A Unified Risk-Informed Framework to assess the proliferation risk and license the Proliferation Performance of Nuclear Energy Systems

by

Edoardo Cavalieri d'Oro

MS, Nuclear Engineering (2007) Massachusetts Institute o f Technology

Laurea, Nuclear Engineering (2002) Politecnico di Milano

SUBMITTED TO THE SYSTEM DESIGN AND MANAGEMENT PROGRAM

IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE DEGREE OF

MASTER OF SCIENCE IN ENGINEERING AND MANAGEMENT

AT THE MASSACHUSETTS INSTITUTE OF TECHNOLOGY

May 7, 2011

Signature of Author ....

Edoardo Cavalieri d'Oro

System Design and Management program

May 7, 2011

Certified by ....

George Apostolakis

Professor of Nuclear Science and Engineering and Professor of Engineering Systems

Thesis Supervisor

Certified by ....

Michael W. Golay

Professor of Nuclear Science and Engineering

Thesis reader

Accepted by ....

Pat Hale

Director of the System Design and Management Fellows Program

A Unified Risk-Informed Framework to assess the proliferation risk and license the Proliferation Performance of Nuclear Energy Systems

by

Edoardo Cavalieri d'Oro

Submitted to the System Design and Management Program on May 7, 2011 in Partial Fulfillment of the Requirements for the Degree of Master of Science in Engineering and Management

ABSTRACT

In order to strengthen the current non-proliferation regime it is necessary to guarantee high standards of security for the sites that use, store, produce, or reprocess special nuclear materials (SNM). The current surge of interest in nuclear energy requires resolution of concerns about the appropriateness of the current nuclear non-proliferation regulatory framework for the threats challenging nuclear energy systems (NES). This is especially true also considering that the structure of the current industry is exposed to imminent significant changes such as the introduction of small modular reactors (SMR), and the adoption of nuclear power in countries with unstable political systems.

Over recent decades, countries nominally adhering to the Non-Proliferation Treaty (NPT) violated it by building concealed facilities, by manipulating the configuration of their power plants, and by diverting material from their nuclear energy research and production sites.

These events show evidence of a major paradigm shift in the area of non-proliferation, which started with the rivalry between two major opponents (each being guardian of its arsenal and technologies during the cold-war), and later reconfigured itself into the confrontation between countries hosting nuclear technologies, or networks of opponents, trying to acquire materials, knowledge and skills necessary to build a nuclear weapon.

To create an appropriate response to all the above issues, and thus to strengthen back the non-proliferation regime, while confronting the shifted paradigm of nuclear proliferation, new tools and methods for evaluating the proliferation risk associated with nuclear energy systems become necessary. In this thesis, I discuss some of the fundamental traits and assumptions of the framework I developed in order to assess the proliferation risks associated with NESs. Important decisions within the proliferation domain, can be evaluated by a systematic and holistic approach.

The high-level objective of the framework proposed here is to create a license process for the proliferation performance of NESs, and to provide a platform to assist the evaluations of the different alternatives than can be taken in order to strengthen the current non-proliferation regime.

Thesis supervisor: Dr. George Apostolakis, Professor of Nuclear Science and Engineering and Professor of Engineering Systems

ACKNOWLEDGEMENTS

"Not everything that can be counted counts, and not everything that counts can be counted" – A. Einstein

This work is a product of the project for "Risk-informed balancing of safety, non-proliferation, and economics for the sodium-cooled fast reactor" supported by the US department of energy under a NERI contract (DE-FG07-07ID14888). The views presented here are those of the authors and do not necessarily represent the views of the US department of energy.

This work could not have been possible without the guidance, support, and the knowledge of Prof. Golay and Prof. Apostolakis during these years.

I would like to acknowledge the valuable contribution and the support I received from Prof. Bertozzi, Prof. Choucri, Dr. Lanza, and Dr. Kohse.

I thanks all my SDM friends for their friendship, my girlfriend Roberta, and my sister Elena for their patience, kindly support, and love.

Last but not least, I am grateful to Pat Hale, for believing in me and making me part of this community, and Maria Brennan of the ISO office for introducing me to the SDM program and for her support over these years.

Table of Contents

List of Figures

ABBREVIATIONS

ANL: Argonne National Laboratory
GNEP: Global Nuclear Energy Partnership
IAEA: International Atomic Energy Agency
NES: Nuclear Energy System
ST/ET: Success Tree and Event Tree Method
SFR: Sodium Fast Reactor
LWR: Light Water Reactor
IFR: Integral Fast Reactor
ABTR: Advanced Burner Test Reactor
EBR-II: Sodium Fast facility, which operated in the U.S.
FUM: Fuel Unloading Machine
FHM: Fuel Handling Machine
IBC: Intra Building Cask
IBT: Intra Building Transfer Tunnel
REDAN: see note
SR: Storage Rack
NRF: Nuclear Resonance Fluorescence
ATD: Antineutrino Detection System
DA: Design Alternative
SQ: Significant Quantity
DBT: Design Basis Threat
CDF: Core Damage Frequency
LEU: Low Enriched Uranium
HUE: Highly Enriched Uranium
NWD: Nuclear Weapon Device
SNM: Special Nuclear Material
WG: Weapon Grade
MA: Minor Actinides
Pu: Plutonium
U: Uranium
Zr: Zirconium
Np: Neptunium
PR&PP: Proliferation Resistance and Physical Protection
LBE: License Basis Event
QHO: Quantitative Health Objectives
DBA: Design Basis Accident
TNF: Technology Neutral Framework
NPT: Nuclear Non-proliferation Treaty
LOCA: Loss of Coolant Accident
DoE: Department of Energy
IAEA: International Atomic Energy Agency
NRC: Nuclear Regulatory Commission
DiD: Defense in Depth
PSA: Probabilistic Safety Assessment
PRA: probabilistic risk assessment
LBAT: License Basis Acquisition Threats
MA: Material Attractiveness
LA: Location Attractiveness
HTC: Handling and Transportation Capability
PT: Primary Tactic
ST: Secondary Tactic
CEM: Competition Elementary Module
TEM: Tactic Elementary Module
T0: No tactic physical Threat
T1: Hardware Physical Threat
T2: Software Modification Threat
T3: Transmission Alteration Threat
T4: Substitution Of The Sample Threat
T5: Detector-Sample Interface Threat
T6: Human Interface Threat
3S: safeguards, security, and safety
CoK: Continuity of Knowledge
MC&A: Material Counting and Accounting
C/S: Containment and Surveillance
UM: unattended Monitoring
MBA: Material Balance Area
KMP: Key Measurement Pont
XRF= X-ray Fluorescence
PPA = Pulsed Photon Accelerator

INTRODUCTION

PREFACE

This work is a product of the project for "Risk-informed balancing of safety, non-proliferation, and economics for the sodium-cooled fast reactor" supported by the US Department of Energy (DoE) under a Nuclear Energy Research Initiative contract (DE-FG07-07ID14888).

The project lasted three years and received an extension of one year to complete the analyses and integrate them into a final report.

During this time, I have been in charge of the non-proliferation segment of the project, which I developed under the supervision of Prof. Golay and under the lead of Prof. Apostolakis.

Some of the findings, results and insights included in this thesis are part of the project's final report. The objective of the study is to use risk information to balance the evaluations of three driver performance factors for a modern nuclear power plant which are economics, safety, and non-proliferation. Specifically the study is targeted to a technology called sodium fast reactor (SFR), which embeds many, if not all, of the most interesting functions and features of modern power plants. Central to the project has been a draft of a NRC regulation, NUREG-1860, also known as the technology neutral framework due to its goal to license future generation reactors, regardless of their technology.

Regarding the non-proliferation segment of the project, the main objective has been to create a framework consistent with NUREG-1860, and in general with risk-informed regulations. Since the beginning it was clear that in order to have such a framework two key elements were required: an assessment method to calculate the non-proliferation performance of a nuclear energy system, and a policy to set what are the acceptable criteria for the non-proliferation performance.

My focus has been to develop these two key elements, consistently with safety regulations and the risk-informed approach. This thesis describes these two elements and how to spouse them in a way that the resulting framework can be used to address the proliferation performance of nuclear energy systems.

The research questions I tried to address in this study are many and wide in their nature. Key questions, and objectives for this work are reported below. I tried to answer these questions, by creating a holistic and systematic framework, and I tried to rely on concepts rather than on numbers. The framework is a first step for the solution of the proliferation problem.

- How to formalize the proliferation performance of a nuclear energy system into a risk-informed assessment?
- How to capture the entire array of the potential proliferation risks associated with the deployment of nuclear energy systems?
- How to determine acceptable criteria for non-proliferation, consistent with risk-informed analyses?

The section entitled Policy of a dual technology and the following ones, will clarify better these research questions originate from by inserting them in the framework that was envisioned to portray the proliferation control problem of nuclear facilities. The next section explores the motivations that call for an urgent resolutions of the issues discussed in this work.

MOTIVATIONS

The proliferation problem is traditionally characterized by many inter-related dimensions which include dismantling the existing fleet of nuclear weapons, preventing the diffusion of nuclear materials and information from NESs, and securing nuclear weapon arsenals. Among these dimensions, in light of the projected worldwide energy needs, protecting nuclear energy systems from the proliferation threat is candidate to become a dominant aspect of the problem. Many countries in the last five years re-wrote their energy agenda deciding to include nuclear power into their energy mix as a way to meet the energy needs forecasted for the next half of this century. However, the overall context in which the so called nuclear renaissance is expected to take place will be fundamentally different from the context which characterized the initial development of this source of energy. Relevant features include the high number of newcomers from undeveloped countries[1], the closure of nuclear fuel cycles planned by countries such as France and Japan, and the adoption of small modular nuclear power plants to meet local energy needs.

All these novelties call to address new challenges that to be solved will require to combine pure technical and economical aspects with legal and political ones. For example consider the impact into the global economic system potentially carried by the introduction of modular reactors. Compared to traditional power plants, this technology is particularly suitable for undeveloped countries because it is easier to connect to the grid system, and it can be managed in absence of matured nuclear knowledge. Its adoption on a large scale, has the potential to reconfigure the architecture of the current nuclear industry, of its current business models, and of the relationships existing between government and industry. SMRs represent

[1] Director General Yukiya Amano in his opening speech to the IAEA's 54th conference, held September 20-24 in Vienna, declared:" it is not an exaggeration to say that we entered in a new era. We expect between 10 to 25 new countries to bring off their first nuclear power plant online by 2030".

the first example of technological disruption for nuclear technology since its adoption. The introduction of modularization in other industrial sectors, as the one faced by the computer industry in the eighties[2], revolutionized the structure of their original markets. If modularization enters the nuclear sector, it would add new features relevant to proliferation, such as the decentralization of nuclear power plant installations and it would lead to the multiplication of nuclear components' suppliers.

Assuming this scenario, past paradigms for non-proliferation would not suffice to control and to mitigate the proliferation risks associated with nuclear power, and the development of new mental models and approaches will be needed. The high complexity of the new proposed technical solutions will require stakeholders and decision makers to have a wider understanding of nuclear technologies and nuclear markets. Holistic thinking and systemic approaches will be essential to deal with new technical solutions and new threats.

In the new nuclear era, the need for scientific and technical knowledge of the new nuclear threats is essential to inform policy decisions and to frame regulations capable to reduce the proliferation risks associated with NESs. The scientific foundations for such a knowledge are remarkably broad and range from nuclear physics and engineering to risk assessment and statistics, detection physics, social science and international politics[3].

---

[2] The computer industry in the eighties faced a revolution when the architecture of computers went from an entire integrated system to a modular one. At that time no one would expect that it was possible to modularize the architecture of a computer as well it was not expected that the industry had the structure to react to such a change. When few IBM designers left the company and started working on a new hard disk, IBM reacted to this threat by creating new interfaces in their motherboard and by giving economic incentives to the customers and suppliers using their products. Despite these efforts, the new hard disk succeeded and the idea of modular components entered the markets very, radically changing the nature of the PC's business.

[3] Ryukichi Imai, in a 1977 paper published on the Annals of American Academy of Political and Social Science, first discussed the need to combine political and technical knowledge to efficiently address the proliferation problem. James E. Doyle, in a book published 30 years later *(Nuclear Safeguards, Security and Nonproliferation: Achieving Security with Technology and Policy)* remarked this aspect emphasizing how the technological progress done in the last 30 years in the area of statistic modeling and detection has to be integrated into the possible set of solutions.

THE PROBLEM: POLITICS OF A DUAL TECHNOLOGY

Nuclear non-proliferation is a political objective, and key decisions in this field belong to the realm of politics. However, the challenges associated with the complexity of today's world require one to tackle the issue of non-proliferation from different perspectives. Availing myself of the expertise of specialists in various fields, I developed a framework capable of supporting decisions and of helping to identify the most valuable policies for reducing the proliferation risk associated with nuclear energy systems (NES).

Exegesis of the problem

All nuclear energy programs have the potential to degenerate into a nuclear weapon program. In other words, nuclear power is essentially a dual-use technology.

Since its discovery, the nuclear power industry has focused on the aspects of safety and economics. Today, a revitalization of nuclear power development is expected, and proliferation is truly the unsolved piece of the puzzle. Appropriate anti-proliferation policies, novel detection systems, and agreements regarding international cooperation are the enablers required to develop this source of energy sustainably.

A new framework to address new challenges

A wide range of politicians and experts in the field of nuclear proliferation agreed about the need of a new framework for proliferation control. For example in his opening speech at the IAEA on May 2007 M. ElBaradei said: "The time has come to think of a new framework for the use of nuclear energy: a framework that accounts both for the lessons that have been learned and the current reality", more recently Energy Secretary S. Chu re-stated the concept saying: "We need to build a new framework of cooperation so that countries can access peaceful power without increasing the risk of proliferation". Former Secretary of State George P. Shultz, in a speech given at MIT in 2010 said: "Central to the nuclear security project's mission is developing a new international system to manage the risks of producing fuel for nuclear power".

In parallel to these explicit requests to reframe the current terms of the non proliferation regime other politicians and new players in the proliferation arena anticipated different solutions to deal with the problem. President B. Obama on May 28 2010 said: "The NPT must be at the center of our global efforts to stop the spread of nuclear weapons around the world, while pursuing the ultimate goal of a world without them", and W. Buffett at the end of 2010 announced: "It is my pleasure to write a $50 million check, fulfilling the promise to help fund an international nuclear fuel bank". Even B. Gates proposed a solution and in a public speech intervened saying: "We are ready to test a new modular reactor; the basic idea is to create a reactor that needs only a small amount of enriched uranium to get started. This will limit the proliferation risk".

As these statements suggest, new threats, emerging technologies, and newcomers in nuclear markets, all challenge the opportunity to find solutions and to develop them coherently with today's world complexities. Framing the problem in terms of risk allows one to assess the level of performance associated with a NES in correspondence of the implementation of different fissile control mechanisms. To achieve this goal, scientific and technical knowledge ranging from nuclear physics and engineering to social science and international politics is required. If these disciplines are bound together, then the solutions can forge the connections existing between the socio-economical and legal-political aspects required to create a policy framework capable of strengthening the current proliferation regime.

Using an analogy with safety regulations, I illustrate the representation of a proliferation policy that I proposed, and the research questions that came to mind during its development.

Synopsis of the framework

The figure below shows a diagram of the policy portion of the framework I have helped to develop. Each point in the diagram represents a NES exposed to a threat. Risk is defined by the probability of realization of the threat, and by the consequences associated with it. In the case of proliferation, risk is defined by the product of the probability of a proliferator eluding all the technical and legal barriers conceived for the protection of a NES, and the consequences of such a malicious act. Since acquisition is the goal for a proliferator, the consequences are expressed in terms of amount of material potentially obtainable during a proliferation attempt.

The risk space so determined is divided into two sectors following a risk acceptability criterion; risk acceptable solutions (i.e., a NES and the proliferation barriers added to it) fall below the bold line; all other points are unacceptable, or too risky. With this representation the proliferation threats can be grouped accordingly to the amount of material acquirable; from left to right, the transition from the diversion (or theft) of material to the breaking of the non-proliferation treaty (called "break-out", or abrogation) is accompanied by a rising level of complexity (of the technical-institutional barriers applicable to protect the NES) and of organizational effort required from a proliferator willing to acquire nuclear material from the NES (i.e., diversion scenarios can be pursued by single individuals, the decision to break-out from the Nuclear Non-proliferation Treaty (NPT) is made by a state).

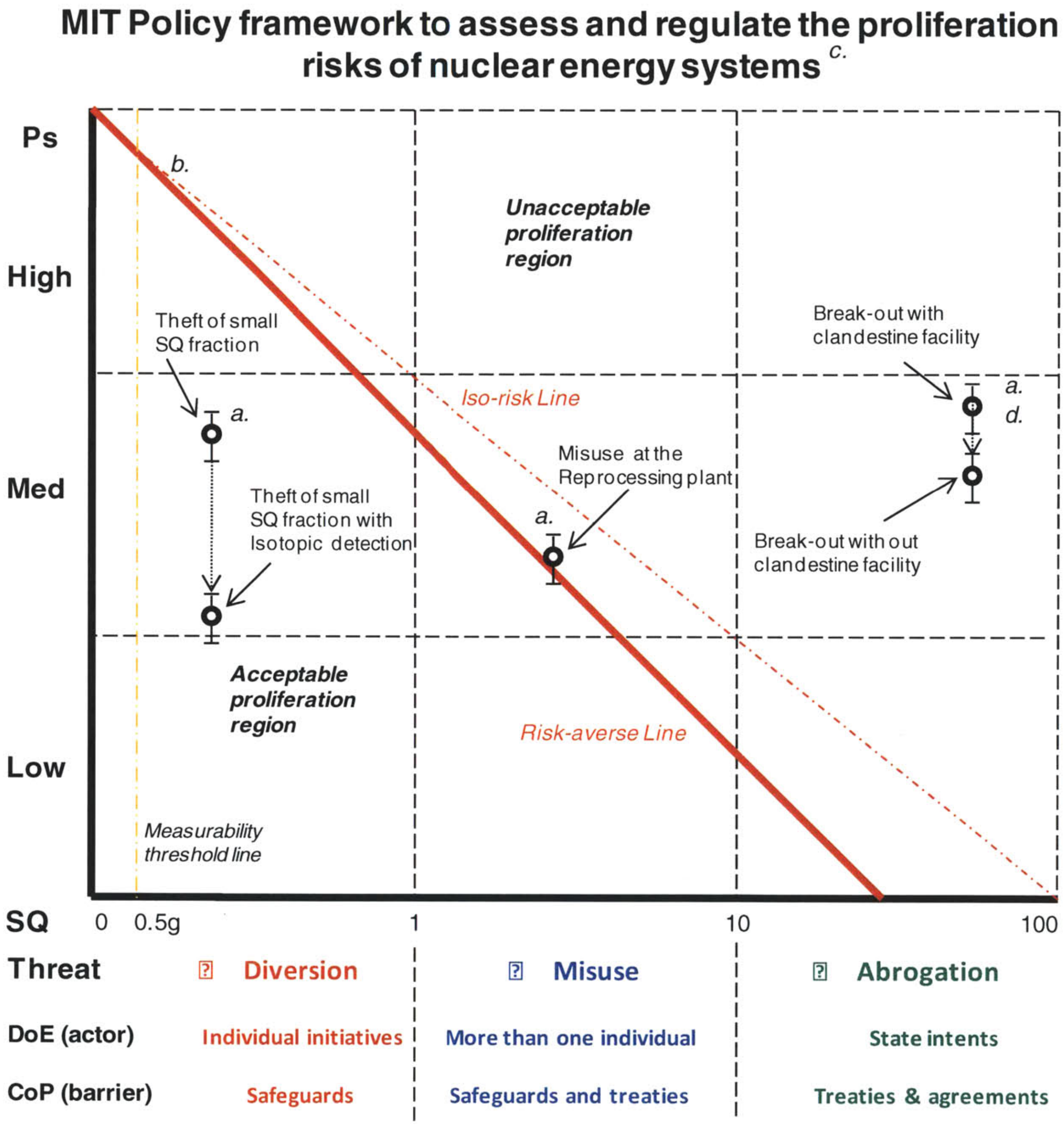


Figure 1. Probability vs. consequences space formulated to represent and limit the proliferation risk. [SQ: Significant quantity, from the IAEA definition is the approximate quantity of nuclear material needed for its use in a nuclear explosive; Ps: Success probability conditional upon attempt to acquire nuclear materials; DoE: Degree of organizational effort required to acquire special nuclear materials; CoP: Complexity of the technical-legal system empowered for the NES protection]

RESEARCH QUESTIONS

The proposed representation implicitly contains a set of relevant questions (marked in Figure 1 by lower case letters) and grouped as follows:

a. Risk Definition

The problem of evaluating the proliferation risks of a NES is more difficult than that of the safety risks. This is because the events of interest are mainly intentional or reactive human actions, and also employ systems such as those for safeguards, and institutional barriers. In this analytical framework the probability of concealed acquisition of materials from the NES provides a measure of the non-proliferation performance of a NES, including the barriers used to mitigate the risk. The performance is obtained relying upon quantitative expert judgments. In that fashion, and differently from traditional classical risk assessments, the analyses are empirically grounded in the knowledge of experts and need to be conducted via tools such as surveys and questionnaires. Relevant questions can be: What are the right methods to collect experts' opinions and how can the needed data be analyzed? How to create questions able to minimize the error in the assessment of the proliferation risk?

b. Risk Acceptance

Iso-risk and risk-averse scenario acceptance boundaries are shown in the figure. The quantification of these boundaries is not an easy decision; in the case of nuclear safety, values of acceptable probabilities in the risk space needed to be determined via a social process, requiring consensus from the society, and involving the Nuclear Regulatory Commission and the Congress. In case of proliferation, what would be the mechanism by which what is an acceptable value is determined? Would different societies have a different sense of what is the level of perceived and tolerable risk, according to the political system into which they are embedded?

c. Decisions

For the safety case in the U.S., the Nuclear Regulatory Commission licenses a nuclear reactor basing its decision upon risk information. If a given technology is considered too risky, the regulator requires the applicant to protect it further and otherwise rejects it. Let's now consider the risk acceptability line of the figure and imagine how to regulate the proliferation risk accordingly. From the previous question about acceptability immediately descends the question of how to enforce conformity with the line, or how to enforce the control of fissile material, as shown in the figure? What is the most appropriate regulatory body to designate for the use of this framework? Are all regulatory organizations to be trusted, or are there inefficiencies in the portion of the regime system that concerns their competence? Do they have the authority and the means (i.e., resources) to exercise control? Is there a way to empower these institutions?

d. Solution Identification

The analysis in the figure shows that NPT abrogation opportunities are much greater, in terms of success probability, than diversion or misuse. The NPT and the additional protocol do not prevent a state from building underground facilities for uranium enrichment, as the recent developments of the Iranian case are showing. New frontiers of technology can mitigate this risk, although not systematically (e.g., the recent cyber attacks from Israel), or make it worse (e.g., the advances of laser technology for isotopic separation). Would institutional mechanisms such as the employment of a fuel bank (as supported by W. Buffett) to defend NESs from the abrogation threat? Would in this case the role of the NPT remain central (as recommended by President B. Obama)?

SUMMARY

Nuclear non-proliferation is a political objective that can be achieved only when knowledge of all the complexities associated with it is understood and integrated into a coherent policy. This is an international problem that requires a solution that is also international in its scope; it requires an international consensus regarding the structure of a potential regulatory body entitled to create new regulations and policies, and empowered to make decisions regarding nuclear fissile material control.

Using risk information is a way to create a clear, and powerful framework capable of integrating all the instruments needed to strengthen the current proliferation regime. Policies, safeguards, and nuclear design improvements are all means to reduce the proliferation risk, but to do it successfully a rational weighting of all these elements is required. The policy framework I illustrated in Figure 1 constitutes a first step for the comprehension of this problem, and a key interpretative element that can be used to formulate a more broad and coherent set of policies. Beside its mathematical connotation, it can be considered as an exploratory vehicle to approach the problem of proliferation control and to solve it systematically.

The creation of a comprehensive multilateral framework, as stated by S. Chu, M. ElBaradei, and G. P. Shultz, is an urgent need. Its development is particularly urgent in view of key proliferation risk contributors associated with the imminent phase of expansion of nuclear energy: the increase of plutonium inventories due to growing energy demand, the arrival of nuclear power newcomers in unstable regions, the introduction of new technologies (such as the modular reactor proposed by B. Gates, which can change the actual configuration of nuclear markets), and the recent advances in laser-based enrichment techniques.

Having such a framework in place would allow effective strengthening of the current non-proliferation regime and enabling of the radical change that nuclear energy is urgently waiting for.

However, many questions for politics are still unanswered. Much work needs to be done, and the creation of new policies to reduce the risks associated with the expansion of nuclear energy constitutes a fundamental piece of the overall solution to the problem of control of nuclear fissile materials.

This thesis tries to solve this task and lays the foundations to create a framework for nuclear non-proliferation by means of multidisciplinary approach which combines political science, nuclear engineering, nuclear physics and management aspects of this unique problem.

STRUCTURE

The structure of the thesis follows the structure of the mental thinking process I went through since I dedicated to the solution of this problem. Most sections are referenced to papers I published about this topic. Following the SDM philosophy, many sections contains a set of system design principles (SDP), and most of the concepts are explained by supporting them with visual information.

PART I. describes the project goals, and in particular the metrics used for non-proliferation and the various steps that the entre framework, once completed might include.

This section is adopted from two papers. The first presented at the global 2009 conference in Paris and the second submitted to nuclear technology to be part of a special number about nuclear non-proliferation.

PART II. contains the inspiring analogy with safety case used to benchmark the new framework. existing paradigms of safety are described and from those are inferred the milestones and principles used to create a proliferation assessment model and policy.

This section is adapted from a paper submitted for a special number about nuclear non-proliferation.

PART III. describes the structure of the assessment method. The metrics and sub-metrics used to determine the proliferation performance of a nuclear energy system based on the barriers, safeguards, and policies used for its protection from proliferation risks.

PART IV. describes the non-proliferation acceptance criteria that has been defined in order to compare different design alternatives. The section focuses on the description and use of the probability-consequence space and of the curve that can be used to distinguish designs having good proliferation performance from those having poor and weak anti-proliferation features.

This part of the work is readapted from a presentation done in Albuquerque in 2009 and that was awarded by the DoE for its contribution to the advancement of R&D of nuclear fuel cycles after competing with many Us laboratories and universities.

PART V. reports some of the results obtained from the simulation we run using the assessment technique. The results are referring to a SFR nuclear power plant and its protection systems.

Most of the results reported are re-adapted from the final report of the NERI project.

PART VI. reports conclusions and summarizes the work done.

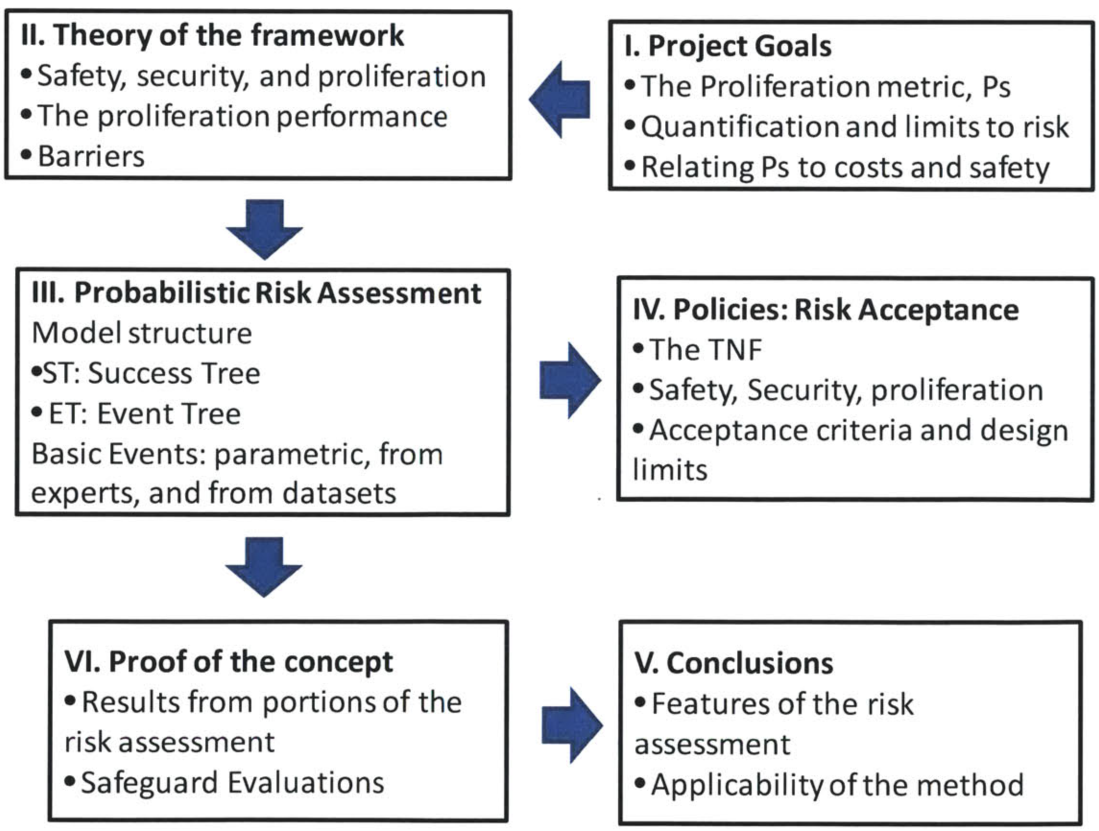


Figure 1. Structure of the thesis.

PART I: INFORMING NUCLEAR ENERGY SYSTEMS WITH PROLIFERATION RISK

A novel non-proliferation metric is proposed, and described through a competition model between two actors: the energy system's safeguarder and a potential proliferator interested in acquiring SNMs. The method developed is analogous to that of plant reliability fault tress in that it includes the creation of a event and success tree models that start from basic events and lead to the top metric, measuring the proliferation performance. The method allows measuring the proliferation performance by means of a metric expressing the proliferator's success probability in acquiring SNMs. However measuring the likelihood of a scenario is not enough if not coupled with the assessment of the consequences associated with its realization. For this, a new probability-consequences (P-C) curve, is proposed for use in regulating the non-proliferation scenarios dealing with acquisition of SNMs.

The addition of new design options such as detection devices and of degraded materials as means to reduce the opportunities attracting a proliferator to divert the SNM, are used as illustrative applications of the new framework. The examples use a reference design based on preliminarily proposed designs. Then the framework is implemented using security and safety criteria in a fashion consistent with recently proposed US regulations.

The framework demonstrates a method for the quantification of proliferation risks and shows how it can be integrated with other design considerations. Ultimately, it is a first step toward strengthening IAEA's current ability to protect nuclear systems from proliferation risks.

INTRODUCTION: PROLIFERATION RISKS

Energy, produced on a large scale, is essential for modern life. Its provision involves sustainability, carbon free, and base load electrical generation. This has led to the return of nuclear energy as an important source of energy. Yet as excellent an option this source may be, issues such as security and safety are still concerns, in addition to those of attacks upon the plant and proliferation resistance.

Security can be seen as a new area of performance constraints, posing new challenges to the safety analysis of systems and their protective barriers. Security management systems must be developed using data from analyses based upon classical reliability framework-related methods and utilizing risk analysis methods in addition to considering factors of organizational behavior and policy making.

"Related modeling needs include those of dynamic and stochastic processes, the integrated dynamic response of the systems/hardware and software components and operating crews during accidents "[1].

This thesis describes the development of these methodologies and their inclusion in a new regulatory framework for security and non-proliferation.

METRICS AND CRITERIA FOR ASSESSING THE SYSTEM PROLIFERATION PERFORMANCE

Regulation of proliferation risks involves engineering and policies, which can include a multi-disciplinary approach joining system engineering and political science. From an engineering standpoint, one must address proper metrics and establish criteria in order to measure security and proliferation performance. The current policies and regulations are not yet capable of both regulating vulnerabilities and assessing power plant performance for these domains. Current international and homeland security policies neither use such performance measures nor do they state clear acceptance criteria for events such as a proliferator's diversion of weapon-usable material. In order to do so, a security framework for proliferation is required.

In particular, new nuclear power plant designs need the entire nuclear energy system (NES) to be integrated with a "security culture", sensitive to assessing design choices from a proliferation perspective.

For this methodology, PRA-like techniques and organizational behavior related tools can be adopted. The difference between a safety scenario and a security scenario is the nature of the initiating events; e.g., safety scenarios are caused mostly by unforeseen random component failures while intentional human malicious actions lead to security related scenarios. The proliferation attempt scenario can thus be seen as a complete sequence of human actions aimed to exploit the vulnerabilities of a hardware system.

Concerning acceptance, few regulations have been proposed considering proliferation, and they remain inadequate for assessing overall performance during an attack. For example, the U.S. NRC's planned framework for licensing future generation nuclear power plants vaguely mentions the inclusion of non-proliferation criteria in the regulations such as NUREG-1860 [2].

In essence, building a regulation proliferation framework requires use of guidelines, design methods and a policy specifying acceptance criteria. All of these constitutive elements can be adapted from the nuclear safety domain. A series of specific observations related to these two tasks is described in sections V and VI.

THE PROJECT: A MULTI-GOAL OBJECTIVE

For three years the U.S. Department of Energy (DOE) has funded a study to improve the performance of the Sodium Fast Reactor (SFR) concepts [3]. Because the SFR technology has been studied for more than 30 years and successfully built in several countries, it is recognized as one of the promising GEN IV technologies. Although many design variations have been proposed for the SFR, its economic feasibility has not yet been demonstrated. Thus, a primary objective remains that of identifying more economical design alternatives, ranked according to their economical feasibility, safety, and non-proliferation based contributors. The creation of tools and methods needed to rank such designs is an integral part of our work.

In doing this, a set of design architectures were investigated concerning their safety, cost, and proliferation performance. We focus upon the definition of the proliferation resistance metric, its associated criteria, and its relation to cost and safety metrics. The result is the development of a system based framework that allows for the exploration of different designs from a proliferation resistance perspective.

THE TECHNOLOGY: SODIUM FAST REACTORS

In total, twenty-one sodium cooled fast reactors have been constructed worldwide, ranging from early experimental machines to electricity-producing prototype or demonstration reactors.

By 2007, only six of these reactors were operating or scheduled to resume operation. The accumulated global experience with SFRs clearly indicates that this technology is feasible for production of industrial scale electric power. Technological feasibility aside, the challenge concerns practicality. Recently, four overarching criteria were proposed for the developmental guidance of Generation IV reactor systems: sustainability, cost, safety, and proliferation resistance [4]. Nevertheless there is still much work needed before the SFR can satisfy these objectives.

In the following sections, we address the design of security metrics for identifying system vulnerabilities, the ability to interface designs with the imposed criteria, the formulation of these criteria and their inclusion within regulations, the designers' ability to include organizational dysfunctions in their evaluation, and the integration of security metrics with economic and safety metrics in a probabilistic design fashion.

THE MODEL USED TO ASSESS PROLIFERATION RISKS

Quantitative analysis: the ST/ET model

In order to perform proliferation risk evaluations a proliferation competition model was developed based upon a prior study [5]. The model allows one to assess the capability of a system to resist proliferation. A success tree/event (ST/ET) tree topology measures the proliferation resistance of the NES, and logically depicts it throughout the competitive interaction between two actors aiming to acquire and defend the special nuclear materials (SNM) present in the SFR's fuel cycle. Respectively these two actors are named the proliferator and the safeguarder.

To set up the model, four sub-steps are necessary:

1) Characterize the systems in which the actors compete,
2) Select the contended target,
3) Implement a plausible competition strategy with tactics,
4) Construct the success/event tree model.

The first part of the assessment requires one to formulate all the above four steps in a qualitative fashion. First one is to become aware of the systems and processes vulnerable to attacks and their location. For example, in a diversion of fuel elements scenario, the likely regions for diversion should be identified.

The preliminary screening of regions is determined by characteristics later explained in this paper, that led to identifying these three diversion points: the storage rack, the washing station area, and the transportation system (see Figure 3).

The identification of these regions is driven by the determination of the contended amount of SNM[4] required to create a nuclear explosive device. In particular, this amount is calculated in terms of a significant quantity (SQ) which, in the IAEA definition, is the approximate amount of nuclear material for which the possibility of manufacturing a nuclear device cannot be disregarded.

The second part of the assessment requires one to quantify the strategies and the tactics identified by the preliminary analysis already described.

---

[4] In this analysis only plutonium mixture is considered amongst all the possible fissible materials that can be used to build a nuclear weapon device.

Qualitative analysis: system element identification and fuel operations

Preliminary to the quantitative analysis, a qualitative analysis helps in determining the point of interest within the NES. This section describes how the qualitative analysis of the SFR is carried out, specifically how the potentially vulnerable sub-systems composing the nuclear energy system and the associated proliferator's actions, were selected.

The nuclear energy system of interest is that of the SFR fuel cycle that has been further decomposed into the SFR power plant and the fuel processing facility. Figure 2 shows the fuel processes in a SFR power plant and the segmentation in its sub-systems.

Following the scheme used for EBR-II and replicated for the ABTR [6], the operations reported in the figure are categorized by restricted and unrestricted operations like shutdown time, which is costly and time operating. The fresh fuel is initially loaded into the core and is later moved, after being spent, to the storage rack located in the outer periphery of the core. This maneuver is conducted with a pantograph fuel handling machine (FHM) that operates between the outside of the core barrel and the inside wall of the redan[5].

The rack has a dual purpose: it provides a temporary location to fresh fuel elements preloaded into the reactor vessel, and it allows for cooling of the spent fuel element. Unrestricted operations of fuel elements occur after fuel insertion into a shielded cask called the inter-building cask (IBC).

The fuel-unloading machine (FUM) is located at the top of the vessel and uses a shielded cask mounted on a self-propelled frame traversing the transfer port on top of the vessel and the IBC pit area. Before reaching the external boundaries of the plant, the fuel first exits from the containment building through the inter-building transfer tunnel (IBT) into the area of operations where transits into the washing station and then goes to the air cells. In these areas the spent fuel is treated and cleaned from residual sodium and then parked in a buffer area waiting to be transported to the fuel processing facility.

Following this scheme of operations allows for detecting the locations more vulnerable to potential diversion attacks as given by their characteristics.

These physical characteristics are defined by the location accessibility, the material contained within it, and the handling difficulty in removing it. They are described using metrics referred to as facility attractiveness, material attractiveness and fuel handling ability. These intermediate metrics all concur in defining the overall top metric, which for the analyzed scenario of diversion, in combination constitute the 'diversion' resistance of the SFR power plant.

[5] The redan is a right circular cylinder fabricated from stainless steel hosting the core barrel attached to the inlet plenum. It provides a barrier for the hot sodium at hot outlet temperature from the inlet cold sodium.

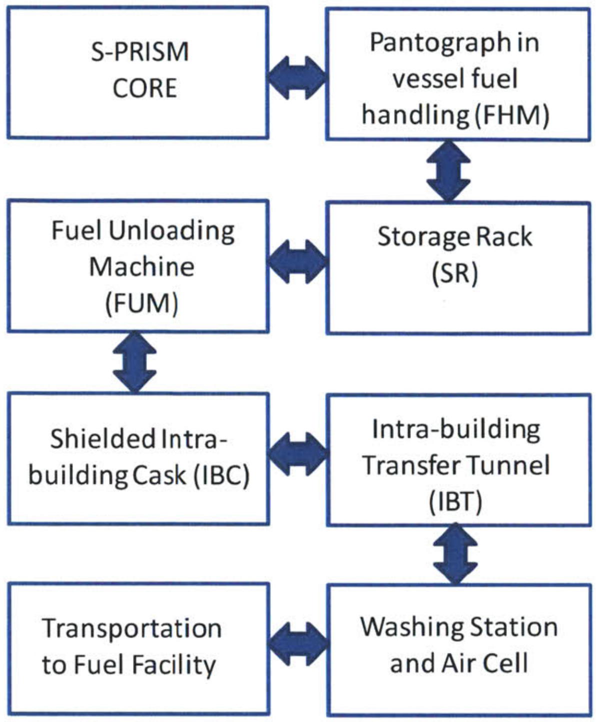


Figure 2: Fuel movements and operations at the SFR site.

Diversion scenarios construction and mitigation

Scenarios can be defined as the potential steps or sequence of events taken by the proliferator to achieve its goal. The scenario consists of the pathway followed by the proliferator in order to defeat barriers and to ultimately obtain SNMs. Classical scenarios considered to be of interest for a state hosting a NES are theft, diversion, misuse, and abrogation. Specifically, a diversion scenario is defined as a set of actions, or tactics taken, by the proliferator to divert weapons material from the site.

All of the pathways can be formulated by the event trees showing how the material is being transported out the site. The process for acquisition of such material from one of the potential vulnerable points is instead formulated by the success tree. Figure 3 depicts one of the potential pathways in a SFR site not co-located with the fuel fabrication and processing facilities. The pathway is illustrated in this section and later re-proposed in a quantitative formulation of the SFR's proliferation resistance. A complete realistic set of scenarios will include all the possible pathways, and their union will depict the overall vulnerability for the systems considered. The creation of such a scenario is both expensive computationally and in terms of efforts. Thus, this thesis only reports the structure of the analysis with a focus on the methodology rather than the completeness of the scenarios.

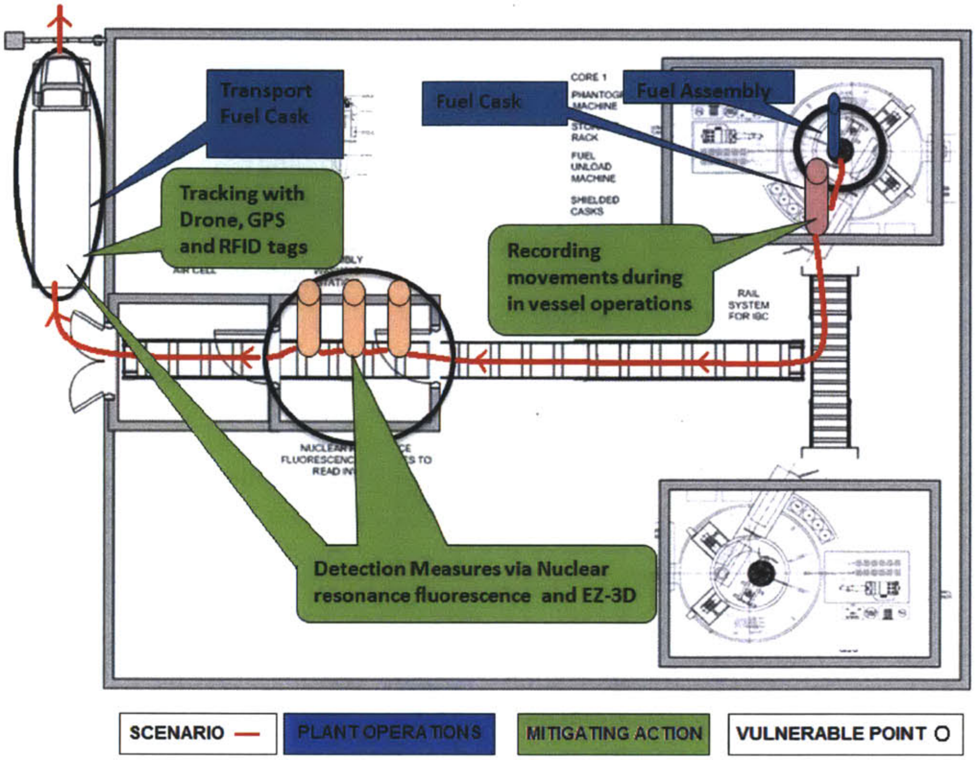


Figure 3: SFR power plant schematic diagram: points of diversion and preventive measures.

The hypothesized scenario shown in the figure represents the diversion of SNM by means of a dummy fuel element being substituted for the stolen fuel element. This can occur if some measures are not taken to prevent diversion at the points circled in the figure. A fresh fuel element could be extracted from the storage rack by falsifying the fuel-handling machine data, and replacing it with a dummy. The fresh fuel element would travel together with other spent fuel elements through all the intermediate areas shown in the figure. Without introducing isotopic measurements, then the dummy fuel could bypass the safeguards in the air-cell and go throughout the plant. It is noteworthy that a proliferator needs to bring the dummy into the power plant, and thus, more refined tactics using dummies need to be developed (e.g., by using combined strategies supporting options such as defeating the camera recording systems or falsifying cask controlling signals).

EVALUATION OF THE SFR DESIGN ALTERNATIVES

A systemic approach to evaluate the SFR's design alternatives

Every technology based design, including that of a nuclear power plant, can be seen as the sum of all the possible design options available before assembly. A design option than usually is represented by a system having a function contributing to the overall plant's performance. For example, in a SFR reactor the production of electricity comes from burning the fuel, however many fuel types and various core types might be available to satisfy the goal of producing electricity. The SFR is an advanced plant, and while it has been constructed and operated by few countries, it is still considered a prototype. This leaves its design open to design choices, in the sense that designers still have not adopted a preferential design. Our work required the choice of a reference design. This required that an initial dominant design options be selected (or pivotal [7] design option). Once a core pivotal structure of the plant is set, set, designers can evaluate the benefits derived by addition or removal of less critical components. The overall design, as well as its single pieces can then be evaluated from different performance perspectives (i.e. proliferation, safety, and economic performances). Once all design decisions are taken and a final version of the NES is assembled, one obtains a design alternative.

Table 1: Design options for the reference SFR design

The architecture of the design used in the following examples is given by the sum of all of those marked in bold and with a blue background options.		
Fuel type	**Metal**	Oxide
Reactor type	**Loop**	Pool
Reprocessing type	**Pyro (dry)**	aqueous
Pump types	Centrifugal	**Electromagnetic**
Facility's location	Co-located	**Stand-alone**
Conversion ratio	Less than 1	**More/equal 1**
Secondary circuit	Water	**S-CO_2**
Intermediate loop	**Intermediate**	None
Fuel types	**Blankets**	No-blankets
Blanket & driver fuel strategies	• **w/o MA (DA_1)** • **with MA (DA_2)** • **hydride ($DA_{3/4}$)**	• w/o MA (DA_1) • with MA (DA_2) • hydride ($DA_{3/4}$)

We selected a reference SFR architecture expressing an initial preference concerning some pivotal design features such as the design of the reactor core and the fuel type. The choice was driven mostly, but not only, by available information and national capabilities; the choice went on a pool type reactor with metallic fuel. Once a pivotal design option is set, this in turn determines a set of sub-design options which are compatible with this initial configuration. For example, the metallic fuel choice favors a fuel reprocessing scheme using pyro-reprocessing. Although pivotal design options set the choice of some design options, or establish a preference among the entire set of design alternatives, they still leave the design open to many possibilities of customization. Table 1 summarizes the range of possible design choices associated with the reference SFR design. Table 1 shows the pivotal features, and the design alternatives for the SFR plant and fuel cycle, some of which affect the proliferation performance of the NES.

In particular, different strategies can be used either for driver fuels and for blanket elements in order to increase their proliferation resistance. If the fuel strategy includes use of blankets, then the proliferation resistance of this design is promptly decreased by the presence of significant quantities of the high grade plutonium produced during operations.

In order to reduce the vulnerability of designs involving blankets, additional features can be introduced. The lowest part the table reports the subset of options analyzed for the example described in the paper. Specifically, the addition of minor actinides (MA) or of hydride fuel to the fuel blanket, are the four design options explored.

Each of the four proposed alternatives is first evaluated using the ST/ET to determine its proliferation features, and then using a procedure that relates the proliferation assessment to cost metrics and safety metrics.

Relating non-proliferation metric to other design metrics

A consortium of universities participating to this project is currently developing[6] a comprehensive model to evaluate the SFR design including the different perspectives of safety, economics, and non-proliferation. This section describes how a risk-informed design procedure can be established starting from the results of our model and how non-proliferation metrics can be coupled with other design metrics such as damage frequency and cost for various design alternatives. Figure 4 shows the general framework that has been used to link the different metrics of safety, non-proliferation, and cost [8].

Each of these perspectives has to be evaluated on the basis of a different metric. For each of the three metrics of interest, the calculated value must satisfy the acceptance criteria of the regulator (i.e. the minimum safety standard) or by the marketplace (e.g., the maximum cost allowable).

We iterate within the design space to find attractive options.

[6] At the time this part of the work was written for the Paris Global 2009 conference in September 2009, the project was in its initial development. Today the project is in the final stage of development.

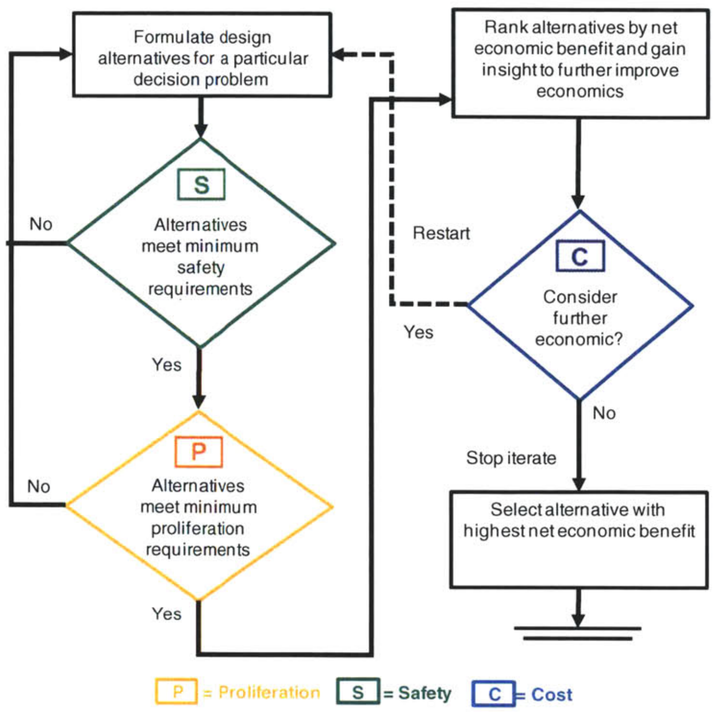


Figure 4: Schematic decision process used to acceptability of a NES determined by three fundamental design metrics.

Current regulations provide criteria for determining the maximum allowable core damage frequency for a power plant. The economic metric used is the levelized cost of electricity associated with the design, evaluated in comparison to that of a current LWR. Regarding non-proliferation, the metric that is being used to evaluate the design is the proliferator success probability, Ps. This metric is complementary to the capability of the NES to resist to an attack from a proliferator, or its proliferation resistance, PR, (i.e., PR = 1-Ps). However currently regulatory bodies do not indicate acceptance criteria defining the minimum acceptable value of PR. Thus, proliferation acceptance criteria must be proposed to guide designers throughout the proposed design screening process.

A way to visualize the screening process shown in Figure 4, is to describe each design alternative by a vector relating all of the metrics being used as the 3D vector reported in Figure 5.

Within this design space, the design concepts that meet the multi-goal criteria, are represented by the points falling into the acceptable region delimited by the Ps-S plane and having the lower cost on the vertical C-axis. Following this logic, among the two acceptable design vectors of Figure 5, the one that is more promising from an economic standpoint is the vector labeled as DA_2 because of its lower quote. However, the first logic might favor the first design alternative, DA_1, because of the advantage offered by its safer and more proliferation resistant design.

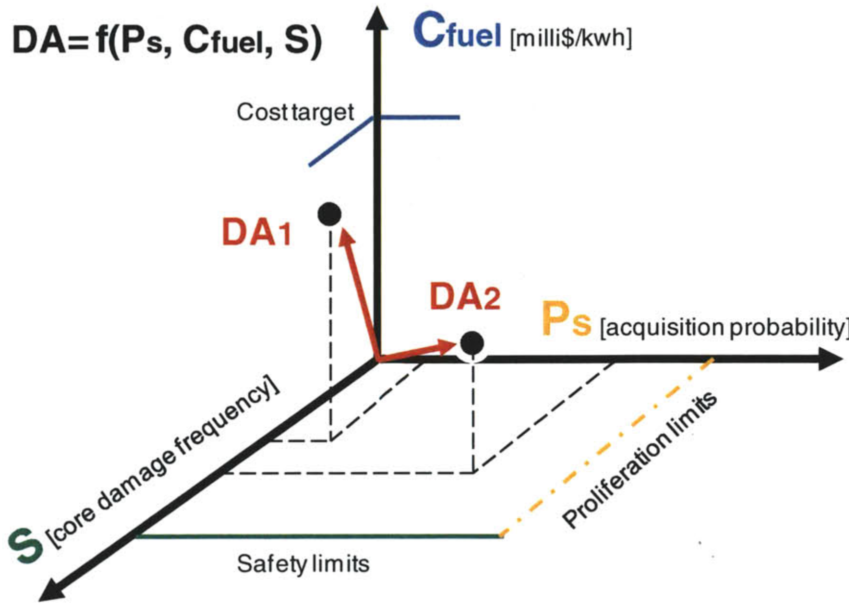


Figure 5: Two different design alternatives, DA_1 and DA_2, in a performance metrics space.

PROLIFERATION RISK AND ANTI-PROLIFERATION PERFORMANCE

How the risk is measured by the ST/ET model

The model built to assess the proliferation features of a generic NES, and extended to the SFR fuel cycle, is inspired by the models used in nuclear safety measuring the risk performance, or probabilistic performance assessments (PRAs). In a similar fashion to PRA models, the ST/ET model recreates the spectrum of potential consequences following an initial event. While for safety, the initiator is a stochastic event, for proliferation it is a agent driven intentional event.

The risk evaluated using the ST/ET model considers the threat of a potential proliferator, for any scenario ranging from theft to abrogation, and it is always associated with the intent to acquire illicitly SNMs. For the case of diversion, the model calculates an estimate of the probability Ps taking into account the probability of acquiring the material from a given location and the probability to transport it out of the NES, without being detected. This estimation also implicitly takes into account all the relevant features for the evaluation of the proliferation risk. The following summarizes the relevant features considered in our work:

1. The risk of proliferation is calculated by means of an overall metric, Ps, which is a estimate of the conditioned probability of SNM acquisition given an attempt, and the consequences associated with each scenario;
2. The risk evaluation, utilizes sub-metrics, considering the characteristics of the NES, the features of the target material, the difficulties encountered by the proliferator in acquiring, and transporting the material out of the NES;

3. The risk evaluation includes all of the physical, institutional, and organizational counter measures that the safeguarder might use;

4. The dynamic interactions of the two competing actors, including the resources they can spend to succeed in their respective missions;

5. The uncertainties of the results especially considering that most of them are obtained via subjective expert's judgment.

From the last perspective we see that the proliferation evaluation is an exercise to organize logically the beliefs of experts regarding the actual level of proliferation risks. However, this exercise is useful because it allows to compare the proliferation risks associated with different design alternatives, and to measure the cost-benefits associated with the introduction of new features to protect the NES from proliferation risks.

Although major international activities in the area of nuclear proliferation proposed assessment methods similar to the one here anticipated, none of them was able to capture the entire set of features above proposed yet. Also most of these studies relied on hybrid representations containing both multi-attribute approaches and pathway analyses, while the model we propose here is set to be more close to a PRA analysis. However, at the current stage of development it is not possible to rigorously determine the differences between our approaches and others, and thus this section limits to illustratively describe the ST/ET approach.

Measuring proliferation risk changes

The present discussion explores the way risk information can be used to evaluate the addition of barriers within the NES. The combination of intrinsic anti-proliferation features (such as minor actinide addition) with extrinsic counter measures (such as a real time accountancy system like NRF) are explored. The example is provided with the purpose to show how risk information can effectively help to improve the performance of the system from a proliferation standpoint.

The proliferation risk associated with a given nuclear energy system's design can vary depending on the features introduced into the design and how it is operated. For example for the scenario of Figure 3, if blanket fuel elements are introduced in the reactor core, the overall risk associated with the SFR design increases. The risk increase reflects the potential increase of interest for a proliferator because the blankets choice implies the presence of significant quantities of high grade plutonium along all of the vulnerable points determined by our analysis. Thus the proliferator would find more valuable to attack the system, and, using the previous example, to swap a fuel blanket with a dummy fuel element. To contrast this substantial increase of attractiveness and of associated risk, the safeguarder's role, that for simplicity in this context we can identify with a designer, has to introduce some additional counter measures to reduce the probability that such proliferation pathway occurs. These counter measures can be added in form of technological or institutional measures, and they can be either intrinsic or extrinsic to the NES. Intrinsic features are embedded in the systems and processes of the considered design from its first scratch. Extrinsic features are generally added to complement the intrinsic ones. Whether these features are institutional or technological in their nature is not discussed in this paper, although a complete assessment all these counter measures have to considered. The example that follows refers on technological counter measures.

