requirement
CC-40	PES must prevent operation of the tritium storage bed following shutdown until all safety constraints and set points are satisfied	Design Requirement
CC-44	PES must enable operation of the tritium storage bed following shutdown within [TBD] seconds of satisfaction of all safety constraints and set points	Design Requirement
CC-54	The POC must provide bed temperature and valve configuration commands to the tritium storage beds to maintain SC-1.1.# and SC-1.2.#, and meet all operational and safety set points.	Design Requirement
CC-58	The POC bed temperature and valve configuration commands must be verified before being provided to the Tritium Storage Beds	Design Requirement
CC-62	The POC must provide bed temperature and valve configuration commands to the tritium storage bed within [TBD] seconds of violations SC-1.1.#, SC-1.2.#, or operational or safety set points	Design Requirement
CC-66	The POC must continue to provide bed temperature and valve configuration commands to the tritium storage bed until the system satisfies operational and safety set points	Design Requirement
CC-28:UCA-22.2:CS-4.1	PES-Tritium Storage Bed control interface must transmit commands with a reliability of [TBD - Reliability Measure]	Interface Requirement
CC-28:UCA-25.2:CS-1.1	PEC-Tritium Storage Bed actuation status feedback to PES must be accurate within [TBD - Accuracy Measure] with a reliability greater than [TBD - Reliability Measure]	Interface Requirement
CC-28:UCA-26.2:CS-1.1	PES-Tritium Storage Bed control interface must provide feedback within [TBD] seconds of unsafe condition	Interface Requirement
CC-32:UCA-23.2:CS-4.1	PES-Tritium Storage Bed control interface must be designed to reduce spurious commands to a rate of less than [TBD - Reliability Measure]	Interface Requirement
CC-54:UCA-39.2:CS-3.1	POC-Tritium Storage Bed control interface must transmit commands with a reliability of [TBD - Reliability Measure]	Interface Requirement
CC-62:UCA-41.2:CS-1.1	POC-Tritium Storage Bed control interface must transmit feedback within [TBD] seconds of unsafe condition	Interface Requirement

Notes: (1) Many of the constraint requirements are left as "to be determined" (TBD) and would need to be specified based on the final system design characteristics.

Review of the derived constraints in Table 5.29 illustrates the potential impact of STPA evaluations on the design and regulation of commercial fusion systems. Despite a limited amount of available design information, a functional hazard-based approach enabled systematic identification of 48 different design constraints or requirements related to a relatively simple Tritium Storage Bed system. These constraints include both general design constraints (e.g., "CC-40: PES must prevent operation of the tritium storage bed following shutdown until all safety constraints and set points are satisfied") and specific operational requirements (e.g., "CC-40:UCA-27.2:CS-4.1: Tritium Storage Bed must remain in safe state [emergency actuation enabled] until all safety constraints and set points are verified"). These requirements could serve as the basis for system specific, performance-based licensing requirements that are derived using a standardized, common regulatory evaluation progress.

The large number of constraints for a simple system, many of which require additional details or decomposition into enforceable design or operational constraints, simultaneously highlights potential drawbacks of STPA evaluations. The first major drawback is the number of constraints developed. This drawback is challenging because a high number of constraints highlights potential vulnerabilities eliminated by design or operation but also may become a regulatory or operational burden. The number of constraints will also increase if the constraints are further decomposed based on increasing levels of design information.

The second major drawback is the additional detail required for many of the requirements. Many constraints have "To Be Determined [TBD]" left as a placeholder for quantitative requirements. Developing these values would require additional system specific analyses or policy decisions on design characteristics such as minimum reliability for systems important to safety. This process could require significant additional design or regulatory effort. Additionally, it is possible for analysts to intentionally or unintentionally revert to either casual event safety paradigm (safety through multiple layers of protection) or a probabilistic event safety paradigm (safety through sufficiently high reliability). Care must be taken when developing requirements to ensure that the evaluation does not simply revert to a deterministic or probabilistic analysis method, missing potential safety insights gained from a hazard-based approach.

Despite these limitations, these constraints demonstrate how a technology and design agnostic regulatory evaluation process can be used to develop facility-specific design and performance requirements based on hazard centered approach.

5.7.3.9 Identify control degradation mechanisms

The ninth step in the STPA evaluation is to identify potential control degradation mechanisms and develop additional controls to mitigate or prevent loss of protection. Each of the design or operational constraints developed in step eight of the STPA evaluation should be reviewed to identify any potential degradation mechanisms (e.g., physical, operational, organizational) that may lead to a loss of hazard control. Additional controls are then developed for each of these mechanisms to enable robust safety during facility operations.

In this work, control degradation mechanisms and additional controls are developed for the Tritium Storage Bed safety constraints developed in step eight. As an example, degradation mechanisms and additional controls for the UCA-39.2 causal scenarios (Table 5.28) are developed and presented in Table 5.30 for each causal scenario controller constraint. The full set of control degradation mechanisms and additional controls for the Tritium Storage Bed safety constraints developed in step eight are provided in Appendix 5D.

Review of the degradation mechanisms in Table 5.30 highlight that the degradation and breakdown of control mechanisms considered in this analysis are tied primarily to degradation physical components relied up for control actions or actuation, and the impact of configuration changes on control structures, set points, and operation. For operational systems with human operators discussed in Appendix 5D, degradation of operator action or response was also identified as a potential degradation mechanisms. These mechanisms align with historically observed root causes identified for major accidents. Major systems rarely fail catastrophically upon first operation due to the care taken by initial commissioning and operational teams to act cautiously, observe all procedures, and ensure proper operation – instead failing once operation has become routine and physical degradation mechanisms or configuration changes (human initiated or environmental) have changed the operational characteristics and behavior of a complex system. Identification of these mechanisms as part of a licensing evaluation is a unique feature of STPA evaluations.

Review of the additional controls in Table 5.30 demonstrate how one possible outcome of an STPA evaluation is the explicit need for an additional facility organization to manage system quality assurance, change management, and testing and maintenance. The first major class of degradation mechanisms in Table 5.30 is degradation physical components relied up for control actions or actuation over time. Inspection, testing, and maintenance were identified in this work as primary mechanisms to prevent or mitigate this control degradation over time. Note that this testing process is just one possible type of additional controls for this degradation mechanism – specification of design or operational changes could alternatively be used to achieve the same desired result. This is both an advantage and weakness of STPA evaluations – it is a performance-based process, enabling the analyst to select different means (and not necessarily the optimal means) to achieve the same function.

The second major class of degradation mechanisms in Table 5.30 is configuration changes that affect control structures, set points, and operation. These changes may be internal or external to the system of concern. Evaluation and analysis of system interactions is critical to ensuring that the operational characteristics, basis, and operating conditions are still valid after changes. These possible interactions were the basis for the degradation control mechanism of configuration change control and verification. This recommendation is not a physical system changes but reflects the necessary fact that configurations will change during operation for a number of reasons including inspections, maintenance, and facility upgrades. Controlling these configuration changes and ensuring safe operation during them is critical to protecting the on-going safety constraints.

Table 5.30. Tritium Storage Bed Control Action Degradation Control Mechanisms

Constraint Number	*Constraint Requirement* (Note 1)	*Degradation Mechanism Number*	*Potential Degradation Mechanisms*	*Degradation Control Mechanism Number*	*Degradation Control Mechanism* (Note 1)
CC-54: UCA-39.2: CS-1.1	Tritium Storage Bed conditions provided to POC must be accurate within [TBD - Accuracy Measure] with a reliability greater than [TBD - Reliability Measure]	CC-54: UCA-39.2: CS-1.1: DM-1	Gradual physical degradation of systems and loss of accuracy/reliability	CC-54:UCA-39.2: CS-1.1:DM-1:CM-1	Test, calibrate, and verify Tritium Storage Bed operational condition feedback system performance for accuracy and reliability with a frequency of [TBD]
				CC-54:UCA-39.2: CS-1.1:DM-1:CM-2	Perform preventative maintenance on Tritium Storage Bed operational condition feedback system performance for accuracy and reliability with a frequency of [TBD]
		CC-54: UCA-39.2: CS-1.1: DM-2	Configuration changes change required accuracy or reliability	CC-54:UCA-39.2: CS-1.1:DM-2:CM-1	Review and verify operational performance requirements after configuration changes in Tritium Storage Bed or any interfacing system
		CC-54: UCA-39.2: CS-1.1: DM-3	Configuration changes results in loss of accuracy or reliability	CC-54:UCA-39.2: CS-1.1:DM-3:CM-1	Review and verify operational system characteristics after configuration changes in Tritium Storage Bed or any interfacing system
CC-54: UCA-39.2: CS-2.1	POC must provide operational commands (heating, valve configuration) to Tritium Storage Bed with accuracy of [TBD - Accuracy Measure] and a reliability of [TBD - Reliability Measure]	CC-54: UCA-39.2: CS-2.1: DM-1	Gradual physical degradation of systems and loss of reliability	CC-54:UCA-39.2: CS-2.1:DM-1:CM-1	Surveillance test POC operational commands to Tritium Storage Bed for reliability, response time, duration, and performance with a frequency of [TBD]
				CC-54:UCA-39.2: CS-2.1:DM-1:CM-2	Perform preventative maintenance on POC Tritium Storage Bed operational system and associated systems with a frequency of [TBD]
		CC-54: UCA-39.2: CS-2.1: DM-2	Configuration changes change required accuracy or reliability	CC-54:UCA-39.2: CS-2.1:DM-2:CM-1	Review and verify POC performance requirements for Tritium Storage Bed operational commands after configuration changes in Tritium Storage Bed or any interfacing system
		CC-54: UCA-39.2: CS-2.1: DM-3	Configuration changes results in loss of accuracy or reliability	CC-54:UCA-39.2: CS-2.1:DM-3:CM-1	Review and verify system characteristics for POC Tritium Storage Bed operational commands after configuration changes in POC or any interfacing system

Table 5.30. Tritium Storage Bed Control Action Degradation Control Mechanisms

Constraint Number	*Constraint Requirement* (Note 1)	*Degradation Mechanism Number*	*Potential Degradation Mechanisms*	*Degradation Control Mechanism Number*	*Degradation Control Mechanism* (Note 1)
CC-54: UCA-39.2: CS-3.1	POC-Tritium Storage Bed control interface must transmit commands with a reliability of [TBD - Reliability Measure]	CC-54: UCA-39.2: CS-3.1: DM-1	Gradual physical degradation of systems and loss of accuracy/reliability	CC-54:UCA-39.2: CS-3.1:DM-1:CM-1	Test and verify POC-Tritium Storage Bed control interface reliability and timing for transmitting feedback and commands with frequency of [TBD]
				CC-54:UCA-39.2: CS-3.1:DM-1:CM-2	Perform preventative maintenance on POC-Tritium Storage Bed control interface for acceptable reliability and timing with frequency of [TBD]
		CC-54: UCA-39.2: CS-3.1: DM-2	Configuration changes change required accuracy or reliability	CC-54:UCA-39.2: CS-3.1:DM-2:CM-1	Review and verify performance requirements for POC-Tritium Storage Bed control interface after configuration changes in POC, Tritium Storage Bed, or any interfacing system
		CC-54: UCA-39.2: CS-3.1: DM-3	Configuration changes results in loss of accuracy or reliability	CC-54:UCA-39.2: CS-3.1:DM-3:CM-1	Review and verify system characteristics POC-Tritium Storage Bed control interface after configuration changes in POC, Tritium Storage Bed, or any interfacing system
CC-54: UCA-39.2: CS-4.1	Tritium Storage Bed must have an on-demand operational reliability of [TBD - Reliability Measure]	CC-54: UCA-39.2: CS-4.1: DM-1	Gradual physical degradation of systems and loss of reliability	CC-54:UCA-39.2: CS-4.1:DM-1:CM-1	Surveillance test Tritium Storage Bed operational reliability, response time, and performance with a frequency of [TBD]
				CC-54:UCA-39.2: CS-4.1:DM-1:CM-2	Perform preventative maintenance on Tritium Storage Bed operational and associated systems with a frequency of [TBD]
				CC-54:UCA-39.2: CS-4.1:DM-1:CM-3	Operational failure of Tritium Storage Bed must be tracked, with incidents reviewed for root causes and design, maintenance or operation changes pursued if Tritium Storage Bed on-demand operation reliability falls below [TBD]
		CC-54: UCA-39.2: CS-4.1: DM-2	Configuration changes change required accuracy or reliability	CC-54:UCA-39.2: CS-4.1:DM-2:CM-1	Review and verify performance requirements for Tritium Storage Bed operational reliability after configuration changes in Tritium Storage Bed or any interfacing system
		CC-54: UCA-39.2: CS-4.1: DM-3	Configuration changes results in loss of accuracy or reliability	CC-54:UCA-39.2: CS-4.1:DM-3:CM-1	Review and verify system characteristics for Tritium Storage Bed operational reliability after configuration changes in Tritium Storage Bed or any interfacing system

Table 5.30. Tritium Storage Bed Control Action Degradation Control Mechanisms

Constraint Number	*Constraint Requirement* (Note 1)	*Degradation Mechanism Number*	*Potential Degradation Mechanisms*	*Degradation Control Mechanism Number*	*Degradation Control Mechanism* (Note 1)
CC-54: UCA-39.2: CS-5.1	Tritium Storage Bed must provide feedback if POC operational commands do not produce expected system behavior within [TBD] seconds of actuation and a reliability of [TBD - Reliability Measure]	CC-54: UCA-39.2: CS-5.1: DM-1	Gradual physical degradation of systems and loss of accuracy/reliability	CC-54:UCA-39.2: CS-5.1:DM-1:CM-1	Test, calibrate, and verify Tritium Storage Bed feedback system performance for POC operational feedback commands with frequency of [TBD]
				CC-54:UCA-39.2: CS-5.1:DM-1:CM-2	Perform preventative maintenance on Tritium Storage Bed operational feedback system for POC normal operation
		CC-54: UCA-39.2: CS-5.1: DM-2	Configuration changes change required accuracy or reliability	CC-54:UCA-39.2: CS-5.1:DM-2:CM-1	Review and verify performance requirements for POC operational feedback commands after configuration changes in Tritium Storage Bed or any interfacing system
		CC-54: UCA-39.2: CS-5.1: DM-3	Configuration changes results in loss of accuracy or reliability	CC-54:UCA-39.2: CS-5.1:DM-3:CM-1	Review and verify system characteristics for POC operational commands after configuration changes in Tritium Storage Bed or any interfacing system

Notes: (1) Many constraint requirements and degradation control mechanisms are left as “to be determined” (TBD) and would need to be specified based on the final system design characteristics.

One additional interesting consideration arising from step nine of the STPA evaluation is the need to recursively examine the functional control relationships between a new testing and configuration organization and the systems, components, and interactions that they are interfacing. The recommended additional controls are, themselves, vulnerable to unsafe control actions and degradation over time. This analysis is outside of the scope of this work but would be additional level of analysis needed to help ensure the overall operational characteristics of the facility.

5.7.4 Advantages and disadvantages of STPA evaluations

STPA evaluations differ from all analyses previously discussed in this section due to the difference in fundamental philosophies on accident initiation and progression (e.g., a direct causality model in prior analyses versus a system behavior or hazard model for STPA)[72]. In a direct causality model, sufficient layers of independent redundant active systems will result in a sufficiently high reliability system with no credible release events. A system behavior model, however, may suggest that organizational factors and other systematic uncertainties open the opportunity for credible release events even in high reliability systems. This change in model radically alters the analysis process and produces evaluation deliverables and assessments that differ from traditional safety evaluation methods. The primary driving force for use of STPA is the belief that the system behavior model enables the identification and mitigation of design and operational factors that have repeatedly contributed to industrial disasters and been missed by other methods.

The main advantages of STPA are the ability to explicitly incorporate operational and organizational characteristics into the evaluation process, an emphasis on design for safety rather than design for acceptable losses, the ability to develop design-specific performance-based regulatory requirements using a standardized process, and traceability of all safety constraints and requirements to facility specific hazards and losses.

The first advantage of STPA is that the method enables the explicit incorporation of operational and organizational characteristics into the licensing evaluation process. This change reflects the lessons learned from catastrophic accidents – the failure of highly reliable, complex engineered system can rarely (if ever) be tied to the anticipated failure of one or more engineered systems. Major accidents are more often tied to the failure of physical systems simultaneous with the operational errors or systems operating outside of design conditions. As a result, these observed event sequences would be vulnerable to being missed by traditional direct causality model analyses. STPA, however, enable incorporation of physical, digital, and human systems in analyses to identify situations where unsafe conditions can occur that would lead to losses. These evaluations allow analysts and regulators to consider how all aspects of facility design and operation contribute to facility safety and, on a facility specific basis, design and justify the need for organization programs such as quality assurance or audits that are normally considered prescriptive best practices for high hazard systems.

This incorporation of operational and organizational characteristics into the licensing evaluation process may lead to a more cohesive regulatory process where safety is fully integrated into facility design and operation. This integration most contrasts explicitly with other direct causality model evaluation methods where additional assurances on performance and operation are tacked on as regulatory requirements following the licensing evaluation process. While these methods may be effective for a majority of cases and are based on best practices or industry lessons learned, they are not necessarily reflective of facility or activity specific needs. STPA enables licensing processes more holistic evaluation of facilities and recognition of safety as an emergent behavior from a well-controlled system, better protecting against losses of concern for all stakeholders. This promotes the equal importance of development and treatment of organizational and operational safety with physical safety features that are historically the focus of both industry and regulators. The need for project-specific effective quality assurance processes and audits emerge as a natural and critical safety feature through the STPA evaluations.

The second advantage of STPA is a refocus of licensing evaluations as proactive processes that ensure safe operation rather than reactive processes that demonstrate acceptable losses. Use of STPA forces analysts and regulators to consider how to make designs and operation safer through incorporation of additional safety controls or changes to design that eliminate inherent hazards for a facility or activity. In other licensing analyses, analysts may chose to meet regulatory hazard limits by refining analysis methods rather than improving safety. While this approach may be appropriate when simply meeting regulatory limits, the actual safety of the system has not changed – the increased safety margin exists only on paper. The elimination of strict quantitative safety goals as the main basis for meeting regulatory requirements may enable a change in the philosophical safety and licensing basis for high hazard facilities.

The third advantage is the ability to develop design-specific performance-based regulatory requirements using a standardized process. Development of performance-based regulatory requirements has been a goal for regulators interested in enabling innovation in highly regulated and complex engineering systems [85]. One challenge of performance-based requirement development, however, has been ensuring that the requirements are applicable to the activity and that compliance with the requirements will result in safe operation. STPA functions as standardized, technology (and in fact activity) independent process that facilitates development of performance-based requirements and is directly tied to losses of interest to stakeholders. This work illustrates how performance based requirements for the design and operation of the Deuterium Tritium Storage Bed can be developed without having regulatory precedent on the design and operation requirements of the system. This process could be effectively repeated for other major systems to develop performance-based design requirements.

The final advantage is traceability of all safety constraints and requirements to facility specific hazards and losses. Traceability of constraints and requirements helps ensure that all regulatory requirements are needed for safe operation. Confining the safety basis to needed requirements helps reduce costs associated with excessive regulatory requirements and focuses attention on the safety issues that matter most. The traceability also enables designers to quickly and easily examine "lineage" of requirement to understand the technical basis of requirements and how altering the requirements may affect upstream systems, hazards, and losses. This traceability also extends to operational requirements so human operators and organizations are explicitly tied into the safety basis of a facility.

The major challenges of STPA are the lack of regulatory precedent with STPA and questionable compatibility with existing regulatory frameworks, the large scope and engineering effort associated with evaluations, and the challenge of performing reduced scope evaluations of facilities.

The first challenge is a lack of regulatory precedent with STPA and questionable compatibility with existing regulatory framework. One of the most important characteristics of any regulatory process is predictability. While use of STPA is growing in regulated industries such as a commercial aerospace and automotive, it is still not used widely in the commercial chemical or nuclear fission industries [93]. As a result, there is a lack of precedent in using STPA evaluations to support licensing or legal assessments of a variety of regulated activities and it is unclear how STPA evaluations could be integrated into existing regulatory frameworks. It is likely possible to integrate STPA evaluations into regulatory frameworks, but there may be some unpredictability in the regulatory process for both industry as they gain experience preparing and utilizing insights from STPA evaluations and for regulators as they determine appropriate review controls for these evaluations. Shifting regulatory frameworks and regulator/ industry practice towards accepting STPA evaluations would represent a significant near-term disadvantage for STPA evaluations.

Another challenge is the large scope and engineering effort associated with evaluations. The narrowing scope of analyses performed as a part of this work at later steps in the STPA evaluation highlight how detailed the STPA evaluation process is. Table 5.29 provides 21 different control degradation constraints for one of 154 unsafe control actions for one of the simplest systems of the 37 identified in the Level 3 system engineering model for a commercial fusion facility. If a similar number of requirements could be expected for other systems, a full facility could be expected to have over 120,000 tracible constraints analyzed as part of an STPA evaluation at this level of design detail. It is likely that this number could be several orders of magnitudes higher if the STPA evaluation were performed on a more detailed component level model of fusion facility. It is expected that a large engineering project will have a significant project management overhead burden related to the requirements, design, and lifecycle operations, this burden is not always explicitly linked to the regulatory basis of a facility. This represents a significant potential burden for both industry to prepare and regulator to review.

This challenge could be handled by changing the licensing paradigm for both industry and regulators. For some system designers, licensing and safety evaluations are considered for post-design requirement. Safety evaluations are performed sequentially after the functional design process with safety controls added as needed. This process treats safety as a lower priority item and results in safety systems that may not be integrated with the larger design and safety evaluations that may require substantial rework or detailed analysis to meet regulatory requirements. Integration of licensing and safety analyses and requirements into the design process with functional design requirements enables design that works to minimize or eliminate hazard by design rather than controlling or mitigating them. Formally implementing STPA evaluations into the design process for facilities could facilitate safer design and enable designers to credit a documented, traceable design practice as a significant part of their licensing basis. The recursive nature of STPA enables evaluation and decomposition of safety functions, similar to a system engineering design approach and can incorporate design objectives such as production capacity and operability as stakeholder losses of interest. In this way, the large scope and engineering effort associated with evaluations can be diffused into the design process, resulting in safer design and lower direct costs associated with use of STPA evaluations as a licensing tool.

For regulators, the type and level of review performed on licensing evaluations varies significantly depending on the regulatory framework used. The other licensing evaluation methods described in this work are focused on a quantitative evaluation that is compared with specified hazard limits. Regulatory reviews may thus focus on the evaluation inputs, assumptions, methods, or calculations and consider if the evaluation is appropriate to demonstrate compliance with the required hazard limits. Operational and organizational practices within industry are most often used to justify evaluation inputs or assumptions, and are not explicitly included in the evaluation. STPA, by contrast, is primarily a process-based evaluation method that utilizes a simplified final quantitative analysis to help confirm compliance with general regulatory limits. Safe operation is achieved through adequate treatment of system hazards and controls using the STPA process, and not strictly through compliance with specific prescription or even performance-based requirements.

Regulator focus on evaluating specific derived requirements would not provide assurance of safety unless all requirements and constraints were evaluated. Instead, the implementation process of STPA should be reviewed by regulators to ensure that adequate direction, resources, and expertise were available in evaluations and that the insights from these evaluations were incorporated into design and operation. Spot checks of portions of STPA evaluations can be useful for point assessments of process implementation but the focus of these checks should be on the process and not for debating specific technical merits of each spot check. Process reviews, spot checks, and on-going review of the STPA evaluation program can provide assurance to regulators and the public that a facility is appropriately controlling hazards and ensuring safe operation for all stakeholders. This change in review reduces the scope and effort required of regulators, focusing regulators on the evaluation process central to STPA evaluations in ensuring safety.

The third challenge is that the STPA evaluation cannot effectively be performed independent of facility operations or performed with varying levels of detail to provide preliminary estimates of facility safety. Simplified or partial analyses may be performed for other licensing evaluation methods to quickly generate insights regarding the safety characteristics of a facility. For example, a worst-case release analysis may be performed using sitewide hazards, unrealistically conservative meteorological data, and simplified calculation methods to quickly characterize potential hazard consequences of the facility and compare them with relevant hazard limits. These inputs and assumptions may be refined in subsequent analyses but the initial scoping analysis could be performed quickly to provide “order-of-order-of-magnitude” insights on facility compliance with relevant hazard limits. The process-based evaluation approach of STPA, however, may limit the ability for analysts to quickly and roughly approximate the hazard control characteristics of large, complex systems. Development of incomplete but bounding STPA evaluations may be more difficult due the challenge of correctly characterizing complex hazard control interactions using incomplete information.

Generating limited scope licensing evaluation insights with STPA based methods may be possible using STPA evaluations to characterize the hazard control behavior for subsystems or components within a larger facility and limiting physical scope. Systems with complex control interactions that are not easily characterized using other evaluation methods (e.g., digital instrumentation and control systems) could benefit from STPA evaluations. STPA methods may also be applied for higher level system functions to identify general facility or system hazards, unsafe control actions, and constraints. These analyses will likely not be detailed enough to ensure safety at a component level but could provide insights into whether plant-level constraints adequately bound facility operations.

5.7.5 Summary of STPA evaluations

Use of STPA for licensing evaluations is an innovative way to analyze and regulate hazardous activities and facilities. STPA is a paradigm shift for evaluating safety, focusing on the systematic control of hazards rather than identification and mitigation of causal event sequences. STPA enables an extremely comprehensive, system evaluation based on the losses and hazards relevant to all stakeholders. The evaluation method can be used to transparently and robustly develop performance based regulatory requirements for any high hazard activity, scaling both based on the size of the system and the level of design. STPA, when integrated into the design process, enables the analysis of system hazards and development of constraints that highlight potential failure modes of interest. Certain prescriptive organization safety mechanisms such as quality organizations and change management processes emerge organically as systems important to ensuring long-term safe operation and are traceable to specific hazards and losses of interest to stakeholders.

This paradigm shift and detailed analysis, however, may complicate integration into existing regulatory frameworks. STPA evaluations require substantial engineering effort to complete if not integrated into the design process and development of “simplified” analyses to roughly characterize facility safety would be extremely difficult to produce. Additionally, STPA evaluations do not normally result in a quantitative assessment of safety that can be compared with other activities or regulatory hazard limits. The lack of a defined safety margin may complicate implementation of STPA evaluations as the primary licensing evaluation. The tradeoffs between the integrated operational and organization safety enabled by STPA evaluations and the potential significant regulatory burden and process requirements should be considered when determining if this analysis method is appropriate for specific commercial fusion facilities.

5.7.6 Parallel quantitative licensing evaluations to support STPA evaluations

As previously discussed, STPA methods does not result in a quantitative assessment of safety. In some regulatory frameworks, a quantitative hazard consequence analysis may be required to demonstrate compliance with hazard limits. If a quantitative hazard consequence analysis is required, a simplified quantitative licensing evaluation may also be performed in parallel to the STPA evaluation. This simplified quantitative analysis is not intended to ensure the safety of the facility or activity but to demonstrate compliance with hazard limits. The work performs a quantitative analysis separate from the STPA evaluation to illustrate a hybrid licensing evaluation method.

The scope of this evaluation is limited to the analysis of the D-T Storage System. Review of system hazards in step 3 of the STPA evaluation suggest that worker and public exposure to tritium and tritiated materials are the dominant hazard of concern for the D-T Storage System. The total mass of hydrogen gas processed in the system is relatively small (likely less than 10 kg depending on specific design) and worst-case detonation or deflagration of this mass of hydrogen would only produce local affects. Evaluation of a 10 kg hydrogen vapor cloud explosion using standardized EPA RMP methodologies show that significant damage (greater than 1 psi of explosion overpressure) would be limited to 50 meters. Thus, the radiological hazards posed by tritium are the dominant hazard for consideration.

A simplified deterministic maximum credible releases analysis is performed for the D-T Storage System using a similar process to that described in Section 5.4. Based on the discussion of hazards of regulatory significance in Chapter 3, the boundaries of this analysis are limited to the catastrophic, acute, local geographic releases of tritium or tritiated materials from a commercial fusion facility. Deposition of tritium into the biosphere and chronic impacts of tritium contamination are not considered. Further additional analyses would be required to demonstrate compliance with chronic or worker exposure pathways. The maximum credible release analysis end point for this worst-case release limit is the off-site dose or total exposure. Note that other types of end points (such as total vulnerable inventory) could be used but would depend on the specific hazard limit and the associated processes used to develop it.

Two separate analysis cases are considered: worst-case release conditions where doses are evaluated against a 25-rem dose limit (maximum legally permittable exposure) and alternative release conditions where doses are evaluated against a 1-rem dose limit (lower bound evacuation limit for emergency planning purposes). The following conservative inputs and assumptions are used to support the corresponding model factors in this maximum credible release analysis:

- Hazard inventory (vulnerable to release): The design and operation controls implemented for the Tritium Storage Bed are assumed to prevent the credible release of a full tritium bed inventory of 70 grams of tritium or simultaneous release of multiple tritium storage bed inventories. A maximum credible hazard inventory of 10 percent of the individual storage bed inventory (7 grams) is assumed. This represents both the unbound and in-process tritium in the Tritium Storage Bed and tritium inventory in Tritium Process Piping that would be vulnerable to release. Additional analyses and operational or design constraints may be required to ensure the validity of these limits and these assumptions align with the analysis performed in Section 5.5.

- Hazard inventory released (fraction released): Due to the challenge of containing tritiated gasses, 100% release of the analyzed hazard inventory is assumed. No credit for mitigating design or engineering features to reduce the release fraction is taken.
- Hazard inventory release conditions (time, location, form): A release time of 2 hours is assumed on DOE and NRC regulatory guidance for acute release [20] [21]. The release location is conservatively assumed as a ground level release to produce the highest concentrations closest to the release point. All tritium is assumed to be released in the oxidized form (HTO, DTO, or T_2O) in a neutrally buoyant plume.
- Dispersion conditions (meteorological, geographic, location): It is assumed that the facility site boundary (and the maximum exposed off-site individual) is located 160 meters from the release point. This distance is based on the average distance from existing power plants to property boundaries for 200 – 500 MW power plants in Massachusetts. A second distance will be calculated to determine a limiting boundary for emergency response purposes. Two separate release conditions are assumed in this analysis:
    - Worst meteorological and geographic dispersion conditions are assumed in accordance with EPA regulatory guidance for worst-case release off-site consequence analyses [31]. This include Pasquill stability class F, 1 m/s wind speeds, cropland dispersion coefficients, and Gifford plume meander. Site specific meteorological conditions could likely be used but are not assumed for this specific analysis.
    - Alternative meteorological and geographic dispersion conditions are assumed in accordance with EPA regulatory guidance for alternative release off-site consequence analyses [31]. This include Pasquill stability class D, 4.5 m/s wind speeds, countryside dispersion coefficients, and Gifford plume meander. Site specific meteorological conditions could likely be used but are not assumed for this specific analysis.
- Exposure/dose conditions (physiological, duration): It is conservatively assumed that an MOI is exposed for the entirety of the release. A typical breathing rate of $3.33 \times 10^{-4}\ \mathrm{m^3/s}$ for an adult is assumed [20]. Based on existing guidance for exposure to tritiated water vapor, it is conservatively assumed that the MOI has two major exposure pathways: inhalation and skin absorption. For skin absorption of HTO, the dose is assumed to be 50% of the inhalation dose [22]. A dose exposure coefficient for HTO from the ICRP recommendation of 1.8×10^{-11} Sv/Bq is used [23].

Using these model factors, the off-site acute radiation dose is calculated using a Gaussian plume model. This model is based on DOE and NRC regulatory guidance for analysis of acute radiation releases [24]. Two values are calculated for each set of release conditions:

- acute dose at the site boundary (160 meters),
- distance to case specific dose boundary
    - 25 rem (0.25 Sv) dose for worst case release
    - 1 rem (10 mSv) dose for alternative case release

The results of these calculations are presented in Table 5.31.

Table 5.31. STPA Evaluation Maximum Credible Release Analysis

Release Condition	*Dose at 160 m Site Boundary*	*Exclusion Boundary Dose*	*Distance to Exclusion Boundary Dose*
Worst-case release	18.4 rem (0.2 Sv)	25 rem (0.25 Sv)	134 m
Alternative-case release	0.98 rem (9.8 mSv)	1 rem (10 mSv)	158 m

The deterministic maximum credible release consequence analysis show that for the D-T Storage System that STPA process could justify facility operations on a quantitative basis. These evaluations show that for a 7-gram vulnerable tritium inventory, standardized meteorological conditions, and a 160-meter site boundary, the system could meet relevant regulatory limits. This analysis could provide final confirmatory quantitative support for the licensing of a facility using STPA evaluations.

Reviewing this evaluation reveals some important limitations and challenges associated with confirmatory quantitative analyses. The major challenge of these analyses is selecting and defending the calculation inputs and assumptions used, particularly when these inputs and assumptions are not fully conservative. This may lead to disagreements between stakeholders as different groups may seek different levels of inherent conservatism in the analysis. The example analysis of the Deuterium Tritium Storage Systems in this work has three major potential factors for stakeholder disagreement: vulnerable inventory, release conditions, and the regulatory limit end points. In all three cases, the inputs and assumptions selected were not fully conservative and may be subject to disagreement without a quantitative basis for defending selection.

The definition of a vulnerable inventory highlights the challenge of the quantitative release analysis performed as part of an STPA evaluation. In this analysis, the vulnerable inventory was defined as 7 grams of tritium gas released from the Tritium Storage Bed or Tritium Process Piping. This value is lower than the inventories considered in the deterministic or probabilistic analyses of the same system. Inventories of 70 grams (1 bed), 140 grams (2 beds), or even 1400 grams (full bed storage inventory) could be justified as plausible bounding inventories.

An STPA evaluation, however, is intended to facility safer facility design and operation through the identification of hazards, unsafe control actions, and development of robust safety constraints for systems. The explicit description and justification of the engineering and operational controls completed as part of the STPA evaluation suggest that use of a lower vulnerable inventory (7 grams versus 70 grams or higher) may be justifiable. The lack of a traditionally qualitative assessment of safety by deterministic rule (e.g., design by the single failure criterion and defense-in-depth) or quantifiable assessment of safety by probabilistic means (e.g., sufficiently low event probability) means that demonstrating applicability of the lower vulnerable inventory is technically impossible. Use of a lower vulnerable inventory would therefore become a social process of negotiation as relevant stakeholders seek an acceptable end state that satisfies their desired level of conservatism or tolerable excess risk.

This social process would need to be repeated for each input to the quantitative release analysis. This negotiated process is similar to that described in Section 5.3 for the maximum credible release analysis but is complicated by the desire to justify less conservative analysis conditions based on implications of the STPA evaluation process on improved system safety. In this way, the STPA evaluation method could be construed as attempting to take credit for engineered safety features (similar to deterministic design basis methods) without performing the actual design basis analyses. This statement is accurate but largely due to the differences in safety philosophy between a causal safety based method (deterministic or probabilistic design basis analyses) and an emergent safety or hazard based method (STPA).

Use of less conservative inputs and assumptions that produce more favorable (and arguably more realistic analyses) may arise if adversarial stakeholders are able to advocate for use of maximum credible release analyses despite use of STPA evaluations to produce a more robust safety design. Additional regulatory processes or guidance may be needed to ensure that the safety benefits from an STPA evaluation based licensing process may be considered when quantitative release analysis in parallel to an STPA evaluation.

5.8 Summary of licensing evaluation methods and commercial fusion facility insights

This chapter presents and discusses five proposed licensing evaluation methods for the analysis of commercial fusion facilities:

- Worst case event evaluation
- Maximum credible event evaluation
- Deterministic design basis event evaluation
- Probabilistic design basis event evaluation
- Hazard control-based evaluation (STPA)

These five methods represent a variety of approaches to assess the safety of a facility or activity. Each of the methods also provide different insights on the potential safety of future commercial fusion facilities.

5.8.1 Licensing evaluation methods summary

The first two evaluations (worst case event and maximum credible event) focus on hazard consequence evaluations; given a specific activity, what consequences can be expected and how do these consequences compare to a variety of hazard limits. These evaluations are largely performed independent of engineering safety features of a facility. Instead, they consider the inherent hazards present in a facility and help regulators simplistically assess the possible consequences of an event. These methods are robust, simple to prepare and review, and easily integrate with existing regulatory frameworks that compare quantitative hazard consequence to regulatory limits but are extremely conservative and predict unrealistic (but mechanistically possible) consequences that limit facility design and operation.

The second two evaluations (deterministic and probabilistic design basis events) focus on event sequence evaluations; given the design of a facility and sets of initiating events, what consequences occur for different event sequences and how do these consequences compare to a variety of hazard limits. These evaluations allow facilities to credit engineered safety features and operator actions to prevent or mitigate consequences of an event. This more detailed analysis enables analysts and regulators to more realistically model system behavior and assess different possible outcomes from initiating events. These methods are well characterized, easily integrated with regulatory frameworks, and help answer the "what-if" questions posed by a direct causality model of accidents. These methods, however, are also costly to prepare and review, may result in ineffectual approaches to safety (e.g., excessive defense-in-depth derived from the direct causality model), and are subject to both analyst bias and lack of imagination that leave unquantifiable "unknown unknowns" forever outside the scope of the analysis. These drawbacks can result in facilities that are costly to construct and operate under normal conditions but are also subject to "black swan" (unknown low probability, high consequence) failure sequences.

The final evaluation (hazard control-based evaluations or STPA) focuses on the holistic evaluation of system behavior and interactions; given a system hazard, what physical, operational, and organization constraints are in place to prevent unsafe control actions. This method rejects the direct causality model of accidents and views safety as an emergent system behavior – not just result of sufficiently diverse and independent layers of safety. This process can, in theory, enable the development of more effective organizations that better reflect the actual characteristics and needs of the facility. These hazard control based methods can help ensure the safety of highly complex system (especially those utilizing digital systems) and may help identify potential interactive failure mechanisms normally missed by other evaluation methods. These methods, however, may be costly to prepare and review, are best integrated into the design process and not left as a post design activity, and it is unclear how these methods may be integrated into existing regulatory frameworks.

These five methods represent different approaches to both the definition and evaluation of safety for activities. They vary in terms of nearly every evaluation characteristic:

prescriptive vs. performance based, low effort vs. high effort, conservative vs. realistic, quantitative vs. qualitative. Each evaluation method has a different appropriate application that likely varies based on the activity, the hazards, the desired regulatory framework, and the techno-economic constraints of the activity. This work illustrates the advantages and drawbacks of each method through the application of the method to the licensing of a commercial fusion facility. It is in no way a complete evaluation of facility safety but helps to highlight the potential benefits and consequences of each evaluation method in specific cases. Industry, regulators, and the public will, in the end, need to enable use of evaluation methods that meet all stakeholders needs to ensure that licensing and regulation is not a barrier to the development and deployment of commercial fusion technology.

5.8.2 Commercial fusion facility safety insights

The five preliminary licensing evaluations of a commercial fusion facility provided several interesting insights into the safety of commercial fusion and the potential licensability of future facilities. Major insights include the effect of tritium inventory and release assumptions on offsite consequences, the role of engineered safety systems on releases, and trade-offs between design flexibility and licensing burden for facilities.

Table 5.31. Commercial Fusion Facility Evaluation Results

Evaluation Method	*Vulnerable tritium inventory*	*Site boundary dose (160 m)*	*Maximum dose distance (25 rem)*	*Evacuation dose distance (1 rem)*
Worst Case Release	2925 g	4140 rem	3850 m	49.4 km
Maximum Credible Release	1565 g	117 rem	390 m	2.8 km
Deterministic Design Basis	70 g	0.17 rem	N/A	N/A
Probabilistic Design Basis	7 g	29 rem	175 m	1.2 km
Hazard Control Analysis (STPA)	N/A	N/A	N/A	N/A

Table 5.31 provides high-level evaluation results from each of the five evaluation methods considered in this work. The conservatively calculated doses for worst-case oxidized release of the full site inventory of 2925 grams of tritium results in catastrophic off-site radiological consequences. While the analysis assumptions of full site inventory release, worst-case meteorological conditions, and 100% oxidation of tritium are highly unrealistic, they are mechanistically possible and represent a bounding accident scenario for a commercial fusion facility. As the vulnerable tritium inventory is reduced using relatively simple engineering arguments (e.g., physical separation of systems) and more realistic meteorological assumptions, the off-site consequences are significantly reduced but still are unacceptably high.

These analyses suggest a commercial fusion facility with significant tritium inventories may not be "inherently safe" facility with off-site consequences comparable to other industrial facilities [104]. The "backward" worst case release analysis performed in Section 5.3 indicate that less than 1 gram of total vulnerable tritium could be present on-site to avoid off-site evacuation regulatory requirements at 160 meters using worst case release conditions. Scaling the maximum credible release analysis performed in Section 5.4 indicate that less than 14 grams of total vulnerable tritium could be present on-site to avoid off-site evacuation regulatory requirements using more typical release conditions. Commercial fusion facility may be considered "inherently safe" and could be evaluated using these simplified licensing evaluation methods if these inventory limits are met but the current engineering and physics limitations of D-T fueled tokamaks may limit designers ability to reduce the total vulnerable tritium inventory to these levels.

Reduction in the effective vulnerable tritium inventory using separation of systems and crediting use of engineered safety features (considered through event sequence analysis) to minimize or mitigate release are required to reduce the off-site consequences to levels acceptable using existing regulatory guidance. These reductions were significant but require significantly more detailed evaluations and qualification of engineered safety features to ensure they will perform their credited safety function. Note, however, that these deterministic and probabilistic design basis evaluations are quite limited in scope and do not consider all systems or all initiating events; further analyses would be needed to confirm if these evaluations were bounding for all facility event sequences.

