Using Risk-Based Regulations for Licensing Nuclear Power Plants: Case Study of the Gas-cooled Fast Reactor

by

Grégoire Jourdan

Diplôme d'Ingénieur, Ecole Polytechnique, Palaiseau, France, 2003

Submitted to the Engineering Systems Division
in Partial Fulfillment of the Requirements for the Degree of

Master of Science in Technology and Policy

at the
Massachusetts Institute of Technology
February 2005

Signature of author.....
Technology and Policy Program, Engineering Systems Division
December 20, 2004

Certified by.....
Michael W. Golay
Professor of Nuclear Engineering
Thesis Supervisor

Read by.....
George E. Apostolakis
Professor of Nuclear Engineering
Professor of Engineering Systems
Thesis Reader

Accepted by.....
Dava J. Newman
Professor of Aeronautics and Astronautics and Engineering Systems
Director, Technology and Policy Program

Using Risk-Based Regulations for Licensing Nuclear Power Plants: Case Study of the Gas-cooled Fast Reactor

by

Grégoire Jourdan

Submitted to the Engineering Systems Division on December 20, 2004
in Partial Fulfillment of the Requirements for
the Degree of Master of Science in Technology and Policy

Abstract

The strategy adopted for national energy supply is one of the most important policy choice for the US. Although it has been dismissed in the past decades, nuclear power today has key assets when facing concerns on energy dependence and global warming. However, reactor licensing regulations need to be changed to get all the advantages of the most promising technologies.

After reviewing the well-known drawbacks of the current regulatory system, the ongoing reforms from the Nuclear Regulatory Commission (NRC) are presented. We argue that full benefice of modern risk analysis methods could not be obtained unless adopting a more ambitious and risk-based regulatory framework.

A risk-based licensing framework is then presented, based on previous research from MIT. Probabilistic Risk Assessment (PRA) analyses are used to drive the design toward more safety, and serve as a vehicle for a constructive discussion between designers and the NRC. Mandatory multilevel safety goals are proposed to ensure that adequate safety and adequate treatment of uncertainties are provided.

A case-study finally illustrates how this framework would operate. It is based on the Gas-cooled Fast Reactor (GFR) project developed at MIT. We show how PRA provides guidance for the design. Especially, PRA work makes designers consider otherwise overlooked uncertainties and find proper solutions. In a second phase, a simulation of the review by the regulator is conducted. Few new safety concerns are brought. The discussion shows that the proposed risk-based framework has been effective. However, it also highlights that improvements of PRA methodology and clarification over the treatment of key uncertainties are needed.

Thesis Supervisor: Michael W. Golay
Title: Professor of Nuclear Engineering

Acknowledgments

I would like to express my gratitude to my advisor Prof. Golay, who gave me the opportunity and the needed freedom to complete this work.

I also wish to thank Prof. Apostolakis from MIT for his help and his very pertinent comments, Prof. Driscoll and Dr Hezlar from MIT for their total cooperation, Kenneth Kiper and Vesna Dimitrijevic from Areva and Wesley Williams from MIT for their frequent technical help.

I want to especially thank my aunt Dominique for her careful proofreading and all my friends and relative who supported me from Cambridge or France.

Table of Content

List of Figures

List of Tables

List of abbreviations

AC	Alternating Current
ALARA	As Low As Reasonably Achievable
ATWS	Anticipated Transient Without Scram
CCF	Common Cause Failure
CCDP	Conditional Core Damage Probability
CDF	Core Damage Frequency
CDP	Core Damage Probability
CV	Check-Valve
CP	Check-Valve (when the coolant is flowing under passive flow)
DC	Direct Current
ECCS	Emergency Core Cooling System
ET	Event-Tree
FT	Fault Tree
FV	Fussell-Vesely
GFR	Gas-cooled Fast Reactor
IE	Initiating Event
LERF	Large Early Release Frequency
LPRA	Living Probabilistic Risk Assessment
LOCA	Loss Of Coolant Accident
LOOP	Loss Of Offsite Power
LWR	Light Water Reactor
MGL	Multiple Greek Letter

NEI	Nuclear Energy Institute
NRC	Nuclear Regulatory Commission
PRA	Probabilistic Risk Assessment
QHO	Quantitative Health Objective
RAW	Risk Achievement Worth
RIR	Risk Increase Ratio
RY	Reactor Year
SCS	Shutdown Cooling System
TMI	Three Mile Island

1. Introduction

With 103 operating reactors, nuclear power produces today 20% of US electricity. The last construction permit for a nuclear power plant was issued in 1973, six years before the accident of Three Mile Island. Since then, due to public safety concern as well as poor economical results, no other nuclear power plant has been built in the US. The problem of nuclear wastes, dramatically underestimated during the early development of nuclear power plants, has become an increasing concern as polemics rise around the choice of a final depository.

However, political interest for nuclear energy is increasing. Nuclear power is one option for reducing carbon emissions. It could be an essential part of a future hydrogen economy. It is also an option to reduce national energy dependence.

Although nuclear energy currently does not compete economically under current conditions with the most competitive energy sources (like coal and natural gas), designers claim that new generations of reactors would allow considerable construction and operation savings. If regulatory, construction, and operating cost uncertainties are resolved, then nuclear power could become very competitive.[1] Its competitiveness would be further increased if the cost of carbon emissions of all sources would be internalized.

The designers of these new reactors also claim they can achieve much greater safety. For example, the new AP-1000 [2] design of Westinghouse has a calculated core damage probability of $2*10^{-7}$. These new designs use passive safety features and new technologies to reach such low values. Such a high reliability could make acceptable the option of a fleet of numerous nuclear power plants.

However, the current licensing framework, presented in Part 2 (after the introductory Part 1), is not adequate for developing a safe and economically competitive fleet of nuclear power plants. Current regulations are deterministic, prescriptive, and would not allow getting full advantage of new design options.

A more rationalist regulatory approach, based on quantitative risk measures, would allow fitting safety requirements to the characteristics of each design. An optimal safety level could be achieved, that would not impose useless burden to the licensees. The outcome of the regulatory process would also be easier to predict.

Therefore, the Nuclear Regulatory Commission (NRC) has initiated a resolute move to include risk measures in licensing safety regulations. However, risk measures would be used indirectly. They would be used to produce more efficient deterministic regulations, but would not allow a rational and predictable case by case safety evaluation of each design. Some inefficiency would thus remain.

We therefore think that it is necessary to investigate the feasibility of a risk-based approach. Although actual risk analysis capabilities would need to be improved to support such a framework, we do not see theoretical grounds for dismissing this option. An iterative framework for risk-based licensing was already presented at MIT.[3] Under this system, risk analysis is driving the design of the new reactors. A discussion is then initiated between designers and the regulator, using the risk analysis as a vehicle for stating informed beliefs. We make a proposal in Part 3 of this thesis for a complete risk-based system based on this framework.

To illustrate the use of this framework, a case study is then presented in Part 4 of this thesis. This case study is based on the project of a generation IV Gas-cooled Fast Reactor (GFR) currently under development at MIT. The risk-driven design phase and the discussion phase with the regulator are both simulated. In Part 5, the main conclusions from the case study to the applicability of the risk-based framework are presented.

2. How to regulate safety of nuclear power plants?

2.1. The role of the regulator

2.1.1. The regulatory agency and its mission

The NRC is the federal agency regulating civilian use of nuclear materials.

Pursuant to the Atomic Energy Act of 1954, the agency is required to ensure that "the utilization and production of special nuclear material... will provide adequate protection to the health and safety of the public".[4]

It is also granted the power to: "[E]stablish by rule, regulation, or order, such standards and instructions to govern the possession and use of special nuclear material, source material, and byproduct material as the Commission may deem necessary or desirable to promote the common defense and security or to protect health or to minimize danger to life or property".[5]

Thus, the NRC has three regulatory functions: (i) to establish standards and regulations; (ii) to issue licenses for nuclear facilities and users of nuclear materials; and (iii) to inspect facilities and users of nuclear materials in order to ensure compliance with the requirements.[6]

Nuclear power plants are complex systems. It is impossible to predict deterministically their behavior. Thus, the main challenge that the regulator has to deal with is the management of uncertainties. The various safety regulatory frameworks constitute different responses to these uncertainties. The different types of uncertainties are therefore first presented, before examining what responses can be introduced.

2.1.2. The different types of uncertainties

Uncertainties can be separated in two broad categories, i.e. aleatory and epistemic uncertainties.[7]

Aleatory uncertainty appears when an event occurs in a random or stochastic manner. Its occurrence can then be described by a probability value. This type of uncertainty is also

qualified of being "irreducible", because it will not decrease with further studies. In contrast, epistemic uncertainty results from to our lack of knowledge and understanding of a phenomenon, and is therefore also referred to as "state-of-knowledge" uncertainty. It can be decreased by further studies.

Three kinds of epistemic uncertainties can be separated:[8 9]

- **Parameter uncertainty:** It refers to our incomplete knowledge on the values of the parameters used in a model. For example, a failure rate or an ultimate strength value may be used in an analysis, although the expert using it is not certain of its true value. These uncertainties can be characterized by establishing probability distributions on parameter values.

- **Model uncertainty:** It refers to the inability of any model (would it be probabilistic or deterministic) to replicate exactly the physical phenomena considered.[10] Thus different models can be proposed for the same process, leading to possible different outcomes. Expert opinions may differ on how the model should be formulated. There is model uncertainty because there is no one right model choice, and any model could possibly give bad results.

- **Completeness uncertainty:** It arises from the fact that it is impossible to foresee everything. The scope of any model or analysis is always limited by what is known. It is impossible to know what has been forgotten in the model. Thus it may stems from a lack of knowledge. It may also come from a deliberate choice, e.g. the analyst may have deliberately excluded something from its model to simplify it. Completeness uncertainty can be considered as a kind of model uncertainty, but because of its importance, it is often considered separately.

All these types of uncertainties are present when analyzing the functioning of a nuclear power plant. Parameters are used in any deterministic or probabilistic safety analysis, but their values are usually uncertain. The models used have been chosen among others, or rest on specific assumptions that are not always respected. Finally, it is impossible to prove that everything has been foreseen.

2.2. The classical regulatory scheme

2.2.1. The development of deterministic safety principles

The first legislation governing nuclear safety is the Atomic Energy Act,[11] enacted in 1954. At this time, no attempt was made to quantify any risk, largely because there was no experience available to do so. It was known that there were important uncertainties, but they could not be quantified.

Therefore, the original philosophy of nuclear safety regulations in response to the uncertainties is one of precaution.[12] The essential elements of these regulations are: (i) conservative design and operations, (ii) large safety margins, (iii) use of design basis accidents (DBAs), and (iv) defense in depth.

Conservative design means that, when they face various hypotheses, designers have to choose a pessimistic one. Using large safety margins means that the components and the whole plant have to be designed to operate far from possible failures. It is a response to parameter and model uncertainty. It is known that deterministic descriptions are not adequate, but it is believed that the variation coming from stochastic behaviors and epistemic uncertainties will not overwhelm the margins.

To define the necessary safety features, the regulators first brainstormed on the question "what can go wrong?". Their goal was to identify all the possible accidents, and then make sure that the plant would be able to withstand them. This gave rise to the Design Basis Accidents system. A design-basis accident is:

> "a postulated accident that a nuclear facility must be designed and built to withstand without loss to the systems, structures, and components necessary to assure public health and safety".[13]

Worst case scenarios are considered and it is assumed that if the plant is able to withstand them, then it will be able to withstand any less serious one. It is a response to completeness uncertainty. It is not possible to predict everything, but the system will be designed to withstand the worst conditions imaginable.

Finally, defense in depth philosophy is used to globally deal with all the uncertainties. It originated in the 1940's, and has been developed in the first nuclear safety regulations in

response to a systematic question: "what if this barrier or safety feature fails? What if I am wrong?"[14] The response was a design and operational philosophy that called for multiple layers of protection to prevent and mitigate possible accidents.[15] An example of this philosophy is given by a 1967 statement[16] submitted to the Joint Committee on Atomic Energy by Clifford Beck. He identified three basic lines of defense: (1) prevention of accident initiators, (2) engineered safety systems to prevent escalating into major accident, and (3) confining fission products or minimizing their escape.

Defense in depth has since been formally defined by the NRC as:

> "...a design and operational philosophy with regard to nuclear facilities that calls for multiple layers of protection to prevent and mitigate accidents. It includes the use of controls, multiple physical barriers to prevent release of radiation, redundant and diverse key safety functions, and emergency response measures."[17]

This philosophy has guided the imposition of redundant safety features, so that no single failure, error, or event could lead to a serious accident.

The safety regulatory system is still based on these deterministic and prescriptive rules. They present important drawbacks that justify their modification.

2.2.2. Drawbacks of deterministic rules

2.2.2.1. Uncontrolled safety

The main drawback of this regulation system, used purely so until the eighties, is that the level of safety in each nuclear power plant is not effectively known. The safety margins are set deterministically, without knowing how they relate to the uncertainties on the system considered. The level of redundancy required is also set arbitrarily, without controlling the efficiency or the utility of the various redundant levels. Finally, it is believed that if the plant is designed to withstand serious accidents, then it will be able to withstand less serious ones. No attempt is made to design adequate response to small accidents.

Therefore it is believed that safety investments have been highly misallocated, focusing sometimes on insignificant safety issues (that are often more expensive to combat) and possibly neglecting the important ones. Enormous discretion is left to the subjective safety evaluation by NRC experts. The industry has had long-standing problems with this safety enforcement method, which has often been found too arbitrary. The Nuclear Energy Institute (NEI) also considers that this policy is "not safety related, timely, or objective." [18]

2.2.2.2. Little incentive for innovation

The prescriptive nature of many of the regulations has made it very difficult for designer to implement innovations. Plants already licensed have to ask for exemptions to implement innovative features not fitting into prescriptive regulations. This process usually takes years, even for minor modifications, and there is clearly no assurance that it will be accepted. As a result, the costs of seeking an exemption are often greater than those of using the traditional technology.

An even more serious consequence is the very high regulatory uncertainty for the new reactors (generation IV reactors). Most of them would be impossible to license under current water reactors based regulatory framework. Should specific regulations be issued to allow the licensing of their reactors, designers would not know what would be the new prescriptive requirements. These uncertainties make it difficult for designers to optimize their work, and they fear that expensive redundant system will be imposed later.

2.3. Attempts to change the regulations

In spite of these drawbacks, the safety record of the actual plants are good. Only one major accident occurred (Three Miles Island accident). However, safety regulations could be improved by using risk analysis methods to allocate better safety expenses. The state of the art in probabilistic risk analysis makes it possible to change regulations. Therefore, the NRC has initiated a crucial change in its regulations so that risk insights could be used systematically.

2.3.1. The usefulness of Probabilistic Risk Assessment

Probabilistic Risk Assessment (PRA) [i] is a systematic method to calculate the failure probability of a system. It is used in situations where the system is so reliable that classical statistics cannot be used because data for some important events are too scarce. The first step in a PRA is to logically identify relevant "initiating events" (IEs), i.e. events that could cause an accident. Then, event trees are drawn to describe the possible sequences of events from the IE to possible accidents. The failure probability at each step of the event tree is quantified using fault tree logic. This is a deductive method in which a final outcome is assumed and the failures leading to it are logically determined. The system causing the failure is decomposed logically into its subsystems, which are then further decomposed. The process stops when data are available for the components in each branch of the tree. It is then possible to go down to up and get the failure probability of the whole tree, integrate it in the event tree, and finally get the probability of the accident sequence.

The first large-scale application of PRA for nuclear safety was the famous Reactor Safety Study (WASH-1400) [19] led in 1975 by Rasmussen. It was the first attempt to describe logically the safety issues that nuclear power plants were facing. According to a comprehensive review, it was successful "in making the study of reactor safety more rational... and in delineating procedures through which quantitative estimates of the risk can be derived for those sequences for which a database exists." [20] It was, however, initially dismissed because of the inadequate treatment of the uncertainties that it highlighted. It had

---

[i] PRA is defined as "a systematic method for addressing the risk triplet as it relates to the performance of a complex system to understand likely outcomes, sensitivities, areas of importance, system interactions, and areas of uncertainty. The risk triplet is the set of three questions that the NRC uses to define "risk": (1) What can go wrong?, (2) How likely is it?, and (3) What are the consequences?. NRC identifies important scenarios from such an assessment." NRC web-site glossary, http://www.nrc.gov/reading-rm/basic-ref/glossary/probabilistic-risk-analysis.html

to be reconsidered after the Three Mile Island (TMI) accident four years later in 1979, [ii] when it became clear that it could provide essential risk information that was overlooked by the traditional approach.

Since then, PRA has been increasingly used. Additional PRAs performed in the US and abroad have allowed making important methodology improvements.

A letter from the NRC Advisory Committee on Reactor Safeguards presents the main achievements of PRA. [21] Now, the fundamental questions "What can go wrong?", "How likely is it?", and "What are the consequences?"[22] can be quantitatively addressed. Thousands of accidents are considered through PRAs, in contrast to the few represented by the design-basis accidents system. Although completeness is always an issue, the application of PRA by diverse practitioners makes it less and less likely that major contributors are not identified. Quantification of accident sequences is now possible, and risk contributors are ranked. PRA also allows analyzing facilities as integrated systems and implementing important safety improvements. Resources can be used for the most safety important sequences and risk is more effectively managed. Thus, since industrials begun to perform plant specific PRAs, the number of IEs has decreased substantially (threefold between 1987 and 1995).[23]

In spite of all these achievements, nuclear safety regulations in the US have used only marginally risk insights. Current regulations are largely based on deterministic analyses that do not take into account quantitative risk measures.[24]

2.3.2. The NRC move toward Risk-Informed regulations

Aware of these challenges, the NRC has initiated a move toward the use of PRA in regulations when it issued a Policy Statement in 1995 on the use of PRA, [25] stating that:

[ii] One very important finding of WASH-1400 was that small loss of coolant accident and human errors had an important contribution in the overall risk. TMI accident was caused by a small loss of coolant accident and a series of human errors.

> "The use of PRA technology should be increased in all regulatory matters to the extent supported by the state-of-the-art in PRA methods and data and in a manner that complements the NRC's deterministic approach and supports the NRC's traditional defense-in-depth philosophy".
>
> PRA and associated analyses should be used "to reduce unnecessary conservatism associated with current regulatory requirements".

PRA has since been used in some particular safety rules. For example, the Maintenance rule (10 CFR 50.65), which was implemented in 1996, integrates PRA insights to rank components according to their risk-significance. Regulatory Guide 1.174 [26] has provided a framework for plant-specific decisions based on risk information and initiated by the licensees.

Currently, the NRC is preparing an important reform of its procedures to move toward risk-informed regulations, that the agency defined as:[27]

> "...an approach to regulatory decision making that uses risk insights as well as traditional considerations to focus regulatory and licensee attention on design and operational issues commensurate with their importance to health and safety."

Although no definitive decision has been taken yet, the current thinking is to use the risk insights at a high level, only to determine the appropriate deterministic requirements:

> "Established quantitative health objectives (QHOs) and related subsidiary quantitative objectives will be used to guide the development of risk-informed regulatory requirements. The intent is to develop requirements, which retain deterministic characteristics, in such a way that compliance will provide reasonable assurance of meeting the principal goal of protecting public health and safety. The quantitative objectives provide risk-informed guidance for the establishment of practical and enforceable regulatory requirements. They do not represent acceptance criteria and will not generally appear in risk-informed regulations."[28]

This statement emphasizes that the licensees will not have to prove that they meet any quantitative safety objective. Quantitative risk values would be used to select appropriate deterministic requirements, but they would not appear in the regulations themselves. Thus, DBAs and deterministic requirements would still be the center part of licensing regulations. Risk insights would be used only to select which DBAs would be the most important to consider.

QHOs and "subsidiary quantitative objectives" have already been proposed to define "Quantitative Objectives for Risk-Informing Regulatory Requirements".[28] They are reproduced on Table 2-1 and their justification is presented in Part 2.3.3. The underlying strategy is to:

> *"1. limit the frequency of accident initiating events (initiators)*
> *2. limit the probability of core damage given accident initiation*
> *3. limit radionuclide releases during core damage accidents*
> *4. limit public health effects due to core damage accidents"*[28]

The distinction of several levels of risk objectives is an application of defense in depth philosophy.

These objectives will constitute a high-level treatment on uncertainties. No compliance with any quantified uncertainty limit will be required, but they will ensure that globally an "appropriate" balance has been achieved.

From the design perspective, uncertainties will still be treated by safety margins.[28] In some cases, safety margins will be defined probabilistically, i.e. the probability that the stress would be higher than the capacity will be calculated. In other cases, the current practice will be kept and conservative or bounding calculations will be used to demonstrate that the safety margins are acceptable.

2.3.3. NRC's Quantitative Health Objectives

As part of its move toward risk-informed regulations, the NRC has been trying to define acceptable levels of risk. QHOs have been defined in the Safety Goal Policy Statement (1986).[29] The approach taken is to compare the additional risk from the nuclear power plants for the persons leaving near the plant to the risk from all the other accidents and from cancer:

> "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%) of the sum of prompt fatality risks resulting from other accident to which members of the U.S. population are generally exposed.
>
> The risk to the population in the area of nuclear power plant of cancer fatalities that might result from nuclear power plant operation should not

exceed one tenth of one percent (0.1%) of the sum of cancer fatality risks resulting from all other causes."

Considering the accident and the cancer risk in the U.S., these objectives translate in respectively $5*10^{-7}$ and $2*10^{-6}$ fatalities per year.

These goals should then been compared to the results of a level 3 PRA [iii] for each plant. However, due to the considerable uncertainties involved in performing a level 3 PRA, and consistently with the defense in depth philosophy, the NRC has developed lower level objectives: Core Damage Frequency (CDF) and Large Early Release Frequency (LERF). 10^{-4} / Reactor Year (RY) for the CDF and 10^{-5} / RY for LERF are the guidelines used.[30]

Based on these considerations, the NRC has proposed Quantitative Health Objectives.[31] They should be used as risk guidelines for issuing new risk-informed regulations for light-water reactors (see Table 2-1). It is still not clear whether higher safety would be required or not for advanced reactors, although NRC's staff currently favors the same standards for all reactors.[32]

[iii] Three levels of PRA are usually distinguished for nuclear power plants. Level 1 PRAs only study the progression of the accidents until core damage, the level 2 PRAs evaluate the response of the containment to the core damage, and finally level 3 PRAs evaluate the transport and consequences of radionuclide releases for each accident sequence.

(1) Prevention-Mitigation Assessment: Consider the Strategies in Pairs

Prevent	Mitigate
Core Damage Frequency $\leq 10^{-4}$ / year	Conditional Probability of Early Containment Failure ** $\leq 10^{-1}$

(2) Initiator-Defense Assessment: Consider the Strategies Individually (Preferred)

	Limit the Frequency of Accident Initiating Events (Initiators)	Limit the Probability of Core Damage Given Accident Initiation	Limit Radionuclide Releases During Core Damage Accidents	Limit Public Health Effects Caused By Core Damage Accidents
	Initiator Frequency	Conditional Core Damage Probability	Conditional Early Containment Failure Probability**	Conditional Individual Fatality Probability
Anticipated Initiators	≤ 1/year	$\leq 10^{-4}$	$\leq 10^{-4}$	*
Infrequent Initiators	$\leq 10^{-2}$/year	$\leq 10^{-2}$	$\leq 10^{-1}$	*
Rare Initiators	$\leq 10^{-5}$/year	≤ 1	≤ 1	*

Notes:

The product across each row gives LERF< 10^{-5}/year. Responding systems and procedures are not designed for rare events. When applying the quantitative objectives of this figure, in general, no individual initiator sequence should contribute more than 10% of the value listed.
* No quantitative guideline proposed, using LERF as a surrogate.
** This strategy does not imply that risks associated with late containment failure can or will be ignored. Potential causes of late containment failure and associated mechanisms for radionuclide removal prior to containment failure will be considered. A quantitative guideline of <0.1 is proposed for the probability of a late large release given a core damage accident.

Table 2-1: NRC Quantitative Health Objectives and surrogate risk guidelines [33]

2.3.4. The limits of Risk-Informed regulations

Although risk-informed regulations would clearly represent an improvement compared to the current system, the regulations would still be deterministic, and would therefore keep most of the drawbacks presented previously.

Using risk inferences to define DBAs should reduce the current inefficiencies of DBAs addressing too rare sequences and potentially forgetting important ones. However, because risk-insights would be used at the regulation level, the deterministic requirements will not

have the same efficiency for all the designs. They would also require the formulation of a design as the basis for the deterministic prescriptions. As the optimal balance between safety features should *a priori* change for different designs, the risk-informed framework will continue to impose non useful requirements. The level of safety obtained in each plant would not be known either, and important safety discrepancies could be maintained. Finally, the persistent use of conservative deterministic safety margins will perpetuate undue conservatism.

But above all, potential plant specific PRA information will not be used optimally. First, it is not clear whether a plant specific PRA would be required. Risk-informed regulations do not require plant specific PRAs, although such additional information would improve regulatory decision-making.[34] Neither is it clear whether any quality standard for PRA would be enforced. PRAs are expensive to conduct, so that in the absence of specific high quality requirements, plants will have little incentives to conduct high quality PRAs. Possible valuable insights could be lost. The investments in PRA third party reviews would probably be low. Finally, with no high quality plant specific PRA, it would be harder to handle uncertainties properly. It is likely that uncertainties will not be systematically quantified and integrated in the analysis.

2.4. The risk-based approach

In a risk-based approach, a risk limit is stated explicitly in the regulations. To prove that they meet the limit, a licensee has to perform a full-scope risk analysis of his plant. This analysis would be reviewed extensively by the regulator or a third party.

Such a process ensures that all the plant-specific risk information is considered and logically integrated. The review should grant that the risk analysis has been appropriate.

This approach first requires formulating all the success criteria probabilistically. For any system considered, the uncertainty on the stress and on the capacity would both have to be quantified. Uncertainty distribution of both the stress and the capacity instead of point values will have to be used as model inputs. This can represent a major challenge. Some work has already been done on passive systems to quantify probabilistically the success of specified

safety functions.[49] [55] In several cases, expert judgment will have to be used and probabilistically expressed. This should be accepted as long as appropriate justification is brought into the analysis.

The opposition to a risk-based approach has been motivated by current limitations of PRA methods. The most important limitations identified are: the quantification of human errors, common cause failures (CCFs), modeling uncertainties and use of engineering judgment, and the integration of component aging, and safety culture.[35]

However, these limitations do not seem to be theoretical limitations of PRA. Progress is made in each of these domains. More realistic models are proposed to deal with human errors. The NRC Human Reliability Handbook [36] already provides reasonable models for evaluating human performance during routine activities. Other models are being developed to use during accident conditions. Concerning CCFs, extended databases have been developed by the NRC, with data collection from 1980 to 2001,[37] which allow a more accurate estimation of CCF events. New methods are being investigated for handling model uncertainties.[38] Engineering judgment should be stated systematically and integrated in the PRA uncertainties. Adequate PRA standards and careful peer review should encourage engineers to make their judgments explicit. Training in probabilistic theory can help experts to elicit their knowledge.

The development of living PRA (LPRA) techniques [iv] is very promising. It can allow integrating the effects of component aging. As inadequate preventive maintenance could cause an increase in repair maintenance and failure rates measured in the plant, its effects could be integrated into the LPRA. This could also be an indication for bad safety culture. Moreover, LRPA will introduce constant safety concerns in the plant and could, thus, increase the safety culture.[39] International experience shows so far that LPRA implementation has led to more plant-specific data collection. It has also increased

[iv] LPRA is a method to update a plant specific PRA sufficiently frequently so that the risk insights remain valid at all times

cooperation between plant staff and PRA analysts, so that plant safety will regularly be reviewed by measuring the actual plant experience against PRA results, input data, models and assumptions.[40]

Finally, a different approach could be taken for different domains of nuclear power plant safety regulations. It is proposed in this study that a risk-based framework should be taken for the licensing of new designs. However, this does not preclude adopting deterministic rules for other domains, in which a purely risk-based system approach, although conceivable, may be harder to implement. For the plant construction phase, deterministic rules could be adopted, as long as they are conforming to an underlying risk analysis. Concerning the actual operation and management of the plant, sole LPRA monitoring may be insufficient to prevent any kind of management misconduct. Prescriptive rules will probably be needed.

To conclude, although it is true that the current PRA state-of-the-art does not support risk-based regulations, there seems to be little argument against the theoretical application of risk-based regulations. Therefore, in the light of the advantages that a risk-based regulatory framework would bring, improving PRA methods should be one of the highest NRC priorities. However, the regulator will also need to investigate how to use quantitatively risk information for design guidance and approval. This is the purpose of this study to propose a risk-based regulatory framework and illustrate on a specific case study how it could be used by the designers and the regulators.

3. PROPOSED RISK-BASED FRAMEWORK

The principle of risk-based regulations is clear: a risk limit has to be respected. The first step is thus to define the risk threshold. Once this limit is set, the licensee can optimize his design to achieve the desirable safety. In a process proposed by MIT,[3] a discussion is initiated between the licensee and the regulator about the appropriateness of the design from early design stages. This discussion uses the PRA as a vehicle to state informed beliefs. It can ensure that the views of the designers and of the regulator are in agreement. Before the license would be granted, an extensive review of the PRA would be performed.

3.1. Setting quantitative goals – an example

3.1.1. A matter of policy

However powerful it may be for safety analysis, PRA is only a tool to apply a given policy. In any regulatory framework, the use of PRA is conditional on the determination of a set of quantitative goals by the regulator.

Therefore the next questions are: who should decide on the risk acceptability levels? What should this level be?

One could argue that this choice should be left to scientific experts. Based on objective scientific information (such as how much risk people usually accept for what benefit), it would be possible to set objective safety goals for nuclear power plants operation. However, a variety of studies clearly show that the approach taken by experts is never value-free.[41, 42] As pure science does not give any answer, the question of risk acceptability cannot be a political-neutral determination. It must therefore involve some non-scientific decision-making and political decision-making.[43]

The statutes of the NRC require that "adequate safety" should be ensured, but no guideline is given to translate it into quantitative limits. Moreover, the courts have ruled "the level of adequate protection need not, and almost certainly will not, be the level of 'zero risk'".[44] Therefore, the NRC has some room to define a quantitative level of acceptable risk.

The definition of QHOs by the NRC constitutes a first step in this direction. Our proposal for safety goals will be based on them, but we will insist on the treatment of uncertainties and we will choose slightly more stringent safety goals.

3.1.2. Higher goals for advanced reactors

We see four reasons to justify taking more stringent standards for advanced reactors.

First, the risk thresholds would be the center part of licensing application. The designers would be granted a license if they prove that they respect the thresholds with appropriate consideration of uncertainties. In contrast, in the risk-informed framework developed by the NRC, the risk threshold would only be part of the licensing process. Therefore it is justified that, by making them the only requirement, the risk threshold would be made more stringent.

Second, advanced reactors will include several safety enhancements that should enable them to reach higher levels of safety at a lower cost.[v] Thus, requiring higher level of safety would be a high level application of the As Low As Reasonably Achievable (ALARA) principle. Moreover, current PRAs have shown that several of the current reactors would meet a 10^{-5} /RY CDF threshold, although they were not optimally designed to meet it. Although the quality of their PRA may be insufficient in a risk-based regulatory framework, it shows that it is not unreasonable to require higher standards.

Third, the uncertainties related to many of these new technologies will be higher than the one used for current reactors. It will therefore be part of the defense in depth strategy to require a higher safety standard.

Finally, the current guideline of 10^{-4} /RY for the CDF is rather high. Core damage accidents, even without any release to the environment, are very harmful for the entire nuclear sector. Public reaction to such events is likely to be irrational and call for the end of nuclear power. The TMI accident showed us that core damaging accidents should be avoided, if durable

---

[v] For example, in their PRA, AP-1000 designers claim to achieve a CDF of $2.4*10^{-7}$ and a Large Release Frequency of $1.95*10^{-8}$

public trust toward nuclear power is to be built. Therefore, a very low CDF should be imposed, independently of public health objectives. It is a goal in itself. With a mean CDF at 10^{-4} /RY and around 500 nuclear power plants in the world, we would expect 1 core damage accidents every 20 years, and one in the US every 100 years. There would be even more if the number of nuclear power plants is to be increased significantly. Considering the uncertainties, the chances that the frequency of core damage accidents would be higher are substantial. The need to avoid any core damage accidents in the years after new nuclear power plants construction justifies the imposition of a lower CDF level.

3.1.3. Proposed safety goals for advanced reactors

The philosophy underlying the proposed safety objectives is illustrated on Figure 3-1. It is consistent with NRC's current thinking of risk acceptability.[8] Current reactors are in the tolerable region, and have a small chance of being in the unacceptable region, due to the uncertainties. **Future reactors should be in the acceptable region, with small chance of being in the tolerable region, and practically no chance of being in the unacceptable region.**

To apply such a statement, both a best estimate and an uncertainty limit goals have to be established. The best estimate value would ensure that the future reactors will stand in this acceptable region. Additional epistemic uncertainty treatment has to be required to ensure that there will be only a little chance that the future reactors will be in the tolerable region. It would thus be a two-part safety requirement.