If the safeguarder is able to establish a robust counter strategy to the proliferator's tactics, these will be less effective. One way to counter balance the risk increase due to the introduction of fuel blankets is given by the addition of minor actinides into the fuel scheme, which offers the safeguarder an opportunity to reinforce the design against the dummy strategy. However, adding minor actinides to fuel does not necessarily guarantee a proliferation performance increase to the entire fuel scheme. In fact, the addition of MAs is possible only if at the current fuel scheme an aqueous reprocessing facility is added. On opposite using MAs is an effective strategy, especially when combined with a safeguarding strategies; the concept we proposed consider using minor actinides with the dual purpose to both degrade and tag the spent SFR fuel. In this way, the fuel has less attractive quality, and also becomes identifiable by specific isotopic detection machines capable to detect the concentration of MAs added to the fuel.

The inclusion of specific detection systems capable of detecting in a short time frame the presence of MA contents in the fuel elements travelling through the plant, allows monitoring the plant continuously and therefore guarantying the robustness from diversion attempts over time. One system that has been showing to have these features is the Nuclear Resonance Fluorescence (NRF) proposed by Bertozzi [9]. The NRF is an active interrogation detection system, capable to detect the presence of small quantities of isotopes within a fuel mix.

Thus, if the MA strategy is combined with the use of a detection machine for isotopic identification such as NRF, the overall proliferation performance of the NES to which these strategies are applied increases as due to the degraded properties of the fuel together with the increased detection capabilities of the NRF accounting system. These proliferation performance gains, in a risk framework, can be easily quantified by means of appropriate indicators known in the field of safety as importance measures.

In conclusion, robustness in design has to be achieved from both a system and an organization perspective. One way to reduce the system's vulnerability, is to reduce the uncertainties due to technological limits in detection. This can be done by adding to the NES specific safeguards with near real time detection capabilities and able to track the presence of isotopes in the fuel. When these capabilities are supported by strategies to reduce the attractiveness of nuclear materials on site, a more robust design is created.

ACCEPTANCE CRITERIA AND DESIGN LIMITS FOR PROLIFERATION

Security criteria used in NUREG-1860

Along with the development of the method, the support of clearly stated regulatory limits is needed in order to define the acceptability of the proposed design changes.

For safety, opportune criteria are established in the current regulations and expressed by limits imposed on safety performance metrics. For example, NUREG 1.174 describes the performance changes on existing nuclear power plants in terms of a safety metric called Core Damage Frequency (CDF) and it provides the regulatory limits corresponding to acceptable safety performance of the plant.

The current international framework for non-proliferation including norms, treaties, and policies does not contains proliferation performance acceptance criteria. Also domestic regulations such as NUREG-1860, describe a treatment using a risk-informed and performance-based approach. The approach integrates decision processes accounting for uncertainties and barrier mitigation rules with deterministic and probabilistic criteria.

However, while this regulation contains a safety framework well substantiated and refined, for proliferation there is nothing specific that goes beyond a chapter on security. However security and proliferation, as discussed in detail in Section II, are two distinguished problems that deserve separate approaches to their resolution. So, our task, in parallel to the development of the ST/ET model, has been to propose specific proliferation acceptance criteria, established consistently with novel regulations such as NUREG-1860.

Acceptance criteria for diversion

Safety regulations availing of risk information usually classify the risk associated with a given nuclear for an accidental scenario is represented by means of its frequency and its consequences. Following the initial representation provided by the English regulator F. R. Farmer, a line can be traced to delineate the separation between acceptable and non acceptable scenarios.

Figure 6 shows the curve we propose representing the probabilities and the associated consequences invoked by a proliferation scenario[7]. The proposed curve is expressed in terms of conditional probability of success of a given diversion scenario and the fraction of significant quantity, or SQ %, acquired by a proliferator succeeding in his attack. Thus, the proposed curve

[7] In this case the scenario discussed is covert theft of nuclear materials, or diversion. In the next sections the representation is going to be extended to other scenarios, such as misuse and abrogation.

is a P-C curve rather than a F-C curve because it plots the probability, Ps, to succeed in an acquisition attempt versus the consequences deriving from such acquisition. There are some beneficial features resulting from this representation. The chosen domain decomposes the risk into a two dimensional vector made of the probability to succeed in a proliferation attempt, or a series of attempts. This conditional (upon attempt of proliferation) probability is plotted versus a consequence scale functional to the feasibility of any acquisition attempt, and considering the potential weapon device development associated with the malicious attempt.

The first is the exclusion of the consideration of the uncertainty associated with the initiating event. The probability Ps obtained from the ST/ET model, excludes from the calculation the probability that the proliferator is going to initiate a pathway to proliferation. It is effectively impossible to quantify the initial willingness to initiate a diversion attempt to the system; by using a conditional probability the analysis gets rid of the uncertainties associated with the quantification of this event.

The second important feature is that the consequences associated with each scenario of calculated probability Ps, are evaluated in terms of the simple amount of material that can be subtracted from the NES. This direct way to evaluate the consequences, also in this case, allows removing the uncertainty deriving from the ultimate consequences of an illicit acquisition of SNMs.

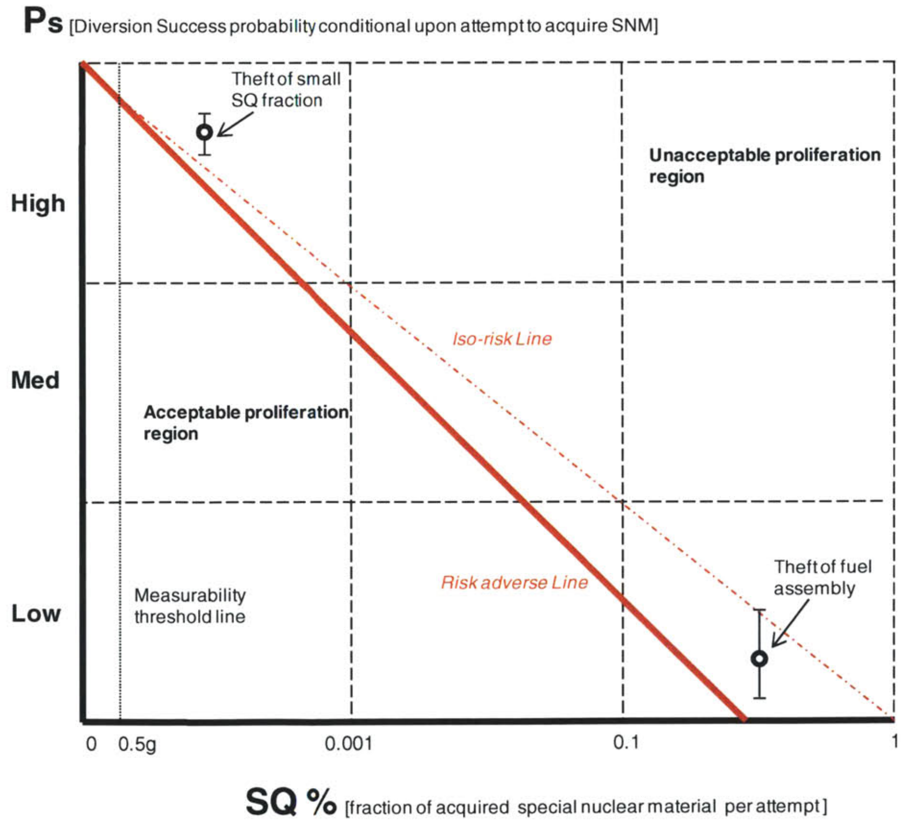


Figure 6: Probability-Consequences curve for proliferation.

This treatment is analogous to that of a PRA level 1 analysis, in contraposition to level 3 PRAs that consider the consequences on the population surrounding the nuclear site. In the same manner, calculating the consequences deriving from the acquisition of the sufficient amount of material needed to create a weapon does not push the analysis to evaluate what these consequences are in terms of fatalities. This last aspect is even more correct if we consider that the consequences inferred from the concealed acquisition of SNM from a NES do not occur in proximity of the nuclear site and do not happen at the time the SNM acquisition attempt takes place. Contrary to the safety case, the potential effects associated with a diversion event are measurable far in space and also in time from the place where the original scenario take place.

The third feature is the boundary line dividing the riskier scenarios from those potentially acceptable to society. The determination of the actual curve to be used is not trivial, and requires further study, however the graph in the figure reports two possible curves. The dashed upper line represents a iso-risk curve, corresponding to the case where society is attributing more importance to the overall range of consequences rather that to unlikely scenarios but with potentially devastating consequences. A more plausible curve is the bold steeper (risk averse) one portraying a situation where society does not accept designs allowing diversion of one entire SQ. This is because the consequences associated with its realization directly could lead to the development of a nuclear explosive device.

The new scale of consequences, ranging from the acquisition of very tiny fractions of SQ to an entire SQ in a single attack, immediately allows one to relate the probability of a threat, calculated via the ST/ET analysis, with the consequences resulting from the realization of the acquisition scenario.

Although at the current stage of development it is not possible to recommend a slope for the criterion line, in absence of information, we use a conservative risk adverse criterion in order to screen the design alternatives used as examples in this work.

In conclusion, the selected approach reflects the philosophy of the newly proposed regulations, such as NUREG-1860, and allows for defining acceptance criteria for the frequencies obtained from the ST/ET scenarios.

Proliferation design limits

The approach used in safety to regulate nuclear power plants design in most of the cases consists of two components: the acceptance criteria and the design limits. Acceptance criteria in the current US regulation system can be seen as limits to overall probability of failure for a power plant. They therefore represent a limit to the overall design performance of the plant, which is formulated by regulators on the basis of what is considered to be an acceptable risk for the society. To the contrary, design limits represent limits imposed on the value of certain parameters that are measured by mean of intermediate metrics.

For the proliferation case, imagining a parallel structure to the one used in safety, acceptance criteria are limits to the overall measured proliferation performance of a NES, while design limits refer to specific sub-metrics that in have a considerable influence on the overall system's performance. Within this context, certain levels of acceptability on individual measures can be set to inhibit the occurrence of a given scenario. For example, the attractiveness of the plutonium available in a certain area of the SFR is an important driver to the value of the overall metric Ps. The attractiveness of the material should in turn depend on many factors.

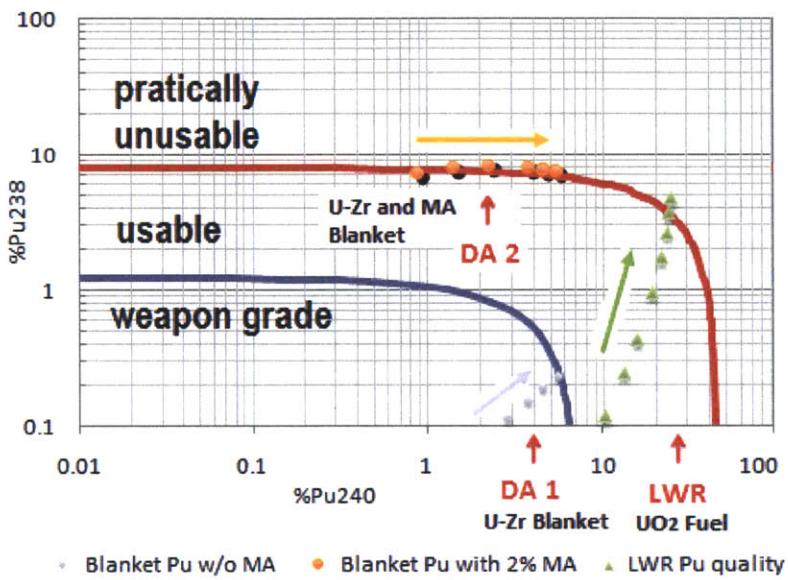


Figure 7: Design limits for plutonium blanket elements for two different SFR design alternatives (DA1: standard blanket design and DA2: blanket design with minor actinides) compared to the case of LWR fuel. Each design is a function of increasing (from left to right) burnups.

In order to show how these design limits can be set as requirements for a nuclear fuel alternative, for simplicity we assume that the material attractiveness of a nuclear fuel depends only upon the plutonium quality. The quality of a given plutonium mixture can be expressed as a function of the relative abundance of the 238 and 240 isotopes [10]. By plotting their relative abundances we can define design limits for proliferation using two curves: the IAEA definition of weapon usable material and the definition of unusable material provided by a recent study [11]. Figure 7 reports the concentrations of the two plutonium isotopes at different burn-up levels. The fuel alternatives considered are fuel blankets, with and without the use of MAs in the fuel, and traditional LWR fuel.

The first design limit is represented by the outer line of Figure 7. Any design outside of this boundary will be not practically suitable for a nuclear weapon device. If the fuel properties fall below this curve, then the fuel might become usable in a nuclear explosive device, conditioned to the proliferator's availability of a separation facility, or to his ability to assemble a low yield weapon. For very low concentrations of the two even Pu isotopes, the material is, accordingly to the IAEA definition, weapon usable material.

To summarize, the two boundary curves in Figure 7, show the regions of the material attractiveness of various SFR fuel blankets as a function of their relat be abundance of the 238 and 240 plutonium isotopes and also a function of the measured fuel burn-up. The set of points in the figure show how, from modest burn-up values (1 month spent in the core at full power) to their refueling value, the quality of the fuel varies from weapon grade to practically-unusable. Three different design fuel alternatives, oxide fuel from LWRs, metallic fuel from a SFR with no actinides, and metallic fuel from a SFR with minor actinides, show how the addition of MA to the SFR fuel can shift the entire fuel quality from the weapon grade region to the usable-unusable region.

- Regarding LWR fuel, the lowest points of the trend line in the UO_2 series of Figure 7 falls into the usable zone. This result implies that LWR fuel is proliferation resistant only when that it has spent more than 1 month in the reactor core.

This last results implies that diverting fuel from low burn-up LWR fuels can be attractive scenario for a state with proliferation ambitions. However, in general the LWR fuel is not considered attractive for diversion, and therefore its attractiveness can be utilized as a design limit to which compare the attractiveness of SFR fuel, as shown in the next section.

Finally, note that the approach used to set design limits is at a material level. However, material attractiveness is not the only possible measure of attractiveness considered in the ST/ET framework. Other intermediate metrics such as the facility attractiveness and the material transportation difficulty have to be included into the set of potential design limits.

RESULTS FROM A PRELIMINARY ASSESMENT OF THE SFR FUEL CYCLE

In this section some results from our quantitative assessments are shown reflecting the analyses conducted on the SFR fuel cycle. Three illustrative examples, concerning different nuclear fuels for the SFR, are proposed with three different purposes: the first example shows the potential cost-benefits of a MA strategy coupled with NRF detection. The second, using our preliminary results from the ST/ET model, constitutes an application of the design limits concept, and it shows the relationship between proliferation performance and cost. The third example shows how the current evaluations can be extended from two design alternatives to the entire spectrum of alternatives available for the SFR fuel cycle concept, and it proposes a method to manage solutions.

Recalling the discussion about design alternatives evaluations, the first example compares the cost and benefits of three different DAs reported in the matrix of Table 1:

DA_1: metallic fuel with no MA addition and no NRF;

DA_2: metallic fuel with MA addition;

$DA_{2'}$: metallic fuel with MA addition, and NRF detection.

The costs of the studied design alternatives were derived from the Integrated Fast Reactor (IFR) study [12], and calculated using appropriate cost models [13]. Figure 8 on the x-axis reports the proliferation performance increase due to the addition of minor actinides to the fuel (in turn due to the corresponding decrease in quality of plutonium), and the further gains from using nuclear resonance fluorescence detectors (due to the dual increase in accuracy of detection and in the ability it provides for tracking the fuel tagged with MAs). However in terms of costs, considering the difficulties with fuel manipulation in hot cells and the lack of experimentally derived data, we can only recognize that the transition from DA_1 to DA_2 implies a high marginal cost difference due to the capital and operating expenditures associated with fuel handling.

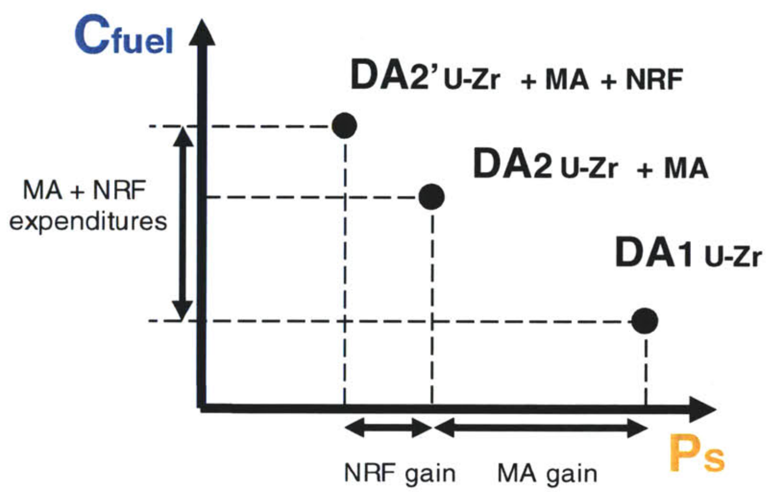


Figure 8: Metrics variations due to MA and NRF strategies.

Nonetheless, the benefits obtained from adopting a minor actinides strategy can be important, especially when including the NRF detection strategy. Such cost-benefits are listed below:

- Combined NRF and MAs strategies favor accountancy, (i.e., fuel elements with MA footprints allow to recognize via NRF the nature of the fuel elements based on their Pu/MA ratio), which allows one to decrease the average time spent on detection;
- Cost reduction due to better criticality safety and improvements of safety coefficients in case the MA strategy is used for metallic fuel (oxide fuel actually faces problems of positive reactivity in case the concentration of MAs goes above the 2% limit due to coolant void[11]);

• Cost reduction due to better fuel waste management and due to lower outage times resulting from the use of a continuous verification system.

Figure 8 summarizes all of the above observations and includes the results derived from the analysis of the considered design alternatives by positioning them in a design space described by the metrics P, and C.

The second example, shown in Figure 9 compares four different design alternatives in terms of Ps and costs. The differentiating factor for the considered design alternatives is the cost of fuel fabrication. The four designs are screened using as a design limit the value of Ps obtained from a LWR fuel with a standard burnup of 50 MWD/tonn. From a proliferator's perspective, high values of Ps mean an higher chance to succeed in the diversion of the fuel alternative considered. The results are presented in the forms of point estimate, mean value, and the 10^{th} and 90^{th} percentiles, as obtained from an uncertainty analysis performed using the ST/ET model. The figure shows that the modified fuels including the MA option described previously (DA_2) are below the LWR line, while the U-Zr fuel (DA_1) is well above the threshold line.

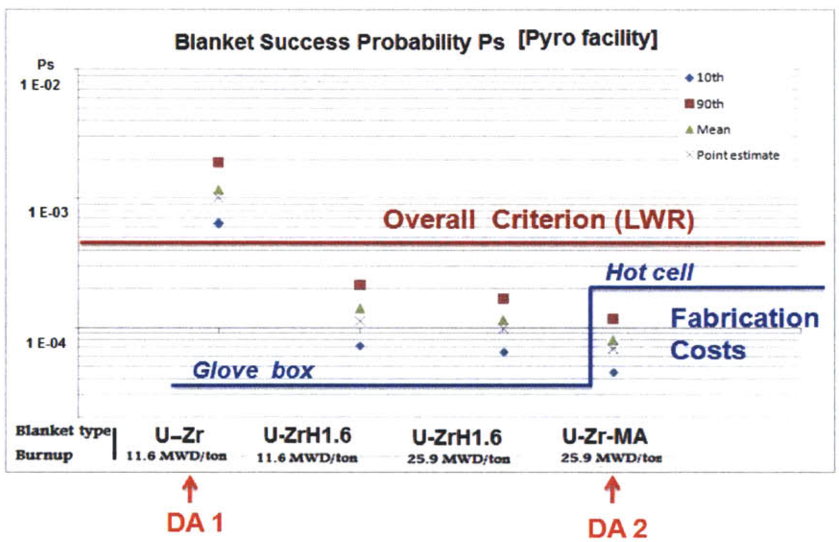


Figure 9: cost and non-proliferation risk metrics.

Two intermediate design alternatives, hydrate fuel for two different burnups, are considered as additional solutions for increasing the intrinsic quality of the fuel. As shown, from an economic standpoint, the MA strategy implies a net fabrication cost increase due to the shift from glove box to hot cell technology. Note that the cost representation in form of a step curve is qualitative, and also that the DA_2 costs are not escalated from the above mentioned positive contribution in the performance guaranteed by the MA strategy. Considering these factors and the entire spectrum of design alternative in a NES, such as the SFR, represents an element of complexity and of computational effort.

One way to explore the space of DAs with moderate computational effort, and to reduce the number of options to be considered, is offered by the Pareto[8] technique. Figure 10 illustrates the method for the two metrics, cost and proliferation success probability. The two-dimensional design space can be explored starting from two pre-selected representative points (i.e. two of the fuel design alternatives selected in our previous examples). The Pareto optimal front (curved line in the figure) contains all of the economically feasible designs while the dashed lines group them accordingly to various cost categories.

Describing the method in detail goes beyond the scopes of this analysis, but it is important to note as it offers an opportunity to rank the different design alternatives in different cost regions identified by the Pareto fronts. Ultimately the method provides a tool for choosing among different design options aimed to reinforce the proliferation resistance of the NES and to determine optimal costs- proliferation performance configurations.

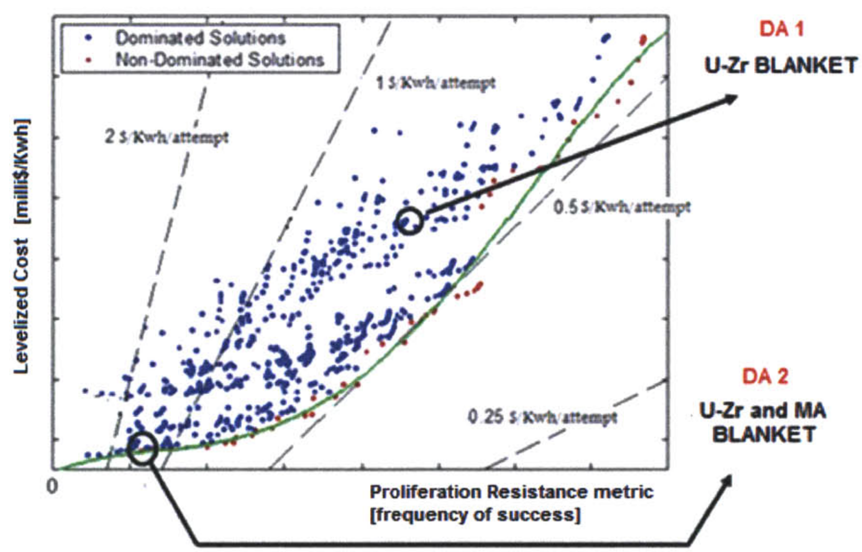


Figure 10: Visual representation of the Pareto method.

---

[8] W. Pareto, Italian economist which studied optimization problems in the field of engineering and microeconomics. The popular *Pareto efficiency* concept is widely used today in various economic optimizations.

CONCLUSIONS

The last examples show evidence of how the holistic approach that we envision would allow one to insert proliferation evaluations within the current design process of nuclear energy systems. If models, acceptance criteria, and design limits are available, the proliferation risk can be quantified and used, under proper conditions, as a measure of performance for a nuclear energy system. If all the suggested features are part of a PRA-like evaluation model, then the calculated proliferation risk becomes a powerful measure of the potential anti-proliferation capabilities of a NES. Furthermore, when such a comprehensive evaluation framework is available, it is possible to use risk to inform the decisions of major stakeholders such as designers, and regulators. Few examples of the model applicability and of how risk information might be used to inform nuclear energy designs are shown. These examples illustrate some features of the framework such as the quantification of the synergic benefits deriving from combined strategies aimed to increase the robustness to proliferation of the NES (i.e., by degrading the quality of SNM and by adding safeguards for the timely detection of specific isotopes). Therefore our preliminary results suggest continuing the development of this framework, and extending the model thus built to other scenarios such as misuse and abrogation. Our current efforts also focus to extend our study beyond the physical boundaries of the facilities and to insert into the framework the institutional barriers such as treaties and agreement. A description of this framework is provided by [14], and it is partially reported in the next Chapter.

REFERENCES

[1] E. Zio, *"Reliability engineering: Old problems and new challenges"*. Reliability Engineering and System Safety 94.125–141, 2009.

[2] U.S. Nuclear Regulatory Commission - Office of Nuclear Regulatory Research' *"Feasibility Study for a Risk-Informed and Performance-Based Regulatory Structure for Future Plant Licensing"*. NUREG-1860. Washington, DC, December 2007.

[3] Apostolakis et al.: *"SFR Project Narrative"*. June 2007 - June 30, 2008".

[4] Department of Energy, *"Generation IV Roadmap - R&D Scope Report for Liquid Metal Cooled Reactor Systems"*. GIF 005-00, DOE 2002.

[5] H. Ham and M. W. Golay, *"An integrated Methodology for Quantitative Assessment of proliferation Resistance of Advanced Nuclear Systems Using Probabilistic Methods"*. CANES PhD Thesis, MIT-NFC-TR-084, May 2006.

[6] Y. I. Chang, P. J. Finck, and C. Grandy, *"Advanced Burner Test Reactor Preconceptual Design Report"*. Argonne National Laboratory. Nuclear Engineering Division: ANL-ABR-1 (ANL-AFCI-173), September 5 2006.

[7] Bryan K. Smith and O. L. de Weck, *"Definition, Expansion and Screening of Architectures for Planetary Exploration Class Nuclear Electric Propulsion and Power Systems"*. MS in Engineering and Management, MIT, 2003.

[8] Apostolakis et al., *"Internal 3rd Quarterly Report for the project: Risk-Informed Balancing of Safety, Non-Proliferation, and Economics for the Sodium-Cooled Fast Reactor (SFR)"*. April 1 - June 30, 2008".

[9] W. Bertozzi, S. E. Korbly, R. J. Ledoux, *"Nuclear Resonance Fluorescence and effective Z determination applied to detection and imaging of special nuclear material, explosives, toxic substances and contraband"*. Nuclear Instruments and Methods in Physics Research B 261 pp. 331-336, 2007.

[10] M. Saito et al., *"Development of methodology for Plutonium Categorization (II) – Improvements of Evaluation Function "Attractiveness– "*. Reactor Physics Book, pp. 669 Tokyo Institute of Technology, 2008.

[11] Nicolas Stauff, 2008 Master Thesis, *"Resolution of proliferation issues for a SFR blanket"*. MIT Nuclear Science and Engineering Department and Ecole Supelec.

[12] M.J. Lineberry et al., *"Commercial-size IFR Fuel Cycle Facility: Conceptual Design and Cost Estimate"*. ANL, Argonne, Illinois 60439 -1985. DOE contract N. W-31-109-Eng-38.

[13] GIF/Economic Modeling Working Group. *User's Manual for G4ECONS Version 2.0.* OECD Nuclear Energy Agency for the Gen IV International Forum. March 2008.

[14] E. Cavalieri d'Oro and M. W. Golay, *"Applying Lessons From Nuclear Safety to Structure a Risk-Informed Framework for Proliferation"*. Nuclear technology - PR&PP special issue, paper under revision.

PART II: THE SAFETY ANALOGY

This Section describes the analysis that was done to create a similitude between the methods and the criteria used in nuclear safety to address safety risks, and the corresponding ones under development in the area of nuclear security, and non-proliferation to respectively address security and acquisition risks.

These three domains (safety, security, and non-proliferation) are examined one by one and major similitude and differences are identified. This analysis brought to major conclusion utilized later in this work to define the assessment model and the criteria we developed to evaluate and limit the proliferation risks associated with nuclear energy systems.

Key highlights and conclusions derived from the safety analogy study are:

- The principles of safety can be helpful in defining those for preventing proliferation;
- The goals of safety differ clearly from those of preventing proliferation;
- The consequences for proliferation are delayed and are not local to the NES;
- Barriers in safety and proliferation are conceived differently;
- Methods for assessing proliferation risks need to be developed further;
- Risk-information and PRA analysis are needed to systemically analyze proliferation scenarios.

The terminology used by other relevant analyses in this field was reviewed in view of the approach we established here, we then preferred to use terms such as:

- "Proliferation performance" instead of "proliferation resistance" which seems to recall to the existence of a maximum value of acceptable risk, and which does not immediately recalls the resistance to acquisition;
- "Acquisition threats" to group all the possible scenario sharing the intent to acquire covertly or to covertly prepare to acquisition;
- "Active" and "passive" as are used for safety, and to avoid expressions such as "intrinsic" or "extrinsic" which imply conclusions about the performance;
- "3S", or "safeguards by design" were avoided despite referring to concepts such as the inclusion of safeguard systems, or the combination of safety, security, and safeguards metrics in the early design of nuclear facility, to avoid confusion between domains that, with respect of our analysis, have to remain separate at least during the evaluation process.

The key conclusion derived from the safety analogy is that the consequences of acquisition threats have to be considered in terms of amount of mass acquired, similarly to a PSA level 1 analysis of safety.

A. EXTENDING THE SAFETY PARADIGM TO PROLIFERATION

The domain of safety was progressively built around the concept of radioactive material transport. The continuous advancements of safety assessment techniques and safety systems are both anchored to the unchanged principle that the cause and the effects of an accident in a nuclear site are respectively due to radiation and to the measured effects that it potentially generates on humans. The theory of radiation transport is the underlying mechanism used in safety analysis, which allows to relate the causes of an accidental release of radioactive material to the consequences it might have on human's health and safety. The nuclear safety discipline coherently developed around the founding principle that the threat was radiation, and the focuses of the scientific community and regulators converged toward reinforcing transport analysis codes, and regulating the maximum admissible consequences to humans exposed to radiation release. The advancements of science and technology, as well as the understanding of complex phenomena and systems, led to gradual increase of the comprehension of the technology-policy system that is in place today.

The proliferation discipline did not benefit of the same coherent development. Proliferation initially did not build its foundations around a science theory such as radiation transport but rather grew within the more broad domain of political sciences and diplomacy. After the discovery of nuclear energy and during the cold war period, the main focus was to avoid states to adopt nuclear weapons. Therefore the field structured around the need of institutional policies for the prevention of the spread of nuclear weapons. Into this framework the attention given to the potential spread of knowledge, materials and technologies associated with NESs was very limited. After the cold war period, the attention for this aspect reinforced after many states, such as India, Israel, and more recently, North Korea and Iran, proved that the development of a nuclear weapon program can initiate from the civilian use of nuclear energy. To analyze the differences and explore the common basis between these two disciplines, a third intermediate and cross sectional discipline has to be introduced, and that is security. Instead of considering the realm of proliferation as a sub set of security, we propose to treat safety, security and proliferation as three distinct domains. The insights obtained from this categorization are reported by Table 2 and synthesized next. Henceforth the analogy between safety, security and proliferation is supported by explaining each of the rows, or key metrics, of the table reported by.

Key metric	Safety		Security	Proliferation
Provenience	Internal accident	External accident	External attack	Internal attack
Cause	Stochastic, or unintentional event		Intentional, agent based event	
Outcome/ motivation	Dispersion of radioactive material		Attacking the target	Material/info acquisition
Scenario/ threat	*Design basis accident (DBA)* • Loss of coolant accident (LOCA) • Other *Beyond design basis accident* • Small LOCA • Other	*External events:* • Earth quake • Accidental plane crash • Fire • Other	*Design basis threats (DBT)* • Intentional plane crash • Cyber attack • Radiological Sabotage • Theft of material/info • Other	*Acquisition threats (ADBT)* • Theft/ Diversion • Misuse • NPT abrogation or breakout
Consequence	Human health and safety for people close or within the NES		Human health and safety Publicity, harm to NES, economic disruption, etc.	Acquisition of special nuclear materials
Barrier/ counter measure	*Passive counter measures:* • Material • NES operating conditions • Systems based on natural phenomena *Active counter measures:* • Physical Barriers • Safety systems • Human procedures		*Passive counter measures:* • Material • NES Technology *Active counter measures:* • Physical protection systems • Human procedures • Institutional tools	*Passive counter measures:* • Material • NES Technology *Active counter measures:* • Detection systems • Human procedures • Institutional tools
Assessment method	Deterministic analysis, Probabilistic Risk Assessment, Test and experiments.	Deterministic analysis, Test and experiments, Simulations.	Human simulations, Game theory, Data generated scenarios,	Qualitative analysis, Game theory, Markov chain, PRA techniques.

Table 2. A visualization portraying the different domains of safety, security, and proliferation.

Causes: motivations and outcomes

For safety, the threats are the accidents, or unpredictable events of random nature potentially leading to core damage. The cause of safety accident is then stochastic by definition which means that a nuclear system lose control only due to the occurrence of a series of events that are of random nature. Human driven actions in the course of an already initiated sequence might concur favorably to its realization. All the sequences that create core damage are the outcomes of interest for a serious accident, or an accidental sequence leading to harm to the NES or to the people within and outside the NES.

For security and proliferation, the outcome is intentionally driven by a human, thus it is not random. The motivations are different in the two cases; for security, the motivation is to harm the targeted NES, while that of a proliferator is to acquire the material, the information, or the capabilities necessary for his ultimate scope of building a nuclear weapon device. To the contrary, the scopes of a 'security violator' are broader than those of a proliferator and change from situation to situation.

Scenarios and threats

In the domain of safety any sequence of events leading to a severe outcome is called accident, or scenario. On opposite for security, the sequences are called threats, driven by the malicious intent of humans. In the domain of proliferation it is the current practice to also use the word threat. However, while the labeling is correct since proliferation sequences are agent based, it is worth noting that their scope is acquisition of material, or information and not to harm the NES site.

In general, a sequence of events constitutes a pathway to the realization of the ultimate event that in the table we term as outcome. Each sequence is driven by an initiating event, that is the event from which an accident or a threat starts, like the starting of a fire, or swapping of a fuel bundle with a dummy one.

The identification of the sequences to be considered is of primary importance to determine the vulnerabilities of the NES and to consequently add adequate protection systems to it. However, the sequences are potentially infinite and the analyst has to establish criteria for deciding which ones are more relevant.

Safety analysis, during its early stage of development when probabilistic risk assessment (PRA) was not yet available, grouped under the name of Designed Basis Accidents (DBA) [1] that set of deterministic scenarios which the NES, and its subsystems must withstand without releasing any harmful amounts of radioactivity to the outside environment[9]. This means that amongst all possible sequences, analysts and regulators decided to investigate those leading to the most severe consequences, even though potentially they are very unlikely to occur. The driving criterion at that time was that protecting the NES and humans from the worst postulated accident was also implicitly going to protect them from less catastrophic, and more likely accidents. Based upon their expertise and knowledge, analysts and regulators formulated a set of scenarios covering all of the possible factors potentially leading to undesirable consequences and protected nuclear plants so to prevent these events from initiating. So for example, considering a standard power plant technology using a light water reactor, the plant in order to be licensed need show that it can withstand a loss of coolant accident (LOCA). The DBA of a LOCA is designed according to a prescribed list of failures based upon past experience and judgment.

Once Probabilistic safety assessment was introduced [3], computer codes allowed to consider all the scenarios and to select the ones with the higher combination of consequences and probability to occur, in other words the riskier ones.

---

[9] More serious accidents that may involve significant core degradation and/or pose the real danger of a significant release of radiation to the environment were later on (i.e., after the three mile islands accident) classified as beyond DBA or severe accidents.

Table 2, in the security portion under scenarios and threats, reports the wording design basis threats (DBT). This nomenclature if properly adopted from safety would define DBTs as the set of postulated threats to which the NES, and its subsystems must withstand for different types of attacks without leading to the successful realization of the attack, thus without leading to any harm to humans and to the structures of the NES. Whether this definition was extended correctly or not to security analysis is not our concern. However, if the term design basis scenario has to be imported from the safety to the security domain, we want to be sure that to its domain of applicability are also being adopted and some of its limitations understood. If we want to use the analogy with safety it has to be kept in mind the concept of DBA is carrying the following features and constraints:

- It refers to a set of deterministic and stylized accidents postulated by experts who sometime used very unphysical assumptions or set variables to their most pessimistic value;
- It is designed using expert's judgment, analysts' experience, and knowledge;
- The mitigation system designed to prevent its occurrence and not set to reduce the associated consequences but rather to prevent the accident to start;
- Its use is not appropriate in a probabilistic formulation using risk because no probabilities of frequencies can be quantified and associated with the consequences of the selected scenarios.

These peculiar characteristics and limitations are such that the use of DBAs in safety, while maintained in the current US regulatory body for historical reasons, was complemented and substituted by PSA techniques. In the case of security, the DBT concept is then useful to guide designers throughout a comprehension of the different threats posed by a malicious act to the system. Since the evolution of assessment techniques in this field has not still reached the level of maturity and of consensus required, the use of deterministic sequences to characterize the threats is satisfactory. However, DBTs for security and proliferation as it is for safety, by definition are limited to the view of their creator who might dismiss some sequences; accidents and pathway to proliferation might evolve in unusual ways and far from the mental models of designers and regulators.

Thus the DBT classification will not find alternatives until risk assessment method for security and proliferation will be introduced as standard evaluation techniques.

A final aspect to mention is the relevance that some categories of scenarios acquired over time due to the contingent happening of some historical events. Table 2 reports some categories of accidents or threats that in the last years gained a special relevance and consideration as due to the occurrence of some facts. Some of these examples will be recalled in the thesis to explain relevant aspects of the discussion.

Consequences

The consequence and the different levels of protection are two interrelated topics and the understanding of one requires the other. We consider consequences by examining the various layers required of protection of the NES for three different types of scenarios, one for each of the three domains analyzed.

Initially consider a typical accidental sequence. The evolution of a severe accidental sequence, such as a loss of coolant accident (LOCA) that affects, or takes place in the core of a nuclear power plant. Any other accident not involving or starting from the core is not considered a relevant nuclear accident, but a traditional safety occurrence. The dominant accident phenomenon is nuclear radioactive material transport, and 'tracking' of such material is equivalent to following the trajectory of the accident. The material, does not know which barriers it will encounter on its pathway and for this reason, the accident develops from the inner part of the plant propagating trough the last one, the containment building. The first barrier to transport is the fuel bundle that is designed to retain the radioactive material. If this barrier should accidentally fail and all mitigations systems also fail, the plant could suffer a structural damage. The consequences in this case are represented by the structural damage of the core.

However, in case a core damage accident evolves, the radioactive material may reach the next barrier, represented by the reactor vessel. If this next barrier should fail, and other special circumstances occur, the radioactive material might reach the environment, either within or outside the plant. In such an event, the damage can reach not only the structures but also the workers. Therefore, beyond this second serial level of protection, the consequences might be also measured in terms of harm to workers on site, and to the public offsite.

Power plants are designed to prevent harm to public and to shield operators during such highly improbable event. As the radioactive material moves to and trough the containment, the probability of successful transport decreases progressively and the uncertainty of such outcomes increases, as each step outward adds to cumulative uncertainty of all of the previous steps. Assuming that the radiation successfully travels beyond the containment barrier, it then reaches the external environment and if abundant and harmful, it can reach the population located out of the plant. In this case the consequences are measured as functions of the injuries and fatalities that radiation might cause around a plant. The top graph of Figure 11 reports this stylized evolution of the accident marking as at every stage of the plant's physical protection system, or barrier, a different type of consequence. Each consequence is evaluated depending on what and whom the radiation finds on its pathway. This unidirectional scenario evolution is the one hypnotized for an internal accident and the reverse mechanism for an external sequence is not for the moment considered to support our analogy.

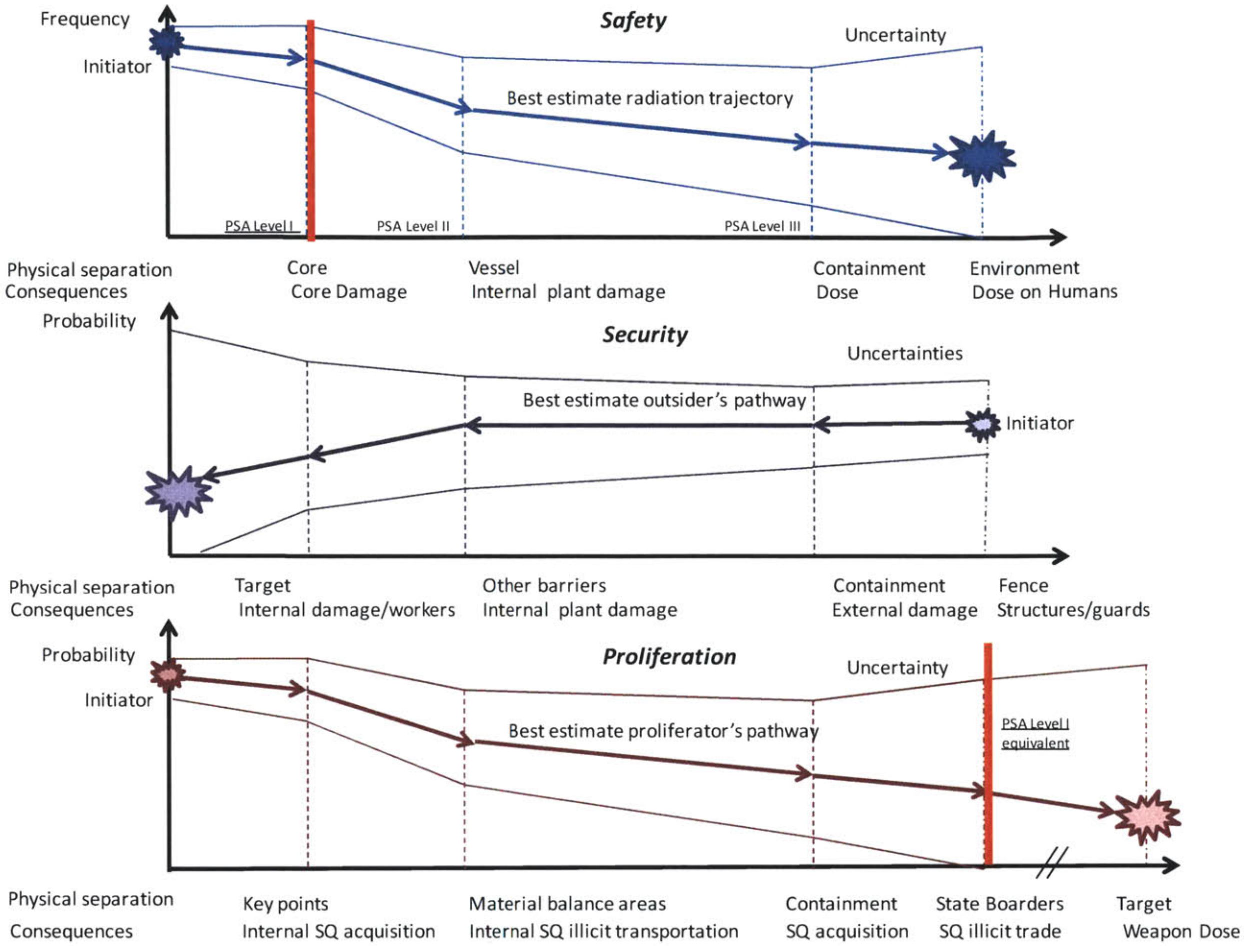


Figure 11. Illustrative representation of accident and malicious acts trajectories. A declining arrowed line shows the probability of success and the outer boundaries show the associated increase of uncertainty. During the progressions also the consequences changes as different physical distances are reached.

Most of the regulations for safety focus on the first barrier, to avoid core damage, or after the third barrier, to plan evacuation and prevent fatalities. However most of the calculations are executed in the first stage of the accident, to prevent and mitigate it, and also because the uncertainties are lower.

The second graph of the figure, again using a simplified representation, recalls the evolutions of two security threats. The first one, from left to right, by means of an insider, the second from an outsider. There are broad categories of security threats, and while we realize some of them do not imply a physical violation of the plant, such as cyber attacks, or others do not involve individuals entering the plant such as stand-off attacks, we here picture a case of armed intrusion for its most immediate analogy with the safety case. So, in case of an armed intrusion, with any purpose between pure disruption and any secondary intent such as material theft, the pathway of the intruder will also face different barriers in correspondence of which a different type of consequence can be measured. While the analogy with the safety case stands up under many aspects, for example the progressive increase in the uncertainty to hit the target after more layers of protection, conversely the trend of consequences passing from physical damage to harm to humans does not find correspondence with the previous case. Given the generality of the example, we can assume that the harm to humans potentially occur in proximity of the target and of the outer perimeter of the NES. However, for both cases, intrusion or outsiders, the consequences still change in proximity of a defense barrier and they vary from physical disruption, to deaths, which in this case are circumscribed to the onsite population.

The same type of evidence can also be found in the third example in the lower graph of the figure, where the pathway of proliferator is taken into consideration. In this case, concealed theft of a significant quantity (i.e., a quantity of fissile material potentially sufficient to derive a nuclear weapon) of special nuclear materials from a bribed operator is assumed. The pathway to proliferation passes then throughout a series of barriers that are not necessarily just physical. Again, thinking about a model describing the sequence, the uncertainties increase as we move from the initial acquisition event to the ultimate delivery of the fissile material to another state or criminal organization commissioning the threat. As it will be explained in detail in the next section, in this case the consequences are by any mean related to either physical measurable damage or fatalities on site. The action of a proliferator, in this case is clandestine by its nature and the consequences are not immediately amenable to fatalities.

This last example suggests two major differences between the three cases: the first, and discussed in more detail in the next section, is that the barriers for proliferation are not necessarily just physical. The second is that proliferation scenarios do not in general involve fatalities in any of the stages of protection of the NES. Fatalities as a consequence of a successful realization of an acquisition can be found after all the barriers to proliferation are covertly bypassed, thus far in distance and also in time from the NES. This last observation suggest that measuring proliferation pathways in terms of the potential final disruption generated by a nuclear weapon is not a good way to measure the consequences. By looking at the scale of consequences of the example used in Figure 11, it is evident how, differently from what we observed for safety and security, proliferation pathways break the spatial correlation existing between the barriers and the consequences. Although the ultimate outcome of a proliferator action is the spread of nuclear weapon development, it is more convenient and efficient to measure the outcome as a potential spread of material.

This approach is equivalent to the safety approach [1], which focus its attention on the first layer of protection (i.e., PSA Level I analysis) where the uncertainties of the sequences are modest. This approach might rise the doubts of those who believe that arresting the evaluation to material acquisition exclude from the equation the proliferator's weapon capabilities, such as his ability to assemble the weapon. However, these types of statements would be correct from a safeguarder perspective. Our approach indeed is valid from a proliferator's standpoint; the proliferator's behavior not necessary is a rational one. He would in fact act knowing a priori his weapon capabilities, or back-to-front he will pursue a proliferation attempt simply based on contingent facts, such as the opportunity to successfully acquire material and information in that very moment. Measuring the consequences in terms of material acquisition, or amount of material acquired in a proliferation attempt, would then consider these irrational behaviors and set a more conservative approach in the analysis.

Counter measures and barriers

Barriers have different functions and natures. In nuclear safety barriers are designed to prevent and mitigate the effects of radiation, and they are mainly constituted by physical systems, in some cases assisted by human procedures. Material properties in safety are seen as physical impediment thus as a barrier too.

Safety Transport of radiation	**Security** Transport of humans/material/info	**Proliferation** Transport of fissile material	*Proliferation Threat*
Prevention barrier	**Prevention measures** Espionage, surveillance outside the NES, leak of information	**Material composition degradation** • Minor actinides doping, Plutonium degradation, no blankets, etc. **Facility robustness design** • Physical resistance and robustness of the NES design	Diversion, theft Diversion, theft, misuse
	Detection measures •Detection and alarm systems (i.e., signaling breeches and violations) •Surveillance systems •Sentinels	**Technological counter measures** •Detection and alert systems •Measurement systems •Monitoring systems • Algorithms to integrate all above functions	Diversion, theft Diversion, theft Diversion, theft, misuse
Protection barrier	**Physical impediments** walls, fences, firewalls, etc.	**Physical barriers**	Diversion, theft
Mitigation systems	**Response activities** Human procedures of armed guards, military forces, etc.	**Institutional counter measures** • *Treaties and agreement* o Verification of facility design conformed to its declared purpose o Nuclear material accountancy to measure/verify SNMs o Inspections and oversight of site and records o Containment & Surveillance, monitoring • *Independent verifications* o Additional protocol o INFCIRC 1540, etc. • *Enforcements from governments and states* • *Commercial and legal arrangements* • *Special cases of limited use agreements*	Diversion, theft, misuse Diversion, theft, misuse, NPT abrogation Illicit cooperation Illicit trade
	Delay barriers	**Punitive measures** o Sanctions o Embargo	Diversion, misuse, NPT abrogation
Accommodation barrier	N.A.	N.A.	

Passive barrier	Active barrier

Table 3. Counter measures and protection systems used for safety, security and proliferation.

In security, protection systems in general have a purely physical connotation.

In case of proliferation the definition of barriers takes into account not only physical systems and material properties but also institutional counter measures such as treaties and agreements.

A useful strategy in improving safety is use of multiple levels of protection for the defense of a NES. By analogy one may attempt to use this formulation in emphasizing the differences between safety and proliferation barriers.

The principle, termed "Defense in Depth" (DiD), states that the barriers have to be independent, preferably relying on different mitigation principles, and not necessarily designed accordingly to barrier's performance. This last point means that the DiD philosophy, as it was used in the early development of nuclear safety, by adopting it from military strategy, does not have a precise safety goal and denotes a multi-layer approach thought to provide protection from sequences excluded explicitly from the design basis of the safety analysis.

An important aspect of this approach is that it is grounded to the concepts of physical distance. It then assumes that the reactor core is the unique critical point around which multi-layer barriers are disposed concentrically to prevent and mitigate accidental effects.

For proliferation, this last set of assumptions is not really valid. First because in case of a NES, there is more than one critical point, or acquisition point rather than the core. Therefore, the definition of serial barriers is seen to be less appropriate in the proliferation domain, and the barriers cannot be seen as concentric. Secondly, the directions of a proliferator's pathway are not randomly determined, but rather have preferred directional routes, seeking weaknesses in the barrier system. Finally, the rationale of functions for which anti proliferation barriers are designed are different from those used for safety. This is the case of institutional barriers to proliferation, which might seek to delay rather than prevent the advance of an attacker seeking to acquire SNM from the NES. In addition, not all the counter measures used by the current non-proliferation regime are able, and designed to, withstand efficiently to all the acquisition threats. For example, the current regime is particularly vulnerable, if not incapable, to react to the occurrence of States withdrawing from the NPT. We call this scenario NPT abrogation, or break out, and we discuss it next.

Because of all these differences between proliferation and safety, a way to approach the role of the actual counter measures, or barriers to risk, is to analyze the function for which they were designed. Together with the function of the barrier we also decided to report the mechanism which drives the barrier; if the barrier is capable to self react to a threat then it is a passive barrier. Barriers relying on human intervention or requiring the assistance of human driven actions or organizations are called active barriers.

Once again, the proposed classification is adopted from nuclear safety and reflects the discussion that drove the introduction of self actuating barriers to radiation transport after the Three Miles Island in the US [5].

Table 3 reports the functional classification of the barriers employed by the three domains analyzed. The functions marked in gray are classified as passive features, while the one marked in white are active ones. The classification used for proliferation barriers used in the table is derived from the standard functions which characterize the safety barriers of a nuclear power plant:

- Prevention barrier (passive);
- Protection barrier (passive);
- Mitigation (passive and active);
- Accommodation (passive, and active).

This classification plays an important role if a framework addressing the proliferation risk has to be created. Knowing the function of a barrier it is in fact a key aspect for the evaluation of its performance.

Assessment Methods

The probabilistic approach used in safety analysis provides a rational framework and it is useful to cast our study of safety, security and proliferation in those terms. Probabilistic Safety Analysis (PSA) seeks to categorize each event by probability of occurrence and then to demonstrate that certain criteria are met. PSAs therefore proceed using the following methodology:

- Generate a set of accidents to consider,
- Predict the frequency and consequences of the event,
- Define the acceptance criteria,
- Show that the appropriate risk-based criteria are met.

Although the establishment of a similar analysis to assess the proliferation risk is viable and witnessed by presence of different approaches[10] a real complete risk assessment method which includes all the possible counter measures to nuclear proliferation was not fully developed yet. The next section of this thesis focuses on the integrated method that we developed in our work, showing also what are the issues related to the quantification risk that we obtained from our simulations.

---

[10] Non-proliferation models available in the literature are: the US department of Energy (DOE)' TOPS analysis, Generation IV international forum (GIF)'s PR&PP evaluation (2006) [6], IAEA's INPRO (2007) [7], National Nuclear Security Administration [8] and W. Charlton et al. (2006)'s Multi-attribute Utility Analysis (MAUA)-based study [9], and R.A. Bari's Markov Chains [10], and the Sandia Risk-informed proliferation analysis [11].

Discussion part A

This concludes the first part of this chapter where an analogy between safety, and proliferation was carried out either to set the stage of current evaluations methods used in proliferation and for security with the respect of the analogous ones used by safety analysis. Security was also considered a in intermediate domain useful to bridge the two domains under investigation. We conclude that partial analogies exist relating safety and proliferation, but not security. Regarding the analogy existing between safety and proliferation we observe that:

- The principles of safety can be helpful in defining those for preventing proliferation;
- The goals of safety differ clearly from those of preventing proliferation;
- The consequences for proliferation are delayed and are not local to the NES;
- Barriers in safety and proliferation are conceived differently;
- Methods for assessing proliferation risks need to be developed further;
- Risk-information and PRA analysis are required for proliferation.

The next sections deals with this last aspect and present the risk-informed framework that we developed using our underlying analogy between safety and proliferation.

B. RISK INFORMED FRAMEWORK FOR SECURITY AND PROLIFERATION

As we saw different and complementary principles dominate the treatments of nuclear safety. Another fundamental principle is that it can be beneficial to risk-inform the design of the NES, as a means of seeking improvements. This section extends this concept to nuclear proliferation and provides the bases for evaluating the NES in terms of proliferation risks.

Proliferation Model

This section describes the features of the risk-informed method used to assess proliferation risks of NESs. Combining the model with opportune policies, results into a risk-informed framework.

The model we built captures the competition between two actors within a nuclear facility, one aiming to acquire nuclear materials illicitly, and the other aiming to protect the same material from being acquired.

The model, built to assess the proliferation features of a generic NES, is inspired by the models used in nuclear safety measuring the risk performance, or probabilistic performance assessments (PRAs). In a similar fashion to PRA assessments, the model we formulated recreates the spectrum of potential consequences following an initial event driven by an agent called the proliferator. The capability to resist to a proliferation attempt is being evaluated by means of a metric called proliferator success probability, Ps, which determines the ability of a proliferator to acquire SNMs by eluding all the possible barriers designed against their acquisition, including institutional barriers.

The risk evaluated by the model considers the threat of a potential proliferator, for any scenario ranging from theft to abrogation. For instance, in case that diversion is being attempted, the model calculates an estimate of the probability Ps taking into account the probability of acquiring the material from a given location and the probability to transport it out of the NES, without being detected. The following summarizes the relevant features of the model:

1. The risk of proliferation is calculated by means of the overall metric, Ps, which is a estimate of the conditioned probability of SNM acquisition given an attempt, and the consequences associated with each scenario.
2. The risk evaluation, is conducted starting from the computation of sub-metrics considering the characteristics of the NES, the features of the target material, and the difficulties encountered by the proliferator in acquiring and transporting the material out of the NES.
3. The risk evaluation consider also the dynamic interactions of the two competing actors, including the resources they can spend to succeed in their respective missions.
4. The model considers the effects deriving from the addition of different barriers that the safeguarder might use (i.e., physical, institutional, and organizational barriers).
5. The results obtained, including the uncertainties associated with the subjective evaluations of the experts that are used to determine the performance associated with the barrier systems, are transferred into an opportune policy risk space.

As this last statement suggests, providing an assessment model is not sufficient to have a comprehensive framework for non-proliferation, which needs to include acceptance criteria. The role of acceptance criteria is to define the level of acceptability for the risk quantified by the model. Therefore, in parallel to the development of assessment techniques it is necessary to establish limits to the proliferation risk. It is then evident how while the quantification of risk is a problem confined to technical evaluations and methods, the establishment of acceptable risk limits requires social, legal and political into the evaluation. The next section reports the approach we used on this matter.

Proliferation Policies

Once risks are evaluated, acceptance criteria are needed in order to regulate designs and behaviors. Risk informed safety regulations typically [4] classify the risks associated with a given nuclear design in a two dimensional space where an accident scenario is represented by means of its frequency of occurrence and by the associated consequences. Within this space, following the initial representation provided by F. R. Farmer[11], a curve is being traced to delineate the separation between acceptable and non-acceptable scenarios. The acceptability of a scenario is determined by the safety goals imposed by the regulator which in turn are an expression of the level of nuclear power risks that the society is willing to tolerate. If the scenario fall above the curve, its risk is considered intolerable and the configuration of the NES exposed to this scenario needs to be reinforced with appropriate safety barriers.