The STPA based evaluation does not demonstrate compliance with quantitative regulatory limits but instead focuses on ensuring continued control and mitigation of hazards. This method provides important insights on the design operational safety of a facility. The demonstration of safety through design may be sufficient from some regulatory frameworks and requirements but quantitative analyses may still be useful to demonstrate general compliance with quantitative hazard limits..

These evaluations show that given the facility design parameters in Table 5.2 though Table 5.4, there are three major paths to achieving and demonstrating facility safety:

- Reduction of vulnerable inventory
- Implementation of engineered safety features to reduce released inventory
- Analysis using detailed evaluation methods

Each of these paths comes with significant tradeoffs. Reduction of vulnerable inventory (primarily by design changes) reduces the inherent hazard of a facility but may require substantial changes to the design. This process could limit design or be costly if attempted later in the design process, requiring substantial rework of previously designed systems. Implementation of engineering safety features reduces the effective hazard of a facility and allows designs with inherent hazards that would normally be unacceptable. These engineered safety features, however, require additional analysis to ensure their operability under all possible conditions and represent a potential significant failure mechanism. The robust design and operation of the engineered safety features and the associated analyses may be costly for facilities. Use of detailed evaluation methods has no impact on the actual design of hazards of a facility but enable facilities to meet regulatory limits by providing more accurate assessment of event consequences. These detailed methods can be costly to conduct and review but provide the least conservative evaluation of safety.

Balancing tritium inventory and release assumptions on offsite consequences, the role of engineered safety systems on releases, and trade-offs between design flexibility and licensing burden for facilities will be critical for commercial fusion facilities. Each licensing evaluation method could be used to support licensing and regulation of a commercial fusion facility but these trade-offs will need to be balanced with design and project specific characteristics, as well as with the regulatory frameworks used. The next section discusses different regulatory frameworks that can be used for commercial fusion facilities, their benefits and limitations, and the compatibility of these frameworks with the licensing evaluation methods discussed in this section.

Finally, it is important to mention that the quantitative licensing evaluations performed in this section are not applicable to all commercial fusion facilities. Any commercial D-T fueled facilities that are able to utilize smaller tritium inventories due to their design or operational characteristics may be able to demonstrate compliance with regulatory hazard limits without the need for more detailed licensing evaluation methods. Commercial fusion facilities that do not rely on tritium fuel but still produce high energy neutrons from fusion reactions would need to address material activation hazards but would not need to consider any of the tritium hazards discussed in this section. Commercial fusion facilities that utilize aneutronic fusion reactions would not have any of the radioactive or activation hazards and would have hazards more similar to other industrial energy facilities. Utilizing the system engineering models (Chapter 2), hazard identification and down selection process (Chapter 3), and the hazard limit development methods (Chapter 4) facilitate the development and demonstration of compliance with regulatory limits applicable to any fusion technology. These regulatory process can help support technology inclusive requirements for a diverse commercial fusion industry.

5.9 References

[1] Environmental Protection Agency. General Guidance on Risk Management Programs for Chemical Accident Prevention (40 CFR Part 68): Chapter 9. Technical Report EPA 555-B-04-001, Environmental Protection Agency, March 2009.

[2] Environmental Protection Agency. General Guidance on Risk Management Programs for Chemical Accident Prevention (40 CFR Part 68): Chapter 2. Technical Report EPA 555-B-04-001, Environmental Protection Agency, March 2009.

[3] Occupational Safety and Health Administration. Process Safety Management of Highly Hazardous Chemicals; Explosives and Blasting Agents. (57 FR 6356), 1991.

[4] Wisconsin Department of Natural Resources. Power Plants. https://dnr.wi.gov/topic/Sectors/PowerPlants.html.

[5] U.S. Code. Clean Air Act. (42 USC 7401), 1970.

[6] U.S. Code. National Environmental Policy Act. (42 USC 4321), 1969.
[7] E. Biber and J. Ruhl. The permit power revisited: The theory and practice of regulatory permits in the administrative state. Duke LJ, 64:133, 2014.
[8] U.S. Code. Occupational Health and Safety. (42 USC 15), 1970.
[9] R. W. Best. Advanced fusion fuel cycles. Fusion Technology, 17(4):661–665, 1990.
[10] A. Kuang, N. Cao, A. J. Creely, C. A. Dennett, J. Hecla, B. LaBombard, R. A. Tinguely, E. A. Tolman, H. Hoffman, M. Major, et al. Conceptual design study for heat exhaust management in the arc fusion pilot plant. Fusion Engineering and Design, 137:221–242, 2018.
[11] B. Sorbom, J. Ball, T. Palmer, F. Mangiarotti, J. Sierchio, P. Bonoli, C. Kasten, D. Sutherland, H. Barnard, C. Haakonsen, et al. Arc: A compact, high-field, fusion nuclear science facility and demonstration power plant with demountable magnets. Fusion Engineering and Design, 100:378–405, 2015.
[12] G. Jackson, V. Chan, and R. Stambaugh. An analytic expression for the tritium burnup fraction in burning-plasma devices. Fusion Science and Technology, 64(1):8–12, 2013.
[13] Nuclear Regulatory Commission. Guidelines for Preparing and Reviewing Applications for the Licensing of Non-Power Reactors. Technical Report NUREG-1537, Nuclear Regulatory Commission, 1996.
[14] Occupational Safety and Health Administration. Determination of Toxic Thresholds. Technical Report OSHA-S026-2006-0659-0014, Occupational Safety and Health Administration, 1992.
[15] Environmental Protection Agency. Accidental Release PreventionRequirements: Risk Management Programs Under Clean Air Act Section112(r)(7). (61 FR 31718), 1996.
[16] Environmental Protection Agency. General Guidance on Risk Management Programs for Chemical Accident Prevention (40 CFR Part 68): Chapter 4. Technical Report EPA 555-B-04-001, Environmental Protection Agency, March 2009.
[17] Environmental Protection Agency. RMP*Comp. https://www.epa.gov/rmp/rmpcomp.
[18] Chemical Accident Prevention Provisions. 40 CFR Part 68, 1994.
[19] Environmental Protection Agency. PAG Manual: Protective Action Guides and Planning Guidance for Radiological Incidents. Technical Report EPA-400/R-17/001, Environmental Protection Agency, January 2017.
[20] Department of Energy. DOE Standard: Preparation of Nonreactor Nuclear Facility Documented Safety Analysis. Technical Report DOE-STD-3009-2014, Department of Energy, November 2014.
[21] Nuclear Regulatory Commission. Atmospheric Dispersion Models for Potential Accident Consequence Assessments at Nuclear Power Plants. Technical Report Regulatory Guide 1.145, Nuclear Regulatory Commission, 1983.
[22] ICRP. ICRP Publication 30: Limits for Intakes of Radionuclides by Workers. 1979.
[23] K. Eckerman, J. Harrison, H. Menzel, C. Clement, et al. ICRP publication 119: compendium of dose coefficients based on ICRP publication 60. Annals of the International Committee on Radiation Protection, 41:1–130, 2012.
[24] Department of Energy. Maccs2 computer code application guidance for documented safety analysis final report. Technical Report DOE-EH-4.2. 1.4, 2004.
[25] Nuclear Regulatory Commission. Emergency Preparedness for Fuel Cycle and Other Radioactive Material Licensees. (54 FR 14061), 1989.

[26] Nuclear Regulatory Commission. Emergency Preparedness for Fuel Cycle and Other Radioactive Material Licensees. (52 FR 12921), 1987.

[27] Nuclear Regulatory Commission. A Regulatory Analysis on Emergency Preparedness for Fuel Cycle and Other Radioactive Material Licensees. Technical Report NUREG-1140, Nuclear Regulatory Commission, 1988.

[28] Nuclear Regulatory Commission. Planning Basis for the Development of State and Local Government Radiological Emergency Response Plans in Support of Light Water Nuclear Power Plants. Technical Report NUREG-0396, Nuclear Regulatory Commission, 1978.

[29] G. T. Mazuzan and J. S. Walker. Controlling the Atom: the Beginnings of Nuclear Regulation, 1946- 1962. University of California Press, Berkeley, 1985.

[30] Department of Homeland Security. Health and Safety Planning Guide For Planners, Safety Officers, and Supervisors For Protecting RespondersFollowing a Nuclear Detonation. December 2016.

[31] Environmental Protection Agency. Risk Management Program Guidance for Off-site Consequence Analysis. Technical Report EPA 550-B-99-009, Environmental Protection Agency, March 2009.

[32] F. I. Khan. Use maximum-credible accident scenarios for realistic and reliable risk assessment. Chemical engineering progress, 97(11):56–64, 2001.

[33] UK Office of Nuclear Regulation. Safety assessment principles for nuclear facilities. Technical report, UK Office of Nuclear Regulation, 2020.

[34] Center for Chemical Process Safety (CCPS). Guidelines for hazard evaluation procedures. Wiley, 2011.

[35] Nuclear Energy Institute. Diverse and Flexible Coping Strategies (FLEX) Implementation Guide. Technical Report NEI 12-06, August 2012.

[36] Occupational Safety and Health Administration. Interpretation of OSHA's Standard for Process Safety Management of Highly Hazardous Chemicals. (72 FR 31453), 2007.

[37] Reactor Site Criteria. 10 CFR Part 100, 2015.

[38] Westinghouse. AP1000 Design Control Document: Chapter 2 - Site Characteristics. Technical Report NRC Accession Number ML11171A420, 2011.

[39] Southern Nuclear. Vogtle Combined Operating License Updated Final Safety Analysis Report: Chapter 2 - Site Characteristics. Technical Report NRC Accession Number ML21179A107, 2021.

[40] NuScale. NuScale Design Control Document: Chapter 2 - Site Characteristics. Technical Report NRC Accession Number ML20224A482, 2020.

[41] Nuclear Regulatory Commission. White Paper on Risk-Informed and Performance-Based Regulation. Number SECY-98-144. 1999.

[42] Future of Nuclear Energy in a Carbon-Constrained World. Massachusetts Institute of Technology, 2018.

[43] Nuclear Regulatory Commission. Design-basis Events, Design-basis Information, and External Events. Technical Report NRC Accession Number ML14328A170, Nuclear Regulatory Commission, 2014.

[44] J. S. Walker and T. R. Wellock. A Short History of Nuclear Regulation, 1946-2009. US Nuclear Regulatory Commission, 2010.

[45] J. Thompson. Signficant Operational Experience: 7 Major Industry Events with Regulatory Implica- tions. Number NRC Accession Number ML16006A288. Nuclear Regulatory Commission, 2016.

[46] Edson G. Case. Information Report: Single Failure Criterion. Technical Report NRC Accession Number ML060260236, Nuclear Regulatory Commission, 1977.

[47] Nuclear Regulatory Commission. Design-Basis Tornado and Tornado Missiles for Nuclear Power Plants. Technical Report Regulatory Guide 1.76, Nuclear Regulatory Commission, 2007.

[48] Nuclear Regulatory Commission. Technical basis for interim regional tornado criteria. Number WASH- 1300. 1974.

[49] Nuclear Regulatory Commission. Request for information pursuant to Title 10 of the Code of Federal Regulations 50.54(f) Regarding Recommendations 2.1, 2.3, and 9.3, of the Near-Term Task Force Review of Insights from the Fukushima Dai-ichi Accident. Technical Report NRC Accession Number ML12053A340, Nuclear Regulatory Commission, 2012.

[50] J. M. Acton and M. Hibbs. Why Fukushima was preventable. JSTOR, 2012.

[51] K. Satake. Lessons learned regarding Tsunami Hazard assessment and protection against tsunami of nuclear installations. Technical report, Earthquake Research Institute at Univesity of Tokyo, June 2012.

[52] Nuclear Regulatory Commission. Standard Review Plan for the Review of SafetyAnalysis Reports for Nuclear Power Plants: LWR Edition. Technical Report NUREG-0800, Nuclear Regulatory Commis- sion.

[53] International Atomic Energy Agency. IAEA Safety Standards - Safety of Nuclear Power Plants: Design. Technical Report SSR-2/1, International Atomic Energy Agency, 2016.

[54] American Nuclear Society. Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants. Number ANS 51.1-1983. 1983.

[54] Department of Energy. DOE Standard: Safety of Magnetic Fusion Facilities: Requirements. Technical Report DOE-STD-6002-96, Department of Energy, May 1996.

[55] Nuclear Regulatory Commission. Fault Tree Handbook. Technical Report NUREG-0492, Nuclear Regulatory Commission, 1981.

[56] Nuclear Regulatory Commission. PRA Procedures Guide. Technical Report NUREG-2300, Nuclear Regulatory Commission, 1983.

[57] American Society of Mechanical Engineers. Probabilistic Risk Assessment Standard for Advanced Non-Light Water Reactor Nuclear Power Plants. Number ASME/ANS RA-S-1.4-2021. 2021.

[58] Nuclear Regulatory Commission. Application of the single-failure criterion to safety systems. Technical Report Regulatory Guide 1.53, Nuclear Regulatory Commission, November 2003.

[59] Nuclear Regulatory Commission. Quantifying Reactor Safety Margins. Technical Report NUREG- 5249, Nuclear Regulatory Commission, 1989.

[60] Domestic Licensing of Production and Utilization Facilities. 10 CFR Part 50, 2007.

[61] Nuclear Regulatory Commission. Application and testing of safety-related diesel generators in nuclear power plants. Technical Report Regulatory Guide 1.9, Nuclear Regulatory Commission, March 2007.

[62] Nuclear Regulatory Commission. Anticipated Transients Without SCRAM for Light Water Reactors. Technical Report NUREG-0460, Nuclear Regulatory Commission, 1978.

[63] Nuclear Regulatory Commission. Historical Review and Observations of Defense-in-Depth. Technical Report NUREG-KM-0009, Nuclear Regulatory Commission, 2016.

[64] Nuclear Energy Institute. Risk-Informed Performance-Based Guidance for Non-Light Water Reactor Licensing Basis Development. Technical Report NEI 18-04, 2018.

[65] Department of Energy. DOE Standard: Tritium Handling and Safe Storage. Technical Report DOE- STD-1129-2015, Department of Energy, September 2015.

[66] J. Nathwani, A. Busigin, and R. Tulk. Safety evaluation of the tritium removal facility (TRF) at Darlington NGS. Fusion Technology, 14(2P2B):1121–1129, 1988.

[67] Klein, J. et al. A New Hydrogen Processing Demonstration System. (SRNL-L2100-2015-00033), 2015.

[68] Nuclear Energy Institute. Revised NEI 97-04, Appendix B: Guidance and Examples for Identifying 10 CFR 50.2 Design Bases. Technical Report NEI 97-04, 1999.

[69] Nuclear Regulatory Commission. Design Specific Review Standard for NuScale SMR Design: Chapter 15 - Transient and Accident Analyses. Technical Report NRC Accession Number ML15355A302, 2016.

[70] Nuclear Regulatory Commission. Design-Basis Hurricane and Hurricane Missiles for Nuclear Power Plants. Technical Report Regulatory Guide 1.221, Nuclear Regulatory Commission, October 2011.

[71] R. P. Martin. Content, completeness, and consistency of analytical models for regulatory consideration. Nuclear Technology, 193(1):96–112, 2016.

[72] N. G. Leveson. Engineering a Safer World. Massachusetts Institute of Technology, 2011.

[73] E. Broughton. The Bhopal disaster and its aftermath: a review. Environmental Health, 4(1):1–6, 2005.

[74] The official report of The Fukushima Nuclear Accident Independent Investigation Commission: Executive Summary. The National Diet of Japan, 2012.

[75] Farmer, F. G. et al. Risk Assessment Handbook. Department of Energy, September 1990.

[76] International Atomic Energy Agency. Component reliability data for use in probabilistic safety assess- ment. Technical Report IAEA-TECDOC-478, October 1988.

[77] Nuclear Regulatory Commission. Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants. Technical Report NUREG-6928, Nuclear Regulatory Com- mission, 2007.

[78] L. Cadwallader and S. Eide. Component failure rate data sources for probabilistic safety and reliability. Process Safety Progress, 29(3):236–241, 2010.

[79] S. M. Jing Xing. White Paper: Practical Insights and Lessons Learned on Implementing Expert Elici- tation. Number NRC Accession Number ML16287A734. Nuclear Regulatory Commission, 2016.

[80] L. Cadwallader. Failure rate data analysis for high technology components. Technical report, Idaho National Laboratory (INL), 2007.

[81] Nuclear Regulatory Commission. Tutorial on Probabilistic Risk Assessment (PRA). https://www.nrc.gov/about-nrc/regulatory/risk-informed/rpp/pra-tutorial.pdf, 2016.

[82] NuScale. NuScale Design Control Document: Chapter 19 - Probabilistic Risk Assessment and Severe Accident Evaluation. Technical Report NRC Accession Number ML20224A508, 2020.

[83] Department of Energy. DOE Standard: Development of Probabilistic Risk Assessments for Nuclear Safety Applications. Technical Report DOE-STD-1628-2013, Department of Energy, November 2013.

[84] Nuclear Regulatory Commission. Human Factors Engineering Program Review Model. Technical Report NUREG-0711, Nuclear Regulatory Commission, 2012.

[85] Nuclear Regulatory Commission. Feasibility Study for a Risk-Informed and Performance-Based Reg- ulatory Structure for Future Plant Licensing. Technical Report NUREG-1860, Nuclear Regulatory Commission, 2007.

[86] K. Jung, J. H. Park, J. Kim, S.-H. Yun, and H. Chung. Tritium accountability of a uranium hydride bed using a calorimetry methodology. High Temperatures–High Pressures, 48, 2019.

[87] T. Hayashi, T. Suzuki, M. Yamada, W. Shu, and T. Yamanishi. Safe handling experience of a tritium storage bed. Fusion Engineering and Design, 83(10-12):1429–1432, 2008.

[88] L. Cadwallader and D. Sanchez. Secondary containment system component failure data analysis from 1984 to 1991. Technical report, EG and G Idaho, Inc., Idaho Falls, ID (United States), 1992.

[89] International Atomic Energy Agency. Risk informed regulation of nuclear facilities: Overview of the current status. Technical Report IAEA-TECDOC-1436, February 2005.

[90] Nuclear Regulatory Commission. Guidance for a Technology-Inclusive, Risk-Informed, and Performance-Based Methodology to Inform the Licensing Basis and Content of Applications for Li- censes, Certifications, and Approvals for Non-Light Water Reactors. Technical Report Regulatory Guide 1.233, Nuclear Regulatory Commission, October 2020.

[91] Information Notice No. 90-25: Loss of Vital AC Power With Subsequent Reactor Coolant System Heat-Up. Nuclear Regulatory Commission, 1990.

[92] National Research Council and others. Lessons learned from the Fukushima nuclear accident for improving safety of US nuclear plants. 2014.

[93] Leveson, N., Thomas, J. STPA Handbook. March 2018.

[94] Torok, R., Geddes, B. Systems Theoretic Process Analysis (STPA) Applied to a Nuclear Power Plant Control System. Electric Power Research Institute, 2013.

[95] L. A. Dawson, A. B. Muna, T. A. Wheeler, P. L. Turner, G. D. Wyss, and M. Gibson. Assessment of the utility and efficacy of hazard analysis methods for the prioritization of critical digital assets for nuclear power cyber security. Technical report, Sandia National Lab.(SNL-NM), Albuquerque, NM (United States), 2015.[20

[96] J. Thomas, F. Lemos, and N. Leveson. Evaluating the safety of digital instrumentation and control systems in nuclear power plants. NRC Technical Researcy Report2013, 2012.

[97] NuScale. NuScale Design Control Document: Chapter 7 - Instrumentation and Controls. Technical Report NRC Accession Number ML20224A495, 2020.

[98] Nuclear Regulatory Commission. Design Specific Review Standard for NuScale SMR Design: Chapter 7 - Instrumentation and Controls. Technical Report NRC Accession Number ML15356A416, 2016.

[99] Nuclear Regulatory Commission. Design Specific Review Standard for NuScale SMR Design: Chapter 7 - Instrumentation and Controls Appendix A. Technical Report NRC Accession Number ML15355A316, 2016.

[100] Program on Technology Innovation: Early Integration of Safety Assessment into Advanced Reactor Design. Technical Report 3002011801, September 2018.

[101] National Research Council and Winter, Donald C and others. Interim Report on Causes of the Deep- water Horizon Oil Rig Blowout and Ways to Prevent Such Events. National Academy of Engineering and National Research Council, 2010.

[102] L. W. Cullen. The public inquiry into the Piper Alpha disaster. UK Department of Energy.

[103] A. D. Shugard, C. R. Tewell, D. F. Cowgill, and R. D. Kolasinski. Uranium for hydrogen storage applications: a materials science perspective. Technical report, Sandia National Laboratories, 2010.

[104] A. C. Roma and S. S. Desai. The regulation of fusion: A practical and innovation-friendly approach. Hogan Lovells, 2020.

[105] S. Bruske and D. Holland. Risk assessment techniques for the evaluation of tritium accident mitigation. Nuclear Technology-Fusion, 4(2P2):539–543, 1983.

[106] M. Abdou. Tritium Fuel Cycle, Tritium Inventories, and Physics and Technology R & D Challenges. 13th International Symposium on Fusion Nuclear Technology (ISFNT-13), 2017.

[107] R. D. Stambaugh, V. S. Chan, R. L. Miller, and M. J. Schaffer. The spherical tokamak path to fusion power. Fusion Technology, 33(1):1–21, 1998.

[108] F. Najmabadi, L. A. I. of Plasma, and F. Research. The ARIES-I tokamak reactor study, Final Report. na, 1991.

[109] C. Rivkin, R. Burgess, and W. Buttner. Hydrogen technologies safety guide. Technical report, National Renewable Energy Lab.(NREL), Golden, CO (United States), 2015

Appendix 5A – Tritium fueling rate calculations

Determine steady state tritium fueling rate for fusion reactor as a function of fusion power and other plant parameters. The steady state tritium fueling rate ($\dot{m}_{T_{fuel}}$) for a 50/50 D-T plasma can be determined based on three factors: the tritium burn rate ($\dot{m}_{T_{burn}}$), the fuel injection efficiency (η_{eff}), and the fuel burn fraction (f_b). The steady state tritium fueling rate can be calculated as:

$$\dot{m}_{T_{fuel}} = \dot{m}_{T_{burn}}\, \eta_{eff}\, f_b$$

In non-ideal cases, an additional factor related to tritium losses due to tritium hold up and release (f_{loss}) could be included. The non-ideal steady state tritium fueling rate can be calculated as:

$$\dot{m}_{T_{fuel}} = \frac{\dot{m}_{T_{burn}}\, \eta_{eff}\, f_b}{1 - f_{loss}}$$

The non-ideal case is not considered in this analysis due to large uncertainties related to this value.

In prior work, the fuel injection efficiency and the fuel burn fraction have been calculated as both separated and combined factors [12][106]. In this work, the two factors are separated to allow for discussion of the discrete design and engineering choices that can affect these factors.

Tritium burn rate

The tritium burn rate ($\dot{m}_{T_{burn}}$) describes how much tritium must be consumed by fusion reactions to produce a specified fusion power output. This rate is based on a simple energy balance using engineering and physical parameters. The tritium burn rate of the plasma is written as:

$$\dot{m}_{T_{burn}} = \frac{P_{fusion}\, M_T}{N_a\, Q_{fusion}}$$

where:

P_{fusion} – Fusion power of plasma
M_T – Molar mass of tritium
Q_{fusion} – Energy from fusion
N_a – Avogadro's number

Fuel injection efficiency

The fuel injection fraction (η_{eff}) describes what fraction of fuel injected into the torus reaches the plasma and can be consumed. This factor can be hard to separate from the fuel burn fraction because the two factors are often experimentally measured together based on the torus mass and energy balance.

The fuel injection efficiency varies based on a number of design parameters including fueling injection method, fuel injection location, and plasma conditions. This fuel injection rate can vary from below 20% for gas puff fueling and as high as 90% for pellet injection systems. This parameter is highly design specific and selection of a reasonable assumption is viable.

Tritium burn rate

The fuel burn fraction (f_b) describes what fraction of fuel in the plasma fuses before leaving the plasma and being removed by the torus exhaust system. The fuel burn fraction is a function of a number of parameters including plasma density, temperature, and confinement time. The fuel burn fraction is also a function of the recycle coefficient (R), describing how frequently a fuel ion cycles in and out of the plasma before being removed by the torus exhaust system.

The fuel burn fraction estimations can vary dramatically based on the device design and there are still significant questions regarding the calculation of this factor. Two different methods for calculating this factor are described [12][106].

A fuel burn fraction is calculated as (Abdou) [106]:

$$f_b = \frac{1}{\left(1 + \frac{2}{n_e\ \tau^* \langle\ \sigma\ v\ \rangle}\right)} = \frac{1}{\left(1 + \frac{1}{n_T\ \tau^* \langle\ \sigma\ v\ \rangle}\right)} = \frac{n_T\ \tau^* \langle\ \sigma\ v\ \rangle}{n_T\ \tau^* \langle\ \sigma\ v\ \rangle\ +\ 1}$$

where:

$n_T = \frac{n_e}{2}$ (with 50:50 D-T fuel mix)

$< \sigma v > = 3.68\ \times\ 10^{-18}\ T_i^{-2/3}\ e^{-19.94\ T_i^{-1/3}}$ [107]

$\tau^* = \frac{\tau_\rho}{1 - R}$ [106]

$\tau_\rho = 4\ \tau_e$ [108]

and

n_e (electron density, m^{-3})
T_i (average ion temperature, keV)
R (recycling coefficient) [106]
τ_ρ (particle confinement time, s)
τ_e (energy confinement time, s)

The fuel burn fraction is alternatively formulated (without the fueling injection efficiency) as (Jackson) [12]:

$$f_b = 10^{14}(1 + S_n)\, \tau_\rho^* \, n_{020}\, T_0^2\, I$$

where:

$S_n = \frac{n_{020}}{\bar{n}} - 1$
$S_t = \frac{T_0}{T_i} - 1$
$\tau_\rho^* = \frac{\tau_\rho}{1-R}$
$n_{020} = \frac{n_e}{2}$ (50:50 D-T ion mix, units of $10^{20}/\mathrm{m}^3$)

and:

T_0 (central ion temperature, keV)
T_i (average ion temperature, keV)
τ_ρ (particle confinement time)
n_{020} (central ion density)
I (fusion reactivity integral [12]

Comparison of these two fuel burn fractions suggests that the Jackson approximation predicts higher fuel burn fraction than the Abdou approximation. As a result, an average of these two approximations is used as the basis for the fuel burn fraction and the overall tritium burn rate.

Appendix 5B – System description for deuterium-tritium storage system

This appendix documents a simplified design concept description for the deuterium-tritium storage system analyzed in Chapter 12. The system function as described in Chapter 2 is to “store reserve or backup separated tritium and deuterium fuel”. This section describes a general arrangement and concept of operations for the deuterium-tritium storage system described in Chapter 3 and parameterized in Chapter 5. Overall, the system is designed to store approximately 1.4 kg of reserve tritium that could be used to fuel plant systems during outages of either the exhaust processing system or breeding blanket tritium extraction systems.

This storage system is designed on the principle of separating tritium storage inventories to minimize the potential for catastrophic inventory losses. The tritium inventory stored on separated depleted uranium metallic hydride storage beds. Storage beds with acceptable loading and uploading rates have a typical maximum capacity of 70 grams are assumed based on existing tritium storage technology [67]. Each of the storage beds is assumed to be stored in an secured, reinforced structure that protects it against external hazards such as explosions or impacts failures of nearby systems. This assumption is based on the use of similar systems (called Highly Invulnerable Encased Safe [HIVES]) at SRNL for protection of tritium storage beds [65].

This system is designed with 3 barriers to radiological release for significant radiological inventories and 2 barriers to radiological release for minor radiological inventories. The tritium storage beds are double walled containers designed to minimize tritium leakage and ensure confinement of the radiological inventory. All tritium storage beds, associated pipes, valves, and other components are enclosed in a glovebox with an associated glove box clean-up (primarily detritiation) system [65]. This is the second barrier for large tritium inventories (storage beds) and the first barrier for smaller tritium inventories (process piping and system leakage). This approach is standard practice industrial practice for handling of large tritium inventories. The glovebox allows for operator access and remote maintenance of tritium storage systems. The glovebox may also have an inert atmosphere to reduce the likelihood of hydrogen fires or explosions [65].

The glovebox system is enclosed by a secondary containment structure. This D-T storage system building is intended as a low quality confinement structure that can slow the release of radiological material but is not credited as very low leakage barrier. This structure can, however, slow the ground level release of radiological material and provide additional response time for other engineered safety features to clean up or remove radiological material though more favorable release pathways. Per DOE guidance on use of buildings as low-quality confinement structures, a leak rate of 5% of the radiological inventory per hour at ground level could be assumed [65].

The D-T storage system building is equipped with two additional engineered safety features to reduce the on- and off-site consequences associated with release of radiological material. The first feature is a high-capacity, single-pass building ventilation system. The purpose of this system is to quickly cycle the air in the structure to remove airborne radiological material. The second feature is a building stack. The stack, along with the building ventilation system, is enables the elevated release of radiological material under certain accident conditions. While the confinement of radiological material is preferred to the release of radiological material, in cases where the confined material could initiate additional releases (e.g., subsequent fires or explosions from confined gaseous tritium), dispersal is an effective method at reducing individual exposures to radiological material [65]. In this case, these two engineered safety features enable the dispersal of released radiological materials and reduce the hazard consequences associated with these releases.

In addition to the systems described above, standard industrial practices regarding the design of hydrogen processing systems (e.g., ASME Standard B31.12 for Hydrogen Piping and Pipelines) would be used to dictate required additional engineered safety features (e.g., emergency shut-off valves, instrumentation) but these features are not considered in this simplified design concept [109]. Figure 5B.1 shows a general schematic of the D-T Storage System and associated containment structures. Note that only top-level systems and structures are shown.

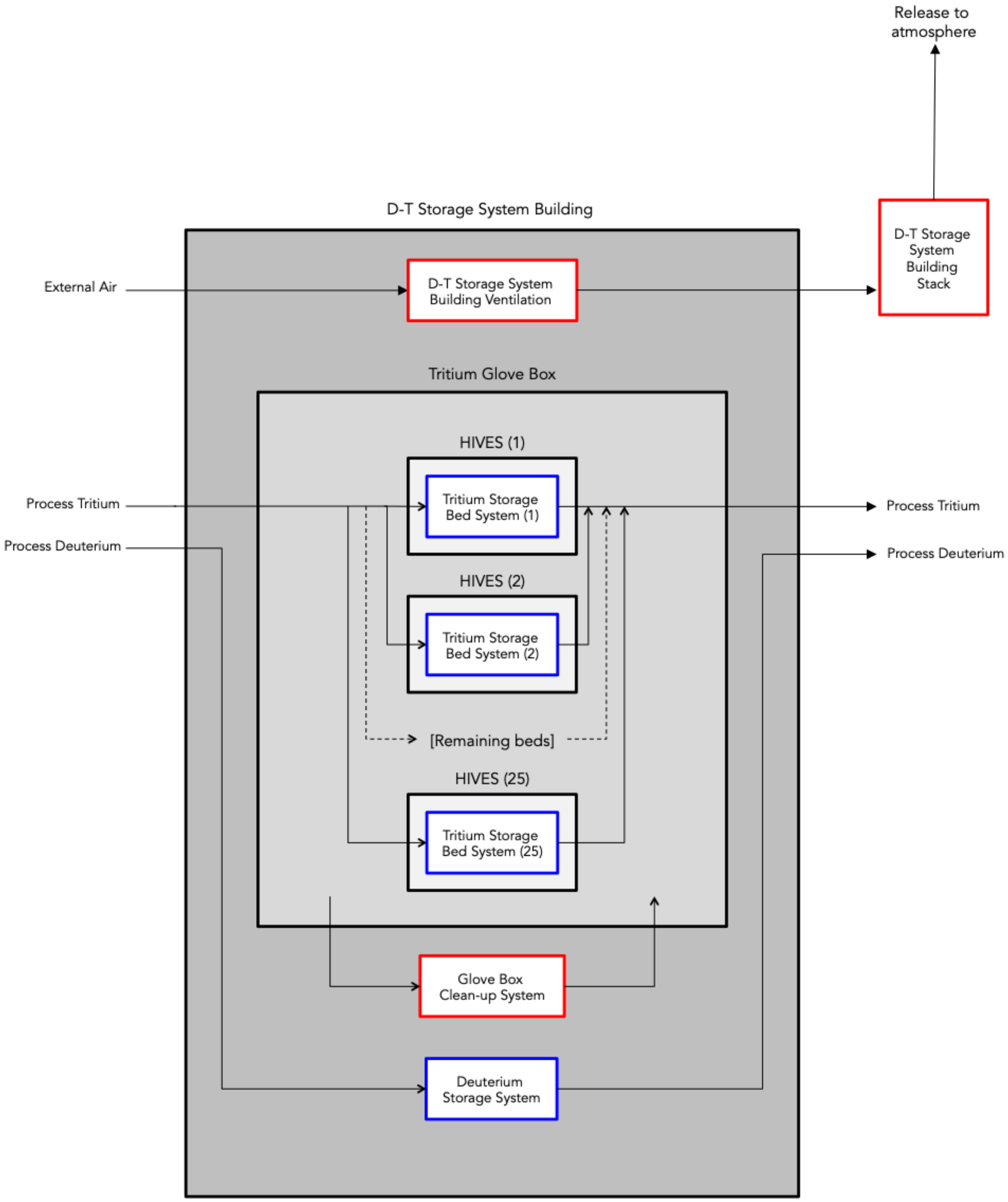

Release to atmosphere
D-T Storage System Building
External Air
D-T Storage System Building Ventilation
D-T Storage System Building Stack
Tritium Glove Box
HIVES (1)
Process Tritium
Process Deuterium
Tritium Storage Bed System (1)
Process Tritium
Process Deuterium
HIVES (2)
Tritium Storage Bed System (2)
[Remaining beds]
HIVES (25)
Tritium Storage Bed System (25)
Glove Box Clean-up System
Deuterium Storage System

Figure 5B.1 D-T Storage System Design Concept

Appendix 5C – PRA fault tree and event tree parameters and calculations

This appendix contains the fault trees, event trees, and parameter calculations for the probabilistic design basis evaluations.

Table 5C.1 PRA Fault Tree Results

Event No.	*Events*	*Probability* (yr^{-1})	*Source*
INT-1	Loss of glove box clean up	1.00E-02	[105]
INT-2	Loss of process pipe integrity	3.00E-01	[105]
INT-3	Loss of glove box integrity	4.00E-02	[88]
INT-4	Loss of storage bed integrity	4.00E-02	[88]
INT-5	Loss of storage bed inventory	8.24E-04	Calculated based on SSC-1 Fault Tree
INT-6	Loss of multiple storage bed inventory	N/A	Either independent and negligible OR common cause and external event
INT-7	Simultaneous loss of storage, glove box	N/A	Bounded by Int-5 sequence
SSC-1	SSC-1: Storage bed inventory lost	8.24E-04	Calculated based on SSC-1 Fault Tree
SSC-2	SSC-2: Glove box integrity not maintained	1.20E-02	Calculated based on SSC-2 Fault Tree
SSC-3	SSC-3: Glove box clean up not functional	6.21E-01	Calculated based on SSC-3 Fault Tree
SSC-4	SSC-4: Facility building confinement not maintained	3.20E-02	Calculated based on SSC-4 Fault Tree
SSC-5	SSC-5: Facility building ventilation not functional	1.20E-02	Calculated based on SSC-5 Fault Tree
SSC-6	SSC-6: Facility building stack not functional	1.98E-03	Calculated based on SSC-6 Fault Tree

The full data tables are not feasible to reproduce in this file. Please contact the original author to obtain the electronic files. R. Patrick White – r.patrick.white@gmail.com

Appendix 5D – STPA evaluation parameters

This appendix contains the evaluations for the STPA assessment of the Deuterium-Tritium storage system.

The full analysis tables are not feasible to reproduce in this file. Please contact the original author to obtain the electronic files. R. Patrick White – r.patrick.white@gmail.com

Chapter 6 – Regulatory frameworks for commercial fusion facilities

This chapter develops and describes regulatory frameworks that could contribute to an overall regulatory framework for commercial fusion facilities. A conceptual model for the characterization of operating states that result in system failure relative to operational and regulatory limits is first presented and discussed. The five proposals for regulatory frameworks including their basis and compatibility with the licensing evaluation methods of Chapter 5, for commercial fusion facilities are presented. The potential impacts of the regulatory framework on the development of commercial fusion facilities is also discussed.

6.1 Conceptual model for operational failure space

System failure is rarely a desired or expected outcome of system operation; operators will rarely decide consciously to take actions that will lead to system failure and harm. System failures still occur, however, in both complex and simple engineered systems. A general characterization of system failure and its relationship to designers, operators, and regulators is helpful at understanding how we can design regulatory frameworks that mitigate, reduce, or eliminate both the probability the consequences of system failures. Prior work on operations and safety in complex engineering systems have highlighted the importance of system interactions and different operational actors [1]. This work builds off of prior models of system failure by characterizing the system operation using five different limits and an operational point:

- Operational Point: conditions where the system currently is operating
- True Failure Limit: condition limit beyond which failure actually occurs
- Understood Failure Limit: condition limit beyond which failure is expected to occur given mechanistic system understanding and uncertainties
- Regulatory Operating Limit: condition space where operation is permitted
- Operator Comfort Limit: condition space where operators will operate
- Normal Operating Limit: condition space where operators should operate

The operating point and the five limits characterize the full operating space, and provide a model for discussing the effects of different regulatory frameworks on system safety. Figure 6.1 shows a general graphical representation of an ideal engineered and operating system where the limits are arranged with increasing levels against system failure and the operational point is inside of the Normal Operation Level.

This conceptual arrangement of layered design and operational limits is similar to the process used for quantification and management of uncertainties for engineering parameters such as minimum departure from nucleate boiling ratio (MDNBR) in water cooled fission reactors [2] or margin quantification for analytic modeling codes and best estimate analyses [3]. This conceptual model is more generalized (encompassing a multi-dimensional failure space) than the conventional engineering limits model. This model also introduces two additional limits: the Operator Comfort limit that includes expected deviations between facility procedure and operator actions and the True Failure Limit that includes the actual system conditions that result in failure.

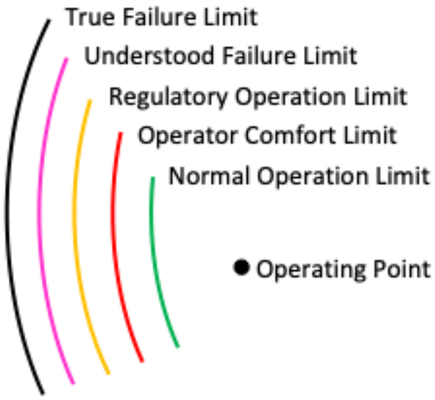


Figure 6.1. Ideal system operating limits

An example loaded cantilevered beam system (Figure 6.2) is used throughout this section to illustrate the different failure limits.

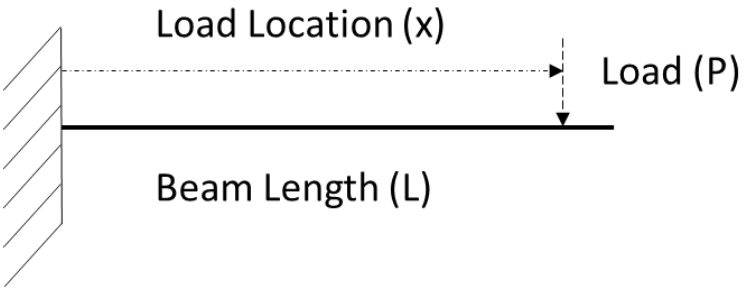


Figure 6.2. Cantilever beam loading illustrative example

6.1.1 Operational Point

The operational point consists of the instantaneous and time dependent factors, conditions, and states that describe the system. The operational point is, in many ways, a point that can be described but not ever fully defined due to the epistemic uncertainties related to definition of a state and aleatoric nature of the operating point. All factors relevant to system operation and system failure may not be known or may not be measurable. Rare, unknown events may be critical to system failure but would not be characterized as operational factors until observed. Determining all of the relevant characteristics to an operating point is extremely challenging and requires deep (sometimes unknowable) mechanistic understanding of the system behavior and interactions.

In the cantilevered beam system example, the operating point consists of actual factors and conditions (loads, locations, other factors) for the system. Definition and quantification of this space is limited by our mechanistic understanding of relevant factors. While characterization based on load and location may seem like the relevant operational conditions, more detailed knowledge of system failure mechanics provides insights that other factors and conditions such as static versus transient loading, historical loading and fatigue, beam condition and manufacturing, and fixed location anchoring may be critical operating points to include in a description. This full set of points constitutes the operating point for a system.

6.1.2 True Failure Limit

System failures and the concept of system safety are highly dimensional problems. The operating point of a system is a combination of different operating conditions, some instantaneous while others are history dependent. It may include physical conditions, operator conditions, environmental conditions, or any other factors that contribute to loss of system form or function. The True Failure Limit is defined in this work as the set of all limiting conditions and factors that result in system failure and loss. The True Failure Limit cannot be known *a priori* and can only be characterized through actual system failures. System failure occurs when the system operating point intersects with the True Failure Limit space. In the cantilevered beam system example, the True Failure Limit space consists of all factors and conditions (static and time dependent) that result in system failure.