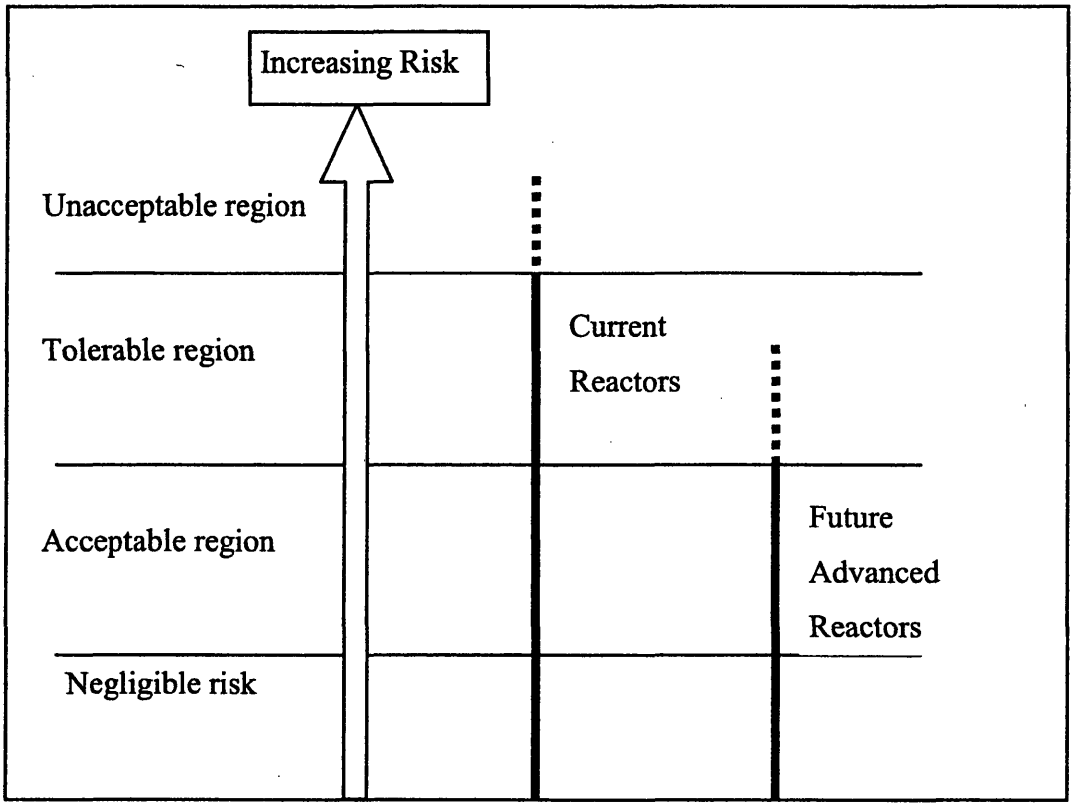


Figure 3-1: Risk acceptability for current and advanced reactors[8]

Tolerable and acceptable risk levels have to be defined. These levels could be based on the $5*10^{-7}$ fatalities per year limit defined by the NRC. For example, the tolerable limit could be set at $5*10^{-7}$ fatalities per year, and the acceptable limit at $5*10^{-8}$ fatalities per year. The best-estimate part of the safety goal could be expressed with a mean fatality number, and the uncertainty goal could be a limit on a high percentile, e.g. the 95th percentile (often chosen because it makes calculations easier).

Thus a global safety requirement could be stated as:

- **A limit for the mean: $5*10^{-8}$ fatalities per year,**

- **And a limit for the 95^{th} confidence level: $5*10^{-9}$ fatalities per year.**[vi]

A purely risk-based approach would require the satisfaction of these goals only. Although regulations may tend to such an approach in the long run, we think that the current state of the art for uncertainty analysis and the current safety approach require a more stringent control of uncertainties. Consequently, we propose to introduce explicitly defense in depth requirements in the regulations.

3.1.4. Advanced treatment of uncertainties

The defense in depth philosophy has been a convenient and powerful way to treat uncertainties. We saw nevertheless that, applied without any risk insight, it is believed to have led to inefficient safety allocations.

There are today two schools of thought on how defense in depth should be applied in a risk context.[14]

The "structuralist" (or "traditionalist") approach on defense-in-depth asserts that it should be "embodied in the structure of the regulations and in the design of the facilities". Specific barriers of protection are required in the regulations themselves. The four traditional lines of defense are introduced Part 2.3.2.

In contrast, in the rationalist approach, defense-in-depth "is the aggregate of provisions made to compensate for uncertainty and incompleteness in our knowledge of accident initiation and progression".[14] Thus, given a quantitative goal, rational defense in depth application is

---

[vi] These goals are slightly more stringent than the one currently proposed at the NRC (see Part 2.3.3). Some justifications is presented in Part 3.1.2 for setting more stringent goals for advanced reactors. However, as explained in Part 3.1.1, setting quantitative goals is primarily a policy matter and it is out of the scope of this study to enter safety policy questions.

the process through which the designer ensures that the goals have been achieved and all the analytical uncertainties treated. The purpose of defense in depth is to "to increase the degree of confidence in the results of the PRA or other analyses supporting the conclusion that adequate safety has been achieved".[14] In the face of important uncertainties, the designer could choose to add another barrier or to try to decrease the epistemic uncertainties by performing new tests or simulations. Both possibilities would be an application of the rationalist approach of defense in depth.

We propose to apply a combination of both approaches. This is consistent with the recommendations of some members of the Advisory Committee on Reactor Safeguards of the NRC.[14] Figure 3-2 illustrates the overall safety strategy.

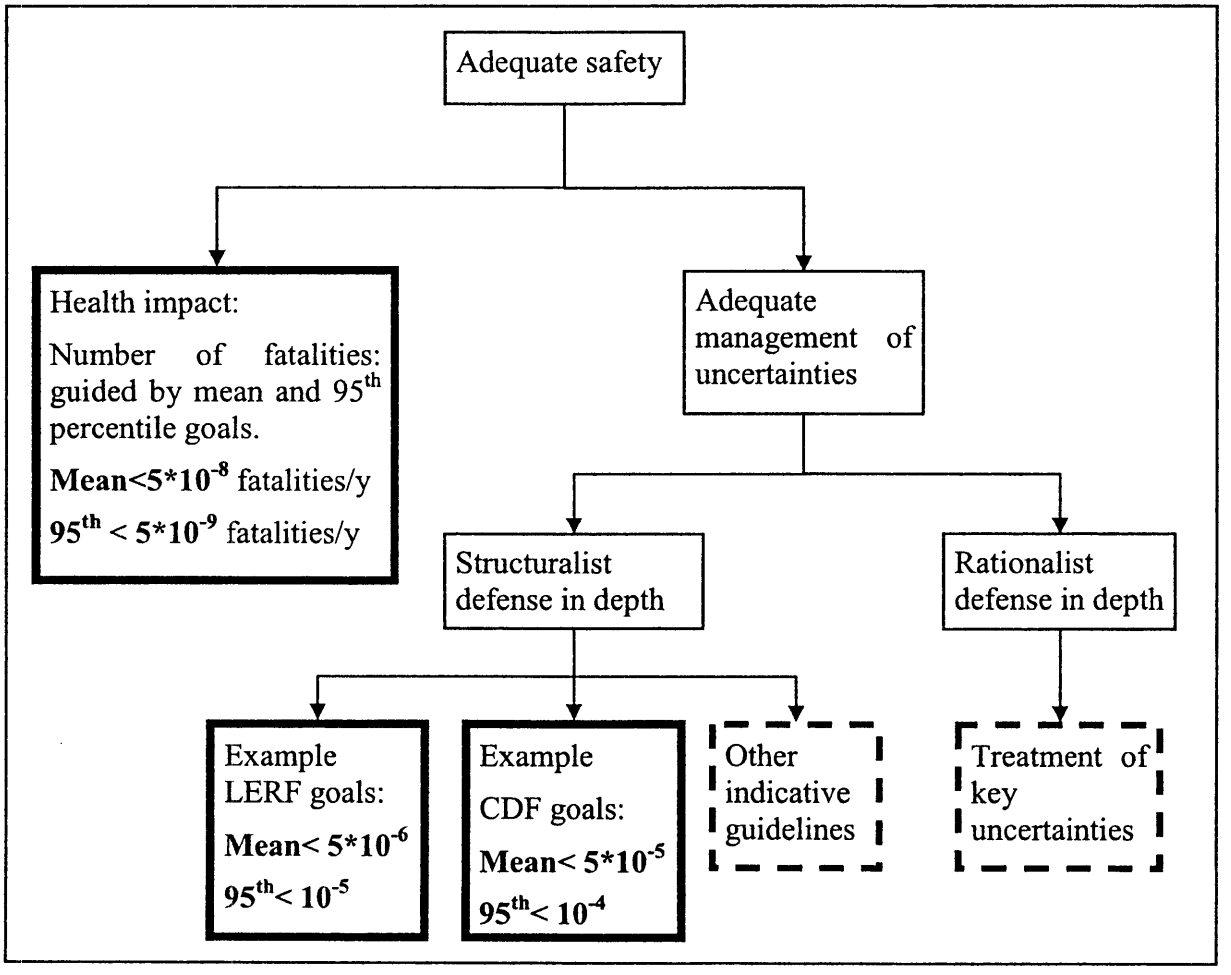


Figure 3-2: Multiple safety goals for a risk-based framework

Structuralist defense in depth:

We propose to use here the traditional distinction between CDF and LERF. Again, the risk values are stated in terms of mean and 95th percentiles values. Indeed, uncertainties have to be explicitly controlled at every level.

Thus a global safety requirement could be stated as:

The mean CDF shall be under $5*10^{-5}$ per reactor year and the 95th confidence level shall be under 10^{-4} per reactor year.

The mean LERF shall be under $5*10^{-6}$ per reactor year and the 95th confidence level shall be under 10^{-5} per reactor year.

Just like the previous global safety goals, these values are proposed examples for the purpose of this study. The CDF and LERF requirements are slightly more stringent than what is currently proposed.

Setting these intermediate thresholds serves two purposes. The first is related to the traditional idea of safety allocation between several barriers. The purpose is to avoid reliance upon one single barrier, because it is feared that this unique barrier, although theoretically very reliable, might have been badly evaluated or affected by an unforeseen event.

The second reason for setting intermediate goals is that, even if they do not lead to any fatalities, core damage and radioactive material release are harmful events in themselves. Any core damage accident could jeopardize public acceptance of civil nuclear power. The effect of release of radioactive materials would be even worse. Extreme reaction should be expected, even if there were no fatalities. Therefore it is justified to set intermediate goals for the CDF and the LERF.

Finally, we propose voluntary guidelines for the review and the design. The purpose of these guidelines is to avoid reliance upon a single sequence of events. Indeed, should the

probability of this single sequence be slightly under evaluated, then the impact on the risk would be high. The guideline could be expressed as: ***no single event sequence should contribute for more than 5% of the mean risk threshold.*** Another possibility would be to state a similar criterion at the initiating event level: ***the total contribution from the sequences of one initiating event should not be more than 10% of the mean risk threshold.*** [vii,viii] It should be emphasized that these two limits have been chosen arbitrarily. The precise number is not crucial, as these limits should not be seen as strict requisite, but rather as trends to follow to increase the confidence in the safety achieved.

Rationalist defense in depth:

It is harder to guide the application of the rationalist defense in depth concept. Indeed, this concept lies precisely in the idea that the designer should be able to choose the best way to increase the safety and decrease the uncertainties. Therefore, there can be no strict requirement for the application of rationalist defense in depth (except to meet the high level safety goals).

[vii] It is important to note that these guidelines are expressed in terms of percentages of the risk threshold, and not of the risk level actually achieved by the design. The robustness concept here is distinct from the "balanced design" view that would require that there would be no sequence accounting for more than some percentage of the risk of the plant. Consider a design with a CDF of 10^{-6} and with a sequence accounting for 50% of the CDF (i.e. leading to core damage with a $5*10^{-7}$ probability). Then, even if the design is clearly not balanced, it is very far from the risk threshold and should be considered as robust.

[viii] The NRC is currently requesting that no individual initiator contribute for more that 10% of any of its surrogate risks thresholds (see Table 2-1). The effect of this request may depend on how initiators are being defined. We think that the most important level is that of the sequence, because it represents the actual failure of safety strategies. We did no want to keep the NRC's distinction between anticipated, infrequent and rare, as such rigid classification can induce an incoherent risk treatment: initiators with a probability of 10^{-2} would be frequent initiators, and would be requested to have a CCDF of 10^{-4} and a CDF contribution of 10^{-6}, whereas for one with a probability of $5*10^{-3}$ the CCDF threshold would be of 10^{-2}, leading to a CDF contribution of $5*10^{-5}$. In this example, there would be a factor 50 between how both initiators would be treated.

However, the rationalist approach of defense in depth commands that particular attention should be brought to the treatment of key uncertainties and key assumptions. [ix] We give an illustration of how to identify key uncertainties regarding event failure probabilities. Key uncertainties will arise concerning failure probabilities that can have a high contribution to the total risk. Therefore it will concern events having a high value of the Risk Increase Ratio (RIR, also called Risk Achievement Worth [RAW]). As key uncertainties are related to domains were there is no knowledge consensus, a simple diagram RIR-"State of knowledge" illustrates the position of key uncertainties (see Figure 3-3).

[ix] From NRC Regulatory Guide 1.200:[59] *A key source of uncertainty* is one that is related to an issue in which there is no consensus approach or model (e.g., choice of data source, success criteria, reactor coolant pressure seal loss-of-coolant accident model, human reliability model) and in which the choice of approach or model is known to have an effect upon the PRA results in terms of introducing new accident sequences changing the relative importance of sequences, or affecting the overall CDF or LERF estimates that might have an impact on the use of the PRA in decision making. *A key assumption* is one that is made in response to a key source of uncertainty.

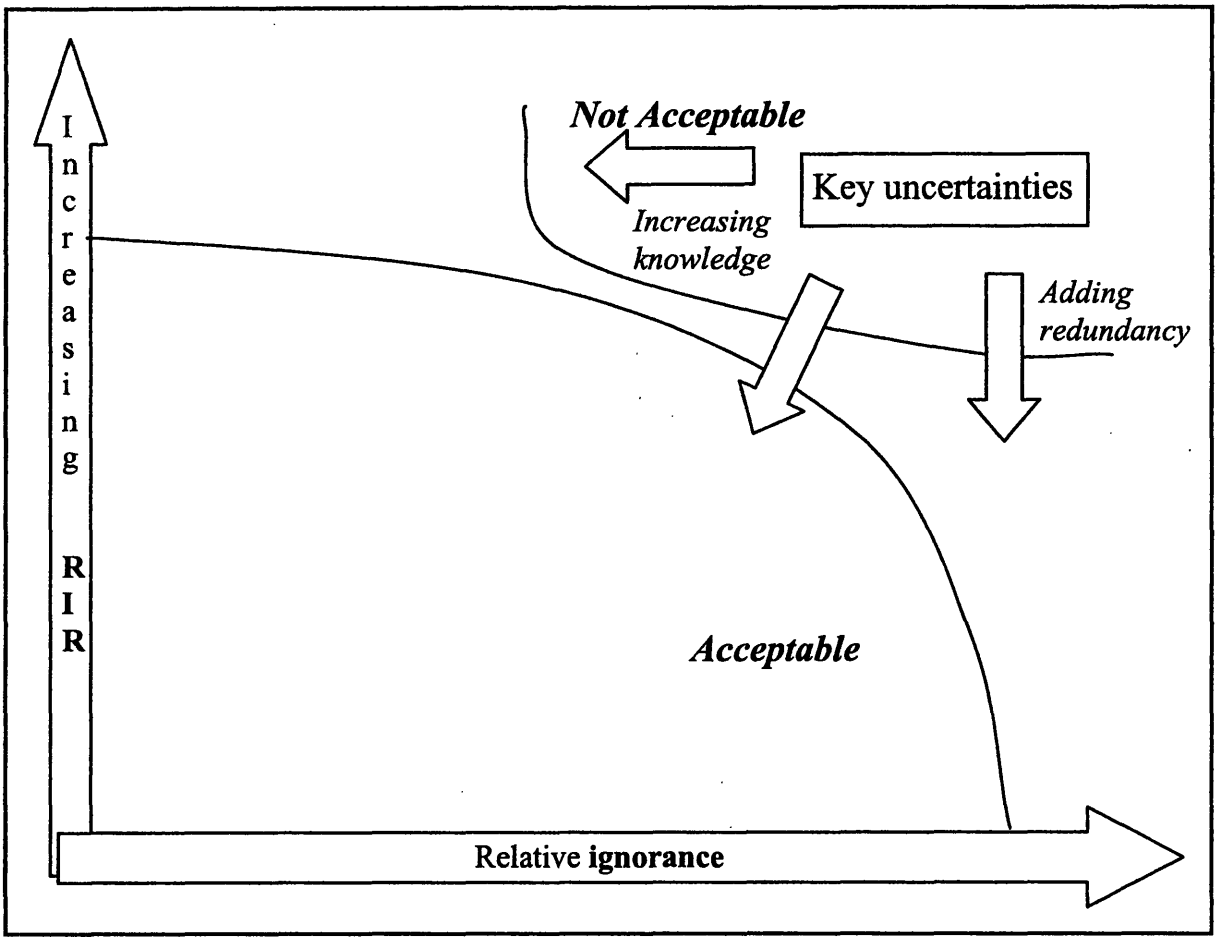


Figure 3-3: RIR-"Sate of Knowledge" generic diagram

Here, the abscissa is a subjective representation of the scientific state of knowledge on basic events. The failure probabilities that could represent key uncertainties are located in the right upper part of this diagram.

The treatment of key uncertainties and assumptions will have to be done case by case. The licensee will have to lead careful analyses and present all the evidence for the peer review and the NRC review. When facing key uncertainties, a general alternative for the designer will be to increase its knowledge (e.g. by doing additional tests or modeling) or to add redundancy so that the failure considered would have a smaller effect upon the total risk. In the case study of Part 4, we present how the design team could identify and deal with some key uncertainties.

The defense in depth strategy is summarized on Figure 3-4.

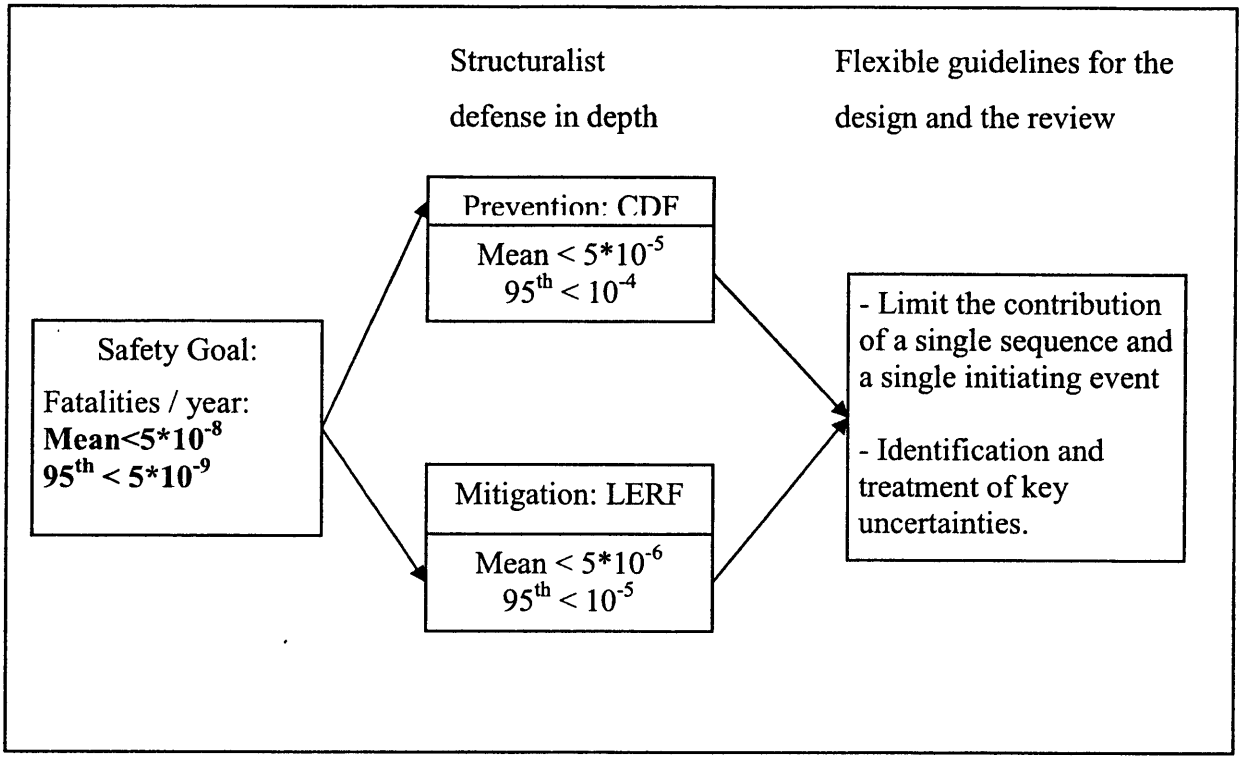


Figure 3-4: Levels of defense in depth.

3.2. Risk-Driven design

In the absence of prescriptive deterministic requirements to guide the design of new plants, concerns of safety and economical efficiency will drive the design choices.

A methodology has been proposed [45] to integrate all the relevant parameters before choosing a specific design option. Safety, economics, and stakeholder relations are evaluated. Such a methodology applies best when most of the design is already known.

At earlier stages of the design, economical information is not easily obtained, and stakeholders' positions are not known. In contrast, the safety impact of design options can be evaluated, using the best available generic failure values together with expert subjective judgment.

A methodology to guide the design from the earliest stages has been proposed at MIT.[3] It is reproduced on Figure 3-5. The first proposed design includes only the most basic features to produce electricity from a specific plant type. This is the "bare-bones" plant. This design is then deterministically analyzed to identify paths to unacceptable consequences. Then a PRA is made to identify the main failure modes. The PRA results are compared with safety goals (e.g. CDF or LERF mean or 95^{th} percentile, depending on the stage of the design). Safety features are then added to mitigate the main failure modes, until the design meets the safety objectives.

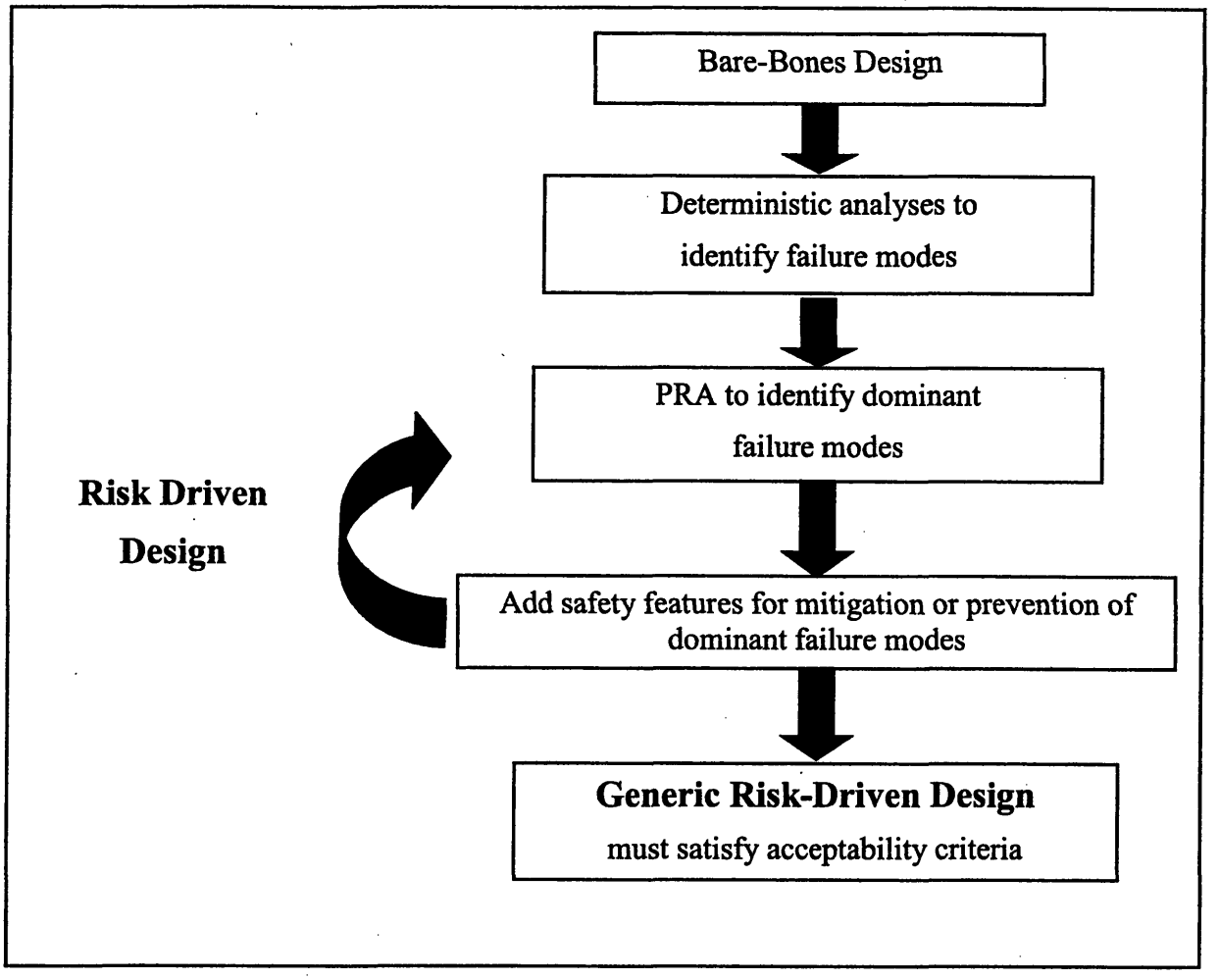


Figure 3-5: Schematic Diagram of the Risk-Driven Generic Design. [3] Several iterations are typically needed to satisfy the acceptability goals.

This methodology would be used regularly during the design evolution. Depending on the advancement of the design, the safety goals could be only an individual IE limit, or several higher levels limits.

Designers will then ask for a review of their design by the NRC.

3.3. The use of PRA as a Bayesian tool: the MIT iterative framework

Figure 3-6 illustrates how the review of the design will take place.

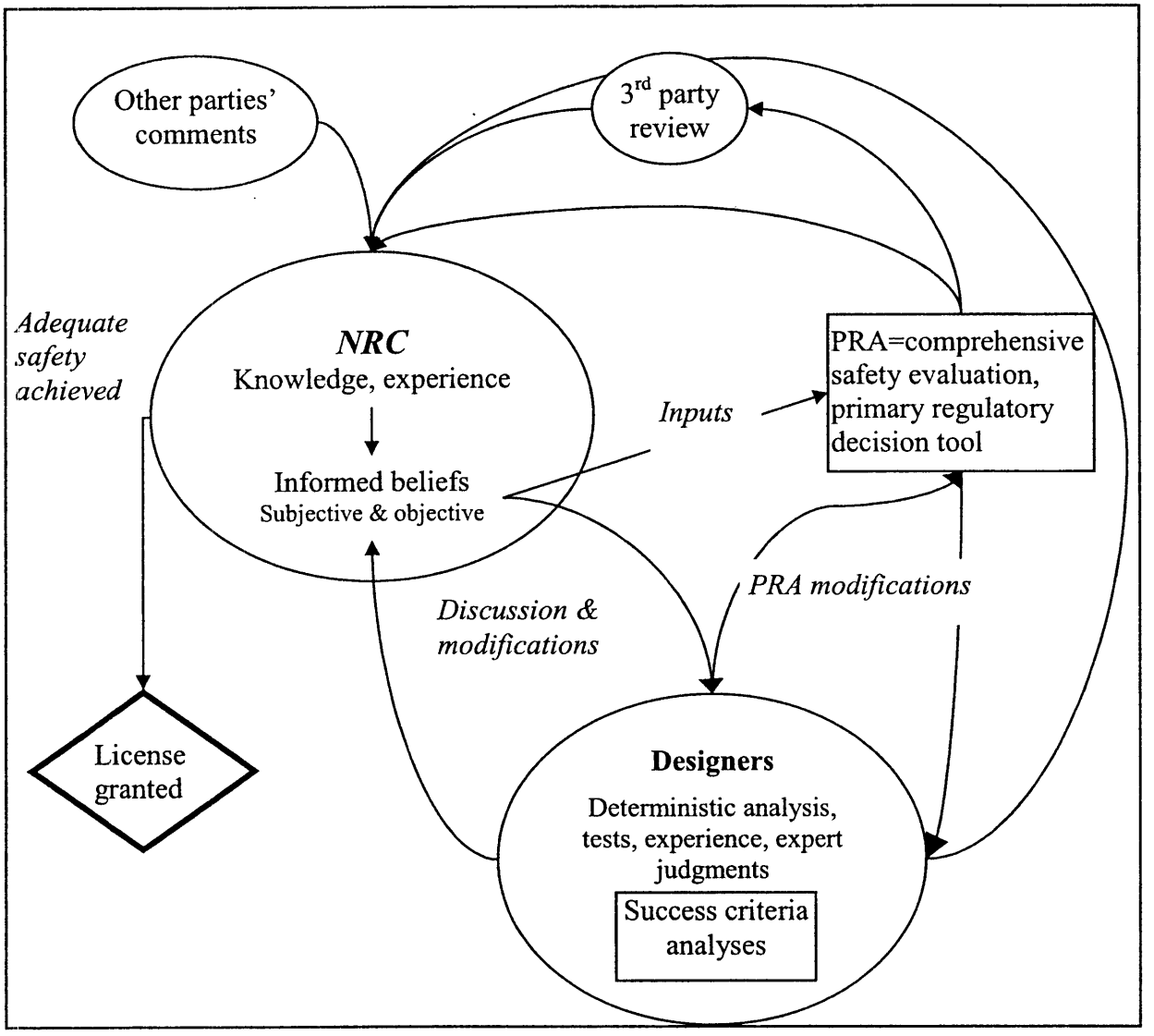


Figure 3-6: Framework for the risk-based discussion process involving the licensee and the NRC.

On the basis on deterministic analyses, testing, experience with other designs and their own judgment, designers propose to the NRC a safety analysis of their plant. Depending on the maturity of the design, the PRA goes directly to the NRC, or / and is reviewed by a third party. NRC experts then review the analysis. They review extensively the data used, the assumptions made and their justifications. On the basis of their own knowledge and of the

information they received from the third party reviewers and from other external parties, they may have a different view than the one of the designers. This constitutes the "informed beliefs" of the regulator.

The informed beliefs of the regulator are used as inputs in the PRA. Some data, uncertainty bounds, or even models may be modified. Some uncertainty may be added on the results of some models if NRC experts think that the models are not well-justified. The PRA results must satisfy the risk limits with these new inputs. NRC experts may also think that some parts of the PRA are inadequate, and ask the designers to change them.

For important disagreements between NRC experts and designers' analysis, discussions will be opened. NRC experts will present the points of disagreement. The designers will have the opportunity to bring additional information to defend their position. In case they are not successful, they will change the design (e.g. adding other safety barriers) or they can decide to improve relevant models or databases. Their purpose will be to bring new evidence to modify the informed beliefs of the regulator.

It is proposed that a discussion with the regulator could be led through all the development stages of the design. Clearly, the details in the PRA required will depend on the maturity of the concept.[46] A proposal is made in Table 3-1. During the initial stages, the safety analysis would rely primarily on previous quantitative analysis. An NRC expert could lead a rough preliminary review and would not require a high level of component testing. As the design becomes more detailed, additional probabilistic analysis and testing will be required.

Development Stage	Goals and Acceptance Criteria	Evaluation Tools	Relevant Evidence
Initial Concept	High level - qualitative	Qualitative, simple, deterministic	Experiences of other concepts, deterministic analyses
Initial detailed design	High level - quantitative	Quantitative – probabilistic, deterministic	Prior quantitative analyses
Final detailed design	Detailed – quantitative (design-specific subgoals)	Detailed – quantitative – probabilistic, deterministic	Prior quantitative analyses
N-th of a kind for a given plant type	Very detailed – quantitative	Very detailed – quantitative, probabilistic, deterministic, tests	Prior quantitative analyses, tests, field experience

Table 3-1: Stages of Nuclear Power Plant Concept Development and corresponding review levels.[46]

In order to obtain a final license approval based on their PRA, the scope and the quality of the analysis will have to be considerably broaden compared to the current practice.

The scope of the final PRA proposed for license approval will have to be broadened to be as large as the set of power plant systems and include all its performance phenomena. All the plant states (full-power, low-power, shutdown, refueling...) have to be included in the PRA.

All the uncertainties will be quantified as well as permitted by the PRA state of the art. Success criteria will have to be stated probabilistically and included in the PRA. Plant specific data will complement generic data as far as possible. The analysis will be supported

by data and model calculations, but inevitably some level of expert judgment will have to be used. Appropriate documentation and justification for model choices and any subjective assessment will be provided to reviewers.