A similar representation does not exist in the proliferation domain because mature proliferation risk assessment methods have not been developed. In our work we developed such a method and a consistent proliferation acceptance criterion curve.

We formulate risks in terms of conditional success probability, Ps, and of the amount of material acquired in an illicit scenario. We define the amount of SNM acquired as a fraction, or multiple of a significant quantity[12], SQ. Then the product of Ps for the associated SQ value defines the proliferation risk involved in an acquisition attempt.

Section V reports the details of this new representation, here we limit to observe that, as opposed to safety regulations, the SQ scale immediately allows one to directly relate the probability of a threat calculated via our PRA-like analysis, with the consequences associated with the acquisition attempts. This approach permits one to determine the consequences with a lower level of uncertainty than by expressing them in form of dose, or fatalities generated by the detonation of the nuclear explosive device assembled with the acquired material. Recalling the parallelism established with the safety case in Figure 1, evaluating the SQ acquired is equivalent in safety risk analysis to evaluation of the core damage frequency on a site, thus referred as a Level 1 PRA analysis.

Discussion part B

In order to pass from a schematic representation of the threats (i.e., a DBT representation) to a more comprehensive evaluation of all the possible scenarios concurring to the proliferation risks associated with a NES, new assessment techniques for non-proliferation (i.e., PRA techniques) have to be deployed. Although the capability to resist to proliferation threats has been modeled by many authors, a complete framework needs to include compelling performance measures such as the effects generated by the addition of barriers, and the

[11] F. R. Farmer was a regulator working for the UK government known for his contribution to the area of risk assessment. He in fact considered public acceptability of safety risks associated with a NES.

[12] Significant quantity, following the IAEA definition is the approximate quantity of nuclear material in respect of which, taking into account any conversion process involved, the possibility of manufacturing a nuclear explosive device cannot be excluded.

uncertainties in their calculations. In addition, the model becomes a valid decision making tool only when coupled with defined acceptance criteria for the calculated risk. Risk, in case of a proliferation scenario, can be defined by means of the consequences calculated in terms of amount of mass potentially subtracted in an acquisition attempt. The risk representation we propose allows one considering the three different risk contributors (i.e. diversion, misuse, and NPT abrogation) also considering the progressive level of efforts and potential consequences associated with them.

The resulting framework is potentially usable to license NESs in a similar fashion to safety regulations, and it is consistent with regulations currently envisioned to certificate generation IV nuclear designs [2].

CONCLUSIONS

In this Section we linked the safety, security, and proliferation domains. To favor the conversation, and the transition of concepts between these domains we used simplifications, such as the exclusion of internal attacks in acquiring SNMs. We explored some of the key concepts upon which the modern theory of safety was linked to the design and regulation of nuclear energy systems. The concepts that we use emphasized the scenarios and the associated counter measures of each domain, specifically passing through key definitions such as intentions, causes, and consequences. This approach leads one to explore the validity of assumptions for the mental models used to seek commonalities that they might have.

The insights derived from this first part of our analysis were then used to create the ground for the second part of the paper, where the narrative continues explaining how risk information, in the specific case of proliferation, can be used to create evaluation models which are coherent with the mental model proposed by the first part. A brief discussion concludes each of these two section.

It is worth to note that we have avoided or limited the use of words, and sometimes slogans, that are every so often used concerning proliferation, such as "safeguardability", "safeguards by design", "3S", and "proliferation resistance". The recent raising needs to formalize new concepts in the proliferation area, sometimes has led to improvisation of some definitions adopting them from other areas such as safety, resulting in an unstable nomenclature. However, some of these definitions are not supported by the evidence of practice, and sometimes they are so confused that the words lose their value. We have stayed away also from a more traditional nomenclature, thus from words such as "safeguard" that usually defines an active system of protection, but that in many circumstances is being used more broadly to mean both use of passive and active features. We then preferred to use terms such as "active" and "passive" as are used for safety, and to avoid expressions such as "intrinsic" or "extrinsic" which imply conclusions about the performance.

In conclusion, the risk insights offered by an assessment framework built on the safety analogy inform the decision process of major nuclear stakeholders such as designers and regulators by helping them selecting among different design alternatives based on the assessment of their relative non-proliferation performance.

REFERENCES

[1] U.S. Nuclear Regulatory Commission, *"Title 10, Code of Federal Regulations"*. Title 10, Code of Federal Regulations. NRC website directory.

[2] U.S. Nuclear Regulatory Commission, office of nuclear regulatory research, *"Feasibility study for a risk-informed and performance-based regulatory structure for future plant licensing"*. NUREG-1860, December 2008.

[3] Rasmussen, Professor Norman C.; et al. (1975-10). *"Reactor safety study. An assessment of accident risks in U. S. commercial nuclear power plants. Executive Summary."*

[4] NUREG-1150, *"Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants"*. Office of Nuclear Regulatory Research, December 1990.

[5] Walker, J. Samuel, *"Three Mile Island: A Nuclear Crisis in Historical Perspective"*. Berkeley, University of California Press, 2004.

[6] Proliferation Resistance and Physical Protection Evaluation Methodology Expert Group, PR&PP Group: *"Evaluation Methodology for Proliferation Resistance and Physical Protection of Generation IV Nuclear Energy Systems,"* Revision 2, September 30, 2004.

[7] Taylor, J., et al., *"The Technological Opportunities to Increase the Proliferation Resistance of Global Civilian Nuclear Power Systems"*. Report by NERAC Task Force (TOPS), 2000.

[8] NNSA, National Nuclear Security Administration. *Guidelines for the Performance of Nonproliferation Assessments*. PNNL-14294, 2003.

[9] W. S. Charlton et al., *"Proliferation Resistance Assessment Methodology for Nuclear Fuel Cycles"*. Nuclear Technology vol.157 February 2007.

[10] Peterson, P.F., Bari, R., and Roglans, J., *"Assessment Methodology Development for Proliferation Resistance and Physical Protection of Generation IV Systems,"* submitted to Global 2003, November 16-20, 2003.

[11] Rochau, G.E. et al., *"Risk-informed Proliferation Analysis,"* Sandia National Laboratories Report, SAND2001-2020, June 2002.

PART III: ASSESSMENT MODEL

A PRA-like assessment technique has been built starting from a pre-existing evaluation model tested by Ham and Golay in 2006 [1]. The existing evaluating technique was essentially a simple parametric model calculating the proliferator's success probability for diversion within a nuclear power plant. The new model is a fully developed assessment technique capable to evaluate the performance of a NES to resist to proliferation. The model calculates a metric complementary to the proliferation resistance of a NES to a set of potential threats. The proliferation risk is evaluated for each of scenario by coupling the calculated probability with its associated consequences. Each NES can be then expressed in term of the risks associated with the three fundamental threats. The threat for proliferation is the acquisition of SNMs. The amount of material potentially acquirable by means of a proliferation threat set its consequences. By representing a given NES throughout the risk associated with a proliferation threat, it is possible to evaluate the performance variations when additional protection systems are added to the basic design. The effectiveness of the supplementary barriers is expressed in terms of risk variations, or measures of risk importance. By adding new features, and by protecting them adequately from the threaten of supportive tactics aimed to reduce their effectiveness, the anti-proliferation performance of the NES rises and with it also the cost associated with its protection. The assessment can then be used to determine optimal cost-benefits points, to identify the most beneficial, or less risky, combinations of design features and protection systems. In other words the model allows to risk-inform nuclear energy systems. If appropriate risk acceptance criteria are going to be deployed, the resulting framework can ultimately be used to license NESs from a proliferation performance perspective.

THE OBJECTIVE: SPECIAL NUCLEAR MATERIALS

Definition of Special Nuclear Materials

Nuclear Reactors produce power by burning a special fuel made of nuclear materials. The nuclear material contained in a fresh fuel element is called fissile material. A fissile material is an heavy element that can fission under certain circumstances, which are being created within the reactor core. When a fission occurs, power is produced. Those materials that are capable to fission, and that thus having a critical mass, are also called special nuclear materials (SNM). These materials, if extracted from a reactor and processed in opportune ways, can be used to build a nuclear weapon device (NWD).

The objective of a proliferator is to acquire the SNMs that are present into any of the stages of a nuclear fuel cycle. The nuclear reactor represents one of the many possible stages of a nuclear fuel cycle. Other possible stages are for a closed fuel cycle: reprocessing, transportation, fabrication and fuel waste deposits.

Special nuclear materials are defined by Title I of the Atomic Energy Act of 1954 as: *"plutonium, uranium-233, or uranium enriched in the isotopes uranium-233 or uranium-235".* The definition includes any other material that the Nuclear Regulatory Commission (NRC) determines to be special nuclear material, but does not include source material. The NRC has not declared any other material as SNM [2]. An objection that groups, such as the union of concerned scientist have expressed in the past, is that also other fissile materials such as Thorium, Americium, and Neptunium, and sometimes abundantly present in nuclear fuels, can be used for a NWD and therefore they should be included in the SNM classification.

Source and special nuclear material, production facilities, and utilization facilities are affected with the public interest, and regulation by the United States of the production and utilization of atomic energy and of the facilities used in connection therewith is necessary in the national interest to assure the common defense and security and to protect the health and safety of the public. This statement refers to the motivations pushing the NRC to define the SNM categorization and to protect the SNM when above certain quantities. Also in this case, the Union of Concerned Scientist, in more than occasion, expressed concerns about the classification that the NRC established in order to define the requirements of the safeguards chosen to protect the locations containing SNMs. The concern, has been that the amounts of material defined by the NRC that set the different safeguard categories are different from the amounts chosen by the IAEA and by the DoE [4]. These concern however are not justifiable since the two criteria used to define SNM and SQ, are different. In fact the amounts of SNM to which the NRC refers to are intended for domestic protection via safeguards. The SQ amount defined by the IAEA is instead a proxy for critical mass.

Special nuclear material is only mildly radioactive, but it includes some fissile material (uranium-233, uranium-235, and plutonium-239) that, in concentrated form, can be the primary ingredients of nuclear explosives. These materials, in amounts greater than formula quantities indicated by the NRC classification, are defined as strategic special nuclear material (SSNM).

Quantity of nuclear materials

According to the IAEA glossary guide [3], the amount of material that is considered to be of interest for the construction of a nuclear weapon device is equal to a Significant quantity (SQ) defined as *"the approximate amount of nuclear material for which the possibility of manufacturing a nuclear explosive device cannot be excluded".* Significant quantities take into account unavoidable losses due to conversion and manufacturing processes and should not be confused with critical masses. Significant quantities are used in establishing the quantity component of the IAEA inspection goals. Significant quantity values currently in use are reported in Table 4.

Table 4: SIGNIFICANT QUANTITIES (IAEA)

Material	SQ
Direct use nuclear material	
Pu [a]	8 kg Pu
^{233}U	8 kg ^{233}U
HEU ($^{235}U \geq 20\%$)	25 kg ^{235}U
Indirect use nuclear material	
U ($^{235}U < 20\%$) [b]	75 kg ^{235}U (or 10 t natural U or 20 t depleted U)
Th	20 t Th

[a] For Pu containing less than 80% ^{238}Pu.
[b] Including low enriched, natural and depleted uranium.

Quality of nuclear materials

The quality of the nuclear material, that from now on is going to be defined as SNM, that is strategic for the construction of a nuclear weapon device, is also of primary importance. In order to describe Uranium and Plutonium qualities it is necessary to consider the entire life cycle of production of nuclear device. For instance, an uranium mixture, when above the 20% enrichment level, becomes weapon usable material (WUM). When the percentage of enrichment arrives above the 80-90% then the material is defined as weapon grade (WG), which means it has a quality level to be used directly in a NWD, such a gun bomb.

As shown in Figure 12, Plutonium mixtures are more complicated than uranium ones since they include more isotope species. Also in this case the fissile element is the pivotal element to consider for the creation of a NWD. High level of Pu-239 are desired to have weapon grade Pu. However, the definition of WG Pu also considers the percentages of pu-240 and Pu-238; if their concentrations are low, then the overall mixture can be used directly in a NWD.

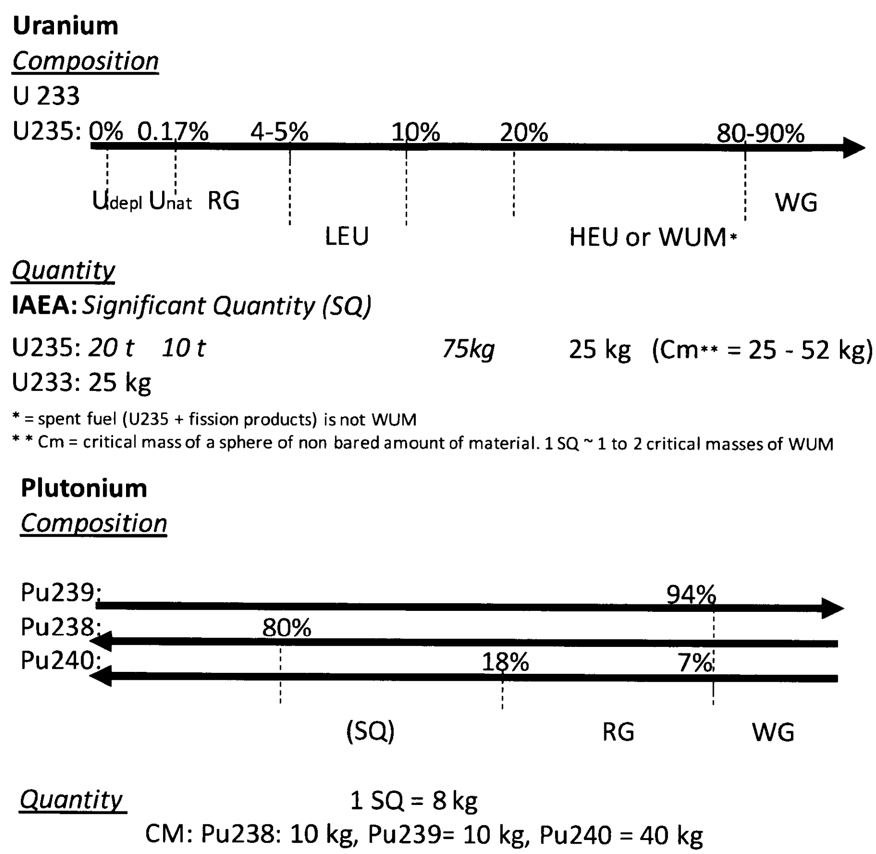
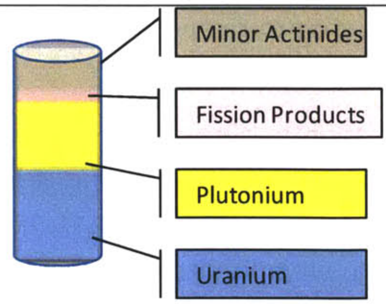


Figure 12. Definitions used to define the various "qualities" of Plutonium and Uranium mixes.

The material target for a proliferator trying to acquire materials for assembling a nuclear weapon device is the fissile material contained into SFR fuel elements located in the SFR power plant. While the above figure graphically reports the definitions and various categories into which Plutonium and Uranium are classified accordingly to IAEA, the following table reports the labeling and the color used for the different isotopic species considered in this study. It is worth to note that while the framework we built is valid for each fissile material, for this dissertation plutonium (marked in yellow) was selected as the main and most relevant SNM.

Table 5. Agenda showing the fuel composition labeling and colors used in this study.



Fuel Element schematic	***Color***	***Isotopes***
	Brown	Minor Actinides or TRU mixture including also the Neptunium and Americium
	Pink	Fission Products: Strontium, Cesium, Beryllium, etc.
	Yellow	Plutonium: Pu238, Pu239, Pu240, Pu241, Pu242
	Blue	Uranium: U238, Udepl, U235, U233

Scenarios determining the proliferation risk

Ideally, a regulatory framework in place to assess the proliferation performance of a nuclear energy system, should be able to demonstrate the degree of vulnerability of a facility to any plausible threat. This vulnerability analysis should be included in the current licensing process for nuclear plants and also be part of the design process of nuclear power plant designers.

Any action aimed to the concealed and illicit acquisition of nuclear materials within a NES is conceived as an acquisition attempt. The tree material acquisition scenarios considered in this study do not lead to the creation of fatalities near or within the NES site, they cannot be conceived as threats but simply as acquisition attempts.

A scenario is the entire set of actions required by a proliferator in order to complete successfully an acquisition attempt. This study identified three main potential scenarios sharing the common ultimate goal to acquire relevant amounts of SNMs, and these are diversion or theft, misuse, and abrogation.

The union of the risk components associated with these three scenarios, and of its variants (i.e., theft and misuse, misuse and then break-out), constitute and cover the spectrum of proliferation risks to which a NES can be exposed.

The risks associated with these three scenarios differ by the modality of acquisition chosen by the proliferator, by the organizational effort required to succeed in each scenario, and by the different tactics used to support the selected acquisition modality.

The diagram of Figure 13 shows how the amount of material obtainable per attempt, the level of organizational capability required for each scenario (i.e., people required to successfully acquire SNMs from a NPP), and the tactics used to support each scenario progressively increase from left to right. The resources that the proliferator needs to devote (i.e. amount of money spent by the proliferator to succeed in the attempt) to pass from a diversion scenario to misuse, or from misuse to abrogation, also increase in a similar fashion. All these factors increase proportionally with the amount of material potentially acquirable for each scenario. If we measure the material mass in units of nuclear weapons potentially deployable (i.e., the number of significant quantity) we can immediately relate the scenarios to the potential consequences that can be generated when succeeding.

It is worth to note that the observed trend from diversion to abrogation is obvious when material mass is involved. However, there is not such obvious trend when the risk (i.e., the probability to succeed in an acquisition attempt multiplied by its consequences) is considered; pathways to proliferation originate from the intention to acquire nuclear material sufficiently to build, at least, one nuclear explosive device via one or more consecutive acquisition attempts, and not from a risk evaluation. These three scenarios are discussed in detail below.

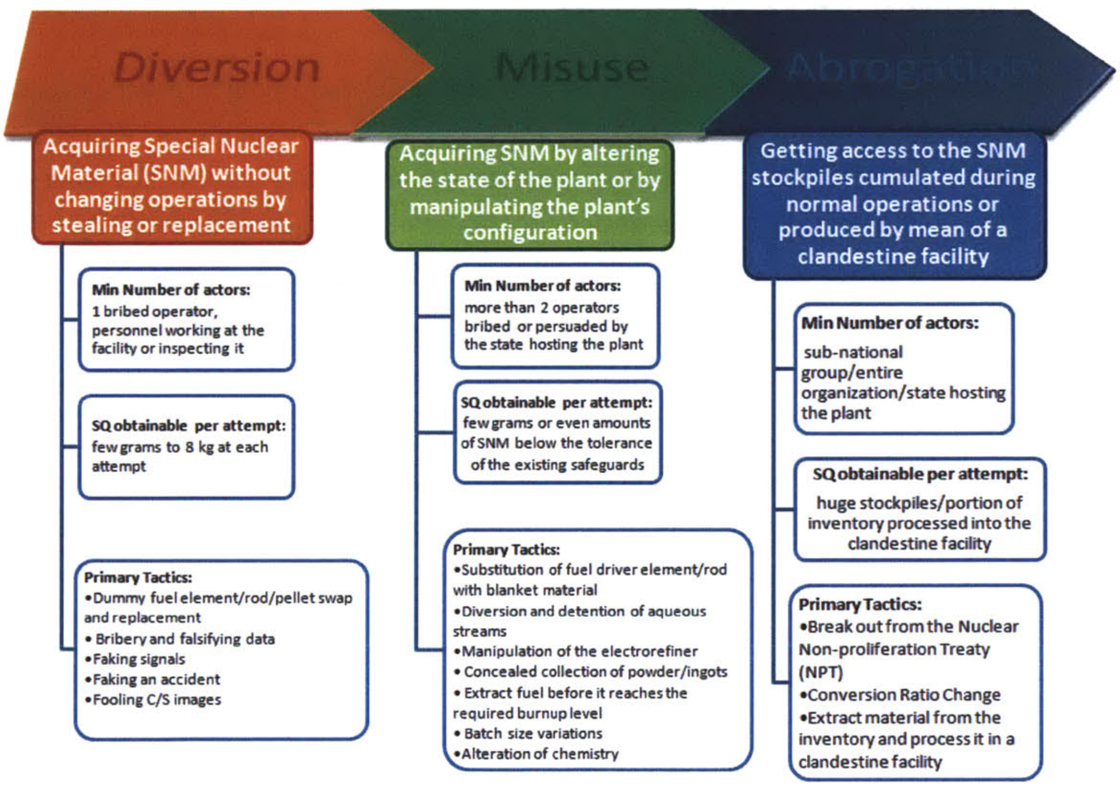


Figure 13: Scenario classification used in the non-proliferation assessment of the SFR.

Diversion/theft: the difference existing between a theft and a diversion scenario is the actor perpetuating the acquisition action. In case of theft, we assume the actor to be one operator (in particular circumstances even two or more) working at a given nuclear facility, acting under the mandate of a third party such as a terroristic organization. To the contrary, diversion scenarios are under the mandate of the state hosting the NES, thus acquisition of SNMs is an activity that might involve many, in not all, of the NES operators. Diversion intents are less complicated than theft ones because they avails of the complicity of almost the entire staff at the NES. In terms of modeling, diversion scenarios, by requiring less concealed actions, are less complicated than theft scenarios which instead require to use all the features of the model. Diversion and theft of SNMs constitute a real existing threat as documented by the IAEA illicit database[5], reporting considerable amounts of materials missing from declared nuclear facilities in the last 20 years.

Diversion scenarios required limited organizational efforts and can rely on the capability of a single individual. This imposes a limitation on the capacity of each scenario, because one individual can at most acquire a single fuel element per acquisition attempt.

Misuse: these scenarios generally refer to the alteration of system processes at the plant, as shown by Figure 14. Whether the action is led by a single individual or by the State owning the NES, a misuse attempt is not an acquisition accomplishment itself, thus it requires to be coupled with a consequent theft/diversion action. For example an operator might act to deviate SNMs into a waste stream, or increase the production of SNMs in a the separation process of a reprocessing plant; all these illicit operations require additional acquisition actions from the proliferator. Therefore misuse is modeled as an additional anomalous operation occurring ahead of a diversion/theft scenario. The misuse scenario is a greater challenge to the proliferator because it is not limited to individual actions but long-term, complicated actions carried out by many actors.

The Israeli research plant built in the desert at Dimona is an example of misuse strategy: the 24 MW_{th} research reactor was built by over sizing the cooling systems and waste facilities. Once built, the reactor was operated at double the power level declared to the IAEA and the detection instruments were calibrated to half the tolerance. By means of this strategy Israel was able to produce twice the amount of SNM the inspectors were looking for and to refine it in the secret reprocessing facility built not too far from Dimona.

The misuse scenario is a greater challenge to the proliferator because it is not limited to individual actions but long-term, complicated actions carried out usually by more than one actor. To justify this organizational effort, misuse usually involve acquisition greater to the equivalent mass of several fuel elements.

NPT abrogation: abrogation scenarios represent the last possibility by which a proliferator might acquire SNMs from a nuclear site. the Proliferator in this case needs to be the hosting State which after having enough stockpiles and knowledge to initiate a nuclear program decides to break out from the NPT to start a declared nuclear weapon program. For abrogation (or breakout) the proliferating state amasses an inventory of fissile material (e.g., spent fuel, MOX or separated Pu) while adhering to the NPT and cooperating with the IAEA. Then, in one move, when it wishes to acquire weapons, the state abrogates the NPT, extracts the fissile material from the accumulated inventory, and then reprocess it in a clandestine reprocessing or enrichment facility. The evaluation of this scenario can be evaluated in probabilistic terms by considering the conditions that generally proceeds its actuation, such as declaring covert enrichment facilities. Iran recently seemed to move toward this scenario and the Republic of North Korea did few years ago.

These scenarios have been under-emphasized because they are very difficult to defend against and are not particularly sensitive to the types of nuclear technologies being used. However the employment of complex satellite systems or advanced safeguards such as antineutrinos detectors can be thought to mitigate abrogation threats.

To justify this organizational effort, misuse usually involve acquisition greater to the equivalent mass of many fuel elements.

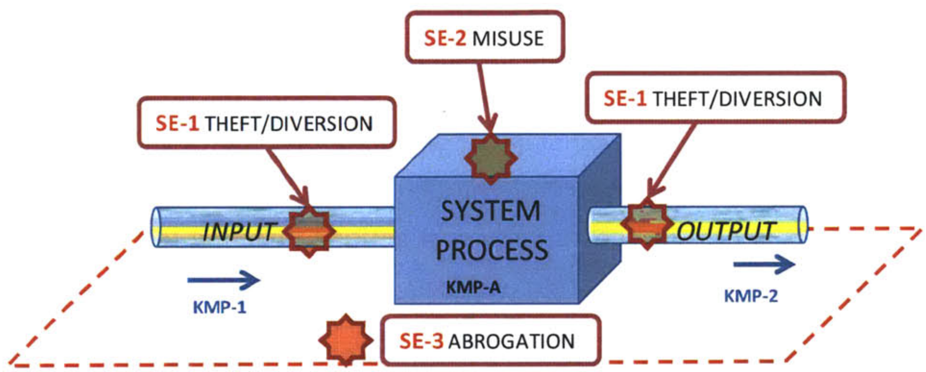


Figure 14: Attack points of the three different scenarios used to illicitly acquire SNMs.

Stages required for the illicit acquisition of SNMs

Amongst the different scenarios that characterize the proliferator strategy (i.e. diversion, misuse, and abrogation), the one that is more suitable for a probabilistic representation is diversion. Misuse can also be represented by an acquisition and a transportation phases, and it can be seen as a sub-set of diversion where the acquired material is produced by an upfront manipulation of a nuclear reaction, or of a chemical process. Abrogation scenarios do not need either to illicitly acquire or transport the materials within or out of the NES, and thus are less suitable to the representation used for the other two cases. Figure 15 portrays the sequence of decisions and events that characterize a diversion/theft scenario described as a competition between the safeguarder and the proliferator within a portion of the NES of interest (i.e., in this case the SFR's fuel cycle). All these decisions and events can be integrated into a probabilistic model capturing the sequence of actions shown in Figure 15. Ending a sequence determines a successful realization for a proliferator. Success from a proliferator's perspective means the acquisition of a significant quantity of SNM throughout one, or a sequence, of diversion attempts. The complement to one of this probability represents a success for the safeguarder.

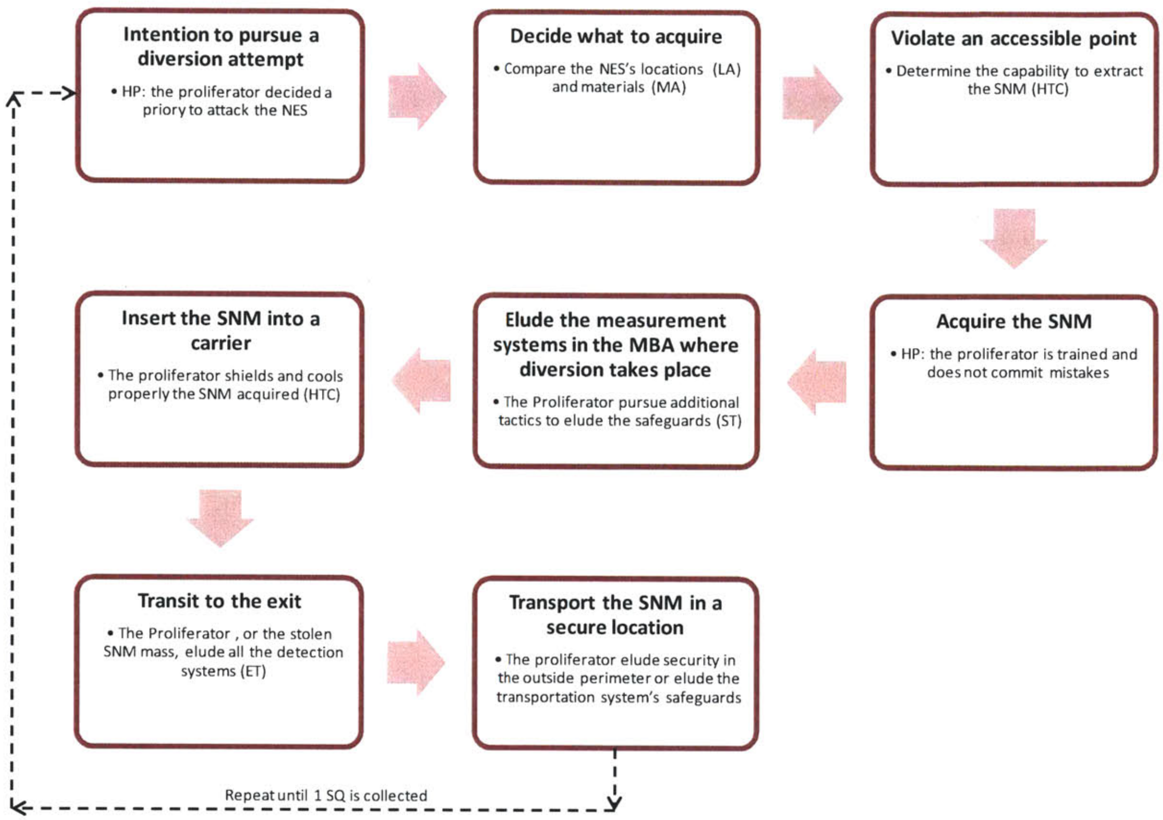


Figure 15. Sequence of events that lead the proliferator to succeed in a diversion attempt.

Many sequences, such as the one reported in the figure, can occur at each of the Key Measurement Points (KMPs) located within every of the Material Balance Areas (MBA) into which the plant is conceptually divided. All these sequences, for each KMP and all MBAs, have to be accounted into the probabilistic formulation of the diversion problem, so that the resulting probability takes into account all the possible realizations generated from a preselected initiating event. The probabilistic model also needs to take into account that an attempt can be repeated in a given KMP unless one significant quantity of SNM is acquired by the proliferator, as shown by the dashed arrowed line of Figure 15.

Principles characterizing the acquisition mechanism

The undeclared and illicit acquisition of nuclear materials at a nuclear facility by an individual is the core action of the chain of actions presented in the previous section. The considerations that drive the proliferator's decision to acquire SNMs are wide and complex. However at the basis of the decision is the material itself, of which he evaluates the form, quality and potential use of the material. Figure 16 shown the underlying mechanism of diversion, or theft of SNMs at a nuclear site. the following list of observations summarizes the key features of the diversion mechanism, or *system design principles* (***SDPs***) for acquisition:

1. The target material (i.e., the special nuclear materials) are bounded to a material mixture that in most cases occupies the majority of the volume. Acquiring the material target therefore implies to acquire the entire material mixture;
2. The material mixture o a nuclear fuel cycle includes all other istopes being part of the material fuels and of any of its byproducts;
3. The material mixture also might includes structural materials constituting the envelope for fuel assemblies, or the solvent used to liquify the fuel assembly (e.g., for example in acqueous plants);
4. The target material is not separable from the rest of the mixture on the site (i.e., it would be too complex for a proliferator to manipulate the acuired materials while on site);
5. The diverted material contains all the above elements, mantaining also the same proportions,and therefore mantaining the features and properties of the original mix.
6. The remaining material, or residual mixture, it it also maintain all the previous characteristics it had before a portion of it is being acquired;
7. The illicit acuisition of the material mixture can be detected in two ways: by measuring the difference betweeen the initial expetcted mass of the mixture, MM, and the diverted amount of material, md (MM-md), or by detecting the acquired material md while tranported to the facility's exit.

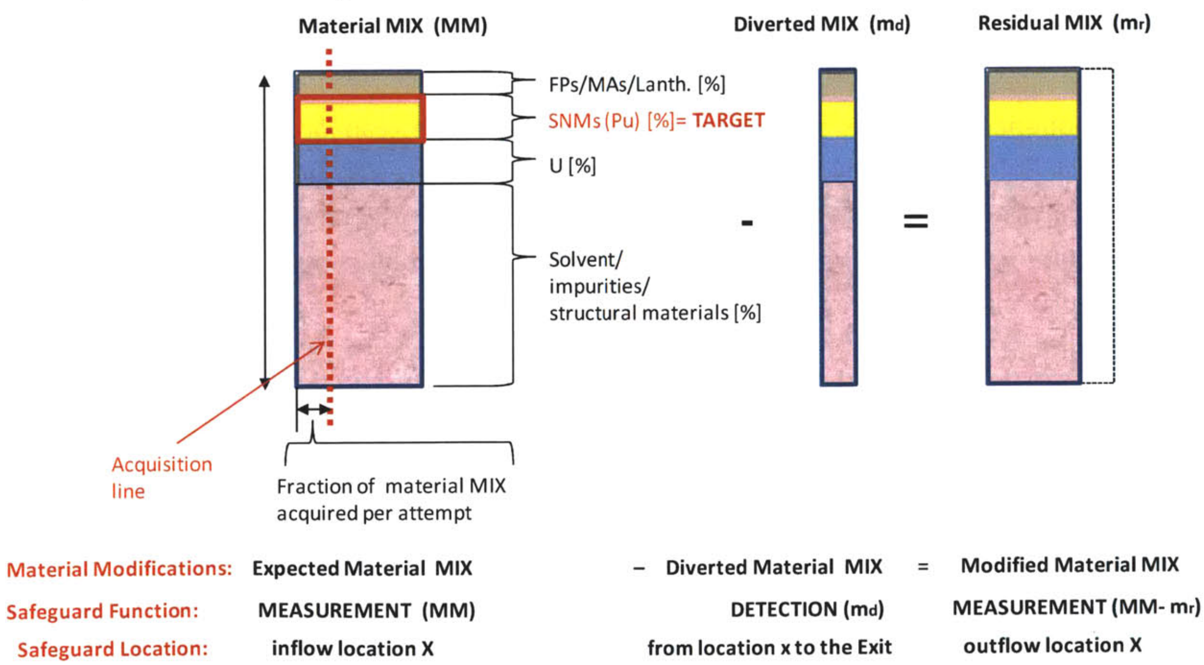
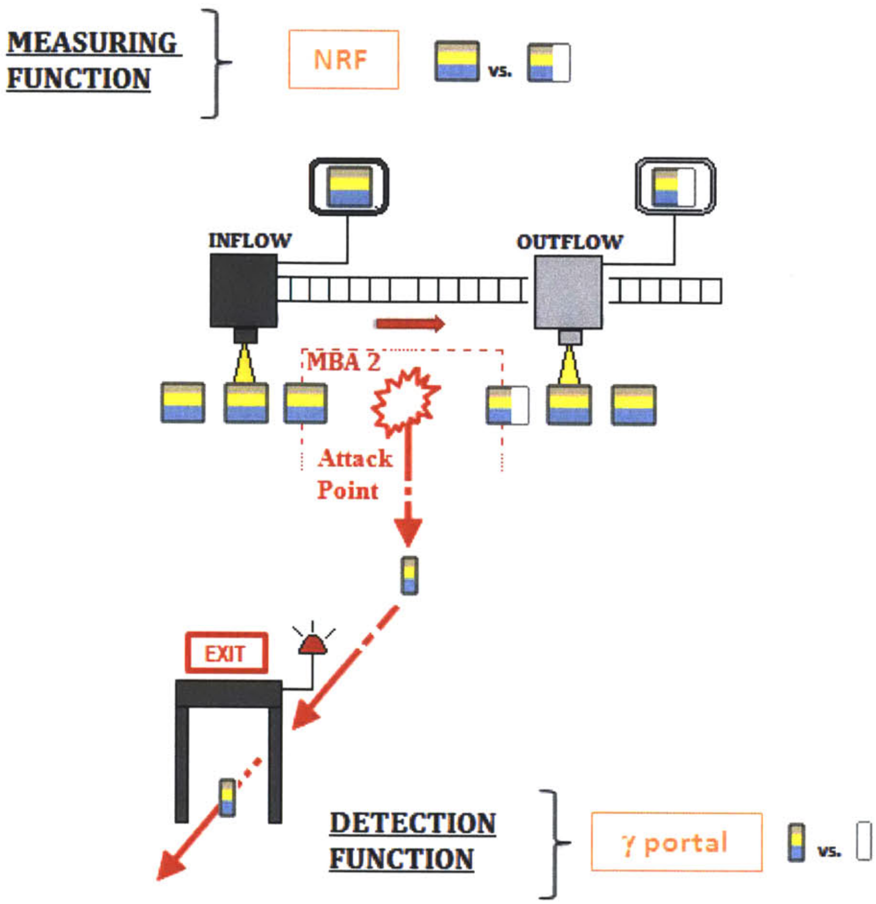


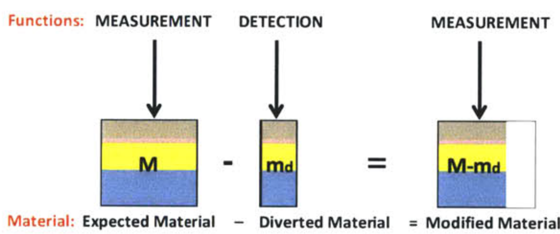
Figure 16. Visual representation of an hypothetical subtraction of material from a nuclear material MIX.

Note that many acquisition models imprecisely neglect one or more of the above observations. For instance, the concept of material attractiveness is often subjected to misinterpretations which are reflected in the choice of the sub-metrics used to characterize it [1]. Very often, material attractiveness definitions do not consider correctly the nature of the acquired material as defined by the list of observations already described, or sometimes these quantities are defined theoretically without considering the practical terms of a real scenarios.

Another common mistake is to evaluate the risk of acquisition only by considering it partially; for instance, many assessments only calculate the acquisition probability without considering the high chance of detection of a voluminous mixture, or fuel element. The proliferator's objective is to acquire 1 SQ of SNM by mean of one or more repeated attempts, in the most efficient and less risky manner. Risk evaluations to be complete have to consider all the components of the diversion mechanism. Specifically, all the ones giving a chance discovered the proliferator attempt along any of the steps characterizing the two following primary acquisition steps: acquisition and transportation of the mixture containing the SNMs.

This last aspect, visually reported by Figure 17, is very important to determine the proliferator and safeguarder dynamics. Furthermore the two different stages of acquisition and transportation determine the structure of the assessment model presented in the next Section.





SAMPLE TYPE	FUNCTION	DRIVER VARIABLE	SAFEGUARD
 VS. = 	MEASUREMENT	PRECISION (M- (M-md))	NRF NC
 VS. = 	DETECTION	THRESHOLD, BACKGROUND md	GP

GP = Gamma portal; NRF = Nuclear resonance fluorescence; NC = Neutron counter

Figure 17. Relationship existing between the measurement and detection functions of nuclear safeguards, and the acquisition and transportation stages of an illicit acquisition attempt.

ASSESSMENT MODEL: BASIC FEATURES AND DEFINITIONS

Proliferation risk

Non-proliferation is a special sub-set of security dealing with protection of the special nuclear materials. Non-proliferation further divides into the proliferation resistance problem and the physical protection one. The objective of this work is the reinforcement of nuclear security by improving the proliferation resistance of nuclear energy systems. In order to defend NES and prevent malicious attempts aimed at the acquisition of strategic materials from sites, or during transport, the theme of safeguard performance is a key aspect.

Similarly to the analogous definition in safety, the proliferation risk is defined as the product of the probability that a diversion event occurs and its associated consequences. Nuclear facilities need to be designed accordingly to this risk. Nuclear safeguards are added to mitigate it. The introduction of new safeguard systems has to be functional with respect to the potential threats associated with any portion of the nuclear fuel cycle scheme. For example if reprocessing facilities are deployed, this would generate high traffic of SNM within and outside the plant's boundaries. These facilities will be very attractive for potential proliferators because they will process high stocks of SNM, difficult to track and easy to handle in some stages of the process. Nonetheless, the level of uncertainty in today's accountancy measures is still too high to guarantee the timely detection of SNM (when high stocks of materials are involved the error in the measure can exceed the amount required to detect a significant quantity, SQ).

Competition Model

The two competitors have distinct but complementary goals: the proliferator's goal is to acquire the material needed to construct a NWD (i.e., the acquisition of one significant quantity of SNM), while the proliferator's goal is to contrast the proliferator by the introducing barriers in the NES to counter act (i.e. detect) the proliferator's diversion attempts.

The core element used to model the proliferator-safeguarder competition is the Success Tree. The Success Tree is a logical tree in the form of the ones sued for safety analysis but with a set of distinguishing features:

- The top is event does represent a success event instead of a system failure;
- The basic events in the tree are represent successes events;
- The probabilities associated with the events are random but they are generated by humans;
- The tree structure also integrates random events when the realization of a human action depends on the state of the physical systems where the human stages his actions.

The Success Tree effectively model the competition between a proliferator attempting to acquire SNM from the NES and therefore trying to elude all the safeguard systems in place and the safeguarder a priori acting to contrast by building and efficiently locating these systems in the NES.

The ST structures captures the decision sequence shown in Figure 15 except for the first event, which represents the intention to pursue an attack to the NES, which is assumed to be a given (i.e., we assume that the intentions to acquire SNM exists and therefore that it is equal to 1), and for the semi-last event, which is instead model by mean of an event tree.

The model is used to evaluate which portion of the NES the proliferator is going to attack and how successful he might be in defeating all the protection systems.

SDP: *We therefore design a facility throughout the integration of the counter measures with the original design by following the insights provided by the pathways to proliferation.*

Success Tree

The ST models the pathways to proliferation, in this case via diversion, by calculating the probability of success for a proliferator, Ps, that is trying to acquire the material from a specific material balance area located on site. The success tree allows calculating the probability Ps with the presence of tree types of counter measures:

- *Material accountancy safeguards*: detectors used to detect potential losses of material from the stocks or flows on site. They measure the quantity, and type of SNM on site and compare it to their expected value. These safeguards measure the radiation field, the heat generated, the weight, of the SNMs on site for each location.
- *Security Systems:* surveillance systems, guards, personnel on site, and containment systems such as seals.
- *Physical Protection Systems:* detectors of the movements of special nuclear materials on site, or any type of system monitoring variables such as the position of SNMs, the level of criticality, the dose, etc.
- *Policies:* they express the conditions at which the above systems can be operated and the presence of certain systems on site (e.g. environmental sampling can be used only if the country hosting the plant is a signatory of the additional protocol).

All the counter measures are included into the design for each of the facilities considered and they are calculated for all the individual locations (i.e. the material balance areas).

Event Tree

The ET models the proliferator 's probability of not being detected while the proliferator moves from the diversion point to the exit of the considered facility. During his pathway he has to elude counter measures that he encounters on his way from the acquisition point to the facility's exit.

The success probability Ps, for a given scenario (i.e., once the amount of material, the material type, the location at which diversion occurs, and the plausible primary and supportive tactics are specified) is calculated by combining the probabilities to elude all the above proliferation counter measures with the probability that the proliferator is not detected while it travels from the diversion point to the plant's exit.

For instance, considering that all the events on site are independent, the overall probability to divert SNM following a given strategy, will be given by the product of the probability to acquire the SNM (i.e. the probability to elude the counter measures located on site to account for missing portions of SNM) with the probability that the stolen mass carried by the proliferator is not going to be detected while moving from the acquisition point to the exit.

Primary tactic: is the primary strategy that the proliferator decides to follow in order to acquire the material of interest.

Secondary tactic: this is the set of strategies that the proliferator has to follow in order to succeed in his primary one. The secondary strategies define the way with which the proliferator tries to elude the individual counter measures he encounter on his pathway.

Safeguards can be eluded by acting on the different functions of the system architecture:

- The intrinsic function;
- The transmission function;
- The visualization function.

In addition to these functionalities, external events (i.e. faking an accident) and manipulation of the sample are the other two strategies used to support the primary tactic.

Scenario: the elements constituting a scenario are, for a pre-selected location:

- Strategy type: diversion, misuse, or break out;
- Material target type: SNMs, level of purity, and abundance in the mix;
- Amount of target material: the amount of material acquired per attempt;
- Counter measures: the type and number of protection systems on the pathway;
- Number of attempts: number of repeated scenarios in order to acquire 1 SQ.

STRUCTURE OF THE ST/ET MODEL

The proliferator success probability, Ps, is calculated by combining a set of sub-metrics, each expressed by a probability function. The probabilities represent the complete set of events that the proliferator need to realize in order to successfully acquire the SNMs. At the current stage of the model's development (alpha version), it is assumed that these probabilities all independently contribute to the realization of the top event Ps. These are the basic features of the model expressed in terms of probabilities:
The probability *Ps* is calculated by multiplying the probability *Pa* to illicitly acquire materials from a given location of the NES with the probability *Pt* to transport the same material from the acquisition point to the NES's exit.

The acquisition probability *Pa* is obtained from a **Success Tree (ST)** that takes into account:

- The **motivations to pursue** an acquisition attempt at a given location of the NES. These are expressed in terms of parametric probabilities functional to the attractiveness of the material (P_{MA}), and to the attractiveness of the specific location from which it can be acquired (P_{LA}).
- The parametric probability P_{HT}, which represents the capability to transport and handle the acquired material, including the material being part of any type of container used to carry, shield, and cool the illicitly subtracted portion of SNMs.
- The proliferator's **capability to elude** all the protection systems, P_E, added to a facility in order to prevent, control, and mitigate proliferation risks.

The ST tree is further decomposed into functional sub-trees considering the various barriers being employed the SNMs from proliferation risks. Accordingly to this classification the tree model is referred as a functional tree. The features of each of the barriers, part of the entire technology-policy system employed to protect the SNMs from acquisition threats, are represented by a protection function. This portion of the tree evaluates the proliferator's probability to contemporarily elude all the countermeasures created to control, mitigate, and prevent proliferation risks. A set of functions, and of associated probabilities was identified:

- ***Function 1: Material counting and accounting function (MC&A).*** *The* probability P_{Em} represents the likelihood that the proliferator eludes a technical system (e.g., a gamma ray detector) designed to measure the amount of material present in a specific location, or key measurement point.
- ***Function 2: Containment and Surveillance Function (C/S).*** *The* probability $P_{EC/S}$ represents the likelihood to that the proliferator eludes a technical system (e.g., an optical camera) designed for the surveillance of the material in a specific location or for the location itself.

• ***Function 3: Process Monitoring Function (PM).*** *The* probability P_{Epm} represents the likelihood that the proliferator eludes a technical system designed to monitor the processes occurring in a specific location.

• ***Function 4: Institutional Policies Function (Pol).*** *The* probability P_{Epol} represents the likelihood with which the proliferator might violate any policy, agreement, or rule established to verify that the processes in a specific location are conducted without altering their original scope.

The ST model also contemplates the possibility that specific tactics are going to be used to reduce the capabilities of the above functionalities. An average of four supportive tactics, to a maximum of six, are being identified in correspondence of each of the above functional barriers. Their quantification rely on an experts' elicitation process which was established ad hoc for this model. The scope of a proliferator's tactic is to make the detection system vulnerable to a specific threat (e.g., diversion of theft of SNMs).

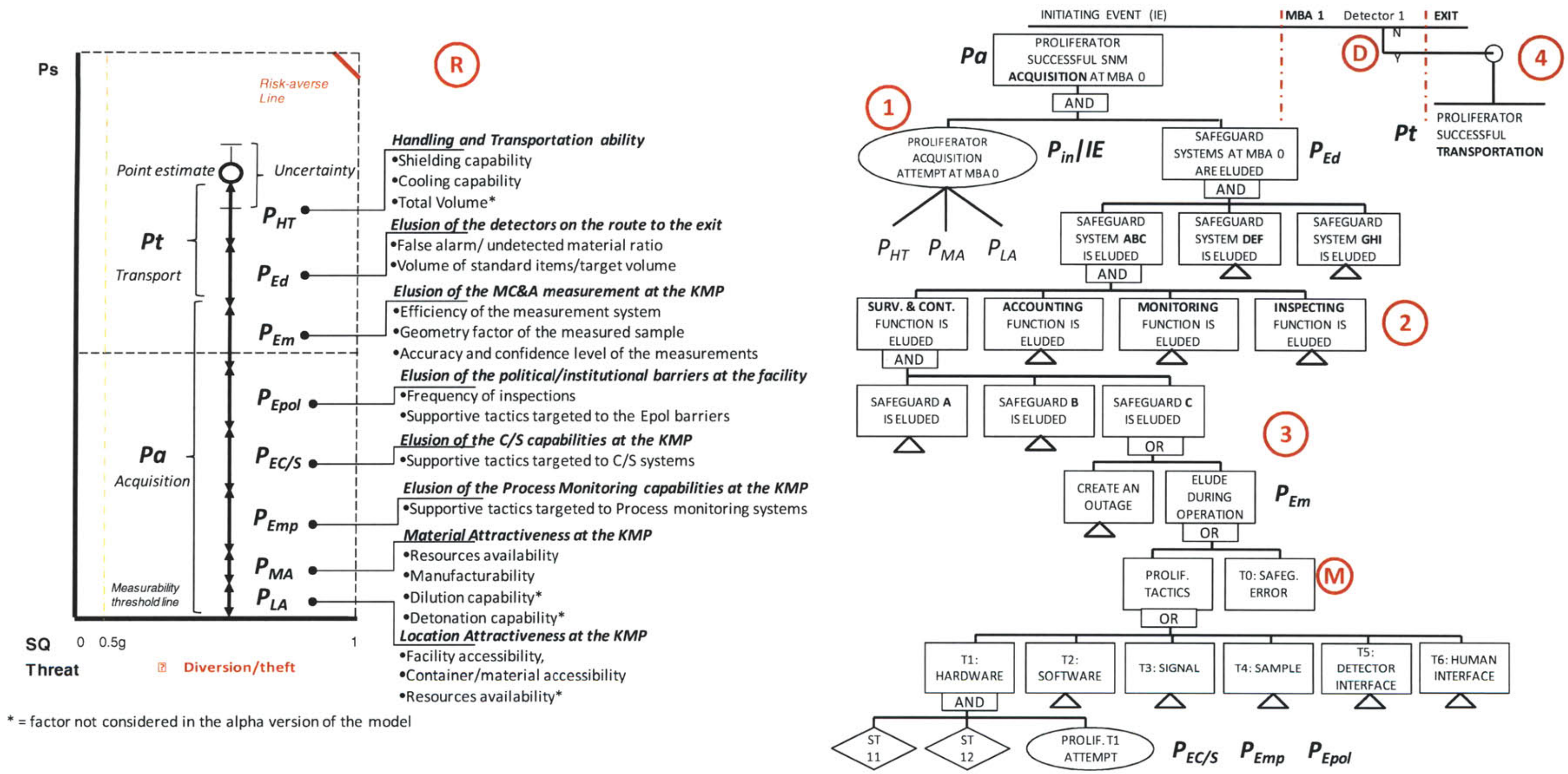


Figure 18: Topology of the ST/ET model and factors considered in the determination of the proliferator's success probability. The figure relates the probabilities concurring to the creation of the probability Ps reported in the risk space (left figure) to the structure of the model (right figure[13]).

[13] The letters and numbers used to label the ST/ET modules of the structure are also used to label the Sections that describe them in detail.

BASIC EVENT PROBABILITIES

The success tree is built using the principle of Boolean logic; logic ports determine the relationship existing between two or more of the events. The events describe the course of actions of a competition model between a proliferator, trying to acquire special nuclear materials, and a safeguarder, trying to prevent illicit acquisition. When these actions cannot be further decomposed, the tree is arrested and the events at the base of the tree need to be defined with a probability. These events are called basic events (BE). The top event probability results from the combination, obtained via Boolean operations, of all the basic events.

The probabilities associated with the basic events are of different types and only few of them are known a priori. For this reason Expert opinion is required for the determination of most of the basic events represented in the assessment. Furthermore, the experts are valuable for the identification and definition of:

- Basic events probabilities associated with tactics to the safeguards;
- Basic event probabilities of events not directly related to proliferation performance (e.g., unavailability, reliability, probability to fake accident in a selected room of the NPP);
- Costs of the barrier systems and of their variants;
- Acquisition Strategies, or modalities and tactics used to acquire SNMs.

The calculation of the overall probability, Ps, to successfully acquire a significant quantity of SNMs by means of one or more acquisition attempts, has been decomposed following the modularization of the model reported in Figure 18, and thus taking into account the following different probabilistic sub-models, which are described in the next Sections:

(1) Parametric probabilities;
  (1.A) Drivers for the probability to initiative an acquisition attempt;
    Material attractiveness;
    Fuel handling and transportation capability;
    Location attractiveness;
  (1.B) Probability of multiple proliferation attempts;
(2) Functional classification of the barrier systems, and functional trees;
(3) Individual safeguards analysis;
(M,D) Models used to determine the probability to elude a system with no tactics;
  (M) Counting and accounting probability;
  (D) Detection probability.

Two separate sections describe the expert elicitation process used to determine the Bes, and the experiment used to relate the probabilistic model to the expert elicitation process:

(BE) Elicitation process for the determination of the basic event probabilities;
(SE) Standardized Experiment used to determine the accuracy of (M) and (D).

System Design Principles used to formulate the parametric proliferation metrics

The list of ten principles that follows was used to formulate quantitative metrics, and sub-metrics useful to define and decompose the intentions of a proliferator willing to acquire SNM from a given segment of the fuel cycle with the ultimate scope of building a nuclear weapon device. The enunciation of the principles, and the formulation of the parametric properties consistent with these principles was preceded by a literature review considering recent studies conducted on this matter. Although many of the formulations provided in the literature are very accurate, very often lack of applicability, or the resulting metrics are so complex that their interpretation results too difficult, and thus inapplicable to the more practical evaluations. The following authors and works have been considered and included into our evaluation:

- C. G. Bathke et al., *"The attractiveness of materials in advanced nuclear fuel cycles for various proliferation and theft scenario's*. Proceedings of Global 2009. Paris, France, September 2009.
- E. Hamase and M. Saito, *"Effects of MA doping in fast breeder reactor"*. Proceedings of Global 2009. Paris, France, September 2009.
- W. S. Charlton et al., *"Proliferation resistance assessment methodology for nuclear fuel cycles"*. Nuclear technology vol.157 February 2007.
- Ham, H. and Golay, *"An Integrated Methodology for Quantitative Assessment of Proliferation Resistance of Advanced Nuclear Systems Using Probabilistic Methods"*, Department of Nuclear Engineering. Massachusetts Institute of Technology, Cambridge, MA, 2005.
- *Proliferation Resistance and Physical Protection Evaluation Methodology Expert Group of the Generation IV International Forum*, (Revision 5). OECD Nuclear Energy Agency for the Generation IV International Forum: Washington, D.C., 2006.

System Design Principles used to determine proliferation sub-metrics

1. ***Interpret the proliferator's interest in actuate an acquisition attempt and his capabilities in successfully completing it:*** Each overall attribute, and it sub-attributes, have to provide an evaluation (i.e., benefits) of the proliferator's intention to acquire the material from a pre-defined location.
   This requirement in turn translates into the following features:
   a. A **Material Attractiveness** metric has been introduced to include into the evaluation the typology of material available in the considered fuel cycle, or segment of the fuel cycle.
   b. A **Location Attractiveness** metric has been introduced to include into the evaluation the opportunities provided by the various segments and locations of the fuel cycle.

c. A **Fuel Handling and transportation** metric has been introduced the evaluation of the capabilities necessary to handle and transport the acquired materials out of the facility.

2. ***Refer clearly to a single target:*** the evaluation has to be clearly referred to one type of SNM, to one type of associated nuclear weapon device, and using a single metric for the amount of materials required. This notion translates into the following set of assumptions which applies to the example reported next:
   a. **Plutonium was chosen as the SNM target** material for a proliferator having the ultimate scope to build a nuclear weapon device. No other materials classified as SNM (i.e., 237Np, 241Am, 2325U, 233U, or Th) are considered in the quantitative formulation of the model, although account in the qualitative analysis;
   b. **The measure unit selected to quantify the amount of SNM** material necessary to build a nuclear weapon device is, accordingly to the IAEA, defined as significant quantity (SQ). No other measures, such as critical mass, reflected bare mass, or combined measures such as the critical bare mass of the entire mixture are considered in the analysis;
   c. **Only one type of nuclear weapon device is being considered**, accordingly to the type of SNM selected. In this case, an implosion device is assumed. All the attributes of the parametric model (e.g., manufacturing specifications) are referenced to this assumption.

3. ***Provide a means of comparison between different acquisition options:*** Each overall attribute has to be expressed from the perspective of a proliferator comparing the different fuel cycle segments and who has to decide which one offers the major benefits.
   a. **Normalization factors** of the main metrics refer to the highest value obtainable for that metric within the entire fuel cycle.