Completely describing the failure space for even this simple system is challenging due to the nature of epistemic uncertainties related to system failure. While we can characterize some observable characteristics of the True Failure Limit such as the limiting load (e.g., load location, load magnitude) under specific conditions, our understanding of factors and conditions that contribute to system failure are limited by our knowledge of the mechanistic nature of failure and correct characterization of system boundaries. The True Failure Limit is a function of time, space, and other unknown number of factors, ultimately representing an infinite set of possible failure conditions.

6.1.3 Understood Failure Limit

The True Failure Limit is challenging to use for the design and engineering of systems because it can only be observed at discrete operating points when failure occurs. Design and engineering of systems requires description of system conditions and factors relationships that are believed to produce system failure. The Understood Failure Limit is defined in this work as the set of specific conditions and factors that lead to system failure and loss based on best mechanistic understanding of system behavior and interactions. The Understood Failure Limit reflects operating experience with a system. Operational points that resulted in system failure (i.e., observed True Failure Limit points) are known points on the Understood Failure limits while the remainder of the Understood Failure Limit must be characterized through interpolation or extrapolation.

The Understood Failure Limit consists of models, relationships, and other methods that can be used to characterize the expected failure of a system. Most failure models recognize both epistemic and aleatory uncertainties that can lead to a distribution of failure probabilities for operating points that are otherwise identical based on the conditions and factors described. As a result, the Understood Failure Limit may be given a probability distribution space, with confidence intervals given based on variations in different conditions and factors. The Understood Failure Limit is ultimately a characterization of the understanding of system behavior and where system failure may occur.

In the cantilevered beam system example, the Understood Failure Limit space consists of all factors and conditions (loads, locations, other factors) that may lead to system failure. This could be based on analytic models (e.g., beam bending models), computational simulations, and collected data regarding the failure of similar cantilevered beams. Other factors (e.g., fatigue, loading conditions) may be included if there is sufficient mechanistic understanding to characterize and include these factors.

The Understood Failure Limit is not a fixed limit. The limit will change based on the varying mechanistic understanding of those who specify it. For novel technologies or systems, operating experience with related technologies or preliminary understanding of the mechanistic basis of its operation is used to develop the Understood Failure Limit. Conditions or factors of importance may be very limited in the initial Understood Failure Limit. The Understood Failure Limit will change as observations of success or failure is developed through practical observation of actual operating points. This practical experience may also lead to development of insights on new conditions or factors of importance that affect system failure. The Understood Failure Limit and underlying models will also change due to development of better mechanistic understanding of system behavior through detailed study of theory and operational performance.

An unexpected failure occurs when an operating point intersects with the True Failure Limit but not the Understood Failure Limit – the existing mechanistic models did not predict the failure. The inability to predict the failure may result from issues including incomplete or incorrect system mechanistic or behavior models, system conditions or factors incorrectly excluded or absent from the Understood Failure Limit space, or incomplete or incorrect understanding and characterization of system interactions. These unexpected failures are challenging because they represent the emergence of new (or previously neglected) failure modes. An importance nuance to the Understood Failure Limit space is that it must correctly identify the mechanistic behavior that lead to system failure. Models that correctly predict system failure but predict the wrong failure mechanism are particularly dangerous because they provide a false sense of mechanistic understanding and predictive power regarding the safety of similar operational states.

Full comparison of the True Failure Limit and the Understood Failure Limit is challenging due to the *a priori* unknowable nature of the True Failure Limit. Instead, observation of operational points against the Understood Failure Limit provides evidence on where the Understood Failure Limit accurately predicts system failure, incorrectly predicts failure will occur, or does not correctly predict that failure will occur. In the cases where the Understood Failure Limit does not accurately predict system failure (or lack of failure), the Understood Failure Limit should be reviewed to determine how models, relationships, or methods could be improved to more accurately predict system failure. This may include changes to mechanistic models or the inclusion (or exclusion) of different conditions and factors in the Understood Failure Limit.

For a novel technology with limited operating experience and mechanistic understanding, it is likely that there will be deviations between the Understood Failure Limit and the observed system behavior and system failure. If operating experience is adequately incorporated into the Understood Failure Limit and mechanistic models are improved through deliberate study, it is expected that the Understood Failure Limit will begin to better reflect the True Failure Limit over time. The main challenges limiting convergence of the Understood Failure Limit to the True Failure Limit are the ability to correctly incorporate operating experience, changes to system design or operation that limit the applicability of prior operating experience, and the quality and availability of operating experience at specific off-normal operating points with high uncertainty.

6.1.4 Regulatory Operation Limit

The primary goals of health and safety regulators is to protect workers, the public, and the environment from the acute and chronic harms associated with regulated activities (Table 6.1). Regulators will seek to eliminate (or reduce to acceptable levels) system failures and operational modes that result in acute or chronic harm. One method regulators may utilize to prevent harm is to prohibit operation points that will result in system failure or irrecoverably lead to system failure.

Table 6.1. U.S. Safety Regulator Missions

U.S. Regulator	*Regulator Mission*
Environmental Protection Agency	"...protect human health and the environment." [4]
Occupational Safety and Health Administration	"...ensure safe and healthful working conditions for working men and women by setting and enforcing standards and by providing training, outreach, education and assistance." [5]
Federal Aviation Administration	"...provide the safest, most efficient aviation system in the world." [6]
Nuclear Regulatory Commission	"...provide reasonable assurance of adequate protection of public health and safety and to promote the common defense and security and to protect the environment." [7]

In principle, exclusion of all operating points within the True Failure Limit space would result in completely safe system operation. In practice, the True Failure Limit space cannot be fully defined *a priori*, so exclusion of operating points is based on the Understood Failure Limit. Using the Understood Failure Limit instead of the True Failure Limit means that there is the potential for unexpected system failures if the Understood Failure Limit fully bound the True Failure Limit. Defining a limit on operational points with engineering margin beyond of the Understood Failure Limit can help prevent unexpected failures by accounting for uncertainties in inputs such as system conditions, factors, system interactions, and mechanistic model understanding in the Understood Failure Limit.

The Regulatory Operation Limit is defined in this work as a limit on operational points that provides additional engineering margin before the system failure characterized by the Understood Failure Limit. This space reflects a set of understood specific factors and conditions that, if operated within, will result in safe operation with an acceptably low probability of exceedance while accounting for uncertainties in Understood Failure Limit. This probability of exceedance is critical because it acknowledges that a facility may satisfy all Regulator Operation Limits but still experience an unexpected system failure if the Understood Failure Limit and additional margin provided by the Regulatory Operation Limit do not fully exclude operation points at the True Failure Limit. Defining different levels of additional engineering margin for the Regulatory Operation Limit will result in both different expected probability of exceedance and actual probability of exceedance.

Definition of a Regulatory Operating Limit is based on the regulator's understanding of the True Failure Limit and the Understood Failure Limit, assessment of quantified and unquantified uncertainties, confidence in the mechanistic models underlying the Understood Failure Limit, and the accepted risk (probability and consequence) that the True Failure Limit will exceed the Regulatory Operation Limit for an unexpected failure event. This Regulatory Operating Limit may also account for expected variances in operator (or other operation controller) behavior, as well as system transients that could result in unsafe operating points before operations could be corrected and mitigated.

Defining a Regulatory Operating Limit is extremely challenging due to the potential impacts on facility system operation. If Regulatory Operating Limits are not sufficiently conservative, acute or chronic harm may result from unexpected failures. If a Regulatory Operating Limits are overly conservative, facility operations may be constrained to the point of inhibiting production despite adequate operational margin to the True Failure Limit. Definition of an appropriate Regulatory Operating Limit that protects against harm but enables facility operation is dependent on an accurate Understood Failure Limit and characterization of uncertainties and engineering margin.

In the cantilevered beam system example, the Regulatory Operating Limit space consists of all permissible operating factors and conditions (loads, locations, other factors) for the system. This would be based on Understood Failure Limit, the known and unknown uncertainties associated with the Understood Failure Limit, desired margin against the Understood Failure Limit, and an assessment of the consequences associated with different types of system failure. An example Regulatory Operating Limit would be a maximum load of no greater than 75% of the median failure load in the Understood Failure Limit model at any point on the cantilevered beam. This limit would help control factors such as load and its location, and provide additional margin against unknown factors. Depending on the level of system understanding, the exact needed margin against failure could be more accurately quantified.

The Regulator Operating Limit is largely fixed based on the requirements propagated by regulators. These limits may be changed over time based on events such as observed operational failures, changes to the Understood Failure Limit, changes in regulator confidence regarding the Understood Failure Limit, or changes to the societally accepted occurrence of unexpected system failures. The Regulator Operating Limit, unlike other limits, is fully defined and characterized.

For a novel technology with limited operating experience and mechanistic understanding, the large expected deviations between the True Failure Limit and Understood Failure Limit creates significant challenges for the definition of Regulatory Operating Limit. Regulators may be forced to define overly conservative Regulatory Operating Limits to prevent unexpected systems failures and risk making the technology infeasible to develop, or accept the unexpected failures and harms associated with non-conservative Regulatory Operating Limits.

An overly conservative Regulatory Operating Limit can significantly hamper the initial development and deployment of a novel technology. Demonstration and testing strategies for novel technology, however, can be designed to develop in parallel with changes to Regulator Operating Limits. Scale technology demonstrations, separate effects testing, or prototype operation and testing with additional safety features or considerations can all be utilized to meet initial conservative Regulatory Operating Limit. Development of operating experience through controlled testing programs enables the verification of mechanistic models, quantification and reduction of uncertainties, and validation of the Understood Failure Limit though demonstrated operation. Controlling the hazards of testing through the methods described above can help justify the revision of Regulatory Operating Limits and development of less conservative Regulatory Operating Limits that still ensure safe technology operation.

Regulators are challenged to define sufficiently conservative Regulatory Operating Limits that protect public health and safety while still facilitate testing and improvement of Understood Failure Limits for novel technologies.

6.1.5 Operator Comfort Limit

An operator's understanding of system conditions and operation is separate from a system's operational point as defined in this work. Each operator (or operational controller) possesses a model of the current system based on their perception of the system conditions and understanding of system behavior and interactions. This distinction reflects that operator understanding through is a function of past experience, system knowledge, and the system instrumentation, monitoring, and control that allows operators to develop working mental (or physical) models of the system. The more complete and accurate the operator's model of the operational point and system trajectory, the greater their capability to accurately characterize and predict the system conditions.

The Understood Failure Limits describes the operational limits where failure is expected to occur based on the best understanding of the mechanistic behaviors and conditions but does not directly reflect the operating points where operators are willing to operate the system. The Operator Comfort Limit is defined in this work as the set of all plant conditions and states (both static and time dependent) that an operator (or other operational controller) permits the system to operate. This Operator Comfort Limit characterizes, in part, the plant conditions and states that the operator believes that they can safely operate the system within before experiencing failure or irrecoverable system states that will lead to failure.

The Operator Comfort Limit is largely based on operator understanding of the system behavior and conditions, believed accuracy of Understood Failure Limits based on their operational experience, importance of Regulatory Operating Limits, individual knowledge of plant specific operating experience, and other organizational factors that affect assessment of safe operational points. Operators will often have intimate knowledge of plant systems and understand the affects of deviations from normal procedure. Their operational experience can provide insights not always included in the Understood Failure Limits. This experience provides better insights into plant operations and can help better characterize the safe operating space for a facility. Conversely, operators may have an erroneous understanding of safe operating points based on their experiences, understanding of exact system conditions or factors, or organization factors that push them to operator plants beyond their normal conditions. These factors can all lead to unexpected system failures.

The concept of an operator and the resulting Operator Comfort Limit is not constrained to physical, human operators. Software and hardware based control systems both rely on operational assumptions, behavior models, and inputs to perform their control functions. The role of faulty process models in software related system failures has been previously documented and the challenges associated with the integration of software into complex, high hazards systems is well known [8]. Non-human operational controllers may function correctly but assumptions present in the design of the controller or in their models can contribute to incorrect control actions that lead to unexpected system failures.

Catastrophic system failures such as the Boeing 737 Max 8 crashes highlight how software operational controller model can contribute to a system failure [9]. The Maneuvering Characteristics Augmentation System (MCAS) software was designed to automatically adjust plane pitch if certain airspeed and angle conditions occurred during flight. During both Boeing 737 Max 8 accidents, the MCAS system correctly automatically adjusted plane pitch down based on readings from flight instrumentation. The flight instrumentation, however, was in a failed condition that produced incorrect but unrecognized data on plane angle. The MCAS software repeated adjusted the plane pitch into the ground against pilot commands and ultimately contributed to the two catastrophic 737 Max 8 crashes. The operational controller (MCAS) had a faulty operational model of the operating point and, despite correctly functioning according to the design specification, lead to an unexpected system failure. This accident highlights how the operator or operational controller model of the system behavior is critical to operations.

Human operators, non-human operational controllers, and human-machine hybrid control systems all rely on conceptual models of system conditions and behavior to guide operational decision making. These models may be implicit (e.g., human operator understanding of system behavior) or explicit (e.g., control logic assumptions and set points) but they affect the control of system conditions. If the conceptual model and understanding of system conditions and behavior is incorrect, an operator or operator controller may take actions that result in system failure while believing (or executing code) that is believed to result in safe operation. These conceptual models serve as the basis for the Operator Comfort Limit for human operators, non-human operational controllers, and human-machine hybrid control systems.

The Operator Comfort Limit will vary over time, operator-to-operator, facility-by-facility. Characterizing the experience of operators and the resulting Operator Comfort Limits is critical at developing Understood Failure Limits that more accurately reflect the True Failure Limits. Simultaneously, developing Operator Comfort Limits that align with Regulatory Operating Limits is important if the regulator limits serve as a legitimate bound on safe operating points. “Human error” accidents often occur when the Operator Comfort Limit is misaligned with the Regulatory Operating Limits, and the operator acts outside of the Regulatory Operating Limits due to external pressures (time, cost, schedule, environmental) but believes that the operating point will not exceed True Failure Limit and lead to system failure. Regulator, designer, and operator (or operational controller) understanding of system behavior, conditions, and interactions are critical to ensuring on-going safe operation of systems.

In the cantilevered beam system example, the Operator Comfort Limit consists of all operating points (loads, locations, other factors) for the system that the operator (or operational controller) will permit operations. The Operator Comfort Limit would be based on the operator’s understanding the system conditions, behaviors, and interactions. If an operator believes that the loading conditions beyond the Regulatory Operating Limits will not result in system failure and that violating Regulatory Operating Limits is necessary to satisfy other organizational demands (e.g., schedule pressure), then the Operator Comfort Limit may lie outside of the Regulatory Operating Limit for those operating points. These limits vary on an operator-by-operator basis depending on their experience, understanding, and other organizational characteristics.

Comparison of the Operator Comfort Limit with the Regulatory Operating Limit and Understood Failure Limit may be challenging due to the large number of relevant plant conditions and factors, and the varying nature of limits with different operating conditions. One important characteristic to conceptualize, however, is how operator understanding of plant condition varies with changes to the True Failure Limit:

- perfect system understanding: Operator Comfort Level will varies in the same direction and magnitude with True Failure Limit variations

- correct system understanding: Operator Comfort Level will varies in the same direction with True Failure Limit variations
- no system understanding: Operator Comfort Level does not change with regard to True Failure Limit variations
- incorrect system understanding: Operator Comfort Level will varies in the opposite direction with True Failure Limit variations

While perfect system understanding is desirable because the system operators have a constant margin between operational points and system failure, it is not necessarily required for safe system operation if the Operator Comfort Limit does not intersect with the True Failure Limit. Incorrect system understanding is critically dangerous because operators will believe that they are putting a system into a safe state but due to system conditions, behavior, or interactions not understood or known to the operators, they are actually driving the system closer to the True Failure Limit space. The goal of the design and operational organizations for these systems is to eliminate or mitigate situations where operators can develop incorrect system understanding and expand the Operator Comfort Limit to operational points that intersect with the True Failure Limit.

6.1.6 Normal Operation Limit

The final operating limit used in this conceptual model is the Normal Operation Limit. The Normal Operation Limit is defined in this work as the permitted operational points that enable safe and successful facility operation, with sufficient margin to the Regulatory Operating Limits. The Normal Operation Limits may be based on a number of factors including asset protection (e.g., preventing excessive asset depreciation, minimizing acceptable risks), economic factors (e.g., maximizing system output), and risk of exceedance of regulatory limits (e.g., minimizing risks associated with violating Regulatory Operating Limits). The Normal Operation Limit creates an additional set of operating margins that are intended to create an operational envelope far from the Understood Failure Limit and True Failure Limit. Operational points within the Normal Operating Limit should never intersect with the True Failure Limit and result in system failures.

In the cantilevered beam system example, the Normal Operating Limit consists of all normal and acceptable operating factors and limiting conditions (loads, locations, other factors) for the system. This would be based on Understood Failure Limit and the Regulatory Operating Limit. Example Normal Operating Limits would be limits on load and load location that are no greater that 50% of the Regulatory Operating Limit. This limit helps ensures that reasonable operational deviations and other unknown factors would not result in operational points that exceed the Regulatory Operating Limit.

Developing Normal Operation Limits may be challenging due to the competing forces on the space of acceptable operating point. Jens Rasmussen (no relation to MIT NSE Professor Norman Rasmussen) characterized competing constraints on system safety, pressure to maximize economic performance, and worker tendency to minimize effort associated with operations in Figure 6.3. This figure (modified with Regulatory Operating Limits replacing “Boundary of Functionally Acceptable Performance”) illustrates how competing forces may constrain operational points. If the Normal Operation Limits are overly constrained, the feasible operational space may be extremely small or even non-existent. Depending on the Operator Comfort Limits, routine operation outside of the Normal Operation Limit may become normalized as they seek to satisfy an over constrained problem. While this type of normalized off-normal operation may not, in itself, lead to system failure, this represents a functional breakdown in the limits and could lead to invalidation of assumptions critical to the Understood Failure Limit. Development and enforcement of Normal Operation Limits is critical to safe and sustainable facility operation.

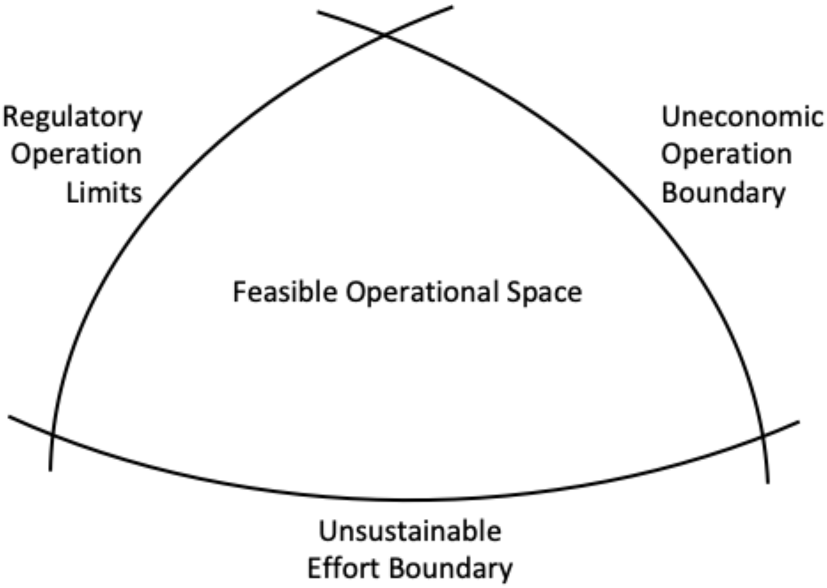


Figure 6.3. Constraints on feasible operational space. Adapted and modified from [1].

6.2 Accidents and failures within the operational failure space model

System failures occur in operational failure space model whenever the operational point intersects with the True Failure Limit. The type, magnitude, and consequences of the resulting accident will depend on the exact system failure and the system dynamics following the system failure. For operationally resilient systems, a system failure may result in return to a safe, non-operational state or even continued safe operation at reduced capacity. For operationally fragile systems, however, the system failure could produce severe, cascading effects. Designing safe systems with inherent hazards require both preventing system failures from occurring and mitigating the consequences of these failures.

Assessing facility, operational, and organization system safety through the operational failure space model requires evaluating conditions when the operational point exceeds any of the operating limits, and evaluating when operating limits violate assumptions regarding margin and relationships between limits.

The conventional concept of system failure relates to operational points exceed limits. Operational points can exceed operating limits in three general ways: operator action, internal dynamics, and external forces. Operator action describes actions that an operator (or operational controller) actively takes to change the system state, condition, or other factor (e.g., controlling a valve). Internal dynamics describes changes that occur within the system absent outside interactions due to internal mechanisms, system interactions, or other self-contained transient behaviors (e.g., release of stored energy). External forces describe any outside actions that affect system states or conditions and are outside the control of the operator or normal operating system (e.g., loss of off-site electrical power). Developing and evaluating controls that prevent or mitigated sudden changes to system conditions is important to ensuring safe design and operation.

System failures related to operator action, internal dynamics, and external forces can be anticipated by design. Designers can provide inherent, engineered, and administrative safety controls that prevent these actions, dynamics, and forces from system limits and moving the system into an unsafe state. The failure of the controls can also be anticipated by design through principles including redundancy, independence, and physical separation of critical safety systems. These methods are extremely effective at preventing known failure modes and meeting the system limits. The more challenging system failures occur, however, when the system operating point satisfies one or more of the system limits with adequate margin but the operational point still result in system failure.

Unexpected system failures occur when the True Failure Limit is less than other system limits and operating point exceeds the True Failure Limit. Table 6.2 summarized the conditions and assumptions that may result in the system limit and operating point exceeding the True Failure Limit.

Review of the conditions and assumptions that may result in system limits exceeding the True Failure Limit reveals two potential causes for unexpected system failures:

- Incorrect or incomplete Understood Failure Limit
- Incorrect or incomplete operator (or operational controller) understanding of system operation and an inappropriately high Operator Comfort Limit

These two causes are strongly related in terms of a fundamental misunderstanding of system states and lead to system failure but differ in terms of their basis in theory (Understood Failure Limit) or practice (Operator Comfort Limit). In both cases, a lack of knowledge regarding system behavior, interactions, conditions, and states results in an unexpected failure at operating points that, by all known accounts, should be safe for operations.

Table 6.2. True Failure Limit Exceedance Conditions

System Limit	*Conditions for System Limit to Exceed True Failure Limit*
Understood Failure Limit	• Understood Failure Limit is based on incorrect or incomplete mechanistic understanding of system theory, characterization of system, understanding of system interactions, or understanding of system condition • Understood Failure Limit does not account for time variation or lag during transients
Regulatory Operating Limit	• Regulatory Operating Limit is based on inadequate Understood Failure Limit • Regulatory Operating Limit allows for certain types of system failures
Operator Comfort Limit	• Operators have incorrect understanding of system interactions, system behavior, system conditions, or limit bases • Operator understanding is based on inadequate Understood Failure Limit • Operator Comfort Limit does not account for time variation or lag during transients
Normal Operation Limit	• Normal Operation Limit is based on inadequate Understood Failure Limit • Normal Operation Limit allows for certain types of system failures

These operating points are particularly hazardous because they may not be accounted for in system design and could be vulnerable to uncontrolled failures. Preventing unexpected and potentially catastrophic system failures requires knowledge, experience, and information on the system interactions, behavior, and conditions to develop Understood Failure and Operator Comfort Limits that better reflect the True Failure Limits. For example, the identification, investigation, and dissemination of precursor events is critical information that, if contextualized and shared, helps better characterize the expected Understood Failure Limit and ensure that it bounds the True Failure Limit.

System failures and accidents are a concern for any system designer and operator, but the need for external constraints and assurance on safety varies by system. For systems and activities that may harm workers, the environment, or the public, additional assurance against system failure and harm may be required. Regulatory frameworks are one manifestation of external forms of assurance against system failure.

6.3 Defining regulatory frameworks to ensure safe commercial operation

Safe, failure-free systems require continuous operation that never exceeds the True Failure Limit. The True Failure Limit is never known *a-priori* so safe, failure-free systems require continued operation that never exceeds the Understood Failure Limit, where the Understood Failure Limit always matches or conservatively bounds the True Failure Limit. Development of this correct or bounding Understood Failure Limit may be challenging due to both the aleatory uncertainty (uncertainty due to random occurrence) and epistemic uncertainties (uncertainty due to random occurrence) of the True Failure Limit.

These uncertainties have two major impacts on the Understood Failure Limit. The first impact is that the Understood Failure limit may be significantly more conservative (e.g., reduced operational limits) than the True Failure space as it must be expanded to exclude any combination of operating points or conditions that are believed (based on theory, analysis, experience, approximation, or even intuition) to cause system failure. This conservatism is intended to produce an Understood Failure Limit that always bounds the True Failure Limit. Second impact is that the True Failure Limit may not be fully bounded by the Understood Failure Limit due to potentially uncharacterized system behavior, interactions, or conditions. This may result in operational failure at operating points below even the most conservative Understood Failure Limits.

Regulating the safety of systems requires providing additional assurances that operating points will not exceed the True Failure Limit and result in an unacceptable system failure. These additional assurances can come in a variety of forms including:

- limits on operation (development of Regulatory Operating Limits for specific activities or operators),
- requirements on physical, operational, and organizational systems that are intended to increase the True Failure Limit or prevent system limits from exceeding the True Failure Limit , and
- requirements on characterization and analysis of systems that are intended to more closely align the Understood Failure Limit with the True Failure Limit, or ensure bounding conservatism of the Understood Failure Limit.

Regulators can seek or provide these assurances through different regulatory frameworks. One way to characterize regulatory frameworks is based on the relationship between the regulator and regulator activity, and the exact regulatory tools used to seek or provide assurance of safe operation.

In this work, five different regulatory frameworks are characterized based on the methods used to provide additional assurance of safety for hazardous systems. The five regulatory frameworks considered are:

- Insurance requirement based regulatory framework
- Permit based regulatory framework
- Delegated review based regulatory framework
- Independent review based regulatory framework
- Operational characterization based regulatory framework

These frameworks are presented and discussed in this Chapter, their potential impacts on design and operation, and their compatibility with different licensing evaluation methods are compared. The licensing evaluation methods are discussed to provide insights on how the regulatory frameworks selected for commercial fusion technology could impact its development and deployment. The insurance requirement based regulatory framework and the operational characterization based regulatory frameworks developed in this section are novel to this work, and are thus presented in additional detail. The remaining frameworks (permit, delegated review, and independent review) are based on existing regulatory agencies and a briefly summarized. Finally, the use of combined regulatory frameworks is presented and discussed for the regulation of organizationally complex activities.

6.4 Insurance requirement based regulatory framework

The first regulatory framework reviewed is an insurance requirement based regulatory framework. This framework minimizes the governmental regulatory burden for both facilities and regulators by shifting major reviews of operation and safety to private insurers with an explicit financial interest in facility safety. A facility must be able to show that it could provide full compensation and remediation for any failures or accidents that could occur at the facility under a strict liability standard. Under the strict liability standard, the owner is responsible for all damages, regardless of fault. Regulated facilities and companies could chose to provide financial assurance for accidents themselves (for either smaller facilities or larger companies) or obtain financial assurances from third party insurance providers or industry groups. This legal and financial liability incentivizes the insurers to require a level of safety commensurate with the probability, consequences, and costs of different facility failures or accidents. The regulatory burden between the facility and the regulator is reduced to an assessment and assurance of compensation required for any activities.

This regulatory framework minimizing the role of government regulators in the development and deployment of a new technology while still incentivizing the adequate protection of the public and environment from harms associated with the technology. The basis for the framework relies upon a principle of harm compensation from tort law that "by awarding any individual monetary damages after their injury, we can make them whole" [10]. Under this principle, it is assumed that financial compensation can be used to provide for compensation and remediation of any harms including injury or death, temporary or permanent displacement, and environmental damage. In short, a monetary value can be appropriately assigned to any damage. This assumption of liability compensation facilitates market regulation of safety.

The principle of liability for harm versus regulation of safety has been addressed by other industries and legal scholars as a method for reducing risk and developing more efficient regulatory systems [11]. Harvard Law School Professor Steven Shavell identifies four factors as critical for evaluating the appropriateness of liability versus regulation for a hazardous activity [11]:

- Difference in knowledge of hazards between facilities and regulators

- Ability of facilities to pay for the full magnitude of harm done
- Challenges of bringing liability lawsuits against a facility
- Administrative costs of the overall framework

Professor Shavell contends that two characteristics (difference in knowledge and administrative costs) favor achieving safety through liability while the remaining two characteristics (ability to provide compensation and challenge of bring liability lawsuits) favor achieving safety through regulation. The main advantages of liability are that it reduces the need for a regulator to have full knowledge of the regulated activity to ensure safety and that significant administrative costs are only incurred if harm from an activity occurs. The main disadvantages of liability are that facilities may be unable (or unwilling) to pay for the full magnitude of harm due to limited assets, resulting in uncompensated harm and that pursuing liability may be challenging for distributed harm or harm that is not easily attributed to the activity. Development of an appropriate liability based framework for commercial fusion requires resolution of these two readily identified weaknesses.

An insurance requirement based regulatory framework is developed and proposed in this section to enable the reductions in regulatory burden associated with a liability based framework while addressing the drawbacks of relying on liability instead of regulation to achieve safety. The insurance requirements based regulatory framework has the following characteristics:

- Standardized, simplified regulator calculation of maximum hypothetical financial compensation and remediation that could be related to facility operation
- Required company financial assurance or third-party insurance that could provide for full financial compensation and remediation
- Regulator audits of financial assurance or third-party insurance to ensure that full compensation or remediation could be paid
- Acceptance of a strict liability standard for any harms resulting from facility operation
- Standardized, simplified method for bringing lawsuits against the facility to receive compensation for harms that does not place undue burden on the public and allows for clear adjudication of claims. Additional standardization or guidance on compensation amounts provides for a more transparent and equitable regulatory framework.
- Standardized method for collecting public judgment against common harms (e.g., environmental damage) that adequately reflects the socio-economic impacts of long term harm and dissuades continued damage

In exchange for these requirements on a facility, the operator would be permitted to operate without any additional regulations. Safety would be achieved through the financial incentives on companies to operate in a manner that minimizes harm due to the clear and assured financial penalties associated with failure. The relationship between the insurer and the facility also contributes to safety by providing a financial incentive for safe design and operation (lower insurance/risk premiums) and the potential for contractual requirements on design or operation ensure the validity of financial risk models used as the basis for the facility insurance. Each of the insurance requirements based regulatory framework characteristics are briefly described in the remainder of this section.

6.4.1 Standardized, simplified compensation formula

The first characteristic of the insurance requirements based regulatory framework is a standardized and simplified method for calculating the financial compensation and remediation costs associated with a maximum hypothetical accident. This calculation is designed to be a high confidence, upper bound on the maximum hypothetical accident that could occur at a facility. The goal of the calculation is to produce an accident cost estimate that would not be exceeded in any accident and ensure that financial assurances from the facility (required within the framework) would always be adequate. A simplified, standardized calculation method is desirable because it would minimize the regulatory burden associated with the regulatory process and enable uniform treatment of facilities and the public, regardless of technical expertise.

There could be a natural push by industry to request use more detailed calculation methods or consequence cost assessments to reduce the insurance requirement. These requests should be rebutted as they shift assessment burden back towards the regulator from the private industry. Instead, facilities should work within private markets to demonstrate that their cost assessments are more accurate and that the overhead differences is largely due to the excessive conservatisms in the regulator calculations. If private companies successfully make this case, they will receive market appropriate insurance rates that reflect the expected risk of the technology. If private companies do not successfully make the case, then the market rates would better reflect the understood risk of the technology and the insurance requirements ensure public compensation for any accidents.

A calculation method for the financial compensation and remediation costs is not developed in this work but would be necessary for an insurance requirement based regulatory framework. The following factors would need to be quantified as a function of facility characteristics and developed into a cost function based on the compensation or remediation costs:

- Population health impacts and fatalities
- Population evacuation or relocation
- Temporary or permanent loss of property
- Property devaluation or loss of function
- Economic impacts (e.g., lost of industry)
- Environmental damage

A radiological inventory-based insurance requirement calculation may be useful at linking the major off-site hazard of commercial fusion facilities with the maximum hypothetical accident costs. This method would need to be openly developed, reviewed, and discussed to ensure that it appropriately bounds potential accident compensation and remediation costs. This portion of the regulatory framework development process would be the most resource intensive as the regulator seeks reasonable consensus on a highly uncertain calculation.

Mandatory financial protection requirements for lower power commercial fissions reactors are an example of a highly simplified regulatory calculation based on facility hazard. Commercial fission reactors with a power level of greater than 10 megawatts thermal power and less than 100 megawatts electric power are subject to scaling insurance requirements that are a function of their thermal power and the surrounding population [12]. The financial protection is calculated:

$$I = \$185 \cdot P_{kW} \cdot PF$$

where I is the total financial protection required, P_{kW} is the thermal power of the reactor in kilowatts, and PF is the population factor around the facility. The population factor varies as a function between 1 and 2 depending on the weighted total population living with a specific distance of the facility. The specific distance is calculated:

$$r = \sqrt{P_{MW}}$$

where r is the radius around the plant in miles and P_{MW} is the thermal power of the reactor in megawatts. A population weighted method is used to determine the appropriate PF for the facility [12]. This method roughly quantifies the potential hazards associated with an off-site nuclear release from a reactor and includes scaling based on the population and siting. The regulator also assumes up to $500 million of indemnification liability for these nuclear sites in addition to their primary financial assurance [13]. The public assurance of indemnity contributes to the need for regulatory requirements on these facilities outside of the private insurance requirements.

6.4.2 Required financial assurance of compensation

The second characteristic of the insurance requirements based regulatory framework is required company financial assurances or third-party insurance that could provide for full financial compensation and remediation of the maximum hypothetical accident. One of the two major identified challenges of the liability-based approach to safety is a lack of assurance that a company will be able to provide compensation for a major accident. Bankruptcy of companies or use of limited liability subsidiaries may limit the ability of plaintiffs to receive full compensation following a major accident. The potential for bankruptcy effectively limits the total market risk of a major accident to the asset valuation of the company that may be less than the total potential compensation for an accident.

In this framework, one major requirement is a continuous guarantee by a company that it has adequate financial assets or third party insurance to provide for a maximum hypothetical accident. The total value of required financial compensation assured would be equal to (or greater than) the financial compensation and remediation costs associated with a maximum hypothetical accident as calculated by the regulator. This assurance would ensure that financial assets are available to fully compensate all harmed parties following the maximum hypothetical accident. It may be highly unlikely that such an accident (or any accident) would ever occur, but this assurance is needed to ensure that companies burden the true market costs associated with the operation and ownership of potentially hazardous facilities.

One important part of this characteristic is that facilities would work with investors or third-party insurers to determine acceptable levels of risk for a facility, and balance these risks with appropriate insurance premiums. This structure directly ties facility design, operation, and potential for catastrophic risk to financial incentives that felt on a going-basis by facilities. While the regulator only requires simplified evaluations to determine the financial compensation and remediation costs associated with a maximum hypothetical accident, facilities would be able to work with inventors or third-party insurers to develop more detailed analysis that they believe more accurately model the actual risk of the facility. If the detail and quality of these evaluations result in a significantly lower risk, it is reasonable that market rates on the insurance would more closely reflect the actual risk of the facility. This process allows for private adjudication of design, operation, and safety without government bureaucracy while still ensuring full financial compensation for all possible accidents.

The required financial assurance for accidents for commercial fission facilities is an example of methods to provide compensation after accidents. The Price Anderson Act requires financial assurance for commercial fission facilities through a combination of individual operator insurance, pooled industry insurance, and government indemnity [13]. The goal of the Price Anderson Act was to facilitate private insurance for nuclear operators by capping catastrophic losses while still ensuring that members of the public would receive compensation for nuclear accidents at facilities regulated by the federal government [13].

Operators first are required to obtain $450 million of first tier insurance against nuclear accidents. The operators then pool their insurance liabilities together in a second tier insurance ($131 million per plant) that covers any accidental releases at any U.S. nuclear power plant. This provides a total industry liability of approximately $12.9 billion against any nuclear accidents. If a total accident cost exceeds $12.9 billion, the reactors operators would be liable for another $6.5 million per plant or a total final assurance of $620 million total. If the total costs of a nuclear accident exceed the total insurance pool of approximately $13.4 billion, the Price Anderson Act provides indemnification against all other liabilities and the federal government would have responsibility for addressing all other costs [14]. This three-tiered system broadens the financial liability to help provide assurance of compensation for accidents at commercial fission facilities but still provides indemnity in the case of catastrophic accidents.

The Price Anderson Act and the financial assurance model described above are applicable to all nuclear utilization facilities regulated under the Atomic Energy Act (AEA). If commercial fusion facilities were regulated by the NRC as utilization facilities under the AEA, they would be statutorily required to comply with the financial assurance requirements of Price Anderson Act [15]. It is currently unclear if commercial fusion facilities would be regulated as utilization facilities and subject to these requirements but the pooled industry insurance model could result in commercial fusion facilities holding liability of commercial fission facility operation [15].

6.4.3 Routine audits required financial assurance of compensation

The third characteristic of the insurance requirements based regulatory framework is routine regulator audits of company financial assurances or third-party insurance to ensure full financial compensation and remediation of the maximum hypothetical accident. This step is intended as an additional guarantee that full financial compensation is available for any accidents. A similar financial assurance process is already conducted by the NRC for nuclear material licensees to ensure that adequate assets are available for the decommissioning of sites handling nuclear materials [16]. Routine audits provide the additional assurance that changes in markets, company structure, or facility operations have not invalidated the key regulatory framework assumption that full compensation must be paid after any accident to ensure correct market self-regulation of safety using liability.

6.4.4 Acceptance of strict liability standard

The fourth characteristic of the insurance requirements based regulatory framework is acceptance of a standard of strict liability. As previously discussed, the principle of strict liability holds facilities responsible for any harms resulting from activities, regardless of fault or criminal activity. This requires the facility (and its financial backers) to base their design and operation on assumption that they will be responsible for any and all harms. This may place higher financial incentive on designs that reduce the maximum hypothetical accident consequences rather than reliance of engineered safety features that may fault without fault or negligence.

The principle of strict liability can be traced through common law, but is specifically relevant to novel industrial facilities based on a definition of “abnormally dangerous activities” [17]:

> § 20 Abnormally Dangerous Activities
>
> (a) An actor who carries on an abnormally dangerous activity is subject to strict liability for physical harm resulting from the activity.
> (b) An activity is abnormally dangerous if:
>
> > (1) the activity creates a foreseeable and highly significant risk of physical harm even when reasonable care is exercised by all actors; and
> > (2) the activity is not one of common usage.

In this way, a novel industrial facility with the potential for significant off-site hazards is, unless proven otherwise, could be engaging in an abnormally dangerous activity. Acceptance of the standard of strict liability by facilities in exchange for no governmental oversight on design or operations acknowledges the trade of public acceptance of assuring reasonable care for acceptance of all harms resulting from activities. This process characteristic also again helps incentivize private quantification and management of hazards and risk due to the wide scope of the liability imposed on the facility.

6.4.5 Standardized, simplified method to compensate harms

The fifth characteristic of the insurance requirements based regulatory framework is a standardized, simplified method for bringing lawsuits against the facility to receive compensation for harms. The second of the two major identified challenges of the liability based approach to safety is the challenge of bringing suit for distributed harm or harm that is not easily attributed to the activity. The challenges associated with bringing suit (e.g., costs, risks, knowledge gap, unfamiliar processes) may dissuade those who have suffered harm from associated with the activity from receiving due compensation. Development and implementation of a standardized compensation process helps ensure that the liability approach to safety properly incentivizes private companies to prioritize safe operations.

The use of a standardized, simplified method for bringing lawsuits against the facility to receive compensation for harms has advantages for both the facility and the public. First, a standardized process could allow for a more predicable adjudication and demonstration of harm, burden of proof for evidence, and clear processes for compensation. These steps add predictability to the process and could be used to reduce the risk of frivolous lawsuits. Additional standardization or guidance on compensation amounts within the compensation system provides for a more transparent and equitable regulatory framework and help ensure that compensation is in line with expected guidelines. This predictability helps prevent biases in compensation or compensation based on the plaintiff's ability to obtain higher quality representation. These processes would need to be developed and clarified as part of development of the insurance requirements based regulatory framework.

6.4.6 Standardized method to compensate public damage

The sixth and final characteristic of the insurance requirements based regulatory framework is development of a standardized method for collecting public judgment against common harms (e.g., environmental damage) that adequately reflects the socio-economic impacts of long term harm and dissuades continued damage. A liability-based approach to regulation relies on financial costs or benefits to incentivize societally desirable behavior. This final characteristic is intended to provide an avenue for compensating the public for harms that cannot be directly attributed to one plaintiff but are understood to damage shared resources (e.g., public lands, air, or water).

Standardized method to compensate public damage ensures that there are private market forces to incentivize safety. Lawsuits brought by the regulator on behalf of the public or standardized fines for damages are two different methods that could be used to ensure public compensation. Effective use of these fines or lawsuits require two conditions: sufficiently large fines or suit judgments to properly compensate for damage and effectively act as a deterrent, and use of collected financial compensation for remediation.

If the compensation collected is insufficient to either provide for full compensation or effectively deter harm, the cost of environmental damage risks become a “cost of doing business”. Development of standardized method to calculate and impose costs of environmental damage on facilities helps ensure that appropriate costs are borne by facilities without the risk of loopholes or extended litigation that results in settlement with minimal fines to ensure some judgment.