During the final iterative stages before the license is granted, the PRA must be seen as a vehicle for stating the informed beliefs of the regulator. It represents a powerful tool to integrate all of the safety concerns of the regulator. It also offers a basis for a constructive dialog with the designers, who will have the possibility to choose the best option to change the informed beliefs of the regulator and meet its requirements.

In Part 4 of this thesis, a case study is presented to illustrate the application of this methodology. A part of the PRA for a new reactor project is performed. The project studied is still at an early stage of its design. It illustrates how the design can be guided by risk insights expressed with the PRA, and how the regulator would review such a preliminary design proposal, to provide guidance to the designers.

4. CASE STUDY

4.1. Presentation of the case study

4.1.1. The Gas-cooled Fast Reactor project

The case study is based on the generation-IV Gas-Cooled Fast Reactor (GFR) which is currently under development at MIT. This project is lead by Prof. Driscoll, and began in November 2001. The main characteristics of the design are summarized on **Table A-1**.

The designers have so far focused on the core and the Shutdown Cooling System (SCS) designs. The SCS is designed to be used also as an Emergency Core Cooling System (ECCS), and is therefore sometimes referred as ECCS in other studies. A preliminary version of the SCS is presented in Figure 4-1.

The work performed on this case study consists in performing one part of the PRA for this reactor. The PRA is performed using the Saphire computer code.[47]

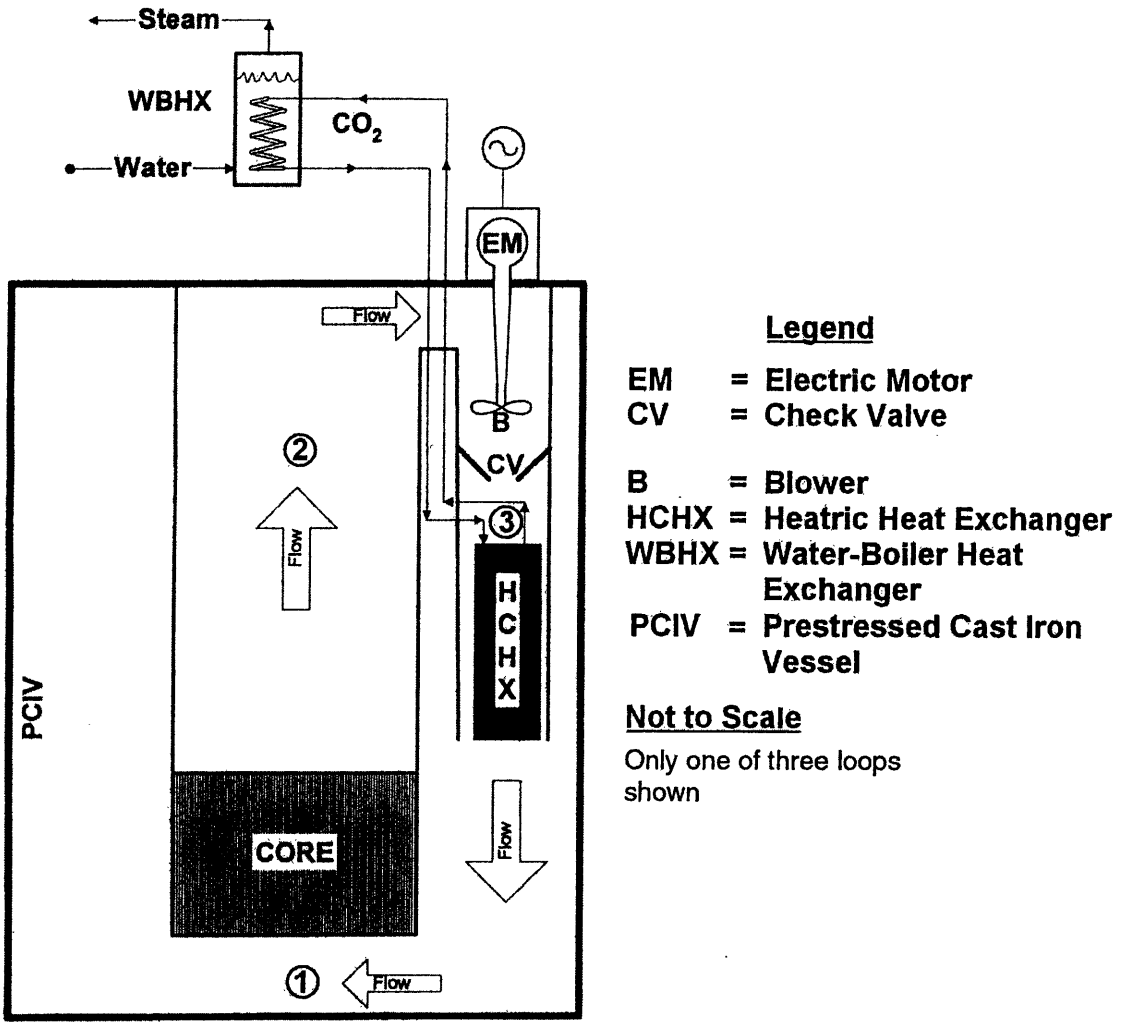


Figure 4-1: Shutdown Cooling System initially chosen by the design team

The core can be cooled either by active cooling or, if it fails, by natural convection (passive mode).

Active mode:

In this mode, an electric motor (EM) obtains electricity from offsite or onsite power sources, and rotates the blower (B). The hot coolant (coming from the core) flows through a check-valve (CV), that it kept closed during full power operation (to prevent backflow from station 3 to 2) and opens for emergency cooling. Then the coolant flows through the Heatric™ Heat Exchanger (HCHX), where the heat is removed (see heat-sink).

Passive mode:

The blower is supposed to be inoperable (failure of the blower or of the power sources). Passive flow is induced by the temperature difference between the heat source (core) and the cold source (HCHX, which is located higher than the core).

The design of the SCS is done so that the passive convection can start from a still state. Thus it does not require any active system to work. However, the CV still needs to open, and its failure probability will be higher without the active flow from the blower. Therefore, in the PRA, the failure of the CV to open under passive flow is a different event than the failure to open under active flow. It is referred as "CP" failure. Thus "SCS-1-CP-OPEN" means that the check-valve of loop 1 fails to open under passive flow. A higher failure probability is taken for this event.

Common Heat Sink:

The heat-sink function is common to the active and the passive modes. The heat is transferred from the core coolant to an intermediate CO_2 loop through the Heatric™ Heat Exchanger (HCHX). The flow in the intermediate loop is passive, and the CO_2 is supercritical. A water boiler constitutes the final heat-sink (evaporatively cooled pool of water).

Some PRA-related work has been performed to-date on the GFR SCS. Delaney [48] performed a level 1 PRA on Loss of Coolant Accidents (LOCAs), which highlighted the importance of a reliable active SCS. However, in his model, he did not give any credit to the passive convection mode. Pagani [49] studied the reliability of the passive cooling mode of the SCS under depressurized conditions (e.g. after a LOCA), and compared it with that of the active mode. However, he did not evaluate the reliability of the combination of passive and active convection modes.

Thus the PRA studies have so far focused on LOCA conditions, and none has evaluated the reliability of a system combining active and passive cooling capabilities.

4.1.2. Loss Of Offsite Power events

This case study is based on the Loss Of Offsite Power (LOOP) initiating event PRA. LOOP events are considered by the Nuclear Regulatory Commission (NRC) as being important contributors to the risk of core damage.[50] LOOP accidents can be particularly challenging for the GFR SCS, as offsite power is the preferred alternating current (AC) source for active

components of the SCS. The reliability of onsite AC sources has traditionally been a concern. Thus, PRAs from the era of the Reactor Safety Study [19] to the more recent NUREG-1150 [51] and since have consistently shown that station blackout scenarios (loss of all AC power sources) are dominant contributors to the core damage risk of nuclear power plants.

The PRA is here limited to the level 1.[x] Thus, the end-states that are considered are either "Core Damage", or "OK" (meaning that no accident has occurred). The analysis method taken is a combined Event Tree (ET) / Fault Tree (FT) analysis. ETs are developed to describe the possible sequences of events after the initiating event occurred, whereas FTs are drawn to quantify the probability of each top event of the ET.

4.2. LOOP PRA

4.2.1. Event Tree and Fault Tree analysis

After discussions with the design team, the following sequence of events has been identified for the LOOP accident sequence:

1st. *The reactor has to be tripped*. The first event in the ET is "Reactor trip". Failure to trip is conservatively assumed to lead to core damage, but it should be addressed in the Anticipated Transient Without Scram (ATWS) event tree. After the ATWS analysis is performed, a more realistic model should be adopted.

2nd. *The decay heat has to be removed through the SCS*. The fluid will flow either via active or passive convection. The active mode is the default mode and will be actuated after the scram. As both AC and DC power are needed for this mode, the next two events after reactor trip are **"Onsite AC Power Generation"** and **"Onsite DC Power Generation"**. The next event is the activation of the SCS itself (e.g. blower, valves...); the event is **"SCS active"**. Then, if it fails, the passive mode is relied on to remove the heat (**"SCS passive"**).

[x] See supra footnote [iii]

Thus, the sequence of events after a LOOP is then:

1. Reactor Scram
2. AC Onsite Power Generation (traditionally with diesels)
3. DC Onsite Power Generation
4. Shutdown Cooling System operation through coolant active convection
5. Shutdown Cooling System operation through coolant passive convection

The description of the top events can be found in Appendix B.

Two offsite power recovery events are introduced in the ET sequence. The first one is after one hour, and the second one after 24 hours. Three time intervals are thus defined: from the initiating event to one hour, from one hour to 24 hours, and finally for the following 200 hours. Subtrees are defined for all intervals and represented in Appendix A. Usual PRA made in the US use typical mission times of 8, 24, or 72 hours. However, longer durations have already been chosen (e.g. 8 days for a PRA in France[52]). The choice of a very long mission time (200 hours) aims at extending the scope of the PRA to very unlikely events. Moreover, an event of this order of magnitude has already taken place (a 135 hours LOOP occurred in 1992[53]).

The quantification of the top events is calculated through fault tree (FT) logic, except for "reactor trip" and for the recovery events, for which the failure probability is assessed directly. The FTs can be found in Part C.

4.2.2. PRA data

The data used in the base case are presented on Table B-1and Table B-2.

These data represent our current best estimates, based on available data. Most of these data are generic data developed for water reactors, and their application to the GFR is discussed component by components in Appendix B. The general methodology is to start from these values and (i) to increase them when the GFR was thought to be more vulnerable, (ii) to take a larger uncertainty range if the conditions in the GFR are different, or (iii) to apply directly the generic values for very similar conditions.

Except for the probabilities of recovery actions, epistemic uncertainties are assessed by using lognormal distributions. Thus for each basic event, a mean failure rate and an error factor (EF) are given. EF values are often given in generic databases, and may be increased according to common PRA practice (the usual EF range gets from 3 to 30, depending whether the uncertainties are small or very large). For recovery action probabilities, an exponential distribution is taken, with the standard deviation adjusted to fit historical data.

The Multiple Greek Letter (MGL) model is used for Common Cause Failures (CCFs). When no CCF factor could be found, the generic CCF factors proposed in AP-1000 PRA were chosen (β=0.1, γ=0.5, δ=0.9 for failures to operate or actuate, and β=0.05, γ=0.5, δ=0.9 for failures to continue functioning).

In some cases, the use of generic data developed for water reactors is clearly not optimal. Although there is some experience worldwide with gas-cooled reactors, it was not possible to obtain data specific to these reactors. The precedent PRA studies for the GFR had similar concerns. Other research teams interested in gas reactors reported the same lack of data.[54] The sensitivity analysis performed in Part 4.4 gives insights on what would be the effect on the licensability if much higher failure probabilities were used.

Among the failure probabilities used, the passive convection failure deserves special attention because it has a critical importance in the licensability and in the design choices made and because its assessment is controversial.

4.2.3. Passive convection issue

The design of systems relying on passive convection is based on thermal-hydraulic (T-H) principles, which in most PRAs are not considered to be subject to any kind of failure. However, because environment and physical conditions may defer from expectations, these systems may fail to perform their functions. [55] Assessing the reliability of a physical process involves many uncertainties and requires a substantial amount of expert judgment. [56] T-H unreliability can be introduced into the fault tree analysis as a single basic event of the form "failure of physical process to perform its function".[57] The challenge is however to quantify its probability.

In the GFR, two failure modes are distinguished for the passive convection: the failure to start (i.e. the failure to reach a proper steady-state), and the failure to run (i.e. to sustain an appropriate steady-state). The failure to run is then divided into the failure during the first 24 hours, and the failure to run during 200 hours. These failures affect all the loops simultaneously (thus they are similar to CCF events).

Pagani [49] studied the failure of the passive convection mode for the GFR SCS design. However, he studied only the steady-state regime, i.e. he did not consider the possibility that the system would not reach any steady-state. Thus his work gives quantitative information regarding the "failure of the passive steady-state" and not regarding the "failure of passive convection to start".

Pagani found that the failure probability of the long term steady state regime was very low ($\sim 10^{-10}$ for the mean [xi]) under conditions of full coolant system pressure, which is the condition during a LOOP initiating event. In his analysis, he included a quantification of the main parameter uncertainties, and propagated it. However, he used only one model (LOCA-COLA code from MIT [58]), which makes it hard to assess all the modeling uncertainties. The fact that other T-H experts found similar deterministic results using the RELAP code is a first indication that the uncertainty introduced by the model choice may not be important.

Based upon these considerations, we took a low failure probability with a high EF for the **failure to run 24 hrs (10^{-8}, EF=30)** and for the **failure to run 200 hrs (10^{-7}, EF=30).**[xii]

[xi] This number comes from a personal conversation with L. Pagani. We do not have the complete uncertainty ranges for full pressure conditions, as we have for depressurized states. Pagani found that the uncertainty range was not very large in depressurized conditions (e.g. one order of magnitude between the mean and the 95th percentile). Moreover, he found that pressure was the most important parameter, and that he had to deal with large pressure uncertainties in the depressurized conditions. Under full pressure, the uncertainties on the pressure are much lower. However, it still justifies using a large uncertainty range to acknowledge the lack of full modeling of the full pressure state.

[xii] Pagani took a mission time of 72 hrs only. However, the failure rate of the steady state should be higher during the first hours when there will be more heat to remove. However, there are high uncertainties on the functioning of any system for such a long duration. Therefore we take a failure probability one order of magnitude higher for the 200 hrs mission time.

The **failure to start** was not studied by Pagani, and until recently no simulation had been done. The concern is that the fluid may stratify and fail to reach the steady-state flow. This would be an extreme situation that the T-H experts estimate to be unlikely, but no quantitative information was available. A simulation was performed recently, and it was found that, even under low pressure, passive convection would start from an initially stagnant fluid. However, no uncertainty calculation was performed and this result is subjected to many modeling approximations and uncertainties. Although this simulation is a good indicator that under full pressure the passive convection will start unaided, we can only derive subjective probabilities from this information. We therefore take a failure probability of 10^{-2} and an EF of 30.

Finally, the same difficulty in assessing the reliability of passive convection systems motivated changes in the design of the intermediate and final heat sink. In the initial design, the intermediate heat-sink removes the heat through supercritical CO_2 passive convection. The failure of intermediate heat-sink loop would cause the failure of the whole SCS loops. Therefore, any CCF of several of these loops to remove the heat would cause the system to fail. Designers thought that this configuration was very reliable, but it was difficult to find enough quantitative information to grant very high reliability values. Uncertainties on gas passive convection were too great (especially for a supercritical gas).

Therefore the preferred design was changed for the option of Figure 4-2. Water removes the heat from the HCHX through passive convection. The steam is vented to the atmosphere. This option was chosen because water passive convection is much better understood than gas passive convection. Thus higher reliability values can be taken.

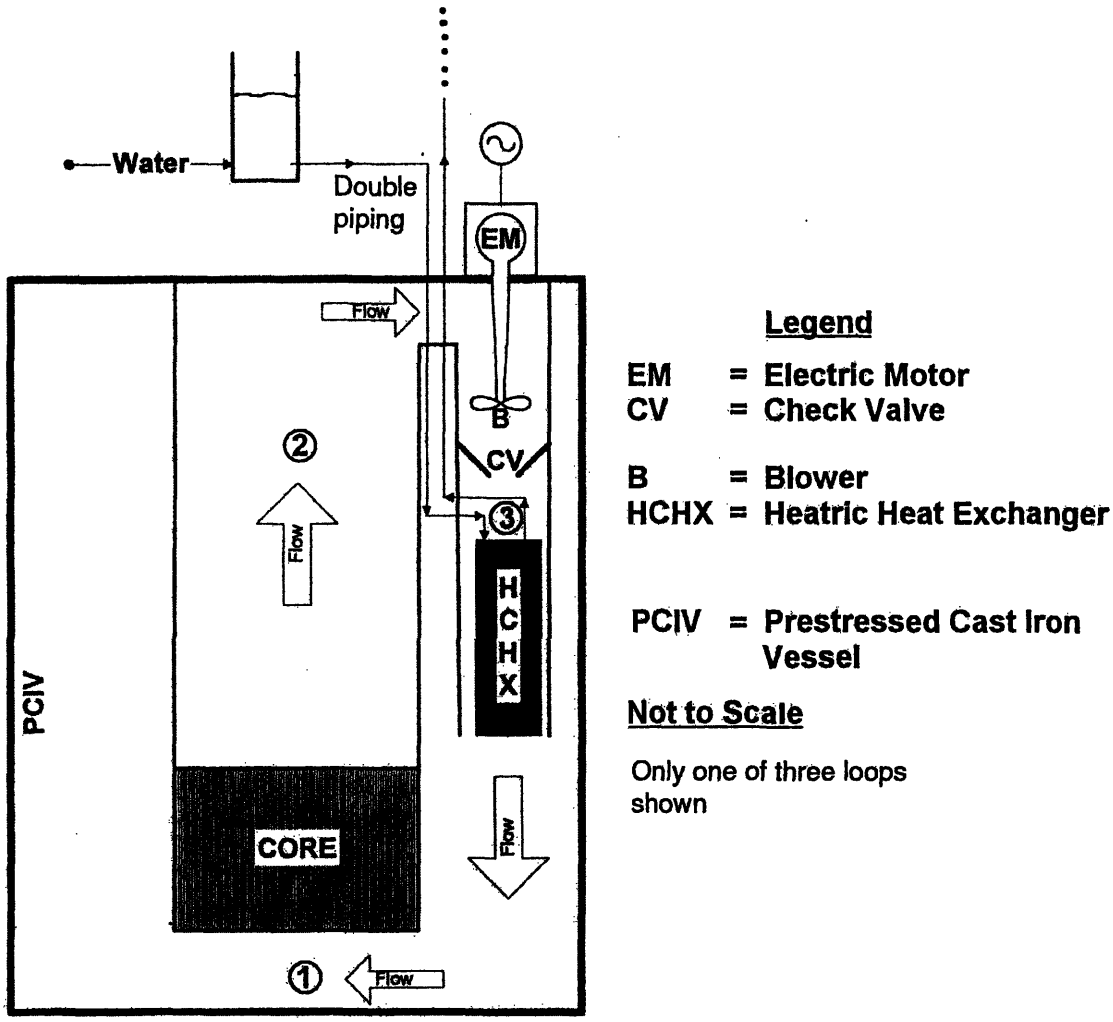


Figure 4-2: Revised SCS design after changing the intermediate heat sink for a water loop

Water heat-sink:

Heat is taken from the HCHX by the flow of water. The water is heated in the HCHX (thus removing heat from the HCHX). It is brought to boiling, and the steam is vented to the atmosphere. Constant water input injection has to be provided.

Double piping is used to make sure no water ingress can occur in the PCIV.

The rest of the design is the same.

4.3. Risk-guided design

4.3.1. Methodology overview

The methodology presented in Part 3.2 is applied to the GFR case. The design of the SCS is already quite mature (Figure 4-1) and is an important focus for the design team. The designers are also worried about the failure of AC power source. They want to have risk insights before choosing to investigate innovative systems to generate onsite power. In contrast, other aspects of the plant have so far not been studied at all and will be dealt with much later (e.g. reactor trip system and DC power system). For these systems with no input from the designers, default design options are taken. Thus three batteries are taken and an historical reference is used to assess the reliability of the reactor trip system (see Appendix B).

The risk-driven design focuses on the key areas of concern for the designers, where the insights from the PRA will be the most valuable. The "decay heat removal" and the "AC power generation" functions are therefore the main focus for the PRA.

Before starting the risk-driven process, the bare-bones plant has to be defined. Its main features are:

- 2 SCS loops, designed to remove 50% of the decay heat each, each loop being as described on Figure 4-1,
- Passive flow in the SCS or active flow with one diesel generating AC power (and capable of generating 100% of emergency the load). Two cases are examined; one with passive SCS convection, and one without,
- A reliable trip system.

The methodology of Figure 3-5 is then applied. At each design stage, the dominant cut sets are identified. They indicate which are the components driving the risks. Safety improvements are then brought to mitigate these risks.

One departure from the initial methodology is that the iteration is terminated not when the risk thresholds are satisfied, but rather when there is no readily available way to increase the safety (i.e. given their state of knowledge, the designers cannot propose demonstrated ways

to increase safety at reasonable costs). There are three reasons for continuing the safety improvements beyond the stated goals:

- The safety performance for advanced reactors is currently viewed by designers as competitive. They think it is preferable to achieve comparable or better safety levels than competitors' designs. Indeed, safety performance is likely to be an important parameter when investors will choose to support building one or another design. Meeting the regulatory safety safety should therefore not be considered as a sufficient goal,
- Presenting a design to the regulator that is just under the regulatory limit is likely to be hard to get accepted by NRC experts,
- Bringing as many safety improvements as possible will provide a wider range of screened option for the designers. It will make later choices easier.

4.3.2. Iterative design

In this Part, the bare-bone plant design has two SCS loops that rely on passive convection to remove decay heat. The case with no passive convection possibility is described in Appendix D.

The results of the iterative process are presented on Table 4-1. As the reliability of the passive convection to start was assessed to be low (see Part 4.2.3), it dominates the risk of the bare-bones plant (*case 1*). A diesel generator is added to power the active convection system (*case 2*). Thus the redundancy of the active and passive modes is created. As diesels have a limited reliability (see Table B-2 in Appendix B), the risk remains above 10% of the CDF threshold. Another diesel is added (*case 3*) and the risk decreases under the 10% thresholds, for the mean as well as for the 95th values. The single failure of a check-valve (CV) is the main remaining risk contributor. Redundancy is obtained by adding another SCS loop (a CCF of two CVs is then needed to cause system failure). The sequence {"Passive start failure" and "diesel start CCF"} dominates (*case 4*). This is a station blackout sequence with failure of the passive convection transient. Another diesel could be added to decrease

the likelihood of a station blackout, but the change would not be very important and this contributor would still be dominant.[xiii]

Therefore, after discussing it with the design team, it appeared preferable to propose an innovative option that would make passive convection more reliable. First, the blowers will be kept running slowly all the time. The operators will be ensured that they will be working. Then, a flywheel will be integrated in each blower. In the case of a station blackout occurring immediately after the LOOP, the blowers would still have some momentum, and they would be able to initiate the passive flow.

With the standby blower and the flywheel, the design reaches a very high reliability. It can still be improved by adding another SCS loop (*case 6*).

Case number	Description	Core Damage Probability		Components limiting risk reduction	Next step
		Mean	95th %		
1	2*50% loops	1.2E-04	4.1E-04	Passive convection Start	*Add diesel*
2	2*50%, **1 diesel**	1.5E-05	4.1E-05	{Passive Start + diesel failure}	*Add diesel*
3	2*50%, **2 diesels**	**3.4E-06**	**7.5E-06**	CV	*Add a SCS loop*
4	3*50%, **2 diesels**	2.4E-07	7.5E-07	{Passive Start + diesel failure}	*Add standby system for blower*
5	3*50%, 2 diesels, **standby blower**	4.7E-08	1.3E-07	CV CCF	*Add a SCS loop*
6	**4*50%**, 2 diesels, standby blower	1.4E-08	4.4E-08	CV CCF	

Table 4-1: Risk-Driven design – with passive cooling. CV: check-valve; CCF: Common Cause Failure; 2 or 3*50%: 2 or 3 SCS loops, each capable of removing 50% of the decay heat

[xiii] Using the Multiple Greek Letter (MGL) model, the CCF of 3 components is half of the CCF of 2 components (with a conventional value of 0.5 for the δ factor).

4.3.3. Preliminary design choices

The comparison of the risk-driven design with passive convection (Part 4.3.2) or without (Appendix D) highlights the safety improvements brought by the passive convection mode. Licensing the GFR without passive convection appears to be possible, but it would be much harder to reach high safety levels. Therefore, the risk calculation provides confidence to the designers in their desire to allow the decay heat removal using passive cooling. However, passive cooling alone would not provide sufficient safety, and therefore a system for active convection has to be included. It is then precisely this combination of passive and active convection that allows reaching very high reliability levels.

Due to diesel CCFs and to reliance on passive convection, the risk does not decrease much if a third diesel is added. The choice was thus made to take two diesels only. Concerning the number of SCS loops, there is a clearer benefit in increasing from three to four loops. However, it was thought that the safety difference may not be worth the additional costs of a fourth SCS loop. The safety achieved is already very high with three loops. While this may still be considered, it is the option that has been chosen in the next steps of the risk-driven design process.

The design chosen by the preliminary risk-driven process is the **design of case 5.**

4.4. Robustness evaluation

4.4.1. Key uncertainties treatment

A key uncertainty "is one that is related to an issue in which there is no consensus approach or model" and "in which the choice of approach or model is known to have an impact on the PRA results".[59] Thus, an event in the PRA that is a source of a key uncertainty will be characterized by a low state of knowledge (high ignorance) and it will also have a relatively high RIR.

Figure 4-3 is used to identify key uncertainties related to the estimations in the basic events probabilities. The abscissa is a subjective representation of the scientific state of knowledge

on one event. Thus, the domain of key uncertainties is on the right part of this axis (no scientific consensus). The ordinate is the RIR. Significant RIR limits have been represented:

- First limit: if the probability of the event is unity, then the risk doubles (RIR = 2),
- Second limit: if the probability of the event is unity, then the 10% threshold of the CDF is reached for LOOP events (RIR = 210%*5*10^{-5} / (5*10^{-8}) ➔ RIR = 100),
- Third limit: if the probability of the event is unity, then the CDF threshold is reached (RIR = 5*10^{-5} / (5*10^{-8}) ➔ RIR = 1000),
- Fourth limit: Core damage happens if the failure of the event is unity (RIR > 2*10^{5})

The failure probabilities that could represent key uncertainties are located in the right upper part of Figure 4-3.

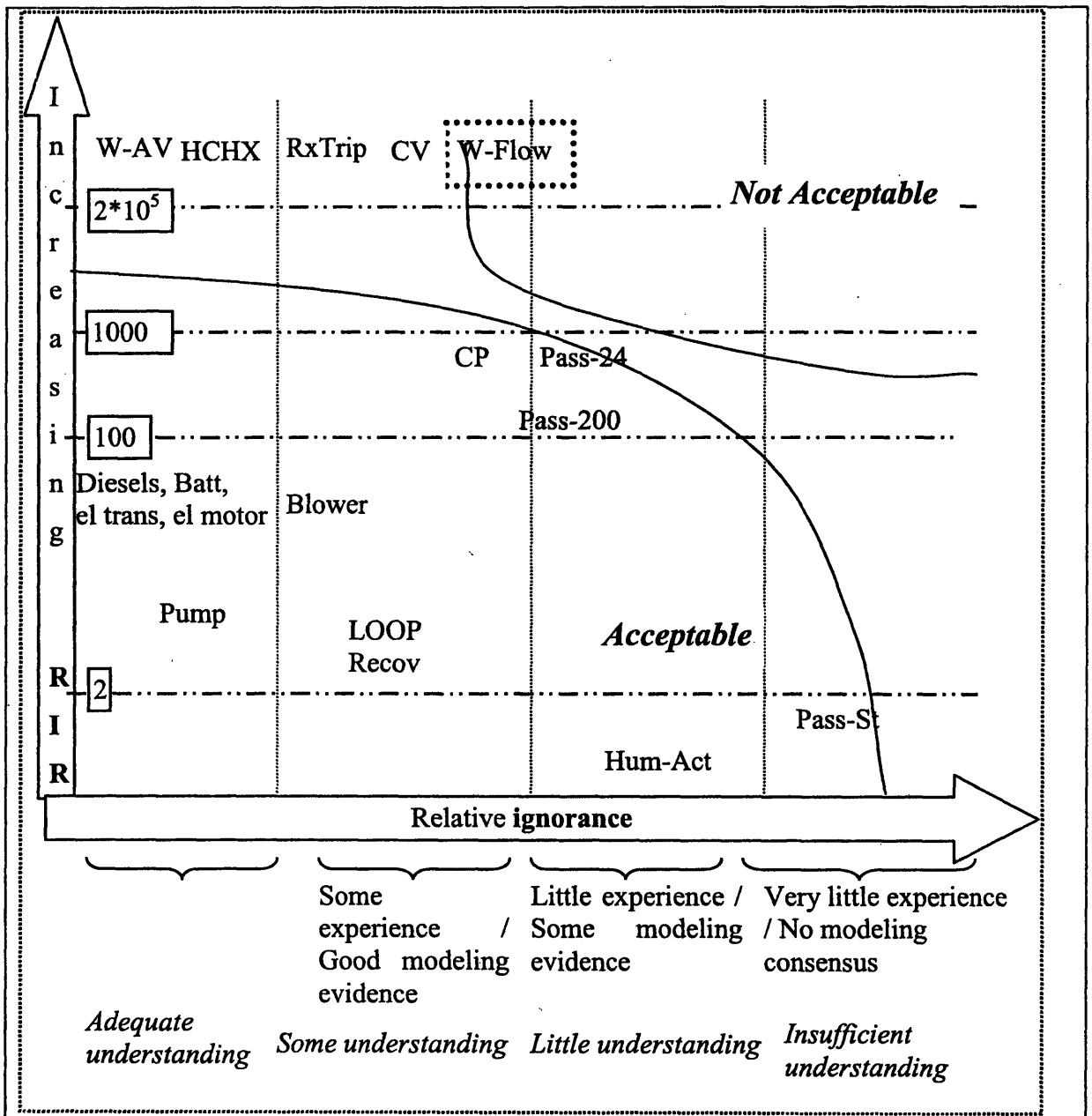
As the design includes systematic redundancy, all the single failure events have a low RIR compared to the associated CCF event. They also have a low FV importance. Therefore, only CCF type events are included in Figure 4-3.

There is no event in the upper right corner, but the failure of water flow in the intermediate heat sink may be a concern and should be considered more carefully (W-Flow event on the graph, which represent a CCF on the 3 Water Boiler Loops [WBLs] to run or to start). This CCF is considered to be very unlikely, as water passive convection is well assessed. However, experience with the exact same configuration is sparse. There could be some unidentified mode for the failure to start. Some blockage could be created for unknown reasons. Therefore, the design team adopted the same approach than with passive convection of the SCS coolant. It decided to add a pump in the WBL, in order to have some redundancy between an active and a passive mode.[xiv]

The effect of this decision can be seen on Figure 4-4. The sequence {pump failure + passive water flow failure} has the same high RIR than previously {passive water flow failure}, but there is much less knowledge uncertainty about it (pumps are well-known system).

[xiv] The pump will not have an active seal (thus it will not be an initiator for pump-seal Loss of Coolant Accidents [LOCAs]). It would have a specific back-up battery to power it in case of station blackout.

Moreover, the failure probability of the sequence {pump failure + passive water convection failure} is much lower than the failure probability of the passive water convection alone.



All the events represented are CCF events.

The limits between the acceptable and non-acceptable zones are subjective.