4. ***Obey to probability rules:*** the MA formulation should be expressed in form of a probability function thus having the following features:
   a. Each sub-attribute has to be defined, or related to, a monotonic function contained in the [0,1] interval;
   b. Each sub-attribute has to be directly related to the likelihood to acquire special nuclear materials on the site;
   c. The resulting probability should refer to the likelihood to succeed in a single acquisition attempt of a given mass of SNM (i.e., opportune derivations are used to compute the probability to successfully obtain higher amounts of material throughout a series of consecutive attempts).

5. **Being simple and interpretable:** each attribute should have a maximum of two sub-attributes. The sub-attributes must keep a physical meaning and not being the result of manipulations with numbers.

6. **Contain time evaluations:** at least one of the attributes, or sub-attributes should change with time in order to capture the opportunity offered by particular time windows such as refueling operations, or maintenance.

7. **Account for initial hypotheses** and **do not double count elements of evaluation.**
   a. The material of SNM material should be enough to build a nuclear weapon device;
   b. The material mix should contain high quality SNM (e.g., enriched uranium or Pu with low percentages of Pu240 and Pu238);
   c. The portion of SNM should be easily separated from the material mix.

   All the above assumptions are satisfied for a SFR fuel cycle. Many parametric evaluations present in the literature calculate metric that in most of the cases, as is the case of the SFR fuel cycle, are simply constant assumptions and do not require to be calculated by means of particular measures but they are simply assumptions that need to be verified beforehand.

8. **Allow the comparison between different design alternatives, such as**
   a. Fuel options (e.g., fuel driver elements, fuel blankets, minor actinides addition, etc.);
   b. Alternative Processes and fuel schemes (e.g., different separation processes);
   c. It has to capture the opportunities given by different fuel morphologies (i.e., items, batches and continuous streams).

9. **Refer to a specific threat, and thus to a specific actor.** The metrics refer to a single threat, or acquisition mode. In this study we specified thee different types of acquisition modes (i.e., diversion/theft, misuse, and NPT abrogation). The parametric evaluations might be reformulated according to the assumptions implied by each of these three different cases. As noted before, the different threats require different organizational efforts and involve different organization levels (e.g., from a single individual to a state driven action).

10. **Consider the overall mixture properties.** Very often parametric measures refer only to the SNMs, which in many cases, represents only a considerably small portion of the entire fuel mixture (i.e., typical examples are considering the radiation field of the Pu mix and not of the entire fuel mixture). Separation from the mixture cannot be assumed unless the proliferator intentions are declared and well known.

(1) PARAMETRIC PROBABILITIES

(1.A) Drivers for the probability to initiative an acquisition attempt

The proliferator's intention to perpetuate an acquisition effort at a given location is driven by different drivers, which are being quantitatively modeled by parametric probabilities. The combination of these driving motivation is computed by assuming that motivations are independent. The resulting probability value, P_{in}, is a measure of the proliferator's intention to acquire special nuclear materials from a given are located within one of the segment of a nuclear fuel cycle. The intention of the proliferator are relative to the various locations and design alternatives offered by a nuclear fuel cycle, however the initial intention to perpetuate the attack is by definition unknown or highly uncertain since it depends of human motivations unpredictable by nature. For this reason the probability Pin modeled in this section is not the initiator of the three that combine the three parametric basic events described next. Therefore the probability is considered to be conditional to the initiating event IE: Pin|IE and it directly concurs to the formulation of the acquisition probability Pa , as shown by Figure 19.

Table 6 reports the parametric results obtained for the reference example of a sodium fast reactor of 2400 MWe, using the three distinct measures of Material Attractiveness (MA), Location Attractiveness (LA), and fuel Handling and Transportation Capability (HTC). The criteria used to determine these three metrics and their descriptions are described next.

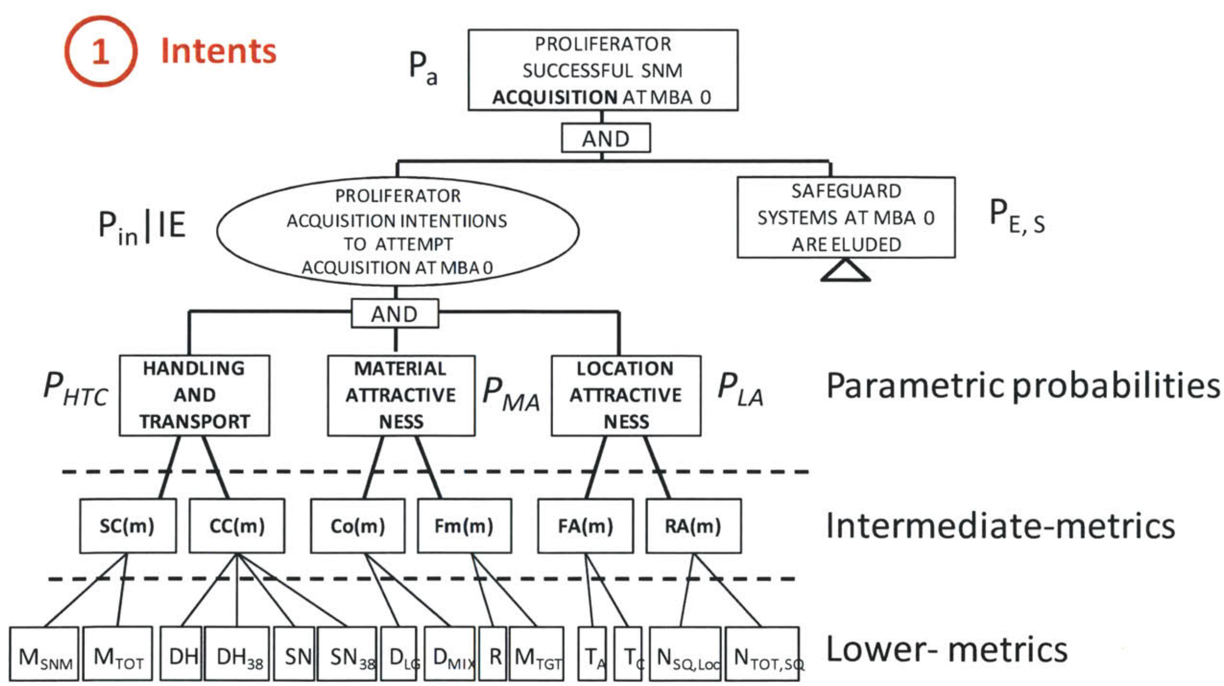


Figure 19. Top structure of the success tree model showing the layers of metrics used to calculate Pin.

The intention of the proliferator are relative to the various locations and design alternatives offered by a nuclear fuel cycle, however the initial intention to perpetuate the attack is by definition unknown or highly uncertain since it depends of human motivations unpredictable by nature. For this reason the probability P_{in} modeled in this section is not the initiator of the three that combine the three parametric basic events described next. Therefore the probability is considered to be conditional to the initiating event IE: $P_{in}|IE$ and it directly concurs to the formulation of the acquisition probability P_a , as shown by Figure 19.

Table 6. Parametric probabilities valued at each of the most vulnerable measurement points.

				1 mass	*mmin*	*mbc*	*mmax*
	fn	**Definition**	**Equation**	w/1Kg	w/1 fr	w/(1/3 fr)	w/fa
MA		Fuel type amount (kg)		1	0.428	38.524	116
MA f1	Co	SNM Concentration	Msnm/Mtot in a FA=Pu conc	0.110	0.110	0.110	0.110
		M_{SNM} = Mass of SNM	Sum Pu-weight,i	0.110	0.047	4.239	12.765
		M_{TOT} = Mass target MIX	Sum Isotope-weight,i	1.000	0.428	38.526	116.006
MA f2	FM	Fissile Manufacturability	(DH/DH38)+(SN/SN38)	8.03E-05	1.47E-05	1.19E-01	1.00E+00
(Saito 2009)		DH/DH_{38}	Sum Isot-w,i*DH/(w38*DH38)	1.43E-05	2.62E-06	2.12E-02	1.92E-01
		SN/SN_{38}	Sum Isot-w,i*SN/(w38*SN38)	6.60E-05	1.21E-05	9.80E-02	8.88E-01
Pr(MA)		Material Attractiveness	Co x FM	0.0000	0.0000	0.0131	0.1100
HTC							
HTC f1	SC	Shield & Cool Capability	1-LN((Dlg/Dmix)+1)/10	0.74	0.66	0.97	0.99
(Charlton 2007)		D_{LG} = dose rate LG Pu	w38*D38+w39*D39	2.73E-04	2.73E-04	2.73E-04	2.73E-04
		D_{MIX} = dose rate MIX	Sum(Isot-w,i*Di)	2.12E-05	9.07E-06	8.16E-04	2.46E-03
HTC f2	CC	Volume factor	Mtot/R/(Mtot,fa/R,fa)	0.01	0.004	0.33	1.00
		R = density (kg/cm3)	weighted sum of all densities	0.01471	0.01471	0.01471	0.01471
		Mtot= mass tot MIX	Mass target mterial mixture	0.856	0.428	38.526	116.006
Pr(HTC)		Fuel Handling Capability	SC x CC	0.005	0.002	0.322	0.989
LA							
LA f1	FA	Facility Accessibility	LN(Ta/Tc+1)/10	0.05	0.03	0.11	0.46
(Ham 2006)		T_A = access time max	max refueling time	4200	4200	4200	4200
		T_C = min time get 1 SQ	Tc/1 att x Natt, 1 SQ	6360	12989	1993	41
LA f2	RA	Resources Availability	N SQ,loc/N SQ, max	0.10	0.10	0.10	0.10
		$N_{SQ,LOC}$ = # of SQ, Loc	Number of SQ in the location	57	57	57	57
		$N_{TOT,SQ}$ = # SQ of MIX	N max of SQ in any location	574	574	574	574
Pr(LA)		Location Attractiveness	FA x RA	0.0051	0.0028	0.0113	0.0464
BE							
Pr(BE)	Pi	Basic Event Par Pr		2.44E-10	1.10E-11	4.80E-05	5.05E-03

Material Attractiveness

The material attractiveness (MA) measure is an overall indicator of the inherent desirability of the material to a potential proliferator. The quality of the material available in a given location is a key driver for the proliferator's intentions. The definition of MA is relative to the proliferator's final scope, which is the construction of a nuclear weapon device. The literature reports many contributors to this parameter, which has an extreme variability in terms of the way the different authors define it. Very often the authors do not specify the final application of the formulations they provide, or sometimes their definitions are extremely theoretical. Our approach was to first establish a set of criteria making the parameters useful for our scopes and consistent with our risk-informed model. Then we explored the formulations contained in the literature to see if these were compatible with our scope. Those which passes this screening process, where used or adapted to our needs. Table 7 lists the attributes most commonly associated with material attractiveness. The criteria we used for the MA formulation, and for the other two parameters defined in the following sections, determined the following features for the MA metric:

Concentration of SNM: this is a factor being constant in each of the location of the power plant. It is an intrinsic property of the fuel changing only when the fuel is transformed by burning it (i.e. it differs at the beginning and the end of a reactor cycle) or in between some of the stages of nuclear reprocessing. This factor constitutes a primary driver for the proliferator's preference to attack a given fuel cycle segment. The concentration of SNM in the total fuel mixture also constitutes an indirect measure of the volume of total material required to manufacture a NWD, and of the probability of being undetected during covert illicit actions such as acquisition and transportation. High concentrations justify the intent.

The metric is not functional to the amount of material acquired; the concentration is simply equal to the declared Pu concentration of the fuel over the fuel mass.

Fissile manufacturability: this metric considers the properties desired to assemble a NWD. The factor used to represent the technical ability in manufacturing and maintaining explosive a NWD is described by Saito and function of the decay heat (DH) and by the spontaneous fission neutrons (SN). Pu238 decay heat and fissions are the main cause of low fizzle yield and of cooling problems for an implosion device. A simple additive formula considering the properties of the overall Pu mixture against the individual 238Pu properties; for lower concentration values of DH and SN of 238, the mixture is attractive.

Table 7. Material Attractiveness determination via functional decomposition.

Functions	*Attribute*	*Equation*	*Parameters*
Function 1: Resources Availability	Available SNM material versus the total MIX	Mass of SNM/total mass of the targeted MIX = M_{SNM}/ M_{TOT}	• M_{SNM} = Mass of SNM • M_{TOT} = Mass of target MIX
Function 2: Fissile Manufacturability	Difficulties in assembling the NWD due to the properties of the SNM	1 over the sum of the decay heat and neutron fissions corrected for Pu238 (ref. Saito)	• DH= decay heat [w] • SN= spontaneous fission [n] • DH_{38}= decay heat ^{238}Pu • SN_{38}= spontaneous fission ^{238}Pu
Function 3: Detonation Capability	Detonation capability of a NWD	Fizzle yield probability formula (ref. Ham & Golay)	• N = spontaneous fission rate [n/ sec] • t_0 = time to max criticality [sec] • ? = neutron mean lifetime [sec]
Function 4: Separation Efforts	Estimated separation cost of the MIX versus total NWD cost	Cost of NWD/ sum of NWD and separation costs (ref. Ham & Golay)	• Cs = estimated separation plant capital costs [$] • C_{NWD} = estimated weapon fabrication cost [$]
Function 5: MIX manufacturability (alternative definition)	Difficulties in assembling the NWD due to the properties of the SMIX	Weighted sum of spontaneous fission decay heat, dose rate and critical bare mass of material (ref. Bathke)	• D = dose rate of 0.2M at d=1 m [rad/hour] • M = critical bare mass of material [kg] • DH_S = specific heat [w/kg] • SN = spontaneous fission production rate [n/kg]
Acronyms	NWD = Nuclear Weapon Device; SNM = Special Nuclear Material; DH = Decay Heat; SF = Spontaneous Fissions; SQ = Significant Quantity		

The metric is a function of the material acquired in each acquisition attempt. The parameter detects different fuel design options and captures intrinsic fuel features connected to the plutonium chain evolution in the core, such as the addition of minor actinides. The two parameters are combined by means of a simple multiplication, thus excluding from the calculations weighting factors or other subjective parameters.

The MA function determines the level of appeal of a given material mixture, however by definition MA represents just a crude factor that considering only the appeal level of a given material mixture and not that the mixture might either be difficult to get accessed or difficult to transport. Therefore the two following functions complement MA by considering the two aspects of accessibility and handling capabilities of the material mixture.

Also for this factor has to defined per unit mass. Defining the handling capability per unit mass is less accurate than for the case of material attractiveness since some derived properties such as the dose are not linearly changing with mass and therefore might change considerably depending on the mass diverted per attempt. However since the decision to divert a given mass here is not relative to the quantity but it is relative to the location to choose, the factors used to describe this attribute refer to unit mass. The dependency of the diversion success probability with the size/amount of the diverted mass is not embedded in this factor but in the Event tree.

The quantities considered have to refer to the entire material mixture, since the dose is determined by adding all the radiation types in the mixture. However in presence of fission products it is not feasible to handle the material especially when compared to the other possible KMP in the facility. Therefore since the solvent and structural materials, unless deeply contaminated do not contribute to dose and heating, only the TRU mixture (Lanthanides and Minor actinides are considered together with Pu and U isotopes).

Fuel Handling And Transportation Capability

The fuel handling and transportation capability (HTC) measure constitutes an indicator of the proliferator's performance in transporting the material acquired from a specific location. The *Shielding and cooling capability* during transportation and the *volume occupied by the total mixture* are the key drivers for the proliferator's intentions, in case theft or diversion are considered. This factor does not apply in case of abrogation scenarios but is still considered in misuse scenarios where the hosting state is not the proliferator.

Shielding and cooling capability: this metric is obtained by the radiation filed of the target material mix. In the literature there are many cases of metric of this type considering only the SNM radiation filed and not including the entire mix into the computation of the radiation field. The SNM materials in most cases emit level of radiation lower than many actinides, or fission products being part of the mixture. The error in other author's evaluation comes from the fact that they implicitly consider the separability, on site ad during acquisition, of the SNM from the rest of the nuclear mixture.

Volume factor: this is simply derived from the density of the target nuclear material mixture by knowing the mass of the subtracted materials. The higher the volume the higher the chance of being detected by cameras, alarm system and by material accountancy systems.

The volume factor is normalized to the highest encumbrance item in the fuel cycle, in this case represented by a fuel assembly.

The two resulting metrics are combined by means of a simple multiplication, once again excluding from the calculations weighting factors or other subjective parameters.

Table 8. Handling and Transportation Capability determination via functional decomposition.

Functions	*Attribute*	*Equation*	*Parameters*
Function 1: Shielding capability	Dose from the diverted MIX to handle versus the base case of pure low grade material	Dose rate of the LG material divided by the dose generated by the MIX	• D_{MIX} = dose rate of the material MIX at d=1 m [rad/hour] • D_{LG} = dose rate of low grade material at d=1 m [rad/hour]
Function 2: Cooling capability	The cooling capability required to handle the material MIX versus low grade material	Decay heat of the LG material divided by the decay heat generated by the MIX	• DH_{MIX} = decay heat of the material MIX [w] • DH_{LG} = decay heat of low grade material [w]
Function 3: Number of Attempts	Number of attempts required to obtain a SQ	Number of attempts required to get 1 SQ	• 1 SQ (8 Kg Pu)/ mass of SNM acquired in a single attempt
Function 4: Volume required to shield & cool (alternative)	Max(volume to shield the MIX, and volume to cool the MIX)/visible volume	Mass of the MIX * density of the MIX * MAX the volumes needed to reduce Intensities to zero	• M_d = diverted MIX mass [g] • ρ_C = container density [g/cm^3] • D_{MIX} , D_{LG} , DH_{MIX} , DH_{LG} • V_T = volume of plant's containers

Location Attractiveness

The location attractiveness (LA) measure evaluates the features of the location where the material is located from a potential proliferator perspective. The amount of SNM available in the location, and the accessibility to the location are the two key drivers concurring to the formulation of this metric.

Facility accessibility: as one of the intermediate metrics constituting the LA metric is measured as T_A/T_C, which is the ratio of total accessible time to the facility compared to the minimum time required for collecting the critical mass of SNMs. The total time that the proliferator can access the facility or particular point could be either less or more than the minimum time required for collecting enough material to create a nuclear weapon. If T_A is less than T_C, the material sufficient for manufacturing one nuclear weapon cannot be diverted.

Resources availability: the resources are evaluated in terms of number of significant quantities of SNM (i.e., Pu available in the Key measurement point exposed to a potential acquisition threat). The availability of plutonium is expressed in terms of multiple or fractions of SQ available on the site. This metric is excluded from most of the parametric evaluations in the literature because considered superfluous or unnecessary to the evaluation. Most of the authors support the lack of this metric by stating that only 1 SQ is sufficient to assemble a NWD. However in terms of probability the likelihood to recreate the desired conditions for a successful covert acquisition increase as the mass of available material increases. Therefore representing the mass of SNM versus the total mass available in the location takes into account of the abundance of SNMs relative to the total mass to be accounted, and of the number of SQ available versus the total number of potential SQ acquirable from the same location.

The factor is normalized to the highest number of SQ present in any of the other locations between which the proliferator can choose as a starting point to perpetuate his acquisition ambitions.

Also in this case, the two resulting metrics are combined by means of a simple multiplication, thus excluding from the calculations weighting factors or other subjective parameters.

Table 9. Location Attractiveness determination via functional decomposition.

Functions	*Attribute*	*Equation*	*Parameters*
Function 1: Facility Accessibility	Accessibility during operations versus accessibility required to divert the material MIX	1 over the ratio between accessible time and the time required for an attempt	• T_A = total accessible time to facility over reactor lifetime [yr] • T_C = minimum time required for collecting 1 SQ [yr]
Function 2: Resources Availability	Available SNM material versus the total MIX	Mass of SNM/total mass of the targeted MIX potentially obtainable in that location (as a stock or as a flow rate)	• M_{SNM} = Mass of SNM [kg] • $M_{TOT,LOC}$ = Mass of target MIX in that location or flowing into that location [kg], or [kg/sec]
Function 3: container/ material accessibility	Capability to obtain the material from the container or process to which it belongs	These are tabulated factors introduced to take into account the resistance of the container or process, the environment, and the cohesion of the materials.	• CMF = Container and material type factors: o Batch: CF=0.4 MF = 0.7 ; o Pipe: CF= 0.5 MF = 0.3 ; o Process: CF= 0.9 MF = 0.2 ; o Stock: CF= 0.7 MF = 0.9 ; • EF = Environment type factor: o Remotely operated = 0.9 o Directly operated = 0.3
Acronyms	HTD = Handling and Transportation Capability		

(1.B) Probability of Multiple Proliferation Attempts

One of the design principles of the previous Sections was rule 4.c, which is each of the evaluations is referred to a single attempt. This section illustrates how the model can be used to calculate the probability of consecutive acquisition attempts. The following model, coupled with the previously presented probabilistic model offers a way to evaluate the acquisition of significant quantities of SNM via the repetition of consecutive, independent acquisition attempts. The present model applies for diversion/theft scenarios.

Each of the metrics concurring to formulate the probability, P_{in} to initiate an acquisition attempt is expressed as a function of the material mass acquirable in an individual attempt. It is in fact possible that the proliferator might include into his evaluations the possibility to obtain the targeted material by fractioning acquisition into a sub set of similar attempts (this assuming that no learning factors are employed in the model).

If we assume that each attempt is independent (i.e. there is no learning factor imputable to the experience gained by the proliferator), then in order to calculate the overall probability to get the desired amount of material in a given number of attempts, is described by a binomial process.

The top event Pa, which takes into account of the two independent probabilities P_{IN} (intention of the proliferator) and $P_{E,S}$ (probability to covertly elude all the safeguard systems in the location) represents the proliferator's attempt success, while (1-Pa) represents failure. Similarly to the toss of a coin, we can state that at each attempt, the proliferator might either succeed in acquiring covertly the desired material with probability Pa, or he might be detected with probability (1-Pa). Let N be the number of successes in a series of n consecutive trials. We refer to N as a binomial random variable with parameters n, and Pa where 0<Pa<1:

$$P_n(k) = P(N = k) = \binom{n}{k} P_a^k (1 - P_a)^{n-k}, \quad k=0,1,\ldots,n \qquad \text{Eq. 1}$$

If we now want to obtain the probability to have N consecutive successful events, accordingly to the binomial properties, and assuming that Pa is constant, this is calculated simply by Pa^n.

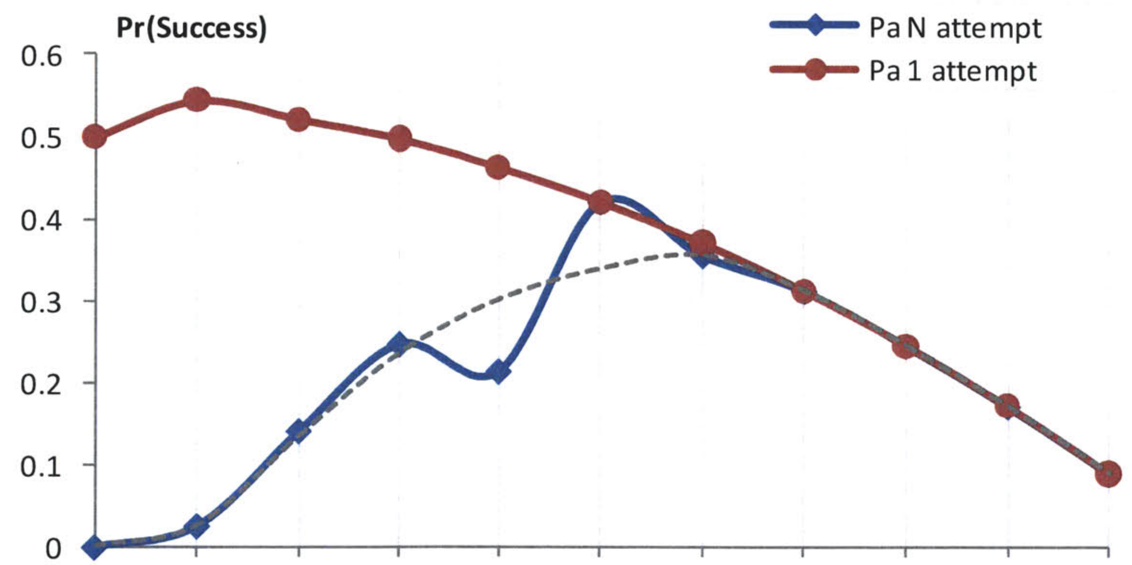
This simple operation, as shown by Table 10, can be used to calculate the probability to acquire SNM throughout a series of identical attempts at a given segment of the fuel cycle.

Table 10. Acquisition probability for a single attempt and for a series N of consecutive attempts.

N rods/attempt	Mass/attempt	Pu Mass/attempt	N SQ/attempt	N attempt 1 SQ	Pin 1 attempt	Pe,s 1 attempt	Pa 1 attempt	Pa N attempt
1	0.43	0.05	0.006	170	0.50	1.00	0.500	0.000
28	11.99	1.32	0.16	6	0.55	0.99	0.545	0.026
55	23.54	2.59	0.32	3	0.58	0.90	0.522	0.142
82	35.10	3.86	0.48	2	0.62	0.80	0.499	0.249
109	46.66	5.13	0.64	2	0.66	0.70	0.464	0.216
136	58.21	6.41	0.80	1	0.70	0.60	0.422	0.422
163	69.77	7.68	0.96	1	0.74	0.50	0.372	0.357
190	81.33	8.95	1.12	1	0.78	0.40	0.313	0.313
217	92.89	10.22	1.28	1	0.82	0.30	0.247	0.247
244	104.44	11.49	1.44	1	0.86	0.20	0.173	0.173
271	116.00	12.77	1.60	1	0.90	0.10	0.090	0.090

The results of the illustrative simulation shown in Table 10 are displayed graphically in Figure 20. The acquisition probability calculated using the Success Tree model shown in Figure 19 represents the proliferator success probability of acquiring a given mass of material from a

SFR power plant. The minimum accountable item, and plausible amount of material, that can be covertly acquired is a SFR fuel rod. To the contrary the maximum amount of material that can be acquired in an attempt is a fuel assembly. A SFR fuel assembly contains 271 fuel rods, and each of them contains 0.05 kg of Plutonium. The first row positioned below the diagram reports the results relative to the acquisition of a fuel rod of 0.4 kg containing 0.05 kg of plutonium and thus roughly more than 0.05% of a significant quantity. In order to collect a significant quantity of plutonium (i.e., 8 kg of Pu), it is require to have 170 identical and successful fuel rod acquisition attempts. Although the probability to be undetected when acquiring a single fuel rod is higher than the one calculated for the acquisition of a single fuel assembly (i.e., $P_{a,fr} = 0.5 > P_{a,fa} = 0.09$), the former requires to have other 169 attempts (i.e., the overall probability of success becomes zero) while the latter requires no further attempts (i.e., $P_{a,fa} = 0.09$). Therefore, with the dataset used for this case, stealing a fuel assembly results more attractive than stealing one or more fuel rods; even the eventuality to acquire sets of 28, 55, 82 and 109 fuel roads per attempt, that are respectively requiring only 6, 3 and 2 consequential acquisition attempts, suggest that the preferred strategy is the acquisition of a fuel assembly in one single attempt. Note that these conclusions apply to the specific assumption formulated for this specific example.



Nro	1	28	55	82	109	136	163	190	217	244	271
N	170	6	3	2	2	1	1	1	1	1	1
SQ	0.006	0.16	0.32	0.48	0.64	0.8	0.96	1.12	1.28	1.44	1.6
M	0.4	12	24	35	47	58	70	81	93	104	116
Mpu	0.05	1.3	2.6	3.9	5.1	6.4	7.7	8.9	10.2	11.5	12.8

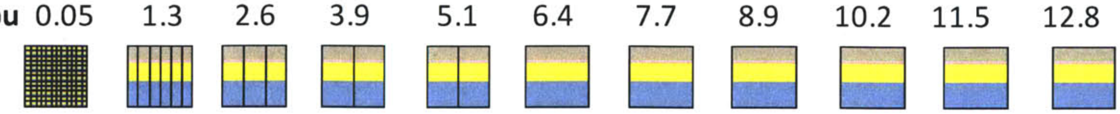


Figure 20. Probability of success per attempt and probability of N consecutive successful attempts.

(2) FUNCTIONAL BARRIERS AND FUNCTIONAL TREES

The higher part of the success tree model has been modeled by means of functional success trees (FST). The FSTs are success trees where the top event are constituted by major anti-proliferation functions rather than particular barrier systems to proliferation. The benefits of this representation are several and different in their nature:

First, this representation is consistent with the Technology Neutral Framework (TNF) representation that has been used for the safety segment of the DoE/NERI project that financed this work. In fact, the safety portion of the project used functional event trees to model the accident sequences.

Second, and related to the previous argument, the adoption of functional trees allows considering different NESs and comparing them using a similar topologic representation of the tree (same initiators and same top events).

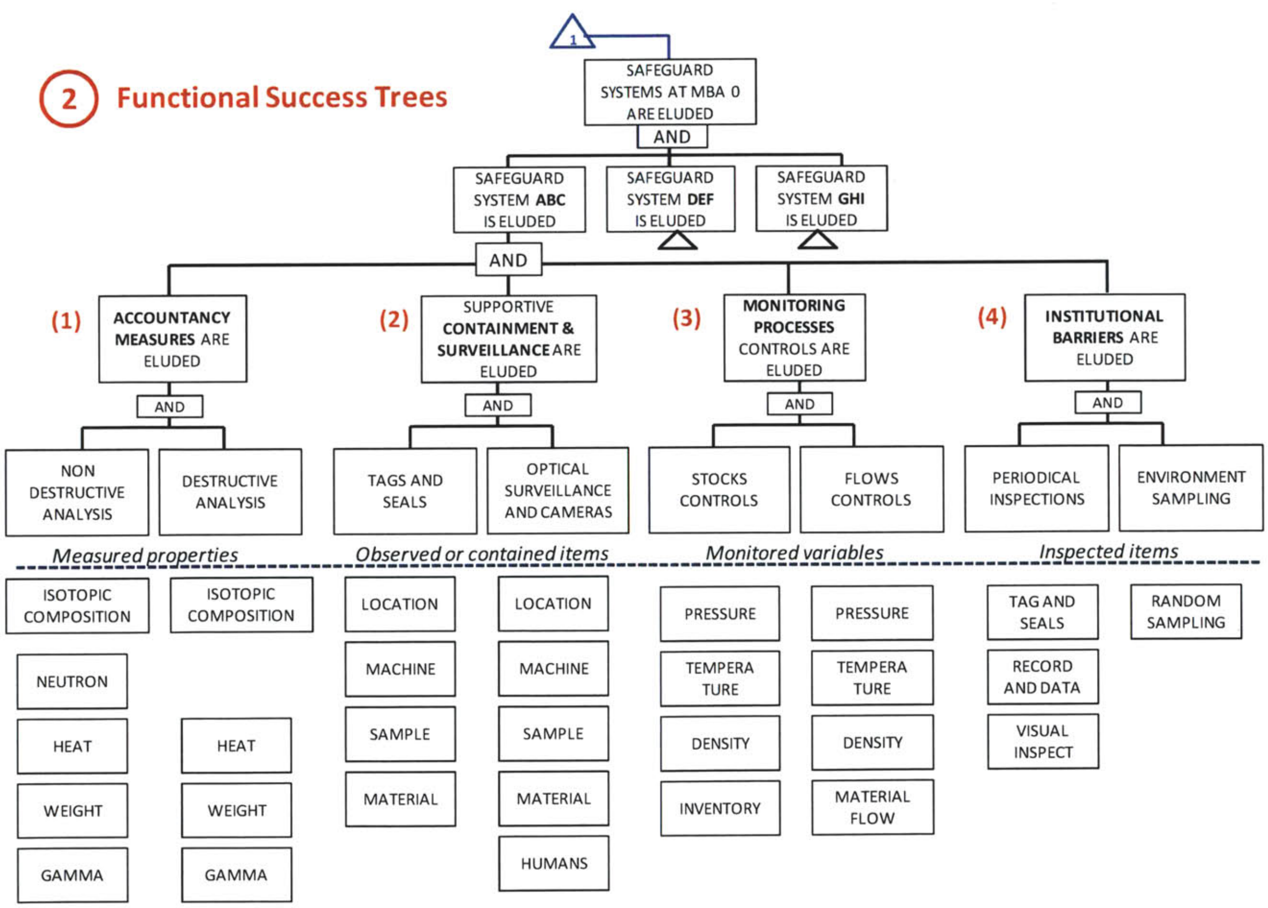


Figure 21. Illustrative sketch of the success tree modeling the principles upon which the different safeguards are based and operated to prevent the acquisition of SNMS as a function of the dominant factors that characterize them.

Although, the response of each NES design is going to be different, those pathways to proliferation passing through the same set of functionalities (i.e., eluding the same safeguards) can be groped, or analyzed together applying a similar procedure to the one used for the License basis events (LBEs) in the safety case. In the safety procedures used in NUREG-1860 (i.e., the TNF), the LBEs are being constructed by binning together safety sequences with similar phenomenology; following the same approach, those pathways to proliferation showing a similar phenomenology can be grouped to determine the worst possible configuration possible.

The functional success tree representation consists of 4 major categories, or top events for the sub-tree shown in Figure 21:

i. Material Accountancy and Counting (MC&A);
ii. Containment and Surveillance (C/S);
iii. Monitoring and Control of processes (M&CP);
iv. Political and institutional barriers (P&I).

These functionalities cover almost the entire spectrum of the counter measures, and barriers which is possible to add to a NES in order to protect, control, and mitigate proliferation risk. these functionalities can be also defined as extrinsic, as opposed to the intrinsic protection offered by the use of nuclear fuels using lower quality plutonium (e.g., addition of with Minor actinides, hydrogen, etc.), or by the construction of NSEs with physical protection systems included by design (e.g., electrorefiner using smaller batch sizes, rooms with smaller doors, etc).

Also note that typically a safeguard systems, which is the sum of more safeguards located to protect the same environment, are composed of systems with different functionalities so that they complete each other's weaknesses and vulnerabilities to specific threats. That is why the events of Figure 21 reports systems that are composed of more than one safeguard. Thus, for example, the first safeguard (ABC), is composed of the three systems A, B, and C. However, the representation of the individual systems start below the function level; this means that System A might be characterized MC&A functionality, while system B and C have both a C/S functionality. The advantage offered by this representation is to permit the analyst to visualize more easily the features of the different safeguards, instead of focusing on the presence of many systems. By recurring to functions and not to systems, the response of a safeguard systems is more immediately related to the threats to which it is exposed to. This concept can be found in form of visual in Figure 22.

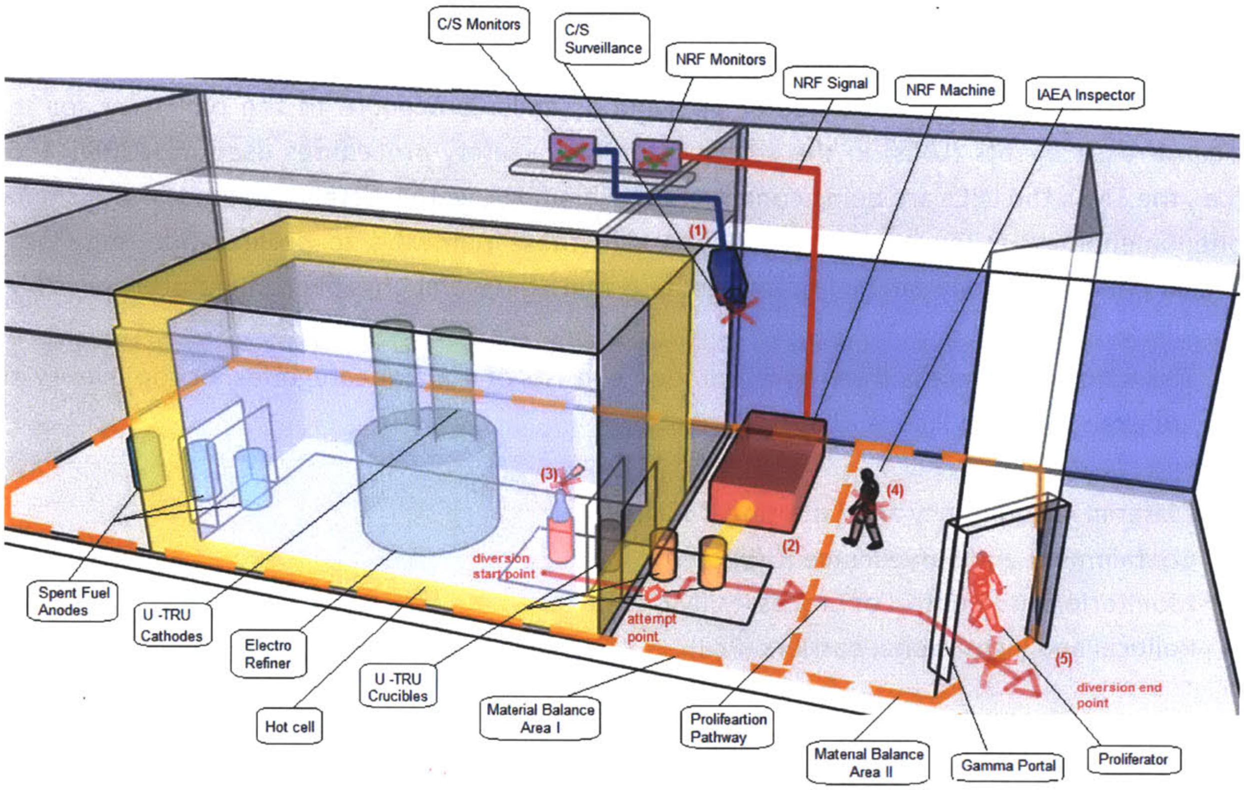


Figure 22. Visualization of covert acquisition at the separation area of a reprocessing facility.

The figure shows a proliferator (red character) eluding all the functionalities from the acquisition point (in this case very unlikely since within the hot cell where separation of nuclear material occurs) to the exit of the facility. On its pathway the proliferator will have to elude an isotopic identification system (1) counting for the difference between the composition of consecutive batches of material, then he will have to elude the surveillance cameras (2), the control on the process done by mean of destructive analyses of samples taken from the separation machinery (3), the verification of inspectors (4). A successful acquisition attempt is not enough to guarantee that the ultimate goal to deploy a NWD is going to come to end. However an important piece of the proliferator' s mission is to transport the acquired material out of the facility, and thus to elude the portal monitors at the facility exit (5). This indeed requires to apply to event trees the same 'functional approach' we used for the success trees.

In conclusion, the adoption of functional trees, provides a useful and ready to visualize matching between the risk assessment model and the real physical sequence of actions that constitute a pathway to proliferation.

In addition, similarly to what we tested for the safety case within the TNF context, it renders simple the evaluations of the proliferation risk by grouping pathways with similar phenomenology Furthermore, the functional trees representation is consistent with the functional classification of the barrier systems defined in the previous section shown in Table 3.

(3) INDIVIDUAL SAFEGUARDS ANALYSIS

For a **physical system**, it is possible to reduce the effectiveness of its primary function (e.g., detection) by reducing any of the sub-functions concurring to the system's response(e.g., signal transmission). For instance, the response of an accountancy measurement system can be decomposed into subsequent sub-responses, for each of which a tactic, finalized to render the system vulnerable to an acquisition threat, can be identified. The list of this possible tactics is explained below and shown in Figure 23.

. ***Tactic 0/ or NO Tactic:*** for certain threats, when the amount of material being targeted is below the accuracy of the measurements system in a given location, no primary tactics are necessary. This happens when the proliferator decide to exploit the accuracy of a detection system. The probability of this event relies on experts' opinion and it can be quantified by means of the so called "standardized experiment" presented in the last Section of this Chapter.

- ***Tactic 1: hardware system.*** This tactic refers to the physical hardware of the measurement system. The proliferator's goal should be to covertly attack the hardware system, in order to change its ability to count SNMs.
- ***Tactic 2: software and signal processing.*** This tactic refers to the software running on the signal processing unit that converts the data collected by the measurement system into opportune spectra of radiation. The proliferator's goal should be to covertly attack this system in order to change the results of the measurements.
- ***Tactic 3: data signal transmission.*** This tactic refers to the transmission systems between the hardware and the processing system. The proliferator's goal should be to substitute the original signal with a fake one.
- ***Tactic 4: analyzed sample.*** This tactic refers to the configuration of the sample being analyzed. The proliferator's goal should be to manipulate the sample in order to generate a fake response to the overall system.
- ***Tactic 5: sample-detector interface.*** This tactic refers to the manipulation of the interface between the hardware system and the sample. The proliferator's goal in this case should be to create to create an interference to the system's response.
- ***Tactic 6: human-system interface.*** This tactic refers to the operators and more generally to the humans employed at the measurement site. For instance, the proliferator's goal should to prevent them communicating any changes in the response of the measurement systems.

None of the above tactics can be perpetuated without the support of additional auxiliary tactics, which in the model are referred as ***supportive tactics***, and that have the essential role to hide the primary tactic from humans, surveillance systems, or remove it from records. Supportive tactics are similar and they can be divided into three categories:

• Supportive tactics to Surveillance systems: optimal cameras pointing material stockpiles, processes, or the access points to a specific location.
• Supportive tactics to Containment systems: seals to the detection and measurement systems.
• Supportive tactics to Humans: bribing, distracting, and neutralizing human operators.

The approach described above applies for functions referring to physical systems and thus for functions from one to three of the functions previous list.

System design principle: *proliferation resistance and physical protection are two interrelated metrics. The success tree combines them together. The primary function of a safeguard is accuracy. Accuracy of measurement is a non-proliferation metric. However, to reduce its effectiveness the proliferator recurs to the use of tactics which are targeted to the secondary functions of the system (physical attacks) to reduce the effectiveness of the primary functions.*

Policy barriers are usually composed of humans and rules that humans have to respect. However policy barriers are not completely human based and they often rely on systems. For instance, countries adhering to the NPT and also signatories of the additional protocol, allow IAEA inspectors to frequently verify the status of operations in their nuclear sites, only in some locations and by means of specified detector types. The current version of the model considers this type of political barrier, and it expresses its performance by measuring the frequency of inspections, f_{INS}.

Once the probability *Pa* is determined, an **Event Tree (ET)**, computes the probability *Pt* to elude the detection of the acquired portion of SNMS by means of instrumentations, or detection barriers, placed between the acquisition point and the facility's exit. The probability *Pt* is in turn obtained by evaluating two independent events:

• The probability P_{Ed} to elude all technical system (i.e., in this case mainly detectors, such as gamma portals, and surveillance systems such as optical cameras) designed to detect the anomalous presence of radioactive material, and positioned along any key route connecting the acquisition point to the exit. P_{Ed} is calculated by means of questionnaires to experts. The elicitation process, similarly to the one used for the ST, also refers to tactics targeted to the various stages of the detection process. However the *NO tactic* scenario in this case does not refer to the proliferator's ability to exploit the instrumentation accuracy but considers the capability to have an alarm not detecting an anomaly when the material is in reality present at the detection point. The probability of this event is in turn determined by:
  - The ratio of fake alarms to the ratio of true positives;
  - The background radiation in the area;
  - The shielding effect of the container holding the stolen piece of SNMs.

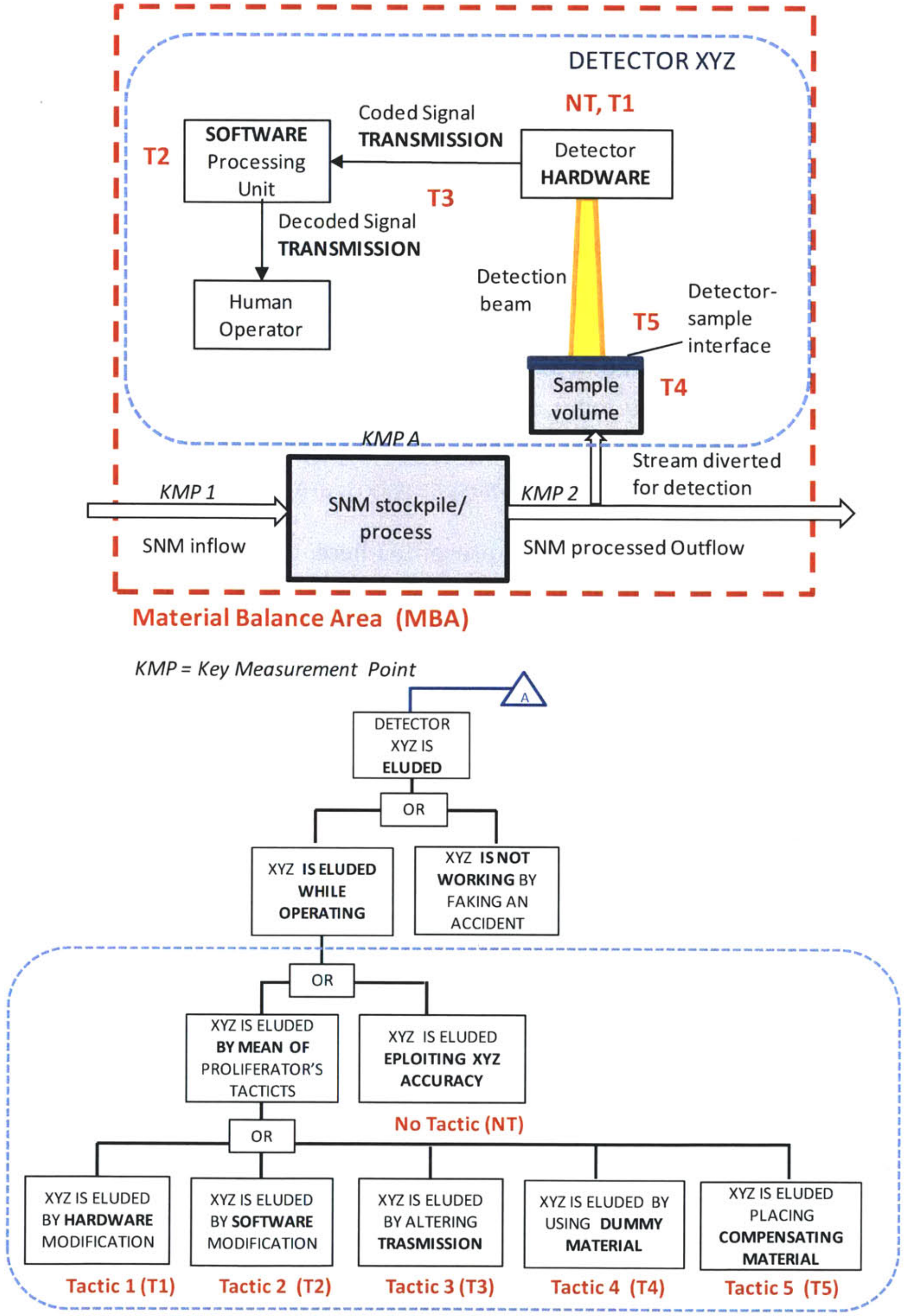
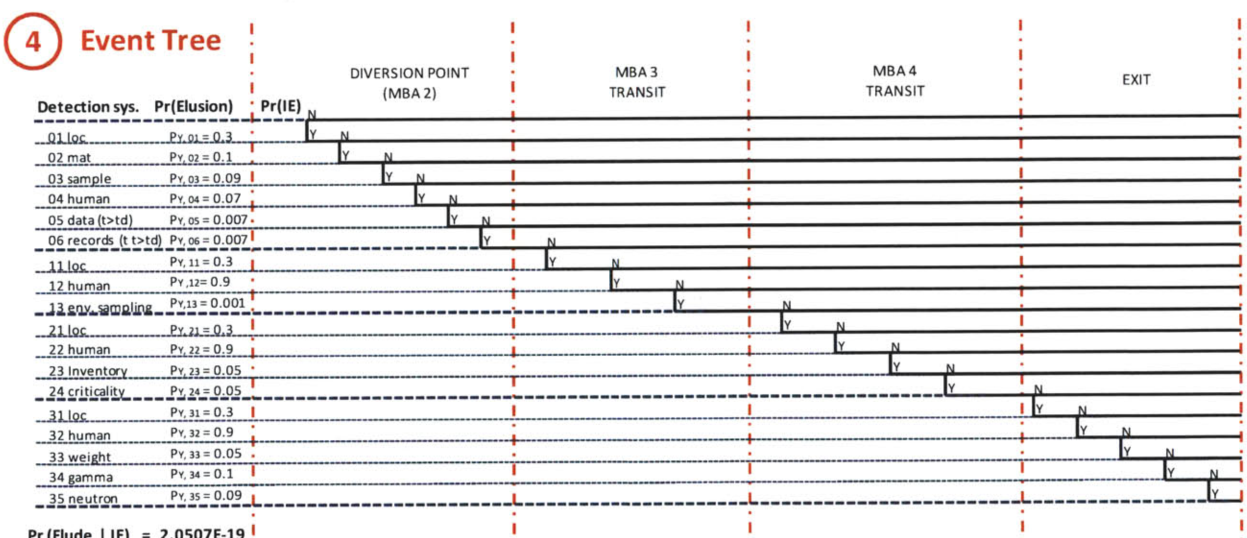


Figure 23: Approach used to determine the proliferator's tactics at a safeguard system. The upper graph shows the human-technology architecture of a detection system monitoring the outlet of a generic process. The tree structure below shows how these tactics are being incorporated into the ST model.

(4) EVENT TREES AND PROLIFERATION PATHWAYS

The last component of the risk assessment model is the event tree. Very often in the literature assessments models measuring the proliferation performance of NESs deliberately omit the transportation phase that has to follow the illicit acquisition of SNMs, or vice versa. Most of the papers in the literature focus on one of the core aspects of the proliferation problem such as acquisition capabilities of a proliferator, or the attractiveness of nuclear materials on site, or the efficacy of the safeguards placed for the protection, or the detection capabilities of safeguards located in a port located miles away from the place where acquisition took place. This tendency in to focus on one of the many aspects of the problem, is such that very few complete assessments incorporating all the features, in this assessment divided into the modules from 1 to 4, explained in the past sections, are present in the literature.

This is not the case of the assessment presented here, where the final and resolute stage of covert acquisition has been modeled by means of an event tree, that in analogy with the safety case, provides the probability to successfully bypass all the detection barriers located between the acquisition point and the exit.



Detection System	Diversion point0	Transit Location 1	Transit Location 2	Exit 3
Accountancy	NA	NA	NA	NA
Cont and Surveill.	X (loc, mat, sample, human)	X (loc, human)	X (loc, human)	X (loc, human)
Monitoring Proc.	-	-	X (inventory)	-
NPT measures	X (data, records)	X (env. sampling)	-	-
Detection System Weight Gamma Neutron	- - -	- - -	- X (criticality) -	X (detection) X(detection) X(detection)

Figure 24. Illustrative sketch of the Event Tree modeling the detection systems and barriers designed to prevent the illicit internal transit of diverted portions of SNMs.

The detection probabilities are modeled by individual success trees which are being quantified with an expert elicitation very similar to the one used for the other safeguard systems.

The event tree is a logic tree model that, similarly to the event trees used in safety models, captures how an initiated threat can evolve until it generates some consequences measurable at the NES. As is noted previously, the consequences in this case cannot be represented by damage to people or structures in the proximity of the NES, but simply measured by the amount of material potentially removed.

The acquisition of the material from a given site does not guarantee that the material is successfully transported out of the facility; in order to complete his mission, the proliferator needs to elude all the detectors located along his pathway to the exit successfully. Similarly to the evolution of an accident in the safety case, the acquired material needs to "propagate" to the exit of the facility without being detected.

The probability of successful transportation metric, Pt, is the top level metric measured by the event tree analysis and when combined with the acquisition metric Pa, it provides the overall probability to succeed in a given scenario, Ps. The complement to this metric (i.e., 1-Ps) measures the likelihood to defend the NES from the effective acquisition of fissile material within the site to out of the site. The detector system located along the proliferator's pathway are needed to discover the portion of SNM potentially subtracted from the proliferator.

CONFIGURATIONS USED TO DETERMINE THE BASIC EVENTS ASSOCIATED WITH MEASUREMENT AND DETECTION SYSTEMS

As earlier stated in this thesis, the proliferator's capability to successfully complete his mission (i.e., concealed acquisition of SNMs) is mainly related to those counter measures (i.e., safeguard systems) designed to measure the amount of materials present in a selected location, and to the detection of anomalies along the potential proliferator's pathway.

The probability to successfully elude a MC&A safeguard system, located in a potential acquisition point, depends upon the accuracy of measurements, the way it is operated, and on the tactics that the proliferator pursue in order to elude its functioning. An MC&A safeguard system can be characterized by various and different system configurations. For simplicity we analyze three major configurations, for each of the two operating modes of recognition and counting. When a measurement system is used to recognize objects (i.e., recognize their composition), can be in one of the three following setups:

A. One operating safeguard which measures the amount of nuclear materials in a given location and compares it to a known expected value.
B. Two identical safeguard systems operating at the inlet and at the outlet of a given process or location (i.e., operating at two consecutive key measurement points), measuring and comparing the two amounts of nuclear materials in the two locations.
C. Two different safeguard systems, operating at the inlet and at the outlet of a given process or location, measuring and comparing the two amounts of nuclear materials in the two locations.

Figure 25 illustrates the three setups. The same three above cases but using the safeguard to count items and thus using the safeguard to count objects, and not to recognize them.

On opposite, the probability to successfully elude a detection safeguard, positioned on a potential proliferator's pathway, depends upon its ability to detect anomalies, the way it is operated, and upon the tactics the proliferator pursue in order to elude its functioning.

A detector does not have different configurations since it is not to count or account for items but to detect anomalies during operations at a given facility.

We can synthesize the above classifications by stating that measurement systems are used to detect the lost or illicit subtraction of SNM masses, in most cases seen as a mass difference (M-ma), while detection systems are used to detect the stolen or lost mass (ma) while it transits from the acquisition point to the exit of a predefined facility.

The probabilistic models are all relying on the evaluations provided by experts from the elicitation process earlier described. The objective of the elicitation is to obtain expert judgment estimates of basic events probabilities to be used in the success tree and event tree models. The following sections describe how the answers from elicitation were used to build the probabilities required to measure the anti-proliferation performance of the measurement and detection systems.

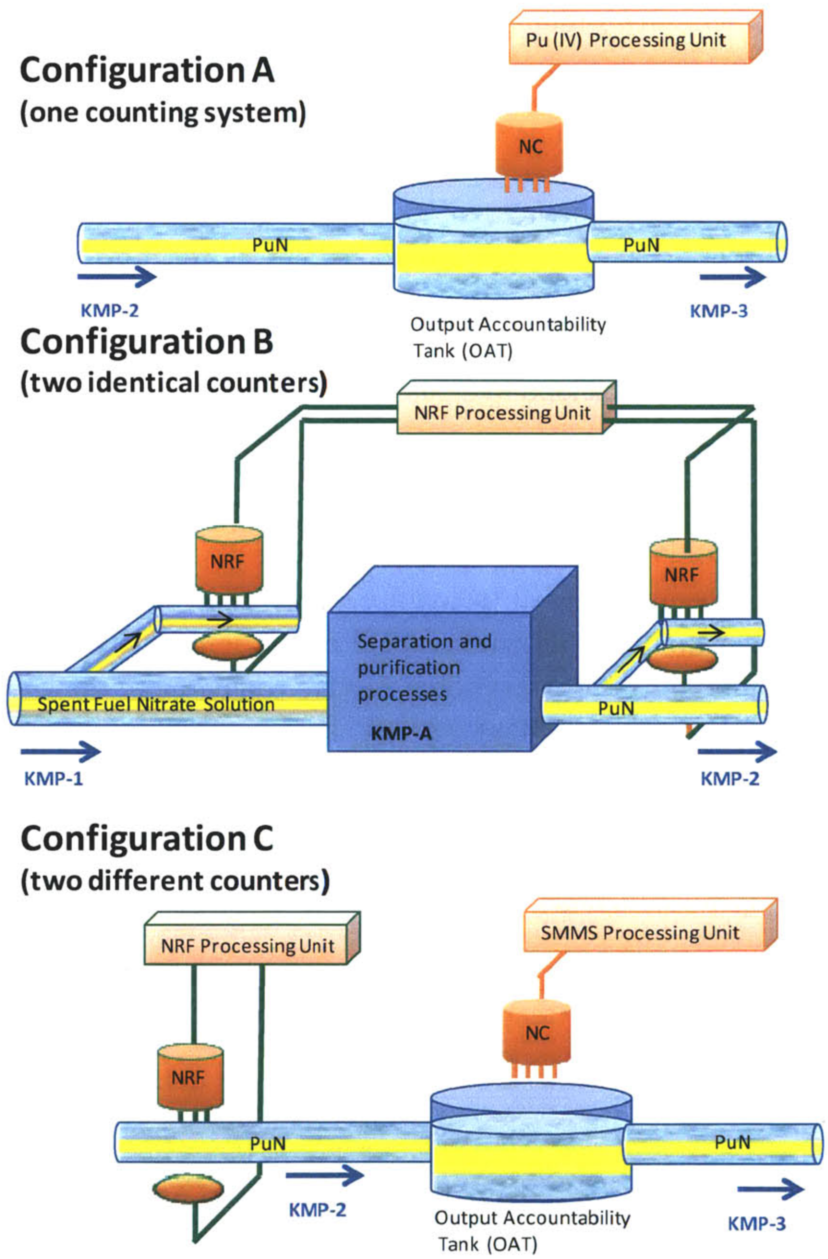


Figure 25. Different configurations used for the safeguard systems.