Additionally, collection of any compensation should be performed so that collection is available only for remediation efforts. The focus of this regulatory framework is to make harmed parties whole through compensation, so diversion of funds to other purposes (e.g., other programs or the U.S. Treasury) violates the assumption that the harm will mitigated through compensation. Punitive judgment could still be pursued through existing regulation for cases of negligence or criminal behavior but the focus of the insurance requirements based regulatory framework remains on ensuring safety through liability requirements. This final characteristic helps ensure that dispersed harms are still included in the regulatory process.

6.4.7 Precedent for an insurance requirement based regulatory framework

An insurance requirement based regulatory framework is not explicitly in use by any major industries. The challenges of a liability based regulatory framework identified by Professor Shavell (ability to provide compensation and challenge of bring liability lawsuits) have limited the applicability of the liability regulatory framework in the past [11]. The behavior of industries before the imposition of major regulatory activities highlights the limitations of a liability regulatory framework if compensation and liability challenges are not addressed. Toxic chemical pollution and worker safety in the United States were not adequately controlled using civil liability processes and contributed to the introduction of several major regulatory frameworks in 1970 including the Occupational Health and Safety Act (establishing OSHA), the National Environmental Protection Act, the Clean Water Act, and executive orders establishing the Environmental Protection Agency. These acts identified that an unregulated liability framework was not resulting in societally acceptable control of hazards.

The limits of an unregulated liability framework are demonstrated by major events that both occurred (inadequate incentive to prevent loss) and were not fully cleaned up (inadequate controls to ensure compensation). Improper disposal of hazardous industrial wastes contributed to the severe environmental contamination of thousands of sites around the United States up through the 1970s. Several major industrial events, including public exposure to toxic materials at the Love Canal neighborhood in Niagara Falls, New York, pushed policy makers to identify better methods to control toxic wastes [18]. A combination of burden of proof related to harms from toxic materials, the inability to identify specific polluters, and the inability for companies to compensate for harm all resulted in situations where toxic material could not be forcibly cleaned up based on existing law [18]. The 1980 Comprehensive Environmental Response, Compensation and Liability Act established new legal requirements and a common liability fund to facilitate the clean up of sites that otherwise could not be tied to a specific polluter [18]. The public was ultimately responsible for many of these “superfund” sites due to the failure of the unregulated liability framework to incentivize appropriate operation, mitigate remaining hazards, and compensate for the harms done. The history of the Superfund program and major industrial incidents that preceded regulation help highlight the weaknesses of an unregulated liability framework. This work seeks to remedy the limitations of the liability regulatory framework with the additional framework specifications present in the insurance requirement based regulatory framework.

The political and social feasibility of implementing insurance requirement based regulatory framework for is unclear due to the lack of regulatory precedent for this framework. The framework may face some challenges due to prior failures of private industry self-regulation of hazardous activities. While the insurance requirement based regulatory framework proposed in this work attempts to overcome historical challenges through specific requirements ensuring accountability for hazard consequences, this framework is novel and untested. The movement of government responsibility for safety to private companies is politically controversial, so the use of this framework may be challenging to implement in the countries such as the United States where there is significant political gridlock. More detailed evaluation of the political viability of an insurance requirement based regulatory framework in different countries may been need to support further development activities.

6.4.8 Summary framework and compatibility with licensing evaluation methods

The insurance requirement based regulatory framework minimizes regulatory burden for commercial fusion facilities by shifting the assessment of facility safety and risk to private companies and third-party private insurers. The regulatory assessment required for this framework is an evaluation of the maximum hypothetical accident costs that bound the compensation and remediation costs associated with any facility accident. Requirements on facility financial assurances, routine audits, strict liability, and standardized methods for receiving compensation associated with facility harm help to ensure that the framework addresses the challenges associated with liability based approaches to safety.

This framework represents a controlled free market approach to safety – facilities may decide on the appropriate level of safety based on cost-benefit analyses but are subject to liability requirements that force them to market-based decisions regarding design and operations to obtain adequate financial assurance. Facilities that operate without accidents may benefit from this framework if they can convince markets that their facilities are as safe as claimed. If facilities have accidents (even without fault), they will be forced to pay for full compensation and remediation without the normal legal avenues used to reduce the financial consequences associated with accidents. If facilities are unable to convince private insurers of the risk of their facilities, their market rates for insurance will reflect the potential risk – either forcing changes to facility design and operations to increase safety, changes to analysis to reduce the perceived risks, or render the technology uneconomical via the imposed private costs. This framework ultimately tests the commercial viability of fusion technology in a free market of risk and insurance.

There may be regulatory costs associated with the set up an insurance requirement based regulatory framework (i.e., development of the insurance cost requirement calculations, development of harm compensation processes) and minor on going costs (i.e., regulator audits of financial assurance). The long-term regulator costs would likely be small if the regulatory system is used by a sufficient number of facilities. Larger regulatory related costs would be borne by facilities and any third party insurance companies.

The insurance requirement based regulatory framework is compatible with all of the licensing evaluation methods described in Chapter 8, but the direct applicability is split between the regulator evaluations and insurance evaluations performed by third parties. This framework uses a worst-case release evaluation in the development of the bounding compensation and remediation costs. That licensing evaluation method would be essential at developing a conservative estimation of costs that could be used ensure adequate financial assurance. The remaining licensing evaluation methods would not be used by the regulator but could be used by the facility to evaluate facility safety and provide more accurate quantifications of safety for the development of market appropriate insurance costs. The level of detail utilized by facility would likely vary on a facility-by-facility basis, as the specific hazard characteristics of a facility are evaluated and a balance between evaluation burden, design burden, and perceived risk is sought by both the facility and the third party insurer.

Reduction of inherent facility hazards are likely the favorable approach for achieving safety in an insurance requirement based regulatory framework due to the simultaneous reduction of the insurance requirements calculated by the regulator and the reduction of predicted harm using all other licensing evaluation methods. Further development or refinement of licensing evaluation methods would likely vary based on specific designs and the preferences expressed by different third party insurers in developing technical assurances on the actual safety risks associated with commercial fusion facilities.

6.4.9 Impacts of regulatory framework on commercial fusion regulation

The insurance requirement based regulatory framework represents a free market approach to the development of commercial fusion technology. Previous attempts to utilize a free market approach to ensure facility safety have failed, in part, due to structural weaknesses that allowed facilities to avoid the full externality costs associated with their technology. The requirements outlined in this framework would help ensure accountability for commercial facilities and provide appropriate market signals to incentivize safe facility siting, design, operation, and decommissioning. There are two main impacts of this regulatory framework on the development of commercial fusion facilities: the costs associated with obtaining the required liability insurance and the design, analysis, operation, and siting requirements imposed by external insurers or for asset risk management.

This approach to commercial fusion regulation reduces government intervention in the development of fusion technology and evaluation of fusion technology safety but requires commercial fusion developers to address the risks associated with catastrophic accidents through private insurance markets. Unlike the commercial fission industry, with to limited liability via the Price Anderson Act, the commercial fusion industry would be required to address the full costs associated with catastrophic accidents. This leads to an, as of yet, uncharacterized problem: assessment of actuarial risk associated with a commercial fusion power and the resulting risk premiums associated with insuring the maximum hypothetical accident.

Estimating the financial costs associated with a maximum hypothetical accident for commercial fusion requires identification of the accident scenario, assessment of the physical consequences of an accident, and conversion of physical consequences to monetary consequences. The discussion of fusion hazards in Chapter 6 and maximum credible release licensing evaluation discussions in Chapter 8 provide some in insights into the identification of the maximum hypothetical accident scenario. Specifically, catastrophic acute release of radionuclides (mobilized neutron activated materials and tritium contaminated materials) has been identified by prior studies as scenarios of regulatory interest for fusion facilities. The bounding physical consequences of this scenario (radiological exposure and contamination) and the resulting monetary consequences (incorporating exposure, contamination, and remediation costs) would need to be characterized to identify the bounding costs associated with an accident. Earlier discussion in this section highlighted the challenges associated with assessing financial costs for physical consequences. These challenges would need to be resolved as part of the development of this framework for commercial fusion facilities. A bounding calculation would be required within the regulatory framework as the basis for financial assurance.

Commercial fusion facility and private insurers would repeat this process of estimating financial costs of accidents (and estimations of the probability of accidents) for a larger set of scenarios to help characterize the risk (probability and consequence) profile of a commercial fusion facility. This risk would be used to help assess the insurance premiums associated with the financial assurance required by the regulator as well as the insurance premiums associated with risk significance as characterized by the insurer. This process would result in an economic cost for a commercial fusion facility that correlates with the free market risk of commercial fusion. This cost would have to be borne by fusion technology in a commercial energy market place as part of its generation costs.

A hypothetical scoping calculation shows the impact of the calculation of insurance premiums on costs and revenue for a commercial fusion facility. The following assumptions are made for a 200 MW$_e$ commercial fusion facility:

- P_e: Net power generation of 200 MW_e
- CF: Average capacity factor of 90%
- T_y: Generation period of 8760 hours/year
- C_e: Average wholesale electric cost of $\$30/MW_eh$ [19]
- C_p: Plant capital cost of \$2 billion (based on $\$10{,}000/kW_e$ capital cost) [20]
- I_p: Percent of capital cost paid in annual premium of 1% [21]

The fraction of plant revenue paid in insurance premiums (F_i) can be calculated using the following ratio of the cost of insurance (C_i) divided by the annual plant revenue (R_p):

$$F_i = \frac{C_i}{R_p} = \frac{C_a \cdot I_p}{P_e \cdot CF \cdot T_y \cdot C_e} = \frac{\$20{,}000{,}000}{\$47{,}304{,}000} = 42.3\%$$

The resulting values for this calculation ($20 million per year in insurance premiums and 42.3% of total plant revenue) would likely have significant effects on the market viability of commercial fusion. Several arbitrary inputs were used to facilitate calculation of the insurance costs:

- wholesale electricity price ($\$30/MW_e h$) was selected based on rough average of 2020 U.S. electricity prices,
- plant capital cost ($2 billion based on $\$10{,}000/kW_e$ capital cost) was selected based on comparison of energy cost projections for commercial fission ($\$6{,}000/kW_e$) [20] and a comparable commercial fusion facility based on major component costs (total estimate $5-6 billion) [22]
- annual insurance premium percentage (1% of total capital costs) were selected based on the upper range standard estimates for annual insurance costs at industrial chemical facilities and the uncertainty related to commercial fusion facility safety and operation [21]

More realistic calculation of both of the bounding accident cost and the insurance premium percentage are much more complex and far outside the scope of this work. Depending on the facility and insurer, the facility specific premiums may not be based on total facility cost but based on maximum hypothetical accident costs and calculated probability of accidents.

While these insurance premium values are completely hypothetical, they highlight the importance of two factors – reducing the costs associated with the maximum hypothetical accident and reducing the likelihood of the maximum hypothetical accident (and other financial risk significant scenarios) to reduce the insurance risk (and resulting insurance premium percent) associated with a commercial fusion facility. Additional insurance considerations may be included related to mitigation, remediation, or compensation for chronic releases of radiological material such as tritium in the form of liquid water or water vapor.

The importance of these two factors (reducing potential consequences and reducing scenario probability) directly tie into impacts of this regulatory framework on the design, analysis, operation, and siting requirements for commercial fusion facilities. Reducing potential consequences associated with a commercial fusion are key to both reducing both the mandatory insurance requirement and the realistic accident scenarios considered by private insurers. Reducing the mandatory insurance requirement requires reductions to the maximum hypothetical accident consequences. The discussion in Chapter 8 on the maximum credible release licensing evaluation provides detailed discussion on evaluating accident consequences, but the consequences associated with this event for mandatory insurance requirements are primarily based on the inherent hazards of a facility. As a result, there is an incentive to minimize hazardous inventories (i.e., mobilized neutron activated materials and tritium contaminated materials) in design and provide remote siting for facilities to minimize off-site exposure. These factors would reduce the consequences and mandatory insurance requirements associated with releases but require trading engineering margin, less favorable siting, and operational considerations for reduced regulatory and insurance costs.

Reduction of effective hazards of a facility through design or reduction of event probability would not affect the mandatory insurance requirements but could impact the insurance premiums associated with this regulatory framework. Commercial fusion facilities could utilize any design and operational methods (inherent hazard reduction, effective hazard reduction, event prevention or mitigation by design) to reduce both the expected consequences and probabilities of accidents at commercial fusion power plants. Insurance companies may credit this reduction in the expected risk when evaluating the financial risk associated with a facility and developing actuarial models for insurance premiums.

It is important to note that developing these risk evaluations and actuarial models may require extremely specialized knowledge. The availability of insurers willing to perform these evaluations and offer insurance will depend, in part, on the perceived economic stability of the insurance product offered. The complexity and challenges associated with commercial fission facility insurance have resulted in only two major nuclear insurance companies (American Nuclear Insurers and Nuclear Electric Insurance Limited). The market conditions and insurance requirements for commercial fusion insurance would likely impact the availability of insurance companies willing to developing these risk evaluations and actuarial models for commercial fusion facilities.

The balance of expected risk and facility design, operation, and siting would likely become a key negotiation between commercial fusion companies and insurance companies. If commercial fusion companies can successfully demonstrate by design, testing, and analysis that the facilities do not represent a significant financial risk despite the mandatory insurance requirements, their free market insurance rates should reflect the actual risk externality without requirements on designs. If, however, commercial fusion companies cannot convince private insurance companies of fusion safety, they will need to work to establish facility parameters that meet the risk tolerance of insurers. These negotiations would occur outside of the regulatory space and allow private assessment and handling of risk, enabling free market development of novel and innovative technologies.

The insurance requirement based regulatory framework would enable the development of commercial fusion technology with minimal government oversight related to safety. Commercial fusion companies would, however, have to work with private firms to fully insure against maximum hypothetical releases. If commercial fusion companies could successfully utilize design, operation, siting, and analysis arguments to demonstrate sufficiently low facility risk for private insurance companies, they would be able to operate without overly burdensome external requirements. Private insurance companies may, however, impose requirements on commercial fusion companies to control their maximum and expected risks. This process would be conducted on a case-by-case basis and could represent a minor or significant impediment to commercial fusion depending on the specific facility. The formal regulatory and impediments with this regulatory framework are minimal but releases could be extremely costly due to the liability requirements on commercial fusion companies. The insurance requirement based regulatory framework is a wager on the free market viability of commercial fusion technology – a convincing safety case and safe operations results in the lowest possible regulatory costs and requirements but uncertainty in the safety case and any accidental releases could be extremely costly for the commercial fusion industry.

6.5 Permit based regulatory framework

The second regulatory framework reviewed is a permit based regulatory framework. This framework emphasizes the use of specific permits that limit facility or operational characteristics to acceptable levels, limiting acute and chronic harm to workers, the public, and the environment. A permit regulatory system reduces the regulatory burden associated with the licensing process, focusing on measurable high-level facility or operational characteristics instead of detailed evaluation of design and performance. The regulator seeks to define a Regulatory Operating Limit that minimizes the consequences of unexpected failures while providing the facility latitude in design and operation. For hazards where normal performance based requirements are not achievable using available technology or hazard should be minimized based an absence of a harm threshold, prescriptive requirements on implementation of equipment or design features (e.g., best available technology) may be utilized as part of the permit process.

This main purpose of this regulatory framework is to reduce the regulatory burden associated with activities by using simplified licensing evaluation techniques and requirements to ensure safe operation. This framework has high initial regulatory burden for regulators, as they are required to assess the adequacy of Understood Failure Limits, develop appropriate Regulatory Operating Limit that meet societally acceptable limits for harm from an activity, and create appropriate evaluation criteria to assess whether a facility is in compliance with Regulatory Operating Limits and meeting social goals.

The permit based regulatory framework is based on the regulatory practices used by many environmental regulators [23]. For activities with the high risk of inequitable harm, use of specific permits for a facility or activity can be useful for tailoring regulatory requirements and ensuring compliance [24]. Hazard permits can be categorized based on whether they cover chronic or acute hazards. For chronic hazards, permits may cover the maximum quantity, rate, or concentration permissible for releases or exposure. For acute hazards, permits may cover the same types of limiting permissible releases characterized for chronic hazards or may place permit requirements related to the hazard inventory in a process or facility. The specific permits can be varied for different facilities and different hazards to ensure compliance and protect workers, public, and the environment.

A permit based regulatory framework is reviewed in this section for its applicability to commercial fusion facilities. This framework defines Regulatory Operating Limits based on a general Understood Failure Limit but does not make further specifications to facility specific Understood Failure Limits or Normal Operating Limits except in cases where a prescribed technology or activity is required to meet Regulatory Operating Limit. The permit based regulatory framework consists of four major parts:

- Definition of Regulatory Operating Limit
- Application for permits
- Compliance with permits
- Enforcing permit conditions

These framework parts create a general, scalable regulatory framework that can tailor the regulatory burden to specific hazards depending on the activity, hazards, and consequences. Regulators such as the Environmental Protection Agency for the control of general environmental hazards have demonstrated the potential for using a permit based regulatory framework.

6.5.1 Definition of hazard limits

The first major part of a permit based regulatory framework is definition of Regulatory Operating Limit. The process for defining these Regulatory Operating Limit is similar to the processes described in Chapter 7 for the definition of different hierarchical hazard limits. The definition of Regulatory Operating Limit includes consideration of what hazards should be permitted and assessment of acceptable levels of release, exposure, or consequence.

The process of identifying hazards for regulation is a scientific, social, and political problem. Some hazards may be regulated before demonstrated harm based on concern for harm (e.g., genetically modified foods) while other hazards may not be regulated until after sufficient harm has occurred (e.g., DDT). Regulation of hazards is a social process that requires sufficient evidence and interest from stakeholder groups to create a sufficient consensus among regulators and legislators that action to control the hazard is required. The social processes for identifying hazards in regulatory systems, while critical to permit based regulatory frameworks are outside the scope of this work and not discussed in further detail.

Once a hazard is identified for regulation, regulators must address a similar multi-stakeholder problem for the definition of the Regulatory Operating Limit. Hazard limits may be defined based on a threshold of detectable harm, acute on-set of harm, chronic on-set of harm, individual risk, collective risk, or many other factors. Correlation of direct and indirect hazard consequences with more directly measurable hazard limits would be performed similar to the discussions in Chapter 7.

One particular challenge to developing these Regulatory Operating Limits is the technical, social, and economic factors important to a variety of stakeholders that must be considered when creating a hazard limit. Balancing harm, risk, and technical-economic realities of hazard control may require a deliberative process. Creation of hazard limits that are not economically achievable results in effective prohibition of an activity and not a functional control on releases. While this may be acceptable for some stakeholders and hazards, use of hazard limits to effectively prohibit an activity is not the most effective method for hazard control. For these hazards, particularly those where there is no safe threshold for exposure or minimizing releases are a driving objective, use of a prescriptive standard (i.e., what method to use) instead of a performance standard (i.e., what limit to meet) may be useful for permitting limits. For example, use of best available technology is required by the EPA for the controlling some toxic effluents from point sources [25]. Use of the best available technology (or other metrics such as "best available technology economically achievable") will help ensure that limits evolve over time with improved technology and provided incentives for the development of new control technology.

The definition of Regulatory Operating Limits is a significant regulatory burden within the regulatory framework. An open collaborative process of hazard limit development with conflicting stakeholders will, inevitably, lead to varying levels of satisfaction on the final limits. Longer, consensus based limit development processes may improve both the science and policy around final limits, but litigation on these hazard limits is possible when economic or public health concerns are at stake. Legal questions on regulatory authority as well as the validity of the underlying regulatory analysis and data may become subject to litigation. The implementation of the 2014 Clean Power Plan by the EPA highlights the political challenges that may arise from these limits [26]. While the process has significant up-front regulatory burden, the initial development of Regulatory Operating Limit can help set the stage for subsequent permit actions.

6.5.2 Application for permits

The second major part of a permit based regulatory framework is developing an application process for permits. The goal of a permit application is to provide regulators with the information necessary to regulate an activity and ensure that the activity is meeting the applicable regulatory limits. Prior work on permitting systems provides more detailed discussion on the purposes of permits [24] and the distinctions between different types of permits.

An application for a permit in a permit based regulatory framework provides general information to the regulator on the proposed activity, what hazards are relevant for regulation and what hazards are exempted due to limited inventory or other rules, and what hazard limits are applicable for the activity. In some cases, an applicant may provide limited information on methods or equipment that will be used to ensure compliance with hazard limits (e.g., presence of emissions control features). The permit application will also generally provide information on how the facility will demonstrate compliance with the hazard limit conditions in the permit.

It is important to note that a permit application will not contain detailed engineering analyses or calculations. The goal of the permit based regulatory framework is to outline the conditions required to allow safe operation. For chronic hazard consequences, controlling long-term trends in plant operation is normally sufficient to ensure public safety and basic calculations regarding plant specific operation may be used to justify certain operational parameters (e.g., emissions based on fuel). For acute hazard consequences, however, ensuring compliance with hazard limits may be challenging due to the assumptions made in release or accident analyses. In these cases, regulators may allow applicants to choose to either use conservative assumptions in a standardized methodology or perform their own simplified analyses using site-specific assumption. This would be similar to the licensing evaluation methods of worst-case release analysis or a maximum credible release analysis depending on the specific Regulatory Operating Limit.

Overall, the regulatory burden associated with the permitting process should be limited. The main goal is to document the proposed activity and relevant regulatory limits. The permit application is not an analytic justification of facility Normal Operating Limit or Understood Failure Limit but a documentation of planned compliance with the Regulator Operating Limit. The regulatory burden is minimized, complimenting the significant regulatory burden associated with the development of Regulatory Operating Limit.

6.5.3 Compliance with permits

The third major part of the permit based regulatory framework is ensuring compliance with permit conditions. Regulatory Operating Limits are only an effective means of ensuring safe operating points if compliance with limits is verified. This compliance assurance may be conducted through a number of factors including documentation of plant operation conditions, periodic sampling of plant emissions, continuous sampling of plant emissions, real time monitoring of plant emissions, or site inspections. The available technical and operational methods to achieve assurance compliance depend significantly on technology and facility.

The appropriate compliance assurance methods vary depending on the specific hazard, the nature of the hazard consequences (minor vs. severe, chronic vs. acute), and the techno-economic considerations related to enforcing compliance. Violation of some hazard limits may present a clear, present danger to acute health and welfare while violation of other hazard limits may simply indicate a need to correct long-term operating conditions to prevent chronic hazard consequences. The impact of a hazard limit violation and the time sensitive nature of returning to compliance is an important consideration in the development of a permit based regulatory framework.

An additional challenge in assuring compliance with permit hazard limits is determining the independence of the compliance assurance. Two bounding conditions on assuring compliance are self-assurance and independent-assurance. In self-assurance, the facility verifies to the regulator that they are meeting the hazard limits associated with their permit based on their own assessment of conditions, emissions, and regulatory limits. While this method has no regulatory burden, the facility may not be directly incentivized to self report permit violations. A self-regulating facility, while ideal, may conflict with the economic incentives associated with operating costs and avoiding regulatory penalties. In independent-assurance, a regulator or other independent organization verifies to the regulator that the facility is meeting the hazard limits associated with their permit. This assessment requires independent measurement of plant conditions or audits of facility provided measures to ensure compliance. This method removes the potential under reporting of limit violations but has a significantly higher regulatory burden associated with monitoring and auditing of facilities. These regulatory burdens would need to be borne by either the facility through fees or taxes, or by the public through taxpayer funded regulators. Additional regulatory burdens through interface requirements would also likely occur. The appropriate balance between self-regulated and independent-regulated compliance enforcement would depend on the hazards, technology, and compliance assessment methods.

Overall, the regulatory burden associated with the compliance monitoring process can vary significantly depending on the compliance method and type of compliance verification. Compliance assurance is the verification that actual operating points meet the Regulator Operating Limit. The type of hazard consequence (acute vs. chronic) has significant impacts on the appropriate compliance method and type of assurance compliance. The regulatory burden may vary based on the hazard and allow for tailoring to a specific hazard and facility.

6.5.4 Enforcing permit conditions

The fourth and final major part of the permit based regulatory framework is enforcing permit conditions. The permit outlines the Regulator Operating Limits that must be complied for safe operation. Operational deviations that exceed the Regulator Operating Limits can occur during operations without resulting in hazard consequences so enforcement of the Regulator Operating Limits is needed to ensure that facilities maintain safe operation and the expected operational envelope. Incentives and penalties for compliance (or violations of) Regulator Operating Limits can help ensure proper operation.

The power of permit enforcement depends on the legal framework used to implement the regulatory framework. Enforcement consists of determining compliance and determining follow-up actions to bring the facility into compliance or punish violations of Regulator Operating Limits. Punitive methods for enforcing permit conditions could include:

- Loss of operating permits
- Restriction on operating permit conditions
- Additional requirements on facility operations
- Additional compliance requirements or audits
- Financial penalties against a facility
- Financial penalties against operators, management
- Criminal penalties against operators, management

Incentive methods (e.g., reduced regulatory fees for sustained compliance) could also be used to enforcement conditions. The selection of the appropriate methods for enforcing permit conditions is extremely challenging and would depend on the regulator, industry, and any legislation. Considerations such as operator or management negligence or repeated violations could be factored into the enforcement process.

It is important for framework designers to remember that the ultimate goal of permit enforcement is safe operation through compliance with Regulator Operating Limits and not simply punitive retribution for violations of Regulator Operating Limits. Enforcement methods should incentivize compliance with both acute and chronic Regulator Operating Limits and produce safe operating conditions.

Overall, the regulatory burden associated with the permit enforcement would vary based on the enforcement method selected. The ability of facilities to challenge or litigate regulator enforcement actions may complicate the implicit (or event explicit) cost-benefit analysis conducted by facilities when determining appropriate compliance with regulatory permits. A permit based regulatory framework that does not assure compliance with and enforce Regulator Operating Limits may not result in safe facility operation, limiting the effectiveness of the regulator.

6.5.5 Precedent for an permit based regulatory framework

The permit based regulatory frameworks have significant regulatory precedent and are the primary regulatory framework for many activities. A permit based framework allows the regulatory requirements to scale with the activity. Permits can be used to accomplish a wide variety of regulatory objectives including ensuring the safety of an activity, verifying the qualifications of those performing activities, facilitating assessment of the cumulative impact of regulated activities, or simply tracking the type and frequency of an activity [24]. Permits are used by many industrial energy facilities for activities including:

- siting, construction, and operation of an commercial facility,
- production of solid, liquid, and gaseous effluents,
- thermal, electromagnetic, visual, or noise pollution,
- production of electricity or other energy production

These permits, issued by different jurisdictional authorities and agencies, have significant regulatory precedent. The effectiveness of these permits in accomplishing their larger regulatory objectives may vary, but the process for creating, issuing, and enforcing permits is well understood.

A permit based regulatory framework has additional regulatory precedent for the regulation of certain nuclear materials in the United States. Both the federal regulator (NRC) and state regulators (state radiation control programs with jurisdictional authority under the NRC Agreement State framework[1]) license the use of certain amounts of radiological materials under a permit based regulatory framework. One of the facilities regulated through this process is a particle accelerator. While the actual operation of the accelerator is not regulated, the production of radiation and radioactive material during

[1] The NRC Agreement State framework allows the NRC to delegate regulatory authority for certain licensing activities to state agencies. These state agencies must to meet or exceed NRC requirements for personnel and processes related to the regulation of nuclear activities [30]

accelerator operation is regulated [27]. Some fusion energy proponents have suggested that the fusion reactors are technically particle accelerators and that they should be regulated using a permit based regulatory framework [28].

The application of a permit based regulatory framework to commercial fusion reactors based on their technical similarity to particle accelerators is creative but may not be appropriate. The regulation of particle accelerators is based on the radiation hazard and production of radioactive material – not based on the actual device itself. Review of the permit based regulatory framework for radioactive material in 10 CFR Part 30 provides inventory based thresholds for permit based licensing for most radionuclides [29]:

- Schedule B exemption limit (no license required)
- Schedule C exemption limit (no off-site consequence analysis required)

An activity is exempted from permit based requirements if the material inventory at a facility does not exceed the Schedule B exemption limit. An activity is subject to permit based requirements if the material inventory at a facility exceeds the Schedule B exemption limit. An activity is required to provide off-site consequence analyses and emergency response plans, and is subject to a limited independent review regulatory framework if the if the material inventory at a facility exceeds the Schedule C exemption limit. This tiered system provides for vary levels of regulatory oversight depending on the actual hazards of the activity.

Commercial fusion facilities will have a number of radiation and radiological hazards depending on the specific facility technology and design. Neutron radiation, secondary gamma radiation, tritium and tritiated materials, and neutron activated materials are all of particular concern for a D-T fueled commercial fusion facility (see Chapter 3). The Schedule B and Schedule C tritium limits in 10 CFR Part 30 can be used to characterize what radioactive material inventories would subject facilities to different regulatory oversight requirements. The Schedule B exemption limit for tritium is quantities of less than 1000 μCi of tritium and the Schedule C exemption limit is quantities of less than 20,000 Ci of tritium [29]. The Schedule C exemption limit corresponds with a tritium inventory of approximately 2 grams of tritium. Facilities will inventories over 2 grams of tritium would be required to submit off-site consequence evaluations and emergency response plans.

These consequence evaluations and emergency response plans may be relatively simple to prepare and review for radioactive tritium inventories close to 2 grams, the processes for inventories significantly larger than 2 grams of tritium may warrant significantly more detailed evaluations and regulatory oversight. Supporting regulatory documents from the development of the Schedule B and Schedule 3 inventory limits suggested that, at the time, maximum licensed possession limits under the 10 CFR Part 30 framework for tritium were limited to 10 to 15 g tritium [31]. It is not clear if significantly larger tritium inventories (tens, hundreds, or thousands of grams) potentially found at D-T fueled commercial fusion facilities would be adequately regulated under this framework. The direct application of particle accelerator permit based regulatory framework to commercial fusion facilities may be not be appropriate unless the design and operation of facilities can reduce radioactive material inventories to those comparable with the Schedule B and Schedule C material limits in 10 CFR Part 30.

6.5.6 Framework summary and compatibility with licensing evaluation methods

The permit based regulatory framework facilitates limit the operational hazard consequences associated with activities while minimizing on-going regulatory burden associated with applications, compliance, and enforcements. The framework clearly defines Regulator Operating Limits and allows facilities to determine how to design and operate their facilities to meet the performance requirements. Compliance and enforcement methods can be tailored to the specific application to ensure that the regulatory framework is correctly incentivizing safe operation of facilities. This regulatory framework has precedent in environmental regulators such as the U.S. Environmental Protection Agency.

This framework is a traditional regulator approach to safe operation of facilities. Regulatory Operation Limits are intended to control the chronic and acute consequences associated with facility hazards. This approach, however, does not review or constrain the Normal Operating Limits, Operator Comfort Limits, or Understood Failure Limit for an activity or facility. As a result, operational deviations beyond the Regulatory Operating Limit or unexpected failures below the Regulatory Operating Limit may occur. The permit based regulatory framework may be prone to some chronic or acute hazard consequences as the deviations and violations occur. Deviations may be controllable for limited violation of chronic hazard limits, but unexpected system failures for acute hazard limits could have significant hazard consequences. Determining appropriate hazard levels and limitations on acute hazards to facilitate safe operation is a challenge for the development of a permit based regulatory framework.

The initial regulatory costs associated with the permit based regulatory framework will be significant as the regulator works with stakeholder to establish appropriate hazard limits, application requirements, compliance methods, and enforcement mechanisms. Once the regulatory framework is established, however, the regulatory costs (and associated regulatory burden) can be tailored depending on the hazards. Regulation of chronic, minor consequence hazards would likely require fewer regulatory resources than acute, severe consequence hazards due to the mechanisms required to assess compliance with limits.

The permit based regulatory framework is only compatible with low regulatory burden licensing evaluation methods, specifically the worst case release evaluation and the maximum credible release evaluation. The goal of the permit based regulatory framework is to minimize regulator burden through use of simplified Regulatory Operating Limits. Use of more complex licensing evaluation methods may provide insights to facilities regarding the methods they will use to meet Regulatory Operating Limits or their likelihood of exceeding limits, but these are both outside the scope of permitting for the regulatory framework. The facility is permitted to use appropriate methods to meet the regulatory limits but will not have reviewed calculations except in cases where a prescriptive or derived facility or design specific hazard limit is used. The compliance and enforcement mechanisms associated with the permit based regulatory framework would ultimately control the facility's design and operational choices as well as Normal Operating Limits to prevent exceedance of Regulatory Operating Limits. The process of compliance would be conducted on a facility by facility basis.

6.5.7 Impacts of regulatory framework on commercial fusion regulation

The permit based regulatory framework represents a regulatory approach to commercial fusion that treats the technology the same as other industrial facilities. The process minimizes regulator reviews of commercial fusion facility design, operations, and safety by focusing on facility compliance with set Regulatory Operating Limits. The permit based regulatory framework would result in larger engineering margins for commercial fusion facilities due to the use of simplified analysis methods in the development and evaluation of compliance with Regulatory Operating Limits. These restrictions could significantly impact operations if they are sufficiently conservative to impede commercially viable design and operation of fusion technology. The major challenges of the permit based regulatory framework for commercial fusion technology are on the handling of acute hazards and the handling of radiological hazards with no safe threshold of exposure.

A permit based regulatory framework is well suited for the regulation of chronic hazards. Definition of sufficiently low Regulatory Operating Limits for chronic hazard limits allows for the monitoring of facility operation and remediation of degraded conditions exceeding Regulatory Operating Limits before harm occurs through cumulative pathways. In a commercial fusion facility, setting permit based regulatory limits on the concentration and total inventory of radiological effluents can help ensure that the facility does not introduce an unacceptable quantity of radiological contaminants to the local environment. This regulatory process is fairly straight forward and aligns with existing permit based regulatory guidance from the U.S. EPA on the regulation of facilities that handle radioactive materials [32].

A permit based regulatory framework is less well suited for regulation of acute hazards because of the challenges related to preventing and enforcing permit violations. Acute releases are marked by sufficiently high releases that are hazardous to workers, the public, or the environment. Acute releases can be generally handled in two ways in a permit based regulatory framework: permit limits on hazard inventories that can produce in acute harm or permit limits on hazard releases that produce acute harm.

The first approach to permit based regulation of acute hazards from a commercial fusion facility is a permit based hazard limits approach. This approach would restrict the quantity of hazardous materials (e.g., mobilized neutron activated materials and tritium contaminated materials) to levels below which an acute release would not cause undue harm or would alternatively require additional emergency planning and administrative controls to ensure public awareness of the facility hazards. This regulatory model is based on the Risk Management Plan (RMP) rule utilized by the U.S. EPA for the regulation of industrial facilities with the potential for significant off-site hazard consequences [33]. This regulatory approach could place significant limits on fusion facility design or result in public concern regarding the emergency planning requirements for acute releases.

Commercial fusion developers would need to consider the impacts on design and social license associated with this approach. This approach has the distinct advantage of preemptively limiting harm associated with a facility.

The second approach to permit based regulation of acute hazards from a commercial fusion facility is a permit based hazard release limit approach. This approach would limit the acute release concentration or quantity of hazardous materials (e.g., mobilized neutron activated materials and tritium contaminated materials) to levels below which an acute release would not cause catastrophic undue harm (e.g., a 5 rem or 25 rem maximum off-site dose). This approach is suitable from a design perspective but the limited regulator reviews associated with a permit based regulatory framework means that the commercial fusion would ultimately be responsible for ensuring limit compliant design and operation. The main challenge with this approach is that if the acute regulatory limit is exceeded, any enforcement mechanisms are purely punitive, as excessive harm has already occurred. If a commercial fusion facility suffers a tritium release that results in excessive off-site radiation doses, the harm cannot be correct so restitution and punishment are the only remaining resolutions. The incentives and consequences must be aligned carefully with this approach to ensure that limits are met.

These two approaches are imperfect but workable methods for solving the challenges associated with acute management of hazards in a permit based regulatory framework for commercial fusion facilities. The impact of these challenges on the development of regulation would depend, in part, on the actual acute hazard characteristics of a commercial fusion facility. Reducing the inherent hazards by design is the most effective method for ensuring safety but may be limited by the economic or operational constraints of the system. The 1984 Bhopal accident spurred redesign of chemical facilities that handled highly hazards materials, and illustrated how the principles of minimizing, substitute, mitigating, and simplifying hazardous material processes can reduce facility risk [34]. These similar principles could be incorporated in the design philosophy of commercial fusion facilities to emphasize minimization of hazards from pre-conceptual design through operations and decommissioning. This approach would not only improve the compatibility of commercial fusion facilities with the permit based regulatory framework but would improve facility safety and compatibility with all regulatory frameworks.

The second major challenge of the permit based regulatory framework for commercial fusion facilities is handling of radiological hazards with no safe threshold of exposure. Safe exposure limits are defined for many chemical hazards, below which harm is not expected to occur. A permit based regulatory framework utilizes these limits to characterize different acceptable release and exposure limits. Radiological hazards, however, are not known to have a limit of safe exposure. The prevailing model relating radiation exposure and health effects is the linear, no-threshold dose model that describes a linear, stochastic relationship between exposure and health effects. While the health effect probability may be low for low doses of radiation, the stochastic nature of radiation damage and the inability to distinguish low dose radiation induced health effects (e.g., cancers) from those caused by other factors. Few other hazardous materials can induce statistical chronic health effects from single acute doses.

Use of a permit based regulatory framework for commercial fusion requires use of Regulatory Operating Limits that are far below those expected to cause significant health effects due to the potential for long-term health effects and the statistical uncertainty related to exposure. Meeting the NRC Qualitative Health Objective of radiation exposures only account for one tenth of one percent (0.1%) of all other cancer related fatalities correlates with a Regulatory Operating Limits of 4 mSv [35][36]. This dose is approximately equal to the annual dose received from naturally occurring background sources but is far below the threshold for detectable acute health effects (250 mSv) or the confidence threshold for applicability of the LNT model (100 mSv). This challenge related to definition of Regulatory Operating Limits absent any other analyses in a permit based regulatory framework may result in extremely low dose thresholds that are challenging for facilities to meet while maintaining commercial viability. Use of best available technology or other prescriptive requirements may facilitate more economic operation of commercial fusion facilities but would require more detailed regulatory discussion and public acceptance of the higher exposure limits. Alternatively, re-examining the regulatory basis for the LNT model in radiation dose consequence evaluations could permit the use of higher Regulatory Operating Limits.

The challenges for commercial fusion facilities associated with the handling of radiological hazards with no safe threshold of exposure will depend largely on the design of the facility. Use of systems with high retention of radiological materials may enable simple compliance with strict regulatory limits but these systems may come at a high cost for facilities. Balancing the inherent conservatisms associated with the simplified analyses and hazard consequences used within the permit based regulatory framework would be a challenge for regulation of commercial fusion facilities.

The permit based regulatory framework would enable the development of commercial fusion technology under similar regulatory rules as other sources of energy. Commercial fusion companies would need to work with regulators to develop appropriate Regulatory Operating Limits that meet social requirements on hazards but also enable commercially viable operation of fusion facilities. The permit based system provides commercial fusion companies wide latitude in the design and operation of facilities but would hold them accountable for compliance with relevant regulatory limits. The challenges associated with managing acute hazards would require facilities to consider the impacts of design and inherent hazards on off-site consequences. Minimizing, substitute, mitigating, and simplifying hazardous material processes could significantly reduce risk but may not be technically or commercially feasible. Incorporation of this safety philosophy into early development and design activities increases the likelihood of successful integration but assessing the likelihood of success at a low level of design completion is difficult at this time. The permit based regulatory framework is based on decades of successful operation of hazardous facilities in the United States but control of acute catastrophic hazards would be key to successful regulation and maintaining social license for commercial fusion facilities.

6.6 Delegated review based regulatory framework

The third regulatory framework reviewed is a delegated review based regulatory framework. This framework emphasizes full review of regulated activities to ensure safety, but permits collaboration between the regulator and licensees to reduce the time, cost, and regulatory burden associated. A delegated review based regulatory framework allows subject matter experts at licensees to serve as regulator representative reviewers for certain licensing activities. A delegated review regulatory system allows for a full review of the Understood Failure Limit, Normal Operating Limit, and basis for the Operator Comfort Limit while reducing the regulatory burden associated with the licensing process by focusing regulator resources on safety critical activities. The delegated reviewers (reviewed to as designees) can approve specific items in the review of regulated activities based on oversight and guidance from the regulator. Allowing experts from certified applicants to review regulatory material can substantially shorten the review period due to their experience and expertise in a specific subject matter area.

This main purpose of this regulatory framework is to reduce the regulatory burden associated with activities that require full regulatory reviews due to the high hazard consequences associated with unexpected failure. This framework has a high regulatory burden as it requires assessment of Understood Failure Limit adequacy and uncertainties, development of Regulatory Operating Limits, verification of the proposed Normal Operating Limits, and review of the Operator Comfort Limit to ensure safe operation points. This framework a high regulatory burden for regulators and licensees, but the use of delegated experts is a way to reduce the regulator burden and eliminate the need for licensees to train regulators on their specific system.

The delegated review regulatory framework is based on the regulatory practices used by the U.S. Federal Aviation Administration (FAA) [37]. The original goal of the expertise program was to allow for the rapid expansion of regulated activities and ensure that the FAA had the technical expertise necessary to perform adequate reviews on licensees. The FAA notes that:

> "Although paid by the manufacturers, these designees act as surrogates for FAA in examining aircraft designs, production quality, and airworthiness. The FAA is responsible for overseeing the designees' work and determining whether the designs meet FAA requirements for safety." [38]

Through the designee program, the FAA is able to streamline the review process while still providing full reviews of all licensed activities. This enables prioritization and focused independent review of safety critical activity by FAA staff. This prioritization is intended by the FAA to not reduce cost but to improve safety:

> "…safety will be enhanced because FAA personnel relieved from tasks accomplished by Designated Airworthiness Representatives [designee

> program] will be able to redirect their efforts to other areas affecting safety." [38]

This regulatory framework can allow a tailoring of the regulatory review process based on regulator's evaluation of the Understood Failure Limits and uncertainties in system behavior or interactions that may lead to unexpected failures. Known failure mechanisms within the Understood Failure Limits but outside of the Normal Operating Limits can be reviewed by designees to ensure compliance with Regulatory Operating Limits under all conditions. This enables a full but focused review of regulated activities.