CV: Check valve
CP: Check valve working under passive flow only

HCHX:	Heatric Heat Exchanger
W-AV:	Water available (for Water Boiler Loop)
RxTrip:	Trip of the reactor
Pass-24:	Passive convection during 24 hrs
Pass-200:	Passive convection during 200 hrs
Pass-St:	Passive convection start
W-Flow:	Passive water flow in Water Boiler Loop
Batt:	Batteries
El trans:	Electric transmission for AC and DC
El motor:	Electric motor
Hum Act:	Human Actions
WBHX:	Water Boiler Heat Exchanger

Figure 4-3: RIR – "State of knowledge" diagram, illustrating the unacceptable event W-Flow

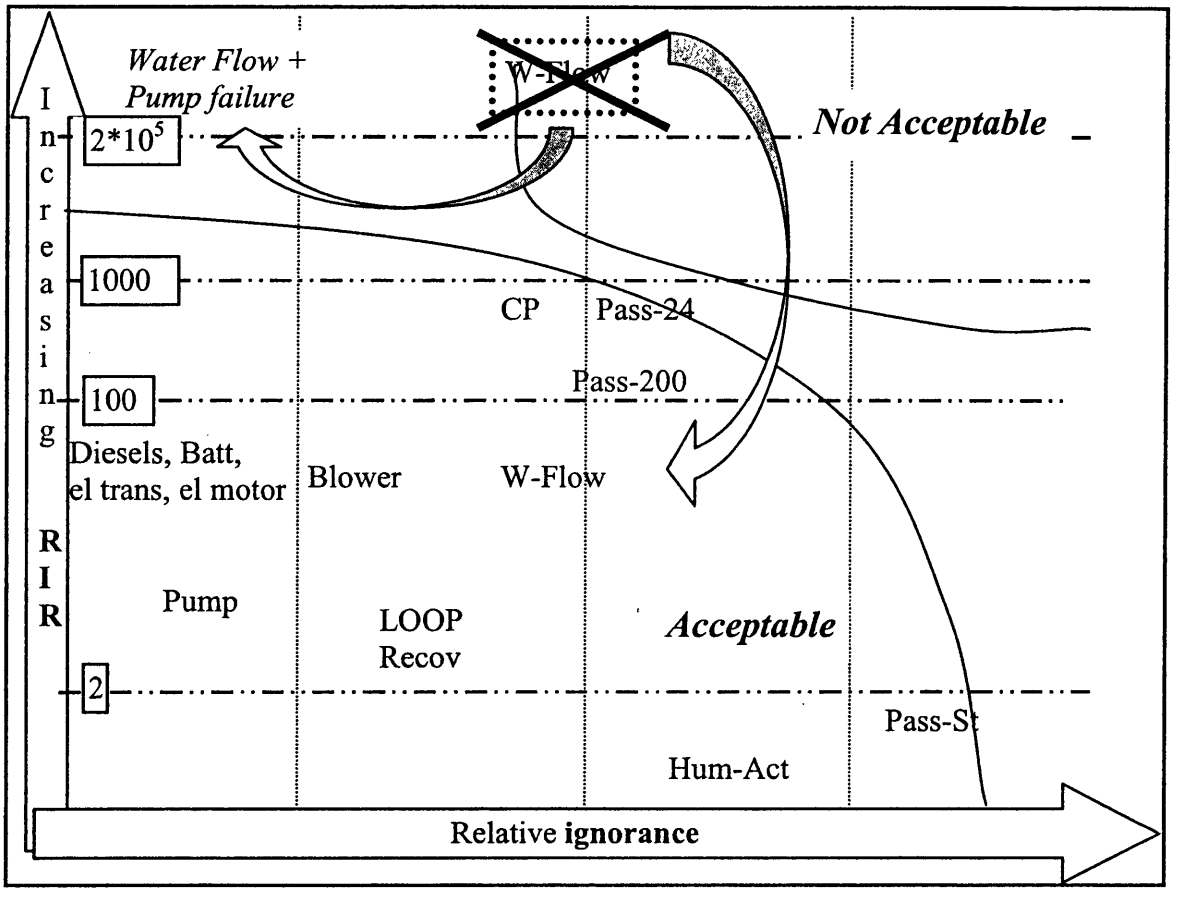


Figure 4-4: RIR – "State of knowledge" diagram, illustrating the effect upon the event W-Flow of adding a pump to the water-based cooling loop.

The new design with the pump added in each WBL is shown on Figure 4-5. It is now the preferred design. New risk calculations have been performed for this design (see Table 4-2). There are very little changes compared to case 5. However, a real design weakness has been identified and corrected.

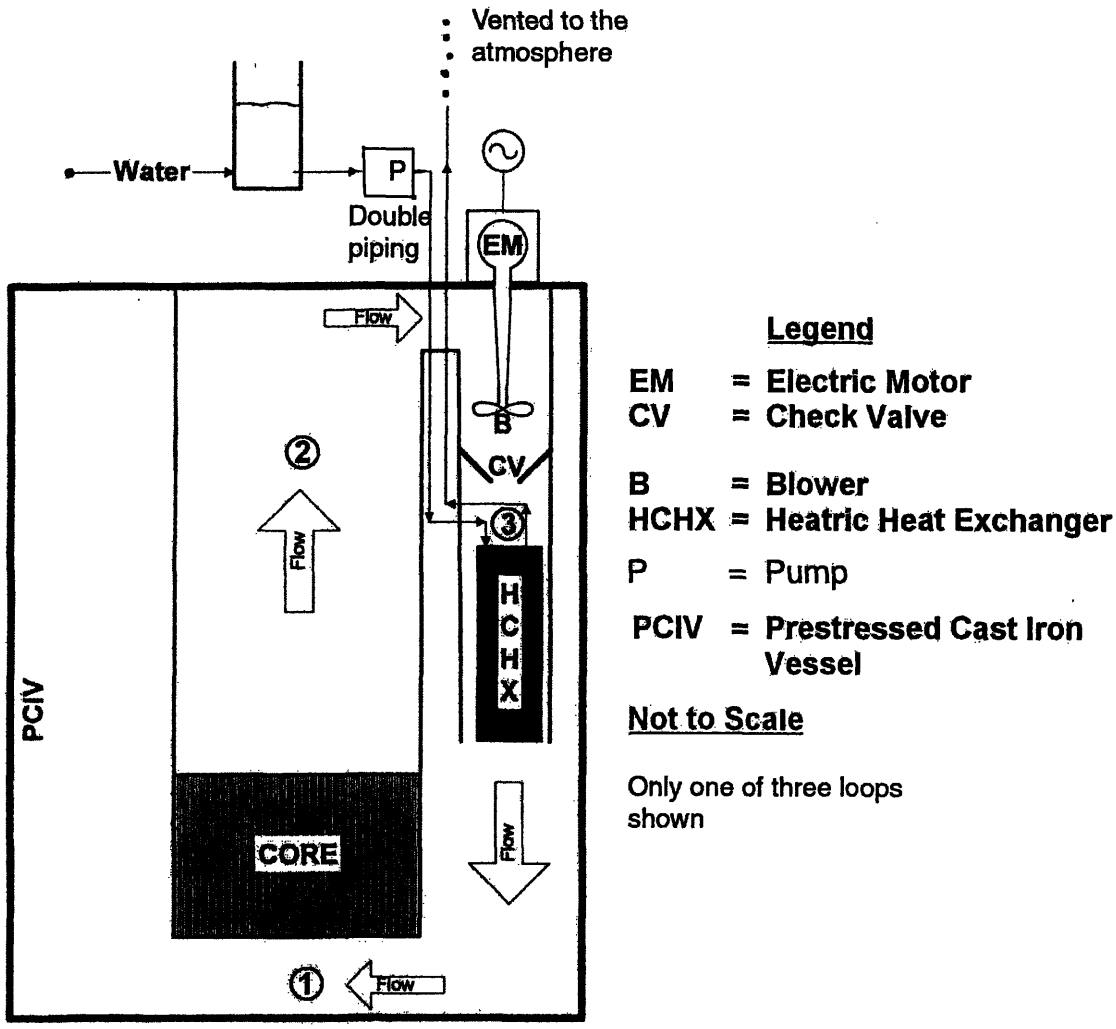


Figure 4-5: Revised (2) and definitive SCS design after adding a pump in the WBL

	Mean		95th percentile	
Risk from LOOP	GFR	Regulatory limit for LOOP	GFR	Regulatory limit for LOOP
CDP	4.6E-08	5.0E-06	1.3E-07	1.0E-05
Sequence contributing the most	2.6E-08	2.5E-06	8.0E-08	5.0E-06

Table 4-2: PRA results for the definitive risk-driven GFR design

The safety level achieved is excellent: it is generally two orders of magnitude below the regulatory guidelines proposed.

4.4.2. Extended sensitivity analysis

To provide additional insights about the robustness of the design, we perform an extensive sensitivity analysis. The events that are included in this analysis are the ones that have a high Fussell-Vesely importance and a high RIR. Other events, for which the state of knowledge is considered to be low, have been included (see Table B-4, Table B-5 and Appendix B for more details). Only CCF type events are considered in the sensitivity analysis.

First, we investigate the limit to which a single individual failure probability can be increased, while still satisfying our guidelines for a robust design. Some results of this analysis (given that all the other failure probabilities remain unchanged) are summarized in Table 4-3. Table 4-3 gives the maximum failure probability of any event, so that no single sequence will be above 5% of the CDF threshold (the other guideline of 10% contribution of the CDF for LOOP events is then automatically satisfied). This maximum failure probability is then compared to the failure probability of the same event in the base case (see Table 4-3 and the graphical illustration of Figure 4-6).

	CCF type[xv]	Probability		Ratio Max/BC
		Base case (BC)	Max failure probability value to stay under 5% limit	
Reactor trip		1.0E-07	2.0E-04	**2.0E+03**
CV	Open	2.7E-06	2.0E-04	**7.4E+01**
	Run 24 hrs	2.4E-07	2.0E-04	**8.3E+02**
	Run 200 hrs	2.0E-06	2.0E-02	**1.0E+04**
HCHX	Run 1 hour	5.00E-08	2.0E-04	**4.0E+03**
	Run 24 hrs	1.2E-06	2.0E-04	**1.7E+02**
	Run 200 hrs	1.0E-05	2.0E-02	**2.0E+03**
Water Available	Run 1 hour	1.0E-08	2.0E-04	**2.0E+04**
	Run 24 hrs	1.0E-07	2.0E-04	**2.0E+03**
	Run 200 hrs	1.0E-06	2.0E-02	**2.0E+04**
Pump*passive water flow	Run 1 hour	2.0E-11	2.0E-04	**1.0E+07**
	Run 24 hrs	6.0E-13	2.0E-04	**3.3E+08**
	Run 200 hrs	5.0E-12	2.0E-02	**4.0E+09**
Passive failure to start*blower standby failure		1.0E-07	1.0E-01	**1.0E+06**
Passive convection	Run 24 hrs	1.0E-08	5.0E-02	**5.0E+06**
	Run 200 hrs	1.0E-07	5.0E-02	**5.0E+05**
CP	Open	1.0E-04	1.0E-01	**1.0E+03**
	Run 24 hrs	4.8E-07	5.0E-02	**1.0E+05**
	Run 200 hrs	4.0E-06	5.0E-02	**1.3E+04**
Probability of Recovery after 24 hrs		1.6E-02	1.0E+00	**6.3E+01**

Table 4-3: Maximum failure probabilities consistent with the guideline of no single sequence contributing more than 5% of the risk threshold.

Base case values are those of Table B-2.

A log-scale illustration of these results is shown on Figure 4-6.

[xv] Important: the numbers in Table 4-3 and Table 4-4 are **CCF values**, i.e. the independent failure probabilities multiplied by the CCF beta factors (there are only double CCFs here). For example, for the CV failure to open:

Independent failure * beta = $10^{-4}*(2.7*10^{-2}) = 2.7*10^{-6}$ (base case); to compare with $2*10^{-4}$

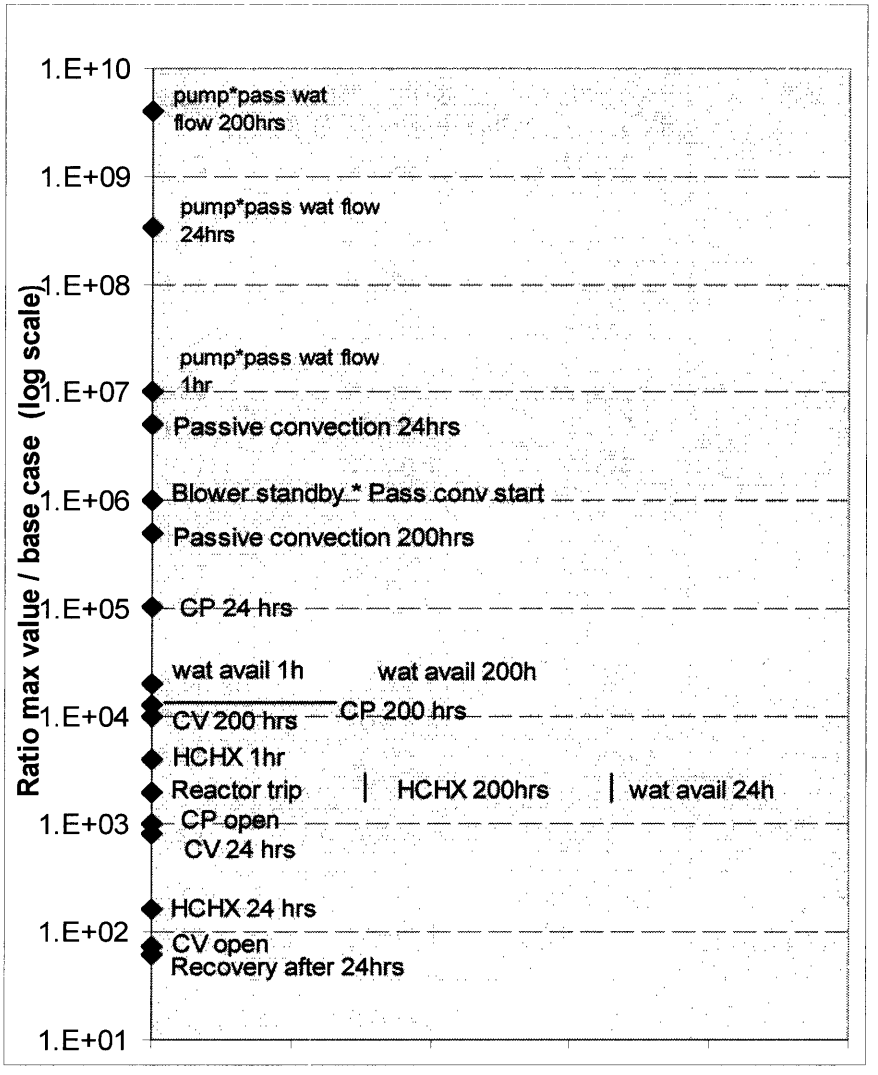


Figure 4-6: Graphical illustration of the results of Table 4-3

These results show that the GFR design has very high safety margins. Even if we have underestimated a failure probability, the robustness guidelines would not be exceeded unless the underestimation was by several orders of magnitude. Actually, all the maximum values are unrealistically high, so that the design safety is robust to any increase in one failure probability.

However, this first sensitivity analysis does not take into account the effects of the simultaneous increase of several failure probabilities. Therefore, to illustrate further the safety of the GFR, a sensitivity analysis is performed with all the failure probabilities

increasing at the same time. With the set of values proposed in Table 4-4, the design satisfies both robustness guidelines (5% maximum for any sequence and 10% for LOOP initiating event) for the mean and for the 95th percentiles values. A graphical illustration is shown on Figure 4-7.

		Probability		
	CCF type [xvi]	Base case (BC)	Max group failure probability	**Max/BC**
Reactor trip		1.0E-07	4.0E-05	**4.0E+02**
CV	Open	2.7E-06	8.0E-05	**3.0E+01**
	Run 24 hrs	2.4E-07	8.0E-05	**3.3E+02**
	Run 200 hrs	2.0E-06	8.0E-04	**4.0E+02**
HCHX	Run 1 hour	5.0E-08	8.0E-05	**1.6E+03**
	Run 24 hrs	1.2E-06	8.0E-05	**6.7E+01**
	Run 200 hrs	1.0E-05	8.0E-04	**8.0E+01**
Water Available	Run 1 hour	1.0E-08	4.0E-05	**4.0E+03**
	Run 24 hrs	1.0E-07	4.0E-05	**4.0E+02**
	Run 200 hrs	1.0E-06	8.0E-04	**8.0E+02**
Pump*passive water flow	Run 1 hour	2.0E-11	5.0E-05	**2.5E+06**
	Run 24 hrs	6.0E-13	4.0E-05	**6.7E+07**
	Run 200 hrs	5.0E-12	1.0E-03	**2.0E+08**
Passive failure to start*blower standby failure		1.0E-07	4.0E-02	**4.0E+05**
Passive convection	Run 24 hrs	1.0E-08	1.0E-02	**1.0E+06**
	Run 200 hrs	1.0E-07	2.0E-02	**2.0E+05**
CP	Open	1.0E-04	4.0E-02	**4.0E+02**
	Run 24 hrs	4.8E-07	2.0E-02	**4.2E+04**
	Run 200 hrs	4.0E-06	4.0E-02	**1.0E+04**
Probability of Recovery after 24 hrs		1.6E-02	1.0E-01	**6.3E+00**

Table 4-4: Maximum allowable failure probabilities for all the events consistent with meeting the robustness guidelines[xvii]

[xvi] See supra note xv

[xvii] Here both robustness guidelines are met in terms of mean and 95th percentile: there is no sequence that contributes more than 5% of the CDF (mean and 95th percentile), and the contribution of the LOOP initiating event is less than 10% of the CDF (mean and 95th percentile).

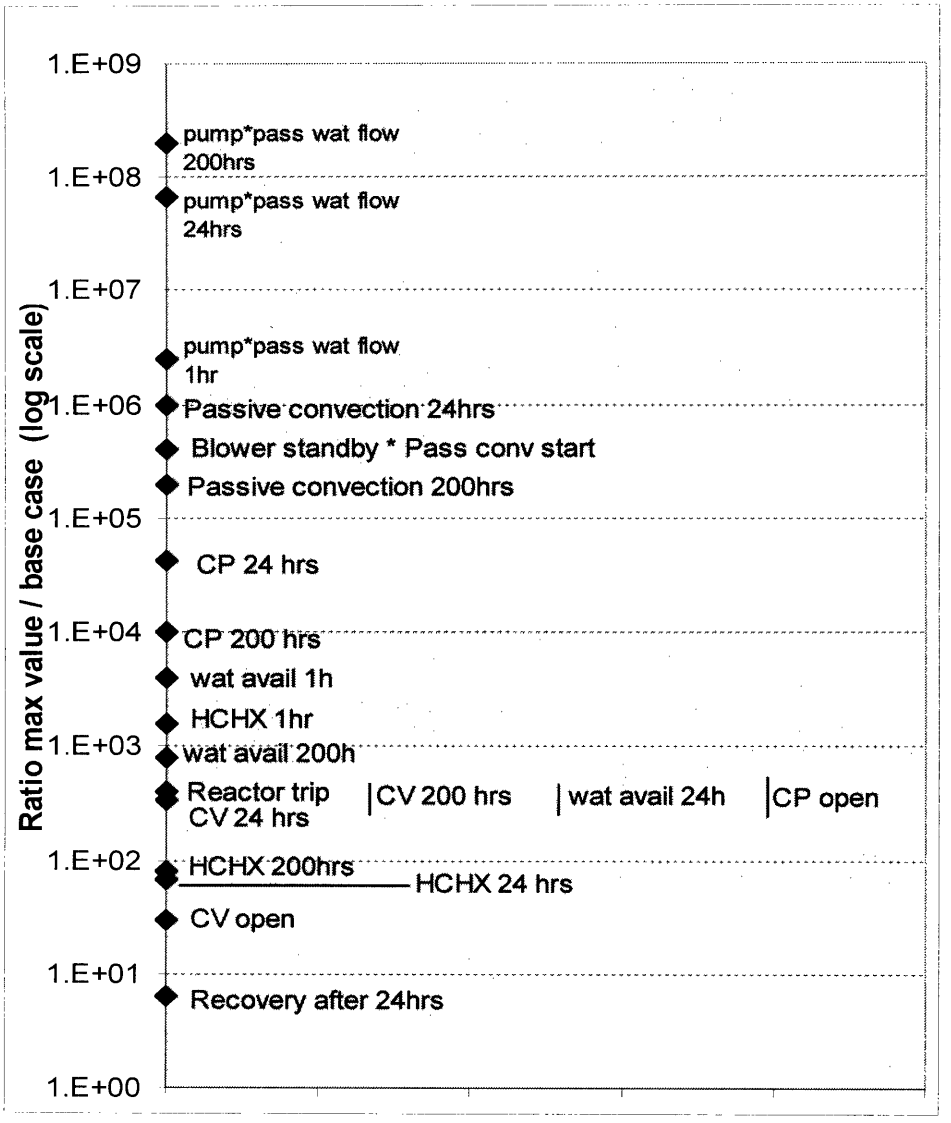


Figure 4-7: Graphical illustration of the results of Table 4-4

Table 4-5 shows the mean and 95th percentile for the CDF due to LOOP when all the failure probabilities take the value of Table 4-4.

	Mean		95th	
Risk from LOOP	GFR	Proposed limit for LOOP	GFR	Proposed limit for LOOP
CDF	3.0E-06	5.0E-06 (1)	8.0E-06	1.0E-05 (2)
Sequence contributing the most	8.0E-07	2.5E-06 (3)	2.6E-06	5.0E-06 (4)

Table 4-5: Safety levels achieved using the maximum allowable failure probability values from Table 4-4.

(1) 10% of $5*10^{-5} = 5*10^{-6}$
(2) 10% of $10^{-4} = 10^{-5}$
(3) 5% of $5*10^{-5} = 2.5*10^{-6}$
(4) 5% of $10^{-4} = 5*10^{-6}$

The values obtained are still unrealistically high. The CCF of the CV to open and the CCF of the HCHX to operate 24 hours or 200 hours are the events that have the relative lowest margin. However, as is explained in Appendice B.2, there is no argument for adopting failure probability values much higher than those used in the base case. Reasons for this are that the forces to open the CV will be very high, and, according to Heatric experiments, their heat exchangers have never experienced a leak.

The values obtained during these sensitivity analysis tests do not have a real physical meaning. The purpose is more to illustrate the margin of safety achieved by the GFR. While such high margin results should not be required by the regulator, this constitutes a powerful response to the concern that several failure rates used for critical events were either generic or highly subjective.

These results should be used in the discussion with the regulator. For example, if a NRC expert disagrees with the failure probability used for the CV, then he should express the value that should be taken according to his experience and the evidence provided. If this value is lower than the one found in the sensitivity analysis (from Table 4-3 or Table 4-4 depending whether only one probability has been changed or several), then this should not be a sufficient argument against the licensability of the GFR.

These last sensitivity results did not change the design that had been chosen. More sensitivity analysis could be performed, but there would probably not lead to further changes. Therefore, the design is thought to be ready for the second phase of the simulation, i.e. the presentation to the regulator. This final design is that of case 5 of Table 4-1, with the pump added in the WBL (see Figure 4-5).

4.5. Discussion with the regulator

A mock licensing simulation was made at MIT to illustrate the discussion that would be initiated between the designer and the regulator, according to the discussion framework presented on Figure 3-6. The goal of this discussion is to check that the direction and the options chosen for the design are acceptable from a regulatory perspective.

Prof. G. Apostolakis [xviii] and PRA graduate student Craig Matos took the role of NRC experts. A meeting was organized, where the safety analysis and results were presented. Prof. M. Driscoll was representing the design team. Previous documentation on the PRA had been distributed, and Craig Matos had reviewed it.

Although the time dedicated to this review by our NRC experts was limited, interesting questions were raised on the GFR design and on the PRA.

Concerning the design, worries were expressed about the reliability of the ultimate heat sink in the SCS. In the design of Figure 4-5, steam is directly vented to the atmosphere. Should there be a leak in the HCHX, a direct flow path between the core and the environment would be created, and some radioactivity could then be released. This concern did not appear in the LOOP PRA, although it would probably have appeared in other parts of a complete PRA.

[xviii] Prof. George E. Apostolakis is Professor of Nuclear Engineering at the MIT. Among other activities, he is a member of the NRC Advisory Committee on Reactor Safeguards (and he was the chairman in 2001-2002). He was therefore well qualified to endorse the role of a NRC reviewer.

Satisfying options were presented by the design team to solve this problem (e.g. venting the water inside the containment, or changing the opened loop to a closed water loop).

Concerning the PRA, the reviewers had some concerns about the use of generic data for critical components, especially for the CV. Although it was shown by the PRA that there were very high safety margins relative to the failure probability value used, reviewers insisted that extensive testing will be required. Because of the high reliability that CVs must reach, it was feared that it may be impossible (or much too expensive) to do enough testing. Therefore it is likely that eventually an additional active actuator will be required.

Some reservations were also expressed concerning the PRA model. More work should be done to integrate explicitly success criteria into the PRA. This would require extensive probabilistic treatment of model uncertainties, which has not been performed yet. The current PRA state of the art should be improved in order to deal adequately with these concerns. The regulator should also be given a more extensive access to the deterministic and probabilistic models and calculations used for the success criteria.

Although it was rather out of the scope of the limited LOOP safety analysis exposed, reviewers expressed the necessity to create a specific framework outside the PRA in order to treat the issue of adequate management.

There were no other critic on the work performed by the design and the safety analysis teams. The reviewers were satisfied with the rest of the analysis. Especially, they thought that the treatment of epistemic uncertainties of passive convection had been adequate. In spite of the few critics, they thought that the GFR was so far in very good shape for future licensing purposes.

For the design team, this review has brought valuable insights. It first confirms that most of the safety issues are being treated adequately. The reservations expressed will not change the design fundamentally, but will help in improving it in a direction more acceptable to the regulator.

5. Discussion of the risk-based framework

5.1. Insights for the MIT iterative framework

No fundamental flaw was found during the licensing simulation using the MIT iterative framework.

The design risk-driven process was very effective in bringing new safety concerns to the designers and allowed them to ranks safety options. One key element in this process was the establishment of a continuing discussion between designers and safety analysts. Especially at early design stages, when data available are generic and more subjectivity has to be introduced, it is essential to discuss PRA results in order to avoid any misinterpretations. For example, in some early analyses, it was assumed that the intermediate heat-sink CO_2 passive loop would be perfect. This assumption was made because there was no data available for assessing its reliability and first discussions with some designers indicated that it would not be an issue. Explicating clearly the PRA assumptions and limitations had the effect of broadening the discussion with the designers. Therefore it is especially important to discuss the results of a PRA, and not merely provide raw numbers to the designers.

The simulation highlighted differences of appreciation about key uncertainties between the safety analyst and the NRC experts. The failure probability of the CV was considered by reviewers as a key uncertainty, and they required either improvements in the relevant knowledge or added redundancy. In the safety analysis, generic values were used for the CV failure probability, as at this stage of the design there was no reason to think it would be less reliable in the GFR. The sensitivity analysis had also demonstrated that good safety results would be obtained even with a failure probability much higher than the generic one. However, these last arguments were dismissed by the NRC experts, who refused to elicit their informed beliefs, and it was required to decrease epistemic uncertainty or change the design.

This example illustrates the issue of the identification and treatment of key uncertainties. Should there be a systematic and replicable definition of key uncertainties, defining up to

what limit are uncertainties acceptable? Could the RIR-"State-Of-Knowledge" diagram (see Figure 3-3) be used for this purpose, provided that an objective quantification of the "state of knowledge" is made? Once key uncertainties have been identified, should it be required to decrease their RIR or their epistemic uncertainty regardless of the implications on the total risk?

Clear guidelines concerning the identification and treatment of key uncertainties would allow better prediction of the reaction of the regulator. Thus the difference of interpretation of the CV failure data would have been avoided.

Finally, the sensitivity analysis performed in Part 4.4.2 was not as useful as expected during the review process. While this may be due to the lack of time available to the reviewers, it is also linked to the previous comment. Indeed, the sensitivity analysis was performed so that the reviewers could compare their informed belief with the maximum values presented in the sensitivity analysis. As reviewers were reluctant to elicit their belief, these values were not effectively useful.

5.2. Dealing with Information asymmetries

One important aspect of the risk-based simulation is the management of information. There is a clear information asymmetry in the sense that the designer has much more information on its plant than the regulator and than the eventual buyer. One concern is that, if the designer does not disclose all the relevant information, then the assessment of the regulator would be distorted. In response to this asymmetry, the regulator may choose to err more on the side of conservatism. This could create a vicious circle: in response to undue conservatism, the designer may be tempted to hide more information...[xix]

[xix] The issue of the regulator obtaining appropriate information is more subtle than just the possibility of the designer hiding some unfavorable data. It can take more insidious forms: for example the designers will have an incentive to do a very careful analysis of the main risk contributors in order to find arguments for decreasing their frequency and for ensuring they have not been overestimated. In contrast there is no incentive for the

A specific domain in which information asymmetries could be found is in the use of generic data values.[60] Indeed a designer would have an incentive to depart from generic values only if he were to think that the safety performance of the plant would be better than the generic data.[xx] The use of default values should therefore be seen by the regulator as "red flags" requiring more careful review.

Therefore a prerequisite for the proper functioning of a risk-based regulatory system is a mutual trust between the designer and the regulator. They must both work in cooperation. Our case study is an example of such a situation, as there was clearly no incentive for the student performing the safety analysis to hide the limitations of the analysis. Thus, they were clearly exposed. However, such a situation is not natural. Designers have natural incentives not to disclose unfavorable information, or at least to emphasize evidence for good safety performances.

Some incentive should therefore be given for the designer to work in real partnership with the regulator.

We think that the discussion framework presented in this study can help achieving this purpose. During early design stages, there are fewer incentives for the designer to try to hide important problems. Its goal is to improve the design and get the feedback of the regulator on important issues. It is thus an opportunity for a real dialog and cooperation with the regulator. The reviews by the NRC and by third parties will try to highlight the areas where the evidence presented is insufficient. If the review is careful enough, there will be few possibilities for not presenting all of the needed information.

---

designer to ensure that other frequencies less reviewed have not been underestimated. It would be the purpose of the reviews to ensure that it has not been the case, but the active cooperation of the designer would make the process go faster and be more efficiently.

[xx] A way to counter this incentive would be to set more conservative generic values. This would provide incentives to perform and disclose more plant specific testing, to justify taking more reliable values than the generic ones. But using conservative values would compromise the goal of PRA, which is to give the most accurate possible quantification of the risk.

Finally, there should be clear financial incentives for the designer to disclose information and to perform needed testing. Heavy penalties should be imposed if after the fact "bad faith" of the designer has been proven. A mandatory strict living PRA program may also be an incentive for the designer to present the best safety analysis possible, as the results of the living PRA could demonstrate whether the design safety analysis had been performed adequately. The regulator could also make the designer pay a high price for the review process: the designer would therefore have an incentive to make it go as fast as possible, and would propose a design with more evidence to support its assumptions.

Thus, there are ways to increase the trust between the regulator and the licensee. Other possibilities should be investigated. However, even if perfect cooperation between the licensee and the regulator may be impossible to achieve, this should not be seen as an argument against using risk-based regulations. This problem exists with deterministic regulations as well, and is currently addressed through formally unjustified decisions from the regulator. The risk-based dialog offers opportunities to create a real dialog and to increase the trust between the regulator and the licensee.

5.3. Licenses for generation IV reactors

The safety analysis of the GFR has highlighted the difficulties of obtaining good data for innovative generation IV reactors. Although it may be possible to obtain some data from existing gas reactors, the applicability to new designs will always be problematic. It will involve important subjectivity, and the regulator should be careful when reviewing how the designers accounted for these epistemic uncertainties. It may be useful to develop guidelines on this subject.

In the case study presented here, engineering analysis are used to justify the use of generic values. For example, concerning the failure of the CV to open, the forces to open it are assessed and are considered very high. Clearly, a more rigorous analysis would be needed at later licensing stages.

However, it is likely that knowledge uncertainties about new reactors will have to be handled by adding redundancy. This was the approach taken for concerns about passive convections reliability. While more extensive probabilistic safety analyses of passive systems are performed in other research projects,[56] the option chosen here was to include active convection capabilities. This approach is comparable to that chosen at the beginning of the civil nuclear era, when precaution imposed several barriers. However, in a risk-based approach, epistemic uncertainties and the effect of redundancy are quantified. Moreover, the designer can choose the most efficient option between the alternatives of decreasing the epistemic uncertainty and changing the design.

6. Conclusion

Starting from the statement that current licensing regulations are not well-adapted to an efficient development of the nuclear power plants fleet, a risk-based regulatory framework is proposed. It is based on previous work at MIT.[3] PRA is used as an instrument to create a dialog between the regulator and the designers and serves as a vehicle to state the informed beliefs of each party. This framework is preferred to the current NRC efforts to risk-inform regulations because it is considered that it would lead to more efficient decisions. We believe that PRA methodology improvements will be able in the medium run to support risk-based regulations.

Possible quantitative safety goals have been proposed as base of the risk-based discussion. Compliance with a high level safety goal ensures that adequate safety is being provided, while satisfaction of lower levels safety goals ensures appropriate management of uncertainties. A treatment of key uncertainties based on the Risk Increase Ratio measure is proposed.

A case study has been conducted to test this methodology. It is based on a project for a generation IV reactor. The safety analysis focuses on Loss Of Offsite Power events.

A first part of the case study illustrates how the design can be driven by PRA results. Discussions between PRA experts and the design team of the PRA results and of the PRA inputs highlighted new safety concerns and led to innovative design solutions. The process was successful in achieving a very high level of safety. Diverse importance calculations demonstrated the robustness of the design.

During the second part of the case study, the review by the regulator was simulated. A discussion took place between mock NRC experts, the safety analyst, and the designers. A few safety concerns were discussed, but the NRC experts globally agreed on the high quality of the design.

This review highlighted the need for systematic probabilistic analysis of success criteria that should be included in the PRA, and presented to the regulator for review. The difficulty of identifying and treating key uncertainties in a predictable way was apparent.