(M, D) PROBABILISTIC MODEL USED FOR SAFEGUARDS CHARACTERIZED BY A MATERIAL ACCOUNTANCY FUNCTION

The model developed formulated in this Section refers to safeguard systems with mass accounting capabilities, such as a neutron counter used to determine the amount of spontaneous fissions of a plutonium mass. If the safeguard system is used to count items, and thus it has only counting capabilities, such as a gamma detector used to simply count the fuel elements flowing into a given location, then the probabilistic model is simpler and identical to that of an optical camera (see next Chapter).

Probability of detection for a counting system - Configuration A

This evaluation considers the basic event of a proliferator attempting to elude a safeguard system without recurring to any concealment tactic, but by trying to take advantage of the intrinsic limitations of the measurements obtainable from the safeguard system. The objective of the model is to transform the intrinsic performance of the safeguard into a probability function that determines the likelihood to elude the system.

Let's first consider a "measurement" system, such as a neutron counter used for material accountancy purposes. For the simplest set up (i.e., configuration A), the measurement system consists of a detector positioned above an accountability tank containing a stagnant sample of a material mixture. The system is used to count over a certain period of time the number of particles (i.e., neutrons) emitted from one, or more of the isotopes, being part of the material mixture. The data gathered by the system obtained are compared to the known, or expected, value of the neutron spectrum for that isotope at the conditions used for the sampling experiment. This non destructive assay scheme can be used to determine the abundance of special nuclear materials contained in liquid mixture flowing into a pipe of an aqueous reprocessing facility, as shown in Figure 26.

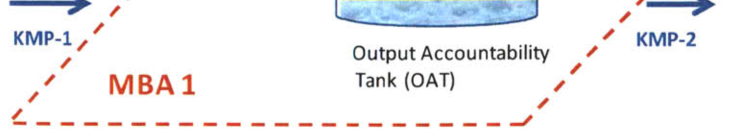


Figure 26. Safeguard system used to measure the amount of materials flowing in a tank.

It is possible to relate the number of particles emitted by the nuclear materials belonging to the total mass. Let *M* be the total mass of material contained inside the accountability tank, and N_M be the number of counts recorded by a generic measurement system. The relationship between the mass *M* and the number of events registered N_M is given by the following equation and shown in Figure 27:

$$N_M = M \cdot \alpha \cdot f \cdot \varepsilon \cdot T \qquad \text{Eq. 2}$$

α is the number of activities per unit mass of material
f is the radiation yield per disintegration, or per fission
ε is the absolute detection efficiency
T is the counting time

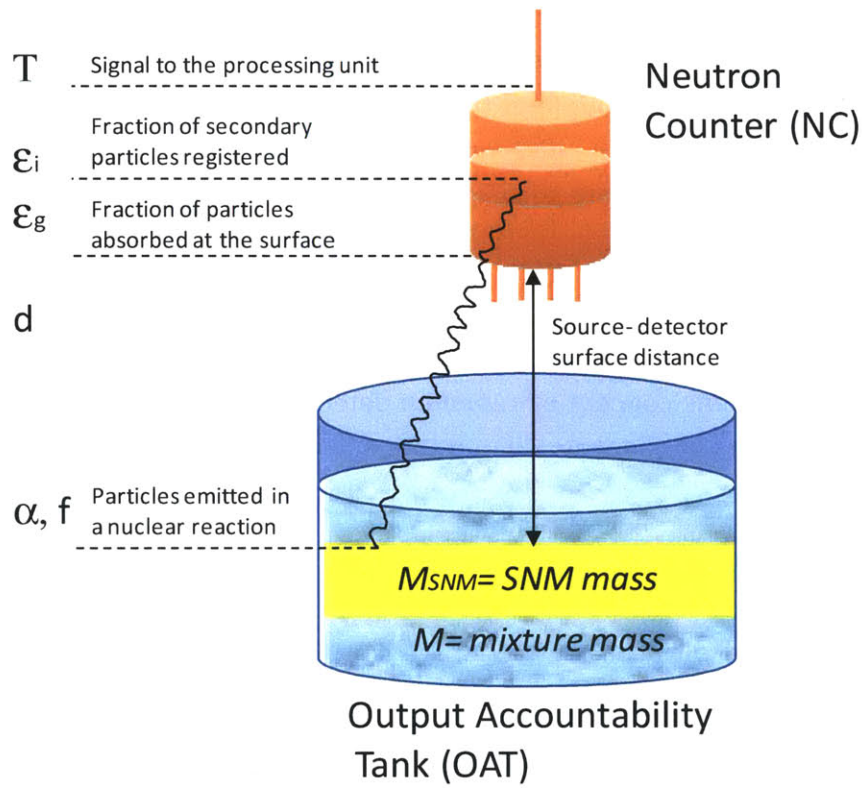


Figure 27. Setup of a safeguard designed to count the amount of nuclear materials.

The radiation yield and the activity per unit mass are known properties of the nuclear material whose quantity has to be determined. The absolute detection efficiency can be divided into two separate components: the intrinsic efficiency and the geometric efficiency. The intrinsic efficiency is a measure of the performance of the detector, and it is the probability that the detector registers a count when a particle hits the detector. The geometric efficiency refers to the material sample and it represents the probability that a particle radiated from the material will reach the detector. The geometric efficiency depends on the distance between the material relative to the detector, the geometry of the detector, and the form of the material sample.

Starting from these input parameters, which are provided by the experts during the elicitation process, the role of the probabilistic model that is being developed is to determine the probability that the measurement system is not going to detect the loss of given quantity of special nuclear materials. Assuming that the proliferator is able to replicate a similar assessment and that he knows the features of the system, then he could elude the system without recurring to any tactic, just by stealing materials in an amount lower to instrument sensitivity.

Definition of the problem

The probability to elude a detection or a measurement system without any tactic, represented by the basic event probability P_{NT} shown by Figure 18, depends on the amount of mass that the proliferator is carrying (and that he originally acquired in the diversion point[14]) with him along his pathway from the diversion point to the facility's exit. The probability to be undetected is determined throughout the expert elicitation process but also a function of other important parameters, primarily represented by L_C and N_B. The first one represent the limit set on the safeguard so to optimize the number of false alarms, while the second are the counts regularly attributable to the background in the KMP where the detection system is located.

In order to define P_{NT}, the concept of minimum detectable amount (MDA) of material has to be introduced and a series of concepts related to it such as the false alarm probability and the detection probability.

Contrarily to a counting system, the primary function of a detection system is not to measure a mass but simply to detect the presence of radioactive source. The performance of a detector system is based on a binary response: only background radiation is present, or a source above background is present. Therefore the problem in this case reduces to a discrimination problem. Let N_T be the number of known counts emitted by a source and N_B the number of background counts. Figure 28 reports the frequency distributions measured by a detector in these two cases, assuming that these are normally distributed and measured over the same detection time.

The performance metric for a counting system used with detection purposes is expressed by the detection probability P_D, by the probability that the detector will erroneously report the

[14] The analysis assumes that the proliferator cannot modify the material after he acquires it. This means that he won't be able to modify the acquired mass (i.e. no separation of the SNM from the rest of the diverted mass), or to fragment the material into sub-portions of the diverted mass.

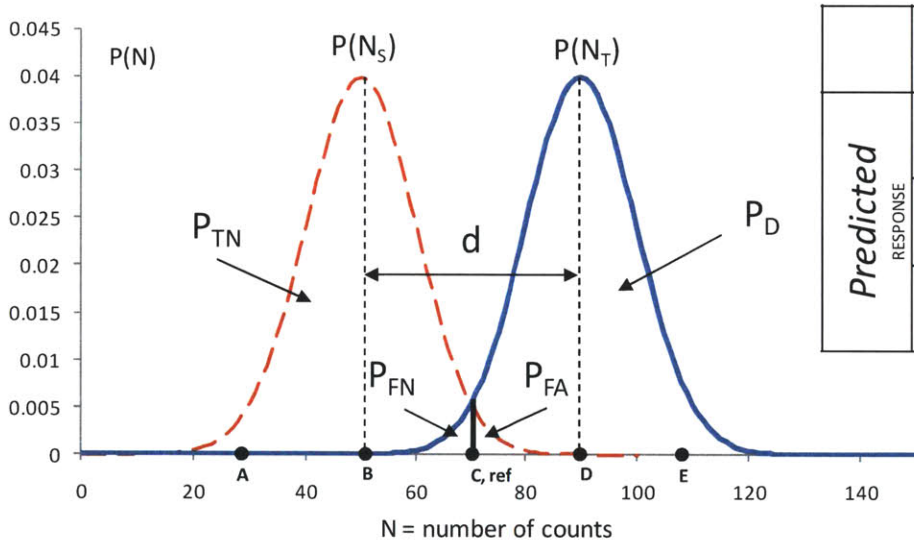
presence of a source when there is no source P_{FA}, and by the threshold value set for the alarm Lc. The optimal point Lc, ref reported in Figure 28 is going to be used for the next definitions.

The probability to detect a weak signal, also referred as true positive, TP, is defined as:

$$P_D = \int_{Lc,ref}^{\infty} P(N_T)dN_T = TP \qquad \text{Eq. 3}$$

The expected systemic fluctuations due to background, also referred as False positives, FP, or false alarm are defined as:

$$P_{FA} = \int_{Lc,ref}^{\infty} P(N_B)dN_B = FP \qquad \text{Eq. 4}$$



		Actual SIGNAL	
Predicted RESPONSE		p PRESENT	n ABSENT
	p' YES	TP HIT	FP ALARM
	n' NO	FN MISS	TN CORR REJ

Figure 28. Example plots of the probability distributions of observing a specific count *N* for background $\boldsymbol{N_B}$ and and for total count $\boldsymbol{N_T}$ when a source is actually present. The four areas delineated by the threshold alarm value $\boldsymbol{Lc, ref}$ determine the possible responses of the instrument. The four responses are summarized by the contingency table reported on the right.

Two other complementary measures can be defined and calculated by the integration of portions of the frequency curves determined by Lc, ref.

A false negative corresponds to a situation where there is no alarm and the source is present:

$$P_{FN} = \int_{0}^{Lc,ref} P(N_T)dN_T = FN = 1 - P_D \qquad \text{Eq. 5}$$

Finally, true negative, is another modality of correct functioning of the detector, also called correct rejection, corresponds to the situation where the alarm does not sound because there is no source to detect.

$$P_{TN} = \int_0^{Lc,ref} P(N_B)dN_B = TN = 1 - P_{FA} \qquad \text{Eq. 6}$$

Two out of the four probabilities above are sufficient to characterize the system properties: P_D, and P_{FA}. These probabilities can be transformed into rates by diving them for the total number of events considered, as shown in Figure 29 which plots the true positive rate versus the false alarm rate. The curves shown above the diagonal are called Receiver Operating Characteristics (ROC). Each curve, including the diagonal represents a different discrimination between the two distributions of Figure 28.

When N_T and N_B perfectly overlapped (curve d_1), the detector is not able to discriminate from the signal and the background (i.e., the system has fifty per cent chance to detect the presence of the source). As the separation distance between the two curves increases, the detector's ability to discriminate the two signals increases.

The ideal detection point is in the upper left corner of the graph (point d_4) which corresponds to an infinite distance between the curves.

Every curve in intermediate position between these two extreme cases, such as Curve d_3, which refers to the separation distance shown by Figure 28, can be obtained by changing the threshold value Lc by running a set of repeated experiments. In the case the two signals (background and source) are normally distributed, the ROC curve is symmetric around point C, which then results to be the optimal point in terms of P_{FA} and P_D. Thus setting the threshold positioned in C, corresponds to a situation where the number of fake alarms are minimized, and at the same time the number of true detected events is maximized. A standard statistic used to describe the overlap of the two distributions, rather than just the separation of their means, is called *"detectability"* [10]. The separations of their means divided by their average, as represented by the average square root of their variance, can be calculated by the equation:

$$d_a = \frac{\mu_{N_T}}{\sqrt{\frac{1+S^2}{2}}} \qquad \text{Eq. 7}$$

where μ_{N_T} is the mean of the source distribution and S is its standard deviation.

It is then evident that a correct choice of the Lc value is critical to the system response. The following section introduces a criterion largely used in nuclear detection application, and that has been adopted as a reference model for the selection of Lc, and used to determined the MDA of detector system throughout the risk-informed framework we developed.

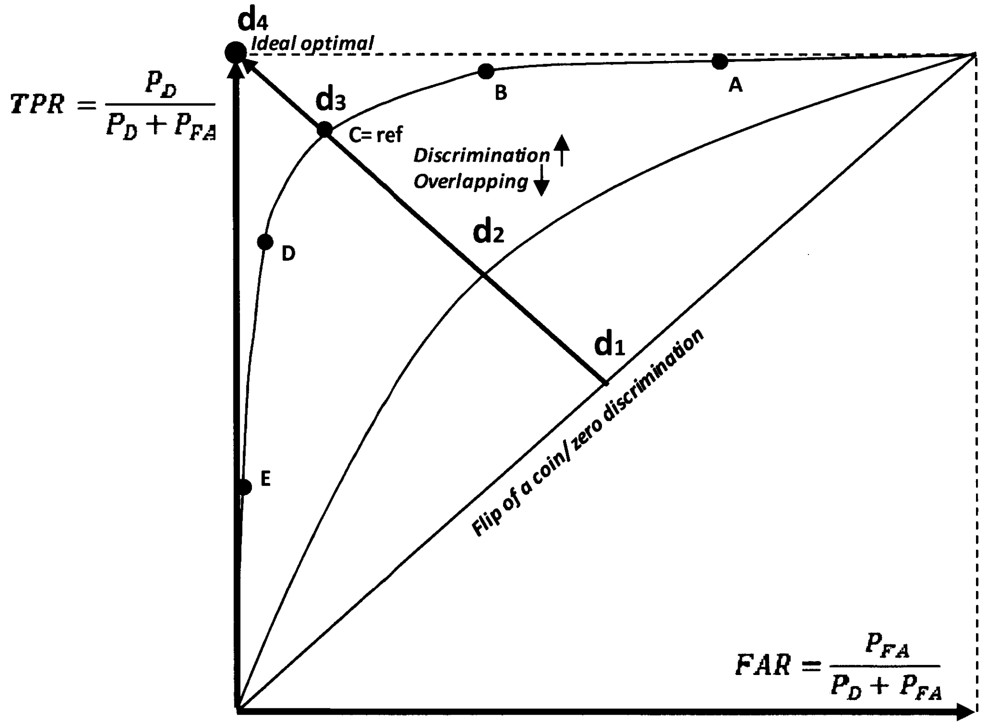


Figure 29. ROC Curve used to generate the summary statistic of a detector.

MDA determination

The concept of MDA implies specific choices that are made for P_{FA} and P_D [10]. One of the most widely used definitions of MDA was introduced by Currie [12] that is based on the arbitrary choice to set up the detection system such that $P_{FA} = 0.05$ and $P_D = 0.95$. For the sake of the present discussion the result obtained by the Currie choice are reported below. The demonstration of their derivation can be found in [12].It is worth to note that the principle used to determine these quantities is true only under the assumption that the background and the source are normally distributed.

Let N_S be the distribution resulting from the subtraction of the number of counts N_B from the total number of counts N_T: $N_S = N_T - N_B$. Let N_m represent the minimum net value of N_S that is high enough to reduce the number of false alarms and simultaneously provide a number of detected responses as specified by Currie, and then modified by Brodsky [13]. Then the two equations below define the minimum number of counts needed from a source to ensure these conditions, and the threshold for the detector:

$$N_m = 4.65\sqrt{N_B} + 3 \qquad \text{Eq. 8}$$

$$L_c = 2.33 \cdot \sigma_{N_B} \qquad \text{Eq. 9}$$

(M) Probabilistic Model Used For Safeguards Characterized by a Measurement Function

N_m can be converted into the mass M_m (i.e., the minimum amount of mass that can be detected by the detector, or MDA) by knowing the source properties (i.e., the geometric efficiency of the sample, its composition and properties), the features of the detector (i.e., its intrinsic efficiency), and the number of counts N_m:

$$\boldsymbol{N_m = MDA = C \cdot N_m} \qquad \text{Eq. 10}$$

where C is equal to the factor reported in Eq. 2.

Procedure used to determine the probability to elude a measurement system without any tactic – configuration A

The following procedure has been set to determine the probability to elude a detection system by simply exploiting its intrinsic ability to detect a mass potentially covertly acquired at a KMP of a nuclear facility.

A pool of experts in a specific safeguard system, for example a gamma portal monitor, is reached and asked to fill a questionnaire. The questionnaire provides a description of a potential acquisition scenario threatening the safeguard system. The questions are of two types: questions dealing with the intrinsic accuracy of detection of the system, and the questions dealing with physical protection auxiliary systems aimed to protect the safeguard from attacked aimed to reduce its primary function. The answers to the first type of questions are used to determine the probability to elude the system with no tactic to which this section refers to.

In order to facilitate the experts' task, a scenario is going to precede the questions. A typical questionnaire is made of the following steps:

1. ***Scenario description***, which include details such as:
   - Type of acquisition threat: for example, theft of SNMs.
   - Typical background in the environment where the system is going to operate.
   - Characterization of the material mixture that is being inspected: SNMs type, other materials, structural materials, and their concentrations per unit mass of mixture.
   - Other relevant information: presence of shielding materials, shielding material and volume, available detection time.
   - Proliferator's strategy and tactics.
2. ***Questions to experts***, who are asked to:
   - Provide the geometric and intrinsic efficiencies of the detector

- Provide the expected number of counts for the masses M_{min}, M_{bc}, M_{max}, and percentage error in their estimate. The criterion with which these masses are selected are: minimum mass detectable, mass conceived for a classical application of the detector, and maximum achievable mass following any design constrain imposed by the detector.

3. ***Collection of the experts' opinions***, averaged following the rules of error propagation.
4. ***Mass computations.*** The resulting point estimates are connected by a fitting function as shown by the graph of Figure 30, and the stolen masses, $M_{thefit1}$, M_{theft2} are inserted into the graph and the corresponding number of counts are obtained via interpolation.
5. ***Sub-probabilities calculations.*** Determine the probability have false negatives and true positives, using Eq. 3 to 6 and using the Currie criterion defined in Eq. 8 and 9.
6. ***Probability of success calculation.*** If the safeguard system is used in a measurement system mode, then MDA is going to be calculated with Eq. 10. The equation is used to calculate all the masses for all scenarios, and to calculate the number of counts for the theft cases. In this case the probability to elude a measurement system, P_{EM}, without any tactic is expressed by the error in the net measurement:

$$P_{EM,1} = E_{M1} = \sqrt{N_S} = \sigma_S \qquad \text{Eq. 11}$$

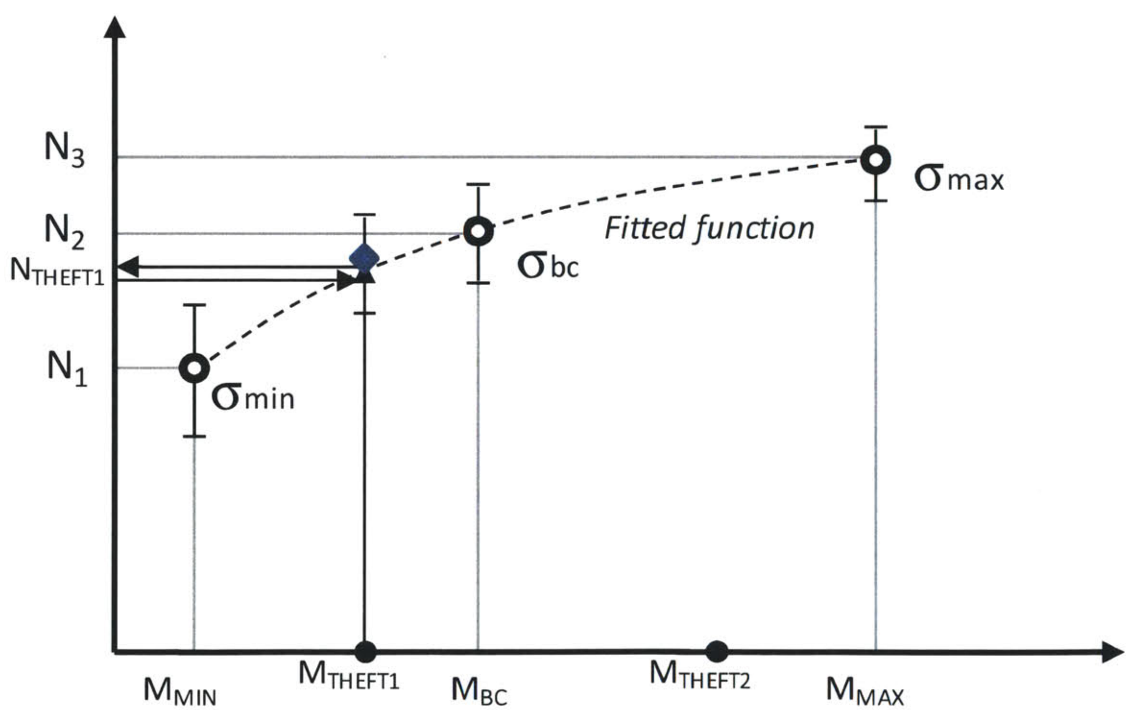


Figure 30. Method used to determine the probabilities to elude a detector system.

Probability of detection for a counting system - Configurations B and C

When a safeguard is operated in conjunction with other safeguards to compute the difference in mass between the input(s) and output(s) associated with a process actuating a transformation of the nuclear fuel or its by-products as shown in Figure 31, this mean that the safeguard system is operating in a material accounting mode. In this case the accuracy evaluation provided by the experts, or systematic error of the safeguards systems can be used to determine the performance measure of the overall safeguard system protecting the material balance area of the figure. If the two systems are identical we call this configuration of type B, if they differ this is a configuration of type C. In both cases the performance of the overall system is calculated by starting from the inventory difference at the MBA of interest:

$$ID(t) = \Delta I(t) + R(t) - S(t) \quad \text{Eq. 12}$$

When a system of safeguards operate in configuration B, or C, they are in a shipper-receiver mode. The shipper-receiver application would require to consider the combined error of two safeguard systems, located at the inlet and outlet of a material balance area, or of a specified process, which is driven by the factor:

$$P_{EM,2} = E_{M2} = \sqrt{\sigma_{Sin}^2 + \sigma_{Sout}^2} \quad \text{Eq. 13}$$

The above equation represents the standard error of the *Inventory Difference* (ID) at a given process which if we assume it is characterized by no in process-changes, when multiplied by $T \cdot m_{in}$ (the flow of materials going through the process over a given time) results into the ID uncertainty expressed in mass, used to regulate nuclear facilities.

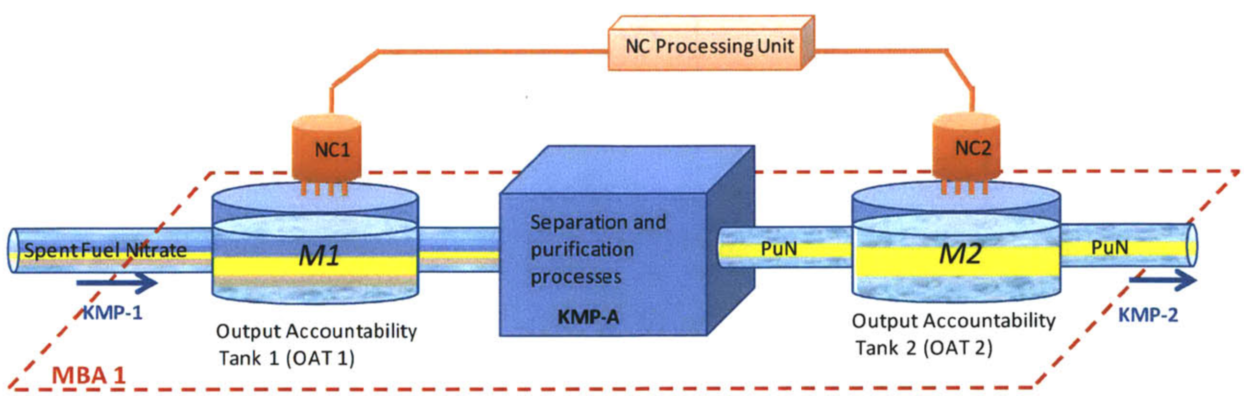


Figure 31. Safeguard system used to measure the amount of materials flowing in a given area.

(D) Probabilistic Model Used For Safeguards Characterized by a Detection Function

The second type of safeguard is the "detection" safeguard, such as the gamma portal traditionally located at the exit of a nuclear facility. The simplest configuration for this system is composed of a gamma detector, a processing unit, and an alarm. The safeguard system is designed to detect and count the presence of items emitting nuclear radiation. The role of the portal is to timely detect anomalies, which typically might be a declared item containing an undeclared SNM mass, or a worker who might carry an undeclared item containing SNMs.

The probabilistic model and the analysis that was carried out to model the performance of this type of safeguard has some similarities with the one in the earlier discussion. However, the evaluation of the number of counts detected by the system considers a new important parameters: the number of counts detected in absence of nuclear sources (i.e., the background radiation in the environment around the portal) and omits a variable that in the previous analysis was pivotal which is the geometry of the sample. Furthermore, while the determination of the minimum detectable amount is still central to the performance evaluation, the output provided by the instrument is not a material mass but a binary signal indicating the presence, or the absence, of extra activity with respect to the background radiation; in presence of a theft attempt, the total amount of radiation detected by the instrument is the sum of the background radiation and of the one generated by the subtracted material mass, M_D.

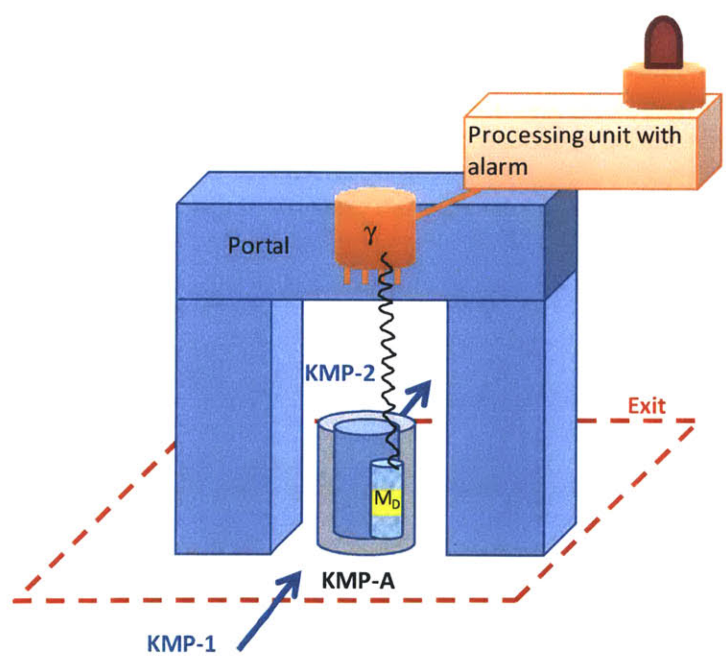


Figure 32. "Detection" type safeguard and diverted material going through the detection region

Consider the shielded canister of Figure 32, containing an hidden pot filled with plutonium nitrate illicitly acquired from the second material balance area of an aqueous reprocessing facility, and travelling through a portal counting gamma radiation. Let N_D be the number of counts of the radiation generated by the undeclared material mass, and N_B be the number of counts of the background radiation present normally in the area where the portal is located. Assuming that the background radiation is constant (i.e., the background radiation during calibration and the one registered over the time of detection are the same), then the total number of counts, N_T, is equal to $N_B + N_D$.

The probability to elude the detector (i.e., the number of events where the counter does not count when a source is present divided by the total number of events) for each of the stolen masses by using the formula:

$$P_{ED} = \frac{FN}{FN+TP} \qquad \text{Eq. 14}$$

(BE) BASIC EVENT PROBABILITES DETERMINATION VIA EXPERTS ELICITATION

Expert elicitation is an explicit and structured process used to incorporate experts' subjective judgments concerning unknown or uncertain quantities and frequencies. Each expert's probabilistic judgment reflects the expert's state of knowledge at the time of response to the question. Examples of experts elicitation processes are widely present in the literature relative to PRA assessments (e.g., NUREG-1150), and in particular to seismic hazard analysis study (SSHAC study). However, principles for collection and use of expert opinion used to evaluate the proliferation performance of safeguard systems have not been established previously [1],[7],[8].

Experts' judgment is used to determine the basic event probabilities being part of the success trees used to determine the acquisition probabilities used to determine the performance of a nuclear energy system exposed to concealed acquisition of SNMs.

Experts in safeguard systems are being asked to participate to a elicitation process consisting of a preliminary telephone interview and of a written questionnaire. The primary interview is carried out to determine the details of a scenario and the setup of the safeguard used to contrast the scenario. The questionnaire is used to determine quantitatively the features of the safeguard system under study in terms of anti-proliferation performance, of physical protection, and costs.

The questionnaire, which was created by first interviewing some experts at MIT [9], is divided into a set of questions of different nature, asking the expert to determine the response of the system in presence of an acquisition attempt, which the proliferator might conduce recurring to specific tactics targeted to the system or to the environment surrounding it. The proliferator might alternatively try to succeed by relying on the intrinsic limits of the safeguard system, or even relying on the fortunate possibility that the system is not going to work as due to its unavailability. Although some of these circumstances might be judged as very unlikely are all included in the analysis. It is possible to categorize the different questions as reported below.

Tactic related questions

These questions are going to be part of a questionnaire targeted to a specific safeguard system. Experts who are asked to answer the questionnaire are familiar with the features of the specific safeguard analyzed.

Type I questions: questions aimed to determine the basic events probability for the case of no proliferator tactic. The safeguard system is assumed to be configured in the regular operational condition and at the expected environmental conditions, as described by the standard experiment reported in the next Section. In this case, the proliferator's objective is to exploit the intrinsic limits of the detection, or measurement, capability of the safeguard system (e.g., the accuracy of measurements). Since the elicitation process reflects the architecture of the Success Tree and Event Tree models, this type of question is going to differ in the two cases of:

- Detection safeguard (Type II.A): the safeguard, located along the proliferator's pathway is used to detect the amount of material acquired. The response of the safeguard is a binary decision whether the safeguard detects a diversion or not (e.g., weight sensor detecting an anomaly).
- Measurement safeguard (Type II.B): the safeguard located in a location plausible for acquisition is used to measure and account for the amount of targeted material, or to verify the level of facility operations. The conclusion from the outputs of the measurement is whether or not some amount of material is missing (e.g., the mass of a radionuclide measured by a NRF detector and the expected mass of the radionuclide in a location), or the existing of any mismatch between a declared level of a process and the measured level(e.g., the power measured by an antineutrino detector close to the reactor core and the actual power level).

Type II questions: questions aimed to determine the basic events probabilities for the cases characterized by a proliferator concealment tactic. The proliferator attempts to attack the safeguard system or sub-systems, or to modify the material, or to interfere with the environmental conditions under which the safeguard normally operates. In this case, the proliferator's objective is to elude the safeguard by reducing or annulling the safeguard's primary function (i.e., detection capability, or measurement capability).

Non tactic related questions

Type III questions: questions aimed to determine the basic events probability corresponding to the eventuality that the safeguards system is not going to actuate as it is supposed to. This probability in most of the cases, corresponds to the unavailability of the safeguard system. This number is usually provided by the manufacturer. Traditionally safeguards systems, are characterized by high standards of availability and reliability, thus this question is included in the assessment for the sake of completeness.

Type IV Questions: are not related to the specific safeguard. However, the determination of the basic event probabilities contribute the overall chance to elude the safeguard system for a proliferator. These basic events are positioned very high in the hierarchical structure of the three and they represents eventualities not related to the safeguard-proliferator competition. These eventualities can be summarized in the following categories:

- Activities are successfully initiated;
- Installation of a system is adequate;
- Installed system operates well;
- Diversion is detected accidentally;
- Intelligence detects diversion.

The questions ask for the safeguard uncertainty of measurement, which can be used to derive the proliferator success probability to elude the safeguard without additional tactic.

Elicitation Protocol

The following list reports the steps for the elicitation process established to determine the basic event probabilities used in the framework. The procedure is an adaptation of the ten steps process formalized for the first time in NUREG-1150, and which consequently became integral part of PRA evaluations [1].

Step 1: Selection of experts.
The credibility of the study relies upon the appropriateness of the experts selection process and upon their expertise.

Step 2: Identification of the scenario and selection of major issues (e.g., safeguard setup, material sample, etc.).
This is a qualitative analysis conducted via phone with the scope to create a realistic situation, evaluated with a certain degree unanimity from the different pool of experts.

Step 3: Provision of a uniform background database and preparation material.
The material has to be prepared in advance, collect all the feedbacks and details provided by the preliminary qualitative survey conducted with experts.

Step 4: Expert training and preparation for the elicitation.
This step is optional, but it becomes mandatory each time experts have no specific preparation in probabilities, and they are not familiar with the Boolean logic of the trees used in the framework.

Step 5: Individual Expert Elicitation.
This constitute the core of the elicitation process. In this phase the experts answer the quantitative part of the questionnaire. From the individual elicitations of probability judgments a precise probability statement of the expert's opinions can be obtained.

Step 6: Aggregation of the individual expert inputs and feedbacks.

The answers provided by the experts are being equally weighted and aggregated into one unique result, which then by definition express their overall opinion on some features of the safeguard performance. Equal weighting of the individual probabilities has been chosen to avoids arbitrary factors such as the evaluation of the experts and to lower the possibility of eliciting extreme non-defensible opinions.

Step 7: Finalizing expert inputs.

This step finalizes all those question that by being aggregated directly provide an evaluation of the basic event probabilities which are going to be used by the assessment model.

Step 8: Conversion, whether necessary, of the expert input into basic event probabilities.

From the previous step, type II question, which is relative to the intrinsic safeguard capability of detection or measurement is being left out. For them it is required to use the combine the information and run a separate model before plugging it into the assessment model.

Step 9: Insertion of the basic event probabilities into the Success and Event Trees.

All the basic probabilities can be inserted into the tree, including the ones obtained from other experts and relative to other type of safeguards. The assessment is thus able to provide consistent replies.

Step 10: Calculation of the model performance and of its associated costs.

The final calculation relates the overall calculated performance of the system to the overall cost of the overall safeguard system.

An extra step to the process included as "resolution of disagreements" or the final "review" from the experts. This step which is normally included in other elicitation process such as the ones used in NUREG-1150 and in the SSHAC study, are not being used because it requires to have the experts located in the same place.

Summary

This concludes the section dedicated to the formal elicitation process used to determine the values of the basic event probabilities used in the assessment model describing the proliferation performance of a safeguard system. The following section provides an example of a questionnaire used to determine the proliferation performance of a specific safeguard.

The proposed methodology drives parallels with the implementation of probabilistic risk assessment (PRA) techniques for safety-related considerations to then propose a PRA-like technique tailored to proliferation-related concerns.

Contrary to previously suggested methods and metrics for proliferation resistance assessment, the methodology here proposed for measuring proliferation performance leaves out rather subjective assumptions for computing proliferation-related quantities and can be structured to rely on quantities that can be obtained from databases, or experiments, in addition to those that can be obtained from well-defined and contained expert's judgment.

For example, probability values associated with the "*system is eluded*" block in Figure 33 can be acceptably estimated via actual/simulated experiments for a particular system, diversion pathway, and diversion barrier of interest.

Uncertainties of the results can thus be reduced by limiting the use of highly subjective expert's judgment. In this regard and to illustrate this point, the methodology also removes the presence of uncertainties deriving from having not only to quantify proliferator's behaviors regarding proliferation (e.g., initial willingness to initiate a diversion attempt, or similarly, initiating event frequency) but also to consider the ultimate consequences of proliferation-driven activities.

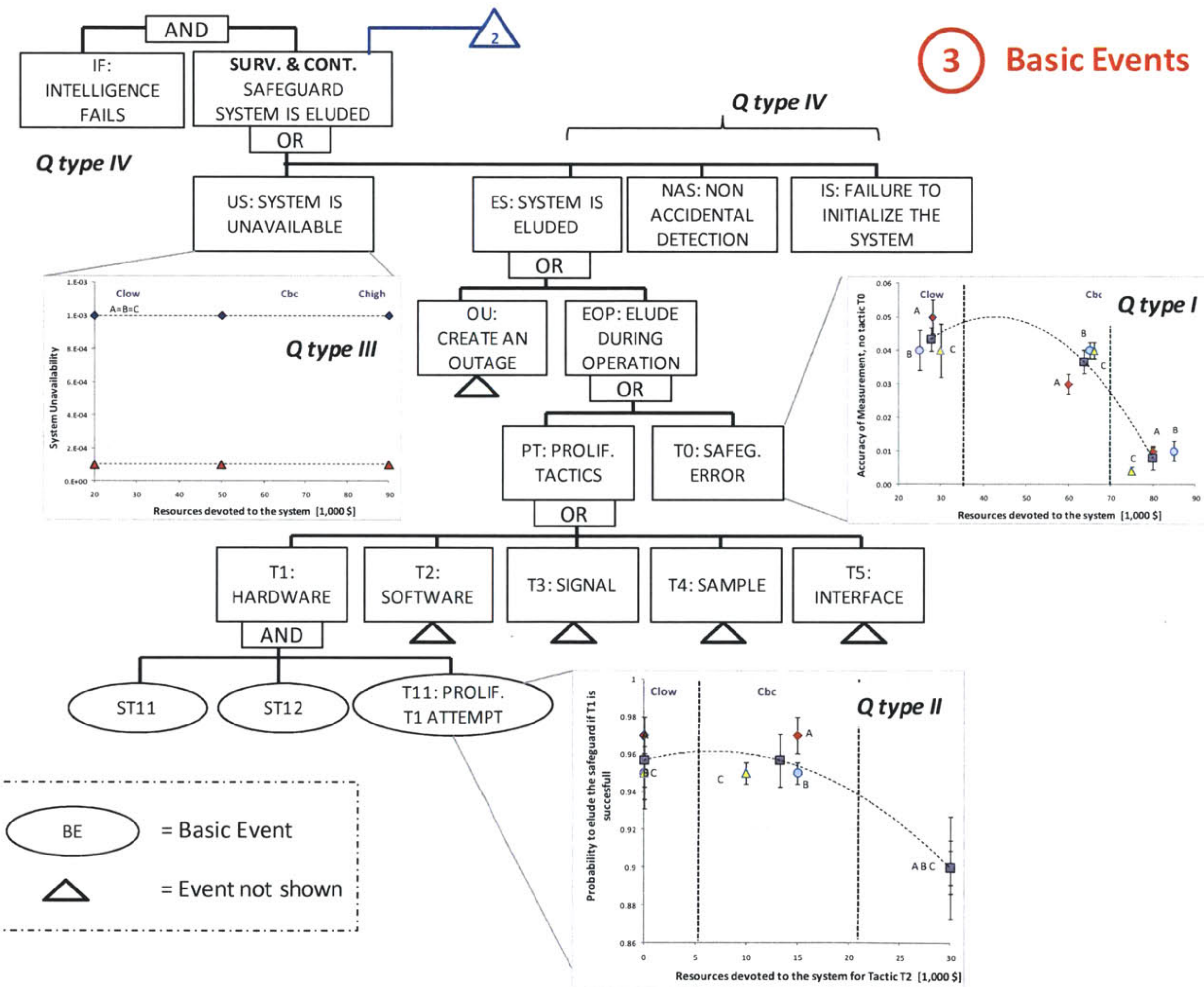


Figure 33. Lower structure of the tree showing the basic event and the aggregated probabilities determined via the systematic expert elicitation protocol.

(SE) THE STANDARDIZED EXPERIMENT

The previous Section provided the general math of detection and measurement theory. This Section bridges those notions with the elicitation process that is required to determine the probability to elude a safeguard without any tactic, which means by simply exploiting its accuracy level. Questionnaires distributed to experts describe an experiment, corresponding to a simplified and standardized set up for the safeguard machine at the NES, and that we call the standardized experiment. The evaluations provided by the experts are used to determine the basic event probability to elude a safeguard without any tactic, with the procedures explained in this and the following Sections.

Region I of Figure 1 contains diversion and theft threats. Diversion and theft are characterized by the acquisition of SNM in amounts that are between 0 and 1 significant quantity. Given the small scale of the mass that is being targeted, in order to defend a NES from the occurrence of these types of threats, barriers to proliferation are mainly represented by measurement systems. The primary function of these systems is to account and count the amount of mass of SNMs, thus they are defined by a functional tree model considering the MC&A function as a top event. The fundamental metric characterizing an MC&A instrument is the accuracy of the measurement, or following definition 10.6 given by the IAEA guide to safeguard systems, is the systematic error of the measurement system.

Systematic error is sometimes referred to as measurement accuracy because it characterizes how close the measurement is to the 'true' value: the higher the accuracy, the smaller the systematic error.

Usually the systematic error is lower for systems executing the analysis on a destructive assay (DA), and less accurate for non destructive assay (NDA) measurements. However, the systematic error is not the only important metric defining a measurement system:

Time is another important metric. For example, DA techniques, in general require longer time than NDA ones. Time is a fundamental metric since IAEA goals require to "timely detect losses of SNMs in a nuclear facility", but many advanced measurement systems are not capable to simultaneously reach time and accuracy requirements. This is a key aspect of the non-proliferation problem.

Another important parameter, or metric, is the geometry of the sample. While DA techniques are designed so that a specified sample form can be throughout procedures aimed to reduce or eliminate sources of disturbance such as the radiation field generated by isotopes that are part of the material mixture, NDA techniques have less flexibility regarding the geometry of the sample, which might decrease substantially the overall accuracy of the measurement.

Because of these problems, an unique standardized process was created in order to favor the comparison between different measurement systems, which is ultimately needed to compare the resistance to acquisition of SNMs (or resistance to undeclared loss of SNMs) of nuclear energy systems protected by different safeguard schemes. The standardized process is part of the expert elicitation process and it consists of setting up a standardized experiment for the safeguard system, whether this is a measurement or a detection system. Since detection and measurement systems present diversities with respect of the parameters that characterize them and that are relevant to the analysis, therefore two types of standard experiments are possible and described as it follows.

Standardized Experiment for a Measurement System

The following procedure has been established in order to evaluate the overall accuracy of a measurement system.

A measurement system is being selected, to be tested against a particular threat in a specific location of a NES (i.e., a Material Balance Area, or MBA). Usually more than one system is placed to protect a given MBA. A simple configuration is to have two measurement systems of the same type located at the inlet of the MBA (i.e., inlet key measurement point, or KMP_{in}) and at the outlet (i.e., outlet key measurement point or KMP_{out}). The following procedure refers to and is being repeated for each measurement system located in a selected KMP. The information obtained from individual KMPs are combined by means Eq. 12.

The three ingredients for the resolution of the problem, in a given location are: the location, the selection of the safeguard systems used to protect that location, and the characteristics of the material in that location.

The location determines the environmental conditions under which the experiment is being set up, such as the background field. The material features, such as the material form, isotopic composition, the activity, and geometric conditions of the sample and of the container holding the sample are specified to the expert.

The selection of a measurement system implies knowing its intrinsic efficiency, and by knowing the features specified above this means also knowing the geometric efficiency.

The only variable not being specified then remain the amount of material to be measured. Given, the experimental set up characterized by the experts are asked to provide the number of counts, and the confidence level in their estimate, that are expected by the instrument for three different amount of material being measured, assuming that counts and background are normally distributed. From the number of counts the accuracy of the instrument can be inferred by using Eq. 2. As an alternative, experts can directly provide an estimate of the expected accuracy for each of the three amounts of material. When the experts provide an estimate of these quantities, the measurement time is being communicate to them and it is constant. The duration of the experiment depends on the facility requirements and from the type of techniques used. NDA techniques are effectively limited by the operations in the facility, and thus time is constrained by an economic factor. The time of a DA technique is usually set to the time required to obtain the best accuracy in the measure. However this might conflict with the IAEA requirements of prompt detection, thus also in this case, time might be imposed by the analyst running the model.

Note that the three amounts of material, are the same for all experts interviewed but change from safeguard to safeguard, since their values are determined by the features of the location (i.e., the maximum, and the reference amount of mass present or flowing in that location), by the features of the safeguard (i.e., the minimum amount of detectable mass by the safeguard), and, or by a combination of these features. It is important to highlight the fact that these three masses are determined following a safeguard perspective, and that they do not by any mean represent the amount of material that the proliferator is targeting for a covert acquisition threat. The mass that the proliferator targets for acquisition is by definition an unknown, thus represented by an intermediate point in the range that defines a theft scenario (i.e., between 0 and 1 SQ). The amount of material targeted for an acquisition attempt, is arbitrarily chosen by the analyst using the model. The accuracy, or the number of counts, corresponding with which a theft threat, or material loss, can be identified are usually obtain by interpolation, with a procedure similar to the one shown by Figure 30. Note that each point of the figure is going to be obtained by computing the difference between the systematic errors of two contiguous safeguard systems, using Eq. 13.

Standardized Experiment for a Detection System

For a detection system, the procedure is similar to one used for a measurement system, the procedure that is being followed focuses on other metrics, such as background, and false alarm rates. Contrary to measurement, the sample of a detection safeguard is simply an unknown. While the objective of a measurement technique is to measure a material property, generally its mass, the objective of a detection system is simply to detect the presence of a material with a given activity. The material is supposed to be of unknown activity, and thus the safeguard is designed to detect any activity above and different from the background signal. However, since the detection system is placed to protect a given plant, which uses and stores materials of known activities, a range of plausible amount of materials can be assumed. In this case the determination of MDA and the use of ROC curves are central to the problem. The accuracy of a detector system is determined by setting up a standardized experiment where the experts are once again asked to provide the number of counts in correspondence of three reference masses determined with the same criteria explained in the previous Section. Assuming a predefined value of *Lc,ref,* and a background value, and very limited time for detection, the accuracy of the instrument is defined by Eq. 14. Although MDA is a key metric in this case since it represents a cut off value for the likelihood to predict detection, above this value is still not possible to affirm that detection is going to occur with certainty. Also in this case an interpolation is being used as shown by Figure 30, where each point of the curve directly represents the estimate of accuracy provided by the experts.

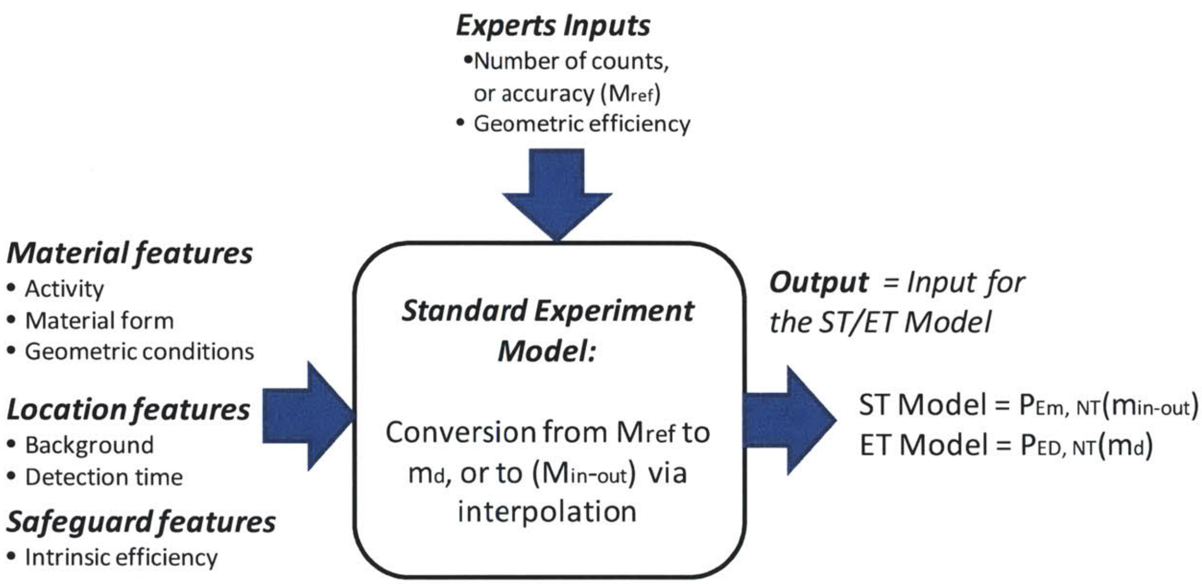


Figure 34. Structure of the experiment used to determine the accuracy of a safeguard system.

Figure 35 reports the basic structure of the standardized experiment as it used to connect the probabilistic models of detection and measurement systems to the ST/ET model. The information, or features required to re-create a standardized experiment are reported in Appendix C.5, under the name of "Safeguards and Samples Features at the Reprocessing Plant". Appendix C shows how an analysis of an entire reprocessing plant can be decomposed systematically into sub experiments collecting the metrics required to determine the accuracy of a safeguard system composed of one, two, or more instruments. Most of the fields of appendix C are left empty since it refers to an existing reprocessing facility in Japan, the Rokkasho facility, that was safeguarded by the IAEA, which is not disclosing the values of most of the parameters characterizing the plant.

EXAMPLE OF A QUESTIONNAIRE USED IN THE ELICITATION PROCESS

PART I: Introduction and Success Tree Methodology

Introduction

This document contains a summary of our methodology to assess nuclear safeguards, and the questionnaire used to estimate the probabilities of the events characterizing typical acquisition scenarios (e.g., diversion, or misuse) in a nuclear facility.

Please note that this document is designed to provide a quick way for an expert to participate to the elicitation process. The present example of questionnaire refers to an antineutrino safeguard system, located at a given distance from a power plant, having the objective to monitor the core power of the plant and therefore prevent the occurrence of misuse and diversion during operations or refueling.

Methodology

In order to determine the effective capabilities of safeguard systems we are utilizing a method called "Success Tree", which adopts the topology of the fault trees commonly used for safety analyses (i.e., Probabilistic Risk Assessment). The tree decomposes the actions that a proliferator has to achieve in order to acquire the Special Nuclear Material (SNM), it defines them in term of probabilities, and then combines them. The top event of the success tree represents the capability to elude a safeguard system, which depends on two main factors: the first factor is intrinsic to the detection system's ability to detect special nuclear materials: depending on the amount of material potentially subtracted by a proliferator, the safeguard might not be able to detect the difference between the initial amount and the final amount after subtraction. This happens when the proliferator acquires an amount of material that is below the mass threshold at which the instrument detects the presence of a given special nuclear material. The probability associated with this event, labeled as 'no tactic', can be inferred by knowing the accuracy of the safeguard. Therefore, in order to determine this probability you are asked to provide evaluations about the safeguard's accuracy and its associate uncertainty for a given mass of material. For example, you should say that an antineutrino detector (ATD) can detect a 80 kg of Pu difference on a total mass of 3 tons of Pu loaded in the core with an error of 10%.

In the case that the amount of diverted material is within the range of detection of the instrument, then the proliferator needs to rely upon additional tactics aimed to reduce the effectiveness of the detection system (see Table 11). The probabilities associated with these events are labeled as 'Tactic A-D". In this case, you are asked to provide evaluations about the probability that the safeguard is going to provide an improper response as due to the specific proliferator's threat. For example, you should try to address what is the probability that the ATD system is not going to provide a reliable response when a portable accelerator, or any other antimatter generator, is turned on at the plant site with the scope to create interferences in the antineutrino's flux.

In conclusion, our method relies on a set of 5 key questions, associated with 5 basic event probabilities that we will derive based upon your answers. These are summarized in Table 11[15].

Table 11. Basic Event probabilities and tactics for an antineutrino detection system.

Tactic	*Inferred Basic Event Probability*	*Tactic Description*
No Tactic	The probability that the proliferator will successfully elude the ATD **without recurring to any tactic** can be easily related to the accuracy of the instrument	Knowing on the ATD accuracy, proliferator diverts the material in an amount that is within the expected error of the measurement. (e.g., the proliferator might decide to swap one fuel element at once and to repeat the swap six times)
Tactic A	Probability that the proliferator will successfully elude the ATD by using **an antimatter generator at the site**	Proliferator disposes of an accelerator which he uses to interfere with the main antimatter flux generated by the reactor. The accelerator can be the one belonging to a nuclear resonance machine installed onsite to verify the fuel composition.
Tactic B	Probability that the proliferator will successfully elude the ATD by **synchronize the misuse-swapping threat with post refueling of other reactor's units** in the region	The proliferator decide to insert the fuel elements in correspondence of the re-start after refueling of other located reactors in the same region, or site. This can alter the ATD response just for a short period of time. Please indicate the time.
Tactic C	The probability that the detector is not going to work properly due to a a **black-out** in the area where the ATD is located caused by the proliferator.	this strategy implies that that the proliferator is aware of the existence of the ATD and that he is also capable to exercise a threat on the electric grid where the ATD is located.
Tactic D	**Operator declares a different level of power** of the reactor to compensate the decrease in the neutron flux generated by the 6 missing fuel elements in the core.	In this case the proliferator should probably be the hosting state or he has to bribe many other operators in the plant.

[15] Note that the tactics in the table are just proposed by the author and that can be readjusted accordingly to your experience.

In some cases, it is possible that your expertise might be more useful to address only the accuracy of the detection system. It is expected that a person dealing with a specific safeguard might not be aware of software related problems or he/she might not have been personally involved in the definition of physical protection systems protecting the hardware components of the detector from being manipulated. It is therefore suggested to either try to qualitatively address the questions or to pass the question to your colleagues/teammates/ people in your company that might have a specific background useful to address these issues. Alternatively, we ask you to do the effort to answer all the questions in the best of your ability.

Factors affecting the probabilities and the accuracy estimates

An important aspect of our framework is that the estimates of the probabilities depends on some variables:

• The accuracy of measurement is a function of the amount of material that is being measured (M), and also a function of the resources that the safeguarder devotes to the safeguard, or its final cost (C).

Example: a traditional measurement system would have an higher accuracy and lower errors as the mass of the sample (M) increases. However, in certain situations the increase in size of the sample generates self shielding effects which might lead to a decrease of accuracy. In these cases the accuracy and the error can decrease as the sample mass increases[16].

The accuracy of a measurement also depends on the resources devoted to the detection system. For example, if multiple ATD systems are employed, and if their size is increased, then the accuracy of the measurements increases. Therefore we can start from a low profile version of the detector of cost C_{low} with a given associated performance and then arrive to an optimal version of the same detector with a cost $C_{opt.}$

• The proliferator's probability to succeed with any of the four key tactics is a function of the additional resources devoted (C_{add})to protect the safeguard system from tactics (e.g., the resources the safeguarder devotes to add physical protection systems).

Example: the proliferator might be aware of the existence of the antineutrino detector on the site and he causes a black-out at the ADT system. The safeguarder might can counter act to this scenario by adding two back-up trains of cost C_{add}. This cost voice represents an extra being

[16] For an ATD system the sample mass M is represented by the amount of materials generating the fissions within the core (i.e., mass of all the fissile species at a given time).

added to the safeguard costs (C_{low}, C_{bc}, and C_{opt}) for each of the three configurations (low, base case and optimal).

The definitions of masses and costs for the three different cases are provided by the following table.

Table 12. Cost and mass factors affecting the probabilities and the accuracy evaluation.

Factor	*Description*		*Example*
Total mass of the material under detection	M_{low}	Lowest detectable mass /mass difference	80 kg of Pu
	$\mathbf{M_{bc}}$	Base case mass, or regular mass of material under detection region in the facility	300 kg Pu
	M_{high}	Highest mass, or maximum conceivable mass	Kg of Pu loaded in the Core
Cost of the safeguard	C_{low}+ C_{add}	Cost of the safeguard for it to operate, or cost of the typical safeguard configuration	1 ATD, small size
	$\mathbf{C_{bc}}$ + C_{add}	Cost of the safeguard with additional features to increase its efficiency and protecting it from tactics	2 ATD, medium size
	C_{opt}+ C_{add}	Cost of the safeguard to let it operate at the optimal efficiency, and to fully protect it from tactics	2 ATD, large size

Other factors contributing to the probability to elude the system

Other contributors to the probability to elude the system in the model are:

- Detector systems' unavailability (U): the probability that the safeguard won't operate at the time it is requested to. This factor is expressed by a probability estimate and a confidence level.

- The probability that the safeguard won't work if a proliferator set up an accident at the location where the safeguard is hosted. Since the ATD system is usually positioned out of the facility, this case is not analyzed in this context.