A delegated review based regulatory framework is reviewed in this section for its applicability to commercial fusion facilities. This framework characterizes the specific Understood Failure Limit for an activity, assesses compliance with Regulatory Operating Limits, and reviews Normal Operating Limits compliance with other limits. Operating training and processes are also reviewed to ensure that Operator Comfort Limits will maintain facility operating points within acceptable limits. The delegated review based regulatory framework can be characterized with five major aspects:

- Establishing Regulatory Operating Limits
- Creating project specific licensing plan and licensing basis requirements
- Delegating authority for licensing review
- Evaluating project licensing basis requirements
- Auditing delegated authority performance

These framework parts compose a regulatory process that allows for the complete review of licensed activities while focusing regulator resources on safety critical functions. Regulators such as the FAA have demonstrated the potential for using a delegated review based regulatory framework.

6.6.1 Establishing Regulatory Operating Limits

The first major characteristic of the delegated review based regulatory framework is establishing the Regulatory Operating Limits for an activity. Different types of limits may be developed for an activity depending on the specific hazard, the mechanistic understanding of the system and consequences, and specific goals of the regulatory system. These limits serve as the basis for the licensing process and may be qualitative or quantitative.

While the permit based regulatory framework may default to performance based Regulatory Operating Limits except in cases where a prescriptive based limit or requirement is more suitable, a delegated review based regulatory framework may utilize prescriptive or performance based regulatory requirements. Prescriptive requirements are more suitable in cases of uniform activities, where development and demonstration of safe design are relatively standard across licensees. Prescriptive requirements can be extremely clear for design and review in these cases and help reduce regulatory uncertainty. Performance based requirements are more suitable in cases where multiple different approaches could be used to achieve the same functional outcome. While utilizing case-by-case exemptions to prescriptive requirements could accommodate these different approaches, use of performance based requirements creates a more uniform standards for design and review of engineered systems and can reduce regulatory uncertainty for novel designs. Table 6.3 provides examples of the initial prescriptive and revised performance based requirements within a delegated authority regulatory framework for small aircraft [39][40].

Use of prescriptive requirements forces a regulator to develop specific Regulatory Operating Limits that, if met by an applicant, would result in safe operation by bounding specific operating points the Understood Failure Limit. Subsequent regulatory reviews focus on assuring the applicant's initial compliance with relevant regulatory requirements and that adequate control processes are in place to ensure continued compliance. The regulatory burden is on the regulator to develop appropriate regulatory requirements while the regulatory burden is on the applicant to meet the minimum requirements and ensure safe operation.

Use of performance based requirements allow a regulator to take a higher level approach to develop general Regulatory Operating Limits that, if met by the applicant, would exclude unsafe operating points in the activity specific Understood Failure Limit. Subsequent regulatory reviews focus on assuring an applicant's safety basis meets the general Regulatory Operating Limits and that there is adequate margin between specific Normal Operating Limits and the Understood Failure Limit. The regulatory burden is on the applicant to develop a safety appropriate safety basis and demonstrate compliance with the general Regulatory Operating Limits while the regulatory burden is on the regulator to review the technical basis to ensure that safe operation will occur.

Table 6.3. Example of prescriptive versus performance based requirements

Prescriptive Stall Requirement	Performance Stall Requirement
Sec. 23.49 — Stalling period. (a) V_{SO} and V_{S1} are the stalling speeds or the minimum steady flight speeds, in knots (CAS), at which the airplane is controllable with— (1) For reciprocating engine-powered airplanes, the engine(s) idling, the throttle(s) closed or at not more than the power necessary for zero thrust at a speed not more than 110 percent of the stalling speed; (2) For turbine engine-powered airplanes, the propulsive thrust not greater than zero at the stalling speed, or, if the resultant thrust has no appreciable effect on the stalling speed, with engine(s) idling and throttle(s) closed; (3) The propeller(s) in the takeoff position; (4) The airplane in the condition existing in the test, in which V_{SO} and V_{S1} are being used; (5) The center of gravity in the position that results in the highest value of V_{SO} and V_{S1}; and (6) The weight used when V_{SO} and V_{S1} are being used as a factor to determine compliance with a required performance standard. (b) V_{SO} and V_{S1} must be determined by flight tests, using the procedure and meeting the flight characteristics specified in §23.201. (c) Except as provided in paragraph (d) of this section, V_{SO} and V_{S1} at maximum weight must not exceed 61 knots for— (1) Single-engine airplanes; and (2) Multiengine airplanes of 6,000 pounds or less maximum weight that cannot meet the minimum rate of climb specified in §23.67(a) (1) with the critical engine inoperative. (d) All single-engine airplanes, and those multiengine airplanes of 6,000 pounds or less maximum weight with a V_{SO} of more than 61 knots that do not meet the requirements of §23.67(a)(1), must comply with §23.562(d).	**Sec. 23.2110 — Stall speed.** The applicant must determine the airplane stall speed or the minimum steady flight speed for each flight configuration used in normal operations, including takeoff, climb, cruise, descent, approach, and landing. The stall speed or minimum steady flight speed determination must account for the most adverse conditions for each flight configuration with power set at - (a) Idle or zero thrust for propulsion systems that are used primarily for thrust; and (b) A nominal thrust for propulsion systems that are used for thrust, flight control, and/or high-lift systems.

Development of Regulatory Operating Limits will depend on the specific activity, hazards, and changes to the Understood Failure Limit as new operating experience improves understanding of system behavior. Regulatory Operating Limits are the basis for review activities so characterization and development of appropriate limits is important to the adequate assessment of applications. Responsibility for safe operation ultimately rests with the operator but ensuring compliance with Regulatory Operating Limits is an additional check on activities.

6.6.2 Creating project specific licensing plans

The second major characteristic of the delegated review based regulatory framework is creating project specific licensing plans and licensing bases for the activity. In this stage, applicants work with regulators to present plans their activity or facility, identify the applicable regulatory requirements, and negotiate a plan for how to adequately demonstrate compliance with the applicable requirements. Early interaction with the regulator can help ensure that design and engineering activities can directly contribute to the licensing basis of a facility (e.g., regulator involvement in physical model validation or testing plans).

One strength of the delegated review based regulatory framework is that the creation of a project specific licensing plan allows for early identification of potential sources of uncertainty in Understood Failure Limit (e.g., limited understanding of system interaction for complex systems, limited or no operating experience for novel technologies). These uncertainties can be clarified through design, analysis, and testing activities to ensure the appropriate application of Regulatory Operating Limits and definition of adequate Normal Operating Limits.

This process is collaborative and iterative, as regulators identify specific design requirements that will compose the licensing basis and applicants propose methods to demonstrate compliance with the requirements. An open, deliberative process between the regulator and the applicant allows for clarification of regulatory requirements and safety critical aspects of the design or facility. The regulator still retains independence in the regulatory process by not prescribing methods to demonstrate compliance but should provide actionable information for the applicant on where deficiencies should be addressed in the proposed method. Iterating the licensing plan development before significant regulatory reviews are completed is intended to reduce the need for time intensive and costly iterations of safety basis documentation.

This stage is completed when the regulator has a complete set of applicable regulatory requirements that make up the licensing basis for the facility and the applicant has an acceptable plan for demonstrating compliance with the regulatory requirements through analysis, testing, and other engineering processes. In the operational failure space conceptual model, this stage is a definition of information needed to validate that the Understood Failure Limit lies outside of the Regulatory Operating Limit and that sufficient margin exists between the Normal Operating Limit and the Regulatory Operating Limit.

6.6.3 Delegating authority for licensing reviews

The third major characteristic of the delegated review based regulatory framework is delegating authority for licensing review and is the defining feature of framework. Regulators can delegate authority for some regulatory reviews and approval to designees, non-regulator technical experts often employed by the licensees, enabling more efficient use of regulatory resources and specific focus on safety critical issues. These designees are overseen and audited by regulator staff that can ensure that they are performing their oversight role as independent surrogates of the regulator, despite their employment with the licensee.

The rational for delegated reviews is to ensure full review of the licensing basis for an activity while leveraging external technical expertise and facilitate regulatory staff focus on safety critical aspects of the licensing basis [41]. Extensive regulatory staff reviews of licensing basis requirements with significant prior operating experience or well characterized Understood Failure Limits, while important to ensuring overall regulatory compliance, are not likely to present significant risk of unexpected failure mechanisms. Novel or complex systems with limited operating experience may not have significant uncertainties related to their Understood Failure Limits. Additional independent reviews by the regulator help ensure that the systems appropriate consider system behavior, interactions, and conditions so that system operation will satisfy the Regulatory Operating Limits and the licensing bases.

Delegation of regulatory authority is limited to specific regulatory functions as part of the review process. Independent review of FAA usage of delegated regulatory authority states that “designees are not authorized to approve departures from policy and guidance, new/unproven technologies, equivalent level of safety findings, special conditions, or exemptions” [41]. These designees utilize their experience and expertise on a particular subject matter area to independently assess (on behalf of the regulator) if analysis, testing, or other documentation submitted by a licensee demonstrates satisfactory compliance with the specific regulatory requirements and licensing bases.

The regulator, through strict process controls and designee reviews, confirms designee expertise and independence to act as a regulatory surrogate. Processes used by other regulators include designee experience requirements, designee trainings, required independent management structures within designee companies to limit corporate pressure on designees, and audits to ensure that designees are acting in good faith as surrogates of the regulator. These process controls are intended to enable designees to adequately perform their regulatory function and ensure that applicants are demonstrating compliance with regulatory requirements.

The designee program within a delegated review based regulatory framework has been successfully implemented by the FAA since 1958 for the review of regulatory activities [41]. The program has been adapted over time based on lessons learned and reviews of the program, but the designees have been able to successfully contribute to the FAA mission of safe aviation in the United States. The program, however, has also been subject to significant criticism related to independence and regulatory capture. Some critics have characterized the designee program as “industry self-regulation” but reviews of the FAA designee program in the wake of aviation accidents have found that the designees functioned appropriately as surrogates of the FAA in ensuring regulatory compliance [41].

Delegating authority for licensing review requires assessment by the regulator on which parts of the project specific licensing plan and licensing basis are suitable for review by designees and which parts should be retained by the regulator for review. In general, aspects of the licensing plan that are novel, safety critical, or have high risk significance will be retained by the regulator for special review. Other aspects of the licensing plan may be delegated out to designees, with conclusions audited by regulator staff to verify process compliance. Use of qualitative or quantitative risk assessment methods may be useful for determining which aspects of the regulatory review are suitable for delegation and which aspects should be retained by the regulator. The licensing review authority may also shift throughout the licensing review process as the regulator gains confidence in the quality of the applicant's compliance methods and designee capability to complete reviews [41].

The delegation of authority allows the regulator to more efficiency perform evaluate applicant's demonstration of compliance with regulatory requirements by utilizing designee expertise in regulatory reviews. The use of focused reviews for routine regulatory activities helps minimize regulator burden and help avoid delays associated with training of regulatory staff for aspects of the licensing basis with low risk significance. Regulator retention of high risk significance aspects of the licensing basis helps ensure that regulator oversight is focused on safety critical functions in the design and operation. Maintaining the independence and review quality of designees is an on-going challenge for regulators, as their employment by the licensee may present a challenging inherent conflict of interest. Establishment of project specific licensing plans and licensing bases before starting the delegated review process aims to reduce the conflicts by creating a clear pathway to successful licensing outcomes given completion of specific licensing requirements.

6.6.4 Evaluating project licensing basis requirements

The fourth major characteristic of the delegated review based regulatory framework is evaluation of the project safety basis requirements. Following delineation of regulator and designee responsibility for regulatory reviews, technical evaluations must confirm that the applicant provides adequate demonstration of compliance with regulatory requirements. The proposed method of demonstration of compliance is outlined in the project specific licensing plans so reviewers focus on ensuring that demonstrated compliance meets all applicable regulatory requirements. This may include review of the specific analyses, models, testing, or other activities that ensure compliance with the project licensing bases.

The evaluations occur at multiple levels to account of interface and interactions that may occur from the component to assembly to system levels. Use of engineering assumptions, while necessary, should be carefully evaluated to ensure their adequacy within the project licensing basis. The evaluations required will vary depending on factors such as prior operating experience with the system, characterized uncertainties in the Understood Failure Limit for the system, proposed margin between Normal Operating Limits and Regulatory Operating Limits, and the risk significance of the system. These factors should be documented, to the greatest extent possible, in the project specific licensing plan. Greater transparency on the expected burden of proof for demonstrated regulatory compliance can help ensure that applicant methods align with the expectations of regulators and designees.

Final evaluation of the project licensing basis is performed to ensure that the applicant demonstrates compliance with all applicable regulatory requirements and that the regulatory bases of the application are adequate. The evaluation process, while briefly summarized here, is a lengthy technical process as reviewers, both regulator staff and designees, examine applicant documents and identify areas for further analysis or improvement. While the responsibility for safety ultimately rests with the licensee, these technical reviews of applicant compliance are central to the regulator's mission of ensuring safe operation and maintaining public confidence in the safety of regulated activities.

6.6.5 Auditing delegated authority performance

The fifth major characteristic of the delegated review based regulatory framework is auditing of delegated authority performance. The use of delegated authority and designees has clear advantages in terms of availability of reviewer expertise, more efficient and focused use of regulatory resources, more scalable regulatory capability, lower cost to applicants, and more streamlined regulatory review process. The use of the delegated authority and designees, however, has a clear disadvantage in terms of appearance of regulatory independence. At first glance, the delegated review based regulatory framework allows the applicant to self regulate without oversight from the regulator. Full self-regulation without oversight can result in an effectively unregulated system where applicants determine their own level of safe operation depending on their own management incentives. Oversight of the delegated authority regulatory process is required to ensure that the designees act as effective surrogates of the regulator within the regulatory review process.

Three main factors need to be addressed when assessing the performance of designees: qualifications to perform reviews, independence when performing reviews, and quality of reviews. Each of these factors could results in an inadequate regulatory system and unexpected failures due to incorrect characterization of the Understood Failure Limit, definition of a Regulatory Operating Limits, and development of Normal Operating Limits.

Designee qualification to perform reviews can be ensured through administrative processes including verification of experience, examination of knowledge, and trainings on specific review activities. Maintenance of these administrative processes by both the regulator and licensees is important to ensuring the quality of designees.

Designee independence to perform reviews is extremely challenging due to the implicit and explicit biases and pressures that may exist on a designee. Designee employees of a licensee have implicit or explicit bias in the successful completion of licensing activities. If a designee believes that approval must be given regardless of data quality to ensure company success, there will be a strong implicit bias to approve. Company and designee culture must stress that the positive correlation between compliance and corporate success, highlighting that regulatory approval followed by unsafe conditions is far worse for a company than delayed regulatory approval with a safe design.

Designee employees of a licensee may be subject to implicit or explicit pressure to approve licensing activities by other employees of the licensee or management. This pressure may be indirect such as pressure to maintain schedule and reduce costs to direct pressure to approve regulatory reviews and prevent delays in the approval process. Formal and informal processes are needed within the company to ensure that designees have adequate independence to perform their regulatory duties without fear of retribution for findings or reward for inappropriate regulatory approvals. Oversight of safety culture at the regulator and licensee levels and clear reporting pathways are key to ensuring that designees can operate independently as surrogates of the regulator.

Quality of reviews is the final challenge within the designee system. The goal of the delegated review based regulatory framework is to reduce the regulatory burden associated with the licensing process. Having regulatory staff audit all designee approvals would be resource intensive and largely negate the purpose of the delegated review system. Implementation of a system or risk based audit approach to oversight enable the regulator to identify trends in designee activities as assess if existing licensee programs are resulting in appropriate assessment of safety [9]. Risk classification of regulatory activities can provide insights into more important regulatory reviews but a systems based approach is useful at capturing system interfaces and interactions can act as initiation or behavior inflection points for unexpected failures in complex systems.

The delegated review based regulatory framework succeeds only if the licensees can be relied up as partners in the regulatory process. Designees must perform regulatory review work independently of their employer (despite their continued employment) and exceed the quality standards expected of regulatory staff. Proper qualification, safety culture, and oversight are all key to ensuring that the licensing benefits delegated review based regulatory framework can be realized without compromising operational safety.

6.6.6 Framework summary and compatibility with licensing evaluation methods

The delegated review based regulatory framework enables the efficient, full review of applicant activities through the utilization of licensee expertise in the regulatory approval of certain licensing activities. The delegation of regulatory authority to designees reduces regulatory staff needed to perform reviews, helps ensure technical expertise is available to fully review licensing documents, and allows regulators to focus resources on safety critical or novel operational features. The delegated review process is vulnerable to self-regulation and abuse if designees are unable to maintain independence and act as surrogates for the regulator. As a result, process controls on the delegated authority process are critical to maintaining regulatory framework integrity.

This framework is limited collaboration between a regulator and industry to ensure safety through compliance with regulatory requirements. The industry ultimately has the responsibility for safe operation and must adequately demonstrate the safety case for an activity while the regulator verifies regulatory compliance. The designees allow the regulator to utilize field expertise and experience in the evaluation of the complex engineering systems without the need to overstaff regulator expertise on all subjects. This allows for more timely regulatory reviews and the regulator capability can more easily scale with the number of applicants as a smaller number of regulatory staff is needed to oversee designee activities. This framework is largely independent of the licensing evaluations used to demonstrate compliance with regulatory requirements. The ability to delegate regulatory authority allows the regulator to focus on safety critical issues while overseeing delegated review on all other aspects of the licensing case.

The regulatory and organization costs associated with a delegated review based regulatory framework are challenging to characterize due to the distribution of costs between the regulator and the licensee. Costs and regulator effort associated with development of Regulatory Operating Limits and project specific licensing plans are likely comparable to other regulatory frameworks. Costs and regulator effort associated with the delegated authority review system, however, is likely a substantial up front regulatory costs as review process and processes to ensure designee qualification, independence, and quality must all be established along with organizational oversight structures. Once this framework is developed, the regulatory burden between the regulator and the licensee will shift depending on the specific activity. For novel regulatory activities, significant regulator review will likely be warranted to ensure through compliance with regulatory requirements. For more routine regulatory activities, delegation of regulatory authority may enable designees to more reviews more efficiently and at known cost for the licensee. Total cost associated with the review process would likely scale with the methods used to demonstrate regulatory compliance. Complex licensing evaluations would require greater review (both by regulatory staff and designees) than simpler licensing evaluations. The selection of appropriate demonstration methods that balance regulatory margin, regulator effort, licensee effort, and other factors could be considered during the development of the project specific licensing plans.

The delegated review based regulatory framework is compatible with all of the licensing evaluation methods described in Chapter 8. In general, use the use of less detailed licensing evaluation methods (e.g., worst-case release evaluations and maximum credible release evaluations) will require fewer regulatory preparation and review resources but require significantly more margin between the Understood Failure Limit, the Regulatory Operating Limit, and the Normal Operating Limit. Use of more detailed licensing evaluation methods (e.g., deterministic design basis evaluations and probabilistic design basis evaluations, and STPA) can result in less conservative designs but will require greater regulatory preparation and review resources.

The use of delegated reviews can reduce the regulatory costs associated with these high resource licensing evaluation methods as designees with specific expertise in the evaluation method may be able to more efficiently review large and complex licensing evaluation than regulatory staff, sometimes at lower cost – the billing rate for regulatory staff work with NRC is $279 per hour [42]. For regulatory reviews retained by the regulatory due to their safety significance, risk, or novel aspects, special care should be taken by the licensee to determine what licensing evaluation methods will be most effective at balancing demonstrated compliance with regulatory requirements, adequate margin for design and operation, and cost associated with preparation and review.

This regulatory framework is a unique approach to the regulation of rapidly evolving, novel technology. The failure modes, hazards, and behavior of modern digital control systems of commercial aircraft regulated by the FAA are fundamentally different than the hydraulic-mechanical control systems used by aircraft half a century ago [43]. Use of a delegated review regulatory framework has, in part, enabled the economic and timely implementation of novel technology while maintaining (and improving) safe operation standards for commercial aircraft. This regulatory framework can enable the efficient regulatory review of highly complex technologies but requires significant infrastructure and processes to ensure that designees can function as independent surrogates for the regulator and to maintain trust with the public. Major incidents with unexpected failure modes reveal underlying concerns with self regulation, and the need to ensure that administrative processes and appropriate safety culture maintain the efficacy of the designee program [41]. This regulatory framework is extremely versatile, enabling effective and efficient regulation of complex technologies but requires constant oversight to ensure that it is providing for safe system operation.

6.6.7 Impacts of regulatory framework on commercial fusion regulation

The delegated review based regulatory framework represents a balanced regulatory approach between a largely self-regulated philosophy to design and operational safety used in a permit based regulatory framework (e.g., chemical production facilities) and an regulator oversight philosophy to design and operational safety used in an independent review based regulatory framework (e.g., fission facilities). The process provides for the full regulatory review of commercial fusion facility design, operations, and safety compliance with Regulatory Operating Limits but allows the regulator to utilize applicant technical expertise through designee reviewers to reduce regulatory costs, reduce regulator burden, and facilitate regulator focus on safety critical issues.

Leveraging applicant experts to critically review and evaluate peer work on behalf of the regulator enhances timely licensing of rapidly evolving or novel technologies. The first generation of commercial fusion facilities developed and deploy will be, by definition, novel technologies. The wide variety of approaches to commercial fusion (e.g., confinement approaches, fuel cycles, power conversion) may challenge regulators and require significant regulator resource development. Use of the delegated review based regulatory framework could enable the efficient and effect regulatory reviews of commercial fusion facilities. The major challenges of this regulatory framework on the regulation of commercial fusion are the development of appropriate regulatory structures to ensure independent and adequate reviews by designees and maintaining public trust in the regulatory process.

Legislators developing the initial regulation of the first generation commercial nuclear fission facilities in the United States in the 1950s faced a significant staffing challenge. An independent regulator was desirable for ensuring regulator focus on health and safety issues but feared that there was insufficient technical expertise in needed areas to provide adequate independent technical reviews without significantly slowing the development and deployment process [44]. This staffing limitation was a major factor in the development of the Atomic Energy Commission as an agency with the dual (and arguably conflicting) responsibilities of development and regulation of nuclear fission energy [45]. These conflicting roles lead to accusations of regulator inaction on safety issues related to first generation commercial fission facilities, loss of public trust in the technology, and contributed to the dissolution of the agency into separate development and regulatory agencies [44]. The history of commercial fission regulation provides important lessons for the development of commercial fusion regulation. An effective delegated review based regulatory framework can help ensure full regulatory review of commercial fusion facilities activities but also allow the regulator to leverage commercial expertise in the timely evaluation of applications to support commercial fusion technology development. This success, however, depends on the strength of the process.

The first major challenge of the delegated review regulatory framework is development of appropriate regulatory structures to ensure independent and adequate reviews by designees for commercial fusion. Without independent reviews by designees, this regulatory framework cannot accomplish the goal of full review of applicant activities to ensure compliance with regulatory limits. The U.S. FAA has over six decades of experience with a delegated review based regulatory framework for the review of complex, high hazard systems. The designee program is based on strong oversight, regulator and industry safety culture, and continuous incorporation of lessons learned and internal audits [37]. A new regulator would need to work closely with the commercial fusion industry to develop the initial regulator structures and process for designee reviews. Using commercial fusion industry employees as surrogates for the regulator requires clear delineation of roles and expectation of regulatory independence.

While the FAA has been able to evolve the regulatory system over time, regulator and commercial fusion industry would need to assess implementation viability for a novel industry, novel technology, and new regulator. Staged implementation of delegated review authority may be helpful at ensuring the development and implementation of appropriate designee processes. A slower deployment process would allow for monitoring of designee activity to ensure that an appropriate independent safety culture develops amongst designees. This staged implementation would allow for the gradual transition to designee review on many topic areas but would require an alternative regulatory structure for initial reviews. Additionally, regulators will need to develop experience and operational comfort on what reviews should be retained by the regulator due to their novelty or safety significance and what reviews can be delegated to the licensees. For commercial fusion facilities, nearly all aspects of a facility will be novel, so initial delineation of review roles to designees must be addressed in regulatory process. This challenge exists in addition the actual technical challenge associated with performing regulatory reviews. While the delegated review based regulatory framework may reduce regulatory burden associated with reviews, the initial process implementation for commercial fusion energy could be a significant challenge.

The second major challenge associated with the delegated review regulatory framework is maintaining public trust in the regulatory process. A delegated review regulatory framework for commercial fusion facilities could be susceptible to accusations of inappropriate industry involvement in regulatory decisions. Regulatory independence is characterized by development organizations as a key attribute of effective regulatory frameworks [46]. Degradation of regulatory independence and regulatory capture can contribute to regulatory failures due to inappropriate industry influence that prioritizes commercial considerations over safety considerations [47].

The delegation of regulatory activities to the licensee in this regulatory framework, despite controls on designee activity to ensure independence, has resulted in accusations of regulatory capture. The FAA has been repeatedly questioned about the impacts of the delegated review regulatory framework (especially after major accidents) despite a safety record that shows improvements in design and operational safety (see Figure 6.3) simultaneous to increases in use of delegated authority to review safety [41]. Operational data suggests that the increased use of delegated authority has not reduced aviation safety and that regulator responses to lapses in delegated authority performance have contributed safety improvements.

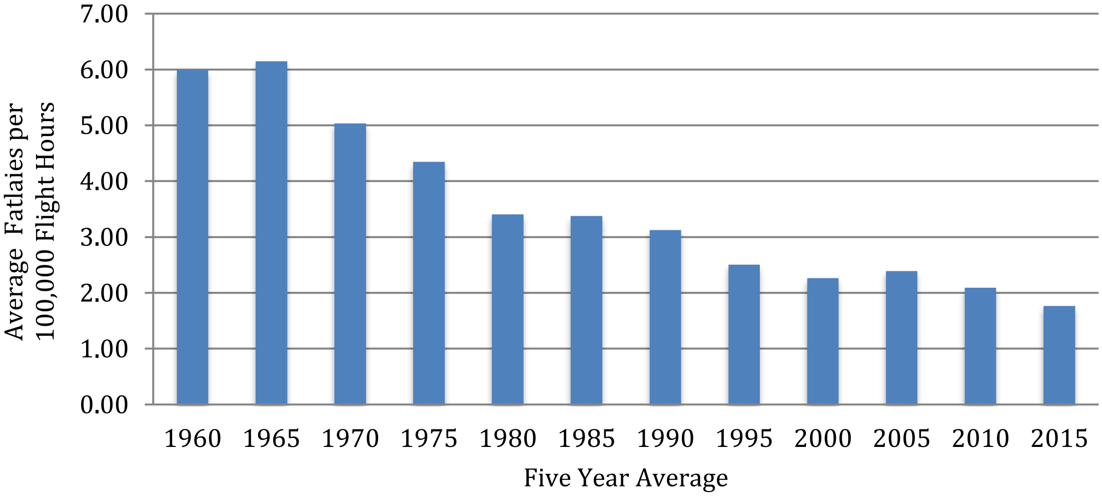


Figure 6.3. Five year forward averaged fatalities per 100,000 flight hours for U.S. air travel [48][49]

Implementation of the delegated review regulatory framework for commercial fusion facilities would need to maintain public confidence in the effectiveness of the regulatory system. Transparency in the authority delegation process, public audits of designees, and clear delineation by the commercial fusion industry of separate designee roles could all contribute to public confidence in the system. The most likely factor in public trust would be demonstrated performance. Regulators and designees must be aware that any lapses in the safe operation of commercial fusion facilities, whether attributable to the delegated regulatory authority or not, will lead to questions regarding the effectiveness of the regulatory system for commercial fusion. Loss of public trust in the delegated review regulatory framework for commercial fusion facilities, whether warranted or not, could significant affect the development and deployment of commercial fusion technology. Designee oversight, transparency, and development of a visible regulatory and industry safety culture will be important to ensuring public trust in the regulatory framework for commercial fusion facilities.

The delegated review based regulatory framework enables the full regulatory review of commercial fusion facilities while reducing regulatory burden and leveraging the expertise of industry in the regulatory process. Incorporating lessons learned from the early licensing of commercial fission facilities could allow the more efficient and effective regulation of commercial fusion facilities. This regulatory framework has been extremely effective at enabling the safe and economic development of complex, high hazard, novel technologies such as commercial aviation, and it could provide the same benefits to commercial fusion technology. The delegated review based regulatory framework enables regulatory oversight while minimizing the burden on regulators and reducing the need to maintain large, highly specialized regulatory staffs. This allows regulators to focus regulator led reviews on the safety critical and novel aspects of commercial fusion facilities and emphasize safe operations. Initial development of this regulatory framework would be time consuming due to the administrative process requirements for performing delegated regulatory reviews but maintaining public trust through designee independence is critical to realizing the long-term regulatory benefits of this framework. The delegated review based regulatory framework is based on decades of successful regulation of commercial aviation and could help promote the safe and economic development of novel commercial fusion technology.

6.7 Independent review based regulatory framework

The fourth regulatory framework reviewed is an independent review based regulatory framework. This framework emphasizes full, independent regulator review of all regulated activities to ensure compliance with regulatory limits. A independent review based regulatory framework requires that the regulatory staff is both technically capable of making independent assessments of all applicant evaluations and submitted documentation and sufficient regulatory staff is available to perform the independent reviews in a timely manner. An independent review regulatory framework provides for the independent development and Understood Failure Limit and Regulatory Operating Limits, as well as full evaluation of Normal Operating Limits and basis for the Operator Comfort Limit. The regulator acts as a check on all licensee activities and ensures operational safety through verification of design and operating conditions

This main purpose of this regulatory framework is to ensure safe operation through the reduce the regulatory burden associated with activities that require full regulatory reviews due to the high hazard consequences associated with unexpected failure. This framework has a high regulatory burden as it requires independent assessment of Understood Failure

Limit adequacy and uncertainties, development of Regulatory Operating Limits, verification of the proposed Normal Operating Limits, and review of the Operator Comfort Limit to ensure safe operation points. This framework may have a high regulatory burden for both regulators and licensees depending on the licensing assessment methods but will generally require the greatest regulatory resources out of any framework due to the repeated work.

The independent review regulatory framework is based on the regulatory practices used by the U.S. Nuclear Regulatory Commission (NRC) [50]. The initial regulation of nuclear activities in the United States was under the jurisdiction of the Atomic Energy Commission (AEC). The AEC was responsible for the research, development, promotion, and regulation of nuclear technology. Legislators recognized the potential for internal agency conflict between the roles of promoter and regulator when developing the agency structure in the 1946 Atomic Energy Act. Limitations on technical expertise for development and regulation, and a desire to accelerate the commercialization of nuclear technology lead to the development of the combined promoter and regulator [51]. Legislators still recognized the importance of independent technical review in regulatory decision making. A long-standing independent external expert review committee, the Advisory Committee on Reactor Safeguards (ACRS), was formally added to the AEC regulatory review process in the 1957. The ACRS provided independent assessment of regulator staff activities and was seen as a vital part of the AEC's regulatory activities [51].

Public concern over the conflicting AEC responsibilities for promotion and regulation of nuclear technology grew throughout the 1960s and early 1970s. AEC management and staff were accused trivializing safety and environmental issues that could harm the commercial viability of nuclear technology [44]. Legislators wanted a regulatory framework that could maintain independence from promotional activities and industry interests. Much like the ACRS already in place, an independent technical regulator was desired to ensure safe design and operation by licensees, and maintain public confidence in the regulatory process. The 1974 Energy Reorganization Act formally dissolved the AEC, placing the research, development, and promotion activities in to the Energy Research Development Agency (later reorganized into the Department of Energy) and the regulatory activities into the Nuclear Regulatory Commission [44].

The NRC's statutory mission was unique as an independent regulatory agency. The agency regulatory mission was focused to licensing and regulatory activities that "provide reasonable assurance of adequate protection of public health and safety" without consideration of the development consequences [7]. The main goal of independence is to prevent regulatory capture, where a regulator acts on behalf of the industry and not on behalf of the public [47]. Regulatory capture has been characterized by four factors [47]:

- Regulator is highly dependent on the information from the regulated entities.
- Regulator has a symbiotic relationship with the regulated entities to resolve the staffing and expertise challenges.
- Regulator avoids conflicts with the regulated entities.
- Regulator determines policy based external intervention or influence by regulated entities, not merely by the objective metrics.

An independent regulatory framework must solve these problems by developing and maintaining separate regulatory staff review capacities and assessment methods, and utilizing regulatory review process that enable transparency and objectivity for regulatory reviews.

An independent review based regulatory framework is reviewed in this section for its applicability to commercial fusion facilities. This framework performs independent assessment of the specific Understood Failure Limit for an activity, determines applicable Regulatory Operating Limits, and reviews applicant evaluations of Normal Operating Limits for accuracy and compliance with other regulatory limits. Operating training and processes are also fully reviewed to ensure that Operator Comfort Limits will maintain facility operating points within acceptable limits. The independent review based regulatory framework can be characterized with five major aspects:

- Establishing Regulatory Operating Limits
- Evaluating applicant compliance with Regulatory Operating Limits
- Performing independent evaluation of safety
- Reconcile differences between appliance and independent reviews

These framework parts compose a regulatory process that allows for the complete, independent review of licensed activities. Regulators such as the NRC have demonstrated the potential for using an independent review based regulatory framework for the review of high hazard activities.

6.7.1 Establishing Regulatory Operating Limits

The first major characteristic of the independent review based regulatory framework is establishing the Regulatory Operating Limits for an activity. This process is very similar to the process used for the delegated review based regulatory framework. Different types of limits may be developed for an activity depending on the specific hazard, the mechanistic understanding of the system and consequences, and specific goals of the regulatory system. These limits again serve as the basis for the licensing process and may be qualitative or quantitative.

Much of the discussion on the development of Regulatory Operating Limits for the delegated review based regulatory framework is applicable for the independent review based regulatory framework due to the use of full regulatory review in both frameworks. The major difference between the two frameworks, however, is the regulatory burden associated with the development and review processes.

Use of prescriptive requirements forces a regulator to develop specific Regulatory Operating Limits that, if met by an applicant, would result in safe operation by bounding specific operating points the Understood Failure Limit. An independent regulator must have sufficient technical expertise on staff to enable the independent (but not isolated) development of adequate regulatory limits. This may include verified testing or operating data, or mechanistic analytic models required to develop appropriate prescriptive limits. This process requires substantial initial personnel and project investment for a regulator but reduces the regulatory burden associated with assessment of applicant compliance with prescriptive requirements. As previously discussed, this also reduces regulatory flexibility unless an exemption process is utilized to provide relief to inappropriate requirements or requirements that can be adequately satisfied using alternative methods. Extensive use of an exemption process requires sufficient technical expertise to evaluate exemption requests and assess if they will meet the underlying technical basis for the prescriptive requirements. Challenges to prescriptive requirements could significantly extend the regulatory review process if the regulator does not have sufficient technical expertise to perform independent evaluations in a timely manner.

Use of performance based requirements allow a regulator to take a higher level approach to develop general Regulatory Operating Limits that, if met by the applicant, would exclude unsafe operating points in the activity specific Understood Failure Limit. Development of adequate performance based Regulatory Operating Limits does not require as specialized technical expertise than that required to develop prescriptive requirements due to the high level nature of the requirements. Performing subsequent regulatory reviews focusing on assessing an applicant's safety basis, however, requires substantially more technical expertise and regulatory effort. The regulatory staff must be able to perform equivalent licensing evaluations to assess the adequacy of the applicant's demonstration of compliance. The regulator performs full safety reviews and, depending on the licensing evaluation methods used by the applicant, could result in significant regulatory burden. This process requires on-going regulator expertise and regulatory effort during the licensing process, but may be more predictable than the regulatory burden associated with deviations from prescriptive requirements.

Development of appropriate Regulatory Operating Limits for an independent review regulatory framework will depend on the specific activity, hazards, and changes to the Understood Failure Limit as new operating experience improves understanding of system behavior. Regulatory Operating Limits are the basis for review activities so characterization and development of appropriate limits is important to the adequate assessment of applications. Responsibility for safe operation ultimately rests with the operator but independent assessment of compliance with Regulatory Operating Limits is an additional check on regulated activities.

6.7.2 Evaluating applicant compliance

The second characteristic of the independent review based regulatory framework is evaluating applicant compliance with Regulatory Operating Limits. The regulator independently reviews all material submitted by an applicant as part of their safety basis and assesses if it adequately and correctly demonstrates compliance with all relevant regulatory requirements. This may include review of the specific analyses, models, testing, or other activities that are used to demonstrate compliance with regulatory requirements. Compliance may be judged based on factors such as usage of guidance documents prepared by the regulator, implementation of accepted consensus codes and standards, alignment with previously accepted regulatory precedent, or expert review and assessment of the specific safety basis. The regulatory burden and cost may vary significantly depending on regulatory staff expertise and the level of engineering detail in any licensing evaluation methods used to demonstrate compliance.

Regulatory staff evaluations occur at multiple levels to account of interface and interactions that may occur from the component to assembly to system levels. Use of engineering assumptions, while necessary, should be carefully evaluated to ensure that they are appropriate and align with the assumptions used in the development of Regulator Operating Limits. The depth evaluations required will vary depending on factors such as prior operating experience with the system, characterized uncertainties in the Understood Failure Limit for the system, proposed margin between Normal Operating Limits and Regulatory Operating Limits, and the risk significance of the system. Greater transparency on the expected burden of proof for demonstrated regulatory compliance can help ensure that applicant methods align with the expectations of regulators and designees.

Recent experience by the NRC in developing review plans for novel technologies have suggested relating the regulatory burden for demonstrating compliance with regulatory requirements to the risk significance of a system or requirements [52]. Systems with higher risk significance based on a probabilistic risk assessment or other probabilistic methods would be subject to earlier reviews and required to provide more substantial demonstration of compliance with relevant regulatory compliance. This risk-informed review process could have two benefits within the independent review based regulatory framework. First, it prioritizes regulatory staff focus on areas that, based on the risk metrics, are most significant to public health and safety. Second, it enables more explicit and efficient allocation of regulatory staff resources and helps minimize regulatory “churn” on low priority regulatory issues. This risk informed process could be beneficial to independent review based regulatory framework but would require prior risk evaluation or probabilistic assessments by applicants to act as a baseline for further analysis.

The review and evaluation process, while briefly summarized here, is a lengthy technical process as regulatory staff independently examine and evaluate applicant documents, and identify areas for further analysis or revision. While the responsibility for safety ultimately rests with the licensee, these technical reviews of applicant compliance are central to the regulator’s mission of ensuring safe operation and maintaining public confidence in the safety of regulated activities.

6.7.3 Performing independent evaluation of safety

The third characteristic of the independent review based regulatory framework is performing an independent evaluation of safety. The regulator may independently perform a limited set of analyses to verify the Understood Failure Limits and Normal Operating Limits proposed by the applicant. Other regulatory frameworks focus on evaluating an applicant’s demonstrated compliance with regulatory limits and regulators may evaluate use of engineering assumptions and methods as part of the application. This framework extends this review by enabling regulators to perform independent technical evaluations to assess all portions of the proposed safety basis. This may include repeating applicant calculations to spot check appropriate use of analysis methods or performing evaluations using alternative methods or codes to independently verify the regulatory conclusions associated with the results. The independent confirmatory evaluation of safety may require significant regulatory expertise and engineering effort to complete, depending on the depth of review, scope of analyses, and the evaluation methods selected for use.

Independent evaluations of safety are high risk – high reward characteristic of the independent review based regulatory framework. These evaluations are high reward due to the following opportunities:

- Independent assessment of applicant claims
- Identification of weaknesses or limitations in applicant evaluations
- Assess adequacy of existing Regulatory Operating Limits
- Improved understanding of mechanistic system behavior
- Transparency in regulatory process with public

These opportunities can all help improve the regulatory process by improving the safety basis developed by the applicant, refining the requirements implemented by the regulators, and increasing confidence and trust with the public. These opportunities, however, are also met with substantial challenges:

- Availability of adequate regulatory technical staff to perform evaluations
- Limiting evaluation scope and not fully duplicating design efforts
- Over reliance of applicants on regulators to identify design weaknesses
- Cost and schedule uncertainties associated with detailed analyses
- Focusing regulatory efforts of risk significant safety issues and not simply high visibility safety issues

These challenges, if not properly addressed, can result in an extensive review process that does not adequately address the safety and regulatory issues associated with a design. For novel technologies, lack of adequate regulatory technical staff may result in an application that the regulator cannot appropriately review or require significant applicant or external resources to train regulatory technical staff to perform evaluations.

Independent technical evaluations enable the regulator to validate safety claims made as part of the licensing basis for an activity. This independent evaluation can be extremely useful at ensuring public safety by serving as an additional check on the applicants engineering process and by allowing technical experts to focus on safety considerations absent other concerns. These independent evaluations can also become a liability for the regulatory process if the regulator does not possess adequate technical expertise to perform evaluation or if the processes associated with review are not appropriately controlled through policy, guidance, or management. Independent evaluations of safety are an invaluable part of the independent review based regulatory framework but must be appropriately used to ensure their role in an effective regulatory framework.