However, the case study did not reveal any serious flaw in the iterative risk-based methodology used. As it would be a very powerful tool to promote the development of nuclear power plants, more research should be done to improve PRA methodology.

Many areas of PRA would need improvements in order to support risk-based regulations. The probabilistic treatment of success criteria and modeling uncertainties should first be generalized. Technical experts should be trained to elicit their judgments so that they could be explicitly integrated into the analysis. A framework for the inclusion of plant construction, operations and management regulations should be designed.

Peer and regulatory PRA review capacities would have to be increased. This would be the best assurance against needlessly large completeness uncertainties.

The NRC should lead part of the research effort to improve PRAs. Indeed, this research would benefit to the entire nuclear industry. The existence of these positive externalities would lead to underinvestment if the private sector does all the research. A strong commitment of the NRC is also needed to set the path for industrials and build trust that PRA use will increase in future regulations.

7. References

[1] Deutch, J., Moniz, E. J., Ansolabehere, S., Driscoll, M., Gray, P. E., Holdren, J. P., Joskow, P. L., Lester, R. K., and Todreas, N. E. "The Future of Nuclear Power: An Interdisciplinary MIT Study". Cambridge, MA, MIT, 2003

[2] Westinghouse Electric Company, "AP-1000 Probability Risk Assessment, Revision 1," Pittsburgh, PA, 2003

[3] Beer, B., Golay, M. W. and.Apostolakis, G.E., "Feasability Investigations for Risk-Based Nuclear Safety Regulation", MIT-NSP-TR003, February, 2000

[4] 42 U.S.C. § 2232(a).

[5] 42 U.S.C. § 2201(b).

[6] USNRC, "NRC - Regulator of Nuclear Safety" , NUREG/BR-0164, Revision 4, Washington, D.C.

[7] Apostolakis, G.E., "The Concept Of Probability In Safety Assessment Of Technological Systems", *Science, **250**,* 1359-1364, 1990

[8] U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, "Regulatory Structure For New Plant Licensing, Part 1: Technology-Neutral Framework," Draft, 2004.

[9] U.S. Nuclear Regulatory Commission, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant Specific Changes to the Licensing Basis," Regulatory Guide 1.174. Washington, DC, 1998

[10] James, W., "Pragmatism: A New Name for Some Old Ways of Thinking," New York: Longmans, Green, 1907

[11] See supra note 4

[12] Apostolakis, G. E., "The Precautionary Principle and Defense in Depth," Presented at the Second ILK SymposiumMunich, October 28, 2003.

[13] From NRC website: Glossary, http://www.nrc.gov/reading-rm/basic-ref/glossary/design-basis-accident.html

[14] Sorensen, J.N., Apostolakis, G. E., Kress, T.S., and Powers, D.A., "On the Role of Defense in Depth in Risk-Informed Regulation," Proceedings of PSA '99, International Topical Meeting on Probabilistic Safety Assessment, pp. 408-413, Washington, DC, August 22 - 26, 1999, American Nuclear Society, La Grange Park, Illinois

[15] Report dated May 19, 1999, from Dana A. Powers, Chairman, Advisory Committee on Reactor Safeguards, to Shirley Ann Jackson, Chairman, NRC, Subject: The Role of Defense in Depth in a Risk-Informed Regulatory System

[16] Beck, C., "Basic Goals of Regulatory Review: Major Considerations Affecting Reactor Licensing," Statement submitted to the Joint Committee on Atomic Energy, Congress of the United States, Hearings on Licensing and Regulation of Nuclear Reactors, April 4,5,6,20, and May 3, 1967

[17] From NRC website: Full-Text Glossary, http://www.nrc.gov/reading-rm/basic-ref/glossary/full-text.html

[18] "Nuclear Regulation: Strategy Needed to Regulate Safety Using Information on Risk", US General Accounting Office, Report to Congressional Requesters, March 1999, GAO/RCED-99-95

[19] USNRC, "Reactor Safety Study – An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants", WASH-1400 (NUREG-75/014), October 1975

[20] "Report Of The Technical Assessment Task Force On Technical Staff Analysis Reports Summary", Leonard Jaffe, Technical Assessment Task Force, Staff Reports to The President's Commission on The Accident at Three Mile Island, October 1979, Washington, D. C

[21] Report dated October 11, 2000, from Dana A. Powers, Chairman, Advisory Committee on Reactor Safeguards, to Richard A. Meserve, Chairman, NRC, Subject: Union Of Concerned Scientists Report, "Nuclear Plant Risk Studies: Failing The Grade"

[22] Memorandum dated February 24, 1999, from Annette Vietti-Cook, Secretary, NRC, to William D. Travers, Executive Director for Operations, NRC, Subject: Staff Requirements Memorandum - SECY-99-144 - White Paper on Risk-Informed and Performance-Based Regulation

[23] Poloski, J. P., et al., "Rates of Initiating Events at U.S. Nuclear Power Plants: 1987 – 1995," NUREG/CR-5750, Idaho National Engineering and Environmental Laboratory, February 1999.

[24] From NRC website: Use of Risk in Nuclear Regulations, http://www.nrc.gov/what-we-do/regulatory/rulemaking/risk-informed.html

[25] USNRC, "Use of probabilistic risk assessment methods in nuclear activities: Final policy statement," 60 FR 42622, Federal Register, Vol. 60, U. S. Nuclear Regulatory Commission, August 1995

[26] USNRC, "An approach for using probabilistic risk assessment in risk-informed decisions on plant-specific changes to the current licensing basis," Regulatory guide 1.174, June 1998

[27] Travers, W.D, "Update Of The Risk-Informed Regulation Implementation Plan," SECY-03-0044, Attachment 2, 2003

[28] Travers, W.D, "Status Report On Risk-Informing The Technical Requirements Of 10 Cfr Part 50 (Option 3)", SECY-00-0086, attachment 1, *Framework For Risk-Informing The Technical Requirements Of 10 Cfr 50* Draft, Revision 0

[29] USNRC, "Safety Goals for the Operation of Nuclear Power Plants; Policy Statement," *Federal Register,* Vol. 51, p. 30028, August 21, 1986.

[30] Callan, L.J, "Elevation of the core damage frequency objective to a fundamental commission safety goal," Technical report, U. S. Nuclear Regulatory Commission, September 1997.

[31] USNRC, , "Framework for Risk-Informed Changes to the Technical Requirements of 10 CFR 50", SECY-00-0198, attachment 1, 2000

[32] USNRC, "Policy Issues Related to Licensing Non-Light-Water Reactor Designs," SECY-03-0047, 2003

[33] USNRC, Office of Nuclear Regulatory Research, "Frame work for Risk-Informing the Technical Requirements of 10 CFR 50," SECY-00-0198, Attachment 1, Washington, DC, 2000

[34] Speech by Dr. Shirley Ann Jackson, Chairman, USNRC, "Transitioning to Risk-Informed Regulation: The Role of Research," speech S-98-26, October 1998.

[35] Organization for Economic Co-operation and Development, "Regulatory Approaches to PSA - Report on the Survey of National Practices," NEA/CNRA/R(1995)2, CNRA Paris, Special Issues, 1996.

[36] A. D. Swain and H. E. Guttmann, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications," Report NUREG/CR-1278, U.S. Nuclear Regulatory Commission, Washington, D.C., 1983.

[37] From NRC website: Common-Cause Failure Database, available at:

http://nrcoe.inel.gov/results/index.cfm?fuseaction=CCFDB.showMenu

[38] Xu, M., "Model Combination by Decomposition and Aggregation," Cambridge, Massachusetts, MIT, Ph.D Thesis, 2004.

[39] Interview of Apostolakis, G.E., by Michal, R., "Apostolakis: On PRA," Nuclear News, p27, March 2000

[40] Organization for Economic Co-operation and Development, "State Of Living Psa And Further Development," NEA/CSNI/R(99)15, 1999

[41]Gillette, C. P., and Krier, J.E. "Risk, Courts and Agencies", University Of Pennsylvania Law Review, 138 U. Pa. L. Rev. 1027, April, 1990

[42] Ashford, N. A., "Science and Values in the Regulatory Process", Stat. Science, Vol. 3, No. 3, 1988, p 377-383

[43] Walker, V. R.,"The Myth Of Science As A "Neutral Arbiter" For Triggering Precautions", Boston College International And Comparative Law Review, 26 B.C. Int'l & Comp. L. Rev. 197, Spring, 2003

[44] Speech by Commissioner Nils J. Diaz, "Remarks Before the American Radiation Safety Conference and Exposition," 46th Annual Meeting of the Health Physics Society, Cleveland, Ohio, June 11, 2001

[45] Apostolakis, G.E., Koser, J.P., Sato, G., "Decision Analysis and Its Application to the Frequency of Containment Integrated Leakage Rate Tests," Nuclear Technology, Volume 146, Number 2, May 2004, Pages 181-198

[46] Apostolakis, G.E., Golay, M.W., Camp, A., Duran, F., Finnicum, D., Ritterbusch, S, "A New Risk-Informed Design And Regulatory Process", 2001

[47] Idaho National Engineering and Environmental Laboratory, SAPHIRE, Available at: http://saphire.inel.gov

48 Delaney, M.J., "Risk-Informed Design Guidance for a Generation-IV Gas-Cooled Fast Reactor Emergency Core Cooling System," MIT-GFR-013, 2004

[49] Pagani, L., "On the Quantification of Safety Margins", Cambridge, Massachusetts, MIT, Ph.D Thesis, 2004.

[50] USNRC, "Loss Of Offsite Power", available at: http://nrcoe.inel.gov/results/index.cfm?fuseaction=LOSP.showMenu

[51] USNRC, "Severe Accident Risk Assessment for Five U.S. Nuclear Power Plants", **NUREG-1150**, Draft 2, 1989.

[52] Dupuy P., Corenwinder F., Lanore J.M., Gryffroy D., De Gelder P. and Hulsmans M., "Comparison of the level 1 PSA for two similar PWR types : the French 900 MWe-series PWR and the Belgian Tihange 1 PWR," Proceedings of the PSAM 5 Conference, Osaka (Japan) 1, 2000, 559-564

[53] C. Atwood et al, "Evaluation of Loss of Offsite Power Events at Nuclear Power Plants: 1980 – 1996," NUREG/CR-5496, Idaho Engineering and Environmental Laboratory, November 1998

[54] Devictor, Nicolas, Commissariat à l'Energie Atomique, personal communication, 2004

[55] European Commission, "Methods of identification and quantification of the sources of uncertainties", Reliability Methods for Passive Systems functions (RMPS) project, deliverable 1, 2002

[56] European Commission, "Reliability Methods For Passive Systems", RMPS project, deliverable 12, 2004

[57] Kopustinskas, V., "Approaches For Introducing Passive System Unreliability In Accidental Sequence", in RMPS project, deliverable 7, 2003

[58] Williams, W.C., Hezlar, P., Saha, P., "Analysis of a Convection Loop for GFR Post-LOCA Decay-Heat Removal," Proc. of the 12th International Conference on Nuclear Engineering, ICONE12-49360, ASME, Arlington, VA, USA (2004)

[59] USNRC, "An Approach For Determining The Technical Adequacy Of Probabilistic Risk Assessment Results For Risk-Informed Activities," Regulatory Guide 1.200 For Trial Use, February 2004

[60] Seung-cheol Jang, Won-dea Jung, Kwang-sub Jeong, Jae-joo Ha and Young-ho Jin, "Implication of Default Values Specified for Use in Risk Analyses," 5th Korea-Japan PSA Workshop, Seoul, Korea, April 1999

Appendices

A. LOOP model

A.1 GFR Design Parameter Summary

The main characteristics of the GFR are summarized in **Table A-1**.

Attribute	Option
Power	2400 MWt
Coolant	CO2 (direct cycle) or He (indirect cycle)
Power Cycle	Supercritical CO2, direct or indirect
Reactor Vessel	Prestressed Cast Iron Vessel (PCIV) or Prestressed Concrete Reactor Vessel (PCRV)
Shutdown Cooling System (combined Shutdown & emergency)	3 x 50% capable loops forced + passive convection water-boiler ultimate heat rejection
Containment	PWR type sized to keep post-LOCA pressure ~5atm

Table A-1: Main design characteristics of the GFR

A.2 PRA Model for LOOP Event Sequences

A.2.1 Event Trees

The event tree analysis for the LOOP is composed of four trees. The first tree (Figure A-1) models the events during the first hour after the LOOP. Then, it is considered whether offsite power has been recovered or not ("RECOV_1 event"):

- Recovery successful: the transfer is made to REC1-24H (Figure A-2)
- Recovery unsuccessful: the transfer is made to NREC1-24H (Figure A-3).

If the recovery has been successful, a 24 hours mission time is considered to check that normal cooling of decay heat can be performed. If normal cooling can be performed during 24 hours, then it is assumed that the accident initiation is terminated.

If the recovery is not successful after 1 hour, then a 24 hours mission time is also considered. If the core can be cooled during 24 hours, another recovery event is introduced ("RECOV_24 event"):. Then:

- Recovery successful: the accident is considered as terminated
- Recovery unsuccessful: the transfer is made to NREC24-200H (Figure A-4).

NREC24-200H is the last subtree. The mission time is 200 hours. No further transfer is made: if the core can be cooled during 200 hours, then it is assumed that the LOOP has been successfully mitigated.

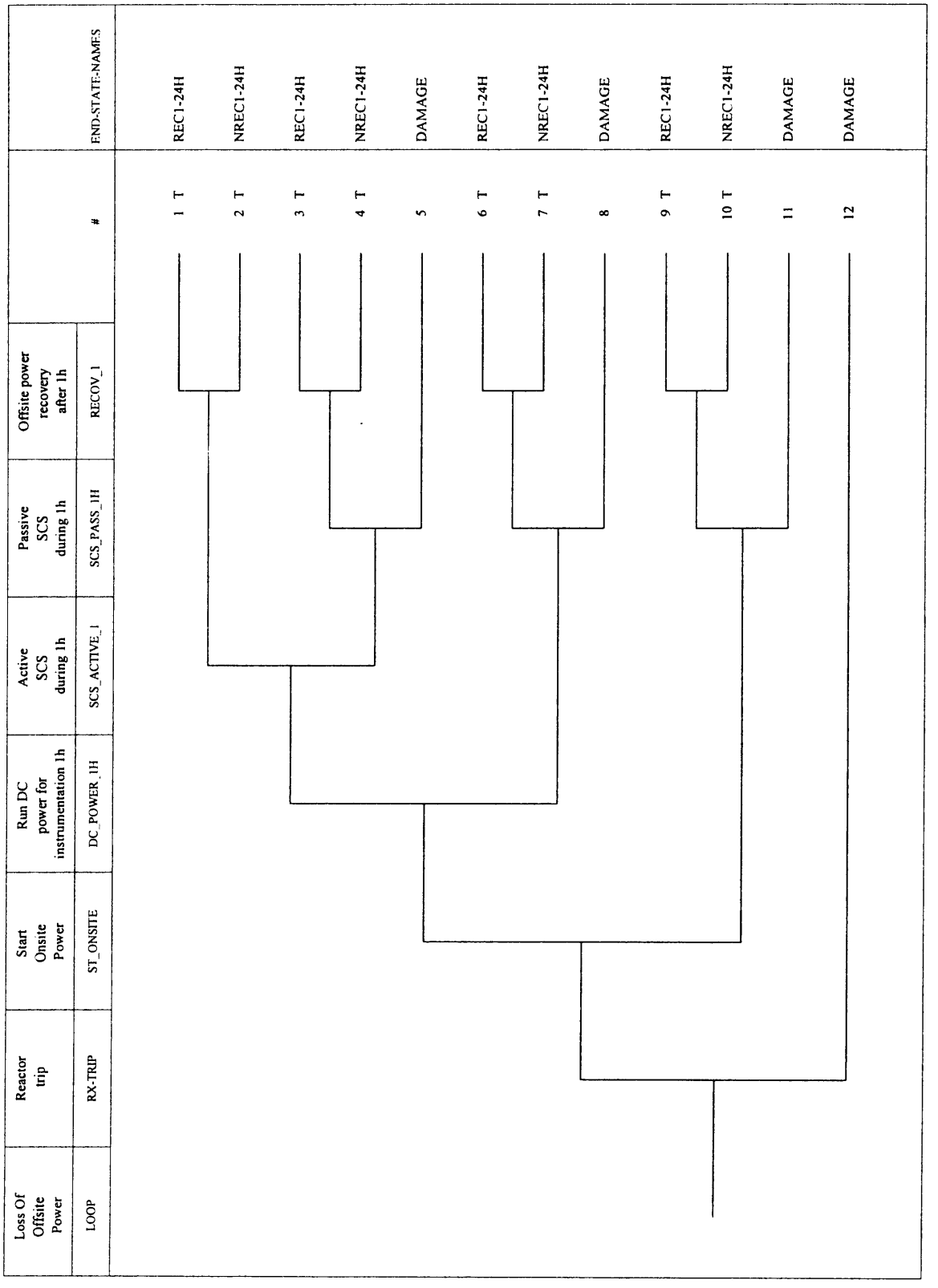


Figure A-1: LOOP event tree (first hour)

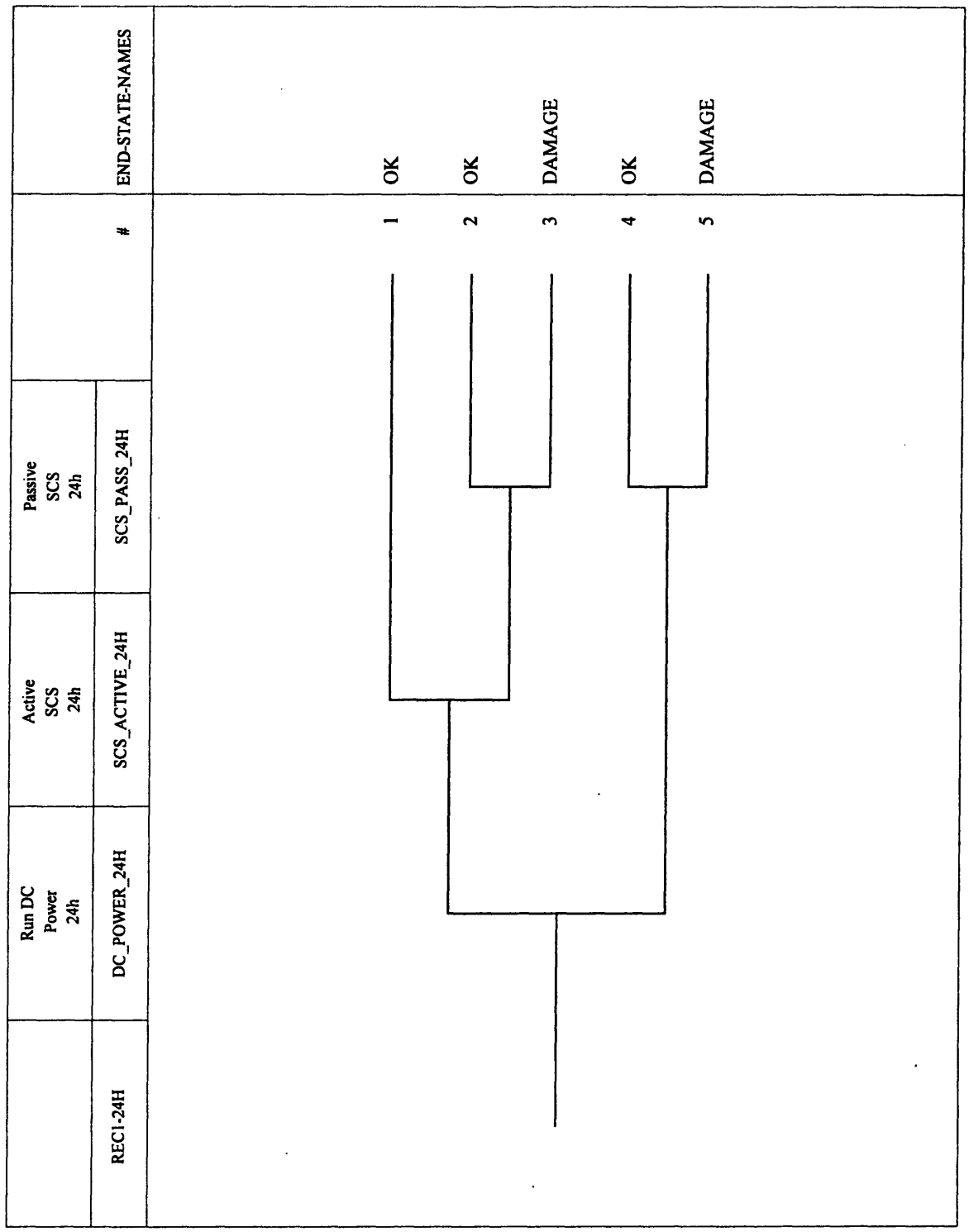


Figure A-2: REC1-24H LOOP event tree (24 hrs mission time)– subtree for the case recovery after 1 hour is successful.

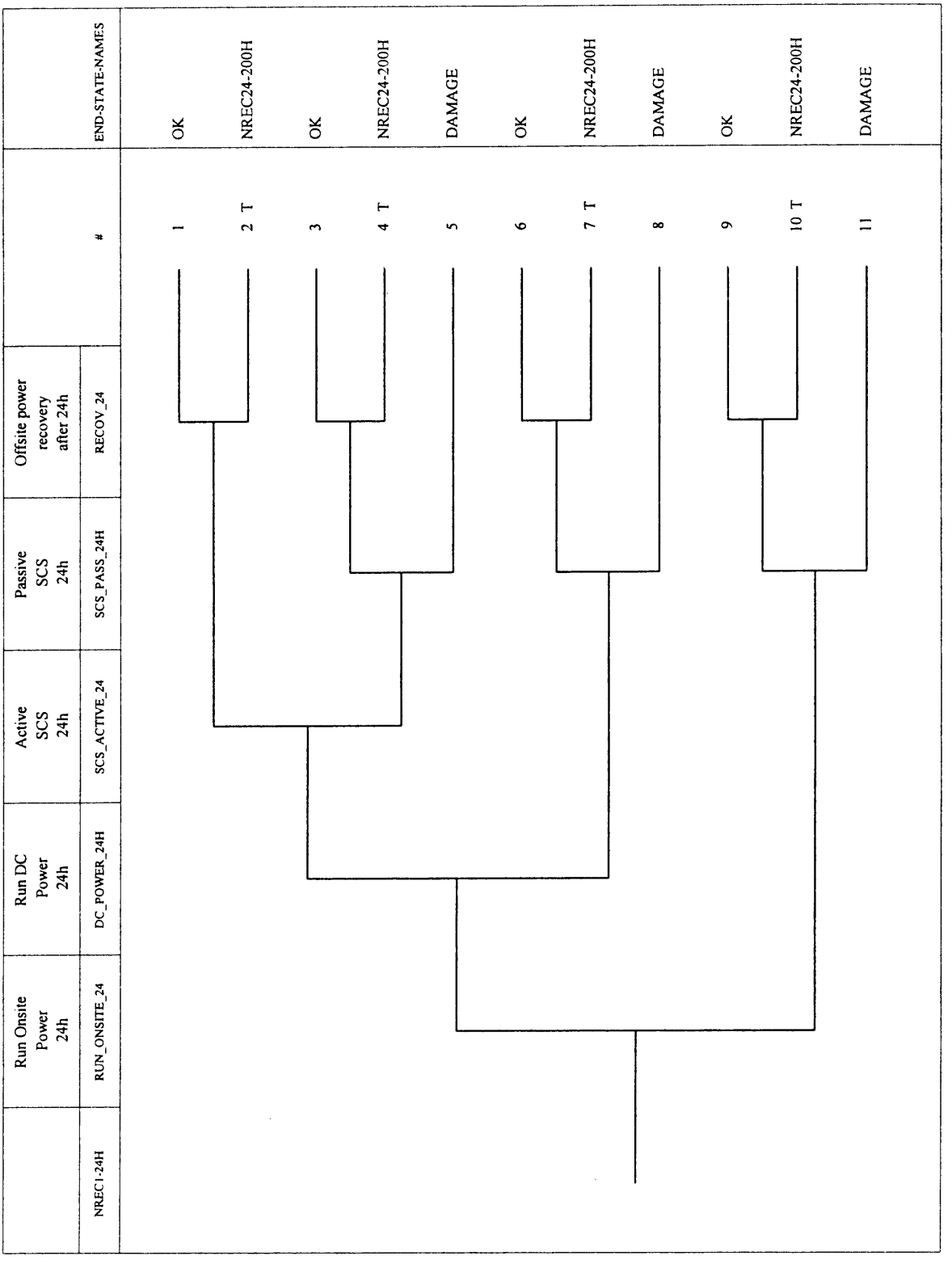


Figure A-3: NREC1-24H LOOP event tree (24 hrs mission time)– subtree for the case recovery after 1 hour failed

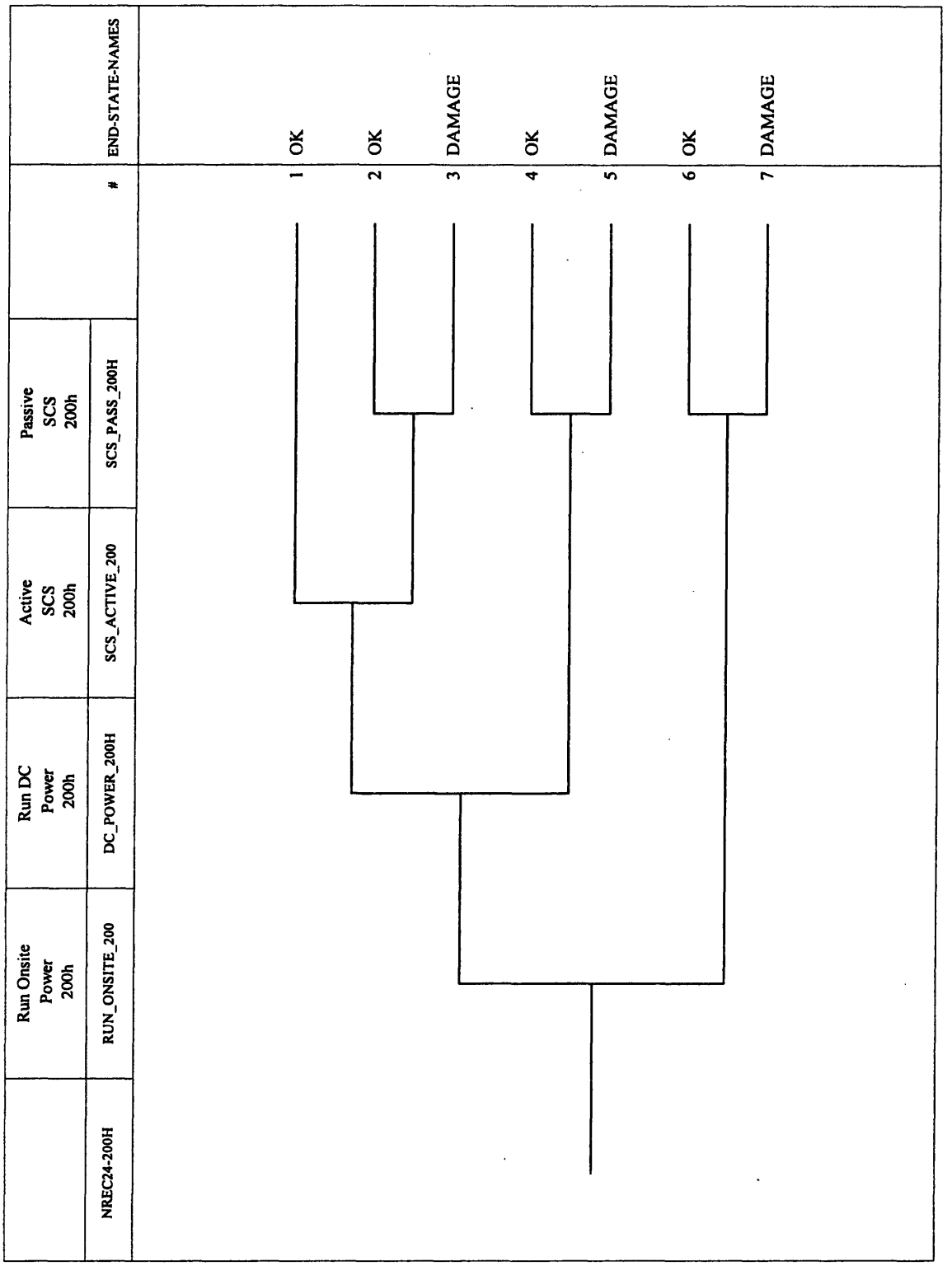


Figure A-4: NREC24-200H LOOP event tree (200 hrs mission time)– subtree for the case recovery after 24 hours failed

A.2.2 Top events

Reactor Scram System:

The reactor must be tripped immediately after the LOOP. The failure of the scram will have to be specifically addressed in the Anticipated Transient Without Scram (ATWS) ET. As it has not been studied yet, we conservatively assume that a failure to scram will lead to core damage.
The scram system has not been designed yet, so that its failure probability must be assessed from other PRA studies. $10^{-6} - 10^{-5}$ are common failure probability values for failure of reactor trip on demand. However, fast reactors need to have especially reliable scram systems. Therefore a better reference is the system licensed for the Clinch River Breeder reactor (also a fast reactor). The scram system was composed of two mechanically independent scram systems, and the unavailability of the systems was supposed to be $7*10^{-5}$ for the primary and $8*10^{-5}$ for the secondary.[xxi]
Therefore, we conservatively took a reactor trip failure probability of 10^{-7} / demand and an Error Factor (EF) of 30.[xxii] The trip will be designed to bring the core to 2% of its maximum power level. Then a system is needed to remove the decay heat.

AC Power Generation

Offsite Power constitutes the preferred AC power source for operation of all the active components, so that onsite AC power generation is needed after a LOOP to cool the core through active convection. In existing power plants, emergency diesel generators are used to generate emergency AC power. This is also our reference AC source. Thus, if nothing else is specified, onsite AC power in the ET means diesel AC power. Two diesels are used in the final design, but options from one to three diesels have been investigated. Each diesel is supposed to be able to support 100% of the load (one diesel is needed and sufficient for success).
The failure modes for the AC system are the following: failure to order the diesels activation, failure to start the diesels, failure to run the diesels for a given time and failure of power transmission. Associated fault trees are represented from Figure C-1 to Figure C-4.

[xxi] Clinch River Breeder Reactor Plant, Preliminary Safety Analysis Report, Appendix C, 1976(?)

[xxii] This is equivalent to assuming that the CCF beta factor for the failure of both trip systems would be $1.4*10^{-3}$. It is a very low value for a CCF parameter, but the system would be designed to be independent. In the Clinch River safety analysis, there is actually no mention of CCF between both systems. In the GFR, even with a CCF factor one order of magnitude higher, the failure sequence involving failure to trip would be 10^{-6}, which would far below the CDF limits.

DC Power Generation

DC power is needed for all plant instrumentation. Its failure therefore makes it impossible to operate the active cooling system. Three batteries, each capable of meeting 100% of the DC demand are used in our model. The failure of DC generation will therefore essentially be CCFs. We used a CCF value found in the Lungmen PRA,[xxiii] and it appears that DC power failure is not an important risk contributor (the failure of the diesels is much more likely). One associated fault tree (FT) is shown on Figure C-5.
If both AC and DC power are available, then the failure of the active cooling system is considered.

Active SCS:

This is the preferred cooling mode. All the licensed reactors in the US rely mainly on an active cooling system after shutdown.
Three loops are used, and each in capable of removing 50% of the maximum decay heat after the trip (2% of full power). The design of one loop is shown on Figure 4-5. In each loop a blower forces the flow between the core and a heat exchanger.
In each SCS loop, the identified main points of possible failure are: flow blockage (CV failure), failure to force the flow (blower, electric motor), failure of the heat exchange (Heatric heat exchanger, Water Boiler Loop). The Water Boiler Loop (WBL) failures modes are: insufficient water flow, and insufficient water available. Associated fault trees are represented from Figure C-6 to Figure C-11.

Passive SCS:

The SCS can be designed so that the core will be cooled by passive convection. But it would be relied on only if the preferred active cooling mode fails.
In this case there are no active components that can make the system fail, but the flow can still be blocked by the failure of a CV. It is all the more important to consider it that under natural convection the forces to open the CV would be smaller (it will open only under gravity, with very limited flow from standby blower). Therefore the CV failure probability is higher in these conditions, and we differentiate between the failure under full active flow ("CV failure") and the one under passive flow ("CV failure", see Appendix B)
The failure of the heat exchanger is also common to the active and passive modes.
Finally, functional failures of the passive convection to start or to maintain steady-state are also integrated in the fault tree analysis of the passive convection mode. The fault trees are represented from Figure C-12 to Figure C-15. We present in Part 4.2.3 the challenge in assessing such failures.