Scenario and setup

The following description is provided for the estimation of the top event probability that a proliferator is going to successfully elude an antineutrino detector located out of a SFR power plant. The scenario described is subject to changes.

Figure 35 shows the setup[17] of 1 ATD machine located at 20 km out of a 2400 MWth SFR plant with a conversion ratio equal to 1.03. The ATD is used to verify that operations within the NPP are regularly conducted. The SFR plant is hosted in a friendly state and under normal operations runs without using fuel blankets but only driver fuel elements disposed in a prism shaped core characterized by three concentric regions (see Table 13).

A proliferator within the plant, might try to acquire special nuclear materials with the goal to transport them out of the plant and then assemble a nuclear weapon device. It is assumed that with the help of a partner in crime working at the fuel re-fabrication facility serving the nuclear power plant, he might be able to obtain 6 fresh fuel element looking like traditional outer core fuel assemblies but that actually are filled with pure depleted uranium (i.e., fuel blankets). The goal of the proliferator is to insert the six fuel elements in the outer region of the core during refueling thus occupying six slots normally dedicated to driver fuel elements.

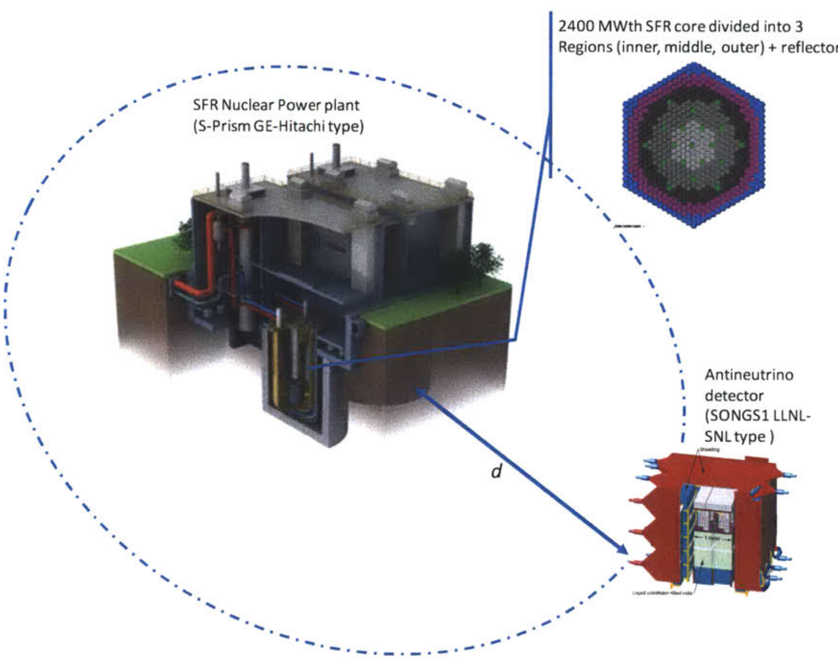


Figure 35. Setup on the ATD located to monitor operations of a SFR power plant.

[17] The setup presented below might not correspond to what you might consider the optimal setup for this safeguard and sample. Also in this case you might provide a description of a more realistic scenario before you answer the questions relative to the detector performance.

Over time the fuel blankets will transform into almost pure Pu. At the next refueling the proliferator extracts the six elements of pure Pu usable to assemble a NWD and transports them in a secret location out of the NPP.

Having an ATD placed out of the plant has to primary purposes. First, to determine if the plant is being stopped to insert the 6 fuel elements (although this won't probably the case for the current scenario where the actor running the threat is not the host state but a single ill-intentioned individual). Second, actually the primary purpose for the ATD, to determine the mass evolution of the plutonium and uranium isotopic species within the core.

Table 13. SFR core properties and fuel characterization within the three core regions.

MEASURED QUANTITY	UNITS	CORE REGIONS		
		1 inner core	2 middle core	3 outer core
Reactor Technology Specifics:				
Power Rating	MW(th)	2400	2400	2400
Fuel Types	dmnl	U-Pu-Zr	U-Pu-Zr	U-Pu-Zr
Enrichment	w/o	10% Pu	10% Pu	10% Pu
Burnup	MWd/kg	77	77	77
Total # of fuel elements in core, Nf	assembly	54	150	156
Density (g/cm^3)		13.7	14.71	16.14
Container Volume, Vc	m3	0.023016	0.023016	0.023016
Fuel Element Net Weight, Wfe	Kg	108	116	127
Pu concentration, Co (EOL)	Kg/T	112.3	115.9	122
Pu Mass per fuel element , Mp (EOL)	Kg	11.71	13.44	14.23
Pu Mass/fuel element Range (BOL-> EOL)	Kg	10.86->11.71	12.79->13.44	13.83->14.23

Table 14. Plutonium isotopic composition for an outer core fuel driver element and for a spent fuel blanket illicitly positioned in the outer region of the core.

Misuse Scenario in the SFR Plant - Pu content evolution for the 6 fuel blankets inserted in the core and comparison of the

BU (MWd/Kg)	0.00	13	27	40	53	67	80	80	80
time (efpd)	0	200	400	600	800	1000	1200	1200	1200
Mass (kg)									
6 assemblies								*1 blanket*	*1 driver*
Pu238	0.00	0.73	1.48	2.15	2.73	3.21	3.59	0.60	0.53
Pu239	0.00	9.76	18.47	26.10	32.80	38.67	43.80	7.30	8.90
Pu240	0.00	0.13	0.43	0.88	1.46	2.13	2.89	0.48	3.87
Pu241	0.00	0.00	0.01	0.02	0.04	0.07	0.11	0.02	0.76
Pu242	0.00	0.07	0.14	0.19	0.24	0.29	0.32	0.05	0.83
Pu total	0.00	10.69	20.53	29.35	37.27	44.37	50.73	8.45	14.89
Pu conc (Pu/tot mass)							0.07	0.07	0.12
Weight (including U and MA)							762	127	127

The ATD can effectively detect the proliferator's attempt to misuse the SFR power plant by means of the following procedure: determine a profile of the antineutrinos produced over a fuel life cycle. Then, compare the results obtained with the actual profile.

The ATD should be able to capture the differences in antineutrino production caused by the illicit insertion of the 6 fuel blankets in the reactor core, and thus reveal the misuse attempt. This of course will depend upon factors such as the its accuracy, the amount of missing Pu in the initial core load, and other variables such as the source-detector distance. Table 14 lists the isotopic compositions for the two types of fuel (driver and blanket), and shows the evolution of the blanket fuel's Pu composition associated with the set of 6 fuel elements.

PART II: Questionnaire

Setup

Please tell us if you think that the described experimental set-up is plausible for the scope of the threat described in the previous section. If you do not agree with the experimental set-up proposed, before answering the next questions, write below an alternative set-up that you propose and to which you will refer when answering the next set of questions.

....

....

....

....

Primary tactics

Please tell us if you think that the described tactics represent plausible threats to the ATD.

If you believe that other threats would better capture the potential vulnerability of the ATD system, please describe them below and refer to them when you address the questions in the next section. If the table is left empty this means that you agree with the set of tactics proposed in the questionnaire.

Tactic	*Target sub-system*	*Suggested tactic (Description)*
Tactic A	...	...
Tactic B	...	...
Tactic C	...	...
Tactic D	...	...

Other contributors

Detector systems' unavailability (U): please insert your estimate of the ATD's unavailability indicating the measure units that you prefer (e.g., 3/10 = number of times the machine did not start when supposed to, 10^{-3} = probability of failure reported in the manual, 1/1000 = measured frequency of unavailable starts, etc.).

Unavailability (U)	Measure units	Point Estimate	± Error with 95% Level of Confidence
Values:	...	...	...

Mass and costs table

Based on your knowledge, please complete the following table by inserting values for the two dependent variables M (mass of SNM) and C (safeguard costs).

Factor	*Description*		*Estimated value*
Total mass of the material under detection	M_{low}	Lowest detectable mass	...
	$\mathbf{M_{bc}}$	Base case mass, or regular mass of material under detection region in the facility	Inventory =34009 kg Pu inventory = 4919 kg
	M_{high}	Highest mass, or maximum conceivable mass	...
Cost of the safeguard	C_{low}	Cost of the safeguard for it to operate, or cost of the typical safeguard configuration	100,000$[18]
	$\mathbf{C_{bc}}$	Cost of the safeguard with additional features to increase its efficiency and protecting it from tactics	...
	C_{opt}	Cost of the safeguard to let it operate at the optimal efficiency, and to fully protect it from tactics	...

You are now asked to estimate the accuracy and the probabilities to elude the safeguard system with the set of tactics we proposed or that you modified.

---

[18] Based on KKNL scientist Dr. Nathaniel Bowden (estimate provided at a interview at msnbc.com released the 4/15/2011).

Accuracy of measurement (no tactic)

Safeguard Estimated Cost	Accuracy of Measurement (%)					
	Total Mass M_{low} =...		Total Mass M_{bc} =...		Total Mass M_{high} =...	
	Point Estimate	± Error with 90% Level of Confidence	Point Estimate	± Error with 90% Level of Confidence	Point Estimate	± Error with 90% Level of Confidence
C_{min} = $ ...	...	...	...	...	...	...
C_{bc} = $ ...	...	...	...	...	...	...
C_{opt} = $ ...	...	...	...	...	...	...

Probability that the proliferator's tactics will successfully elude the safeguard

- **Tactics A: Using dummy material**

Safeguard Estimated Cost	Proliferator success probability of tactic A	
	Point Estimate	± Error with 90% Level of Confidence
$C_{add,A}$ = $....	...	...

- **Tactic B: Placing compensating material in the detection region**

Safeguard Estimated Cost	Proliferator success probability of tactic B	
	Point Estimate	± Error with 90% Level of Confidence
$C_{add,B}$ = $....	...	...

- **Tactics C: Modifying the hardware of the system**

Safeguard Estimated Cost	Proliferator success probability of tactic C	
	Point Estimate	± Error with 90% Level of Confidence
$C_{add,C}$ = $....	...	...

- **Tactics D: Modifying the software of the system**

Safeguard Estimated Cost	Proliferator success probability of tactic D	
	Point Estimate	± Error with 90% Level of Confidence
$C_{add,D}$ = $....	...	...

This concludes the questionnaire used to determine the probability to elude the ADT system.

REFERENCES

[1] Ham, H., An Integrated Methodology for Quantitative Assessment of Proliferation Resistance of Advanced Nuclear Systems Using Probabilistic Methods, Department of Nuclear Engineering Ph. D., advisor: M. Golay, Massachusetts Institute of Technology, Cambridge, MA, 2005.

[2] NRC definition of special nuclear materials and safeguards, http://www.nrc.gov/security/domestic/mca/snm.html

[3] IAEA glossary terms, http://www-pub.iaea.org/MTCD/publications/PDF/nvs-3-cd/PDF/NVS3_prn.pdf

[4] DOE Graded Safeguards Table of DOE Manual 470.4-6.

[5] IAEA Illicit Trafficking Database (Vienna: IAEA, September 2008), www.iaea.org/NewsCenter/Features/RadSources/PDF/fact_figures2007.pdf.

[6] Hora, S.C., Iman, R.L. *"Expert Opinion in Risk Analysis: The NUREG-1150 Methodology."* Nuclear Science and Engineering, 1989: 102, 323-331.

[7] Budnitz, R.J., Apostolakis, G., Boore, D.M., Cluff, L.S., Coppersmith, J. Cornell, C.A., and Morris, P.A., *"Recommendations for Probabilistic Seismic Hazard Analysis: Guidance on Uncertainty and Use of Experts,"* Senior Seismic Hazard Analysis Committee, NUREG/CR-6372, 1997.

[8] Clemen, R.T. and Winkler, R.L., *"Combining Probability Distributions From Experts in Risk Analysis," Risk Analysis*, Vol. 19, No. 2, 1999.

[9] Personal communication with Gordon E Kohse.

[10] Philip F. Judy et al., *"Measuring the observer performance of digital systems"*.

[11] G. F. Knoll, *"Radiation Detection and Measurement"*, 4/e. John Wiley & Sons, Inc., Chapter 3 pp. 96.

[12] L.A. Currie, *"Anal. Chem."* 40 (3), 586 (1968).

[13] *Field measurement methods and instrumentation*. MARSSIM, Revision 1 August 2000.

[14] M. Lineberry, et al., *"Safeguarding the fast reactor fuel cycle"* Center for advanced energy studies, Idaho State University. Summer 2010.

PART IV: POLICIES, REGULATIONS, PERFORMANCE STANDARDS

For security and non-proliferation, there are no regulations, formal license processes, or protocol to follow similar the ones used for safety, such as the safety grade certifications used by the nuclear industry. While in the US and worldwide, the acceptance of nuclear designs has been abundantly regulated and formalized from a safety standpoint, the regulation system of the non-proliferation performance of these systems is vague, not formalized, and sometimes presents some contradictions. Consensus on how to address security and non-proliferation from regulators was not reached yet, although for the industry there is a urgent need to dispose of a clear framework to address security and non-proliferation requirements.

The analogy established in Chapter 2 between safety, security, and non-proliferation is now elaborated in terms of acceptance criteria. The parallelism between these three domains is maintained in this Chapter too, to show the consistency of the novel proliferation curve we ideated with the philosophy of new regulations such as NUREG-1860 [1], also known under the name of TNF, which proposes a F-C curve by which regulators plan to license the safety of future nuclear power plants. Although not being part of the actual regulation system, but only a draft of a regulation proposal, NUREG-1860 contains novel insights in terms of applicability of regulatory frameworks based on risk. Also it contains a proposal of acceptance criteria to license the security of future NPP, which considers proliferation scenarios.

Therefore, together with the formulation of a probabilistic assessment tool, appropriate policies are needed to systematically define acceptable levels of risk. The risk-informed framework we propose combines the risk evaluation technique described in the previous Chapter with a policy, which is being used to determine the acceptability of the proliferation risks associated with a new nuclear facility. The use of these two constitutive elements combined provide an opportunity to compare different NES design alternatives, and to measure the gain in resistance determined by the addition of anti-proliferation barriers. Setting this procedure allows designers and policy makers evaluating the potential resistance to the proliferation risk of the resulting overall system.

Despite the level of maturity of the framework is still not adequate to include in a formal licensing process, the efforts done to develop it have been in this direction. This Chapter illustrates the efforts done to create a F-C curve, and ways to evaluate proliferation scenario within a new risk space analogous to the one used to structure policies, and regulations for non-proliferation. It is therefore useful to understand the approaches envisioned by future safety regulations such as the TNF in terms of safety and security.

THE TECHNOLOGY NEUTRAL FRAMEWORK (NUREG-1860)

The US Nuclear Regulatory Commission (USNRC) has defined as a goal to risk-inform the regulations and make the licensing process more efficient, predictable, and stable.

Indeed, when Title 10 of the Code of Federal Regulations Part 50 (10CFR50) is used to license a design differing from a traditional light water design, a tremendous amount of time is being used to review new design features, to document exemptions, and to include the justifications required for additional systems. This case-by-case analysis is inefficient and mines the predictability and stability of licensing processes.

It is opinion of many observers and authors [2], that the nuclear technologies we use today locked-in the markets before they proved to be effectively the best technology in the market. Nowadays new technologies, based on decades of reactor operation and construction, such as modular reactors are ready to be commercialized. The burden of a regulatory process with technology dependent processes, would prevent promising designs to enter the market in acceptable times.

A systematic set of rules applicable to all reactor technologies is then required to avoid that similar design features might be treated differently.

To overcome these difficulties, in 2006 the USNRC has drafted a technology-neutral framework for new plant licensing, which should in the long term replace 10 CFR Part 50. With similar intents, the International Atomic Energy Agency has started giving guidance for developing a set of requirements that would be applicable to any kind of nuclear design.

An objective of the DOE/NERI study supporting this research work has been to analyze the use of specific risk assessment tools, known as *Frequency-Consequence* (F-C) curves in future reactor licensing within a risk-informed licensing process. Consistently with this objective, one of the scopes of the proliferation segment of the project has been the creation of a F-C curve to evaluate the admissible societal risks from proliferation associated with new NESs.

SAFETY ACCEPTANCE CRITERIA IN THE TNF

NUREG 1860, was designed to create a new licensing framework for future nuclear power plants. Due to the limitations of 10CFR50 which was originally designed to regulate the licensing of essentially the two types of nuclear reactor designs adopted by the US, the NRC drafted the TNF. Many of the *General Design Criteria* (GDC) of 10CFR50 do not necessarily apply to future designs. For example, the use of the core damage frequency as a metric to verify the safety features of a design do not generally apply to all designs. Furthermore, the design basis accident (DBA) of modern regulations do not always meet the representation required for new nuclear reactors; they consider accidents such as LOCA that might not lead to serious consequences, but that has been a major concerns for most of the past nuclear designs, or reversely they might omit accidental sequences, such as core disruptive accidents, that might be determinant contributors to the plant's risk.

NUREG-1860 was designed with the intent to overcome these inherent vulnerabilities of 10CFR50. Some of the major features and new concepts of the assessment of the TNF are:

- The creation of new reference PRA sequences called License Basis Events (LBEs), which are going to replace the deterministic concept of postulated Design Basis Accidents (DBAs);
- The inclusion of new deterministic requirements in addition to the LBEs;
- The use of philosophy in depth as a complementary and conservative tool for safety;
- The use of a F-C curve shown in Figure 36 which express the consequences in terms of dose, and thus of a PRA 3 level analysis.

Therefore the novelty of the safety approach introduce by the TNF is the combined use of probabilistic sequences (the LBEs), which are evaluated within a risk space characterized by an acceptability region determined by the union of multiple regulations.

LBEs play a role in the licensing process similar to the DBAs, for they provide assurance that the design meets various accident challenges with adequate margins. However, LBEs encompass a much broader range of events since they also include, for instance, some events that do not involve radioactive release. Furthermore, unlike DBAs, LBEs are not limited to considerations of single failure and thus allow consideration of progression of a relatively frequent initiating event trough multiple failures to an event with significant consequences.

Interesting for the discussion that is going to follow about the scale to use for evaluating the consequences of an accident, is the introduction of an F-C acceptance criterion that uses the radiation dose absorbed by the public as a consequence measure. This means that traditional quantitative goals, such as the surrogate quantitative objectives of *Core Damage Frequency* (CDF) or *Large Early Release Frequency* (LERF) are excluded from the licensing process.

Another interesting aspect about the LBEs, is their selection. An LBE is selected from a level 3 PRA of a NPP by grouping accident sequences with similar initiating events, or similar consequences. The objective of this procedure is to group accident sequences with a similar phenomenological evolution. This approach is being criticized for the efforts to calculate the LBEs which push the analysis to a level 3 PRA [3]. However, the use of functional event trees, which naturally capture this notion of similar phenomenological evolution, done in our project by another student, demonstrated that LBEs can be practically calculated [3].

As it will be shown next these latest key traits, and applicability notions used by the safety portion of the TNF can be adapted to the non-proliferation case.

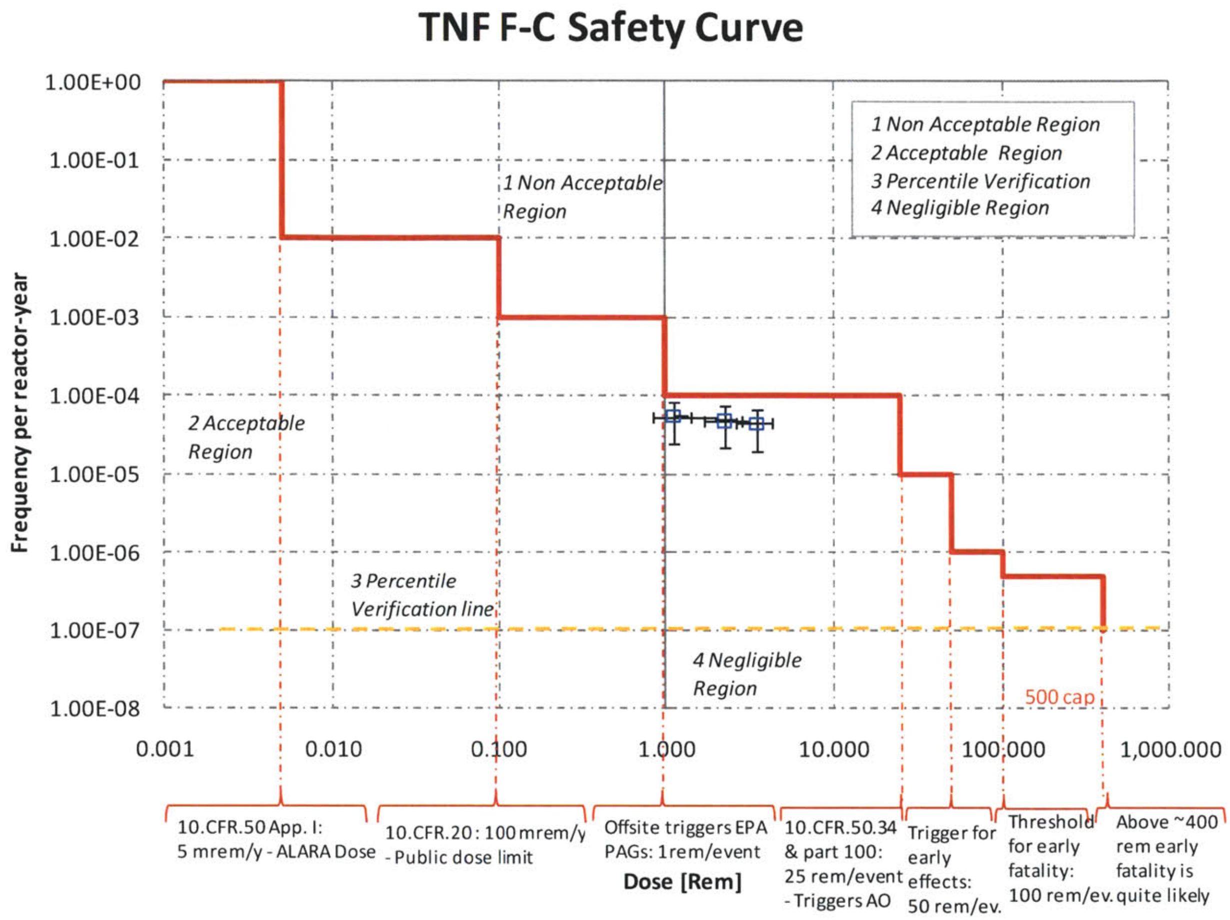


Figure 36. TNF safety curve proposed to license the safety of generation IV power plants.

A basic principle for the curve's applicability is that the sequences of the PRA populate the space under the F-C curve. Some sequences will have little or no consequences, primarily because of the inherent characteristics and design features of the plant. Others are likely to approach the F-C curve and thus make up the important contributors to the plant risk profile. To be acceptable, the frequency and consequences of all the accident sequences examined need to lie in the acceptable region of the F-C curve by meeting the dose criteria. This is the first step in selecting the licensing basis events, and, as it will be discussed later, also the basic principle for acceptance of proliferation scenarios.

One of the goals of the TNF is also the integration of security standards and safety standards. The following section briefly describes the features of a security section that is being part of the regulation, which includes specific F-C curves for security. The major concerns that emerged from the evaluation of this security framework, when applied to the case of proliferation scenarios are summarized and then used to formulate a new F-C curve specific to proliferation.

SECURITY ACCEPTANCE CRITERIA IN THE TNF

NUREG-1860 constitutes the first and substantial attempt to include safety and security acceptance criteria based on the performance and risks of nuclear systems, within the same regulatory framework. Section 6.7 of NUREG-1860, entitled *"Security performance standard"*, provides security criteria in the form of an accident scenario-based frequency-versus-consequences curves. The purpose of this section is to define proposed risk-informed and technology-neutral security expectations and performance standards for new proposed plants. While current regulations, such as 10CFR73 or the post 9/11 orders, contain prescriptive requirements to protect the pant against security scenarios, the TNF propose risk-informed procedures to meet the security performance standards, or performance based requirements of NUREG/BR-0303.

The TNF framework has been developed with the safety expectation that future NPPs are to achieve a level of safety at least as good as that defined by the Quantitative Health Objectives (QHOs) in the Commission's 1986 Safety Goal Policy Statement. Coherently, security expectations are also expressed in terms of QHOs.

This is a list of features mentioned by the TNF security section, relevant to this study:

- Security standards apply to the entire facility, including fuel storage, and fuel pools on site;
- Security needs should be considered during the design stage;
- The security performance standards that are being proposed include deterministic, probabilistic, and design related standards. Also some standards relative specifically to diversion and theft are considered;
- Diversion and theft are considered as potential DBTs challenging the plant. However they refer to HEU and MOX fuel, disregarding completely the eventuality that LEU, in fresh or spent form, is going to be the goal of an intruder;
- The threats assumed during the design stage (i.e., the design basis threats) need to include the broad categories of potential physical protection challenges:

Design Basis Threats

- Insider attack,
- Armed intrusion,
- Standoff attacks,
- Cyber attacks,
- Theft or diversion of nuclear materials,
- A credible combination of the above.

Figure 37 reports two distinct risk spaces for early and latent fatalities. Accordingly, for consistency with the overall plant risk described in Section 6.3 of the TNF, the QHOs were selected as the risk metrics to be used. The QHOs are expressed as individual risk of a latent fatality (2 x 10^{-6}/yr) and an early fatality (5 x 10^{-7}/yr) and are applicable out to 10 miles and 1 mile respectively, from the exclusion area boundary of the plant [1]. The two risk spaces so defined then relate the probability of an attack to the facility (y-axis) with some indirect measurements of the QHOs. Each of the two risk spaces is then divided into three risk zones corresponding to different "distances" from the observation of the QHO limits. Explain in details this approach is out of the scopes of the present work, however it is evident, and this was our major concern in defining new acceptance criteria, that acquisition risks do not find a natural collocation in this framework.

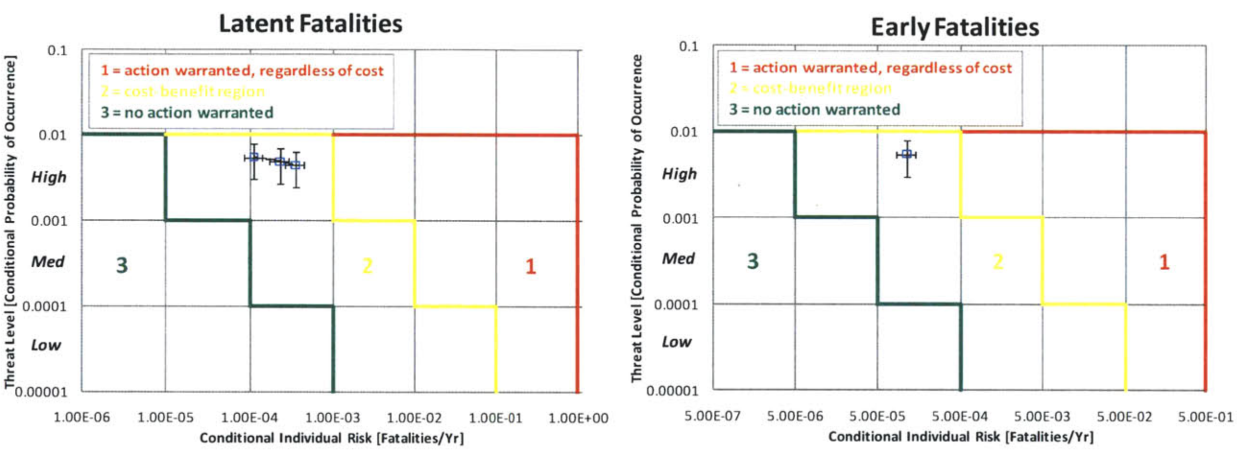


Figure 37. TNF curves proposed to license the security of generation IV nuclear power plants.

Major concerns regarding the construction of the security section of the TNF

Section II of this thesis provided a rational classification to distinguish between safety, security, and the non-proliferation disciplines. Efforts have to be done to include them into one unique evaluation, however understanding the differences between them is key to correctly interpret their individual challenges, and thus to avoid confusion. Three major concerns about the representation used to define the security curves of the security standards section of the TNF are reported here:

1. The inappropriate use of dose consequences for theft scenarios and the inappropriate inclusion of diversion scenarios within the pool of DBTs when these are covert and internal events;
2. The lack of generality in the selection of SNMs. The HEU and MOX selection is not justifiable from both, a security and a non-proliferation standpoint

3. The probability scale, or likelihood that a given threat is going to succeed, is not predictable but conditional to the initiating event (i.e., the probability that the attacker is going to start an attack is completely unknown). This last aspect was in fact incorporated in latest revisions of the NUREG.

1. Inappropriate use of dose consequences

Security scenarios such a plane attack, a cyber attack, and a terroristic attacks, all differ from a diversion scenario because they have no immediate consequences in terms of fatalities or other health effects; a diversion attempt is generally a concealed event, therefore not likely to generate consequences at the site where such an attempt occurs. The confusion between different categories of threats is very popular and justifiable by the lack of understanding of the difference between security and non-proliferation scenarios. Former ones refer to physical and violent attacks against a given system, while latter ones refer to a concealed event aimed toward the acquisition of nuclear materials.

The selection of QHOs, or of parameters derived from them, as the risk metric to evaluate the consequences of a malicious attack, or DBT, does then not apply to nuclear material acquisition scenarios. Therefore the F-C representations of Figure 37, expressed in terms of frequency and fatalities per year does not adequately define the level of protection required for the non-proliferation scope; the consequences of a diversion event are neither directly quantifiable in terms of fatalities in the plant's surroundings nor in the timeframe during which the diversion occurs.

Note that the authors of the TNF first recognized that not all security threats can be measured by consequences expressed in terms of dose[19], then in a revised version of the NUREG decided to completely exclude theft from the security scenarios[20]. Thus, the approach, as it is currently proposed should be either disregarded or revised because it inappropriately describes internal acquisition threats, although, following the representation we suggested in chapter II and summarized in Table 2, it can be used to define external security threats.

[19] Measuring consequences in terms of dose for a proliferation scenario seems inappropriate to describe most DBT scenarios as stated by the regulators themselves in appendix C.4.6 of the TNF: *"The technical issue is whether or not the consequence scale should be based upon dose, the same as that used in assessing other event scenarios in the PRA safety analysis, in lieu of early and latent fatalities"*.

[20] The theft or diversion of nuclear material from a nuclear energy system was excluded from the latest version of NUREG-1860, where it was suggested that the requirements described in 10CFR73[20] remain sufficient to regulate SNMs. However, 10CFR73 is only prescriptive and not risk-informed, and prescriptive measures do not allow for defining metrics inclusive of risk information and performance.

2. The lack of generality in the selection of SNMs

Excluding LEU, or considering only HEU and MOX fuel within the evaluations has to be re-stated:

- If material acquisition is an external attack and uncovered act, then considering HEU and MOX does not cover security scenarios involving reprocessing or fabrication facilities where nuclear materials characterized by higher toxicity can be dispersed in the environment;
- If material acquisition is a covert goal for a proliferator, then other types of SNMs have to be considered (i.e., all the materials having a critical mass, such as Neptunium, Thorium, Americium, etc.).

In conclusion, concerning covert theft and diversion, another frequency-consequence representation should be created in a new risk space considering the ability to develop a future potential threat (e.g., constructing part of a nuclear weapon, one nuclear weapon, or a set of them) rather than setting the consequences in terms of dose, fatalities, or injuries. The creation of this frequency-consequence curve would provide a useful representation for evaluating the danger and long-term consequences generated by the noncompliance of appropriate safeguard strategies. The creation of the curve is necessary for the development of a proper risk-informed regulatory framework for non-proliferation, and this was settled as a priority when the NERI/DOE project started.

PROLIFERATION ACCEPTANCE CRITERIA

Establishing acceptance criteria for proliferation in this context refers to the problem of quantifying limits to the risk of covert acquisition of SNMs from nuclear energy sites. For this reason, using the principles mentioned in Section II, consistently with the risk-informed approach used in the TNF, but also given the common misinterpretations of security and proliferation highlighted in the previous section, a new approach was formulated.

The goal of the Probability vs. consequences curve (Ps-C) of Figure 38 resulting from this study is to provide a representational domain into which nuclear designs can be selected based on their proliferation risk features. The domain decomposes the risk into a two dimensional vector made of the probability Ps to succeed in a proliferation attempt, or a series of attempts, and its consequences, C. This probability is plotted versus a consequence scale functional to the feasibility of any acquisition attempt, and considering the potential weapon device development associated with any concealed SNM acquisition attempt.

The (Ps, C) space allows one to relate the probability of occurrence of a given event to its consequences. The proposed curve is expressed in terms of conditional probability of success of a given proliferation attempt, compared to the fraction, or multiples, of significant quantity (SQ) acquirable, assuming to succeed in the attempt. This representation allows one to relate the results provided by the PRA assessment methods to a scale of consequences for non-proliferation, which is more plausible than other proposed metrics such as dose, or fatalities.

Differently from the safety curve of Figure 36, the measure of occurrence of an attempt is not measured by a frequency but by a probability. This probability is a measure of how likely is for a proliferator to elude all the barriers located in the acquisition point, and placed along his pathway from that same point and the facility's exit. The probability estimate is obtained from the assessment model described in the previous chapter, and that considers all the barriers positioned in the plant to timely detect acquisition threats. In this formulation, the probability of occurrence of the threats, which is the initial intention of the proliferator to pursue an acquisition attempt in a given area of the NES, is highly uncertain. To remove this uncertainty, the initiating event frequency is not considered (i.e. our results are conditional upon the attempt being made). Thus Ps is conditional upon attempt of acquisition, which in mathematical notation is $Ps|p_i$.

The $Ps|p_i$ -SQ domain refers to concealed acquisition of any SNM from any installation along a nuclear fuel cycle. Most fissile materials can be expressed in terms of SQ, therefore the scale is neutral from a material standpoint and it allows comparing different SNMs. For example 25 kg of LEU is equivalent to 8 kg of Pu, since they have the same valence in terms of consequences (i.e., a SQ is the amount defined by the IAEA as the one required to assemble a NWD), but their risk is different since the probability Ps determined by the ST/ET model is different in the two cases, even for similar threats.

As remarked in the previous section, a security scenario can both be characterized by acquisition of SNM unless the acquisition attempt is not secret and therefore characterized by a physical attack to the facility. Excluding this last scenario, acquisition threats are then different from standard security threats, or using the terminology of the TNF, from DBTs.

Therefore a new terminology is proposed to group these type of scenarios: acquisition threats, or LBAT (License Basis Acquisition Threats). Therefore NESs and proliferation barriers have to be designed in order to guarantee enough protection from the three major LBAT categories reported below.

License Basis Acquisition Threats

- Theft or diversion of nuclear materials,
- Misuse, or concealed manipulation of a processes,
- Abrogation, or break out from the NPT.

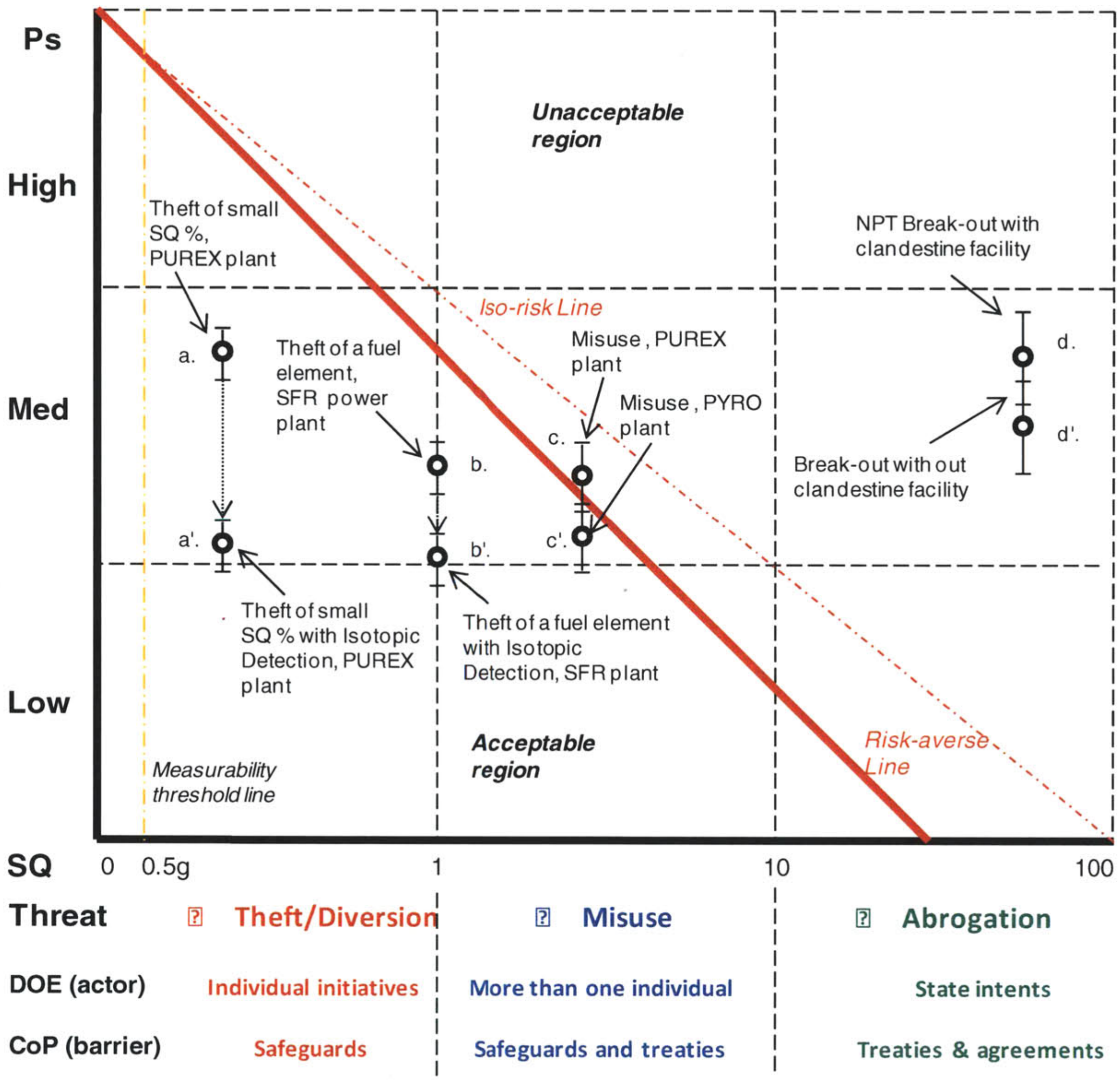


Figure 38. MIT safety curve proposed to license the non-proliferation performance of NESs.

Moreover, since proliferator strategies include covert attacks to the physical system being part of the counter measures, the plant need to be designed in order to guarantee also a certain level of protection from these supportive tactics. Thus, a potential licensing process, will require to protect the plant from these extra sub-threats, or tactics.

Physical protection tactics

- Hardware function (T1),
- Software function (T2),
- Sample manipulation (T3),

• Sample interface (T4),
• Human interface (T5),
• Error exploitation (T0).

The formulation of proliferation scenarios included in the above categories of threats and tactics is consistent with the LBE formulation used in the safety section of the TNF, but with the following differences and similarities:

Acquisition threats are probabilistic scenarios, which contrarily to DBAs, contain more than one system failure. In this case the realization of a scenario is seen from a proliferator's perspective and this means that multiple successes have to occur before the proliferator accomplish his mission (i.e., elude many detection systems).

The new scale of consequences, ranging from the illicit subtraction of a small fraction of material to a multiple of a significant quantity, lists the three regions into which the risk space is being divided. As shown below the x-axis of the figure the three zones also trace the boundaries for the three different type of scenarios, or acquisition threats; the attempts leading to the acquisition of small fractions of materials are, in general, diversion or theft scenarios. The only way to acquire simultaneously multiples of a significant quantity are abrogation scenarios. The scenarios falling between these two categories (i.e. 1<SQ<10) are generally characterized by the misuse of the facility before acquisition takes place. This approach assesses the proliferators' capability to acquire material from a NES given his chance to successfully accomplish the attack.

As opposed to the representation provided in the security section of NUREG-1860, the SQ scale immediately allows one to directly relate the probability of a threat calculated via the PRA analysis, with the associated consequences. This approach permits to determine the consequences with a lower level of uncertainty than by expressing them in form of dose, or fatalities generated by the detonation of the nuclear explosive device assembled with the acquired material. Recalling the parallelism established with the safety case, evaluating the consequences in terms of the number of SQs acquired is equivalent to the core damage frequency evaluation, and referred as Level 1 PRA analysis.

While the stepwise shape and segmentation of the curve into sub-regions used in the TNF was dictated by the QHOs, in this content it becomes unnecessary. However, at the current stage of development of the curve, two possible approaches are maintained in order to determine the proper slope of the curve. The first approach set the curve slope equal to minus 45 degrees, therefore using a line made of points having the same risk. The second approach, envisioning the need to consider unacceptable the scenarios characterized by very high consequences and low probability of occurrence, sets a stepper line, namely a risk averse curve.

The figure can also be used to aggregate multiple acquisition attempts into a single point, and compare it to a single attempt aimed to subtract the same SQ equivalent. At the current stage of development of the assessment method determining the probability Ps, given the uncertainties in its determination, we decided not to set quantitative ranges for the three main regions defining the various levels of risk on the y-axis, but to use confidence level.

The next section describes how to curve can be used for licensing NESs, or to obtain insights about the barrier system being added to protect from acquisition risks.

USES OF THE (PS | P_I, SQ) SPACE

Typical applications of the proposed representation can be used to compare the relative risks of different scenarios for the same system, or alternatively to compare different systems exposed to the same type of acquisition attempt.

The general steps of the risk-informed process used to determine the proliferation performance (i.e., the risk) of a nuclear design demonstrate the applicability of the curve to the method.

The SFR plant is used to illustrate its use, however any technology is a candidate for being screened by the curve since the SQ consequence scale is technology neutral metric. Thus the risk space settled by the P-SQ curve is consistent with the TNF proposition. As stated previously, the SQ also guarantees to be neutral with respect to the material target (i.e., the scale does not change depending on the type of SNM that the proliferator selects as a target for his acquisition attempts).

1. A given technology and a subset of design options are selected. In this case a SFR with a conversion ratio (CR) of 0.7 and a thermal power of 1,000 MWe with no blankets in the core.

2. A SNM material is selected as a candidate material to be acquired. Using a SFR design with a CR=0.7, Plutonium is the most abundant SNM on site. In this case, 1 SQ equals 8 kg of Pu.

3. An acquisition scenario and the associated modality of acquisition are selected. In this example, fuel elements contains an amount of Pu equivalent to almost one SQ, therefore diversion seems the preferred acquisition mechanism and the modality means the number of attempts required for its acquisition, in this case 1 attempt is sufficient to acquire 1 SQ.

4. Run the assessment model* which *determines the success probability associated with the selected scenario for all the pathways following the PRA analysis rules.

5. All the pathways leading to similar consequences are collected and the worst probabilities of success, Ps, and the highest SQ fraction are selected and combined. Analogously with NUREG-1860, this step consider the aggregation of similar scenarios (in the case of the safety assessment, the aggregation of all the LBEs having similar phenomenology) to create an unique scenario characterized by the worst consequences of the set, and by the highest probability.

6. The proliferation performance of a nuclear design is acceptable if it falls within the acceptable region of the (Ps|p, C) plane, or below the risk-averse line.

7. The last step is iterative. If the nuclear design falls out of the acceptability boundaries, this requires to improve the system performance by adding more barriers.

Figure 38 reports four illustrative applications of the framework, each one characterized by a set of two points. Each of the sets is located in a different threat region, and one is on the boundaries between the misuse and the theft region. Theft in a PUREX plant (a), theft of a SFR fuel assembly (b), misuse of a reprocessing plant (c), and abrogation from the NPT (d) are considered. Then each set shows the improvements relative to the addition of extra barriers to reduce the risks. Scenarios (c) and (c') show the difference between two design alternatives exposed to the same threat.

Figure 39, shows two other examples of applications for which the framework can used effectively to evaluate proliferation performance of a NES. The left diagram illustrates the gradually increase or performance (i.e. decrease of Ps) due to the addition of barrier systems to a reprocessing site where a proliferator decides to acquire SNMs by stealing in an amount almost equal to 1 SQ. The right diagram compares two different modalities of covert acquisition via theft; by stealing one fuel element at the plant site, or by stealing 3 fuel samples at a reprocessing site in 3 consecutive attempts. Considering the entire sequence it is most likely to succeed in one attempt although the individual probabilities are less likely for the second case.

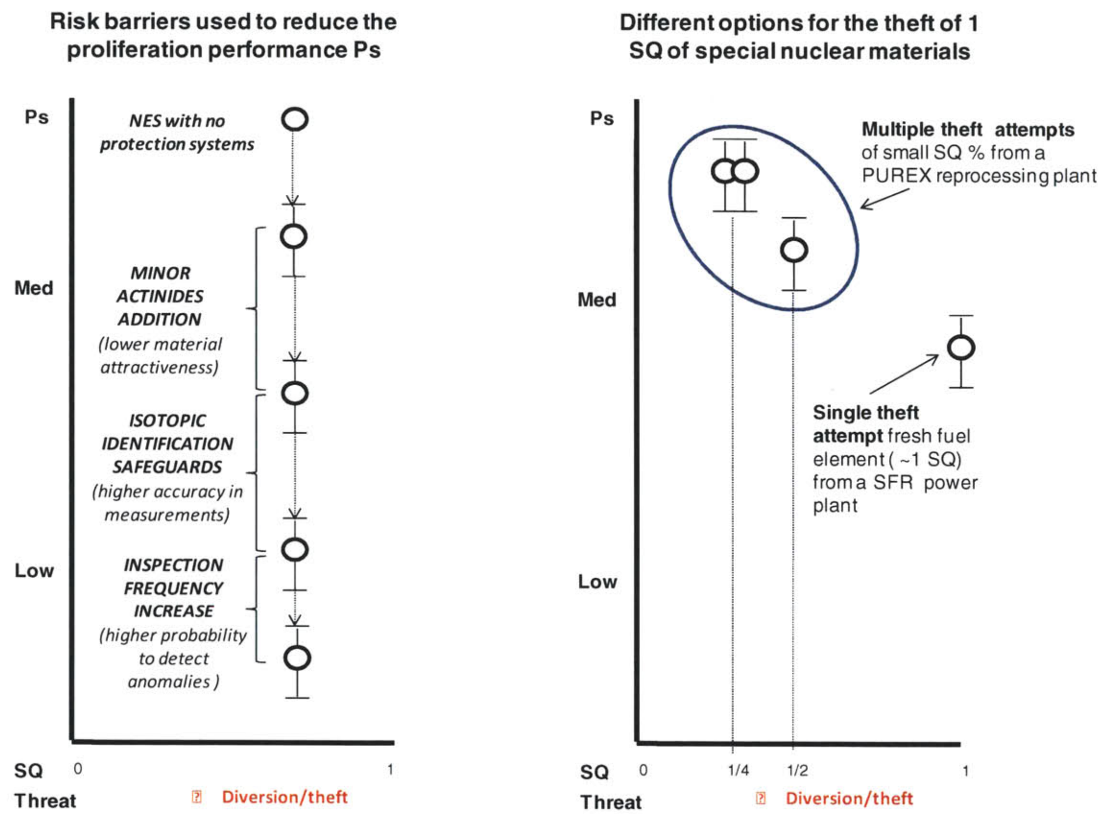


Figure 39. Applications in the proliferation risk space – risk barriers evaluation, and scenarios.

REFERENCES

[1] U.S. NRC, Office of Nuclear Regulatory Research, *"Feasibility Study for a Risk-Informed and Performance-Based Regulatory Structure for Future Plant Licensing"*. NUREG-1860. Washington, DC, December (2008).

[2] Cowan Robin, *"Nuclear Power Reactors: A Study in Technological Lock-in"*. Journal of Economic History 50: 541-567. 1990

[3] M. Modarres, *"Advanced nuclear power plant regulation using risk-informed an performance-based methods"*. Reliability engineering and systems safety 94 (2009) 211-217.

[4] Brian C. Johnson, *"Application of the Technology Neutral Framework to Sodium-Cooled Fast Reactors"*. PhD thesis submitted at the Department of Nuclear Science and Engineering, Massachusetts Institute of Technology, June 2010.

PART V: PROOF OF THE CONCEPT: PROLIFERATION PERFORMANCE OF A SODIUM FAST REACTOR

The previous Chapters illustrated the design rules and provided the elementary construction rules for the two main pieces constituting a risk-informed framework used to assess the proliferation performance of a nuclear energy system, a model and a policy.

The present Chapter shows how the model can be used to evaluate the proliferation risks associated with a pre-selected nuclear energy system. A simplified SFR nuclear power plant is used as a reference technology to test the framework, and two anti-proliferation barriers are used two drive two examples of potential applications of the risk-informed framework.

Specifically, the analyses described in this Chapter are:

- The QUALITATIVE ANALYSIS referring to a simplified SFR plant, considering the stocks of SNMs, the threats, and the potential proliferator's pathways;
- A comprehensive QUANTITATIVE ANALYSIS of an optical surveillance system located in MBA2 and MBA4 of the same SFR power plant;
- The QUANTITATIVE ANALYSIS of a Nuclear Resonance Fluorescence safeguard added to the co-located reprocessing facility used to separate the recycle the nuclear fuel.

The results obtained prove the potentialities of the assessment, although a comprehensive analysis of the entire plant, or of the entire fuel cycles would be desired to draw more insightful conclusions.

QUALITATIVE ANALYSIS

Reference SFR design

A reference SFR power plant designed by tested at the MIT NSE department has been used to validate the model. The SFR island of the SFR power plant hosts two reactors, each of 1,000 MW_{th}. The facility share common areas, resulting in a total of 5 main material balance areas, which excluding the two reactor core zones, are used mostly for refueling operations and to store spent fuel assemblies. The SFR is designed to operate as a breeder, thus it operates with a conversion ratio above 1. A core load is made of 560 fuel assemblies on three concentrically deposed rings . The fuel burnup is on average equal to 70 MWD/ton and the fuel is replaced every 2,400 days. A schematic version of the real plant is used to test the model although the fuel composition and design specifications comes from simulation executed with standard codes and the design is a modification of the advanced liquid metal reactor proposed by Argonne National Laboratories and General Electric in the '70s.

Core specifics

The core of a SFR is made of three different regions. Each of the regions is characterized by different isotopic composition and thus by different initial and final plutonium and uranium contents. The table below reports the characteristics of the fuel elements for each of the elements in the three core regions of the SFR plant used as a reference in this study. The following figure reports the plutonium contents calculated for the inner core region. All other regions' SNM contents were obtained similarly.

Table 15. SFR core specifics for a 2400 MWe and a conversion ratio = 1.03.

MEASURED QUANTITY	UNITS	CORE REGIONS		
		1 inner core	2 middle core	3 outer core
Reactor Technology Specifics:				
Power Rating	MW(th)	2400	2400	2400
Fuel Types	dmnl	U-Pu-Zr	U-Pu-Zr	U-Pu-Zr
Enrichment	w/o	10% Pu	10% Pu	10% Pu
Burnup	MWd/kg	77	77	77
Total # of fuel elements in core, Nf	assembly	54	150	156
Density (g/cm^3)		13.7	14.71	16.14
Container Volume, Vc	m3	0.023016	0.023016	0.023016
Fuel Element Net Weight, Wfe	Kg	108	116	127
Pu concentration, Co (EOL)	Kg/T	112.3	115.9	122
Pu Mass per fuel element , Mp (EOL)	Kg	11.71	13.44	14.23
Pu Mass/fuel element Range (BOL-> EOL)	Kg	10.86->11.71	12.79->13.44	13.83->14.23

Fuel Composition

The main objective of the qualitative analysis consists in the evaluation of all the fuel stocks available in the plant, divided per location and considering all the SNMs of interest. The starting point of this evaluation is to consider the single fuel elements which for the reference plant can be of 2 types: fresh and spent. Then each type can be divided in 3 sub-categories corresponding to the three core regions: inner, middle, outer. Therefore, there are 6 different types of fuel elements circulating in the core.

Figure 40 reports the composition in weight of a inner core SFR fuel element, at the beginning of the fuel cycle (BOC) and at its end (EOC). The selection of the plutonium family is highlighted by the central box which also reports the total weight of the plutonium mixture and its conversion in number of SQs. The diagram indicated that a fresh fuel element initially contains 10.8 kg of Pu, becoming 11.8 (1.4 SQ) at the end of the fuel cycle (1.5 SQ).

The same type of evaluation was repeated for all the other fissile species, potentially usable to develop a nuclear weapon such as Np-237 and Am-241. Not shown in the figure is the uranium composition which actually constitute most of the fuel element mass. Although the uranium of a SFR with CR>1 has very little content of U-235, it can be considered usable for a nuclear weapon. The SQ for natural uranium is the order of thousands of kg, although its use seems to be unrealistic the uranium stockpiles were also calculated and converted in SQs.

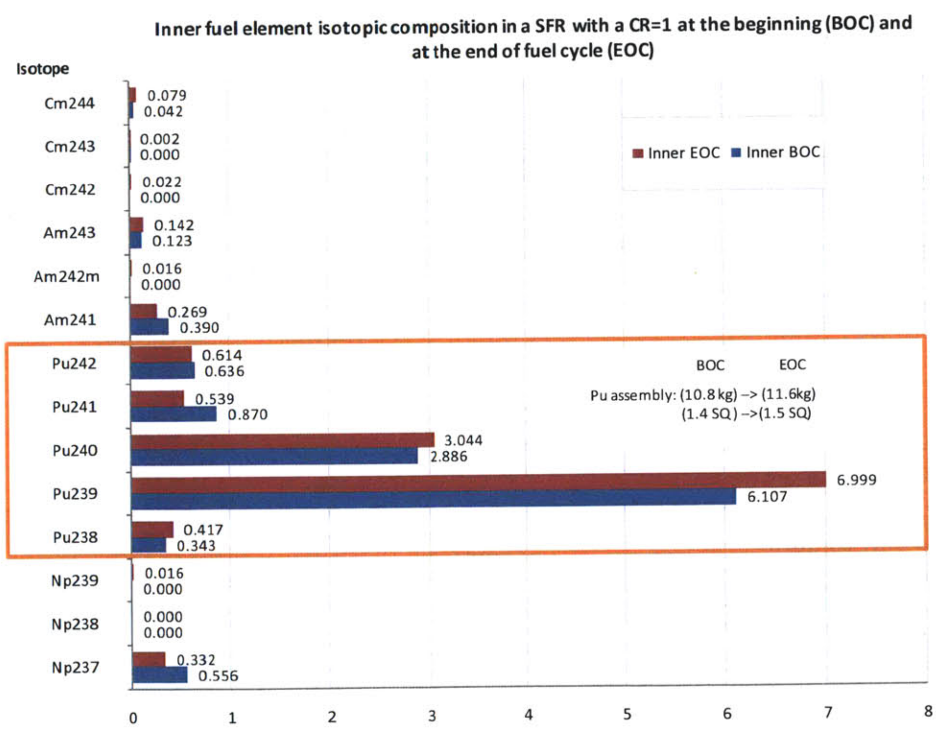


Figure 40. Composition of the SFR fuel assemblies located in the inner core.

SFR Fuel Inventory

Figure 41 reports a map of the facility showing the contents of Plutonium and Uranium calculated at each location within the SFR reference power plant and in correspondence of strategic key points (i.e., potentially vulnerable, or particularly attractive, points that are of interest for a proliferator aiming to illicitly acquire these materials).

Since in a SFR power plant circulate only fuel assemblies, and since on site there is no equipment designed to reduce the size, disassemble, or transform these assemblies, this implies that the minimum amount of material that is potentially acquirable by a proliferator is dictated by the size of a fuel assembly. However in particular circumstances, such as during maintenance, workers might open a fuel assembly and extract, or replace, some its elemental constitutive elements, which are the fuel rods.