6.7.4 Reconciling review differences

The fourth and final characteristic of independent review based regulatory framework is reconciliation of differences between regulatory assessment and applicant assessment of safety, and alignment of the licensing basis with the Regulatory Operating Limits. The reconciliation and convergence process will vary depending on the quality of the application and the differences between the applicant's submitted evaluations and the results of the regulator's independent review. This process, if successful, results in a formal documentation of the safety basis of the application and confirmation of compliance with all applicable regulatory limits.

The limiting positive case for the independent review based regulatory process is the submission of a "perfect" license application – complete demonstration of compliance with applicable regulatory limits, adherence to regulatory guidance and accepted consensus standards, and appropriate use of analysis methods that can be fully verified using independent evaluation methods. In this hypothetical case, no additional reviews or analyses would be required from the applicant and the regulator's independent review could assess and document the compliance.

Regulatory guidance used by the NRC regulatory staff in their review of design basis accident analyses for advanced light water reactors provides a clear example of the type of material that would be appropriate to include in a technical assessment (e.g., Chapter 15.0.3 of the NRC Standard Review Plan)[53]:

> The review should document the staff's evaluation of the applicant's design basis accident radiological consequences analyses against the relevant regulatory criteria. The evaluation should support the staff's conclusions as to whether the regulations are met. The reviewer should state what was done to evaluate the applicant's submittal. The staff's evaluation may include verification that the applicant followed applicable regulatory guidance, performance of independent calculations, and/or validation that the appropriate assumptions were made. The reviewer may state that certain information provided by the applicant was not considered essential to the staff's review and was not reviewed by the staff. While the reviewer may summarize or quote the information offered by the applicant in support of its application, the reviewer should clearly articulate the bases for the staff's acceptance and conclusions.

This type of regulatory staff guidance clearly articulates the level of detail that may be used as part of the final assessment of a regulatory application. The results of the independent review serve as a formal record of an applicant's compliance with all relevant regulatory limits.

A "perfect" license application is the goal of all applicants and regulators, demonstrating complete understanding and compliance with relevant safety requirements. "Perfect" license applications, however, may not be submitted for a variety of reasons. Applicants may submit "imperfect" applications due to lack of available information, engineering or management errors, or differing technical understanding of what constitutes complete demonstration of compliance with applicable regulatory limits. Regulators may perceive an application as "imperfect" based on an incomplete mechanistic understanding of system behavior, limited experience with novel systems, or differing technical understanding of what constitutes complete demonstration of compliance with applicable regulatory limits. In almost any regulatory process, both the applicant and regulator may have some incomplete understanding that leads to conflict over application of regulatory requirements and demonstration of adequate assurance of safety. The goal of the reconciliation process is applicant and independent regulator convergence on a licensing basis that adequately satisfies all applicable Regulator Operating Limits and will result in safe operation.

Reconciling applicant and independent regulator technical opinions in a timely and effective manner (while maintaining independence) requires direct and transparent communication. Development and use of project specific licensing plans (similar to those explicitly used in an a delegated review based regulatory framework) can be extremely effective at establishing a clear pathway to demonstration of compliance with regulatory requirements. Pre-application interactions and discussions regarding acceptable licensing methods can be effective at establishing mutual understanding of application quality before application submission, helping ensure that the application meets regulator expectations. Open technical discussions during the review process between applicants and regulators can be invaluable in reaching technical consensus on open licensing questions but these discussions have certain inherent challenges. Regulators must be careful not to over prescribe application methods and ensure that the applicant maintains ownership over the safety and licensing basis. Regulators must also control the scope of the review discussions, seeking resolution that satisfies regulatory requirements without getting stuck in an endless cycle of regulator questions and additional analyses. Many of the lessons learned from initial NRC regulatory efforts with advanced light water reactors are relevant in the development of appropriate processes for this framework.

The reconciliation of differences between regulatory assessment and applicant assessment of safety is ultimately a negotiation process between parties as they seek adequate demonstration of compliance with regulatory requirements. Applicant and regulator technical expertise and communication are critical at ensuring timely resolution and, more importantly, ensuring full compliance with Regulatory Operating Limits. This process of independent review and analysis helps ensure the adequacy of applicant analyses and results in a formal documentation of the safety basis of the application and confirmation of compliance with all applicable regulatory limits.

6.7.5 Framework summary and compatibility with licensing evaluation methods

The independent review based regulatory framework enables a complete and independent regulatory review to ensure applicant compliance with regulatory limits and increase public confidence in the safety basis of high hazard activities. A full, independent, technical review can provide the greatest level of public assurance that a facility will comply with the applicable Regulatory Operating Limits. This framework is comprehensive, but high has a high regulatory burden requiring extended reviews of application materials by an expert technical staff that can critically evaluate the licensing bases arguments. Timely reviews require both a sufficient number of staff and staff with expertise in relevant topics – a challenge for the regulation of novel technologies where expertise is limit or in the approval of alternative regulator methods. Recruiting, training, and retaining an adequate regulatory staff, developing appropriate review processes, and ensuring high quality applicant documentation that support regulatory evaluations are all critical to an independent review based regulatory framework.

This framework facilitates full independent technical reviews of all applicant materials necessary to demonstrate compliance with regulatory requirements. Unlike the insurance based regulatory framework and the permit based regulatory framework that rely on simplified licensing evaluation methods to demonstrate compliance with Regulatory Operating Limits, this framework facilitates technical reviews of detailed licensing evaluation methods. These detailed methods may crediting of engineered safety features and operations to meet Regulator Operating Limits that otherwise would not be feasible using simplified licensing evaluation methods. This permits the regulation of higher hazard technologies that cannot be demonstrated through evaluation of inherent hazards alone. Use of detailed licensing evaluation methods, while effective at reducing engineering margin and enabling compliance with Regulatory Operating Limits, will significantly increase the regulatory burden, cost, and schedule associated with the regulatory process in an independent review based licensing framework.

The regulatory and organization costs associated with an independent review based regulatory framework are generally high due to the need for independent, technically adequate regulatory staff and review process. Costs and regulator effort associated with development of Regulatory Operating Limits are likely comparable to other regulatory frameworks. Initial development of the regulatory system again has high cost and regulator effort due to the need to recruiting, training, and retaining an adequate regulatory staff and to developing appropriate review processes. Once the framework is developed, the regulatory burden for both the regulator and the licensee remain high. Regulators are responsible for independent technical review of all portions of the safety basis, though the level of review detail may be able to vary based on the risk significance of the activity. Applicants are required to submit high quality applications that detail all relevant aspects of their safety basis and demonstrate compliance with relevant regulatory requirements. Discrepancies between the application and the regulator must be reconciled through negotiation and could require additional analyses, testing, or other system design changes. Total cost associated with the review process would likely scale with the methods used to demonstrate regulatory compliance. Complex licensing evaluations would require greater review than simpler licensing evaluations. The selection of appropriate demonstration methods that balance regulatory margin, regulator effort, application preparation effort, and other factors could be considered during the development of a licensing strategy.

The independent review based regulatory framework is compatible with all of the licensing evaluation methods described in Chapter 8. In general, use the use of less detailed licensing evaluation methods (e.g., worst-case release evaluations and maximum credible release evaluations) will require fewer regulatory resources for independent evaluations and resolution of regulatory questions, but require significantly more margin between the Understood Failure Limit, the Regulatory Operating Limit, and the Normal Operating Limit. Use of more detailed licensing evaluation methods (e.g., deterministic design basis evaluations and probabilistic design basis evaluations, and STPA) can result in less conservative designs but will require greater regulatory review resources.

This regulatory framework is the bounding approach for the regulation of high hazard technology. This framework has significant limitations, however, related to the timely regulation of novel technologies due to the time required to develop sufficient regulatory expertise to independently evaluate the licensing basis for an activity. Another significant limitation of this framework is its ability to scale regulatory activities with the number of applicants due to the need to complete independent evaluations of applications. Regulators can choose to either overstaff their workforce or understaff their workforce based on the expected variations in applications overtime. Overstaffing requires significantly more regulatory resources (and funding) to complete while understaffing requires delays in the regulatory process if the regulator is inundated with applications to review and a relatively fixed workforce. A regulator can also vary their workforce size through staff augmentation activities or hiring-firing cycles, but these activities could limit regulator expertise, work culture, and regulatory independence. Despite these limitations, this regulatory framework has proven extremely effective at ensuring the safety of highly regulated industries such as the commercial nuclear fission industry in the United States.

The use of an independent review provides the greatest degree of public assurance in the safety of a hazardous technology. Regulator staff performs independent technical reviews of all portions of the licensing basis on behalf of the public according to the mission of the regulator. For some regulators (e.g., FAA), this may require balancing public safety with operational considerations while for other regulators (e.g., NRC) this may result in public health and safety as the only consideration. The types of review and detail of the review will vary depending on the specific hazards, the Regulatory Operating Limits, and the licensing evaluation methods used to demonstrate compliance with the regulatory limits. This framework is an effective method for helping ensure compliance with regulatory limit through independent reviews but requires substantial regulatory resources and can be subject to cost and schedule delays if not properly managed by the regulator and communicated with the applicants.

6.7.6 Impacts of regulatory framework on commercial fusion regulation

The independent review based regulatory framework represents the conventional method to ensure the safety of potentially high hazard industries. Technical reviews by regulator staff, with expertise in the subject matter area, acting on behalf of the public is viewed by many as the only framework by which accurate assessments of safety can be made due to commercial pressures on industry. This process provides for the full regulatory review of commercial fusion facility design, operations, and safety compliance with Regulatory Operating Limits. A comprehensive technical review can help assure the public of the safety of commercial fusion facilities and increase trust in the safe operation of facilities but comes with substantial regulatory burden. There are two main impacts of this regulatory framework on the development of commercial fusion facilities: the challenge of developing an independent regulator and availability of technical staff to perform reviews, and the regulatory burden associated with independent reviews.

The first major challenge of the independent review regulatory framework is development of an independent regulator and availability of adequate technical staff. The history of initial regulatory process development for commercial fission (Section 6.6.7) highlight the challenges associated with performing complete technical reviews for a novel technology. Recruiting, training, and retaining technical staff to perform independent reviews for first generation commercial fusion facilities may be challenging due to limited expertise with the technology. Finding scientists and engineers with sufficient technical experience to perform independent reviews not already employed by universities, laboratories, or private companies may be difficult or costly when creating an independent regulator.

Technical staff with tangential experience in science and engineer can be recruited and trained to perform technical reviews for commercial fusion, but this development process will require time, funding, and the regulatory staff will ultimately have less relevant experience than their counterparts in the commercial fusion industry. This experience differential may lead to inadequate independent technical reviews if regulatory staff cannot appropriately evaluate applications or lengthy (and costly) reviews as regulatory staff work carefully to evaluate applications and request more detailed regulatory substantiation from industry to make up for a technical experience deficiency. These processes can be overcome to develop an independent review regulatory framework for commercial fusion but require both substantial time and funding to ensure that staff are adequately prepared for timely and accurate independent reviews and that regulatory structures and guidance have been developed to ensure a high quality, reliable independent regulatory review process. Determining the funding mechanisms for this regulatory framework (i.e., applicant funded, public funded, joint funded) would be a difficult policy question depending on the scope and costs of the final framework.

The second major challenge of the independent review regulatory framework is the regulatory burden associated with independent technical reviews. The strength and weakness of the independent review regulatory framework is that all portions of an applicant's safety basis used to demonstrate compliance with Regulatory Operating Limits are reviewed and evaluated. The time and effort associated with the regulatory review process will vary, in part, based on the licensing evaluation methods used by the applicant to demonstrate compliance. The different licensing evaluation methods discussed in Chapter 8 have impacts on the design, operation, and analysis methods that can be used to demonstrate compliance with Regulatory Operating Limits. Commercial fusion facilities that utilize simple licensing evaluations to demonstrate compliance (i.e., worst case release, maximum credible release) may find that the regulatory burden associated with a small number of evaluations are minimal in an independent review regulatory framework. Commercial fusion facilities that choose to use more complex licensing evaluation methods (i.e., design basis event, probabilistic basis event, STPA) may require substantial regulatory reviews due to the number of assessments and evaluations that are required as part of those evaluation methods.

An independent review regulatory framework is well position to provide oversight on commercial fusion facilities that rely on engineering safety features or complex licensing evaluation methods to meet Regulatory Operating Limits, but these reviews come at a cost. The regulatory burden includes preparing application documentation for review, responding to independent review comments, providing responses or revisions to application materials, and working with regulators to determine acceptable resolution on technical questions. This burden can be costly due to the technical expertise required on both sides and potential delays to schedule due to sometimes lengthy technical resolution processes. Commercial fusion facilities within an independent review regulatory framework must assess if the design and operational advantages associated with more complex evaluation methods are worth the increases in regulatory costs and potential schedule delays.

The independent review based regulatory framework enables complete regulatory review of commercial fusion facilities and validates compliance with regulatory limits. This regulatory framework has been effective at enabling the safe operation of commercial fission facilities, and would be considered the "gold standard" for regulation of commercial fusion technology. The independent review based regulatory framework provides full public oversight of hazardous technologies and build trust through transparency. This regulatory framework requires substantial technical expertise to adequately operate and regulators would need to ensure that regulatory staff is adequately prepared to independently review novel fusion technologies. These processes could be costly and time consuming for regulators and the commercial fusion industry and represent a substantial regulatory burden on the emerging industry. The precedent set by the regulation of commercial fission facilities using an independent review based regulatory framework may makes use of this framework politically favorable, but the regulatory burden associated with developing and performing independent reviews for commercial fusion facilities may make this framework economically unfavorable. The independent review based regulatory framework is based on decades of regulation of commercial fission technology and could minimizing regulatory, policy, and safety questions related to the development of commercial fusion technology.

6.8 Operational characterization based regulatory framework

The fifth and final regulatory framework reviewed is an operational characterization based regulatory framework. This framework emphasizes the deliberate and gradual development of operational experience of novel, complex technologies while avoiding operational conditions that may lead to catastrophic losses. Open sharing of operational experience is required to allow for the characterization of the safe operational space for the new technology. The regulator permits greater operational flexibility as lessons learned from increased operational experience is gained and boundaries of the true failure limit envelope are identified through experienced failures.

The main purpose of this regulatory framework is to allow for the accelerated development and deployment of complex, novel technologies through the cooperative and deliberate identification of safe operational envelopes and catastrophic failure pathways. This framework has high initial regulatory burden for both facilities and regulators but is intended to reduce long-term regulatory burden through the better characterization and understanding of safe facility operation.

This regulatory framework is intended to accelerate the development of deployment of novel, complex technology by collaboratively working with technology developers and regulators (as representatives of the public) to characterize safe design and operational regimes. This framework is based on three assumptions regarding system safety:

- Safety for complex systems is a characteristic of the system and not of individual components. Safety cannot be measured or ensured on a individual basis – it is an observed emergent behavior of system interactions [8].
- Safe design requires detailed knowledge of the physical behavior and interaction modes of complex systems. For sufficiently complex systems, this cannot be determined *a-priori* and knowledge must be gained from experience [54].
- Safe operation requires operator knowledge of system behavior and the rational for the system limits the range of comfortable operation is based on experience and physical intuition for a machine. Operator knowledge and intuition for the system is necessary to help ensure that limits observed and that the system is kept in safe operating states [55].

These three assumptions create a paradoxical regulatory challenge for novel complex technologies, especially those with high inherent hazards. A technology cannot be widely deployed until it is demonstrated that it does not pose an unacceptable risk to the public but it cannot develop the engineering and operational basis necessary to validate the safety case without operating experience. Both over-regulation and under-regulation of novel technologies may threaten long-term commercial viability by either hampering development or by failing to prevent harm to the public. Clearer definition of regulatory activities can help clarify and resolve this paradoxical deployment challenge.

Regulators are often tasked with protecting public, workers, and the environment against both chronic and acute hazards. Acute hazards occur when a single operational failure or instance can cause significant harm. Chronic hazards occur when operational culture and facility design lead to the build up of significant harm over time. While both hazards are important to control based on historical experience (e.g., acute radiation exposure from industrial sources and chronic radiation exposure from uranium mining wastes), the time scales to address and mitigate each hazard are extremely different. Chronic hazards, depending on the hazard levels, may be controlled and remediated over a period of days to years without resulting significant harm to the public or the environment. Acute hazards, comparatively, cause harm as soon as the public is exposed so the focus must be on elimination, prevention, or planned mitigation of the acute hazard.

A regulatory system should be designed to separate these two hazards and treat them differently. A regulator should be tough on chronic harm because it should be within the control of the facility and if they cannot meet the regulatory limits then they should not be operating. A regulatory framework should be tough but collaborative on acute harm due to the challenge of characterizing the True Failure Limit for a novel technology. A regulator should:

- Ensure public safety by assessing whether the harm is appropriately bounded and that the imposed risk is proportional to the societal benefit
- Ensure that the facility meet all chronic harm levels to the public
- Ensure that acute harms are properly managed through design and operations

For a novel complex technology, the assessment of acute harms is challenging due to likely high uncertainty on the Understood Failure Limit. The True Failure Limit for similar activities is not well characterized through operation and experienced failure. Operators may have a broad or narrow Operator Comfort Limit depending on their individual operating experience and other safety culture characteristics. The Operator Comfort Limit may not always exist below the Understood Failure Limit or the True Failure Limit if the operators have a different characterization of the safety of the novel complex technology.

Depending on the specific activity and hazards, any implemented Regulatory Operating Limit and Normal Operating Limit may be set well below the Understood Failure Limit with significant margin to account for the significant uncertainties related to the novel technology. This process of defining limits with significant margin has several challenges. First, it may over constrain design and operating by preventing operating points that are well outside of the True Failure Limit. Second, limiting operating experience through excessively conservative margin may prevent development of mechanistic and operational experience that can help better characterize the system interaction and behavior. Limiting experience may result in Understood Failure Limits that are non-conservative and are exceeded by the True Failure Limits, especially under off-normal or infrequent operating conditions. Building operational experience through controlled and documented failures is key to understanding system safety. Finally, impeding development of operational experience prevents that development of adequate Operator Comfort Limits. Better characterization of system behavior and operator understanding of interactions and limit bases can enable development of Operator Comfort Limits that better reflect the Understood Failure Limit.

Improved operation is only viable through experience in conditions that allow for exploration of the operational envelope to identify complex system behavior, interactions, and conditions across a wide array of factors. The real operational envelope consists of all possible permutations of factors. For sufficiently bounded and simple systems that is mechanically understood, identification of factors, interactions, and system behavior may be possible theoretically, enabling development of a closed form solution of the parameter space. This allows for a development of a high confidence Understood Failure Limit without additional extensive testing of the actual system. For a poorly or unbounded system with complex interactions or a system that is not fully mechanistically understood, identification of all factors and evaluation of the combinatorial permutation space of factors to develop a similarly closed form solution of the parameter space may be impossible. While it may be possible to identify bounding factors that allow for collapse of operational envelope (e.g., mechanistic maximum or minimum values), complex system interactions can often invalidate assumptions regarding bounding conditions across all possible factors.

Rather than trying to ensure *a priori* that a novel technology is safe through definition of extremely conservative regulatory limits, the regulatory requirements and evaluations used to assure safety could develop alongside the technology but with an emphasis on preventing catastrophic acute hazard. Table 6.1 highlighted how unexpected failures occur, in large part, due to inadequate Understood Failure Limit and inadequate operator (or operational controller) understanding of system operation and an inappropriately high Operator Comfort Limit. Deliberate incorporation of operating experience, precursor events, and observed failures into the collective Understood Failure Limit of a novel technology will help improve the accuracy of the Understood Failure Limit, enabling development of effective Regulatory and Normal Operating Limits as well as development of appropriate Operator Comfort Limits.

An operational characterization based regulatory framework is developed and proposed in this section to enable the accelerated development and deployment of complex, novel technologies through the cooperative and deliberate identification of safe operational envelopes and catastrophic failure pathways. The operational characterization based regulatory framework has the following six characteristics:

- Transparency and sharing of operating experience
- Identification of catastrophic acute operating points
- Collaborative development of operating limits and licensing assessments
- Explicit characterization of margin and uncertainties
- Focused development of operating experience to reduce uncertainties
- Continuous revision of operating limits to incorporate operating experience

These characteristics are intended to create an open regulatory framework where operators can cooperatively develop the operating experience necessary to identification of safe operational envelopes and catastrophic failure pathways. Transparency is key to this regulatory framework due to the trust required between stakeholders. Facilities must believe that regulators will be willing to reduce regulatory requirements based on operating experience, regulators must believe that facilities are providing complete information on facility safety, and the public must believe that facilities and regulators are both acting in good faith to ensure that they meet and exceed the minimum level of safety.

6.8.1 Transparency and sharing of operating experience

The first characteristic of operational characterization based regulatory framework is transparency and sharing of operating experience. Development of adequate limits requires characterization of system conditions, performance, behavior, and interactions.

Unexpected system failures (especially catastrophic failures) rarely occur without similar precursor events that did not ultimately result in failure. These individual near misses may not be appreciated by facilities as important operational experience that changes the broader characterization of system safety. The major mechanical failure that contributed to the 1979 accident at the Three Mile Island nuclear power plant (stuck open pressurizer pilot operated relief valve) was experienced under nearly identical conditions at the Davis

Besse nuclear power plant 18 months earlier but different operator response prevented a system failure [56]. Identification and communication of known failure modes was an important finding in the wake of the Three Mile Island accident. Creation of the Institute of Nuclear Power Operations (INPO) was an important step in standardizing sharing of operating experience in the commercial fission industry.

Characterization and tracking of operating experience helps develop better mechanistic models of system behavior and system interactions, as well as identification of relevant plant conditions and parameters. Early industry-government research programs lead by the AEC for first generation of fission plants and industry operational experience programs lead by INPO have helped better characterize the safe operation of fission plants in the United States. Lapses in industry focus have contributed, in part) to major near-misses in the U.S. commercial nuclear industry including the 1990 Vogtle loss of offsite power event and the 2002 Davis Besse reactor vessel head corrosion incident [57]. Preemptive development of an operating experience organization could help develop appropriate system understanding before a catastrophic unexpected failure reveals knowledge gaps related to system performance.

Development of an effective organization to collect, distill, and disseminate operating experience is fundamental to operational characterization based regulatory framework. The main challenge facing this organization would be the need for full transparency with facilities. Much operating experience and lessons learned from operation may not reflect well on a facility. Poor design, operation, maintenance, or overall safety culture may all be partial root causes in near-miss events. Organizations and operators may not be keen on documenting and sharing events that reflect their own deficiencies. Public disclosure of these events could result in reputational harm, litigation, regulatory penalties, or other commercial consequences such as protecting trade secrets or other confidential, competitive, or business sensitive information. Review of these events, however, is critical to better understanding system operation.

As a result, the responsible organization will need to develop processes that incentivize the transparent sharing of all operating experience and events. Strict confidentiality agreements have been used by organizations like INPO to encourage transparent sharing of operating experience between members without external disclosures to the public, governments, or regulators [58]. This model facilitates industry sharing of operational experiences (with some experience shared with the regulators) but is opaque to the public. Public groups have sued utilities and the NRC for access to INPO collected operating experience under public records law but were unsuccessful [59]. Developing a organization that can adequately collect, distill, and disseminate operating experience while addressing the challenges related transparency and disclosure is a key facet of operational characterization based regulatory framework.

6.8.2 Identification of catastrophic acute hazards operating points

The second characteristic of operational characterization based regulatory framework is identification of catastrophic acute hazards operating points. Development of operating experience to improve mechanistic understanding of system behavior and interactions is only possible if on-going operations do not constitute an undue risk to worker, public, or environmental safety.

Catastrophic acute operating points are those operating points that lead to the rapid, unmitigated release of facility hazards that may cause significant irreparable harm to workers, public, or the environment. The goal of this operational characterization based regulatory framework is to more accurately characterize the operational space to ensure that facility operations do no intersect with these operating points. Catastrophic acute operating space cannot be fully characterized *a priori* for a novel technology, so potentially catastrophic hazards should be identified based on related operating experience, mechanistic models, and conservative analyses to characterize what operating points are expected to result in harm.

Quantification of hazards and potential harms can be useful for assessing what conditions or factors can be used to help assure non-catastrophic operating points given limited operating experience. Identifying factors such as hazard inventories (e.g., Curies of radiological material) or operating conditions (e.g., operating temperature or pressure) can be used at assessing when catastrophic harm may occur. These factors can be use to help identify uncertainties or other limits that should be reviewed to help ensure safe operations.

6.8.3 Collaborative development of operating limits

The third characteristic of operational characterization based regulatory framework is collaborative development of operating limits. Development of adequate limits requires accurate mechanistic understanding of system behavior and interactions and application of limits that provide appropriate assurance of safe operation. Collection of operating experience is critical to understanding of system behavior, but using the data to build accurate mechanistic models and identify uncertainty is required to develop adequate limits. A collaborative, open process can help ensure the developed operating limits clearly reflect the best mechanistic understanding of system behavior and interactions, while still ensuring that facility operating will not permit catastrophic, acute operating points.

There are four relevant limits that need to be defined for an activity or facility:

- Understood Failure Limit – developed through best understanding of activity
- Regulatory Operating Limit – developed by regulator with uncertainties
- Operator comfort limit – developed by operators with operational experience
- Normal operating limit – developed by facility to sustain operational uptime

Each limit has different stakeholders and goals that need to be considered when developing the limit. While the limits could be developed independently (by the regulator, different operators, and different facilities), collaborative development by stakeholders allows for explicit handling of conservatisms between limits and use of consistent assumptions regarding mechanistic models.

Development of Understood Failure Limit in this regulatory framework is important because it serves, in part, as the basis for the Regulatory Operating Limit and the Normal Operating Limit. Collaborative characterizations of Understood Failure Limit by stakeholders allows for incorporation of all operating experience, expertise, and perspectives. Development of different Understood Failure Limits by different stakeholders can lead to conflict as their assessment of margin between operating limits and their Understood Failure Limit may different significantly. Stakeholders collaborating explicitly on characterization and development of an Understood Failure Limit for a novel technology (and the associated mechanistic models) could help create a limit that best describes the True Failure Limit. Development of the other limits (Regulatory, Operator, and Normal) can be lead by the specific stakeholder group, but consultation with other stakeholders may provide additional insights useful to the limit that would not have otherwise been incorporated into the limit.

6.8.4 Explicit characterization of margin and uncertainties

The fourth characteristic of operational characterization based regulatory framework is explicit characterization of margin and uncertainties. One of the major challenges with development of operating limits for activities with multiple sets of operating limits is an un-quantified build up of engineering margin, uncertainties, and assumptions from the Understood Failure Limit through the Normal Operating Limit.

The un-quantified build up may have several negative consequences on operational safety. First, the accumulation of implicit margin between operating limits may lead to excessive conservatism that inhibits normal facility operation in operational spaces that are otherwise safe. Second, operators working with excessively conservative limits may begin to disregard the importance of limits based on the observed margin during normal operations. This operational deviation may result in operating points outside of the Normal Operating Limits or Regulatory Operating Limits. Third, use of inconsistent assumptions between operating limits may lead to the invalidation of assumptions used in the definition of other operating limits. For example, use of bounding mechanistic values in the development of one operating limit may result in unrealistic conditions for another operating limit. Finally, characterization and quantification of uncertainties is important to the development of more accurate operating limits. Identification of sources of uncertainty that result in additional margin as part of the limit development process enables systematic quantification and reduction of uncertainty.

6.8.5 Focused development of operating experience to reduce uncertainties

The fifth characteristic of operational characterization based regulatory framework is focused development of operating experience to reduce uncertainties. The prior characteristics of the regulatory framework have focused on developing initial operating limits that exclude operation at acute catastrophic operational points while identifying the uncertainties and resulting margin on operating limits. These characteristics help build a safe operational envelope that facilitates development of operational experience to better characterize safe operational points, build mechanistic understanding of the system, and define True Failure Limits.

Development of operating experience to better characterize the operational space may be performed in a number of methods including:

- separate and integrated effects testing,
- staged facility start-up testing,
- normal facility operation with limited performance conditions,
- normal facility operation with additional controls and instrumentation, and
- potentially destructive controlled limit testing of partial or full facilities

All of these methods had been previously conducted to support the development to operating experience with commercial fission reactors [60]. Each of methods has trade-offs in terms of applicability of the collected operating experience to development of mechanistic models and reduction of uncertainty. Complete system testing may provide the highest quality operating experience to support limit development or reduce uncertainties but could have significant acute catastrophic hazards or have high costs or timelines to complete. Separate and integral effects testing may be a cost and time effective method to generate operating experience by may not fully characterize system behavior and interactions. This regulatory framework aims to deliberately develop operating experience to reduce uncertainties and better characterize the safe operational spaces.

This regulatory framework characteristic differs from prior methods for reducing uncertainties and gaining operational experience in two distinct ways: the collection development of operational experience and prioritizing limited operation without complete safety cases.

The first major difference reflects the challenges associated with the design and operation of novel, complex, commercial systems: cost and commercial competiveness. For many companies, operational experience and data can provide valuable engineering insights that develop in commercially competitive advantages. The development of operational experience may also come at a significant cost (e.g., full-scale testing), so companies are incentivized to maximize the financial returns associated with operating experience and testing. In a collaborative operational characterization based regulatory framework, operating experience is collectively used to establish a safe operating envelope for a novel technology and better characterize the True and Understood Failure Limits. As a result, incentive structures would need to be developed for the regulator to encourage development of relevant operating experience that can benefit technology operations.

The second major different reflects the challenges faced by private commercial firms pursuing the development of high capital cost projects. Developing a complete safety case for a novel technology without any prior operating experience may either require substantial pre-application testing to privately develop operating experience sufficient to support licensing or use of extremely conservative *a priori* limits to enable licensing without operating experience. Both of these approaches are extremely economically limiting, resulting in extremely costly and lengthy development cycles before initial commercial deployment or commercial deployment of extremely limited capability facilities. This regulatory framework intends to enable partial initial facility operation given protections against catastrophic acute operating points with transition to full facility operations after sufficient operating experience from the facility and other operations provide adequate assurance of safe operation.

The focused development of operating experience to reduce uncertainties in this framework is a collaborative effort as regulators, developers, and operators all seek to better characterize system behavior and interactions. Identification of uncertainties for reduction through operating experience should balance both their importance to overall safe operation as well as the cost and effort of developing the operating experience. Balancing the priorities of different stakeholders is important when determining how to prioritize testing. Creating appropriate frameworks to share the costs (and benefits) associated with developing operating experience would also be a challenge associated with this regulatory framework. Historical experience with commercial fission technology suggests a potential role for government funding of large testing programs that provide critical operating data.

Overall, this framework characteristic is particularly important for novel technologies where operating experience is key to characterization of economically viable operating limits, and the cost and timelines associated with individual company development of operating experience is commercially infeasible.

6.8.6 Continuous revision to incorporate operating experience

The sixth and final characteristic of operational characterization based regulatory framework is continuous revision of operating limits to incorporate operating experience. The other main characteristics of this regulatory framework focus on developing operating experience and reducing the uncertainties associated with operating limits and mechanistic models of system safety. This operation experience is only useful if it is actively incorporated into the operating limits associated with the facility. Revision of operating limits is key to preventing unexpected failures, reducing unnecessary conservatisms, and improving overall system operations.

Development and review of operating experience is essential for the revision of Understood Failure Limits. Operating experience includes physical conditions, operator conditions, environmental conditions, or any other factors that lead to safe, degraded, or failed system operation. This information, if studied and reviewed, can provide important insights improve or revise mechanistic models of system behavior, provide information on bounding system conditions, or enable identification (or verification) or important factors or system interactions. Operating experience is observation of the True Failure Limit (or it's conceptual inverse – a True "Operational" Limit), so capturing this information to improve Understood Failure Limits and develop more accurate representations of True Failure Space is important to avoiding unexpected failures. The degree of revision to the

Understood Failure Limit will depend significantly on quality of the operating data and the insights gained by the experts who study and review it.

Revising and improving Understood Failure Limits is critical because they serve, in large part, as the basis for the Regulatory Operating Limit and the Normal Operating Limit. These limits should be updated as operating experience provides better insights into True Failure Limit and enables updates to the Understood Failure Limit. These updates may include changing numerical limits based on new data (reflecting constant desired margin or changes to the desired margin), including the effects of identified sources of uncertainty or newly quantified uncertainty, or include new factors or system interactions that are important to safe operation. The basis and assumptions for the Regulatory Operating Limits and Normal Operating Limits should be reviewed, with revisions made to main consistency with the better understanding of safe system operation.

It is important to note that development of operating experience may result in increases or decreases to operating limits. While these changes may be perceived as increase or decreases to system safety, these changes are more accurately adjustments to maintain the initial assumptions and meet the overall safety objectives of the regulatory framework. This characterization is important to clarify that the revision process is not a loosening or ratcheting of regulatory requirements but rather a more accurate assessment of safe operating points. Stakeholders should facilitate increases and decreases in operating limits, with groups resisting the urge to maintain additional margin "just to be safe" or prevent addition of margin "because it's already been operating safely". The adjustments are critical to preventing unexpected failures and enable the safe operation of a novel technology.

Operator Comfort Limits will also vary with increases operating experience, although they vary in a much less controlled manner than other operating limits. Operator perception of the importance of different operating experiences (industry, facility, industry experience), different operating limits (Understood Failure, Regulatory, Normal), and specific operational factors (management pressures or other factors) will all affect the Operator Comfort Limit. Working with operators (or updating operator controllers) to incorporate updated operating experience into their conceptual process models is critical to ensuring safe operation. Dissemination of operating experience, ensuring operating understanding of changes to Understood Failure Limits, and understanding facility organizational conditions should all be considered when facilitating the continuous revision of Operator Comfort Limits.

The deliberate, continuous revision of operating limits to incorporate operating experience is the most important characteristic of this regulatory framework. Incorporation of operating experience allows for the characterization of the safe operational space for the new technology, changing based characterization of operating experience and not just changing after catastrophic acute system failures that spur regulator action on system safety.

6.8.7 Framework summary and compatibility with licensing evaluation methods

The operational characterization based regulatory framework enables the accelerated development and deployment of complex, novel technologies through the cooperative and deliberate identification (and revision) of safe operational envelopes and catastrophic failure pathways using operating experience. Regulatory assessments used as a part of this framework can vary based on the technology and hazards, but the revision of the methods and limits based on better characterization of safe facility operation is key. Processes for the transparent collection of operating experience, collaboration on the development of operating limits and identification of uncertainties, and the continuous revision of operating limits based on operating experience are all designed to help characterize safe operation and prevent catastrophic acute accidents for novel technologies.

This framework is a transparent and collaborative approach to novel technology safety – all operating experience is available for review to help better characterize safe operating points and avoid catastrophic, acute events. The main goal of this regulatory framework is to develop operating experience that enables better characterization of system behavior and interactions, improving the Understood Failure Limit and reducing the potential for unexpected system failures. This improved understanding of system behavior and safe operation allows for development of more appropriate operating limits, reducing unnecessary margin and enabling more efficient system design and operation. A collaborative process with clearly defined margin and uncertainties enables functional independence between regulators and industry. This framework, however, requires collaboration between regulators, industry, and the public and involves a level of corporate transparency rarely seen in commercial operations.

The regulatory and organizational costs and challenges associated with an operational characterization based regulatory framework may be significant. Creation of an organization (private or public) to facilitate sharing and review of operational experience would be a significant effort. Questions such as confidentiality of operating experience, liability questions related to operating events, protection of business sensitive information, and precise role (integrated with or separate from the regulator) still unanswered. Managing development of operational limits in the litigious U.S. regulatory environment may be challenging, as different opinions on operating data and adequate protection become legal questions and not simply technical or social questions. Definition of processes to incorporate operating experience and share the costs associated with reduction of uncertainties would need to be addressed for this regulatory framework. While these questions would likely result in significant up-front regulatory costs, the framework is designed to enable the rapid development and deployment of technology as the operating limits and safety assessments can develop parallel to operating experience. This may reduce the overall regulatory timeline and result in long-term regulatory framework that more adequately characterizes the safe operation and prevents unexpected system failure operating points. This long-term regulatory framework relies, however, on sufficiently widespread technology deployment to justify the initial regulatory costs.

The operational characterization based regulatory framework is compatible with all of the licensing evaluation methods described in Chapter 8. The continuous development of operating experience for novel technologies suggests that licensing evaluation methods requiring less design and operational data (e.g., worst-case release evaluations and maximum credible release evaluations) may be most applicable for initial licensing evaluations. Use of more detailed licensing evaluation methods (e.g., deterministic design basis evaluations and probabilistic design basis evaluations) may be implemented over time, as increased operating experience provides insights into system behavior, interactions, and sources of uncertainty. Initial use of detailed licensing evaluation methods may not be beneficial in an operational characterization based regulatory framework due to the number of uncertainties related to system operation and performance. Use of STPA as a licensing evaluation method may be useful with or without operating experience due to the method's focus on identification of hazardous conditions instead of quantitative hazard assessment. This regulatory framework enables the selection of the evaluations that are appropriate for the specific condition and can evolve over time based on facility hazards, characterization of system behavior, and understanding of uncertainties and operating margin.

This regulatory framework mirrors the regulatory history of commercial fission in the United States – the gradual evolution of licensing evaluation and operating limits based on accumulated operating experience to ensure safe system operation. The changes in commercial fission regulation were often the regulatory reaction to acute catastrophic events or significant near-miss events, this framework seeks to formalize the collection and evaluation of operating experience to minimize unsafe operating points. Explicitly including revision of operating limits based on operating experience provides a mechanism to reduce regulatory conservatism while still maintaining the intended level of safety based on improved understanding of system safety. This process enables more rapid development of novel, high hazard technologies by establishing regulatory limits and processes that evolve with the operational maturity and understanding of the technology.

6.8.8 Impacts of regulatory framework on commercial fusion regulation

The operational characterization based regulatory framework represents a collaborative development based approach to commercial fusion safety. Major accidents rarely occur in highly engineered due to foreseen circumstances or discrete mistakes in engineering analyses – they result from system interactions. Characterization of system interactions and improved understanding of mechanistic behaviors through development of operating experience helps better identify failure mechanisms, quantify engineering margin, and establish safe operating limits to prevent catastrophic acute operational failures for commercial fusion facilities. This framework enables the collaborative development of this operating experience and creation of safe operational envelopes based on characterization and reduction of uncertainties in operational limits. There are two main impacts of this regulatory framework on the development of commercial fusion facilities: the impacts of complete operational transparency on business considerations, and assuring regulatory independence and prioritization of safety in a collaborative regulatory framework.

The first major challenge of the operational characterization regulatory framework is the impacts of complete operational transparency on business considerations for commercial fusion facilities. This regulatory framework relies on transparency in sharing operating experience and lessons learned to better characterize the operational failure limits for novel commercial fusion technology. This transparency, however, may come with business challenges for commercial fusion facilities. The first challenge is that operational experience is valuable only if significant technical and operational details are shared to provide more accurate characterization of system behavior. These details, however, may reveal trade secrets or other business sensitive information that a company would not wish to publically disclose for competitive reasons. The second challenge is that operational experience does not always reflect well on a company's corporate image. Operational experience related to failures in operations, maintenance, quality assurance may lower public perception or trust of a commercial entity, but capturing non-engineering lessons learned are important to contextualizing complex system operation. The third challenge is that transparency may introduce potential social, civil, or criminal liability for individuals or corporations for system failures and operational decisions that would normally be handled internally.

Each of these challenges could discourage companies from fully participating in the transparent sharing of operational information critical to this regulatory framework. Organizations such as INPO and reactor vendor owners groups have addressed this challenge through strict confidentiality policies related to shared operating experience, but integration of this open culture with a public regulator could be a significant challenge. Commercial fusion facilities would need to carefully consider business considerations when developing processes and limits for sharing operating experience transparency with the regulator, other technology developers, and the public.

The second major challenge of the operational characterization regulatory framework is assuring regulatory independence and prioritization of safety in a collaborative regulatory framework. In this framework, the commercial fusion industry would work collaboratively with the regulator to characterize operating experience, create regulatory operating limits, and develop operational experience through planned operational and testing programs. This collaborative regulator-industry relationship, however, appears more similar to the relationships between the AEC and early commercial fission facilities than between the NRC and current commercial fission facilities. Concerns related to the independence of the regulators and the potential for regulator capture due to the close collaboration may arise [47]. The regulatory framework is based on characterization of operating experience to ensure safe operation, but regulators and industry will ultimately have to address questions of adequate safety that could impact the economics of commercial fusion facilities (e.g., requirements on system redundancy or engineering margin). The regulatory framework is collaborative but processes to maintain regulator independence, ensure prioritization of safety in regulatory decision making, resolve differences of professional opinion, and maintain public trust will be critical to the success of the regulator.

The operational characterization based regulatory framework enables the collaborative development of operational experience and system understanding to better characterize the safe operation of novel commercial fusion facilities. This framework requires operational transparency from industry with the public but enables the more rapid development of operating experience needed to support mature regulatory requirements without excessive conservatisms. Deliberate development of operating experience, identification and reduction of uncertainties, and a continuous focus on incorporation of lessons learned can help commercial fusion technology rapidly mature by leveraging industry wide expertise and experience. The operational characterization based regulatory framework enables more rapid development of novel, high hazard technologies such as commercial fusion by establishing regulatory limits and processes that will evolve with the operational maturity and understanding of the technology.