[xxiii] PRA from the Preliminary Safety Analysis Report of the Lungmen plant (Taïwan), available at: http://www.aec.gov.tw/npp4info/lm_document_psar_Aa.pdf

B. Basic Events for the PRA

B.1 Basic events description and failure data

The basic events used in the PRA model are described briefly in Table B-1. Then in Table B-2 the failure probabilities used in the PRA model are given, and the most important ones are discussed in Appendice B.2.

When there are multiple identical components, only one is reported here. Thus "SCS-1-CV-OPEN" refers to the CV located in the loop 1 (similarly there are a "SCS-2-CV-OPEN" and a "SCS-3-CV-OPEN" in the model). The mission time considered for each event is mentioned ("RUN-DIESEL1-24" refers to the failure of diesel 1 to run during a 24 hours mission time).

Basic Event	Description
AC-ORDER-RECOV-1H	Failure to recover after 1h from AC order failure
AC-ORDER-RECOV-24H	Failure to recover after 24h from AC order failure
AUTOMATIC-AC	Failure to initiate onsite generation automatically
AUTOMATIC-SCS	Automatic SCS activation failure
BATTERY-1-CHARGER-1H	Battery 1 charger failure 1h
BATTERY-1-CHARGER-200H	Battery 1 charger failure 200h
BATTERY-1-CHARGER-24H	Battery 1 charger failure 24h
BATTERY-1-POWER-SYST-1H	Failure to provide output on demand batt 1 1h
BATTERY-1-POWER-SYST-200	Failure to provide output on demand batt 1 200
BATTERY-1-POWER-SYST-24H	Failure to provide output on demand batt 1 24h
BETA-BLOWER-RUN	Beta factor for blower failure to run
BETA-BLOWER-START	Beta factor for blower failure to start
BETA-BLOWER-STBY	Beta factor for blower standby failure
BETA-CP-OP	Beta factor for CP failure to open
BETA-CV-OP	Beta factor for CV failure to open
BETA-CV-STAY-OP	Beta factor for CV failure to stay open
BETA-DIES-RUN	Beta factor CCF diesel to run
BETA-DIES-START	Beta factor CCF diesel to start
BETA-EL-MOTOR-RUN	Beta factor for el motor failure to run
BETA-EL-MOTOR-START	Beta factor for el motor failure to start
BETA-HEAT-EXCH	Beta factor for Heat Exchanger failure
BETA-PASS-W-FLOW	Beta CCF factor for passive water flow WBL
BETA-PUMP-RUN	Beta factor for pump failure to run
BETA-PUMP-START	Beta factor for pump failure to start
BLOWER-1-RUN-200H	Blower 1 Failure Run 200h
BLOWER-1-RUN-24H	Blower 1 Failure Run 24h
BLOWER-1-START	Blower 1 Start Failure
BLOWER-1-STBY-IND-FAIL	Standby Blower 1 failure
CCF-BATT-1H	CCF Battery 1H
CCF-BATT-200H	CCF Battery 200H
CCF-BATT-24H	CCF Battery 24H
CCF-BL-R-200	CCF Blower run 200
CCF-BL-R-24	CCF Blower run 24h
CCF-BL-ST	CCF Blower start
CCF-CP-OP	CCF CP open
CCF-CPSTO-200	CCF CP stay open 200
CCF-CPSTO-24	CCF CP stay open 24h

Table B-1: Description of the basic events used in the PRA

CCF-CV-OP	CCF CV open
CCF-CVSTO-200	CCF CV stay open 200
CCF-CVSTO-24	CCF CV stay open 24h
CCF-DIES-200	CCF diesel run 200h
CCF-DIES-24	CCF diesel run 24h
CCF-DIES-ST	CCF diesel start
CCF-ELM-R-200	CCF elect motor run 200h
CCF-ELM-R-24	CCF elect motor run 24h
CCF-ELM-ST	CCF elect motor start
CCF-HX-1	CCF HCHX 1H
CCF-HX-200	CCF HCHX 200
CCF-HX-24	CCF HCHX 24H
CCF-PASS-ST	CCF passive start
CCF-PASS-W-1H	CCF passive water loop 1h
CCF-PASS-W-200	CCF passive water loop 200h
CCF-PASS-W-24H	CCF passive water loop 24h
CCF-PUMP-1H	CCF pump 1h
CCF-PUMP-200H	CCF pump 200h
CCF-PUMP-24H	CCF pump 24h
CCF-STBY-BLOWER	CCF standby blower
CCF-TRANSM-DC-1H	CCF in DC transmission 1H
CCF-TRANSM-DC-200H	CCF in DC transmission 200H
CCF-TRANSM-DC-24H	CCF in DC transmission 24H
DIES-1-UNAV	Diesel 1 is unavailable
DIES-2-UNAV	Diesel 2 is unavailable
DIES-3-UNAV	Diesel 3 is unavailable
HCHX-1-1H	Heatric Heat Exchanger 1 Failure 1h
HCHX-1-200H	Heatric Heat Exchanger 1 Failure 200h
HCHX-1-24H	Heatric Heat Exchanger 1 Failure 24h
IND-FAIL-DIES1-200	Failure probability of diesel 1 during 200h without repair
IND-FAIL-DIES1-24H	Failure probability of diesel 1 during 24h without repair
INDICATION	Indication Failure
INVERTOR-1-1H	Failure of AC DC invertor 1 1h
INVERTOR-1-200H	Failure of AC DC invertor 1 200h
INVERTOR-1-24H	Failure of AC DC invertor 1 24h
LOOP-1-UNAV	Loop 1 is unavailable
LOOP-2-UNAV	Loop 2 is unavailable
LOOP-3-UNAV	Loop 3 is unavailable
LOOP-4-UNAV	Loop 4 is unavailable
MAN-AC-ACT-HARDWARE	Failure of hardware used for manual activation of AC generation
MANUAL-ACT-HARDWARE	Failure of hardware used for manual activation of SCS

Table B-1 (continued): Description of the basic events used in the PRA

MOTOR-SCS-1-RUN-200H	Electric Motor SCS 1 run 200h Failure
MOTOR-SCS-1-RUN-24H	Electric Motor SCS 1 run 24h Failure
MOTOR-SCS-1-START	Electric Motor SCS 1 Start Failure
NO-PASSIVE-DESIGN	NO PASSIVE DESIGN (used to see risk with no passive mode)
NO-REC1-FROM-D-CCF-24H	No recovery from Diesels CCF 24H
NREC1-24H	Introduce Subtree after recovery failure after 1 hour - 24 hrs mission time tree
NREC24-200H	Introduce Subtree after recovery failure after 24hours - 200hrs mission time tree
OPERATOR-AC-ACT-FAIL	Operator failure to activate AC
OPERATOR-SCS-ACT-FAIL	Operator failure to activate SCS
PASSIVE-START	Failure of passive convection to start in SCS
PASSIVE-STEADY-200H	Failure of passive steady state 200h
PASSIVE-STEADY-24H	Failure of passive steady state 24h
PASS-W-FLOW-1-1H	Failure of passive water flow in WBL 1 during 1 hour
PASS-W-FLOW-1-200	Failure of passive water flow in WBL 1 during 200 hours
PASS-W-FLOW-1-24H	Failure of passive water flow in WBL 1 during 24 hours
PUMP-1-FAILURE-1H	Pump 1 failure 1h
PUMP-1-FAILURE-200H	Pump 1 failure 200
PUMP-1-FAILURE-24H	Pump 1 failure 24h
REC1-24H	Introduce Subtree after recovery success after 1 hour - 24 hrs mission time tree
RECOVW_1	LOOP recovery after 1 hour
RECOVW_24	LOOP recovery after 24 hours
RUN-DIESEL1-200	Failure to run diesel 1 200h
RUN-DIESEL1-24	Failure to run diesel 1 24h
RX-TRIP	Reactor Trip
SCS-1-CP-OPEN	SCS 1 CP Failure to Open
SCS-1-CP-STAY-OP-200	SCS 1 CP Failure to stay Open 200h
SCS-1-CP-STAY-OP-24H	SCS 1 CP Failure to Open Open 24h
SCS-1-CV-OPEN	SCS 1 CV Failure to Open
SCS-1-CV-STAY-OP-200	SCS 1 CV Failure to stay Open 200h
SCS-1-CV-STAY-OP-24H	SCS 1 CV Failure to Open Open 24h
ST-AND-LOAD-DIES-1	Failure to start and load diesel 1
ST-FAIL-RECOV-D1-1H	Failure to recover from diesel1 failure to start after 1H
ST-FAIL-RECOV-D1-24H	Failure to recover from diesel1 failure to start after 24H
TRANSMISSION-1	Failure of elect onsite power transmission 1 h
TRANSMISSION-200	Failure of elect onsite power transmission 200h
TRANSMISSION-24	Failure of elect onsite power transmission 24
WATER-AVAIL-1H	Water unavailable 1h
WATER-AVAIL-200	Water unavailable 200h
WATER-AVAIL-24	Water unavailable 24h

Table B-1 (continued 2): Description of the basic events used in the PRA

The failure probabilities are given in Table B-2. The following information is given for each event:

- Calculation type (**Fdt**). It can take the values 1, 3 or 5 depending on the model used to calculate the failure probability:
  - 1: a simple failure probability is used as input,
  - 3: Failure probability of an operating component without repair. The model uses the following formula: P=1-exp(-lambda*mission time),
  - 5: Failure probability of an operating component with the possibility of repair following a failure.
  - c: Compound event. Used for CCFs.
- Uncertainty distribution used to model the epistemic uncertainty (**Udt**). "L" refers to the use of a lognormal distribution, and "N" to the exponential distribution.
- Uncertainty parameters used (**Ud Value**). It indicates the value of the error factor (for the epistemic uncertainties modeled by lognormal distribution) or of the standard deviation (for the epistemic uncertainties modeled by the exponential distribution).
- Single failure probability (**Prob**) used for type 1 calculation type
- Hourly failure rate (**Lambda**) used for type 3 and 5 calculation types
- Repair time for type 5 calculation type (in hours)
- Mission time for type 3 and 5 calculation types (in hours)
- The source of the data:
  - AP1000: From the AP1000 PRA.[xxiv]
  - Lungmen: From the PRA for the Lungmen plant (Boiling Water Reactor, Taïwan)[xxv]
  - S: the failure probability has been subjectively assessed.
  - D: historical data have been used to get the probability value.

[xxiv] Westinghouse Electric Company, "AP-1000 Probability Risk Assessment, Revision 1," Pittsburgh, PA, 2003

[xxv] See footnote [xxiii] for reference

Name of the Basic Event	FdT	UdT	Ud Value	Prob	Lambda	Rep time	Miss. time	Source
AC-ORDER-RECOV-1H	1	L	10	5.0E-01	--	--	--	S
AC-ORDER-RECOV-24H	1	L	10	1.0E-02	--	--	--	S
AUTOMATIC-AC	1	L	10	1.0E-04	--	--	--	Lungmen
AUTOMATIC-SCS	1	L	10	1.0E-04	--	--	--	Lungmen
BATTERY-1-CHARGER-1H	5	L	3	--	7.0E-06	10	1	AP1000
BATTERY-1-CHARGER-200H	5	L	3	--	7.0E-06	10	200	AP1000
BATTERY-1-CHARGER-24H	5	L	3	--	7.0E-06	10	24	AP1000
BATTERY-1-POWER-SYST-1H	5	L	3	--	2.0E-06	10	1	AP1000
BATTERY-1-POWER-SYST-200	5	L	3	--	2.0E-06	10	200	AP1000
BATTERY-1-POWER-SYST-24H	5	L	3	--	2.0E-06	10	24	AP1000
BETA-BLOWER-RUN	1	L	10	5.0E-02	--	--	--	AP1000
BETA-BLOWER-START	1	L	10	1.0E-01	--	--	--	AP1000
BETA-BLOWER-STBY	1		10	1.0E-01	--	--	--	AP1000
BETA-CP-OP	1	L	10	1.0E-01	--	--	--	AP1000
BETA-CV-OP	1	L	3	2.7E-02	--	--	--	AP1000
BETA-CV-STAY-OP	1	L	10	5.0E-02	--	--	--	AP1000
BETA-DIES-RUN	1	L	3	7.3E-02	--	--	--	AP1000
BETA-DIES-START	1	L	3	2.0E-02	--	--	--	AP1000
BETA-EL-MOTOR-RUN	1	L	10	5.0E-02	--	--	--	AP1000
BETA-EL-MOTOR-START	1	L	10	1.0E-01	--	--	--	AP1000
BETA-HEAT-EXCH	1	L	10	5.0E-02	--	--	--	AP1000
BETA-PASS-W-FLOW	1	L	10	1.0E-01	--	--	--	S
BETA-PUMP-RUN	1	L	3	6.0E-02	--	--	--	AP1000
BETA-PUMP-START	1	L	3	1.4E-01	--	--	--	AP1000
BLOWER-1-RUN-1H	3	L	10	--	2.0E-05	--	1	AP1000 + S (see App B)
BLOWER-1-RUN-200H	3	L	10	--	2.0E-05	--	200	
BLOWER-1-RUN-24H	3	L	10	--	2.0E-05	--	24	
BLOWER-1-START	1	L	10	1.0E-03	--	--	--	
BLOWER-1-STBY-IND-FAIL	1	L	10	1.0E-03	--	--	--	S
DIES-1-UNAV	1	L	10	4.6E-02	--	--	--	AP1000
DIES-2-UNAV	1	L	10	4.6E-02	--	--	--	AP1000
DIES-3-UNAV	1	L	10	4.6E-02	--	--	--	AP1000
HCHX-1-1H	3	L	10	--	1.0E-06	--	1	AP1000
HCHX-1-200H	3	L	10	--	1.0E-06	--	200	AP1000
HCHX-1-24H	3	L	10	--	1.0E-06	--	24	AP1000
IND-FAIL-DIES1-200	3	L	3	--	2.4E-03	--	200	AP1000
IND-FAIL-DIES1-24H	3	L	3	--	2.4E-03	--	24	AP1000
INDICATION	1	L	3	1.0E-06	--	--	--	AP1000
INVERTOR-1-1H	5	L	3	--	2.0E-05	10	1	AP1000
INVERTOR-1-200H	5	L	3	--	2.0E-05	10	200	AP1000
INVERTOR-1-24H	5	L	3	--	2.0E-05	10	24	AP1000

Table B-2: Failure data and sources

LOOP-1-UNAV	1	L	10	1.0E-05	--	--	--	S
MAN-AC-ACT-HARDWARE	1	L	10	1.0E-04	--	--	--	S
MANUAL-ACT-HARDWARE	1	L	10	1.0E-04	--	--	--	S
MOTOR-SCS-1-RUN-1H	3	L	3	--	1.0E-05	--	1	AP1000
MOTOR-SCS-1-RUN-200H	3	L	3	--	1.0E-05	--	200	AP1000
MOTOR-SCS-1-RUN-24H	3	L	3	--	1.0E-05	--	24	AP1000
MOTOR-SCS-1-START	1	L	3	3.0E-04		--	--	AP1000
NO-REC1-FROM-D-CCF-24H	1	L	10	1.0E-01	--	--	--	S
OPERATOR-AC-ACT-FAIL	1	L	10	2.6E-03	--	--	--	AP1000
OPERATOR-SCS-ACT-FAIL	1	L	10	1.0E-03	--	--	--	AP1000
PASS-W-FLOW-1-1H	1	L	15	1.0E-06	--	--	--	S
PASS-W-FLOW-1-200	1	L	15	1.0E-06	--	--	--	S
PASS-W-FLOW-1-24H	1	L	15	1.0E-06	--	--	--	S
PASSIVE-START	1	L	30	1.0E-02	--	--	--	S (see Part 4.2.3)
PASSIVE-STEADY-200H	1	L	30	1.0E-07	--	--	--	
PASSIVE-STEADY-24H	1	L	30	1.0E-08	--	--	--	
RECOVW_1	1	N	4.E-02	8.0E-01	--	--	--	D
RECOVW_24	1	N	7.E-03	1.6E-02	--	--	--	D
RUN-DIESEL1-200	5	L	10		2.4E-03	8	200	AP1000
RUN-DIESEL1-24	5	L	3		2.4E-03	8	24	AP1000
RX-TRIP	1	L	10	1.0E-07	--	--	--	See App B
SCS-1-CP-OPEN	1	L	10	1.0E-03	--	--	--	AP1000 + S (see App B)
SCS-1-CP-STAY-OP-200	3	L	30	--	4.0E-07	--	200	
SCS-1-CP-STAY-OP-24H	3	L	30	--	4.0E-07	--	24	
SCS-1-CV-OPEN	1	L	3	1.0E-04	--	--	--	AP1000
SCS-1-CV-STAY-OP-200	3	L	30		2.0E-07	--	200	AP1000
SCS-1-CV-STAY-OP-24H	3	L	30		2.0E-07	--	24	AP1000
ST-AND-LOAD-DIES-1	1	L	3	5.0E-02	--	--	--	AP1000
ST-FAIL-RECOV-D1-1H	1	L	10	5.0E-01	--	--	--	S
ST-FAIL-RECOV-D1-24H	1	L	10	5.0E-02	--	--	--	S
TRANSMISSION-1	1	L	10	1.0E-05	--	--	--	Lungmen
TRANSMISSION-200	1	L	10	5.0E-06	--	--	--	AP1000
TRANSMISSION-24	1	L	10	5.0E-07	--	--	--	AP1000
WATER-AVAIL-1H	1	L	10	1.0E-08	--	--	--	S
WATER-AVAIL-200	1	L	10	1.0E-06	--	--	--	S
WATER-AVAIL-24	1	L	10	1.0E-07	--	--	--	S

Table B-2 (continued): Failure data and sources

Common Cause Failure events								
CCF-BATT-1H	1	L	10	5.0E-05	--	--	--	Lungmen
CCF-BATT-200H	1	L	10	1.0E-03	--	--	--	Lungmen
CCF-BATT-24H	1	L	10	1.0E-04	--	--	--	Lungmen
CCF-BL-R-200	c			2.0E-04	These events are saphire "compound events" (compound of CCF factors and independent failure probabilities). The uncertainty is calculated by Saphire from the uncertainties on the CCF factors and on the independent failure probabilities. The values presented here are "double CCFs" events.			
CCF-BL-R-24	c			2.4E-05				
CCF-BL-ST	c			1.0E-04				
CCF-CP-OP	c			1.0E-04				
CCF-CPSTO-200	c			4.0E-06				
CCF-CPSTO-24	c			4.8E-07				
CCF-CV-OP	c			2.7E-06				
CCF-CVSTO-200	c			2.0E-06				
CCF-CVSTO-24	c			2.4E-07				
CCF-DIES-200	c			2.8E-02				
CCF-DIES-24	c			4.1E-03				
CCF-DIES-ST	c			1.0E-03				
CCF-ELM-R-200	c			1.0E-04				
CCF-ELM-R-24	c			1.2E-05				
CCF-ELM-ST	c			3.0E-05				
CCF-HX-1	c			5.0E-08				
CCF-HX-200	c			1.0E-05				
CCF-HX-24	c			1.2E-06				
CCF-PASS-W-1H	c			1.0E-07				
CCF-PASS-W-200	c			1.0E-07				
CCF-PASS-W-24H	c			1.0E-07				
CCF-PUMP-1H	c			2.0E-04				
CCF-PUMP-200H	c			5.0E-05				
CCF-PUMP-24H	c			6.0E-06				
CCF-STBY-BLOWER	c			1.0E-04				
CCF-TRANSM-DC-1H	1	L	10	1.0E-05	--	- -	- -	Lungmen
CCF-TRANSM-DC-200H	1	L	10	5.0E-06	--	- -	- -	AP1000
CCF-TRANSM-DC-24H	1	L	10	5.0E-07	--	- -	- -	AP1000
PASSIVE-START	1	L	30	1.0E-02	--	- -	- -	S (see Part 4.2.3)
PASSIVE-STEADY-200H	1	L	30	1.0E-07	--	- -	- -	
PASSIVE-STEADY-24H	1	L	30	1.0E-08	--	- -	- -	

Table B-2 (continued 2): Failure data and sources (CCFs)

B.2 Discussion of data used

Check-valve:

During normal plant operation, each loop is closed by a passive check-valve (CV). The CV is kept in the closed position by the same pressure difference as that existing between the inlet and the outlet of the core. Once the reactor is tripped, this pressure drop is lost so that the CV opens under a combination of gravitational force and of the pressure created by the flow due to the blower. The coolant can then flow to cool the core.

Various sources give the failure of a CV to open, but none relies on data specific to gas reactors.[xxvi] The generic failure probability for opening (found for example in Wash-1400 or AP-1000) is 10^{-4}.[xxvii] It seems adapted to take the generic value for the active flow conditions, but it may be too optimistic for the passive flow case. Therefore, in order to allow for more accuracy and flexibility in the PRA, we distinguish between the failure of the CV to open under active flow, and its failure under passive flow only, that we will note CP failure.

Some PRAs also consider a "failure of the CV to stay open". It is included here and we take the AP-1000 values.

The CV will have to be especially designed for the GFR. Therefore, although we think that generic values are justified at this stage of the design, there are still high uncertainties on the reliability that will finally be obtained. The sensitivity analysis in Part 4.4.2 aims at giving reliability goals.

[xxvi] P. De Laquil faced the same problem in his complete PRA of the GA GCFR in 1976. He based his estimation of the valve reliability on Wash-1400 generic values for the failure to open and for the CCF factors. De Laquil, P., "An accident probability analysis and design evaluation of the gas-cooled fast breeder reactor demonstration plant", Cambridge, Massachusetts, MIT, Ph.D. Thesis, 1976.

[xxvii] Westinghouse Electric Company, "AP-1000 Probability Risk Assessment, Revision 1," Pittsburgh, PA, 2003

In order to improve CV reliability, designers will also minimize CCFs by using different designs and / or by using multiple parallel CVs in each loop. If requested, a fail-safe actuator could also be added, as considered in the 1980 GCFR GA design.[xxviii]

Check-valve under passive flow (CP):

The failure of the CV under passive flow (only limited flow from the blower due to its standby momentum) is designated under "CP failure". Failures to open or stay open are considered. The failure probabilities are derived from the generic values taken for CV failures. They are slightly (and subjectively increased) to account for the smaller force opening the check-valve (and keeping it open) under passive flow conditions.

Heatric Heat Exchanger (HCHX):

Heat exchangers are widely used in the industry. Therefore their failure modes are well understood, and hourly failure rates can be found easily (AP-1000, Lungmen PRA). Leakage is the main failure mode. On the one hand the HCHX will be of a new design, but on the other hand the Heatric company claims that they have never experienced any leak.

Balancing their higher safety record with their smaller experience, we think that the generic values are appropriate. We keep the quite high EF found in generic tables (EF=10).

Water Flow in the WBL: see end of Part 4.2.3.

Water available for WBL:

In order to function adequately, the WBL needs to get sufficient amount of water. This means that enough water must be supplied to it. The water tank where water will be stored will be big enough for a few days of cooling, and it will be checked, together with the pipes, for possible leakage. Moreover, the pipes of the WBL will be made of double piping that has a negligible risk of leakage under normal conditions. The risk of water unavailability will therefore be very low, although higher for very long mission time (i.e.

[xxviii] General Atomics, "Gas-Cooled Fast Breeder Reactor Preliminary Safety Information Document – Amendment 10", GA-10298, 1980.

200 hrs). For the CCF events, we take a water availability failure (in 2 loops) of 10^{-8} for 1 hour (EF=10), 10^{-7} for 24 hours (EF=10), and 10^{-6} for 200 hours (EF=30).

Blowers:

A blower will have to be designed to move the fluid in the SCS. Such blowers are not used in current operating US nuclear power plants, but all HTGRs had some.[xxix] However, we could not access operating reliability information.

In order to evaluate the reliability of the blower, we first use the data found on blowers (in AP-1000 and in the Lungmen nuclear power plant PRA). However, as blowers are used for ventilation in these plants, they are not as challenged as the blower in the GFR SCS (see Table B-3). In these designs, pumps are used to move the coolant. Thus, pump reliability gives additional information on what could be the blower's reliability. We therefore combine subjectively the information given by blower and pump failure rates, and we take a high EF to acknowledge the uncertainties.

[xxix] Personal conversation with MIT designer Prof. Driscoll

Source	Component	Failure type	Probability	Error Factor	Comment
AP-1000	Blower	start	6.0E-04	3	Lungmen PRA has the same values for failure to start and to run (but no CCF information was found). The CCF are generic
		CCF beta factor	1.0E-01		
		CCF double	6.0E-05		
		run (/hr)	1.0E-05	3	
		CCF beta factor	5.0E-02		
		CCF double (per hr)	5.0E-07		
AP-1000	Pump	start	2.0E-03	10	Lungmen PRA has the same values for failure to start and to run (but no CCF information was found)
		CCF beta factor	1.4E-01		
		CCF double	2.8E-04		
		run (/hr)	2.5E-05	10	
		CCF beta factor	6.2E-02		
		CCF double (per hr)	1.6E-06		

Table B-3: Data used to assess the reliability of the blower

Electric Motors:

An electric motor is needed to power each blower. Electric motors are used widely in nuclear power plants, and the ones used in the GFR will probably be common to other designs. We therefore used directly the generic values found in the AP-1000 database. The CCF factors used are the generic parameters recommended in the AP-1000 report.

Diesel generators:

Generic values have been used for the diesels. According to WASH-1400,[xxx] the failure probability of diesels following a LOOP may be higher than the generic one. Indeed, both diesel generators will have to pick up the emergency load and this single event could trip both units at a greater failure rate. Therefore we increase the diesel single failure probability from $1.4*10^{-2}$ to $5*10^{-2}$, the EF from 3 to 10, and we keep the same CCF factors. The failure probability to run is kept the same. During a given mission time, we consider that independent failures of diesels can be repaired, and we adopt a four hours

[xxx] WASH-1400 (NUREG-75/014), "Reactor Safety Study, An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," U.S. Nuclear Regulatory Commission, October 1975.

mean repair time in NUREG-1032.[xxxi] However, a simultaneous failure of both diesels would cause the active systems to fail immediately, independently of any repair possibility.

The event referred as transmission failures have been assessed using failure rate on circuit breakers. In the Lungmen power plant PRA, a failure probability of $3*10^{-4}$ is taken for the failure to close of the circuit breakers associated to one diesel. In the INEL-NRC CCF database, a beta factor of $3*10^{-2}$ was found. Thus a failure probability of 10^{-5} is taken for the failure of the transmission during the starting process of the diesels. During operation, a failure of $5*10^{-7}$ was found in AP-1000. Therefore a failure probability of $5*10^{-7}$ and $5*10^{-6}$ is taken for the CCF during respectively 24 and 200 hours.

Batteries:

Batteries are needed to provide DC power for instrumentation and active components control. Three batteries will be used, each capable of providing 100% of the emergency needs. In the current design it is not considered that AC power can be provided through a DC-AC invertor. Therefore, if diesels fail, then the active system fails and it does not matter for the SCS whether DC power is available or not.

The main contributors for DC power failure are battery CCF events. There probability has been found in Lungmen PRA. It is found that batteries will not be important risk contributors with this design. Concerning electrical transmission failures, the same values than for diesels are used.

Pump:

A pump will be used in each WBL to bring additional safety to the passive system (see Part 4.4.1). Generic data from AP-1000 PRA (same than from Lungmen PRA) are taken. It is important to specify that the pumps that will be used will not have an active seal, and therefore will not be subjected to pump seal LOCAs. In case of station blackout, it will be possible to power them with a special independent back-up battery.

[xxxi] U.S. Nuclear Regulatory Commission, 1988. Evaluation Of Station Blackout Accidents At Nuclear Power Plants, NUREG-1032. Washington, D.C.

B.3 Importance measures

Importance measures are given in Table B-4 (ranked by Fussell-Vesely importance) and in Table B-5 (ranked by RIR).

	Event Name	Probability	Fussell-Vesely Importance	Risk Reduction Ratio	Risk Increase Ratio
1	CCF-CV-OP	2.7E-06	5.6E-01	2.3E+00	2.1E+05
2	CCF-HX-24	1.2E-06	2.5E-01	1.3E+00	2.1E+05
3	CCF-CVSTO-24	2.4E-07	5.0E-02	1.1E+00	2.1E+05
4	CCF-CP-OP	1.0E-04	4.6E-02	1.0E+00	4.6E+02
5	RECOVW_1	8.0E-01	3.9E-02	1.0E+00	1.0E+00
6	RECOVW_24	1.6E-02	3.7E-02	1.0E+00	3.3E+00
7	CCF-HX-200	1.0E-05	2.8E-02	1.0E+00	2.8E+03
8	CCF-DIES-ST	1.0E-03	2.2E-02	1.0E+00	2.3E+01
9	WATER-AVAIL-24	1.0E-07	2.1E-02	1.0E+00	2.1E+05
10	RX-TRIP	1.0E-07	2.1E-02	1.0E+00	2.1E+05
11	ST-AND-LOAD-DIES-2	5.0E-02	1.1E-02	1.0E+00	1.2E+00
12	ST-AND-LOAD-DIES-1	5.0E-02	1.1E-02	1.0E+00	1.2E+00
13	DIES-2-UNAV	1.0E-02	1.1E-02	1.0E+00	2.1E+00
14	DIES-1-UNAV	1.0E-02	1.1E-02	1.0E+00	2.1E+00
15	CCF-HX-1	5.0E-08	1.0E-02	1.0E+00	2.1E+05
16	CCF-CVSTO-200	2.0E-06	5.5E-03	1.0E+00	2.8E+03
17	WATER-AVAIL-200	1.0E-06	2.8E-03	1.0E+00	2.8E+03
18	CCF-BL-ST	1.0E-04	2.1E-03	1.0E+00	2.2E+01
19	WATER-AVAIL-1H	1.0E-08	2.1E-03	1.0E+00	2.1E+05
20	CCF-DIES-24	4.1E-03	1.5E-03	1.0E+00	1.4E+00
21	CCF-DIES-200	2.8E-02	1.3E-03	1.0E+00	1.0E+00
22	CCF-BATT-1H	5.0E-05	1.1E-03	1.0E+00	2.3E+01
23	CCF-TRANSM-DC-1H	5.0E-05	1.1E-03	1.0E+00	2.3E+01
24	SCS-2-CV-OPEN	1.0E-04	6.6E-04	1.0E+00	7.6E+00
25	SCS-1-CV-OPEN	1.0E-04	6.6E-04	1.0E+00	7.6E+00
26	SCS-3-CV-OPEN	1.0E-04	6.6E-04	1.0E+00	7.6E+00
27	CCF-ELM-ST	3.0E-05	6.3E-04	1.0E+00	2.2E+01
28	LOOP-2-UNAV	1.0E-05	5.7E-04	1.0E+00	5.8E+01
29	LOOP-3-UNAV	1.0E-05	5.7E-04	1.0E+00	5.8E+01
30	LOOP-1-UNAV	1.0E-05	5.7E-04	1.0E+00	5.8E+01
31	PASSIVE-START	1.0E-02	5.1E-04	1.0E+00	1.1E+00
32	CCF-CPSTO-24	4.8E-07	4.9E-04	1.0E+00	1.0E+03
33	CCF-STBY-BLOWER	1.0E-04	4.6E-04	1.0E+00	5.6E+00
34	CCF-CPSTO-200	4.0E-06	3.3E-04	1.0E+00	8.4E+01

Table B-4: Importance Measures Report – ranked by Fussell-Vesely importance value

Generally, only events with a FV importance higher than 10^{-3} are considered in the sensitivity analyses.