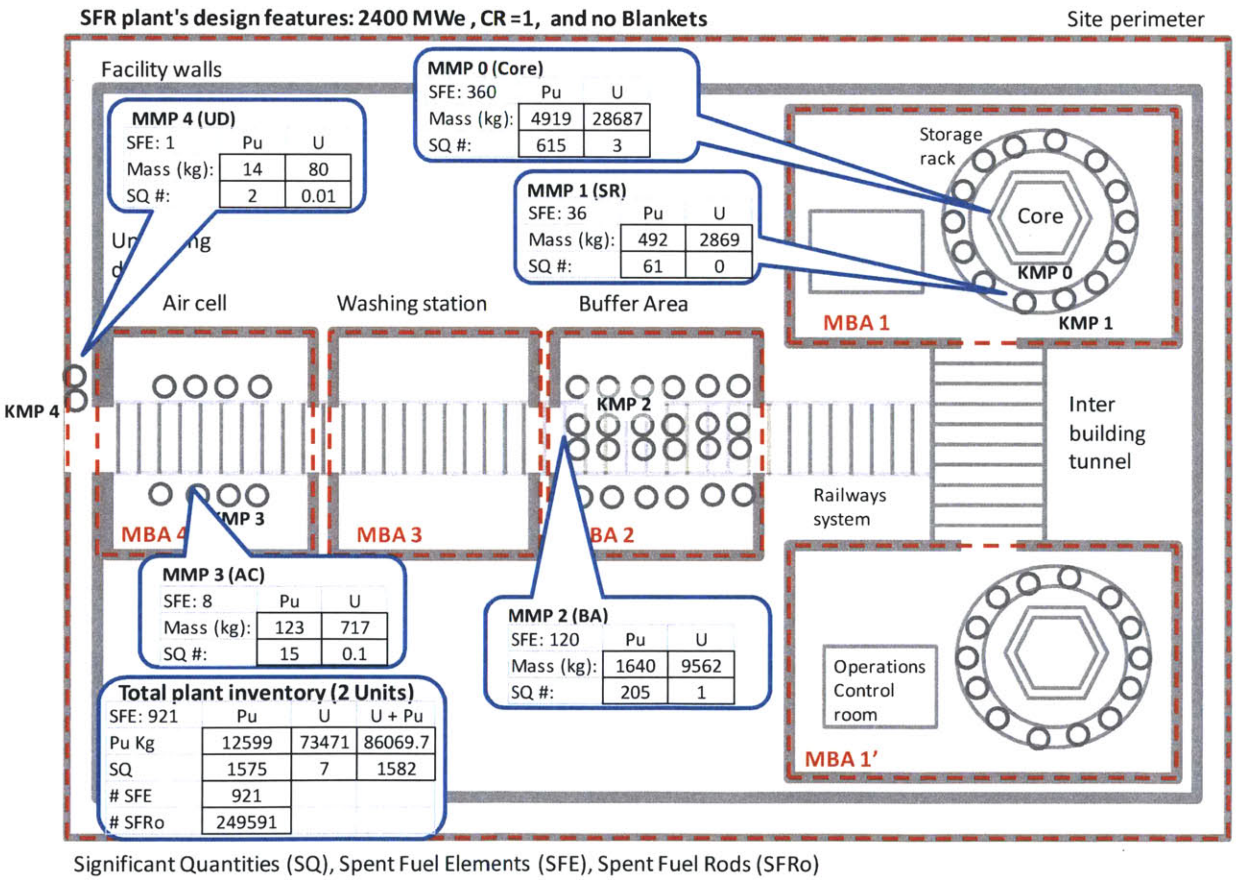


Figure 41. SFR plant inventories of Uranium and Plutonium for each material balance area.

Therefore the total number of potentially acquirable items on site can be seen either in terms of total fuel assemblies and fuel rods. For this plant the number of fuel rods in each assembly is equal to 271. In conclusion, at any given time the SFR plant of the figure contains 921 fuel assemblies and 249,591 fuel rods.

At the bottom of the facility map reports the entire inventory at the SFR plant's site. the number of elements at each location were obtained by considering a photograph of the plant operating at full power after its third refueling.

Considering that each fuel element contains 1 to 2 significant quantities of plutonium, a proliferator would be required to successfully conduce at least 271/2 =135 consequent acquisition trials to obtain the plutonium required to assemble a nuclear weapon device. Note that also americium (Am-241) and Neptunium (Np-237) have critical masses and can be considered in the overall calculation of the SQs located within the plant (see also Figure 55 in the Appendix).

Proliferator's Pathways and Safeguards

Four main theft acquisition scenarios are assumed. Each pathway is defined by an acquisition point and by a trajectory to transport the acquired material out of the plant.. The corresponding pathways are shown in Figure 42 and modeled by means of ST/ET models reported in Appendix A. Each acquisition has been broken into three different modalities: acquisition of a fuel assembly, of a fuel rod and of a bundle of fuel rods. Each of them require a different number of attempts to get 1 SQ settle as the final proliferator's goal.

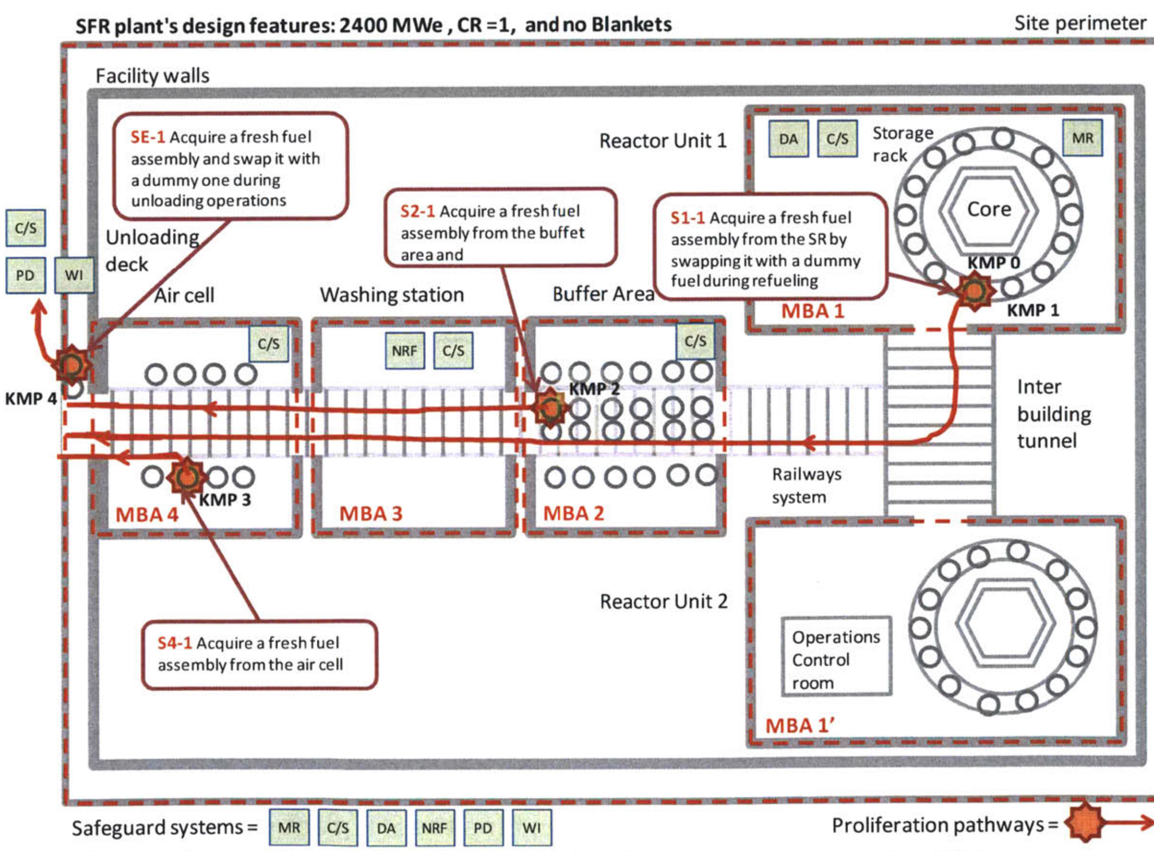


Figure 42. Proliferator's pathways and safeguards systems at the SFR plant.

QUANTITATIVE ANALYSIS

EXAMPLE OF ASSESSMENT OF A SAFEGUARD SYSTEM: OPTICAL SURVEILLANCE CAMERA

System description: Optical surveillance (OS) cameras are part of the containment and surveillance(C/S) function of a safeguard system. The optical surveillance system is generally composed of a primary camera pointing a location, item, or transit area such as a door, and of an auxiliary camera watching the primary camera and the environment around it. The system also includes cables under the walls sending the signal to a control room where operators watch the output on a screen. The cameras are powered by the plant's internal supply system but also each of them is connected with a backup system. Cameras are passive systems since usually data are gathered, collected but visualized just one special circumstances require to do that. In some cases, the system might be connected to a movement recognition system, in turn connected to an alarm. This is the case of cameras installed in some reprocessing facilities such as the Rokkasho one in Japan. Due to these features, the optical surveillance system is always connected to an encrypted storage unit where all the visuals are under custody and restored when inspectors come on site or after an alarm sounds.

OS for nuclear power plant: Optical surveillance systems, especially after September 11, are installed in all the rooms into which is segmented a nuclear power plant. The SFR plant shown in Figure 42 is being protected by an optical surveillance system, with at least a camera in each location. The cameras installed in a power plant has usually some extra features such as: resistance to temperature gradients, low sensibility to radiation field, and an high rate of frames per second (about 60 frames/second).

Main Function: The purpose of an optical camera is to increase the probability to detect anomalies in operations, suspect movements from operators, intruders, and potential accidents.

Source of information: In order to determine the features of an optical surveillance system, its cost and the probability to elude the system, we sent our questionnaires to *Fluidmesh Netork Inc.*, an MIT startup operating in the surveillance system environment since 2004 [1]. The questions were posed to the founders of the company. Also other sources of information to get acknowledged about OS systems and to understand the features used in NPP applications where found in [2].

Proliferator tactics: in order to elude the camera there are various possible tactics:

- ***T0, or NT:*** the first tactic is to rely on the system's accuracy and hope that the proliferator's action is going to be undetected. However, while this strategy could reveals successful for an accounting measurement system, for a surveillance system it is very unlikely that it will not reveal an anomaly. Therefore this tactic is considered for completeness but, as shown next, considered very improbable from all the experts surveyed.

- ***T1, T11, T12:*** the first tactic is to attack the hardware of the optical camera system and to damage it in order to interrupt, disrupt, or falsify data acquisition while the illicit acquisition of SNMs takes place. In order to be undetected the proliferator needs also to attack the surveillance camera pointing the OS hardware (T11), and break and replace the seals placed on the OS system (T12). A plausible strategy is fooling the camera images by physically reaching and removing the memory card storing the recorded photogram. The plausible sequence for this tactic, which was proposed to experts, could be: *tamper with the stored data, defeat the tamper-indicating device such as a seal or tag systems used for protecting data storage system, alter the data stored in the removable memory of the IS system, and finally hide any evidence of the entire operation.*

- ***T2, T22, T21:*** another plausible strategy is fooling the camera images by hacking the software that manages data acquisition. Each image being received, is digitalized, authenticated, and finally encrypted before being stored; a fake signal, with a digital signature and containing false or past images, can be inserted into the system replacing the signal directed to the storage unit. The plausible sequence for this tactic, which was proposed to experts, could be: *intrusion of the operating system managing the station that in the control room controls the OS system, decryption of data, insertion of fake data and tamper with the stored data, defeat the protection and encryption software used to protect the OS data in the storage system, and then cancel any evidence of hacking operations (T21) from the PC's operating system, including the data recorded by the camera pointing the PC's desk in the control room (T22).*

- ***Other tactics:*** another option for a proliferator is to simulate a fake accident within the server room. This accident involves the entire OS system of cameras interconnected in various location of the NPP, therefore it is being added in the upper part of the success tree where tactics having effect on multiple locations are considered.

Elicitation process: using the formal elicitation protocol that we developed to derive experts' subjective judgments, a discrete set of probabilities were derived and used as inputs to the success tree model. In order to gather all the data necessary to compute the success tree structure of the OS system reported in Figure 45, each expert had to provide a set of three points (success probability, error in the estimate, and cost evaluation) for each of the proliferator's tactics. The tree includes 2 primary tactics, 1 no tactic event, and 4 supportive tactics. Furthermore an evaluation of the system unavailability, which comprehends the estimate and its error, is required. Therefore, each expert had to provide 23 different evaluations, which were averaged to determine the evaluation used as inputs for the model.

Fooling Optical Camera Images

Figure 43 plots the probability inferred from the accuracy declared from the three experts. All experts agreed declaring that the event to be undetected for an intrinsic lack of accuracy is very close to be zero and declining as more sources are used to increase the accuracy of the OS camera.

Figure 44 plots the probabilities of the tactics of fooling surveillance camera images in the two cases of hardware and software attacks. All experts made very similar estimates of the cost related to the extra features being added to the OS system in the three different cost regions. Experts B and C in general provided lower probabilities than the ones of expert A. all experts agreed that the probability to defeat the OS system decreases when more resources are devoted to it. However, they also provided higher uncertainties for the values in the high resources range.

Cost evaluations: the estimated cost for an optical camera system, obtained by considering the average value from the evaluation provided by the experts, is ranging from $27,700 cost of a simple camera to $75,000 of a Digital Multi-Camera Optical Surveillance System (DMOS). Adding features to these camera so to reduce their vulnerability to software and hardware related attacks, would bring the overall cost evaluation to range from $20,000 cost of a simple camera with extra seals up to $223,000 which is the cost of a DMOS with additional encryption software, multiple storage system, and redundant cameras.

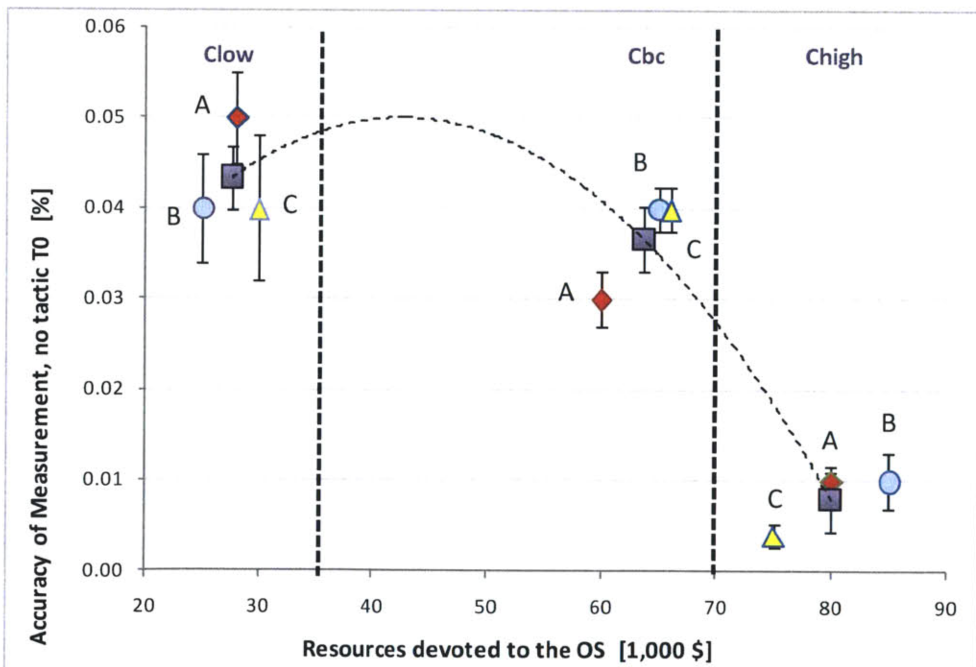


Figure 43. Experts' estimates for the probability to successfully elude an optical surveillance system without recurring to any tactic (T0).

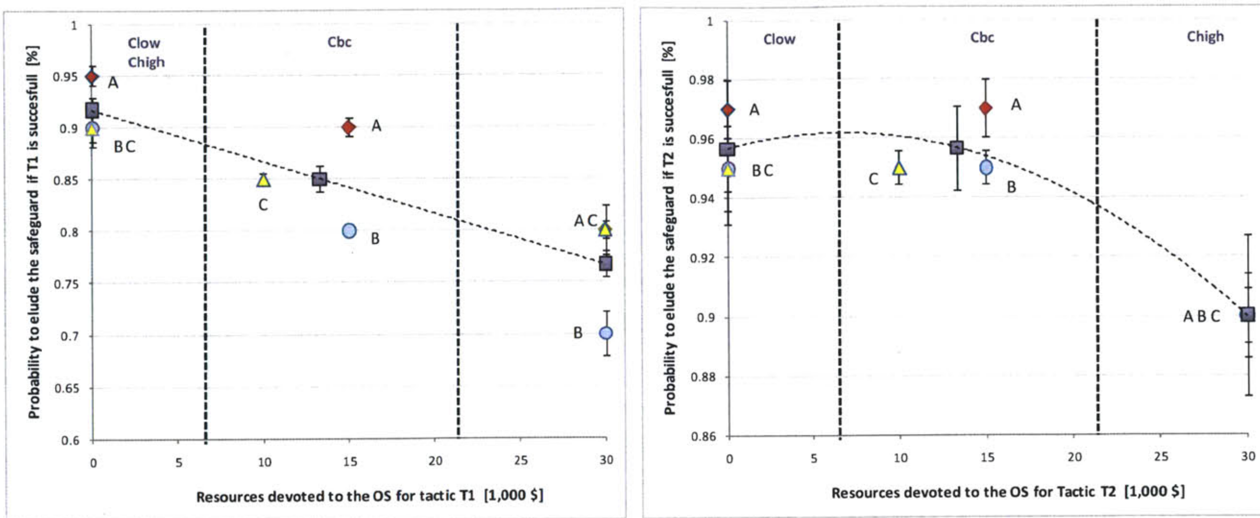


Figure 44. Experts' estimates for the probability to successfully elude an optical surveillance system by manipulating the hardware of the OS system (T1) or by hacking the software managing the system (T2).

Optical Surveillance Success Tree

The probability to acquire SNMs from a location protected from optical surveillance cameras is derived from the success tree structure shown in Figure 45. The successfulness of an acquisition attempt in a given location is determined by the proliferator's willing to pursue it, based on material and location features modeled by the probability Pin, and by the probability capturing the proliferator's ability to elude all the safeguard systems installed to protect the materials in that location. In this example the location is represented by the buffer area of a power plant. The location is protected by cameras, being part of the optical surveillance system, OS, and having the task to detect any anomaly of the fuel elements transiting in this area. The probability to elude an optical camera, *Pe,os,* does not depend upon the target mass since fuel rods and fuel assemblies are considered to be always recognizable and visible items. However, the probability to elude a camera by recurring to tactics such as an hacking attack to the OS software, is possible and functional to the resources that the safeguarder devotes to its physical protection. Thus, the probability to elude the system without recurring to any tactic, , labeled in the tree in Figure 45 as *Pnt,os,* is minimal. However when tactics aimed to reduce its effectiveness are employed, elusion becomes very likely. If the safeguarder efforts to prevent physical threats to the safeguard system are adequate, the chances of success for the proliferator are reduced.

The left side of the tree models the intentions of a proliferator willing to acquire SNMs from a particular location sited within a nuclear installation. The probability that a proliferator is going to pursue an acquisition event, Pin, is modeled by the left branch of the tree, which combines the parametric probabilities of the tree major sub-metrics HTC, LA, and MA. The three metrics are calculated for three different scenarios, each one corresponding to a different amount of mass acquired. The probability to start an acquisition threat is therefore functional to the benefits and cost associated with the amount of mass diverted compared to those of a base case represented by the acquisition of the smallest constitutive unit of material (i.e., a fuel rod for the case of a nuclear power plant).

The initiator probability Pin of the figure refers to a scenario where a mass M2 equals to 38.5 kg (i.e., the total mass equivalent of a sub-assembly made of 90 fuel rods) is being set as the acquisition target. The probability is shown as constant line since the three measurements HTC, LA, and MA are not seen as dependent upon the resources placed to protect the SNMs in the location.

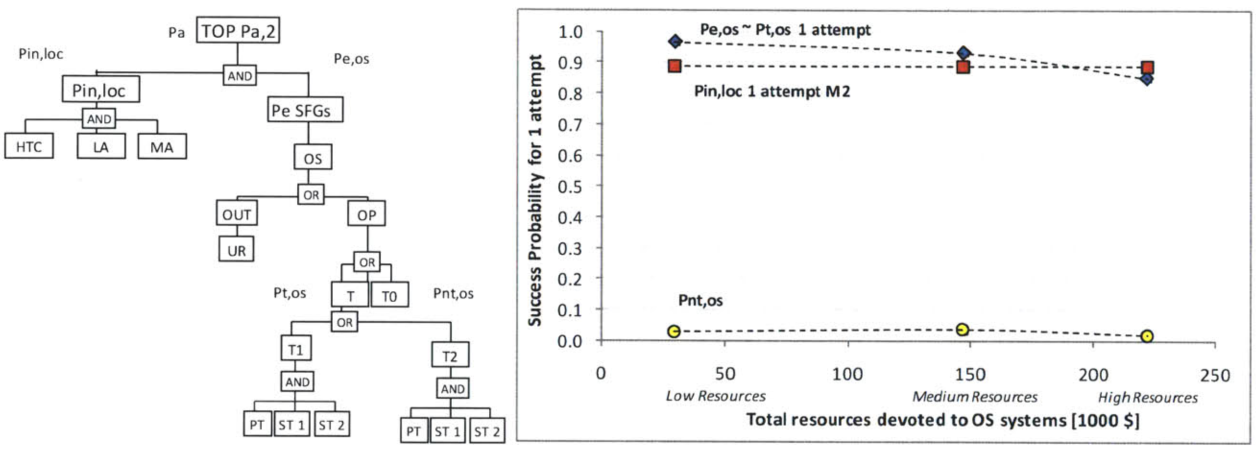


Figure 45. Success tree structure and results for the major probabilities populating the tree shown as a function of the resources that the safeguarder is devoting to the optical surveillance system protecting material balance 2 and 4 at the SFR power plant.

The OS system response to elusion is calculated for three different levels of resources devoted to its protection at about 30, 150, and 220 thousands of dollars. The probability that the proliferator is going to be undetected without recurring to any tactics is extremely low as shown by the *Pnt,os* trend line in the bottom of the figure. The dependence of the probability Pin from the mass of material acquired is shown in Figure 46. The resulting trend takes into account of the three different behaviors of the MA, LA and HTC functions and associated with a mass increase.

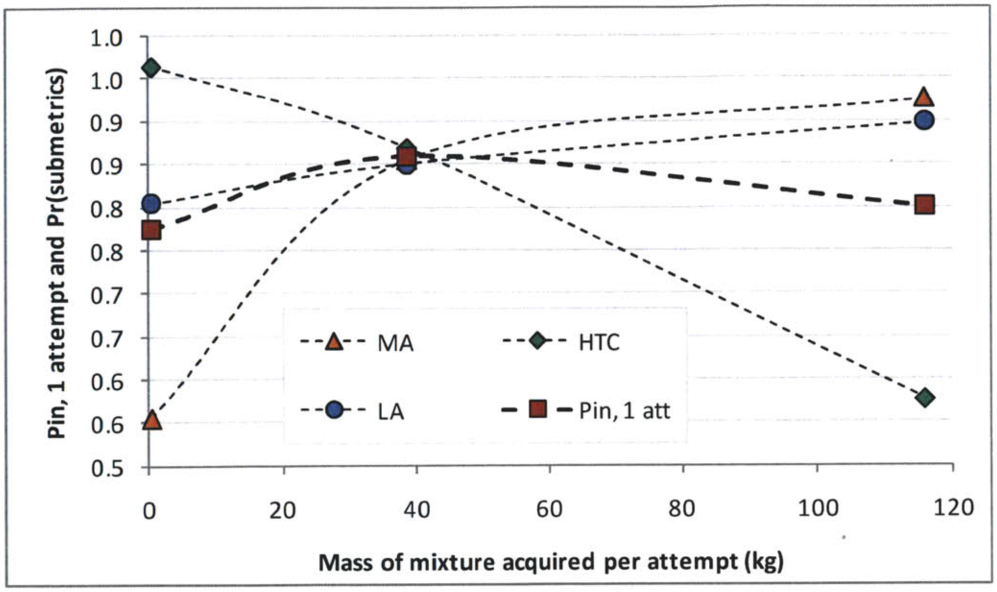


Figure 46. Sub-metrics contributing to Pin as a function of the mass of mixture acquired.

The three calculated set of data points correspond to the case where a fuel rod, a sub-assembly (a set of 90 rods), and an entire fuel assembly (271 fuel rods) are being selected as a target for an acquisition attempt. As shown, the material attractiveness increases as the mass of the acquired target increases. A similar but weaker sensitivity to mass is shown by the location attractiveness function, which considers the time necessary to extract the fuel rods from a fuel assembly. On opposite, the fuel handling and transportation capabilities decrease as mass increase because the material needs more shielding and cooling capabilities, furthermore its volume increases.

Probability Consequence Curve of the OS system

Figure 47 reports the acquisition probability for the location analyzed as a function of the number of significant quantities acquired per attempt. If the individual attempt does not lead to the acquisition of a significant quantity ,then the proliferator will repeat the attempt until it collects the target value of one SQ. If the proliferator decides to steal one fuel rod at once, in order to collect a significant quantity of plutonium, he needs to repeat its malicious act 170 times. Since all the 170 consecutives attempts have to be successful, the probability of success of entire set of trials, deduced from a binomial distribution, is very low and close to zero. When the proliferator decides to acquire a sub-assembly made of 90 fuel rods, if successful, he gets about half of a significant quantity. In this case 2 consecutive attempts are sufficient to acquire the target 1 SQ, and the probability of the two independents events is reasonably high to decide to pursue the series of attempts. The third case is represented by the acquisition of an entire fuel bundle. One fuel bundle contains about 1.6 SQs, therefore if successfully acquired no further attempts are required. Amongst the tree cases analyzed in this example the latter one is the most promising one. One should expect that the acquisition of elements of small size is less likely to be detected; while this statement is generally true for standard safeguard systems. However it is not true in this case because the optical surveillance system is not sensitive to size. Therefore the acquisition probability shown in the figure is not driven by the elusion probability, which has not dependence from mass, but simply by the intentions of the proliferator which increase with mass size. Finally, the chances to succeed decrease for all scenarios when the safeguarder devotes more resources to the physical protection of the optical system increase.

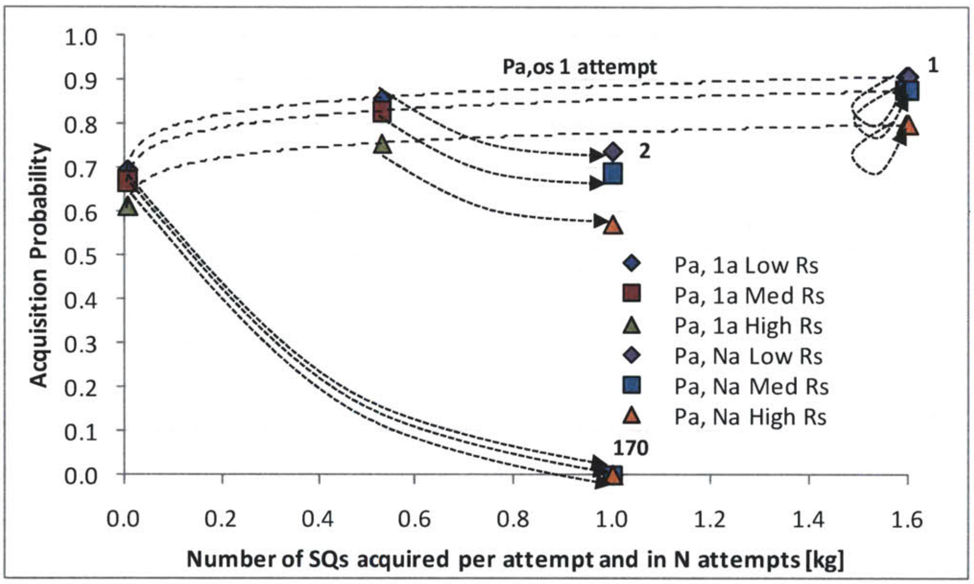


Figure 47. Proliferator success probability as a function of the number of SQ acquired per attempt and after a series of attempts. The results depends on the resources devoted OS.

For each location the parametric probability to start an acquisition attack has been calculated. Figure 48 compares the results of the evaluation at the 5 different material balance areas into which the plant was segmented into. Three distinct radar plots shows the variation of the probability Pin with the acquired mass. Due to the non-linear dependency with mass of some of the sub-metrics used to calculate Pin the three plots are not concentrically disposed following the amount of mass acquirable by an attempt. The most likely, and thus most attractive opportunity for a proliferator is offered by the acquisition of a sub-assembly composed of 90 fuel rods. This is because it contains almost a SQ of plutonium, it is modestly easy to carry, shield, and cool. The most convenient location to acquire the sub-assembly is represented by the core, which has the biggest variety of fuel elements, and the longer accessible time during refueling. The acquisition of an entire fuel assembly is ranked second, since it allows to get 1 SQ in a single attempt, and the acquisition of a single fuel rod third because of the inherent difficulty in its extraction from a fuel bundle. For the three case the location is not a strong discriminator and the reactor core remains the most attractive location.

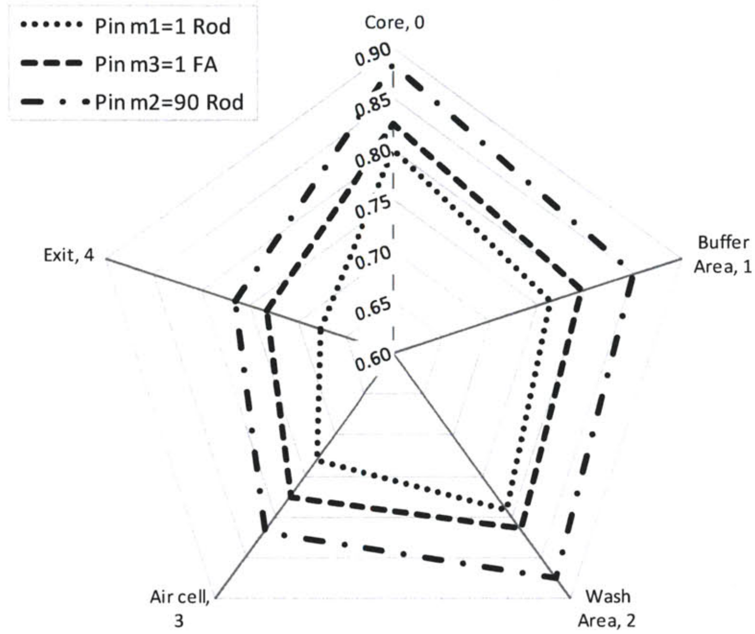


Figure 48. Initiator event probability, Pin, calculated for three different diverted mass sizes at five different locations of a SFR. The results in the radar graph refer to one acquisition attempt.

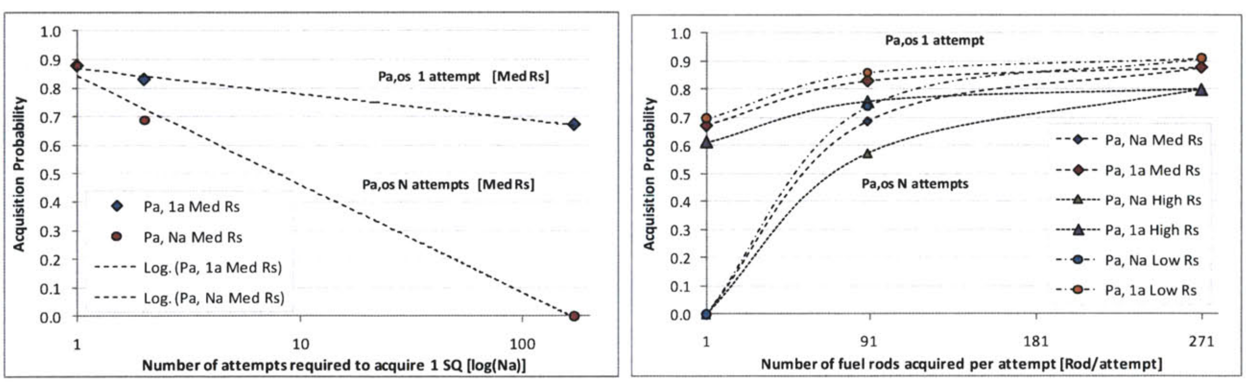


Figure 49. Optical Surveillance systems' results summary from the ST quantitative analysis.

REFERENCES

[1] Personal communications and questionnaires with U. Malesci, C. Malesci, A. Orioli. Boston, December 2010. http://www.fluidmesh.com/

[2] IAEA, "Safeguards Techniques and Equipment," 2003 Edition, International Nuclear Verification Series No.1 (Revised), 2003.

EXAMPLE OF BARRIERS ADDITION: NUCLEAR RESONANCE FLUORESCENCE

The determination of the detection systems performance is an important aspect belonging to the wide domain of non-proliferation. Protecting nuclear energy systems from potential threats, is essential especially in case of a resurge of nuclear power, and of the consequent spread of nuclear technologies in new countries. If reprocessing is going to be employed to couple it with fast reactors or to reduce the waste stockpiles, the current safeguard schemes are inadequate to monitor and account special nuclear materials.

The ST/ET method is being tested to verify the increased performance deriving by the addition of a novel detection technique based on nuclear resonance fluorescence (NRF). In parallel, the standardized experiment or set-up and the assessment of the NRF is conducted to verify the NRF performance in presence of acquisition threats.

The preliminary results obtained on the NRF setup studied confirmed the applicability of NRF to nuclear fuel cycles, and the validity of the ST/ET method to assess the proliferation performance of the NES.

Principle and advantages of the NRF technique

Following the principle that actual safeguard schemes rely on the identification of material properties (i.e. gamma, neutron, heat, and weight) from which the original sample composition can be deduced, and given the unsatisfactory type of responses that these schemes will provide in more complicated contexts where reprocessing facilities are employed, then techniques revealing the fingerprint of the material inspected are essential.

The isotopic identification technique that has been selected relies on the physical principle known as Nuclear Resonance Fluorescence.

NRF is an non destructive active (NDA) interrogation technique and a typical configuration for this system consists of an active Bremsstrahlung beam, which by hitting the target material produces an interrogation based on de-excitation of nuclides; the de-excitation mechanism in turn emits discrete and penetrating photons that are detected by germanium detectors positioned at a certain angle in order to discriminate the natural gamma radiation coming from the sample.

One major advantage of NRF technique is the characteristic gamma radiation generated and induced by the active Bremsstrahlung beam that is able to penetrate a fuel assembly envelope, or, for the example being set in this Section, the canister containing the separated Pu mix deposited within the electrorefiner. The NRF technique can accurately and timely track the amounts of each isotope within a sample even at a great distance from its surface, potentially not interrupting operations.

The NRF technique has other several advantages for the detection of Plutonium coming from spent fuel[1].

Its twin atomic process, X-ray Fluorescence Resonance (XRF) does not get clear signals from portions of material located in depth of the target (e.g. this does not permit to identify diversion of SNM within assemblies or canisters and might lead to stop operations).

Historically, destructive assays (DA) techniques took longer times to identify a sample of spent fuel material. In the case of the US SFR pilot plant EBR-II, a regular verification of the isotopic composition via DA (i.e. sampling and comparing to burn-up code simulations) took between 2 and 3 weeks, a period under which the facility might be arrested if the interrogation of the sample is being caused by suspects on the activities running on site [3].

Therefore, a strategic positioning of the NRF equipment within a plant can accurately monitor material streams continuously, almost in real time (i.e. a lag of about 2 hours has been demonstrated for cargo applications[2]).

Regarding the NRF maturity for its possible application as a safeguard for nuclear fuel detection, a set of preliminary tests using Passport Systems' test bed at the 4 MeV MIT accelerator, collaborative research with Pacific Northwest and LLNLs, revealed that strong NRF signature lines are present in the ^{239}Pu, ^{235}U isotopic elements and they can be effectively detected with a transmission method as it was verified at MIT[4].

Finally, the amount of information available from the company testing this technology made possible to include safeguards efficiency considerations into the ST structure as described in the next sections.

Applying the NRF technology to NMA problems

The original application of NRF technology in detection has been in the area of cargo inspections [2]. This section highlights the principles that have been followed in the adaptation process from cargo inspection to nuclear isotopic identification. Table 16 summarizes the highlighted principles followed in the adaptation phase from cargo to isotopic identification for nuclear facilities.

When making the transition from cargo inspections to nuclear material accountancy (NMA), some critical aspects had to be considered. One key difference between cargo inspection and NMA is the material that is being inspected. In cargo containers, the material that is being detected is primarily low Z. This allows for a greater volume of material to be inspected. Entire cargo containers can be inspected in a single pass, while in the NMA case, only grams of nuclear material can be inspected due to its high Z nature. While this may initially make the nuclear case seem daunting, there is the benefit that when determining the isotopic composition of nuclear materials, the outcome is known. If there is any deviation from the expected outcome, it is a sign of diversion. In the cargo case, the contents of the container are entirely unknown. Anticipating the outcome of the measurement in the nuclear case allows measurements to be made quickly and accurately.

A final important difference is the existence of background radiation for samples obtained from SNM. The material being analyzed is radioactive by itself, but any additional fission products add a great deal more radiation to the system. For this reason, the detectors must be shielded, the beams collimated, and the interrogated photons backscattered to reduce the effects of the background radiation.

While there seem to be some hurdles associated with the NMA application, NRF is capable of determining the composition of the material. Each isotope gives a distinct signal based on its NRF absorption energy. This allows for an accurate measure of the isotopic composition. Not only will the NRF be able to accurately measure the material (chemical processes can be used to do this), but the NRF detection method is non-obtrusive, non-destructive, and most importantly, can be used in real time.

Table 16. Nuclear resonance fluorescence adaptability.

Problem specifics	*Cargo Application*	*Isotopic identification*
Material to detect	Partially unknown	Expected with uncertainties
Material form	Any type	rod, chopped, ingots, powder, pins, liquid
Shielding	Unknown and masked	Cladding, crucible, ER walls, salt, pipe walls
Mapping type	One unique scan	Multi-scan in different streams + mapping
Operating atmosphere	Air	Air, Argonne or inert gas
Barriers to detection	Materials	Radiation, spontaneous fission, background
Elements	Nitrogen, fertilizer, U238, other explosives	^{235}U, P^{239}u, Actinides (Np, Am, ..)
Z separation in the target	Very distinct and not isotopes (High and Low Z)	Very similar high Z (actinides series), FPs (Medium Z)

Although NRF is an ideal method for maintaining NMA, other design alternatives of clandestine material detectors are currently evaluated, such as a variant proposed by LANL that incorporates a pulsed photon accelerator (PPA) to introduce the interrogating photons.

However, while this technology is capable of determining whether a specific isotope is present, it does not provide information prescribing the quantity of that material analyzed, and therefore does not meet the scope of the application of interest.

Other similar techniques (e.g., XRF), as mentioned before, do not allow for going beyond the surface of the material analyzed. This constitutes a major impediment for applications where a hot material has to be identified, a disadvantage that collides with the benefit of using pyro-reprocessing, which instead has the merit to operate separation at very high temperatures in comparison to traditional aqueous processes.

NRF configuration for isotopic detection within a reprocessing facility

A simplified configuration for isotopic detection imagined to be located within a reprocessing facility has been virtually set up during a series of meeting held last summer. The experiment, illustrated by Figure 50, is described by showing the intensities calculated in correspondence with the primary areas in which the photons can be tracked. The division in beam zones was also done to help understand the main vulnerabilities of the apparatus in parallel with the parameters, zones, or part of equipment determining the NRF detection efficiency.

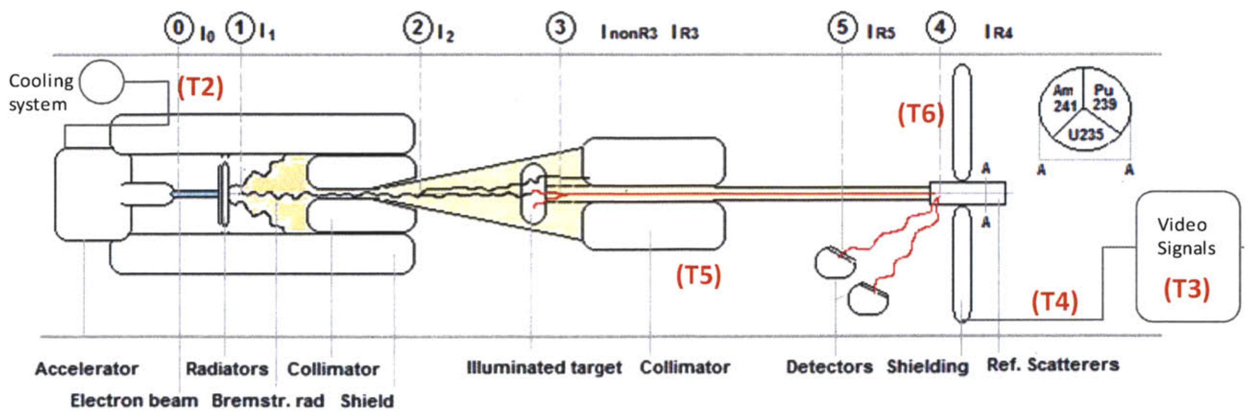


Figure 50. Schematic of the experimental pre-design created to study the NRF detection system showing the potential vulnerable points and beam zones.

Appropriate modifications were made to address the new environment and sample type: the high Z nature of the material and the high background radiation requires that a large number of incident photons be used to penetrate the sample and reduce the effects of the background radiation. The presence of high background radiation, potentially interfering with the characteristic NRF gammas requires a particular setup of the machine called transmission method. The transmission method consists of the incident photons attenuating throughout the sample. There is attenuation at all energies, but within the NRF ranges a greater number of photons are attenuated. The resulting beam passes through a collimator to the reference scatterer. The role of the scatterer is to absorb the photons within the NRF energy ranges, and then back scatters photons which are captured by the detector. These photons reveal the nature of the sample. The use of the reference scatterer is made possible by knowing the contents of the sample, which is a key difference between the original cargo container application and the NMA application.

Although the NRF detector has the potential to accurately determine the isotopic composition of a sample, there are some potential weaknesses of the detector. The first and foremost is due to the nature of the sample itself that is made of a mix of materials coming out from the ER. The relatively small quantities of certain isotopes may diminish the accuracy of the detector. While this effect can be reduced by adding more detectors and increasing measurement time, there will still be a margin of error that could be exploited. Additionally, the background radiation plays an important role in the operation of the detector, therefore it may be possible to modify the background radiation that decreases the accuracy of the detector. These weaknesses can be exploited and are reflected in the success tree structure.

The experiment that was designed has four main components: the creation of the incident beam, the fuel sample being measured, the reference scatterer, and the germanium detector.

Figure 50 provides a schematic of what the experimental configuration looks like. An accelerator creates the electrons that are assumed to have an energy of 3MeV. These electrons then are absorbed in the radiator which in turn, releases a beam of photons that range in energy from 3MeV down to 0MeV. The intensity of the beam that is being tracked is then reduced with the use of collimators. Following this initial reduction of intensity, the photons then pass through the sample of separated nuclear material. The following section describes the vulnerabilities and the critical efficient point identified in the NRF configuration selected.

Accuracy-vulnerability analysis

As a proliferator, the necessity of bypassing the NRF detector is of the utmost importance. The weaknesses of the detector provide potential avenues to disrupting the detection. Any detection system can be disrupted by modifying the signal coming from it, changing the software, or sabotage. Unique to the NRF however is the possibility of adding extra material to change the background radiation or adding shielding to modify the accuracy of the detectors. For each of these categories, the proliferation performance of the NRF detection system can be increased by placing more resources into the detector. For example, more detectors may increase the accuracy of the detector and reduce the chances of disrupting the signal.

The rationale that calls for a vulnerability analysis of the detection systems introduced to increase the proliferation performance of the NES (i.e. extrinsic barrier) is that they are not sufficient to guarantee the protection from potential threats unless their capability proves to operate reliably also when directly exposed to the threat. This is because when the safeguarder improves his defense strategies by introducing new detection systems, such as the NRF, the proliferator might consequently readapt his strategies elaborating new tactics to include in the overall strategic threat. This twisted mechanism is indeed the fundamental principle under which the competition between the two potential actors occurs and therefore needs to be accounted into the PR assessment model.

In order to qualify the performance of the NRF apparatus, an analysis to determine the equipment's vulnerable points has been conducted, and then shown to experts in the area of detection physics.

The NRF configuration, as shown in Figure 50, was divided into six physical regions which were associated with six corresponding threats. The threats were identified, sometimes by running a sensitivity analysis on the parameters of the NRF model to measure variations in its efficiency, and in most cases by direct identification of the sub-systems most sensitive to physical attacks.

Table 17 summarizes the result of the investigation conducted on the NRF configuration, while the following discusses some of the possible vulnerabilities for the NRF configuration presented in this Section.

The first vulnerability refers to the entire NRF set up, and considers a failure of the system originated from a stochastic failure of the machine or by an unintentional initialization of the system. This eventuality distinguish from the rest of the vulnerabilities since it is not due to an external agent. It represents the intrinsic unavailability of the NRF machine.

Table 17. Vulnerability table showing the physical threats to the NRF system.

#	*Threat*	*Causes*	*Mitigation*	*Resource*	*M$*
1	Unavailability, efficiency	Initialization, calibration, false alarm rate, operator	Periodic maintenance, training of the personnel	Inspection personnel	0-0.6
2	Efficiency of the electron beam	Cooling system, power supply	Protect cooling system, redundant power trains	Sealing, monitoring, covering equipment	0-0.4
3	System Interpretation	Software program	Encrypt data, skill more operators, recording	Data encryption, personnel	0-0.2
4	System Interfering	Signal cables	Protect cables with alarms, EM field shielding, tampering, recording	Cables, recording, tampering	0-0.1
5	Beam interfering	Shielding addition to sample or apparatus	Physical protection, sealing, measurement time	Cover, sealing	0-0.3
6	Sample manipulation	Background radiation to sample	Germanium detectors, measurement time	GE detectors	0-0.4

The other five physical regions analyze agent-based events following the same logic illustrated in the example that follows. Region 2 is characterized by the parameters describing the accelerator's electron beam. The equipment on site is the accelerator, the target radiator(s), and shielding materials. The accelerator cooler could be sabotaged to generate a decrease in the beam intensity that in turn could cause a shift in the end-point of the generated spectra. In order to exclude this from occurring, or to reduce the probability to misuse the cooling system, the safeguarder could invest more resources to add physical barriers to the cooling system and to monitor the fluctuations in power at the electron beam source.

For these five cases, experts are asked to determine the probability to fail under a specific threats as a function of the resources devoted to protect the system from that threat. The counter measures necessary to prevent the events 2 to 6 to occur determine an extra cost on top of the resources already allocated for the equipment, reported in the right column of Table 2. The performance and the functionalities of the equipment are then a function of the resources invested to increase its performance. A range for the financial expenditures required to contain the problem has been set so that a minimum of zero corresponds to the situation where no precautions are taken, and a maximum corresponds to the value beyond which additional expenses would have no impact on the mitigation strategy adopted.

The vulnerabilities and inefficiencies revealed by this analysis were, after computed by mean of an expert's elicitation process, subsequently incorporated into the ST structure, as described by the example in the next section.

Success tree structure and basic event probabilities

The proliferator's perspective implies to defeat the safeguard systems by eluding their measures and therefore bypassing the safeguard function built to strengthen the vulnerabilities initially present in the design. In order to capture the concept of safeguardability, the NRF detector was decomposed into sub-regions and analyzed in its behaviors as discussed previously. The events emphasized from the vulnerability-efficiency analyses conducted on the pre-design configuration shown in Figure 50 were logically embodied into the tree structure as shown in Figure 51.

The figure shows how each of threats analyzed is captured by the events represented by the boxes at the bottom of each branch of the tree. In other words, each threats is represented by a basic event in the tree. The entire threat set, in this case composed of 5 tactics and 1 reference event (i.e. the intrinsic unavailability of the NRF system), constitutes the set of tactics that supports the primary proliferator's strategy.

The ST structure's role is to merge all the information obtained and to provide an overall estimate which includes all the realizations of the supportive tactics used by the proliferator to defeat the NRF detection system, assuming these realizations are independently pursued.

Once the structure of the tree is assembled, the next step is determining the basic event probabilities. The following discussion represents how to measure the probabilities of the basic events constituting the minimal path sets. The values of the BEs are evaluated using two different methods. One is to calculate the probability values utilizing measures (i.e., the first basic event referring to the intrinsic unavailability of the NRF system), and the other is to obtain the values of the BEs from the subjective judgments of selected experts. The measured metric, Ps, results to be a function of the level of expenditure that the safeguarder foresees to use in reaction to a potential proliferator's threat. Implicitly in this process, the safeguarder is assumed to know the proliferator's capabilities.

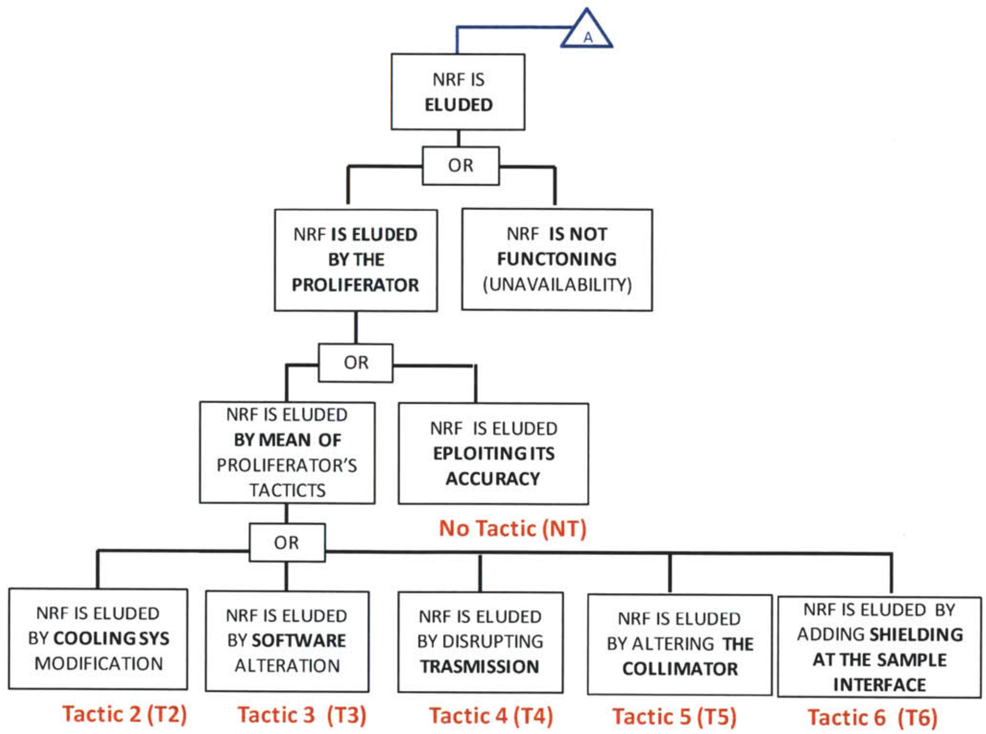


Figure 51. Tree measuring the NRF success probability.

Thus, in reality, the probability to safeguard efficiently the NRF system depends on the level of monetary effort that both parties devote to succeed in their respective goals. However, for a theft scenario, this aspect is left out and the proliferator's resources devoted to succeed are modeled as a constant and hypothesized sufficient in relation to the proliferator's goal (i.e. the diversion of considerably low amounts of material does not require special monetary efforts). Refined versions of this framework will consider the resources of both parties. Provisionally the probabilities are functional to the safeguarder resources.

The relationship between the resources devoted to protect the system from an acquisition threat and the success probability to defeat the systems when these resources are allocated, is provided by the experts.

The aggregation of the four experts' opinion were respectively conducted using the simple equal weighting principle. This approach is consistent with the SSHAC study where the adoption of an equal weighting approach is seen as reasonable since it avoid determining how to assess who the best expert is, if any, and since it provides a decomposition in which different evaluations can be explicitly compared. The uncertainties associated with the cumulative aggregate probability distribution, are not considered at this stage and therefore the curves are meant to be point estimates.

The procedure followed can be replicated and extended to any safeguard or extrinsic barrier of the NES. To prove the concept, only the assessment of the NRF safeguard has been evaluated, and insights coming from the analysis are reported in the example that follows.

The Scenario

A proliferator tries to acquire a SQ of deposited within the main separation machine (i.e., the electrorefiner) in a reprocessing plant of batch type (i.e., pyro-reprocessing facility). In this design, though to reprocess metal spent fuels, the separation unit is positioned within a hot cell containing inert gas where operations are held remotely. The hypnotized threat is the diversion of a SQ from and just right after this inaccessible area during maintenance when some of the traditional safeguarding systems do not operate. The NRF machine is being positioned at the exit of the hot cell with the scope to timely monitor the stream of materials (e.g. plutonium, actinides, etc.) in transit from the hot cell. Two different sequences are analyzed: the diversion of 1 SQ with a single attempt, and a series of attempts aiming to acquire 1 SQ summing all attempts. In this case, the NES can be considered proliferation resistant, if the NRF safeguard efficiently and reliably reveals the amount of materials that is being subtracted in these two scenarios.

Results

The ST/ET model was used to assess a complete Success Tree including four other major safeguards to the reprocessing plant. The results reported in this sections are indicative and shown with mere illustrative purposes. Despite coming from a more complex and exhaustive model, they emphasize the role of the NRF technology in protecting the NES from diversion. The scope is to proof the list of concepts listed as follows:

Concept I: the ST/ET model can be used to determine the initial PR of a NES and its variations when NRF is added to the safeguard scheme. The top event of the three measures the PR of a given NES as well as any variation due to the introduction of design changes;

Concept II: the proliferation performance can be further increased by considering to invest more resources to either reduce the vulnerabilities to single threats, or increase the intrinsic performance of the NRF apparatus;

Concept III: the ST/ET model can be used to compare different scenarios. In this case we compare a single diversion scenario with a multiple diversion scenario (500 attempts to divert 1/500 of a SQ vs. 1 attempt aimed to divert 1 SQ at once). The set of equation below summarizes these two scenarios:

$Pr(\text{Acquire 1 SQ}) = [Pr(\text{SCENARIO} \mid Pa)_K]^N$

Case 1: $Pr(\text{Acquire 1 SQ}) = [Pr(\text{TOP})]$

Case 2: $Pr(\text{Acquire 1 SQ}) = [Pr(\text{TOP})]^{500}$

where Pa is the initiator event expressing the will of the proliferator to proceed a diversion attempt.

The results obtained from the ST/ET model simulated with a simulation software. The calculation were set up using the estimates obtained via experts' elicitation, and uncertainties were associated with the estimates by the analyst.

Concept I

Figure 52 shows the distribution of the success probability Ps of the top event Pr(NEWTOP), considering the entire tree structure, in the two cases where low and high effort in terms of resources are used to safeguard the NES.

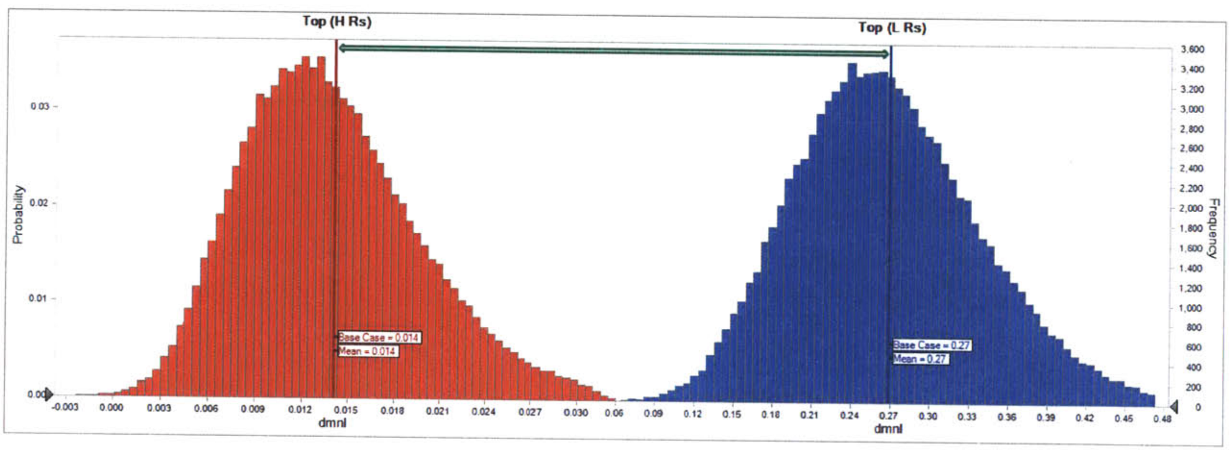


Figure 52. Probability changes obtained by varying the resources devoted to the NRF safeguard.

The blue right curve corresponds to the situation where low resources are used to safeguard the scheme, while the red curve represents the same scheme when potentiated by mean of monetary efforts. The graph therefore confirm the model's capability to capture the inefficiencies of the safeguard scheme as well as to reveal the changes in performance when the individual systems are further protected from the proliferator's tactics.

The proliferator's success probability measured at each attempt results to be 0.27 in the low resources case, and 0.014 when the four safeguards are improved. The corresponding monetary expenses in the two cases are correspondingly of 2.213M$ and 4.013 M$.

Given the provisional value of these numbers at this stage of the project, it is however worth to note that their order of magnitude is relatively low compared to the cost estimates of a reprocessing facility serving a 1800 MWe SFR plant is about 800 M$ considering contingencies, and that the cost of the basic equipment of a NRF detecting device with a 3 MeV accelerator is in the order of 2 M$.