6.9. Use of hybrid regulatory frameworks

This work describes five different regulatory frameworks that can be used to ensure the safe operation of hazardous facilities. While use of a single regulatory framework for a facility may reduce organizational overhead associated with regulatory processes, the presence of different hazards at a facility may incentivize use of multiple different regulatory frameworks to minimize overall regulatory burden. This hybrid regulatory framework approach can facilitate selection of appropriate regulatory frameworks for different groups of hazards hazards and use of licensing evaluation methods that minimize the regulatory costs and time.

This hybrid regulatory approach also reflects the jurisdictional reality of operation of many hazardous facilities. The design, construction, operation, and decommissioning of high hazard facilities or activities are rarely regulated solely by a single agency or organization. Regulation of hazards is often jurisdictional, with regulatory authority separated by location (local, regional, national, international) and by hazard (environmental, worker safety, radiological). This piecewise approach to safety regulation largely reflects the historical development of regulatory requirements on different hazards and facilitates organizational focus on specific hazards. There are very few “green-field” regulatory environments where all relevant regulatory requirements for a technology or process will be created simultaneously without consideration or inclusion of existing applicable regulatory requirements.

The reality of regulatory jurisdictions and the theory of minimizing regulatory burden both result in the common use of hybrid regulatory frameworks for regulation hazardous facilities and activities. The commercial fission industry is subject to a patchwork of insurance based regulatory frameworks (e.g., operational insurance requirements under Price-Anderson), permit based regulatory frameworks (e.g., non-radiological environmental requirements), independent review regulatory frameworks (e.g., nuclear safety requirements from the NRC), and
operational characterization based regulatory framework (e.g., operator requirements through INPO reviews). The hybrid regulatory framework resulting from overlapping regulatory jurisdictions and incremental changes to regulatory requirements have

facilitated safe operation of nuclear fission facilities but the lack of a cohesive regulatory strategy can result in regulatory gaps or conflicts.

Deliberate use of hybrid regulatory frameworks can enable the use of optimal regulatory framework for different types of hazards and hazard limits. Hazard limits can that be satisfied with simple licensing evaluation methods (e.g., inventory based limits) could be regulated using permit based regulatory frameworks. Other hazard limits requiring more detailed licensing evaluation methods (e.g., deterministic design basis event evaluations) could be regulated using compatible regulatory frameworks that facilitate more detailed regulatory reviews (e.g., independent review regulatory frameworks).

6.10. References

[1] J. Rasmussen. Risk management in a dynamic society: a modeling problem. Safety science, 27(2- 3):183–213, 1997.

[2] L. Shishkov, V. Gorbaev, and S. Tsyganov. Safety and design limits. 2007.

[3] F. S. D'Auria, H. Glaeser, S. Lee, J. Mi´ak, M. Modro, and R. Schultz. Best Estimate Safety Analysis for Nuclear Power Plants: Uncertainty Evaluation. IAEA Safety Report Series, volume 52. IAEA, 2008.

[4] Environmental Protection Agency. FY 2018-2022 U.S. EPA Strategic Plan. Technical report, Environ- mental Protection Agency, 2019.

[5] U.S. Department of Labor. FY 2018-2022 Strategic Plan. Technical report, U.S. Department of Labor, 2018.

[6] Federal Aviation Administration. FAA Strategic Plan FY 2019-2022. Technical report, Federal Aviation Administration, 2019.

[7] Nuclear Regulatory Commission. NRC Strategic Plan FY 2019-2022. Technical Report NUREG-1614, Vol. 7, Nuclear Regulatory Commission, 2018.

[8] N. G. Leveson. Engineering a Safer World. Massachusetts Institute of Technology, 2011.

[9] U.S. Department of Transportation - Office of Inspector General. Timeline of Activities Leading to the Certification of the Boeing 737 MAX 8 Aircraft and Actions Taken After the October 2018 Lion Air Accident. Technical Report AV2020037, Federal Aviation Administration, 2020.

[10] C. E. Cantu. Distinguishing the concept of strict liability for ultra-hazardous activities from strict products liability under section 402a of the restatement (second) of torts: Two parallel lines of reasoning that should never meet. Akron L. Rev., 35:31, 2001.

[11] S. Shavell. Liability for harm versus regulation of safety. The Journal of Legal Studies, 13(2):357–374, 1984.

[12] Financial Protection Requirements and Indemnity Agreements. 10 CFR Part 140, 2015.

[13] Nuclear Energy Institute. Position Paper: NRC Insurance and Liability Requirements for Small Reactors. June 2011.

[14] Nuclear Regulatory Commission. Backgrounder - Nuclear Insurance: Price-Anderson Act. NRC Accession Number ML032730606, April 2019.

[15] Lewis, D., Merrifield, J., and Fowler, S. Considerations in the Regulation of Fusion-Based Power Generation Devices. Pillsbury Winthrop Shaw Pittman LLP, November 2020.

[16] Nuclear Regulatory Commission. Consolidated Decommissioning Guidance: Financial Assurance, Recordkeeping, and Timeliness. Technical Report NUREG-1757 Volume 3, 2012.

[17] Restatement of the Law (3d) of Torts—Liability for Physical and Emotional Harm. American Law Institute, 2010.

[18] K. Beins and S. Lester. Superfund: polluters pay so children can play. Center for Health and Environmental Justice, Church Falls, VA, 2015.

[19] Energy Information Administration. Wholesale U.S. electricity prices were generally lower and less volatile in 2020 than 2019. https://www.eia.gov/todayinenergy/detail.php?id=46396, 2021.

[20] Energy Information Administration. Annual Energy Outlook 2021. Technical Report AEO2021, 2021.

[21] M. S. Peters, K. D. Timmerhaus, R. E. West, et al. Plant design and economics for chemical engineers, volume 4. McGraw-Hill New York, 2003.

[22] B. Sorbom, J. Ball, T. Palmer, F. Mangiarotti, J. Sierchio, P. Bonoli, C. Kasten, D. Sutherland, H. Barnard, C. Haakonsen, et al. Arc: A compact, high-field, fusion nuclear science facility and demonstration power plant with demountable magnets. Fusion Engineering and Design, 100:378–405, 2015.

[23] OECD (Organization for Economic Cooperation and Development). Guiding Principles of Effective Environmental Permitting Systems. Technical report, 2007.

[24] E. Biber and J. Ruhl. The permit power revisited: The theory and practice of regulatory permits in the administrative state. Duke LJ, 64:133, 2014.

[25] C. Copeland. Clean water act: a summary of the law. Congressional Research Service, Library of Congress Washington, DC, 1999.

[26] R. Webb and M. Taylor. EPA's Clean Power Plan: Implementation Options. 2015.

[27] Nuclear Regulatory Commission. Consolidated Guidance About Materials Licenses: Program-Specific Guidance About Possession Licenses for Production of Radioactive Material Using an Accelerator. Technical Report NUREG-1556, Volume 21, Nuclear Regulatory Commission, 2018.

[28] A. C. Roma and S. S. Desai. The regulation of fusion: A practical and innovation-friendly approach. Hogan Lovells, 2020.

[29] Rules of General Applicability to Domestic Licensing of Byproduct Material. 10 CFR Part 30, 2007.

[30] Nuclear Regulatory Commission. Backgrounder - Agreement States. NRC Accession Number ML20258A166, September 2020.

[31] Nuclear Regulatory Commission. A Regulatory Analysis on Emergency Preparedness for Fuel Cycle and Other Radioactive Material Licensees. Technical Report NUREG-1140, Nuclear Regulatory Com- mission, 1988.

[32] Environmental Radiation Protection Standards for Nuclear Power Operations. 40 CFR Part 190, 1977.

[33] Environmental Protection Agency. General Guidance on Risk Management Programs for Chemical Accident Prevention (40 CFR Part 68). Technical Report EPA 555-B-04-001, Environmental Protection Agency, March 2009.

[34] National Research Council and others. The use and storage of methyl isocyanate (MIC) at Bayer CropScience. National Academies Press, 2012.

[35] Nuclear Regulatory Commission. Safety Goals for the Operation of Nuclear Power Plants; Policy Statement; Correction and Republication. (51 FR 30028), 1986.

[36] Committee to Assess Health Risks from Exposure to Low Levels of Ionizing Radiation, National Research Council. Health risks from exposure to low levels of ionizing radiation: BEIR VII phase 2. National Research Council (US), 2006.

[37] Designated Engineering Representative (DER) Handbook. Number 8110.37F. Federal Aviation Administration, 2017.

[38] Federal Aviation Administration. Delegation and Designee Background. https://www.faa.gov/about/history/deldes background/, 2014.

[39] Airworthiness Standards: Normal Category Airplanes. 14 CFR Part 23, 2016.

[40] Federal Aviation Administration. Revision of Airworthiness Standards for Normal, Utility, Acrobatic, and Commuter Category Airplanes. (61 FR 5184), 1996.

[41] Official Report of the Special Committee to review the Federal Aviation Administration's Aircraft Cer- tification Process. Federal Aviation Administration, 2020.

[42] Nuclear Regulatory Commission. Revision of Fee Schedules; Fee Recovery for Fiscal Year 2020 . (85 FR 37270), 2020.

[43] H. Al-Lami, A. Aslam, T. Quigley, J. Lewis, R. Mercer, and P. Shukla. The evolution of flight control systems. Technology Development, System Architecture and Operation, 2015.

[44] J. S. Walker and T. R. Wellock. A Short History of Nuclear Regulation, 1946-2009. US Nuclear Regulatory Commission, 2010.

[45] J. S. Walker and G. T. Mazuzan. Containing the Atom: Nuclear Regulation in a Changing Environment, 1963-1971. University of California Press and U. S. Nuclear Regulatory Commission, Berkeley, 1992.

[46] OECD (Organization for Economic Cooperation and Development).Creating a Culture of Independence: Practical Guidance against Undue Influence, 2017.

[47] Choi, KS and Lee, YE and Chang, HS and Jung, SJ. Development of Checklist for Self-Assessment of Regulatory Capture in Nuclear Safety Regulation. In KNS Spring Meeting, volume 1, page 3, 2011.

[48] National Transportation Safety Board. Annual review of aircraft accident data: U.s. general aviation, calendar year 1970. Technical Report NTSB/ARG-74/1, 1974.

[49] National Transportation Safety Board. Aviation Accident Statistics. http://www.ntsb.gov/investigations/data/pages/aviation stats.aspx, 2020.

[50] Nuclear Regulatory Commission. NRC–Independent Regulator of Nuclear Safety. Technical Report NUREG-0164, Nuclear Regulatory Commission, 2012.

[51] G. T. Mazuzan and J. S. Walker. Controlling the Atom: the Beginnings of Nuclear Regulation, 1946-1962. University of California Press, Berkeley, 1985.

[52] Non-Light Water Review Strategy Staff White Paper. Nuclear Regulatory Commission, NRC Accession Number ML19275F299, September 2019.

[53] Nuclear Regulatory Commission. Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition. Technical Report NUREG-0800, Nuclear Regulatory Commission.

[54] R. I. Cook. How complex systems fail. Cognitive Technologies Laboratory, University of Chicago. Chicago IL, 1998.

[55] J. R. Chiles. Inviting disaster: Lessons from the edge of technology. Harper Business New York, 2002.

[56] J. G. Kemeny. Report of the President's Commission on the Accident at Three Mile Island: The Need for Change: the Legacy of TMI, volume 41. The Commission, 1979.

[57] J. Thompson. Significant Operational Experience: 7 Major Industry Events with Regulatory Implications. Number NRC Accession Number ML16006A288. Nuclear Regulatory Commission, 2016.

[58] R. F. Willard. The Role of the Institute of Nuclear Power Operations in Supporting the United States Commercial Nuclear Power Industry's Focus on Nuclear Safety. Institute for Nuclear Power Operations, 2019.

[59] Critical Mass Energy Project, Plaintiff, v. Nuclear Regulatory Commission, Defendant, Institute of Nuclear Power Operations, Defendant-Intervenor. Number 731 F. Supp. 554 (1990). United States District Court, District of Columbia., 1990.

[60] Nuclear Regulatory Commission. Initial Test Programs for Water-Cooled Nuclear Power Plants. Technical Report Regulatory Guide 1.68, Nuclear Regulatory Commission, 2013.

Chapter 7 – Prior licensing efforts and lessons learned

This chapter describes the licensing of two large D-T fusion facilities: the Tokamak Fusion Test Reactor (TFTR) facility at the Princeton Plasma Physics Lab (PPPL) in the United States and the ITER facility in Cadarache, France. The licensing of facility is characterized based on the licensing evaluation methods and regulatory frameworks used. Lessons learned from each licensing project (as presented in post-activity evaluations) are presented. The applicability of each set of lessons learned for the licensing of commercial fusion facilities are presented.

7.1 Historic operating experience with large deuterium–tritium fusion facilities

The past seventy years for fusion energy research have seen the construction of dozens of experimental fusion devices operated by national laboratories, research institutions, or private companies for scientific research and development activities. These devices have varied in design, fusion power output, confinement method and technology, and fuel selection.

The majority of these devices have operated with deuterium–deuterium fuel cycle at lower fusion power output (less than 10 MW of fusion power) for short periods of time. These three design and operational factors result in significantly smaller inherent inventory of hazards of highest regulatory importance (Chapter 4):

- Radioactive Material
- Hazardous Material (Toxicological, Chemical, Biological)
- Explosive Material
- Direct Radiation Exposures

Based on the previous discussion, hazards related to radioactive material are of particular concern for regulation of fusion facilities due to limited regulatory precedent for their safe handling.

The use of a deuterium–deuterium fuel cycle eliminates the presence of large quantities of tritium in the fueling system and exhaust system, as well as retention of tritium in plant systems that rely on tritium as a main fuel source. While tritium is generated during operation of a deuterium–deuterium fueled fusion facility, the quantity of material removed from the reactor and processed during operation is significantly smaller. The use of the deuterium-deuterium fuel cycle in an experimental fusion facility significantly reduces the inherent radioactive material inventory throughout facility systems. It also eliminates the need to produce, process, or store radioactive fuel.

The lower facility fusion power linearly reduces the neutron and secondary gamma production from the fusion device. This simplifies both on-site and off-site shielding requirements to maintain safe radiation levels during operation. The lower fusion power also reduce the fuel input and exhaust processing mass flow rates, as well as the total amount of stored energy and hazardous material in the facility.

The combination of lower fusion power and the shorter operational periods also reduce the total neutron fluence on structural materials. The lower total neutron fluence both reduces damage to materials that could result in failure mechanisms and also reduces the neutron activation of surrounding materials. This includes the radioactive material inventory of fixed activated structural materials, mobile activated corrosion products, mobile activated erosion products (dusts), as well as any activated liquids and gasses. These changes significantly reduce the inherent radiological hazards of a lower fusion power, short pulse experimental fusion facility.

The applicability of regulatory experience from deuterium–deuterium, lower fusion power, short pulse experimental fusion devices to commercial fusion facility licensing is limited due to the small inherent inventories of the highest regulatory importance hazards. Most experimental fusion devices have accordingly been regulated by rules for particle accelerators, radiation sources, and other devices that produce or utilize small quantities of radiation or radioactive material.

Several experimental fusion devices, however, have operated (or are licensed) with hazard characteristics that are comparable to those expected in commercial fusion facilities – specifically those expected in a deuterium-tritium fueled magnetic confinement tokamak configuration. Two relevant experiment fusion devices reviewed are:

- Tokamak Fusion Test Reactor (TFTR) facility at the Princeton Plasma Physics Lab (PPPL) in the United States
- ITER facility under construction in Cadarache, France

These facilities both utilize deuterium-tritium fuel cycles and larger volume devices to achieve higher fusion power (10 MW or greater) for longer periods of time. These characteristics result in hazards that are more comparable to those expected in commercial fusion facilities. The licensing evaluation methods and regulatory frameworks used for these facilities (as well as lessons learned from the licensing process) can provide some insights on the applicability of models and methods described in this work and the potential challenges of regulating commercial fusion facilities.

While these experimental fusion facilities have different operational objectives, concepts of operation, and design characteristics than a commercial fusion facility, they present the closest relevant regulatory experience for the licensing of large fusion experiments with significant inherent radiological hazards.

7.2 TFTR licensing experience

The Tokamak Fusion Test Reactor (TFTR) facility at the Princeton Plasma Physics Lab (PPPL) was a magnetic confinement tokamak fusion device designed and operated with the following technical objectives [1]:

- Investigate plasma physics and operation of large tokamak reactors
- Develop engineering experience with reactor scale fusion devices
- Test deuterium-tritium fueling and demonstrate fusion energy production

TFTR the first magnetic fusion device to extensively operate with the use of deuterium-tritium fuel and set records for total fusion power level during its operation from the early 1980s through the late 1990s [2]. The fusion power produced by TFTR (up to 10 MW), the resulting neutron radiation and materials activation, and the presence of significant tritium quantities used in the plasma and fueling handling systems (up to 50,000 Ci [5 g[1]] of tritium) resulted in significant radiological hazards for the facility [2].

TFTR was licensed and regulated under the jurisdiction of the U.S. Department of Energy (DOE) based on PPPL's status as an U.S. national laboratory for fusion and plasma research. The regulatory processes were based on the DOE's safety analysis and regulatory framework for the licensing of nuclear facilities that handle radioactive and other hazardous materials [3]. The facility was operated under an "Authorization Basis" that included the following technical documents [3][4][5]:

- Hazard Classification (HC)
- Safety Analysis Reports
    - Preliminary Safety Analysis Report (PSAR)
    - Final Safety Analysis Report (FSAR)
- Environmental Reviews
    - Environmental Assessment (EA),
    - Finding of No Significant Impact (FONSI), and
    - Supplemental Analysis (SA)
- Technical Safety Requirements (TSRs)
- Safety Evaluation Report (SER)

These documents provide characterization of hazards (HC), specification of facility requirements (TSRs), evaluation of safety (PSAR, FSAR, EA), and discussion of the facility licensing basis (SER, FONSI) [6].

TFTR was classified as a classified as a Category 3 hazardous facility ("Hazard Analysis shows the potential for significant but localized consequences") based on a total facility inventory of between 16,000 Ci (1.6 g) and 300,000 Ci (30 g) of tritium [28]. Although there were novel hazards associated with a 10 MW, deuterium-tritium fueled experimental

[1] Note that tritium has a specific activity of 9650 Ci per gram. In this work, the specific activity of tritium is approximated as 10,000 Ci per gram to simplify conversion between hazard limits and inventories in Ci and grams.

facility, there were no specific regulations or orders related to the safety analysis and regulation for low hazard facilities such as TFTR during initial design and licensing [3]. PPPL and its contractors chose, therefore, to base the TFTR evaluation of safety process (for PSAR, FSAR, EA) on the regulatory guides issued by the Nuclear Regulatory Commission (NRC) for the safety analyses of commercial nuclear power plant [6].

The comprehensive technical safety evaluations would be conducted for TFTR by PPPL under the jurisdiction of the DOE but the licensing analyses and process were largely novel. The main licensing documents discussed in this work are the PSAR, FSAR, EA, and SER. These documents outline the major safety analyses that were conducted to demonstrate compliance with relevant regulatory hazard limits.
The subsequent experience by TFTR to license and regulate the facility reflected the challenges of simultaneously developing and demonstrating compliance with regulatory requirements.

7.2.1 Licensing evaluation method for TFTR

The licensing evaluation methods used for TFTR are documented in the PSAR, FSAR, and EA to demonstrate compliance with regulatory hazard limits. The PSAR demonstrates that a facility is expected to meet safety related regulatory requirements before beginning procurement and construction activities while the FSAR demonstrates that the facility will meet safety related regulatory requirements before beginning operation [7]. The EA more generally reviews the potential environmental and public impacts of facility operation. These three regulatory documents utilized different licensing evaluation methods to demonstrate compliance with regulatory limits or quantify the impacts of facility operation.

The PSAR focused on the radiological hazards associated with the tritium inventory based on the results of the hazard classification and identification of relevant hazards. The bounding DOE hazard limit presented in the PSAR for off-site public exposure during an "extremely unlikely event" was set at 25 rem (250 mSv) with a design object of 5 rem (50 mSv) []. Compliance with this DOE hazard limit was demonstrated using a worst case release evaluation. The analysis considered complete destruction of the fusion device and release of system inventory of 25,000 Ci in an oxidized form at ground level with a distance of 125 meters to the site boundary. Use of a simplified Gaussian plume model and conservative meteorological conditions resulted in a calculated off-site dose of 2.73 rem [6]. This analysis demonstrated appropriate compliance with the 25 rem DOE hazard limit and 5 rem design object based on the in-process inventory limit of 25,000 Ci (2.5 g). This worst case release, however, may have required off-site emergency planning because it exceeded the protective action dose threshold of 1 rem [8].

The FSAR updated the PSAR and focused on more detailed descriptions of as-built plant systems and refinement of limiting accidents and consequences [6]. The FSAR also demonstrated compliance with the relevant regulatory limits using the same worst case release scenario. Instead of relying on conservative meteorological conditions, however, site specific meteorological conditions were used based on measurements from an on-site meteorological measurement tower that was installed during construction [6]. The use of the site specific meteorological conditions reduced the calculated worst case release off-site dose from 2.73 rem to 0.66 rem [6]. This reduced dose satisfied both the design objectives dose limits and protective action dose threshold limit.

Further updates to the FSAR modified the licensing evaluation method for TFTR from a worst case release evaluation to a maximum credible release evaluation. In the revised analysis, the maximum credible accident release analysis considered was release of the storage system inventory of 25,000 Ci of tritium in an oxidized form through the facility release stack [6]. Crediting the use of the stack in the analysis and elevated release from an 18.3 meter high stack further reduced the off-site dose from 0.66 rem to 0.14 rem. The 140 mrem dose became the documented off-site dose consequences as part of the facility licensing basis.

The EA focused on evaluating the bounding impacts of facility operation on the environment and the public. The EA considers "worst case beyond design basis accident" based on the FSAR maximum credible accident analysis. A maximum credible accident release analysis is effectively used as the licensing evaluation method. The analysis considers was release of the storage system inventory of 25,000 Ci of tritium in an oxidized form but assumes a ground level release due to the failure of the facility release stack [6]. The EA assumes typical meteorological conditions and increase dispersion due to surrounding structures and results in a maximum off-site dose of 390 mrem [6]. This dose meets all regulatory hazard limits.

The licensing evaluations for TFTR used both worst case release evaluations and maximum credible release evaluations to meet off-site dose limits. In these licensing evaluations, four major factors were used to reduce dose from the initial worst-case release evaluation:

- Limiting vulnerable tritium inventory to 25,000 Ci from site inventory of 50,000 Ci by crediting design and separation of inventories
- Use of site specific meteorological data to reduce off-site dose consequences
- Crediting facility release stack with elevated release and dispersion
- Crediting local geographic dispersion and building wake effects

Combinations of these factors were credited to reduce the dose from an initial estimate of 2.73 rem to a final regulatory dose of 0.14 rem. Actual facility design and operation remained the same but changes in the licensing evaluation analysis methods and assumptions enabled a 20 times reduction in the calculated off-site doses and demonstrated compliance with regulatory limits.

7.2.2 Regulatory framework for TFTR

The TFTR facility was regulated under the jurisdiction of the U.S. Department of Energy using an independent review regulatory framework. The DOE operates many of its facilities using a contractor model where the DOE owns facilities and is responsible for safe operation but relies on contractors to design and operate the facilities. In the DOE regulatory framework, the contractors are responsible for preparing licensing basis documents and demonstrating compliance with DOE regulatory requirements while the DOE site offices are responsible for performing an independent review for all safety materials. The results and conclusions of DOE safety review process are documented in a facility safety evaluation report (SER) [9].

Characterizing and evaluating the independence of the review, however, is complicated due to the relationship between the DOE and its facilities. The DOE is ultimately responsible for safety regulation and ensuring facility operation to meet agency goals. The effective independence of this complex regulatory framework has been questioned and revisited over the past several decades. Reports by the U.S. Government Accountability Office have highlighted the DOE's failure to fulfill its function as an independent regulator in reviewing the safety of DOE facilities [10]. The DOE's review process has been revised overtime to help promote more independent review of safety materials [7] and regulatory oversight has been improved through additional independent oversight of DOE safety reviews by the Defense Nuclear Facilities Safety Board [11]. These changes to the DOE's independent review regulatory framework occurred simultaneous to the development and review of the TFTR project from the mid 1970s through the mid 1990s.

PPPL and its contractors were responsible for the design, construction, and operation of TFTR. PPPL and its contractors prepared licensing basis documents and the DOE was responsible for independently reviewing and evaluating the licensing basis documents. The PSAR for TFTR (including documentation of the facility design, siting, operation, safety, and other characteristics) was approximately 1,000 pages and took approximately one year to prepare (in addition to prior design efforts). DOE review of the PSAR took approximately four months and required PPPL response and resolution of 300 technical comments [6].

The FSAR updates to TFTR took place over a period of three years, including approximately one and half years of preparation, one year of review, and six months of revision and approval [6]. This review, revision, and approval process required PPPL response and resolution of another 300 technical comments from DOE reviewers [6].

The EA for TFTR required approximately two years to prepare, review, and approve. Environmental assessments developed for other DOE projects and PPPL were leveraged heavily to facilitate the completion of the TFTR EA [6]. These evaluations were completed to support a regulatory Finding of No Significant Impact (FONSI) under the National Environmental Protection Act (NEPA) and avoid the need to complete a more detailed Environmental Impact Statement (EIS) for the TFTR facility at PPPL.

It is important to note the regulation and licensing of TFTR is also subject to additional regulatory requirements and regulatory frameworks based on overlapping legal jurisdictions related to facility hazards. This included significant requirements by the U.S. Environmental Protection Agency and the New Jersey Department of Environmental Protection related to use of hazardous and radioactive materials [6]. These and other local, state, and federal requirements were primarily promulgated through permit based regulatory frameworks.

7.2.3 Lessons learned from TFTR licensing

The licensing and regulatory processes for TFTR can perhaps best be described as a mixed success. The regulatory process was successful as it enabled safe operation of a first-of-a-kind fusion facility at a suburban DOE lab without resorting to remote siting for assurance of safety. Navigation of regulatory process for TFTR was described as " a painful learning experience since clear, specific safety regulations for fusion devices do not exist" [12]. TFTR struggled with changing regulatory requirements and on-going negotiation between PPPL and DOE regarding the facility safety basis.

Reviews of TFTR regulatory process noted key successes and lessons learned from the development and approval of facility operation. Successes of the TFTR review process included [12]:

- Use of site-specific meteorological data to reduce conservatism in release analyses and reduce the projected offsite doses
- Use facility start-up testing results to refine radiological dose models, and eliminate the need for additional radiation shielding
- Use of cost benefit analysis and hazard analysis to eliminate the need for costly and complex radiation reduction systems that would not have had a significant impact on public health or safety
- Use of exemptions from standard industry codes or practices based on configuration specific analyses and calculations

These successes relate to appropriate reductions in conservatism and better characterization of regulatory requirements through associated with more detailed analyses within the safety basis. The PPPL technical staff was able to trade additional analytic burden and costs for a reduction in regulatory and design requirements.

Lessons learned from the TFTR review process included [12]:

- Need to propose regulation requirements and implementation plans during design rather than waiting for the regulator to develop plans. This can help ensure that the regulations are commensurate with the hazard and that changes can be incorporated into design
- Commitments to regulators need to be carefully considered. Agreeing to make changes without careful consideration of cost, schedule, or complexity can lead to project delays and failure to meet agreed upon schedules
- High quality documentation is critical. Applicants need to understand that any and all documents submitted are subject to rigorous regulatory review.
- Management of audits teams and project reviews is necessary to ensure that they are effective and do not cause compliance for the sake of compliance.
- Regulator expectations must be understood and managed throughout the preparation, review, and acceptance process. Understanding regulatory culture norms and expectations is essential to effective reviews.

- Appropriate codes and standards are essential to ensuring timely and effective reviews. The level of safety and technical rigor must be commensurate with the hazards posed by the technology.

These lessons learned primarily relate to administrative lessons learned that impact the regulatory review process. The licensing evaluation methods were generally appropriate, but the main challenges were related to project management. This is a critical lesson for regulation of commercial fusion facilities. Success or failure of a regulatory system relies heavily on the ability for regulators and facilities to satisfy the underlying intent of regulatory requirements and not become overly focused on compliance absent intent.

The lessons learned were viewed as applicable to the future licensing of commercial fusion power plants and not just the licensing of TFTR [12]. Reviews of the TFTR regulatory process recommended use of a “graded” safety approach that provided for different levels of regulatory oversight and requirements depending on the inherent hazards from the “mission, design, and radionuclide inventory” [12] .

7.2.4 Applicability of TFTR to commercial fusion facilities

The safety regulation of TFTR was conducted using worst case release and maximum credible release licensing evaluations with an independent review regulatory framework. These regulatory processes facilitated the regulation and safe operation of first-of-a-kind experimental fusion facility at megawatt scale, utilizing a deuterium-tritium fuel cycle.

The TFTR regulatory experience provides several key insights into both use of simple licensing evaluation methods (worst case release and maximum credible release) and the implications of an independent review regulatory framework. These insights include:

- Balancing regulatory conservatism and regulatory detail is valuable to project specific best outcomes
- Elimination of credited engineered safety features simplifies licensing
- Minimizing inherent hazard inventories facilitate reduce regulatory burden
- Establishing adequate regulatory requirements simplifies licensing processes
- Appropriate project management can strongly affect regulatory outcomes

The regulation of TFTR is demonstrates that limiting inherent facility hazards can simplify the regulatory process and facilitate use of simple licensing evaluation methods but that adequate regulatory requirements and appropriate project management are essential to an efficient and effective regulatory review process. The independent review was, ultimately, effective at ensuring a safe design and operation but the challenges related to implementation may have contributed to a costly and lengthy review process.

While the insights from the licensing of TFTR are applicable to regulation of commercial fusion facilities, the direct licensing experience is largely not applicable. The relatively low power (10 megawatts), limited tritium inventory (50,000 Ci or 5 grams), and short duration pulses (less than 1 second) are not typical of commercial fusion facility and result in inherently smaller hazards. A commercial fusion facilities with a tritium inventory up to 2 to 4 times than the maximum release tritium inventory at TFTR could likely be regulated using similar regulatory processes based on the off-site dose consequences calculated for TFTR and the need to meet at 1 rem off-site dose limit. These tritium inventories are likely much smaller than the inventories expected for commercial fusion facilities (Chapter 5).

Licensing experience with TFTR highlights how simplified regulatory methods can be used to demonstrate compliance with regulatory limits given sufficiently small inherent hazards. Project management challenges related to the independent review process and uncertainties related to project regulatory requirements resulted in a more lengthy and costly regulatory process than may have been warranted for the facilities based on the inherent hazards. The lessons learned from the TFTR regulatory process show the importance of balancing usage of conservatisms when selecting the most regulatory methods for the design and operational analysis of commercial fusion systems.

7.3 ITER licensing experience

The ITER facility in Cadarache, France is a large magnetic confinement tokamak fusion device currently under construction by an international consortium. ITER is designed a wide variety of technical objectives, including [13]:

- Achieve fusion power to heating power ratio of at least five
- Operate at steady state for periods of hundreds of seconds
- Achieve a total fusion power of hundreds of megawatts
- Facilitate experimental evaluation of net gain or burning plasmas
- Enable testing of technology required for commercial fusion production include tritium fueling and breeding systems

At the time of design and initial licensing, was ITER was a significant step forward for experimental fusion facilities. ITER had linear dimensions twice as large as the JET facility at Culham Centre for Fusion Energy and was designed to produce twenty times as much fusion power. It was expected to be the first fusion device to achieve breakeven, producing as much fusion power as required heating power. The high power output, net gain of energy, long duration of operation would require large systems for the processing and handling of the tritium fuel needed for a tritium-deuterium fuel cycle. The ITER facility designed throughout the 1990s as the last experimental device before the construction of a prototypical commercial fusion facility [14].

The selection of the Cadarache site in France for the ITER facility was announced in 2005 after an extensive selection process. The ITER development plan required that the internationally constructed facility complied with host country regulatory requirements, so the ITER facility was under the regulatory jurisdiction of the French Atomic Energy Commission (CEA) and the French Nuclear Safety Authority (ASN) [14]. The ITER facility was classified as a “basic nuclear facility” (INB) based on the tritium inventory expected at the ITER site and was subject to the same regulatory framework used for other commercial nuclear facilities [15]. The inventory threshold for classification as an INB is an equivalent activity of 370 TBq (10,000 Ci) [16]. This classification meant that the ITER site would be subject to the same regulatory requirements and processes used for commercial fission reactors, nuclear fuel cycle facilities, particle accelerator, and other substantial uses of radioactive material [16].

The licensing of an INB in France is based on a two-step legal licensing process. The two regulatory decisions are "Décret d'Autorisation de Création" (DAC) that permits the start of construction activities and "Décret d'Autorisation de Rejets et de Prélèvements d'Eau" (DARPE) that permits the start of operation by permitting usage and discharge of water [14]. These decisions required adequate demonstration of compliance with the relevant regulatory requirements for an INB. Regulatory compliance is demonstrated through a number of documents including the "Rapport Préliminaire de Sûreté" (RPRS) [14]. The RPRS details the safety basis for the facility and demonstrates expected facility compliance with all relevant regulatory requirements. The RPRS is revised throughout the construction process based on as-built conditions and revised evaluations. The Rapport Définitif de Sûreté (RDS) is reviewed and approved by the regulator as the final licensing basis for the facility.

The licensing processes conducted for ITER by ASN was performed under the same rules used for other nuclear facilities (INB) but the requirements and specific analyses for a large fusion facility were novel. The main licensing document discussed in this work is the RPRS. The ITER facility is still under construction, so the facility is still under the jurisdiction of the DAC authorization and the analyses within the RPRS. The RPRS describes the major safety analyses that were conducted to demonstrate compliance with relevant regulatory hazard limits. The regulatory experience of ITER to license and regulate a large fusion facility reflects both the challenge of regulating a facility using a regulatory framework based on the safety analysis of commercial fission facilities and the challenge of regulating a novel technology with large uncertainties in design and operation.

7.3.1 Licensing evaluation method for ITER

The licensing evaluation methods used for ITER are documented in the RPRS that demonstrate compliance with regulatory hazard limits. The hazard evaluations performed for ITER as part of preliminary design safety assessments identified the following hazards of regulatory significance [14]:

- radioactive materials
    - tritium and tritiated materials
    - neutron activated structural materials
    - neutron activated in-vessel dust
    - neutron activated corrosion products in coolant water
- non-nuclear hazardous materials
    - chemically toxic (e.g. beryllium)
    - reactive (e.g. hydrogen)

- stored energy sources
    - plasma
    - magnets
    - activation decay heat
    - coolant thermal energy
    - chemical energy

These hazards are considered within the RPRS and other regulatory documents to ensure that the design and operation limits hazards to acceptable levels.

A deterministic design basis analysis licensing evaluation method is used in the RPRS to demonstrate ITER compliance with regulatory limits. Probabilistic design basis evaluations were not used for the ITER facility but were used to quantify the probability of certain external hazards (e.g., meteorological, fire, aircraft impact) to justify their inclusion or exclusion as initiating design basis or beyond design basis events.

The consequences associated with the radioactive material hazards (tritium, neutron activated in-vessel dust, and neutron activated corrosion products) were selected as bounding radiological hazards, A set of design basis "reference events" were selected for the ITER facility and the event sequences associated with these initiating reference events are analyzed for compliance with regulatory hazard limits [17]. A set of beyond design basis event sequences was also analyzed to confirm robust facility design and the absence of "cliff-edge" effects in calculated event consequences [17].

The regulatory hazard limits for ITER were based on a combination of ASN regulatory requirements and self-imposed design objectives for the ITER facility. An off-site public dose limit of 1 rem (10 mSv) was selected to eliminate the need for emergency planning related to evacuations or shelter in place [18]. A design objective regulatory dose 10 mrem (0.1 mSv) was also established for the ITER facility based on limiting accident exposures to below the annual operating release limits for the facility [19]. Other regulatory hazard limits were developed for routine exposure and emissions, on-site worker exposure, and long-term exposures to radioactive materials [14].

The radiological source terms used in the deterministic design basis analyses were based on conservative estimates of material inventory with additional margin to provide margin for measurement uncertainties. Table 7.1 provides safety assessment inventories considered in the ITER licensing evaluations [13]. These inventories likely have significant margin to the actual radioactive material inventories expected in the ITER facility but the excessive margin helps ensure that that facility will always remain in compliance with licensing basis evaluations. This trade-off reduces operational burden and risk by increasing the burden associated with design conservatism and analysis.

Table 7.1. ITER Safety Analysis Radioactive Material Inventories

Radioactive Inventory Category	*Safety Assessment Inventory* [13]
Tritium – Site Wide	3 kg
Tritium – In Vessel	1 kg
Tritium – Fuel Cycle	0.7 kg
Activated In Vessel Dust	1000 kg
Activated Corrosion Products	10 kg

The RPRS for ITER is not publically available but review of published ITER accident scenarios provides insights on how the deterministic design basis analyses are used to demonstrate compliance with regulatory hazard limits. One event sequence ("Large ex-vessel divertor pipe break") results in the release and mobilization of the full in-vessel tritium inventory, the full in-vessel activated dust inventory, and a small percentage of the activated corrosion product inventory [20].

During this event sequence, various engineered safety features (e.g., suppression tank pool for limited solid particle release, confinement systems, detritiation systems) are assumed to function and dramatically reduce the final released inventory [20]. These engineered safety features reduce the material release fraction and analyze release of 2 grams or less of the tritium, activated in-vessel dust, and activated corrosion products [20]. The resulting off-site dose consequence calculations (200 meters or 1.2 kilometers depending on receptor) satisfy the regulatory dose limit due to the small radiological inventory [21]. The final dose for this event sequences is less than 2 mSv [20].

The significant reduction in released inventory compared with the vulnerable inventory is common for the ITER accident sequences due to the use of engineered safety features to confine, mitigate, and control the release of radioactive material. These analysis assumptions and evaluation approach within the ITER RPRS deterministic design basis analyses facilitate compliance with all regulatory requirements for radioactive materials.

A comprehensive set of design basis events and beyond design basis events are presented, analyzed, and evaluated in the ITER RPRS. These event sequences are intended to bound facility operation and demonstrate compliance with the regulatory hazard limits for normal and emergency operation. This analysis constitutes the operational safety basis for the ITER facility.

7.3.2 Regulatory framework for ITER

The ITER facility is regulated under the jurisdiction of CEA (site owner) and the ASN (safety regulator) using an independent review regulatory framework. The use of the independent review regulatory framework reflects best practices for the regulation of other nuclear facilities by ASN, including commercial nuclear power plants. The review and the approval of all aspects of the ITER facility (design, operation, management) are independently conducted by the regulator [14]. The ASN review of the ITER licensing basis documents is aided by the “Institut de Radioprotection et de Sûreté Nucléaire” (IRSN), a technical advisory board that provides independent assessment of regulatory documents.

The independent review process of the ITER RPRS has been resource intensive requiring substantial time to prepare, review, and revise. The initial files for the DAC (including the RPRS) were submitted to the ASN in January 2008 after several years of development and preliminary safety analyses by the ITER organization [15]. An initial licensing acceptance review took several months and resulted in 60 identified areas for additional detail in the RPRS [15]. After an additional two years of revision and analysis, the updated RPRS was resubmitted to ASN for review in March 2010. The IRSN began an independent examination process and submitted over 700 questions requiring written responses and changes to the RPRS over a period of 18 months [15]. In June 2012, the RPRS was approved and the DAC was granted to the ITER project. The DAC approval, however, also stipulated 25 demands on the project and 162 engagement and check in points with the ASN [15]. The approved RPRS was more than 2,000 pages with numerous supporting calculations, analyses, and supporting quality documents.

The regulatory framework for ITER will require additional approvals and authorizations before commencing operation. This will include approval of the final RDS and authorizations for D-D operation and authorization for activation from D-T operation [19]. Review and approval of these remaining licensing documents and authorizations will be conducted under the same independent review based regulatory framework.

It is important to note the regulation and licensing of ITER is also subject to additional regulatory requirements and regulatory frameworks based on overlapping legal jurisdictions related to facility hazards. This included significant requirements by environmental regulators related to use of hazardous and radioactive materials, requirements on worker safety, and consultations with local members of the public [15]. These and other local, state, and federal requirements were primarily promulgated through permit based regulatory frameworks.

7.3.3 Lessons learned from ITER licensing

The licensing evaluation methods and regulatory frameworks used by the ITER facility demonstrate how regulation of commercial fusion facilities could be conducted using the regulatory methods for commercial fission and radioactive material facilities. The ITER facility was not held to the exact same regulatory requirements as a commercial fission reactor due to its classification as a INB laboratory and not a commercial nuclear fission reactor [19] but it still followed the same regulatory processes.

The safety and licensing approach for ITER was defined around two safety functions [22]:

- confinement of radioactive materials
- protection from exposure to ionizing radiation

These two safety functions lead to the application of several safety principles for the design and operation of ITER [23]:

- Defense-in-depth (DID): use of multiple, independent, redundant barriers to materials, hazards, events, or other unsafe conditions
- As-low-as-reasonable-achievable (ALARA): minimizing exposures to radiation to as low of a level as is reasonably achievable through facility design and operational activities
- Passive safety: avoid reliance on engineered safety features that require active control and energy to complete their safety function

The three principles are dogmatic within the safety of fission systems but were applied to the ITER facility, in part, due to its licensing as a INB by the ASN but also due to extensive use of DID, ALARA, and passive safety to ensure safe operations in high hazard industries. These safety principles, however, can constrain design requirements and incentivize design features that achieve safety at high cost.