	Event Name	Probability	Fussell-Vesely Importance	Risk Reduction Ratio	Risk Increase Ratio
1	CCF-CVSTO-24	2.4E-07	5.0E-02	1.1E+00	2.1E+05
2	WATER-AVAIL-24	1.0E-07	2.1E-02	1.0E+00	2.1E+05
3	CCF-HX-24	1.2E-06	2.5E-01	1.3E+00	2.1E+05
4	CCF-CV-OP	2.7E-06	5.6E-01	2.3E+00	2.1E+05
5	CCF-HX-1	5.0E-08	1.0E-02	1.0E+00	2.1E+05
6	WATER-AVAIL-1H	1.0E-08	2.1E-03	1.0E+00	2.1E+05
7	RX-TRIP	1.0E-07	2.1E-02	1.0E+00	2.1E+05
8	WATER-AVAIL-200	1.0E-06	2.8E-03	1.0E+00	2.8E+03
9	CCF-CVSTO-200	2.0E-06	5.5E-03	1.0E+00	2.8E+03
10	CCF-HX-200	1.0E-05	2.8E-02	1.0E+00	2.8E+03
11	CCF-CPSTO-24	4.8E-07	4.9E-04	1.0E+00	1.0E+03
12	PASSIVE-STEADY-24H	1.0E-08	1.0E-05	1.0E+00	1.0E+03
13	CCF-CP-OP	1.0E-04	4.6E-02	1.0E+00	4.6E+02
14	CCF-CPSTO-200	4.0E-06	3.3E-04	1.0E+00	8.4E+01
15	PASSIVE-STEADY-200H	1.0E-07	8.3E-06	1.0E+00	8.4E+01
16	LOOP-1-UNAV	1.0E-05	5.7E-04	1.0E+00	5.8E+01
17	LOOP-3-UNAV	1.0E-05	5.7E-04	1.0E+00	5.8E+01
18	LOOP-2-UNAV	1.0E-05	5.7E-04	1.0E+00	5.8E+01
19	HCHX-3-1H	1.0E-06	4.8E-05	1.0E+00	4.9E+01
20	HCHX-2-1H	1.0E-06	4.8E-05	1.0E+00	4.9E+01
21	HCHX-1-1H	1.0E-06	4.8E-05	1.0E+00	4.9E+01
22	CCF-PASS-W-1H	1.0E-07	4.4E-06	1.0E+00	4.5E+01
23	TRANSMISSION-1	1.0E-05	2.2E-04	1.0E+00	2.3E+01
24	CCF-BATT-1H	5.0E-05	1.1E-03	1.0E+00	2.3E+01
25	CCF-TRANSM-DC-1H	5.0E-05	1.1E-03	1.0E+00	2.3E+01
26	CCF-DIES-ST	1.0E-03	2.2E-02	1.0E+00	2.3E+01
27	CCF-ELM-ST	3.0E-05	6.3E-04	1.0E+00	2.2E+01
28	CCF-BL-ST	1.0E-04	2.1E-03	1.0E+00	2.2E+01
29	SCS-3-CV-STAY-OP-24H	4.8E-06	6.8E-05	1.0E+00	1.5E+01
30	SCS-2-CV-STAY-OP-24H	4.8E-06	6.8E-05	1.0E+00	1.5E+01
31	SCS-1-CV-STAY-OP-24H	4.8E-06	6.8E-05	1.0E+00	1.5E+01
32	SCS-3-CV-OPEN	1.0E-04	6.6E-04	1.0E+00	7.6E+00
33	SCS-1-CV-OPEN	1.0E-04	6.6E-04	1.0E+00	7.6E+00
34	SCS-2-CV-OPEN	1.0E-04	6.6E-04	1.0E+00	7.6E+00
35	HCHX-2-24H	2.4E-05	1.5E-04	1.0E+00	7.2E+00
36	HCHX-1-24H	2.4E-05	1.5E-04	1.0E+00	7.2E+00
37	HCHX-3-24H	2.4E-05	1.5E-04	1.0E+00	7.2E+00
38	CCF-STBY-BLOWER	1.0E-04	4.6E-04	1.0E+00	5.6E+00
39	RECOVW_24	1.6E-02	3.7E-02	1.0E+00	3.3E+00

Table B-5: Importance Measures Report – ranked by RIR value

Generally, only events with a RIR higher than 20 are considered in the sensitivity analyses.

The importance measure tables were used to select the basic events to include in the sensitivity analysis of Part 4.4.2. The events with a RIR higher than 100 and a FV importance higher than 5% were automatically included. Then, the events with a RIR greater than 20 and the one with a FV importance 0.1% were generally included, except the following:

- Diesels, battery and transmission failure: these events are well understood (due to the extensive experience in nuclear power plants), and also they do not not have a very high FV importance,
- Blowers, electric motors: it is also believed that these failures are well understood,
- Loop unavailability events (maintenance in one SCS loop): they have a low FV importance and it is quite easy to control that their risk contribution will not increase,
- Single failures: when CCF were considered for one event, the single failure were not integrated in the sensitivity analysis,
- LOOP recovery after 1 hour: it has a very low RIR (1.039), because we consider a 24 hrs minimum mission time, even if power is recovered after one hour. Therefore an increase in this probability affects the risk very little.

The sequences with the failure of passive convection to start (in the SCS loops or in the WBLs) and the failure of the active system (standby blower or pump) have been added in the sensitivity analysis.

C. Fault trees

C.1 Onsite AC and DC Power Generation

The failure modes for the AC system are: failure to order the diesels activation, failure to start the diesels, failure to run the diesels for a given time and failure of power transmission. The FTs on "Start Onsite Power" refer to start and 1 hour functioning of onsite power.

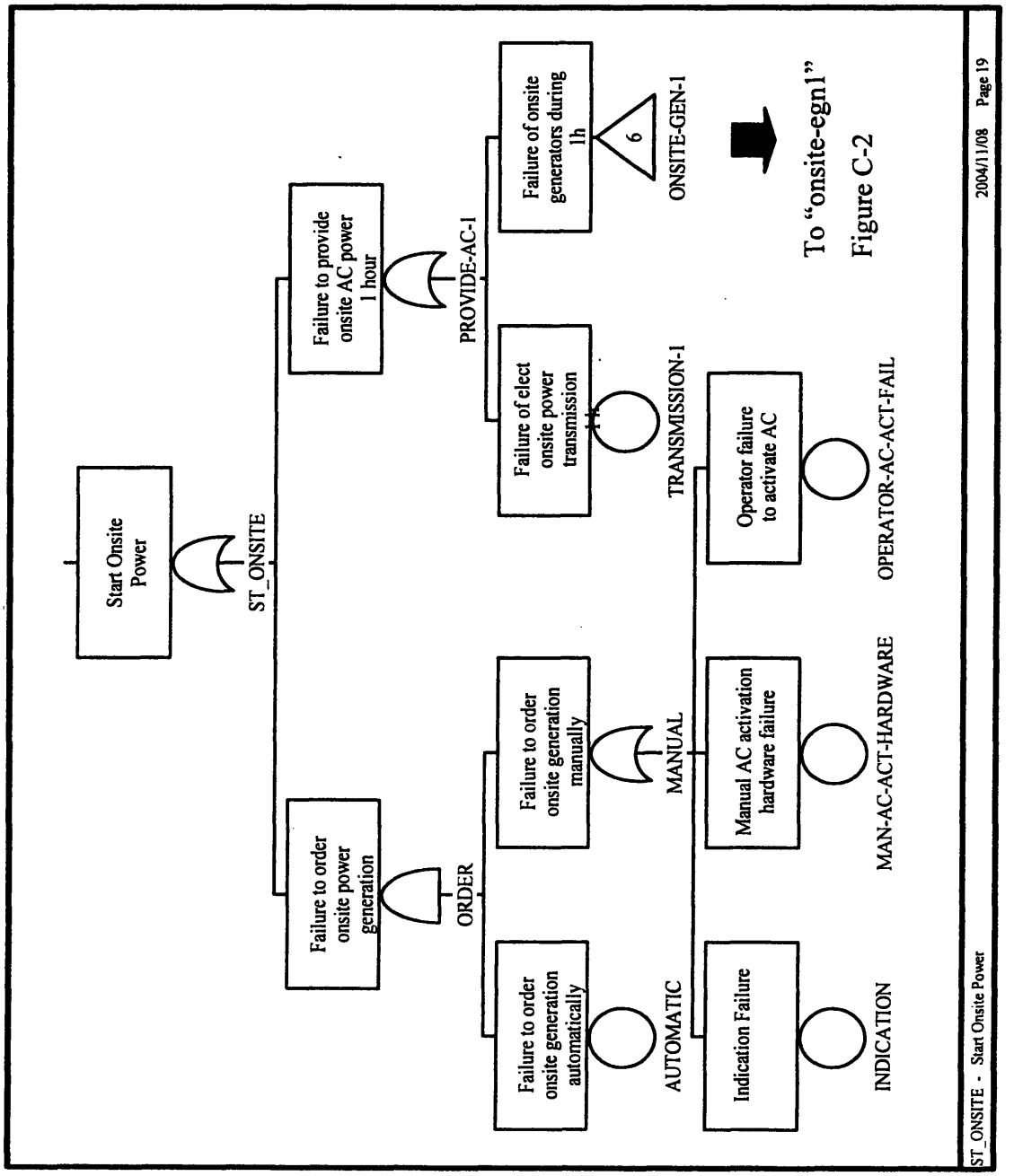


Figure C-1: Start Onsite Power (1)

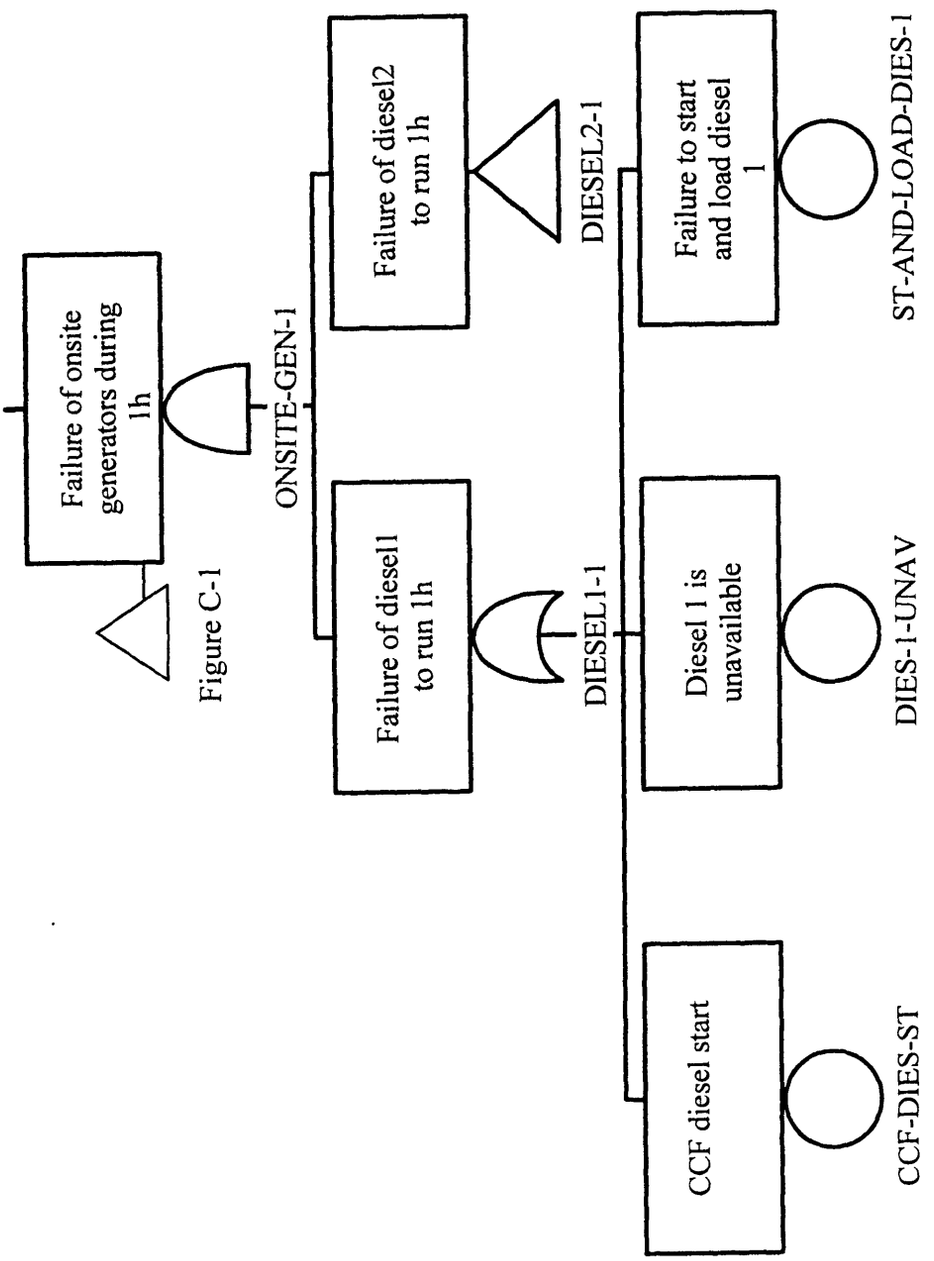


Figure C-2: Start Onsite Power (2)

The FTs for the failure to run 24 hours are represented here (failure to run 200 hrs is similar).

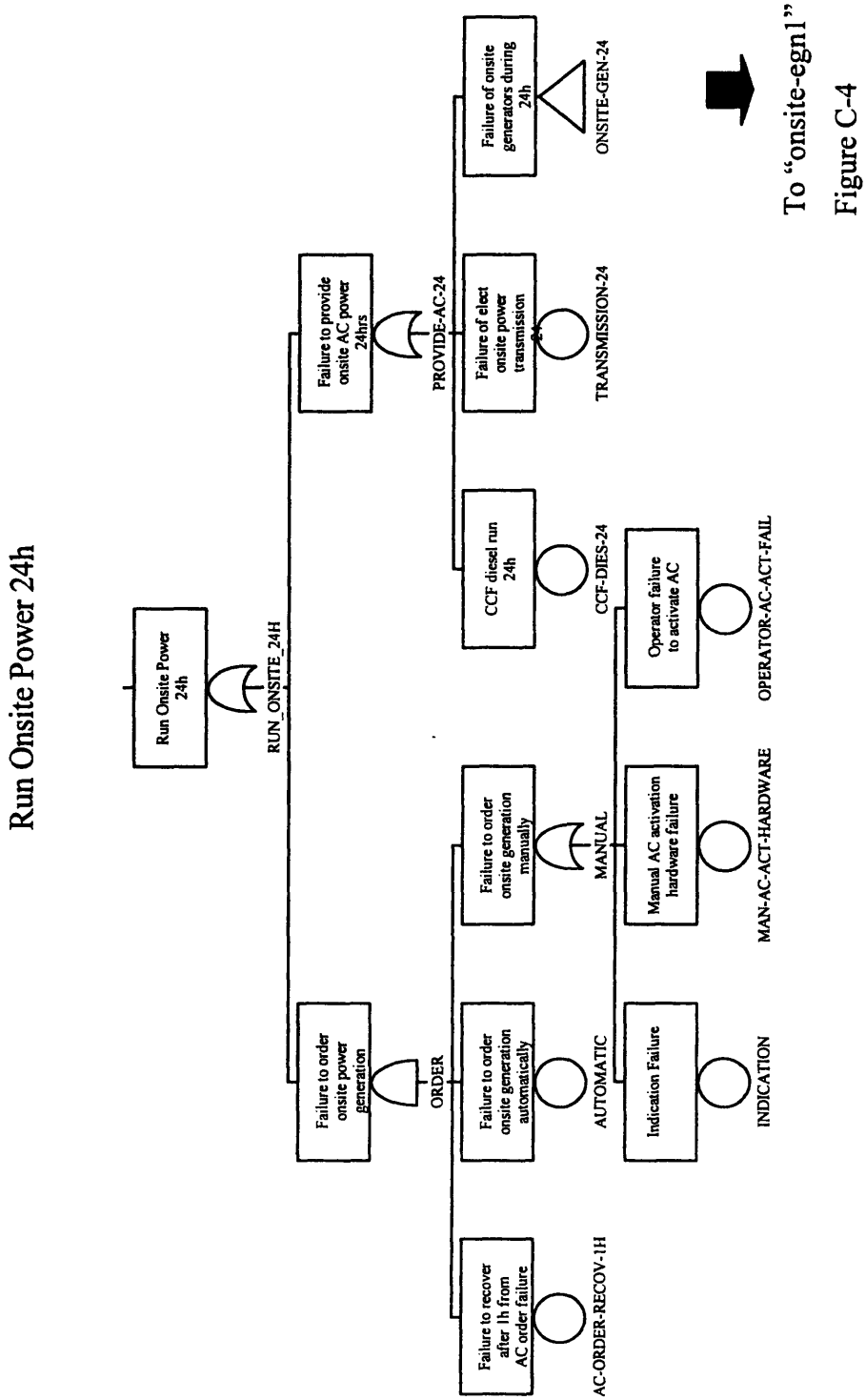


Figure C-3: Onsite Power Generation, 24 hours mission time (1)

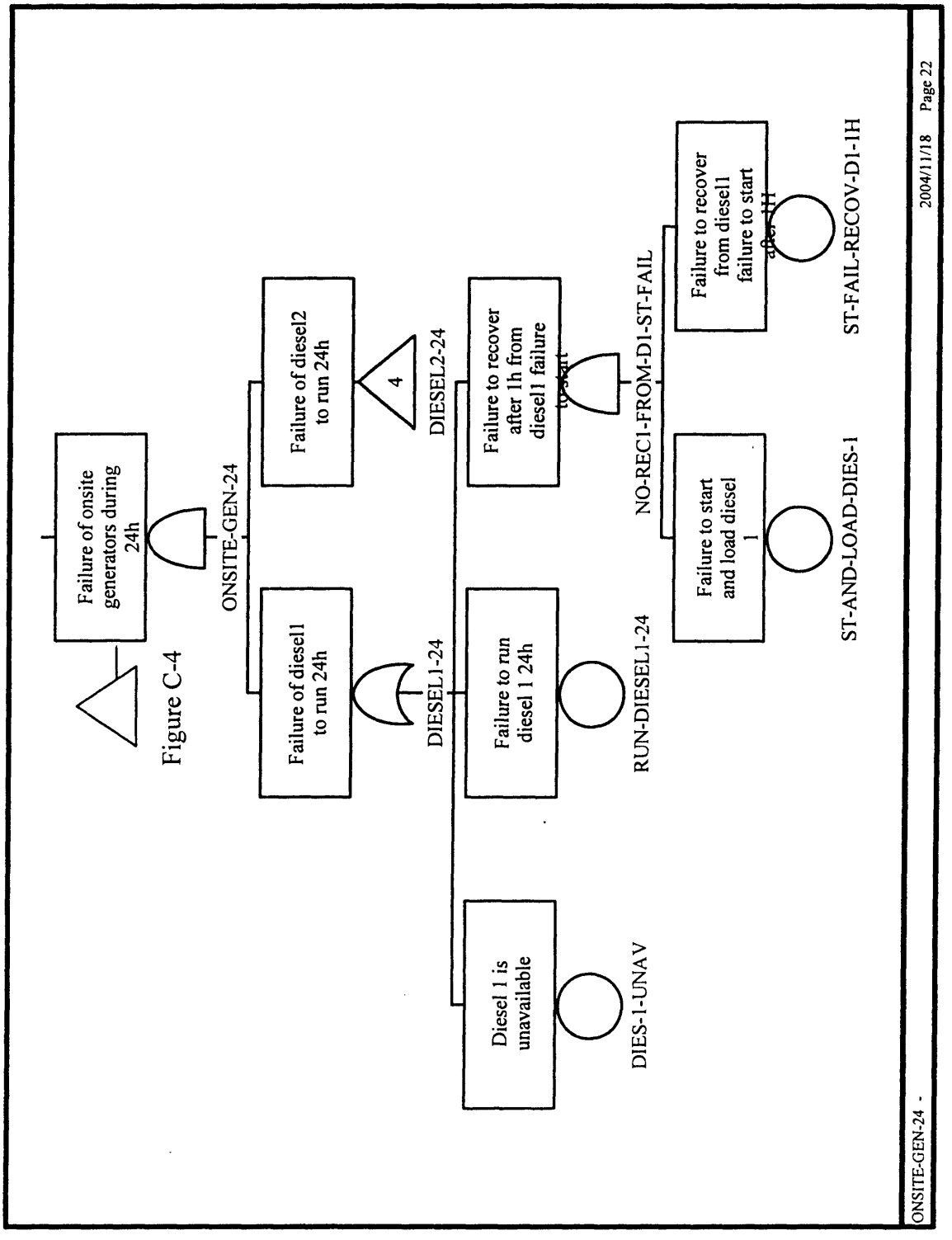


Figure C-4: Onsite Power Generation, 24 hours mission time (2)

FT for DC power during 1 hour (the trees for 24 and 200 hrs are similar).

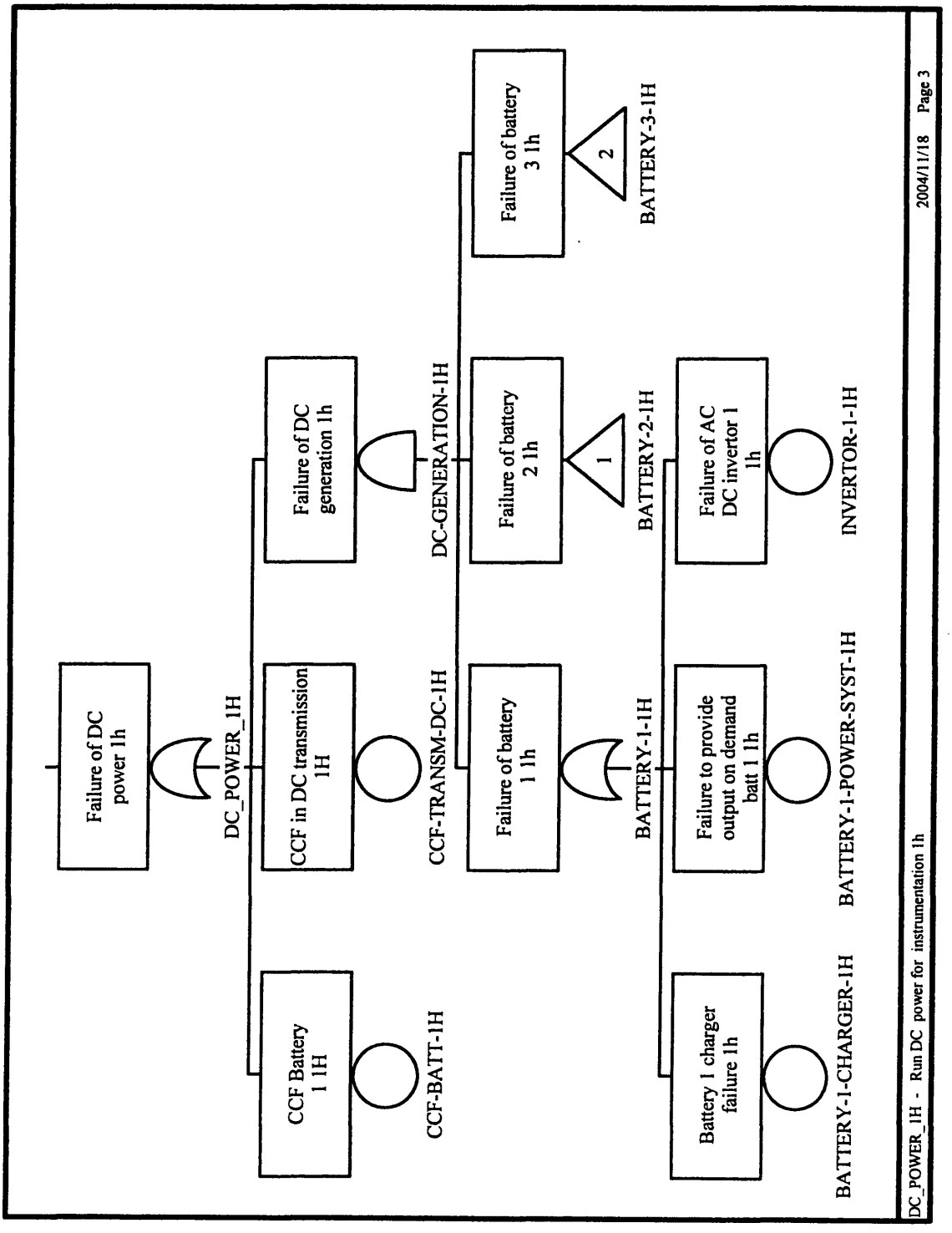


Figure C-5: DC Power Generation, 1 hour mission time

C.2 SCS Active mode

The high level failure modes are: failure to order SCS activation, and failure the SCS itself.

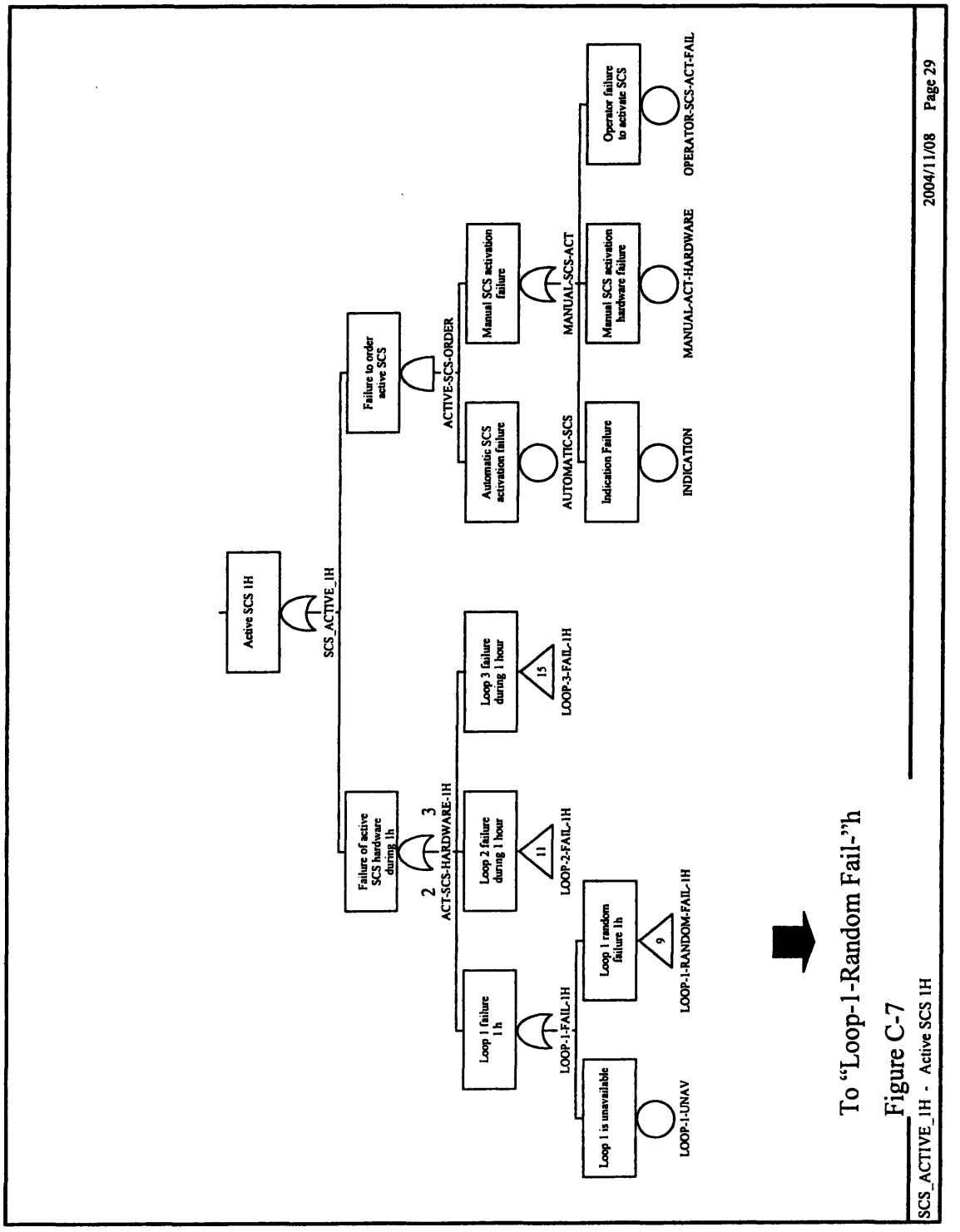


Figure C-6: SCS Active Mode, 1 hour mission time (1)

Failure modes of one SCS loop: flow blockage, failure to force the flow and failure of the heat exchange

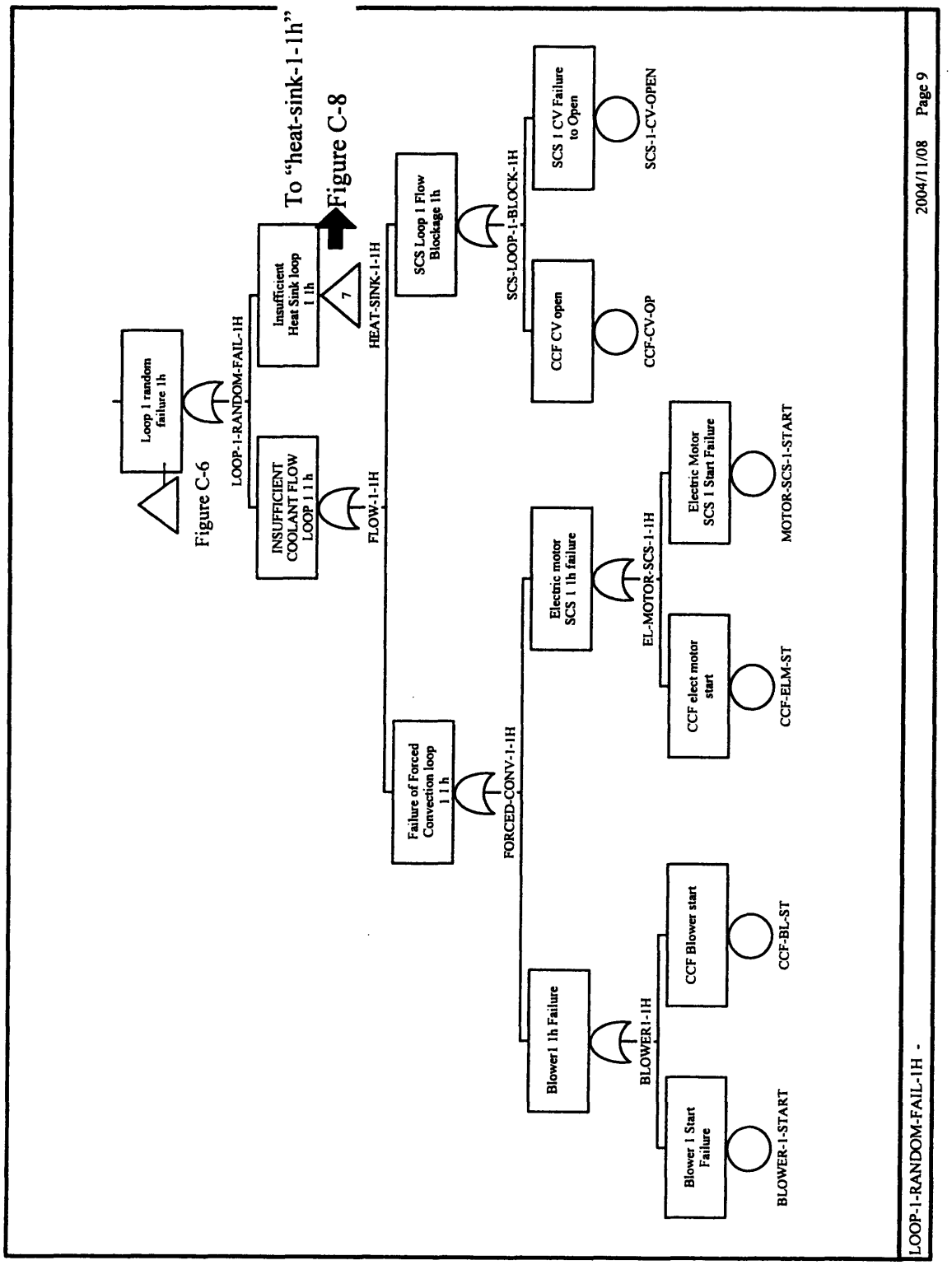


Figure C-7: SCS Active Mode, 1 hour mission time (2)

Failure modes of the heat exchange function: failure of the HCX, failure of the WBL (not enough water or not enough flow)

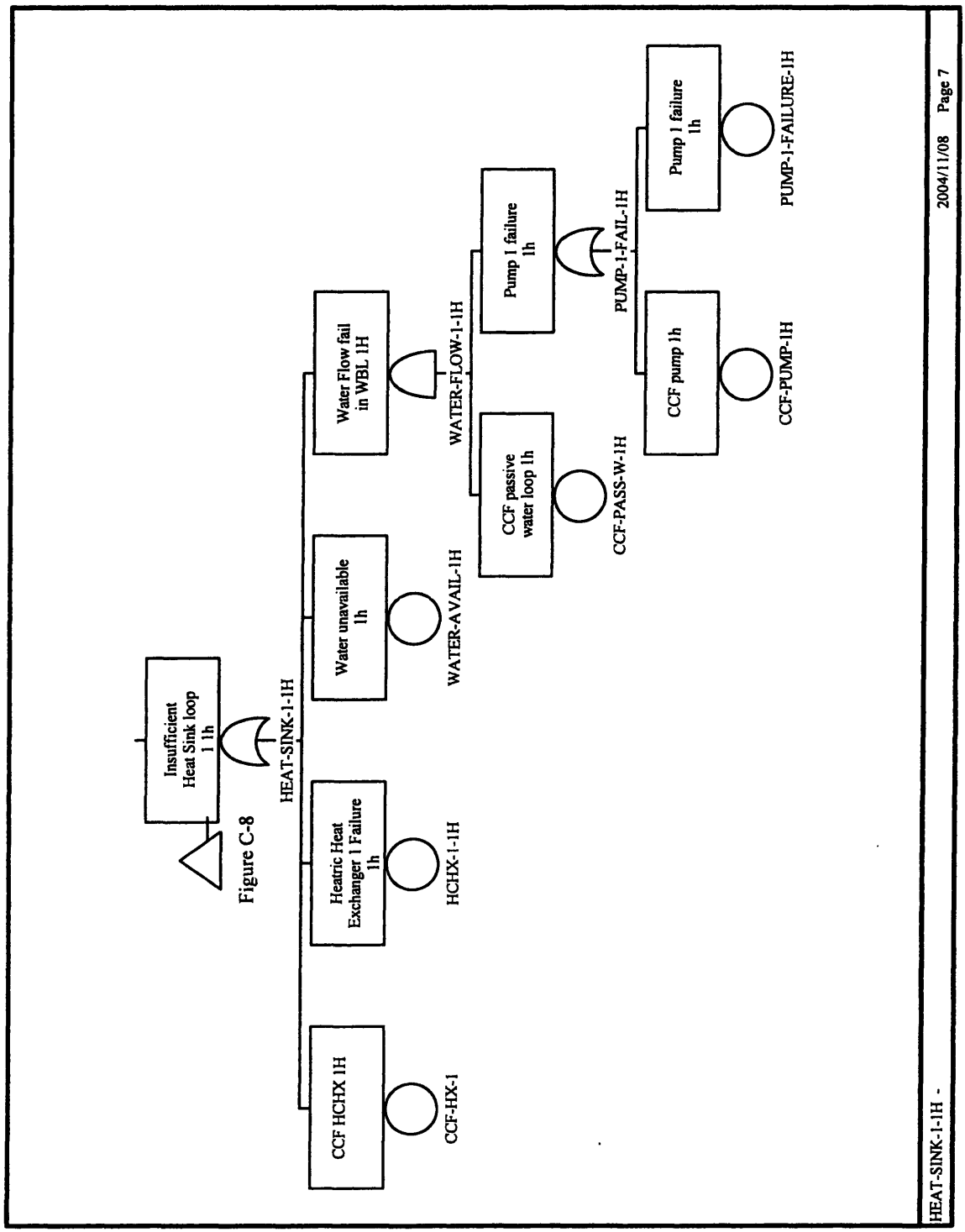


Figure C-8

Figure C-8: SCS Active Mode, 1 hour mission time (3) – heat sink functions

Similar tree for failure to operate SCS during 24 hours (failure during 200 hrs is similar).