For example, the confinement safety function at ITER and the safety principle of DID result in a design strategy that requires confinement by two independent confinement systems (each composed of one or more functional barriers) for all significant inventories of radioactive material [22]. Combined with the safety principle of passive safety for engineered safety features encourages ITER designers to design and credit large vessels and containment structures with a safety related confinement function. While use of confinement structures is common in high hazard facilities, ensuring their performance for all postulated design basis events can require detailed calculations and significant engineering margin. This results in the need for highly engineered systems that can increase project cost and schedule.

The challenges related to the use of DID, ALARA, and passive safety as primary safety principles do not directly relate to either the licensing evaluation method or the regulatory framework. These principles are largely philosophical and more directly relate to an organizational approach to safety. Application of DID, ALARA, and passive safety can promote safe operation if used appropriately but can also promote overly burdensome regulatory requirements and increase costs if used inappropriately.

Another major lesson learned from ITER licensing was the availability and adequacy of regulations, codes, and standards to support regulatory activities [24]. The independent review regulatory framework relies on technical staff ability to assess demonstrated compliance with regulatory requirements. Consensus codes and standards are invaluable for providing an objective technical basis for evaluation of compliance, design methods, and calculation assumptions.

Codes specifically developed were not yet developed for fusion organizations, so regulators relied on codes developed for other nuclear fission facilities already licensed by the ASN [24]. This lead to inappropriate use of regulatory requirements such as applying pressure vessel rules intended for pressurized water fission reactors to any ITER facility vessel or system containing more than 10 Ci (1 mg) of tritium at greater than 0.5 bar of pressure [24]. These requirements, while conservative, were likely inappropriate given the hazards and safety functions of the system as compared with a pressurized water fission reactor. Development and use of regulations, codes, and standards more compatible with fusion facilities may have simplified the regulatory process.

A final challenge and lesson learned from the ITER regulatory process is the impact of design uncertainty on the analytic and engineering margin. Significant radiological source terms such as tritium hold up in the ITER vacuum vessel, neutron activated corrosion products, and neutron activated first wall dusts are not well characterized based on the novel design and operational characteristics of the ITER facility. The quantity, exact form, and radionuclide composition of these radioactive source terms are not well understood. As a result, ITER was force to address the high uncertainty while meeting regulatory limits. The ITER safety analysis considered and analyzed source terms that were far larger than those expected during operation [13]. This additional margin provides for engineering and measurement uncertainties, and provides additional confidence that safety analysis will bound any operational facility conditions. This process trades engineering margin and additional design constraints for greater assurance of facility operability.

7.3.4 Applicability of ITER to commercial fusion facilities

The safety regulation of ITER is conducted using a deterministic design basis event licensing evaluation and an independent review regulatory framework. These regulatory processes, combined with a confinement based approach to safety and principles of DID, ALARA, and passive safety are use to help ensure the safety of ITER design and operations. This approach largely reflects the approach to safety utilized by commercial fission facilities. An independent review regulatory framework helps provide confidence in the safety evaluation of a first of a kind experimental fusion facility that is orders of magnitude larger than existing fusion facilities.

The licensing evaluation methods selected credit the performance of engineered safety features to reduce the consequences associated with design basis events. These engineered safety features protect, confine, and mitigate the release of radiological materials resulting in two or more order of magnitude reduction in release fraction. This approach results in low calculated off-site hazard consequences (often less than 1 mSv) despite large inventory source terms of both tritium and activated materials (tens to hundreds of kilograms). The relatively remote siting of the ITER facility (200 meters for short term exposure and 1.2 km for longer term exposure) also helped mitigate the consequences associated with release.

The ITER regulatory experience provides several key insights into the effects of deterministic design basis event licensing evaluations and an independent review regulatory framework on regulation of large fusion facilities. These insights include:

- Performing and documenting the large number of design basis evaluations requires significant effort to complete and produces lengthy licensing documents
- Detailed licensing evaluations require significant effort to review and can require substantial resources to respond and review to regulator comments
- Crediting engineered safety features allows significant reduction in calculated hazard consequences
- Reliance on engineered safety to meet regulatory limits results in high quality and design requirements for major systems
- Use of certain design and safety philosophies (i.e. DID, ALARA, and passive safety) may have unintended consequences on the design and operation of a facility if not implemented correctly
- Availability of adequate regulations, consensus codes, and standards are can affect the predictability of the licensing preparation and review process

The regulation of ITER is demonstrates that use of deterministic design basis event licensing evaluations and an independent review regulatory framework can be used to successfully licensing a large fusion facility. This success, however, comes at significant costs related to the preparation of regulatory documents and requirements on the design and operation of systems credited with safety functions. The regulatory processes for ITER mirrored those of commercial fission facilities so it is logical that the regulatory results for ITER mirror those of commercial fission facilities in terms of regulatory burden and safety credited equipment.

Many of the lessons learned from the ITER licensing experience are applicable to the regulation of commercial fusion facilities but it is not fully representative of a commercial fusion facility licensing process. The higher power level (500 megawatts) and tritium inventories (tens to thousands of grams) are likely the same order of magnitude of those expected in a commercial fusion facility. The short duration pulses (hundreds of seconds) and limited total operational time (tens of thousands of seconds over the device lifetime) are not typical of commercial fusion facility. This results in inherently smaller facility hazards, specifically those related to total neutron fluence and activation of materials. The ITER facility has many of the systems expected in a commercial fusion facility but lacks certain key system including continuous tritium breeding, exhaust processing, and other fuel cycle facilities to sustain self-sufficient operation as well as the balance of plant systems associated with a energy generating facility.

Licensing experience with ITER highlights how more detailed regulatory evaluation methods and crediting engineering safety features can be used to demonstrate compliance with regulatory limits for facilities with significant regulatory hazards. These analyses, however, presented a significant regulatory burden for the ITER facility when combined with safety principles and regulatory processes used with commercial fission facilities. Use of similar licensing evaluation methods and regulatory frameworks for commercial fusion facilities could facilitate the successful licensing of commercial fusion but would likely result in a regulatory burden similar to that of commercial fission facilities. The lessons learned from the ITER regulatory process show the impact of facility design characteristics that require the use of detailed regulatory evaluation methods and crediting engineering safety features to meet regulatory limits.

The licensing of the ITER facility has been highlighted by commercial fusion industry proponents as a case study inappropriate regulatory requirements [25]:

> Imposing the same fission standards on the fusion sector would create a costly regulatory requirement developed to address risks that will not be present at a fusion energy facility. By comparison, France imposed its existing fully deterministic regulatory paradigms for fission facilities in order to evaluate and approve the ITER experiment. By failing to appreciate fully the significant differences between risks presented by fusion energy facilities as compared to nuclear fission plants, France’s regulatory process increased ITER’s construction costs and lengthened the construction timeline for the facility.

This claim fits a tradition narrative that the regulatory requirements on commercial fission facilities are, in part, responsible for high facility costs and construction delays. This claim, however, does not appear substantiated by any reviews of the ITER project. DOE reviews of the ITER project found that project management and construction procurement problems were main factors at the schedule delays and project costs increases and did not reference any issues related to licensing [26]. It is not clear that the licensing process has significantly contributed to the schedule and cost challenges of the ITER project. The incorrect attribution of project cost and schedule overruns to regulation instead of project management and project management interface with the regulator is common for large regulated projects where cumulative project management effects are not readily apparent [27]. This clarification is useful when assessing the potential benefits and costs of different licensing pathways.

7.4 Contextualizing licensing for commercial fusion facilities

The licensing experience of both TFTR and ITER provide valuable insights into the licensing prospects for commercial fusion facilities. While these experimental fusion facilities have different operational objectives, concepts of operation, and design characteristics than a commercial fusion facility, they present the closest relevant regulatory experience for the licensing of large fusion experiments with significant inherent radiological hazards. The experiences at the facilities reflect the challenges of integrating a novel facility into regulatory systems otherwise developed for the regulation of fission reactors or fuel-cycle facilities.

The limited inherent hazards associated with TFTR facilitated a simple regulatory pathway that did not rely on detailed licensing evaluations or crediting engineered safety features with a safety function to meet regulatory limits. The challenges associated with TFTR licensing can be attributed to project management, the technical preparation of the regulator, and the availability of codes and standards that are applicable to fusion facilities. The licensing experience of TFTR is directly applicable to commercial fusion facilities that can minimize inherent radiological hazard through design and materials selection choices to extremely low levels. The licensing experience of TFTR is indirectly applicable to all commercial fusion facilities based on the need for effective project management as well as regulator relationship management.

The significant inherent hazards associated with ITER and the regulatory environment in France resulted in a high regulatory burden pathway that utilized detailed licensing evaluations and crediting engineered safety features to meet regulatory limits. The challenges associated with ITER licensing can be to the regulatory philosophy used in developing a safe operating strategy and the availability of codes and standards that are applicable to fusion facilities. These contributed to a lengthy regulatory process and reliance on engineered safety features. The licensing experience of ITER is directly applicable to commercial fusion facilities that are regulated under rules quickly adapted from commercial fission. The licensing experience of ITER is indirectly applicable for commercial fusion facilities that are expected to have significant inherent hazards. High hazard commercial fusion facilities will need to determine the appropriate balance of hazard reduction, confinement, mitigation, and control versus hazard justification by analysis to meet regulatory limits.

The licensing of major D-T fusion experiments will factor into the development and assessment of future commercial fusion reactors. Historical precedent is commonly used to justify regulatory decision making. Regulatory and policy makers will need to have clear justification for diverging from existing precedent set by TFTR or ITER for commercial fusion reactors. Clearly characterizing the differences between regulatory framework can help increase public transparency with the licensing process and provide a better understanding of the regulatory safety case. These two case studies demonstrate the challenges of regulating novel fusion facilities and highlight the fact that successful licensing is dependent on a number of factors outside of the licensing evaluation method or regulatory framework. The licensing experience of TFTR and ITER demonstrate the importance of project management, regulatory engagement, and a technically competent regulator in the successful completion of commercial fusion facility regulation.

7.5 References

[1] D. M. Meade. TFTR Twenty Year Perspective. In 17th IEEE/NPSS Symposium Fusion Engineering (Cat. No. 97CH36131), volume 1, pages 10–17. IEEE, 1997.

[2] D. M. Meade. DT experiments on TFTR. Journal of Fusion Energy, 13(2):145–154, 1994.

[3] J. D. Levine. Preparation of Safety & Environmental Documentation, and the Approval Process for TFTR DT Operations. Princeton Plasma Physics Laboratory, 2014.

[4] Energy Research Development Administration. Tokamak Fusion Test Reactor Facilities: Environmental Impact Statement. Technical Report WASH-1544, 1975.

[5] Final Safety Analysis Report, Tokamak Fusion Test Reactor. Technical Report DTSD-FSAR-17, Prince- ton Plasma Physics Laboratory, 1994.

[6] Levine, J. TFTR D-T Engineering - Lessons Learned. 1996.

[7] Department of Energy. Nuclear Safety Analysis Report. Technical report, Order O 5480.23, April 1992.

[8] Environmental Protection Agency. PAG Manual: Protective Action Guides and Planning Guidance for Radiological Incidents. Technical Report EPA-400/R-17/001, Environmental Protection Agency, January 2017.

[9] Department of Energy. DOE Standard: Review and Approval of Nuclear Facility Safety Basis and Safety Design Basis Documents. Technical Report DOE-STD-1104-2016, Department of Energy, December 2016.

[10] Government Accountability Office. Safety Analysis Reviews for DOE's Defense Facilities Can Be Improved. Technical Report GAO/RCED-86-175, June 1986.

[11] P. Offenhauer. Defense nuclear facilities safety board: the first twenty years. In Federal Research Division of the Library of Congress, Washington, DC, 2009.

[12] J. DeLooper. Fusion safety regulations in the US: progress and trends. Fusion technology, 26(3P2):1051– 1058, 1994.

[13] ITER Organization, EDA. Documentation Series No. 24 ITER Technical Basis. Technical Report IAEA/ITER EDA/DS/24, International Atomic Energy Agency, 2002.

[14] European Fusion Development Agreement. Cadarache as a European Site for ITER: Report on the Technical and Socio-economic Aspects. September 2001.

[15] Taylor, Neill and Alejaldre, Carlos and Cortes, Pierre. Progress in the Safety and Licensing of ITER. Fusion Science and Technology, 64(2):111–117, 2013.

[16] Berkvens, Paul and Colomp, Patrick. Safety Considerations for Measurements of Radioactive Samples at the European Synchrotron Radiation Facility. Speciation, techniques and facilities for radioactive materials at synchrotron light sources, page 189, 1998.

[17] L. Rodriguez-Rodrigo, J. Elbez-Uzan, and C. Alejaldre. Iter licensing process from design and construction to dismantling. Fusion science and technology, 56(2):809–813, 2009.

[18] Taylor, Neill et al. Preliminary safety analysis of ITER. Fusion Science and Technology, 56(2):573–580, 2009.

[19] L. Rodrıguez-Rodrigo. Licensing ITER in Europe: An Example of Licensing a Fusion Facility. European ITER Site Studies team, 2006.

[20] Reyes, Susana and Topilski, Leonid and Taylor, Neill and Merrill, Brad J and Sponton, Lise-Lotte. Updated modeling of postulated accident scenarios in ITER. Fusion science and technology, 56(2):789– 793, 2009.

[21] Taylor, Neill et al. Updated safety analysis of ITER. Fusion engineering and design, 86(6-8):619–622, 2011.

[22] Taylor, Neill and P. Cortes. Lessons learnt from ITER safety & licensing for DEMO and future nuclear fusion facilities. Fusion Engineering and Design, 89(9-10):1995–2000, 2014.

[23] N. P. Taylor. Safety and licensing of nuclear facilities for fusion. In 2015 IEEE 26th Symposium on Fusion Engineering (SOFE), pages 1–8. IEEE, 2015.

[24] Girard, Jean-Philippe and Taylor, NP. Lessons learnt during the preparation for ITER licensing. In Fusion power plant safety. Proceedings of a technical meeting, 2007.

[25] Fusion Industry Association. Igniting the Fusion Revolution in America. June 2020.

[26] U.S. Participation in the ITER Project. Department of Energy, May 2016.

[27] Future of Nuclear Energy in a Carbon-Constrained World. Massachusetts Institute of Technology, 2018.

[28] Department of Energy. DOE Standard: Hazard Categorization and Accident Analysis Techniques for Compliance with DOE Order. 5480.23, Nuclear Safety Analysis Reports. Technical Report DOE-STD- 1027-92, Department of Energy, September1997.

Chapter 8 – Conclusions and Future Work

One of the challenges associated with the deployment of commercially viable fusion energy technology is assessment and development of appropriate regulation. Under-regulation, over-regulation, or mis-regulation of a new technology can jeopardize long-term commercial deployment opportunities. Under-regulation may result loss of social license, legal liability, or harm to stakeholders due to inadequate oversight or requirements on a technology. Over-regulation may result in excessive oversight or requirements that make a technology economically unviable. Mis-regulation of a technology may result in both inappropriate and inadequate oversight or requirements, and result in both the harms of under-regulation and over-regulation. Timely assessment and development of appropriate regulatory requirements are critical to the success of commercial fusion technology in the next two decades.

This work examines how licensing and regulation of novel technologies could be based on the fundamental hazards of the technology to provide insights on how to more effectively assess and develop regulatory requirements. This hazard based approach enables the description and characterization of licensing evaluation methods and regulatory frameworks, and assesses their effects on the design, licensing, and operation of regulated activities. The goal of this work is to provide insights to commercial fusion developers and policymakers on the technical and economic tradeoffs of different licensing evaluation methods and regulatory frameworks for the development and deployment of deuterium-tritium commercial fusion technology.

8.1 System engineering model to characterize of commercial fusion facilities operation

Deployment of commercial fusion technology requires developers to demonstrate the safety of a technology that does not yet exist. Evaluation of safety and development of regulatory requirements after significant research and design efforts have been completed would risk the significant capital and time investment required to commercialize fusion technology. Development of initial safety assessments and regulatory requirements before completion of significant design activities is critical to help frame future regulatory discussions and increase commercial assurance that design efforts and regulatory requirements will converge to a societally acceptable and economically viable technology.

The major challenges associated with pre-design evaluation of safety and development of regulatory requirements include:

- required facility systems, inherent operational hazards, and general concept of operations may be unknown for novel technologies that are immature or do not have significant operating experience,

- difficulty in assessing the hazards of a technology before it is designed,
- costs, time, and technical expertise required to develop detailed regulatory requirements for any complex and high hazard technology, and
- potential development of regulatory requirements that preclude or discourage innovative engineering approaches for novel technologies.

These challenges primarily relate to two topics: defining and assessing hazards for novel technologies, and facilitating innovation for novel technologies. This work addresses both challenges by using system functional models.

This work utilizes a systems engineering approach using system function models to facilitate the functional analysis of commercial fusion facilities. This approach allows decomposition of facility requirements into system functions and allocation of system functions into multiple lower level system requirements. This process enables top down development of system functions from high-level system objectives. Development of system functions, interfaces, and performance requirements can be performed without specification of physical system form. Use of function models for commercial fusion technology helps characterize hazards with a focus on inherent function and not design specific form. Models with increasing level of detail can be used to provide greater specificity for certain hazards or enable quantification of previously qualitative hazards. These systems models are initially developed as technology independent; no specific fusion technology (e.g., confinement method, fuel cycle) is assumed and the models are generally applicable to any fusion technology. This approach enables discussion and development of safety analyses and generalized regulatory requirements in a manner that does not discourage innovation and does not assume or prescribe technology specific solutions.

System engineering models for a technology independent commercial fusion power plant are developed with increasing levels of technical detail on hazards and critical plant characteristics. Initial use of a technology independent model enables insights into regulatory frameworks that may be compatible with a variety of technology approaches to fusion energy and do not require technology specific regulatory requirements. The history of commercial fission regulation demonstrates how development of technology specific, prescriptive regulatory requirements may increase short-term regulatory certainty but can discourage technological innovation due to the additional regulatory barriers. A system engineering model specifically applicable to a deuterium-tritium fueled tokamak commercial fusion facility is ultimately developed as the basis for technology specific hazard analyses in this work. The technology specific system engineering model deuterium-tritium fueled tokamak commercial fusion facility identified 39 functional systems that are further assessed for system hazards and regulatory significance.

8.2 Hazard identification and prioritization based on regulatory significance

Commercial fusion facilities will inherently be complex engineering systems due to the specific and extreme physical conditions required to create and sustain fusion reactions. In addition, the limited operating experience and wide variety of proposed fusion technologies ensure that, at the very least, initial commercial fusion facilities will not be operationally well characterized. Evaluating safety based on analysis of initiating accident events may not be appropriate for commercial fusion facilities. Instead, a hazard-center approach to safety evaluations may be desirable.

This work utilizes a hazard-centered approach as the basis for preliminary safety evaluations with the following logical progression:

- what are the inherent hazards of a facility?
- what are the potential adverse consequences associated with the inherent hazards, independent of event sequences?
- what are inherent, engineered, or administrative safeguards or controls are in place to prevent the adverse consequences?
- what initiating events and subsequence events can lead to breakdown of these safeguards and controls?

While the difference between an initiating event centered approach and a hazard-centered approach is subtle, a hazard-centered approach focuses on control and mitigation of hazards rather than on prevention of all accident sequences or initiating events. A hazard centered approach enables the insights of preliminary safety evaluations to be incorporated into the design process because the evaluations are based on inherent system characteristics and not specific event sequences. Incorporation of preliminary evaluations into final facility design facilitates designer focus on limiting inherent hazards rather than trying to prevent all accidents. A focus on eliminating hazards by design can help produce a more robust system, especially for complex or poorly characterized systems.

A repeatable hazard characterization method is developed for the identification and prioritization of hazards with highest regulatory significance based on their potential for significant off-site consequences. This enables the characterization of plant systems with hazards that are most relevant to regulators. This process facilitates the identification of hazards significant for the assessment and development of regulatory requirements for commercial fusion facilities.

This work develops a set of hazards of regulatory interest for commercial fusion facilities based on a D-T tokamak specific system engineering model. The major off-site and on-site hazards of regulatory interest identified in this section are:

- radioactive material
- hazardous materials
- radioactive sources
- explosive materials

Certain hazards, such as neutron radiation sources and handling of radioactive tritium fuel, are inherent to a D-T fusion fuel cycle. These hazards cannot be eliminated through design and operation choices but may be reduced by design. The actual hazards associated with activated radioactive materials, hazardous materials, and explosive materials in a commercial fusion facility will depend significantly on design and operational choices made for a commercial facility.

While the presence of these hazards is noted based on the current concept of operations for such a facility, determination of hazard magnitude and forms is a design specific activity. These hazards are discussed within this work to provide context on the development of regulatory requirements, but it is important to note that not all of the hazards are inherent to fusion technology.

Appropriate implementation of process design methods to minimize hazards by design and research into innovative technological or engineering approaches to reduce hazards could significantly reduce the overall risk associated with off-site and on-site hazards without the needs for engineered safeguards. This hazard reduction approach helps lead to safer designs and safer operation.

8.3 Hierarchical hazard limit model for comparison of regulatory requirements

Regulatory requirements and oversight are used to protect workers, the public, and the environment from the potential consequences of hazardous activities. Hazardous activities may be regulated using three main methods:

- means based: requirements on how specific activity hazards are controlled
- management based: requirements on how a hazardous activity is managed
- performance based: requirements on presence, release, exposure to hazards

The applicability each of these methods varies depending on the specific regulated activity and factors such as the ability of the regulator the monitor an activity to verify compliance and the similarity of different activities being regulated.

Performance based regulatory requirements and performance metrics for the outcomes of management and means based regulatory methods (e.g., harms not prevented by means or management based regulatory frameworks) can be used to compare both regulatory systems and the safety of different regulatory activities. Comparison of these limits and outcomes, however, can be challenging due to significant differences in measurement metrics used by different activities. Radiological material inventory limits, hazardous material emission limits, and car accident fatality rates all characterize hazard consequences of regulated activities but consistent comparison of these hazard consequences is challenging.

A novel hierarchical hazard limit model is developed that enables the comparison of dissimilar limits on hazards and facilitates development of consequence-consistent regulatory limits for commercial fusion technology. This model provides insights on selection of regulatory requirements that better reflect accepted risks for different activities and seeks to facilitate regulatory requirements for commercial fusion that are consistent with other energy generation activities. A hierarchical hazard limit model allows definition of hazard limits for commercial fusion facilities based on other generating technology and not simply based on the limits historically used for fission technology.

Definition and selection of each hierarchical hazard limit presents advantages and disadvantages in terms of the inherent assumptions and conservatisms associated with the hazard limit, as well as the costs associated with monitoring and verifying regulatory compliance. Developing the hazard limits using a consistent model allows commercial fusion facilities to base regulatory limits on societal hazards and not limits based on commercial nuclear fission regulations.

8.4 Licensing evaluation methods for assessment of facility design and operation

Licensing evaluation methods allow the evaluation of facility hazards and demonstrate compliance with regulatory hazard limit requirements. Four licensing evaluation methods widely used for the evaluation of engineered systems are presented. Adaptation of a fifth method, the system theoretical process analysis (STPA) evaluation method, for the regulation of a commercial fusion facility is novel to this work. The technical bases for these evaluation methods are presented, general methodologies are developed and discussed, and a preliminary licensing evaluation of commercial fusion facility or major system is performed for each method. The potential effects of each licensing evaluation method on the design, operation, and regulation of commercial fusion facilities is also reviewed.

8.4.1 Worst-case release evaluation

A worst-case release evaluation determines the maximum possible hazard consequences associated with an activity or facility without regard to event probability. Worst-case analyses for licensing evaluations may be the simplest form of licensing evaluation but can also have the largest inherent conservatisms. This simplified analysis has the potential to minimize the regulatory burden on commercial fusion by eliminating the need to prepare and review detailed regulatory evaluations. A preliminary worst-case release evaluation of tritium hazards D-T tokamak commercial fusion facility suggests that the tritium inventory in some commercial fusion facilities may result in unacceptably high off-site radiation doses. Modifications to facility design (reducing hazard inventory) or updates to facility-specific meteorological and siting characteristics (reducing off-site exposure) would likely be required to demonstrate compliance with relevant regulatory hazard limits for off-site acute exposure to radiological hazards. This licensing evaluation method requires the fewest regulatory resources to complete but will require significant conservatism in design and operation to meet the regulatory limits associated with small hazard inventories.

8.4.2 Maximum credible release evaluation

A maximum credible release evaluation determines the maximum expected hazard consequences associated with an activity or facility based on a qualitative assessment of credible failure mechanisms. Use of maximum credible release analyses for licensing evaluations enables trade offs between decreasing inherent conservatism and increasing regulatory burden. This analysis has the potential to balance inherent hazard design constraints on commercial fusion facilities while still limiting the regulatory burden to those comparable for commercial chemical facilities. A preliminary maximum credible release evaluation of tritium hazards D-T tokamak commercial fusion facility indicates that that major changes would be needed to the facility design or assumptions considered in the analysis to result in acceptable the hazard consequences. Modifications to facility design (reducing inventory), changes to facility operation (reducing inventory at risk), or updates to facility-specific meteorological and siting characteristics (reducing off-site exposure) would likely be required to demonstrate compliance with relevant regulatory hazard limits for off-site acute exposure to radiological hazards. This licensing evaluation method facilitates the use of some engineering principles to reduce facility hazards but will require conservatism in design and operation to meet the regulatory limits associated with controllable hazard inventories.

8.4.3 Deterministic design basis event evaluation

A deterministic design basis evaluation determines the hazard consequences associated with wide range potential initiating events and event sequences that are qualitatively assessed as credible. Use of deterministic design basis analyses for licensing evaluations reduces conservatism from simpler analysis methods and enables the consideration of engineered safety features in hazard consequence analyses. These analyses allow designers and analysts to mitigate significant hazards through the use of active and passive engineered safety features. This approach significantly reduces the calculated hazard consequences for a facility or activity but come at the cost of increased burden of proof and regulatory burden related to systems significant safety and supporting analyses. A preliminary deterministic design basis evaluation of tritium hazards within the tritium storage system at D-T tokamak commercial fusion facility illustrates how use of credited engineered safety features could be used to demonstrate compliance with regulatory requirements. This evaluation method and associated compliance costs would dramatically increase the regulatory costs associated with facility licensing from those associated for industrial chemical facilities to those associated with commercial fission facilities. This licensing evaluation method adds additional regulatory burden and process requirements for commercial fusion facilities but facilitates the credited use of engineering safety features in facility design.

8.4.4 Probabilistic design basis event evaluation

A probabilistic design basis evaluation determines both the hazard probability and consequences associated with sets of initiating events and event sequences. Use of probabilistic design basis analyses for licensing evaluations provides the most detailed analysis of the risk (probability and consequence) of hazardous activities and facilities. This method enables the most realistic modeling of initiating events and evaluation of extremely low probability events without the need to add prescriptive regulatory requirements. The risk insights gained from probabilistic analysis allow applicants to prioritize the SSCs that will contribute greatest to facility risk and safety. This approach significantly further reduces the calculated hazard consequences for a facility or activity but further increases the design, analysis, and regulatory costs associated with facilities. A preliminary probabilistic design basis evaluation of tritium hazards within the tritium storage system at D-T tokamak commercial fusion facility illustrates how use of credited engineered safety feature and fault tree methodologies facilitate compliance with regulatory requirements and reduce the scope of credited safety feature as compared with deterministic analyses. This licensing evaluation method would provide largest degree of design and analysis flexibility based on a realistic assessment of facility design and hazards but also require significant regulatory resources and detailed process requirements for commercial fusion facilities. Development of operational experience for fusion systems, structures, and components would be needed to support use of probabilistic design basis analyses.

8.4.5 System theoretical process analysis evaluation

Use of system theoretical process analysis (STPA) for licensing evaluations is another way to analyze and regulate hazardous activities and facilities. STPA is a paradigm shift for evaluating safety, focusing on the systematic control of hazards rather than identification and mitigation of causal event sequences. STPA enables an extremely comprehensive, system evaluation based on the losses and hazards relevant to all stakeholders. STPA had been previously applied to digital instrumentation and control systems that have technical limitations as commercial fusion technology. The evaluation method can be used to transparently and robustly develop performance based regulatory requirements for any high hazard activity, scaling both based on the size of the system and the level of design. STPA, when integrated into the design process, enables the analysis of system hazards and development of constraints that highlight potential failure modes of interest.

A preliminary STPA evaluation of the tritium storage system at D-T tokamak commercial fusion facility illustrates how operation errors or feedback breakdowns could lead to failure mechanisms not explicitly characterized by other evaluation methods. Certain prescriptive organization safety mechanisms such as quality organizations and change management processes emerge organically as systems important to ensuring long-term safe operation and are traceable to specific hazards and losses of interest to stakeholders. This licensing evaluation method can provide useful insights to the safe design, operation, and maintenance of commercial fusion facilities but it has some unresolved questions related to the high regulatory burden and integration with regulatory requirements. The use of STPA evaluations for the licensing of commercial fusion is unclear without additional work and further examination of regulatory requirements.

8.4.6 Summary of licensing evaluation methods

The five licensing evaluation methods presented in this work are all applicable to demonstrate compliance of commercial fusion technology with regulatory hazard limits. Each method balances the level of analysis detail with the use of conservative regulatory assumptions. At their most fundamental level, they answer the following questions:

- "What is the worst that could happen?" – Worst Case Release Evaluation
- "What is the worst that could realistically happen?" – Maximum Credible Release Evaluation
- "What would happen if…?" – Deterministic Design Basis Event Evaluation
- "What is the risk of…?" – Probabilistic Design Basis Event Evaluation
- "How can this facility lose control? – STPA Evaluation

These methods are all intended to help regulators assess whether an activity demonstrates compliance with regulatory requirements. Each method can be used to demonstrate compliance but will have different impacts on the design and licensing process.

More conservative evaluations (Worst Case Release and Maximum Credible Release) require substantially fewer regulatory resources but require significant limitations on design and operation of commercial fusion facilities to minimize the inherent hazards of a system. This work demonstrates that minimizing radiological inventories (tritium and mobile radioactive materials) by design is essential to demonstrating compliance with these evaluation methods.

More realistic evaluations (Deterministic and Probabilistic Design Basis Event Evaluation) require significantly more regulatory resources but provide designers and operators with flexibility in meeting regulatory limits. This works helps demonstrate how engineering safety features and operational controls can be credited for reducing the consequences of accidents. The characteristics would allow commercial fusion facilities to meet regulatory limits without making substantial changes to facility hazards by design.

The STPA evaluation described in this work may present a new method for the evaluation of facility safety. Its integration with existing regulatory frameworks is challenging due to absence quantitative insights currently produced by the standard analysis method. This work helps demonstrate the broad range of operational insights and requirements that can be generated from review of system operation. Application of STPA evaluations on more detailed designs and further development of regulatory metrics that are compatible with regulatory requirements and frameworks may help demonstrate the feasibility of STPA for licensing evaluations. This method may be particularly useful for the evaluation of novel commercial fusion facilities because it can provide insights on operational challenges that are only normally characterized after developing operating experience with a system.

8.5 Regulatory framework models for licensing of facility design and operation

Regulatory framework models describe regulatory regimes and can characterize different levels of regulatory oversight and relationships between a regulator and the regulated activity. A model of system operating limits to describe unexpected system failures is developed to facilitate discussion of the impacts of regulatory frameworks on system safety. Development of an insurance requirement based regulatory framework for industrial facilities using a strict liability standard and an operational characterization based regulatory framework for full facility regulation are novel to this work. The theoretical bases for each of these frameworks are presented, the major characteristics of each framework are discussed, and the compatibility of each framework with the licensing evaluation methods is assessed. The potential impact of each framework on the regulation of commercial fusion technology is finally discussed.

8.5.1 Insurance requirement based regulatory framework

The insurance requirement based regulatory framework would enable the development of commercial fusion technology with minimal regulatory requirements related to design and operation safety. Commercial fusion companies instead work with private firms to fully insure against maximum hypothetical releases under a standard of strict liability – accepting full accident liability regardless of fault. Commercial fusion companies would be able to operate without major external design requirements if they could successfully utilize design, operation, siting, and analysis arguments to demonstrate sufficiently low facility risk for private insurance companies. Private insurance companies could, however, impose requirements on commercial fusion companies to control and mitigate maximum and expected risks of commercial fusion facilities.

Negotiation of insurance premiums and imposed requirements from private insurance companies would be conducted on a facility-by-facility basis between private companies. These premiums and requirements could represent a minor or significant impediment to commercial fusion depending on the specific facility and requirements. The formal regulatory and impediments with this regulatory framework are minimal but releases could be extremely costly due to the liability requirements on commercial fusion companies. The insurance requirement based regulatory framework is a wager on the free market viability of commercial fusion technology – a convincing safety case and safe operations results in the lowest possible regulatory costs and minimal regulatory requirements. These advantages are complicated, however, by the costs associated with uncertainty in the safety case and any accidental releases that could result in extremely high costs for the commercial fusion industry.

8.5.2 Permit based regulatory framework

The permit based regulatory framework would enable the development of commercial fusion technology under a similar regulatory regime as other sources of energy and industrial facilities. Commercial fusion companies would work with regulators to develop appropriate regulatory limits that satisfy social requirements on potential hazard consequences. The permit based framework provides commercial fusion companies wide latitude in the design and operation of facilities but would hold them accountable for compliance with relevant regulatory requirements. The challenges associated with managing acute hazards would require facilities to consider the impacts of design and inherent hazards on off-site consequences. Minimizing, substituting, mitigating, and simplifying hazardous processes could significantly reduce risk but may not be technically or commercially feasible in all cases. The permit based regulatory framework is based on decades of successful operation of hazardous facilities in the United States but control of acute catastrophic hazards would be key to successful regulation and maintaining social license for commercial fusion facilities.

8.5.3 Delegated review based regulatory framework

The delegated review based regulatory framework would enable the full regulatory review of commercial fusion facilities while reducing regulatory burden and leveraging the expertise of industry in the regulatory process. This regulatory framework has been extremely effective at enabling the safe and economic development of complex, high hazard, novel technologies such as commercial aviation, and it could provide the same benefits to commercial fusion technology. The delegated review based regulatory framework enables regulatory oversight while minimizing the technical burden on regulators and reducing the need to maintain large, highly specialized regulatory staffs. Regulators can on focus independent reviews of safety critical and novel aspects of commercial fusion facilities and emphasize safe overall operation. Initial development of this regulatory framework would be time consuming due to the administrative process requirements for performing delegated regulatory reviews but maintaining public trust through designee independence is critical to realizing the long-term regulatory benefits of this framework. The delegated review based framework could help promote the safe and economic development of novel commercial fusion technology.

8.5.4 Independent review based regulatory framework

The independent review based regulatory framework would enable complete regulatory review of commercial fusion facilities and validate compliance with regulatory limits. The independent review based regulatory framework provides full public oversight of hazardous technologies and builds trust through regulatory transparency and rigorous regulatory reviews. This regulatory framework requires substantial technical expertise to adequately operate. Regulators would need to ensure that new regulatory staff is prepared to independently review proposed novel fusion technologies with limited operating experience. These regulatory processes could be costly and time consuming for both regulators and the commercial fusion industry, and could present a substantial regulatory burden for the emerging industry. The precedent set by the regulation of commercial fission facilities using an independent review based regulatory framework may make use of this framework politically favorable, but the regulatory burden associated with developing and performing independent reviews for commercial fusion facilities may make this framework economically unfavorable. The independent review based regulatory framework could minimize regulatory, policy, and safety questions related to the development of commercial fusion technology.

8.5.5 Operational characterization based regulatory framework

The operational characterization based regulatory framework enables the collaborative development of operational experience and understanding of system behavior to better characterize the safe operation of novel commercial fusion facilities. This framework requires operational transparency from industry with the public but enables the more rapid development of operating experience needed to support mature regulatory requirements without excessive conservatisms. Deliberate development of operating experience, identification and reduction of uncertainties, and a continuous focus on incorporation of lessons learned can help commercial fusion technology rapidly mature by leveraging industry wide expertise and experience. The operational characterization based regulatory framework enables more rapid development of novel, high hazard technologies such as commercial fusion by establishing regulatory limits and processes that will evolve with the operational maturity and understanding of the technology.

8.5.6 Summary of regulatory frameworks

The five regulatory frameworks presented or developed in this work provide different pathways for the licensing and regulation of commercial fusion technology. Each framework balances the roles of an independent government oversight, industry self-regulation, and third party private audits to ensure the safe operation of commercial fusion facilities. The regulatory frameworks used for industrial facilities (permit-based framework) and fission facilities (independent review based framework) have been largely presumed for the regulation of commercial fusion facilities based on legislative precedent but have inherent limitations related to regulation of a novel technology with significant off-site facility hazards. The remaining three regulatory frameworks presented and developed in this work (insurance requirement based framework, delegated review based framework, and operational characterization based framework) all carry distinct advantages for the development and deployment of fusion technologies. These frameworks attempt to accelerate development and deployment of novel technologies by facilitating regulator focus on safety critical issues or shifting regulatory responsibility to private industry while still ensuring financial and social liabilities for accidents.

The development of novel insurance requirement based framework and operational characterization based framework in this work present two radically different but theoretically supported approaches to regulation of commercial fusion facilities. The optimal regulatory framework for commercial fusion technology will likely vary depending on specific technology characteristics and business considerations for private fusion developers. Use of hybrid regulatory frameworks (e.g., selection of different regulatory frameworks for different facility hazards) may be effective at ensuring the optimal regulatory framework for the variety of on-site and off-site hazards present at commercial fusion facilities. Stakeholders will need to work to assess which regulatory frameworks are socially, politically, and commercially tenable to support the development of specific fusion technologies

8.6 Comparison to previous licensing efforts

The licensing experience of both TFTR and ITER provided valuable insights into the licensing prospects for commercial fusion facilities. While these experimental fusion facilities have different operational objectives, concepts of operation, and design characteristics than a commercial fusion facility, they presented the closest relevant regulatory experience for the licensing of large fusion experiments with significant inherent radiological hazards. The experiences at the facilities reflect the challenges of integrating a novel facility into regulatory systems otherwise developed for the regulation of fission reactors or fuel-cycle facilities.

The licensing of major D-T fusion experiments will factor into the development and assessment of future commercial fusion reactors. Historical precedent is commonly used to justify regulatory decision-making. Regulatory and policy makers will need to have clear justification for diverging from existing precedent set by TFTR or ITER for commercial fusion reactors. Clearly characterizing the differences between regulatory frameworks can help increase public transparency with the licensing process and provide a better understanding of the regulatory safety case. These two case studies demonstrated the challenges of regulating novel fusion facilities and highlight the fact that successful licensing is dependent on a number of factors outside of the licensing evaluation method or regulatory framework. The licensing experience of TFTR and ITER illustrate the importance of project management, regulatory engagement, and a technically competent regulator to the successful licensing of a commercial fusion facility.

8.7 Future work

This work provides initial characterization of fusion facility design, hazards of regulatory interest, and hazard limits for commercial fusion facilities using a repeatable and technology independent process. These processes are used as the basis for assessment of hazard licensing evaluation methods and regulatory framework models for commercial fusion facilities and characterization of their impacts on facility design, operation, and commercial viability. These assessments, however, are largely preliminary and intended to provide initial quantitative insights to commercial fusion developers and policy makers.

Several promising areas of future work related to the development of regulatory requirements for commercial fusion facilities are identified:

- more detailed characterization of fusion system design and system hazards

- detailed evaluation of engineering models for non-tritium fusion technology
- quantification and assessment of non-tritium radiological hazards on safety
- quantification and assessment of design constraints based on use of different licensing evaluation methods for commercial fusion facilities
- demonstration of STPA evaluations on more detailed system designs and improved integration of STPA evaluations into regulatory frameworks
- development of more detailed requirement processes and estimation of insurance premiums for insurance requirement based regulatory framework
- development of requirements and methods that can support a operational characterization based regulatory framework for novel technologies
- detailed assessment of the regulatory resources needed to implement various evaluation methods or regulatory frameworks for licensing

These areas for future work would help better assess the impacts of licensing evaluation methods and regulatory frameworks on the development and deployment of commercial fusion technology.

8.8 Conclusions and impacts of this work

This work presents an initial comprehensive approach to the assessment and development of appropriate regulatory requirements for commercial fusion technology. Methods and models based on the fundamental hazards of a technology, with particular focus on D-T fusion, are utilized to help examine the licensing and regulation of novel technologies and provide insights on how to more effectively assess and develop regulatory requirements. Existing methods and models are combined with novel methods and models in this work to better characterize commercial fusion facilities despite limitation on design information, operating experience, and related technologies. These methods and models are applied to help characterize proposed commercial fusion facilities. The tools presented and evaluated in this work can provide policymakers and commercial fusion developers with a common set of methods and models to evaluate and discuss when selecting appropriate regulatory pathways and requirements for commercial fusion facilities.

Development and deployment of commercial fusion facilities by private companies in the next two decades will encounter a variety of technical, social, and economic challenges. Early development of appropriate regulatory requirements for novel technologies can help facilitate commercial efforts and not hinder them. Use of existing regulatory methods based on existing operating experience and the regulatory methods used for similar technologies may result in successful regulation but risks the under-regulation, over-regulation, or mis-regulation of commercial fusion facilities. This work presents methods and models that can help the fusion community evaluate the hazards of commercial fusion facilities and select licensing evaluation methods and regulatory frameworks that satisfy the social and economic constraints on commercial fusion facilities. Regulation is often viewed as inhibiting innovation but the proactive development of regulatory requirements can help maintain social license for fusion technology, facilitate safe operation, and create a stable regulatory environment that will help foster the successful commercial development and deployment of fusion facilities for clean energy production.