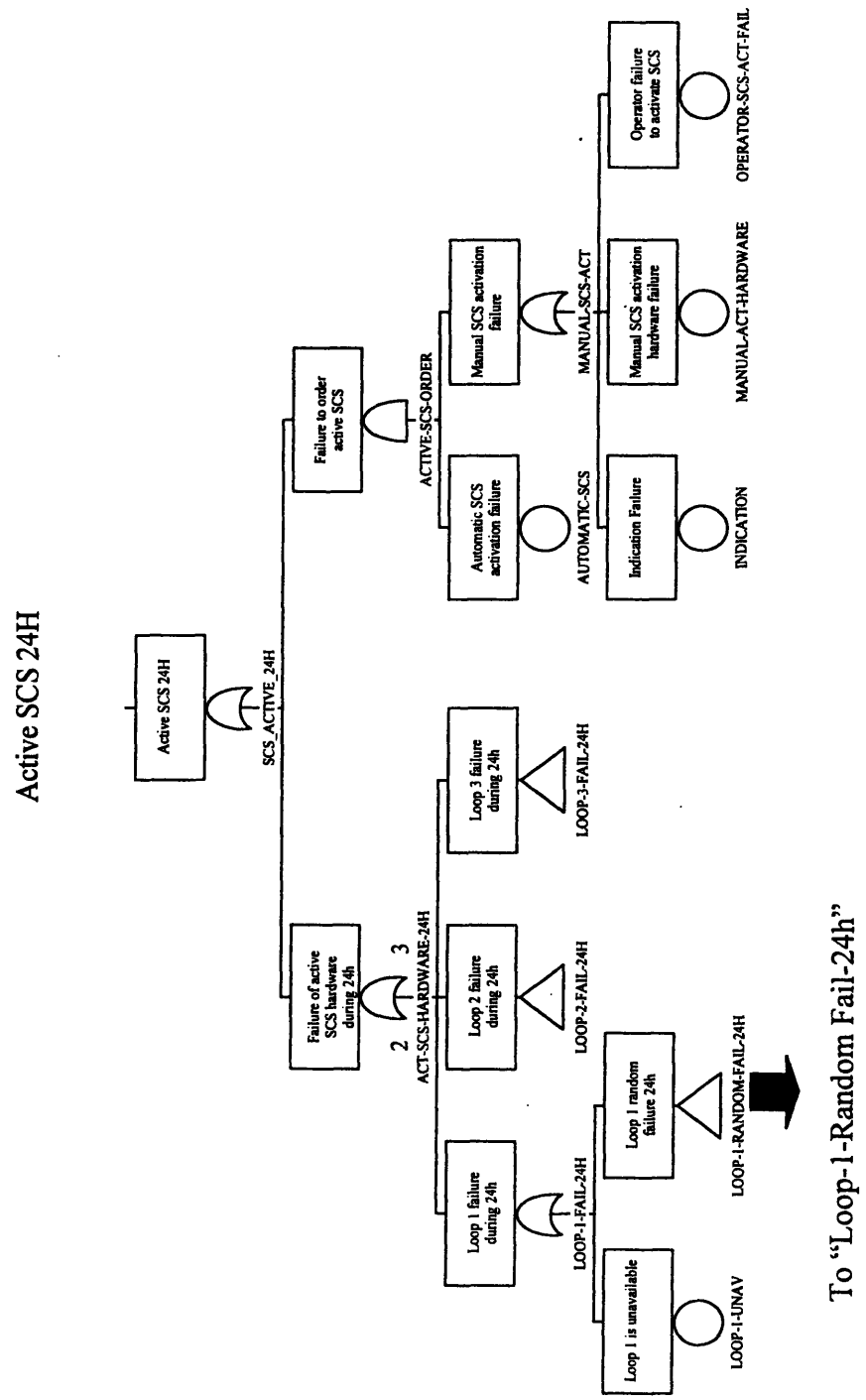


Figure C-9: SCS Active Mode, 24 hours mission time (1)

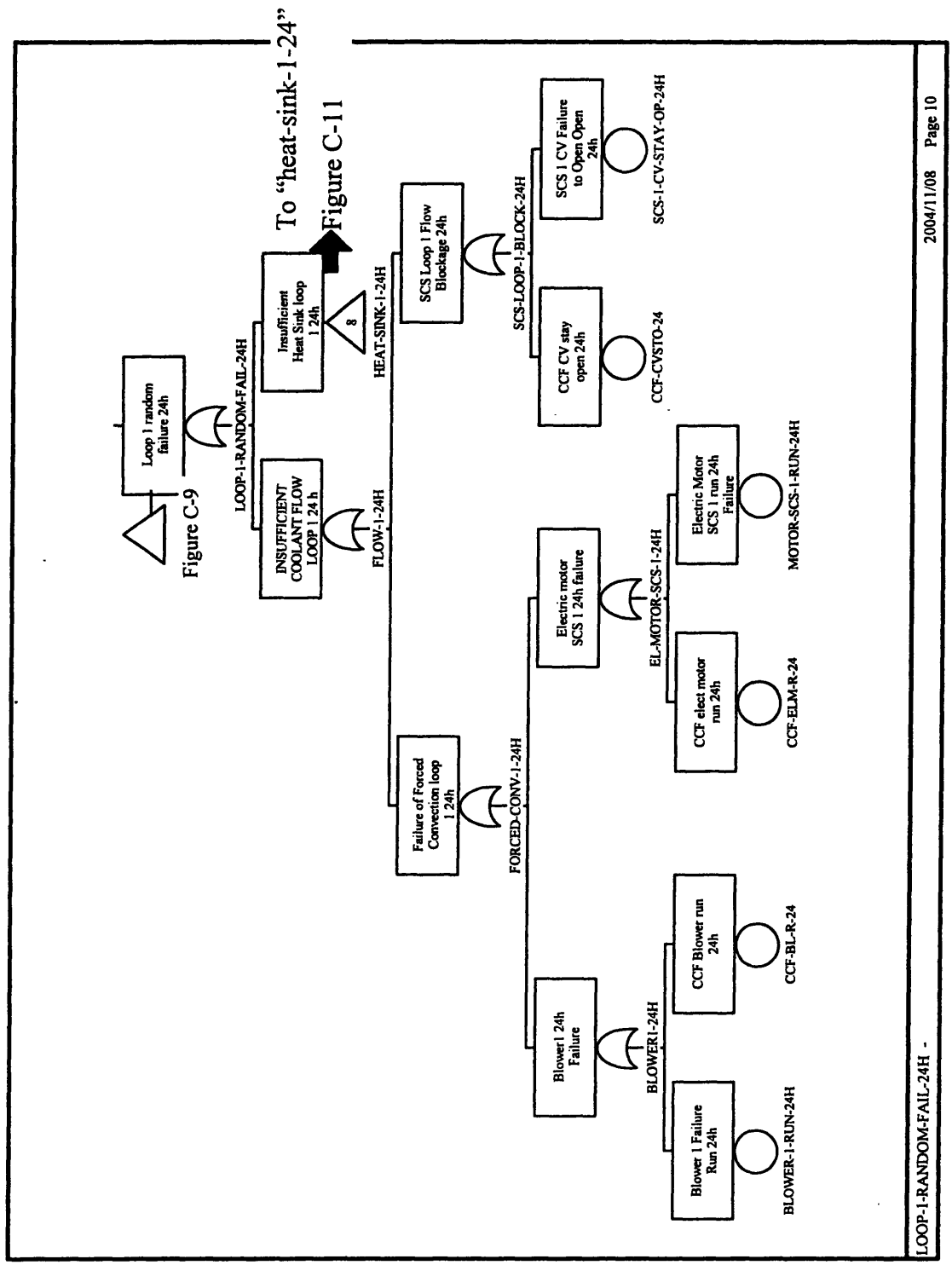


Figure C-10: SCS Active Mode, 24 hours mission time (2)

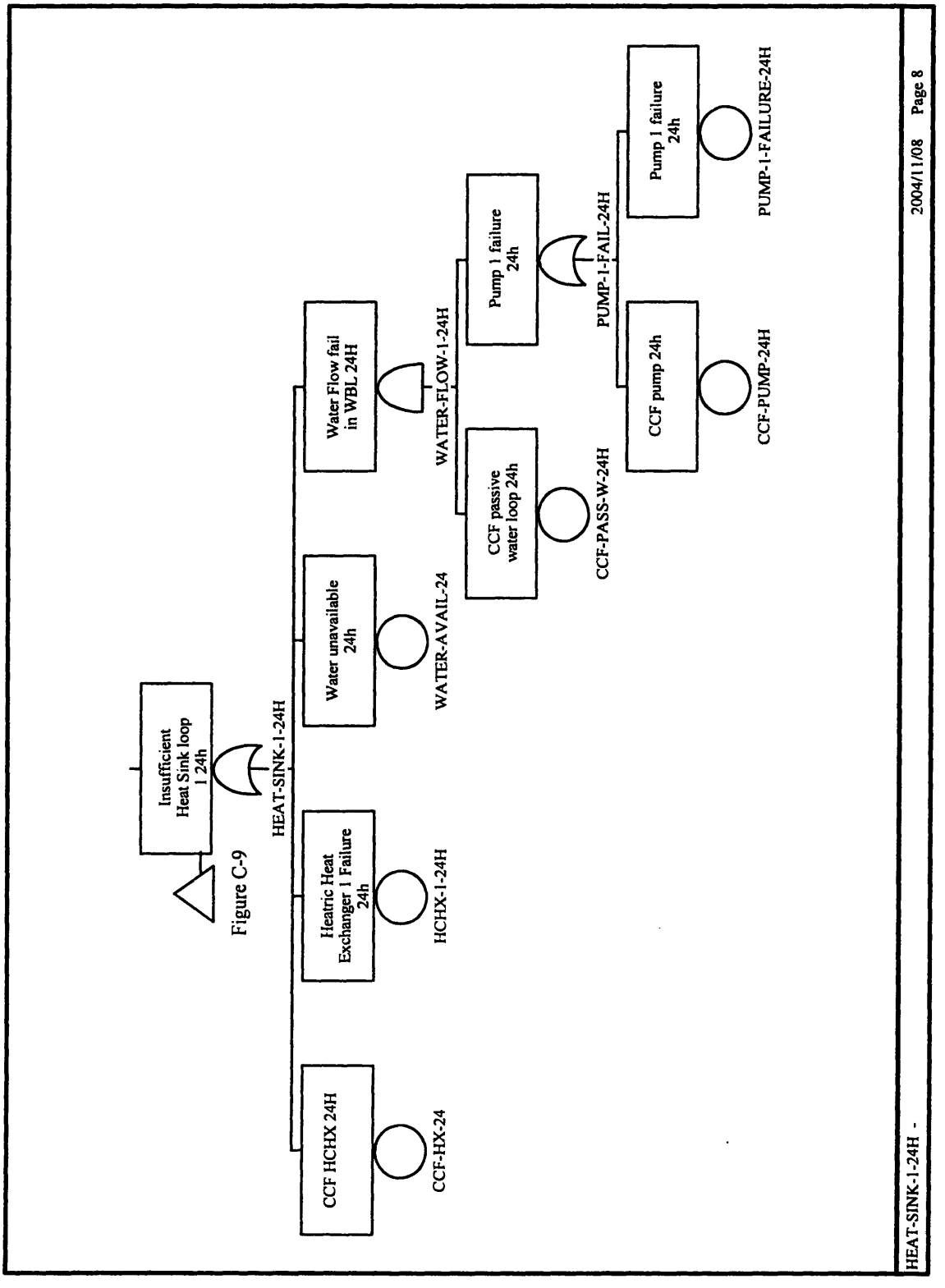


Figure C-11: SCS Active Mode, 24 hours mission time (3) – heat sink functions

C.3 SCS Passive Mode

Failure modes of passive mode: failure of the flow and failure of heat exchange.

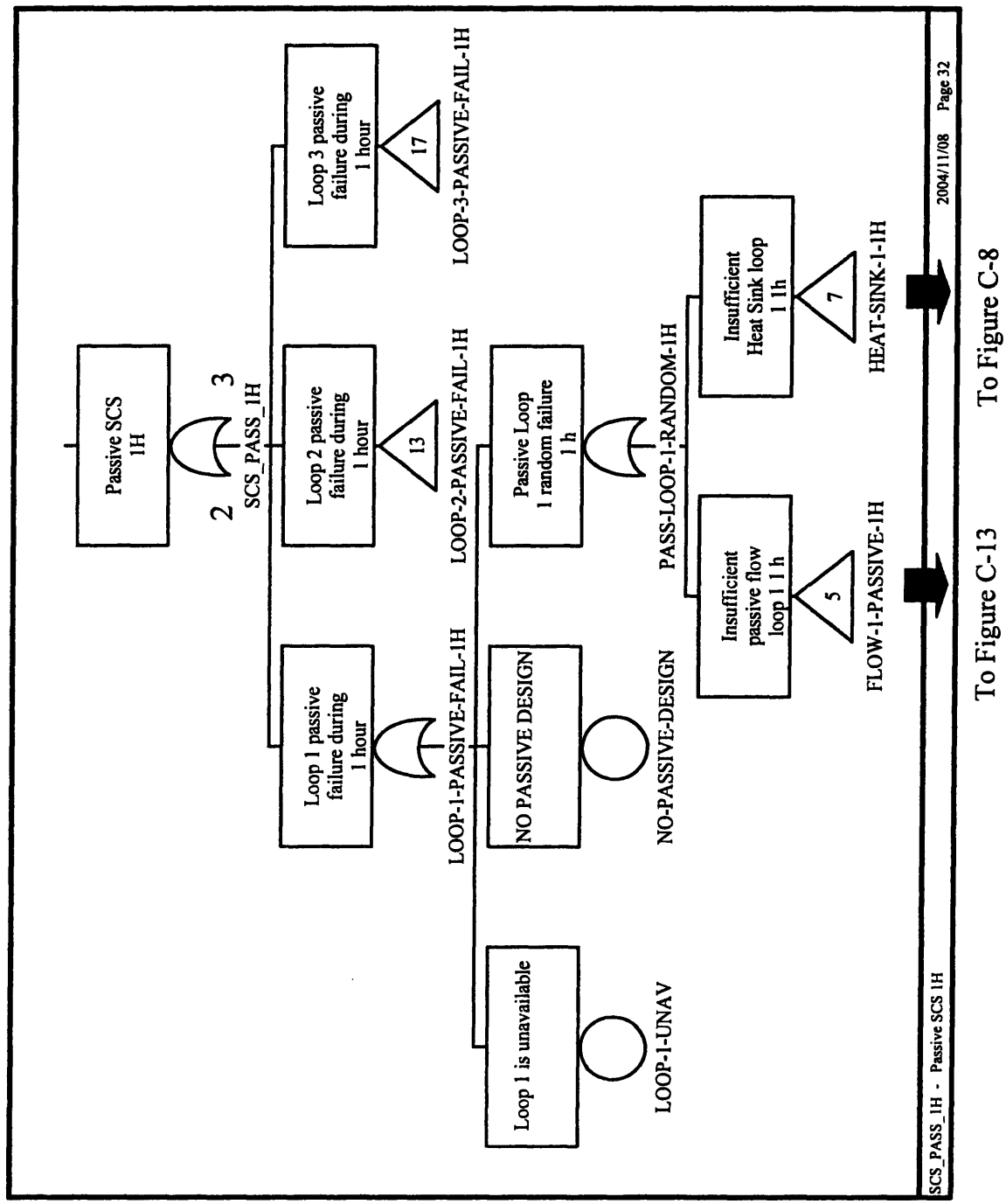


Figure C-12: SCS Passive Mode, 1 hour mission time (1)

(No passive design is an event used for modeling purpose only; to model designs with no passive convection)

The failure of the flow can be caused by a flow blockage (CV), or by the failure of the physical process of passive convection.

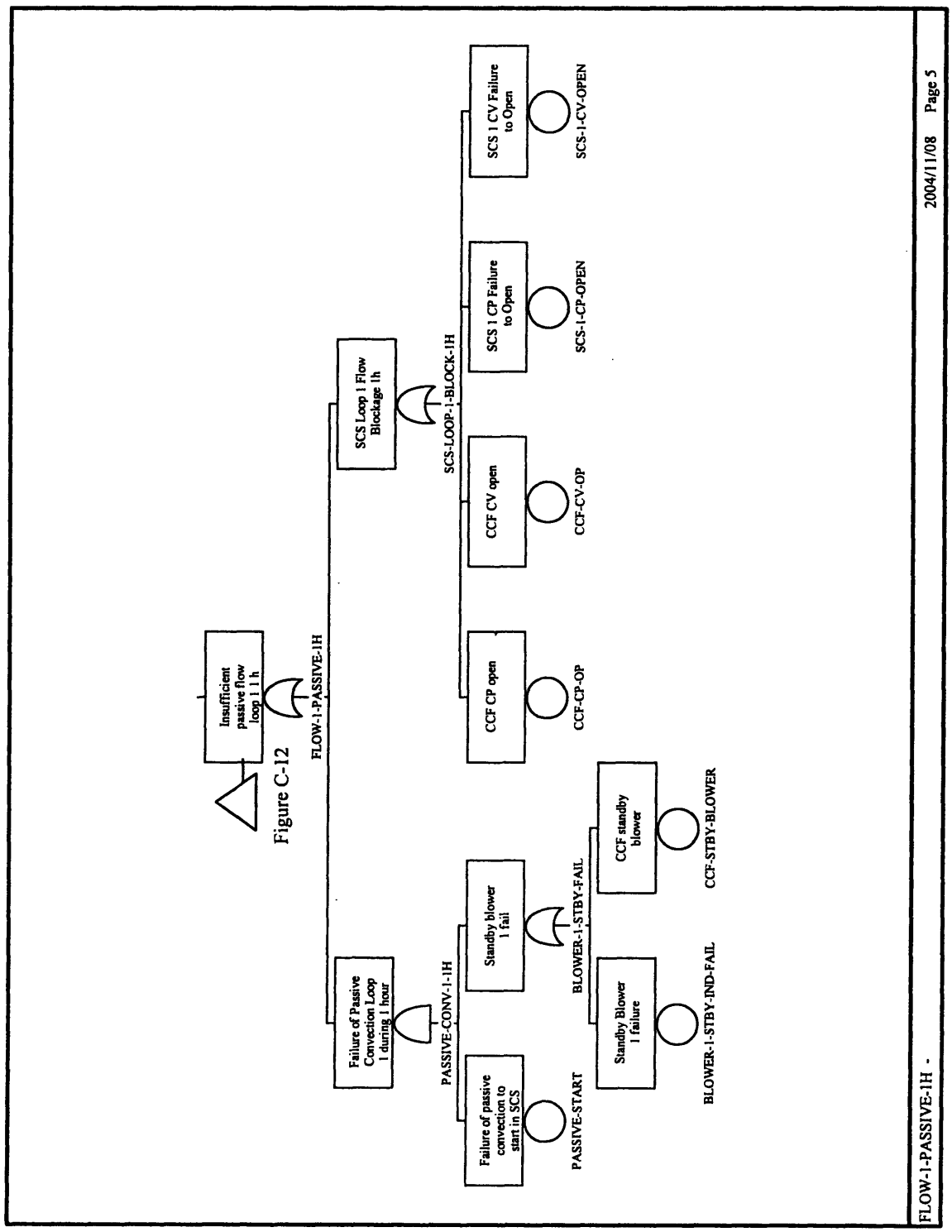


Figure C-12

Figure C-13: SCS Passive Mode, 1 hour mission time (2)

Similar tree for failure to operate 24 hours (failure during 200 hrs is similar).

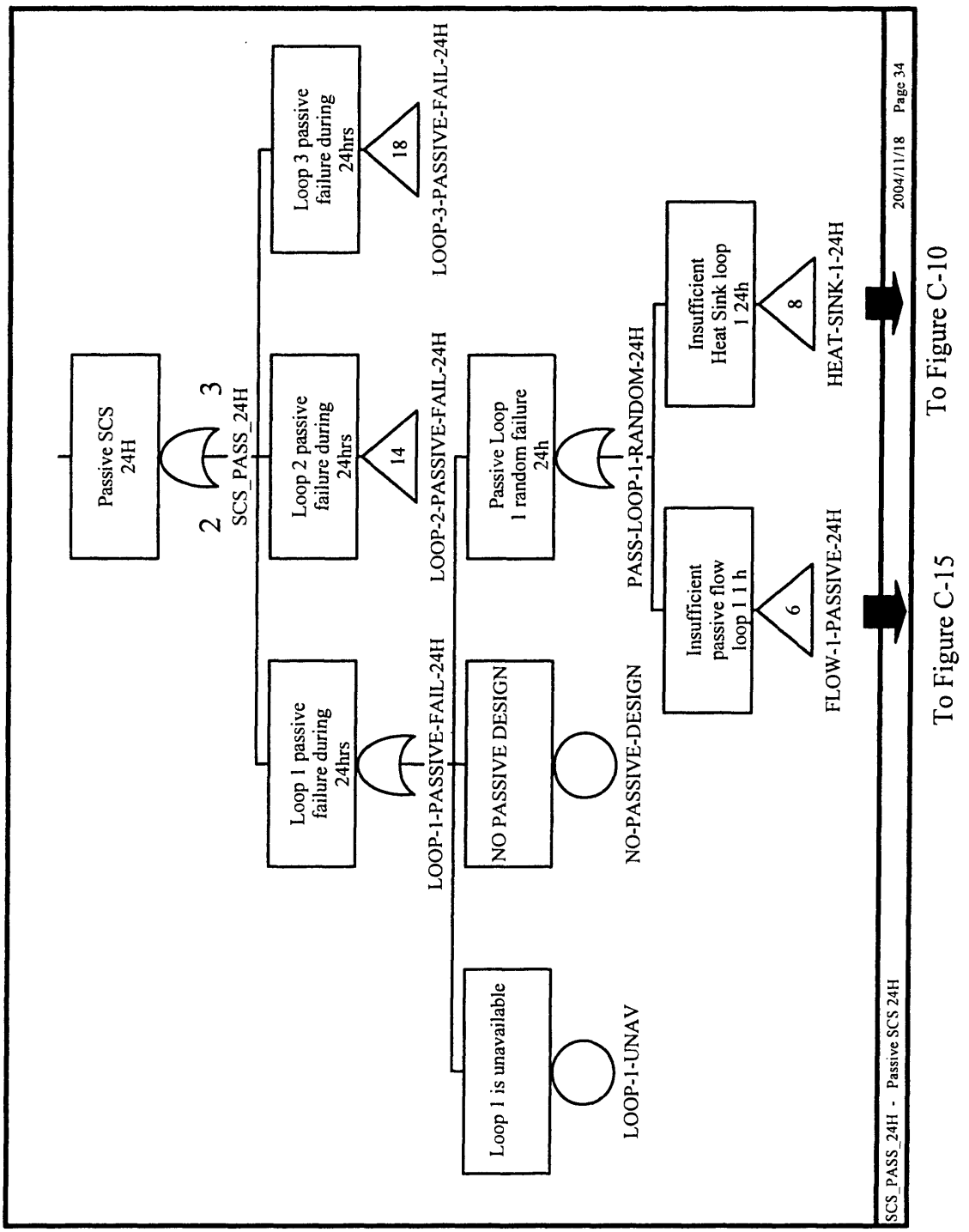


Figure C-14: SCS Passive Mode, 24 hours mission time (1)

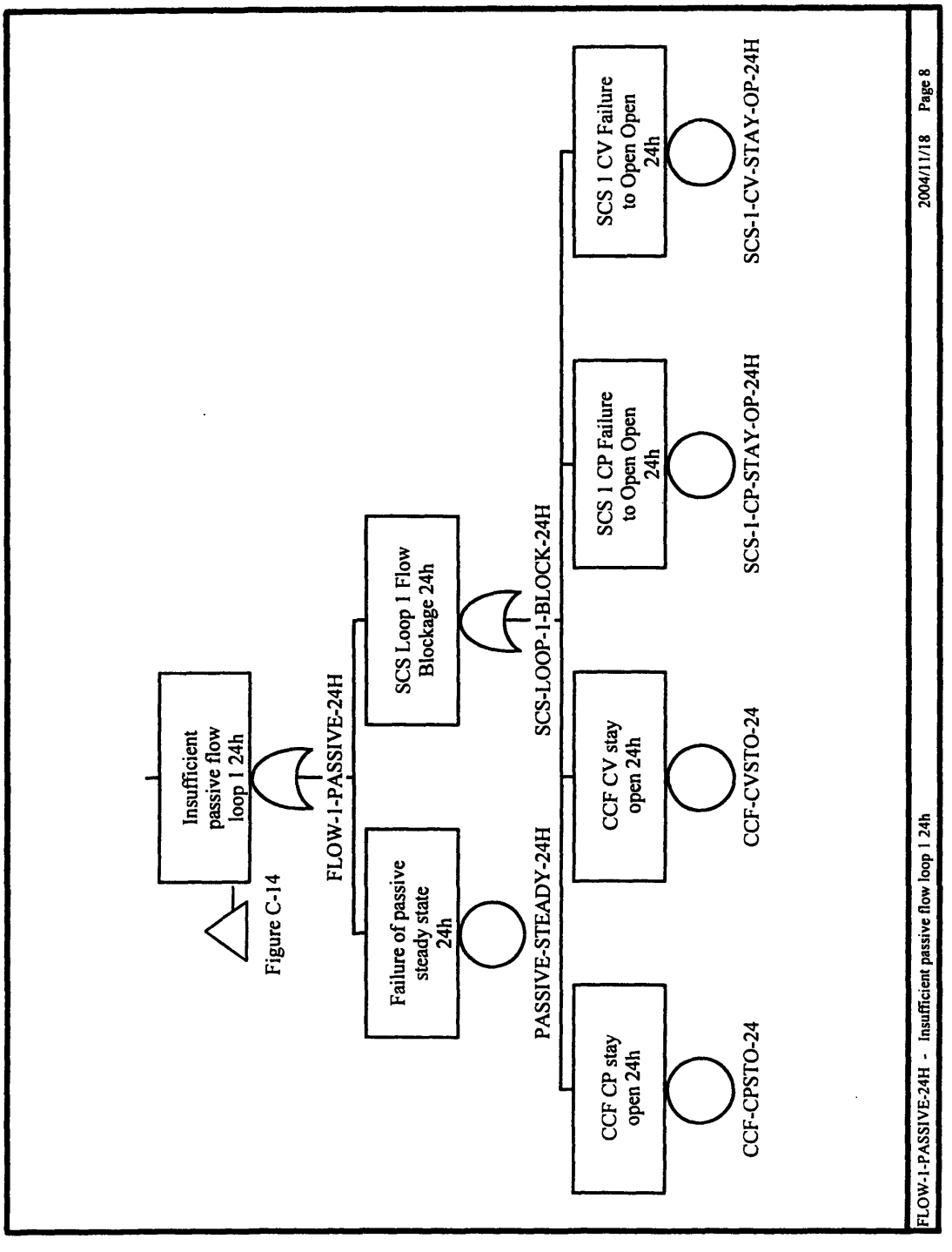


Figure C-15: SCS Passive Mode, 24 hours mission time (2)

D. Risk-Driven design: case without passive convection

This Appendice present the risk-driven process for the case where the plant is not designed to be cooled under passive convection. This case gave a basis for the designer to compare the safety advantages of the passive cooling with its additional design requirements.

In this case the bare-bones plant is constituted of two SCS loops (each capable of removing 50% of the heat) and one diesel (*case 1*). The failure probability of the system is high at this stage. Then diesels and SCS loops are progressively added. However, even with 3 diesels (*case 4*), the design does not pass under the limit of 10% of the CDF limit.

Case number	Description	Core Damage Probability		Limiting components	Next step
		Mean	95th %		
1	2*50%, one diesel	1.1E-03	2.4E-03	diesels availability	*add a diesel*
2	2*50%, **2 diesels**	1.1E-04	2.3E-04	Diesels availability, active SCS components	*add a loop*
3	**3*50%**, 2 diesels	6.6E-05	1.6E-04	diesels availability	*add a diesel*
4	3*50%, **3 diesels**	1.6E-05	4.5E-05	Diesels CCF	*???*

Table D-1: PRA guided design, with no passive cooling, case 1 to 4.

At this stage (*case 5*), the CCF of the diesels dominate the risk. We use the Multi-Greek Letters (MGL) model to quantify the CCF. With this model, adding a fourth diesel would increase very little the reliability of the AC source (improvement by 10% with a classical 0.1 delta factor). Thus, such a design relying only on active convection with diesels as the only AC power source cannot meet our reliability threshold.

Three solutions are possible for the design team:

- Argue that their diesels will be more reliable (generic reliability values have been used), because their design will be improved and the CCF limited. But the case will be especially difficult to defend, as the generic values used are supported by extensive historical data, and this CCF modeling has also been generally used. Therefore, limited tests for the GFR project are not likely to modify the trust that the NRC put into the diesels,
- Take another AC source. Micro-turbines and fuel cells engines have been proposed. The concern here is that, once again, the limited data available will make it hard to support reliability levels better than for the diesels,
- Add another AC source (like micro-turbines or fuel cells) to the diesels. Adding a redundancy with a completely different system, not likely to share the same CCF, is likely to decrease the failure probability of the AC power function of a few orders of magnitude. It seems reasonable to argue that this system can easily reach a 10^{-3} reliability, putting the core damage sequences involving loss of AC below 10^{-6} probability. Thus the AC system will not dominate the risk until such a level is reached.

To evaluate the benefits of investing research in a very reliable AC system, the risk with a **perfect** AC is calculated:

4	3*50%, **3 diesels**	1.6E-05	4.5E-05	Diesels CCF	*add other AC sources => "perfect AC"*
5	3*50%, **perfect AC**	4.9E-06	1.1E-05	SCS active components start, DC power failure	*??*

Table D-2: PRA guided design, with no passive cooling, case 4 to 5.

The 10% of the mean CDF threshold is now satisfies, but not the 10% of the 95th percentile threshold. Failure of various active SCS components keeps the risk high.

The failure of the SCS active components to start (blower and electric motor) can also be made negligible if they are kept on standby. Then the failure of the DC power dominates.

As the design of this system was not investigated by the design team, we cannot propose innovative solutions to improve it here (3 batteries are already used, adding another one would not change the risk). To investigate further what safety level could be obtained with a better DC system, we suppose it could be made almost "perfect".

5	3*50%, **perfect AC**	4.9E-06	1.1E-05	SCS active components start, DC power failure	*standby SCS active system*
6	3*50%, perfect AC, **standby active systems**	3.9E-06	8.9E-06	DC power failure	*Perfect DC*
7	3*50%, perfect AC, **perfect DC**, standby active systems	7.2E-07	2.0E-06	various active components CCF	*add a loop*
8	4*50%, perfect AC, perfect DC, standby active systems	3.3E-07	9.2E-07		

Table D-3: PRA guided design, with no passive cooling, case 5 to 8.

The failure of active components to run long mission time (especially 24 hours) now dominates the risk. The risk-driven design process was stopped here because there was no apparent solution to decrease the risk more, and the safety level achieved was good.

The conclusion from this simulation is that licensing without passive cooling will be difficult, but possible. The key will be in finding AC power sources that are reliable enough. A very reliable DC system would also have to be investigated.