Therefore, it seems that the relative cost of introducing performance changes, in the entire safeguard scheme provides a benefit/cost positive gain in favor of taking the decision to introduce the changes.

Concept II

Regarding the adoption of NRF technology, the variation measured between the low and high resources case, is equal to 4.013 – 2.213 = 1.8 M$. The high resources evaluation provide by the model, implies to almost double the costs of the NRF machine in a standard configuration. Then the introduction of additional systems to protect the NRF equipment should be motivated by a corresponding high gain in the measured performance Ps.

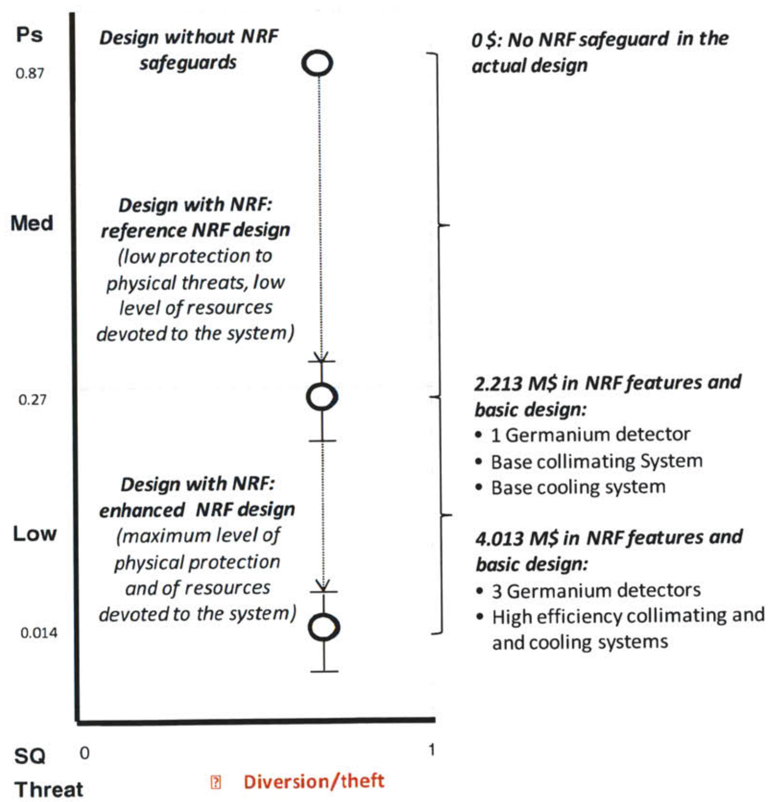


Figure 53. Safeguardability of the NRF detector as a function of the resources devoted.

Figure 53 summarizes these findings and reports the impact generated by the introduction of NRF safeguards in the scheme. The figure suggests that the introduction of NRF significantly reinforces the robustness of the entire scheme. The proliferator's probability of success is considerably high when the NRF technique is not employed and then falls down of about one order of magnitude when NRF is included in the system.

The lowest portion of the figure shows the relative merit deriving from the introduction of additional systems to defend the NRF from the proliferator's tactics for 1 attempt. The improvement in the Ps performance factor does not seem significant when compared to the cost gain above commented. However, the importance of having more resources devoted to protect the NES becomes important when the entire scenario leading to the acquisition of 1 SQ with several attempts is considered, as shown by the next figure.

Concept III

Figure 54 considers the NRF safeguard and the two scenario of low and high resources employed to protect the NES. The graph shows the variation of the NRF performance measured by the metric Ps over a set on N attempts obtained used using the methodology described in Chapter III. The y-axis reports the proliferator's probability to succeed acquiring 1 SQ over one or more attempts, while the x-axis reports the mass the proliferator acquires in each attempt, and that has to be detected by the NRF instrument.

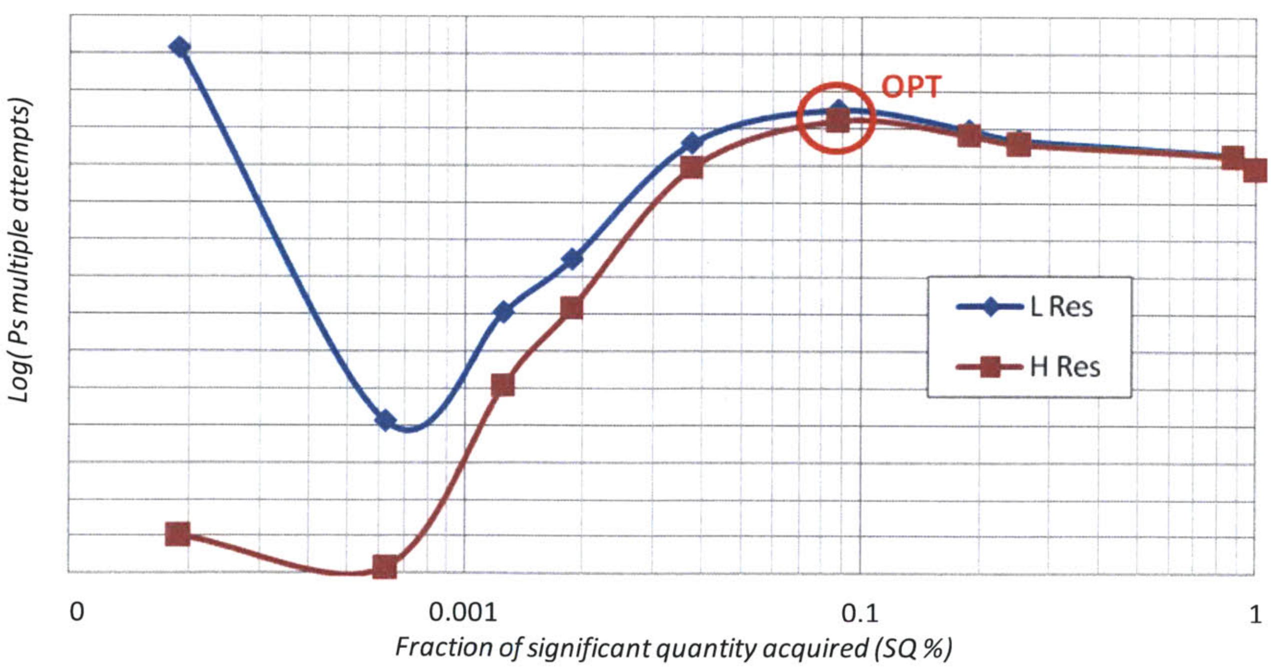


Figure 54. Probability to elude the NRF system as a function of the fraction of SQ acquired.

The two cases of high and low resources are compared. The figure shows that while the trend of the curves is identical, a difference of several orders of magnitude, empathized for the scenarios targeting lower SQ fraction, differentiates the two cases. With respect to the previous analysis, where only one attempt is considered, the analysis considering the entire sequence confirms the importance to devote high resources devoted the safeguard scheme.

CONCLUSIONS

The illustrative example, although oversimplified, confirms the ability of the model to provide adequate responses to changes in a measure of the non-proliferation performance, PR, when design changes are applied to the safeguard scheme of a given NES. The NRF technology is suggested for adoption in a safeguard system for isotopic detection of nuclear fuels for future fuel cycle facilities.

REFERENCES

[1] S. J. Tobin et al., *"Determination of plutonium content in spent fuel with NDA – why an integrated approach?"*. Los Alamos National Labs, 2008. LA-UR-08-03763 (2008).

[2] Bertozzi W., Korbly S. E., Ledoux R. J.,*" Nuclear resonance fluorescence and effective Z determination applied to detection and imaging of special nuclear material, explosives, toxic substances and contraband,"* Nuclear Instruments and Methods in Physics Research B 261 pp. 331-336, (2007).

[3] Personal communication with Prof. Michael Lineberry, MIT (2009).

[4] W. Bertozzi et. al., *"Nuclear Resonance Fluorescence Excitations near 2 MeV in 235U and 239Pu,"* Physical Review C 78, 041601(R) (2008).

[5] Koji Sato et al., *"Conceptual Design on an Integrated Metallic Fuel Recycle System,"*, Takeshi Yokoo, Tadashi Inoue Pyro-Process Fuel Cycle Project, Komae Resesarch Laboratory, Central Research Institute of Electric Power Industry 2-11-1, Iwado Kita, Komae, Tokyo 201-8511 Japan (2001).

PART VI: CONCLUSIONS

In this work a novel framework to address the proliferation performance of nuclear energy systems has been presented. The framework can be used to risk-inform nuclear designs, therefore to assist policy makers, designers, and regulators to make decisions regarding the proliferation risks associated with a nuclear facility. The constituent components of the framework are an assessment technique, which is being used to calculate the probability under which a proliferator might succeed in acquiring nuclear materials from a NES, and a policy, used to determine the risks and the risk limits considered acceptable for a NES.

The present thesis analyzed the framework from a system engineering perspective, highlighting the design principles and mental thinking behind each decision that was taken over the construction of this assessment.

The framework provides an holistic, and systemic solution to solve the problem of nuclear proliferation and nuclear energy systems. The approach used in the creation of such a framework was multidisciplinary and balanced areas of expertise from different disciplines: physics, nuclear engineering, statistics, management, and over all political science.

The framework has been built by using an underlying analogy with the safety framework built in the US by the NRC in the past decades.

The natural application of the framework is a license for nuclear power plant based on their proliferation performance, which might be provided by the NRC. An alternative could be the creation of a certification proving the quality and the performance of a nuclear energy system from an anti-proliferation standpoint. This can be offered from a private company, from a scientific accredited organization, international regulatory body, or a university.

The motivation for introducing this new standard, or standardized process for the evaluation of NES are many. One is the imminent commercialization of new nuclear designs, the so called small modular reactors (SMRs). If these designs enter the nuclear market, they can change the entire structure of the nuclear industry as it is today, and that resulted from long construction cycles of monolithic power plants. The shift of paradigm from big to small designs has an immense potential of disruption not just in the markets but also the structure of the relationships between governments, investors, constructors, and the society. Also from a geographical perspective, nuclear power is ready to move in regions of the world which are undeveloped, less stable, and where terrorism is often remarkably present. In all these eventualities, nuclear proliferation might overcome other metrics such as cost and safety, and take a central role for the development of nuclear power.

Being ready today to address the non-proliferation issue, means having a peaceful world tomorrow!

CONCLUSIONS

Probabilistic risk assessment techniques are normally used to address safety of nuclear power plants. Since the establishment of these techniques, regulators created policies and regulations providing acceptance criteria to quantify the maximum allowable risks associated with the systems failures within a nuclear energy systems. Availing of the safety case, a new assessment technique and an acceptance criterion policy, has been established to quantify and limit the risks associated with proliferation for a nuclear fuel cycle. A sodium fast reactor's fuel cycle has been used to test the new technique, although the framework that is being formulated is technology neutral, and thus extendible to any technology. The framework so created is consistent with the modern approach used by risk-informed regulations [1]. The approach used in its formulation is holistic, systematic, and systemic. Major features and findings derived from the construction of the framework (model and policy) are synthesized as it follows.

Assessment Model

The assessment model replicates the philosophy and topology of the risk assessment techniques used in safety, since their effective introduction in 1975 [2]:

The objective of the evaluation addressed by the model is to measure a specific performance attribute, called Proliferator success probability, Ps, which can be directly related to the proliferation risk.

The performance attribute Ps is the probability to acquire, and successively transport, SNMs from a nuclear energy system. Ps contains evaluations of the intrinsic design barriers embedded in the NES, of the safeguard systems used for SNMs protection, and of the political counter measures introduced to prevent acquisition of SNMs.

In contrast with previous existing models [3], the PRA-like technique developed does not exactly measure the proliferation resistance and the physical protection (PR&PP) of a NES and its systems barriers, but it rather measures the capability of a NES to resist to the covert acquisition of SNMs.

Three main acquisition scenarios cover the entire variety of acquisition possibilities for a proliferator: diversion, misuse, and abrogation. Each of them represents a macro category for the strategies of acquisition which can be employed by a proliferator to complete his mission (i.e., obtain a SQ of SNMs in a pre-defined time). Strategies are further broken down into tactics: core to the model structure is the creation of a success tree (ST) model, which analogously with fault trees in safety analysis, determines the top event Ps by relying any single event contributing to the system's success (i.e., covert acquisition of SNMs).

Central to this representation is a sub-module of the ST structure which was formulated by means of an analysis of the primary and secondary functions of system safeguards, and more generally of any counter measure to the proliferation risk. For each safeguard placed to protect the NES, the sub-module combines the primary function of a safeguard system, or its intrinsic resistance to an illicit SNMs acquisition attempt (i.e., the systematic error of a detection, or of a measurement system), with the resistance from a physical attacks targeted to the secondary functions of the same safeguard (e.g., the structural, computational, transmission functions). This approach is taken from the systems architecture theory, and it was useful to establish a more rational relationship between proliferation resistance metrics and physical protection ones, than the one used in other frameworks [3].

Since risk evaluation techniques are often exposed to criticism regarding the effectiveness of the numbers they rely on, and this is even more true in this case where most of the basic event probabilities are driven by human actions rather than stochastic failure of the system components, it is important to note that:

The assessment model can be seen as a vehicle capable to capture the complexity of the system, and as a tool where the opinion of experts can be used systematically to obtain comparative evaluations for different design alternatives of the NES, and schemes of the counter measures adopted to protect the NES.

Different types of evaluations converge into the model, however while all interconnected one to the other by means of a ST/ET representation, the evaluations has been treated separately and trying to conserve the meaning of each of them sub-modules into which the model can be decomposed. For example, the intentions of a proliferator are expressed in terms of parametric probabilities (probabilities inferred from the evaluation of measurable metrics, such as the amount of SNM available in a location, or the number of spontaneous neutrons emitted by a mass of SNMs), while the probability to elude a safeguard system are obtain from the experts elicitation process (direct estimates of the probability to elude a safeguard). Both the types of evaluations can be used separately to evaluate different aspects of the problem, such as the abundance of SNM in a location, or the vulnerability of a safeguard to physical protection threats. This "property" of the model, to be broken down into different modules, guarantees a form of flexibility against potential mistakes in its construction, and allowed its construction to incorporate various techniques chosen accordingly with different modeling needs.

In summary, the assessment model proposed, benchmarked to similar assessment used in safety analysis [4], although complete and functional, has to be considered as a provisional assessment tool, until more results are available and until validated by comparing these results with the ones obtained by other models.

Acceptance Criteria Policies

Most of the considerations done for the model can be extended to the proposed policy framework, since its construction directly descends from the model. However it is worth to state some of the features of the probability-consequence representation that has been formulated to define the acceptable limits for the proliferation risk associated with a NES.

The probability of successful SNM acquisition, Ps, when related to the associated consequences, constitutes a direct measure of the proliferation risk. The consequences are a function of the acquired amount of SNM, and evaluated in terms of significant quantity. Each point in the two-dimensional space (Ps, SQ) represents the proliferation risk of the NES and its safeguards for a given scenario (e.g., multiple theft attempts). This representation allows analyzing, different designs of NES and of protection barriers.

Since the evaluation immediately descends from the assessment model, it was decided to give more importance to the relative position of points (i.e., the relative difference in the value of Ps between design alternatives) within the design space rather than to their absolute and punctual value (i.e., the absolute results obtained from the ST/ET model). For this reason, the y axis of the (Ps-SQ) space is divided into three confidence intervals corresponding to the three situations of High, Medium, and Low probability, to testify the presence of uncertainties in the evaluation and the use of the model in comparative terms.

In parallel with the creation of risk acceptance criteria, a set of design limits for nuclear non-proliferation was formulated. The design limits define some extra criteria that have to be respected in the nuclear fuel design so that certain conditions in terms of material attractiveness can be excluded a priori.

Also in this case, the policy proposed, which includes acceptance criteria and design limits, represents the best possible solution envisioned to solve the problem of the proliferation risk acceptance, given the knowledge available at this time, and considering the goal to create an assessment technique aligned and coherent with t risk-informed framework [1] used in safety.

REFERENCES

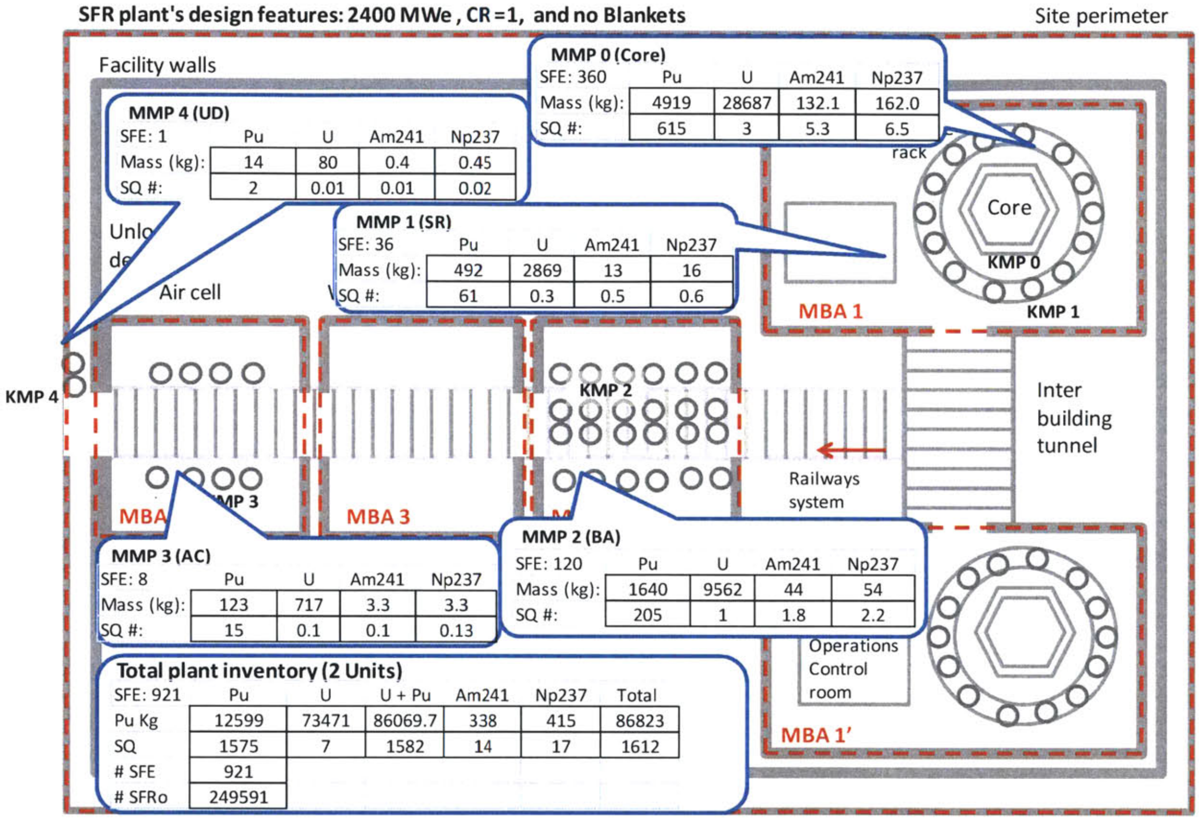
[1] NUREG-1860, "Feasibility Study for a Risk-Informed and Performance-Based Regulatory Structure for Future Plant Licensing". Office of Nuclear Regulatory Research, December 2007.

[2] Rasmussen, Professor Norman C.; et al. (1975-10). "Reactor safety study. An assessment of accident risks in U. S. commercial nuclear power plants. Executive Summary."

[3] PR&PP Group,: *"Evaluation Methodology for Proliferation Resistance and Physical Protection of Generation IV Nuclear Energy Systems,"* Revision 2, September 30, 2004.

[4] NUREG-1150, "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants". Office of Nuclear Regulatory Research, December 1990.

Appendix A: SFR Power Plant Assessment - Success and Event Trees & Additional Figures



Significant Quantities (SQ) and alternative SQs (Np and Am), Spent Fuel Elements (SFE), Spent Fuel Rods (SFRo)

Figure 55. SFR plant inventories of U, Pu, ^{241}Am, ^{237}Np for each material balance area.

ST/ET Model for the SFR power plant

The following figures report the structure of the framework used to model the acquisition and the transportation events.

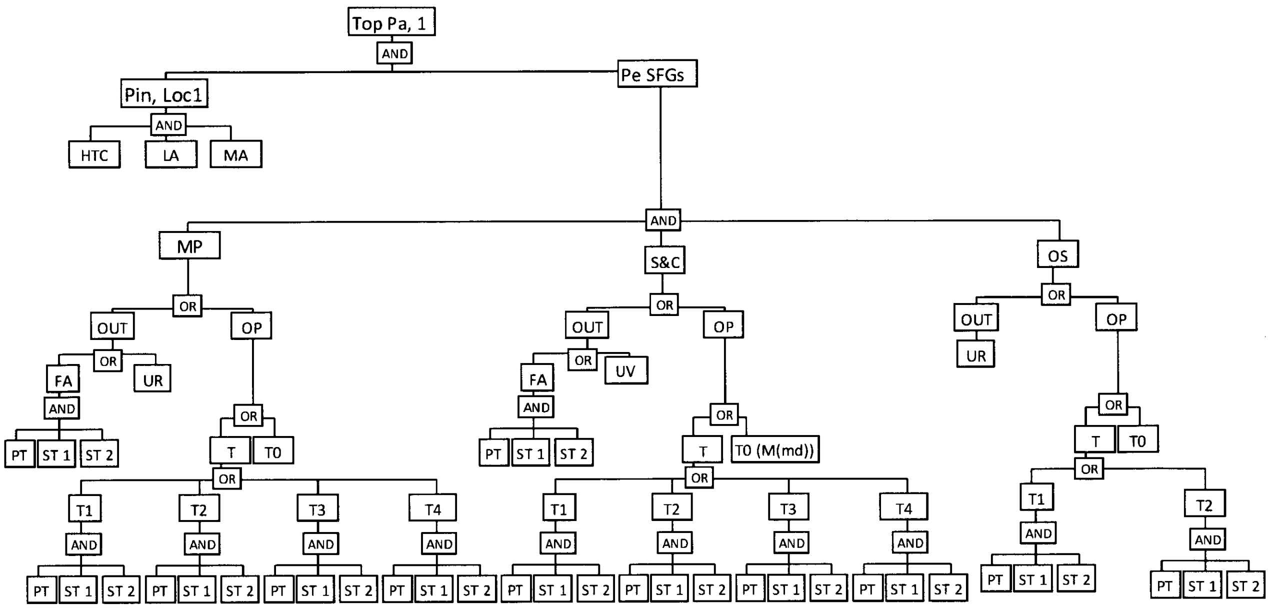


Figure 56. Success tree used to evaluate the proliferator's acquisition probability at MBA 1.

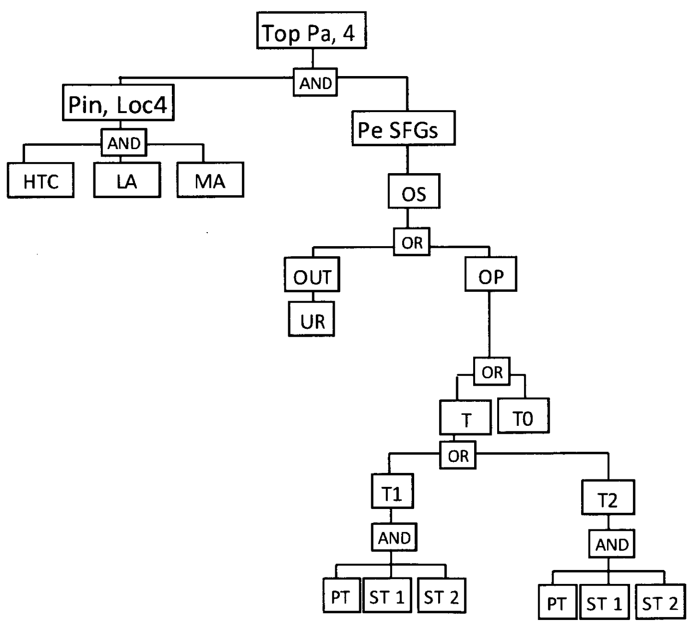


Figure 57. Success tree used to evaluate the proliferator's acquisition probability at MBA 2 & 4.

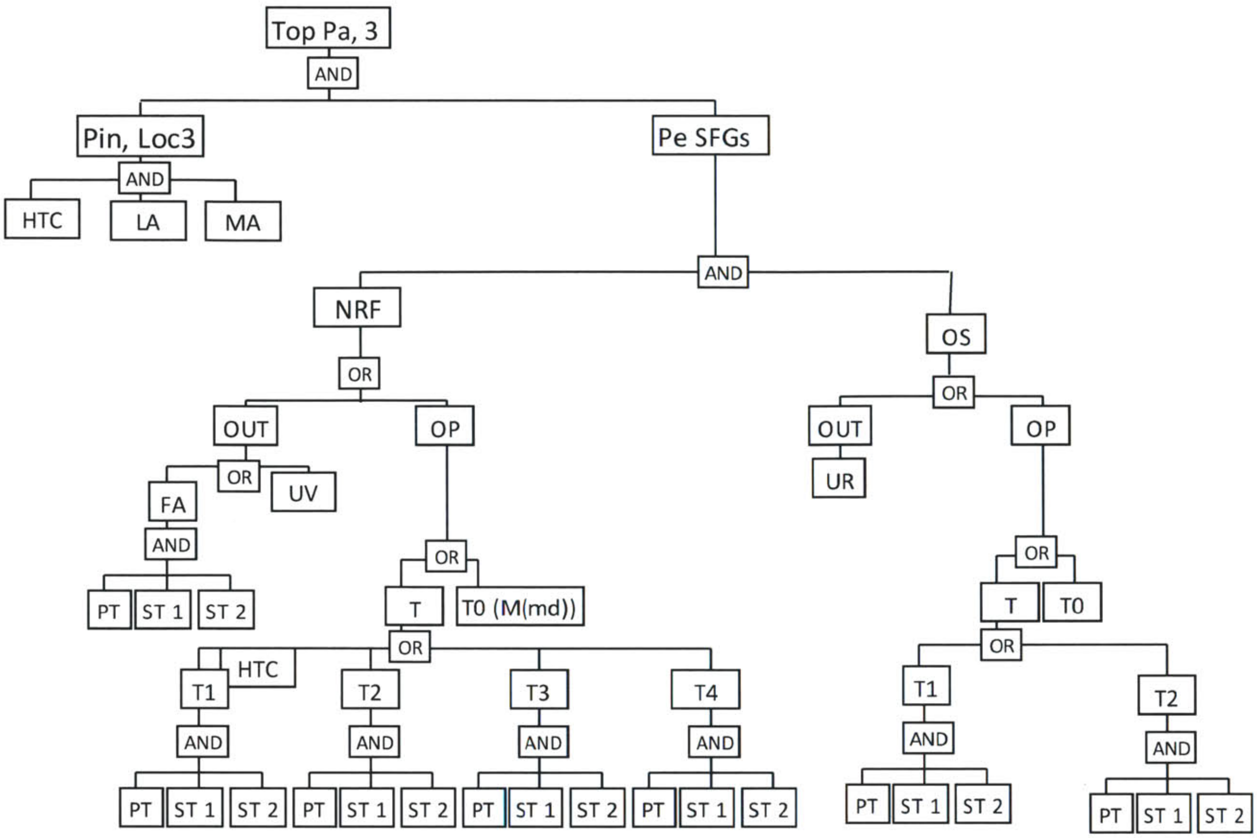
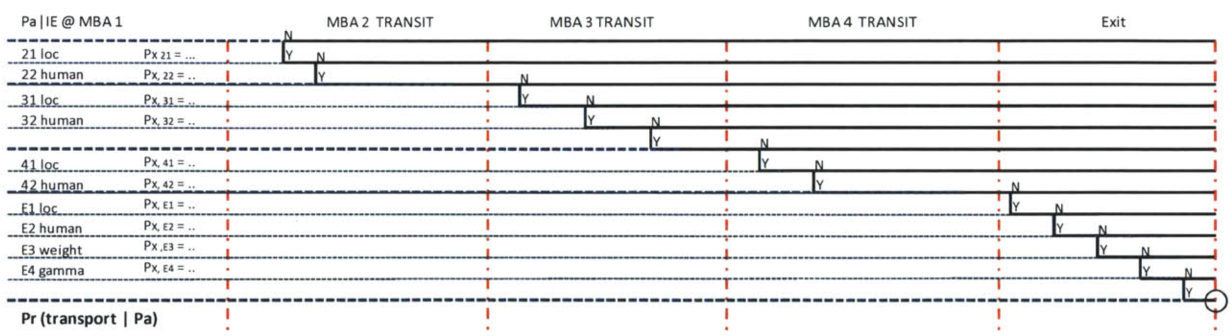


Figure 58. Success tree used to evaluate the proliferator's acquisition probability at MBA 3.



Detection System	Diversion point 2	Transit Location 3	Transit Location 4	Exit
Cont & Surveillance	X (loc, human)	X (loc, human)	X (loc, human)	X (loc, human)
Detection/MC&A System				
NRF	-	X(counting)	-	-
Weight	-	-	-	X (detection)
Gamma	-	-	-	X(detection)

Figure 59. Event tree created to model the proliferator's pathways and used to evaluate the probability of transportation of the acquired material out of the plant boundaries.

Appendix B: Source codes and tables used for the SFR plant assessment

	Energy	Half life	A	Decay	Critical	Cri Refl	Photons	Neutrons	Heat	Dose	SQ
	# peaks	years	Ci/g	MeV	[Kg]	[Kg]	[KW]	[n/s/Kg]	[W/Kg]	[rad/hr]	kg
Pu 238	4	87.74	17.4	5.5	9.7		1.62E-04	2.67E+06	567.13	3.10E-03	
Pu 239	6	24100	0.061	5.2	10.1	5.0	2.31E-07	2.30E+01	1.92	2.49E-05	
Pu 240	4	6560	0.23	5.2	36.9	20.0	2.06E-06	1.03E+06	7.09	1.72E-04	
Pu 241	4	14.4	112	0.021	13.0	5.0	2.32E-06	4.94E+01	3.19	2.02E-04	
Pu 242		376000	0.0038	4.9	83.4	31.0	2.88E-08	1.73E+06	0.11	2.45E-04	
Tot Pu											8
241 Am	7.0	430.0	3.4	5.5	60.0	30	4.96E-04	1.54E+03	113.98	5.52E-05	25
247 Np		2.00E+06			56.0	32.0	1.41E-07	1.39E-01	0.02	1.80E-05	25
235 U					53	25	0	0	0	0	25/75/1E+4
238 U					0	0					2E+04

Figure 60. Special nuclear material properties table being utilized to derive the parametric probabilities used in the risk assessment model.

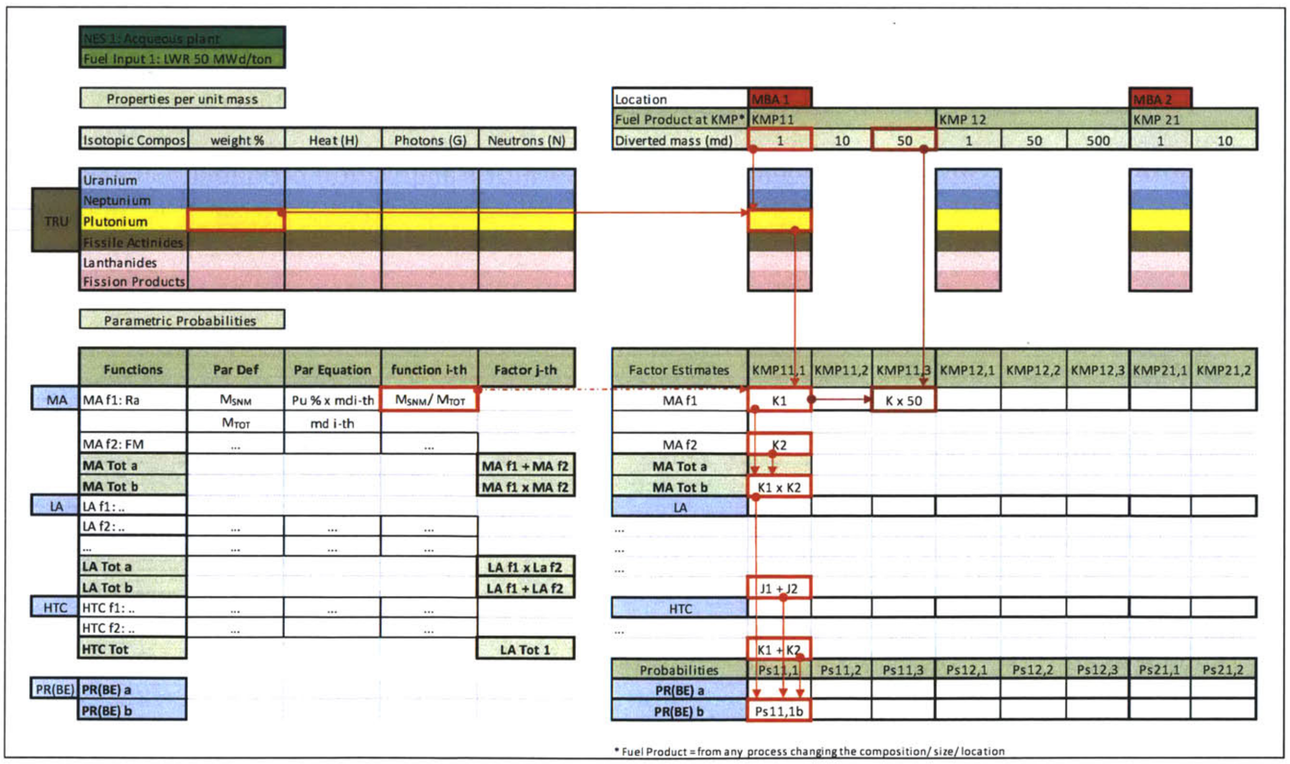


Figure 61. Sketch of algorithm and of the logic structure used to compute the parametric probabilities of the nuclear target at various locations and considering different target masses within key measurement points.

Appendix C: SFR Reprocessing Facility Assessment - success and Event Trees

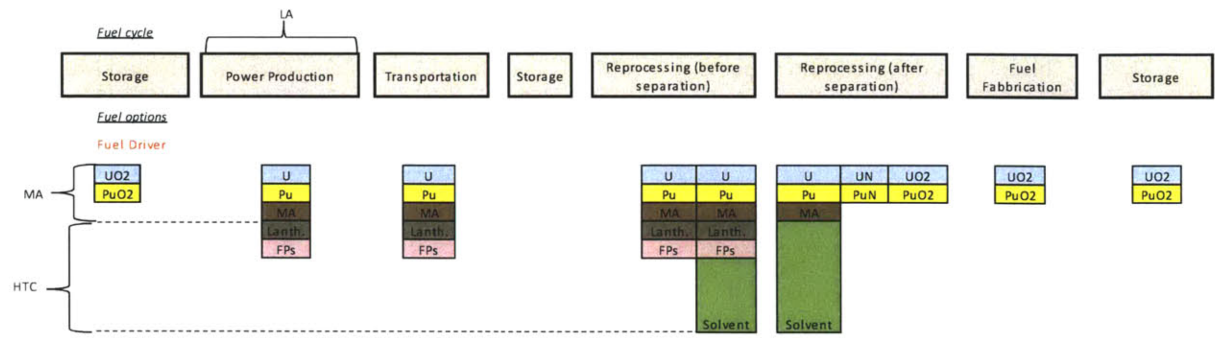


Figure 62. Sketch of algorithm used to monitor SNMs in a nuclear fuel cycle.

C.1 Material Balance Areas (MBA) at the Reprocessing Plant

Material Balance Area	Nuclear Material	Safeguards
MBA1: Feed Storage & Disassembly Area	Spent Metal Fuel U-Pu-Zr/FP	Containment and Surveillance Gamma Ray Spectrometry Neutron Counter Destructive Analysis ID Tracking Weight Inspection Heat Inspection
MBA2: Reprocessing Area	U, U-Pu / Salt, Cd	Containment and Surveillance Gamma Ray Spectrometry Neutron Counter Nuclear Resonance Fluorescence
MBA3: Fuel Fabrication Area	U-Pu	Containment and Surveillance Gamma Ray Spectrometry Neutron Counter
MBA4: Product Storage Area	Metal Fuel U-Pu-Zr	Containment and Surveillance Gamma Ray Spectrometry Neutron Counter Destructive Analysis ID Tracking Weight Inspection Heat Inspection
MBA5: Waste Storage Area	Solid Waste	Containment and Surveillance Gamma Ray Spectrometry Neutron Counter Destructive Analysis ID Tracking

C.2 Key Measurement Point (KMP) at the Reprocessing Plant

Inventory KMP	Flow KMP
• KMP-A: Spent Fuel Storage • KMP-B: Chopping and Dissolution Process • KMP-C: Electrorefining Process • KMP-D: TRU Extraction Process • KMP-E: Distillation Process • KMP-F: Fuel Fabrication Process • KMP-G: Metal Fuel Storage • KMP-H: Waste Storage	• KMP-1: Receipt of Spent Metal Fuel • KMP-2: Transfer of Spent Fuel Material between MBA1 and MBA2 • KMP-3: Transfer of Waste between MBA1 and MBA5 • KMP-4: Transfer of Waste between MBA2 and MBA5 • KMP-5: Transfer of U-Pu between MBA2 and MBA3 • KMP-6: Transfer of Metal Fuel between MBA3 and MBA4 • KMP-7: Transfer of Waste between MBA3 and MBA5 • KMP-8: Shipment of Metal Fuel • KMP-11: Shipment of Waste

C.3 Specific Safeguards at the Reprocessing Plant

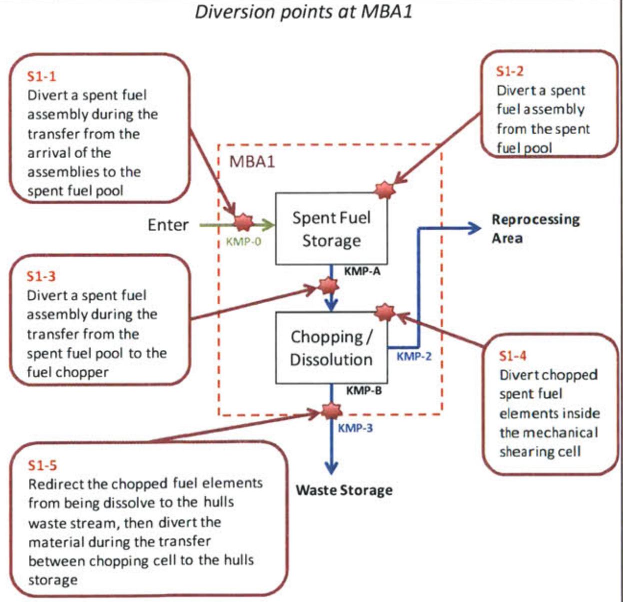
- Integrated Spent fuel Verification System (ISVS);
  - Verifies the unloading and receipt of spent fuel assemblies in an unattended mode for gross defects.
  - ISVS is based on surveillance cameras, neutron detectors and gamma detectors.
- Integrated Head end Verification System (IHVS);
  - Maintains continuity of knowledge of the spent fuel as it moves through the mechanical feeding cells to the shear cells and provides the spent fuel IDs.
  - IHVS is based on camera radiation detector (CRD) systems.
- Vitrified waste Canister Assay System (VCAS);
  - Provides semi-quantitative assay of the nuclear material content in the vitrified waste before being transferred to measured discards for termination of safeguards
- Temporary Canister Verification System (TCVS);
  - Provides inventory measurements of the plutonium in the MOX Temporary Canister Storage.
  - TCVS is based on neutron coincidence based system for measuring the stored MOX powder.
- Waste Crate Assay System (WCAS A/B);
  - Provides semi-quantitative assay of the nuclear material content in the low active waste crates and also the IDs of the waste crates.
  - WCAS is based on helium-3 detectors measuring the neutrons from the curium-244 and digital cameras.
- Plutonium Inventory Measurement System (PIMS);
  - Provides timely inventory measurements of plutonium in the glove boxes of the MOX conversion process lines at the time of the interim inventory verification (IIV).
  - PIMS is based on helium-3 neutron detectors installed on the MOX process glove boxes.
- Solution Measurement and Monitoring System (SMMS);
- Directional Canister Passage Detector (DCPD);

C.4 Diversion Threats and Safeguard Systems at the Reprocessing Plant

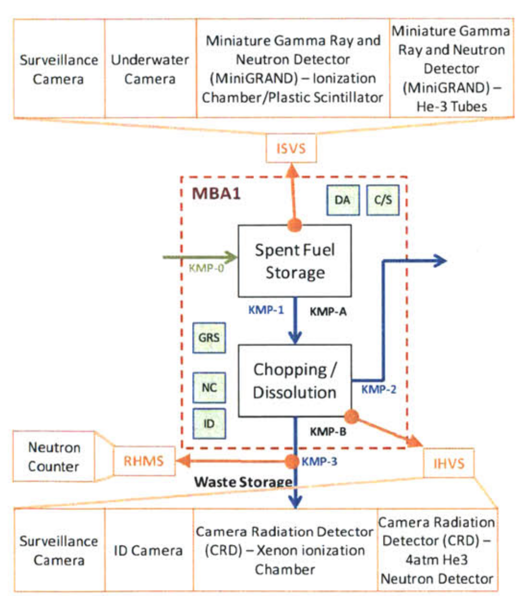
MBA 1: Safeguard systems: 2, # Safeguards: 12, Types of detectors: 5

ID #	*Material: envelope, form, composition*	*Key points [g/m, g]*	*Safeguard Systems*	*Scenario Description*	*Material Acquired*	*Sample Analyzed*
S1-1	SFE, solid oxide, U/Pu/MAs/FPs	KMP-0 [...]	• Surveillance Camera (ISVS_OSa) • Miniature Gamma Ray and Neutron Detector (ISVS_GRS/NCa)	Divert a spent fuel assembly during the transfer from the arrival of the assemblies to the spent fuel pool	Pu in a SFE [xx-yy kg] Pu in a SFR [xx-yy kg]	• SA_{111}: SFE/SFR items • SA_{112}: Pu neutrons in SFE/SFR
S1-2	SFE, solid oxide, U/Pu/MAs/FPs	KMP-A [...]	• Surveillance Camera (ISVS_OSb) • Under Water Camera (ISVS_OSc) • Miniature Gamma Ray and Neutron Detector (ISVS_GRS/NCb)	Divert a spent fuel assembly from the spent fuel pool	Pu in a SFE [xx-yy kg] Pu in a SFR [xx-yy kg]	• SA_{121}: SFE/SFR items • SA_{122}: SFE items • SA_{123}: Pu radiation and neutrons in SFE/SFR
S1-3	SFE, solid oxide of U/Pu/MAs/FPs	KMP-1 [...]	• Surveillance Camera (IHVS_OSd) • ID Camera (IHVS_ ID) • Camera Radiation Detector (CRD) (IHVS_ GRS/NCc)	Divert a spent fuel assembly during the transfer from the spent fuel pool to the fuel chopper	Pu in a SFE [xx-yy kg] Pu in a SFR [xx-yy kg]	• SA_{131}: SFE/SFR items • SA_{132}: SFE/SFR items • SA_{133}: Pu radiation in SFE/SFR
S1-4	CFE, solid oxide of U/Pu/MAs/FPs	KMP-B [...]	• Surveillance Camera (IHVS_OSe) • Camera Radiation Detector (CRD) (IHVS_GRS/NCd)	Divert chopped spent fuel elements inside the mechanical shearing cell	Pu in a SFE [xx-yy kg] Pu in a CFE [xx-yy kg]	• SA_{141}: CFE items • SA_{142}: Pu radiation in SFE/SFR
S1-5	SFE/CFE, Solid oxide/liquid nitrate of U/Pu/MAs/FPs	KMP-3 [...]	• Surveillance Camera (IHVS_OSf) • Neutron Detector (RHMS_NC)	Redirect the chopped fuel elements from being dissolved to the hulls waste stream, then divert the material during the transfer between chopping cell to the hulls storage	Pu in a SFE [xx-yy kg] Pu in a SFR [xx-yy kg]	• SA_{151}: CFE items • SA_{152}: Pu neutrons in CFE

Diversion points at MBA1



Safeguard Systems at MBA1

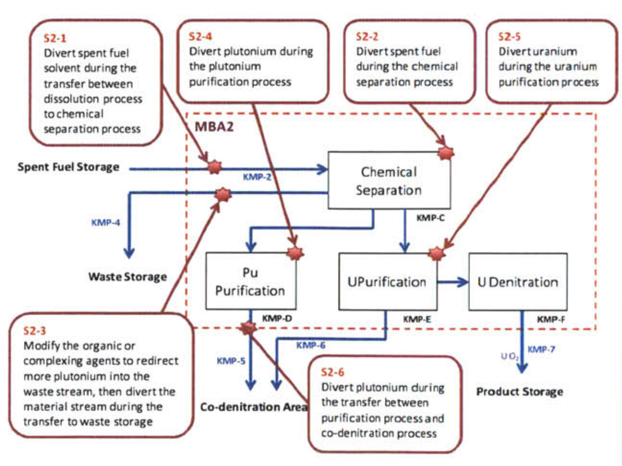


Nomenclature: SFE/SFR= Spent Fuel Assembly, Spent Fuel Rod, CFE= Chopped Fuel Element

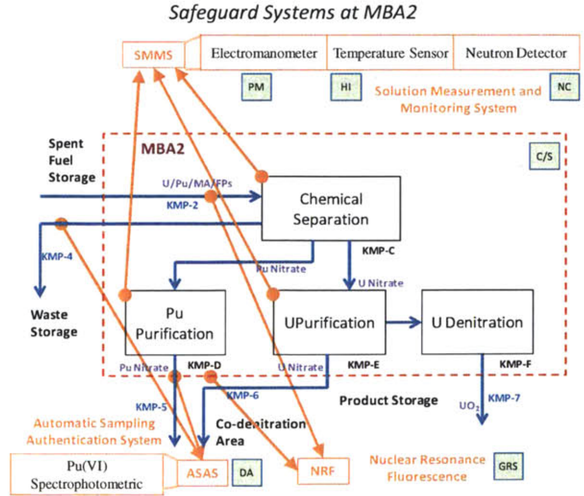
MBA 2: Safeguard systems: 3, # Safeguards: 11, Types of detectors: 5

ID #	*Material: envelope, form, composition*	*Key Point*	*Safeguard Systems*	*Scenario Description*	*Material Acquired*	*Sample Analyzed*
S2-1	Spent fuel solvent, Liquid mixture, U/Pu/MAs/FPs	KMP-2 [...]	• Electromanometer (SMMS_PMa) • Temperature Sensor (SMMS_HIa) • Neutron Detector (SMMS_NCa) • Nuclear Resonance Fluorescence (NRF_GRS)	Divert spent fuel solvent during the transfer between dissolution process to chemical separation process	Pu in a Spent fuel rod [xx-yy kg] Pu in a spent fuel assembly	• SA_{211}: SFE/SFR • SA_{212}: • SA_{213}: • SA_{214}:
S2-2	Spent fuel solvent, Liquid mixture, ...	KMP-C [...]	• Electromanometer (SMMS_PMa) • Temperature Sensor (SMMS_HIa) • Neutron Detector (SMMS _NCa) • Nuclear Resonance Fluorescence (NRF_ GRS)	Divert spent fuel during the chemical separation process		• SA_{221}: • SA_{222}: • SA_{223}: • SA_{224}:
S2-3	Pu Nitrate in waste stream (MA, FPs), Liquid mixture, ...	KMP-4 [...]	• Electromanometer (SMMS_PMa) • Temperature Sensor (SMMS_HIa) • Neutron Detector (SMMS_ NCa) • Nuclear Resonance Fluorescence (NRF_ GRS) • Pu(VI) Spectrophotometric Method (ASAS_ DAa)	Modify the organic or complex agents to redirect more plutonium into the waste stream, then divert the material stream during the transfer to waste storage		• SA_{231}: • SA_{232}: • SA_{233}: • SA_{234}: • SA_{235}:
S2-4	Pu Nitrate, Liquid mixture, ...	KMP-D [...]	• Electromanometer (SMMS_PMb) • Temperature Sensor (SMMS_HIb) • Neutron Detector (SMMS_ NCb) • Nuclear Resonance Fluorescence (NRF_ GRS) • Pu(VI) Spectrophotometric Method (ASAS_ DAa)	Divert plutonium during the plutonium purification process		• SA_{241}: • SA_{242}: • SA_{243}: • SA_{244}: • SA_{245}:
S2-5	U Nitrate, Liquid mixture, ...	KMP-E [...]	• Electromanometer (SMMS_PMc) • Temperature Sensor (SMMS_HIc)	Divert uranium during the uranium purification process		• SA_{251}: • SA_{252}:
S2-6	Pu Nitrate, Liquid mixture, ...	KMP-5 [...]	• Electromanometer (SMMS_PMb) • Temperature Sensor (SMMS_HIb) • Neutron Detector (SMMS_ NCb) • Nuclear Resonance Fluorescence (NRF_ GRS) • Pu(VI) Spectrophotometric Method (ASAS_ DAb)	Divert plutonium during the transfer between purification process and co-denitration process		• SA_{261}: • SA_{262}: • SA_{263}: • SA_{264}: • SA_{265}:

Diversion points at MBA2



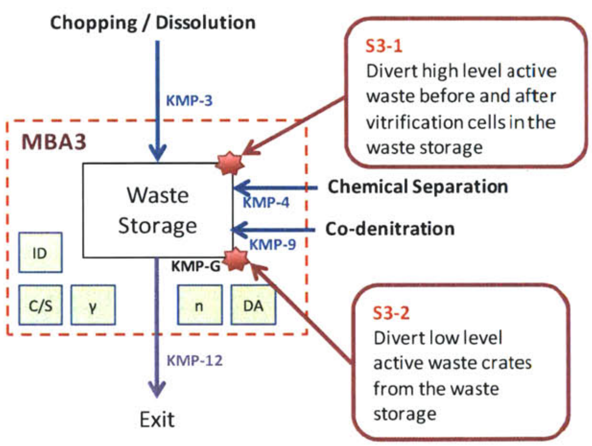
Safeguard Systems at MBA2



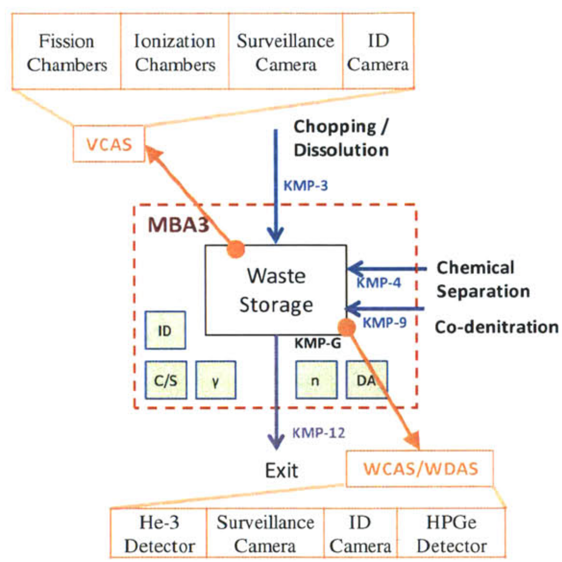
Nomenclature:

MBA 3: Safeguard systems: 2, # Safeguards: 8, Types of detectors: 6						
ID #	Material: envelope, form, composition	Key point	Safeguard Systems	Scenario Description	Material acquired range	Sample analyzed
S3-1	HLAW, Nitrate Solution of MA/FPs, solid structure or MA/FPs in amorphous form	KMP-G [...]	• Fission Chambers (VCAS – NC) • Ionization Chambers (VCAS – GRS) • Surveillance Camera (VCAS – OSa) • ID Camera (VCAS – IDa)	Divert high level active waste before and after vitrification cells in the waste storage	MA vetrified mix [xx-yy g] MA in solution [xx-yy g]	• SA_{311}: MA mix • SA_{312}: • SA_{313}: • SA_{314}: ID bottle image
S3-2	LLAW crates in solid form	KMP-G [...]	• He-3 Detector (WCAS – NC) • Surveillance Camera (WCAS – OSb) • ID Camera (WCAS – IDb) • HPGe Detector (WDAS – GRS)	Divert low level active waste crates from the waste storage		• SA_{321}: • SA_{322}: • SA_{323}: • SA_{324}:

Diversion points at MBA3



Safeguard Systems at MBA3

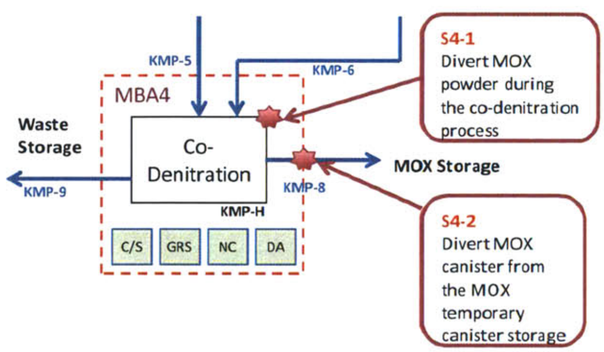


Nomenclature: HLAW: High Level Active Waste, LLAW: Low Level Active Waste

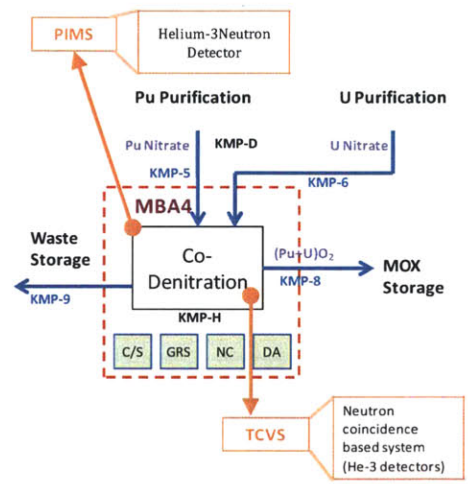
MBA 4: Safeguard systems: 2, # Safeguards: 2, Types of detectors: 1

ID #	Material: envelope, form, composition	Key point	Safeguard Systems	Scenario Description	Material acquired range	Sample Analyzed
S4-1	MOX powder	KMP-H [...]	• He-3 Neutron Detector (PIMS_ NCa)	Divert MOX powder during the co-denitration process		• SA_{411}:
S4-2	MOX Canister	KMP-8 [...]	• He-3 Neutron Detectors in coincidecnce (TCVS_ NCb)	Divert MOX canister from the MOX temporary canister storage		• SA_{421}:

Diversion points at MBA4



Safeguard Systems at MBA4

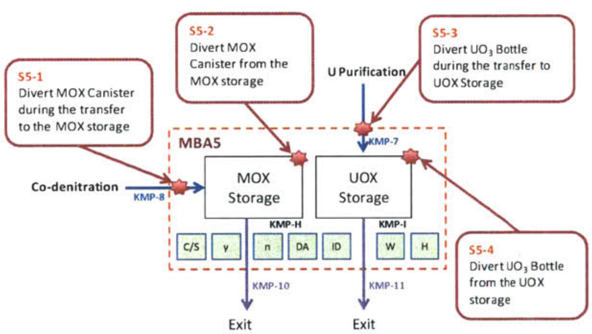


Nomenclature:

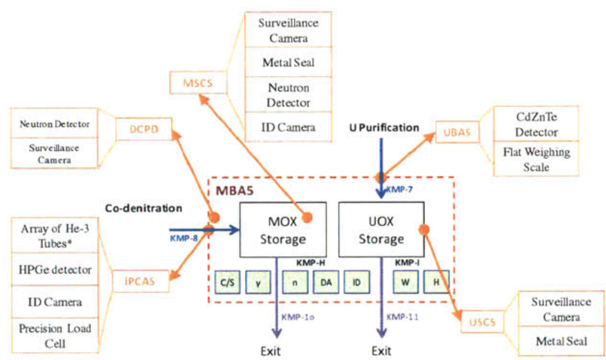
MBA 5: Safeguard systems: 5, # Safeguards: 14, Types of detectors: 10

ID #	Material: envelope, form, composition	Key point	Safeguard Systems	Scenario Description	Material acquired range	Sample analyzed
S5-1	MOX Canister	KMP-8 [...]	• Array of He-3 Tubes (iPCAS – NC) • HPGe Detector (iPCAS – GRS) • ID Camera (iPCAS – ID) • Precision Load Cells (iPCAS –WI) • Neutron Detector (DCPD –NC) • Surveillance Camera (DCPD – OS)	Divert MOX Canister during the transfer to the MOX storage		• SA_{511}: MOX item • SA_{512}: • SA_{513}: MOX item • SA_{514}: • SA_{515}: • SA_{516}:
S5-2	MOX Canister	KMP-H [...]	• Surveillance Camera (MSCS – OS) • Metal Seal (MSCS – SL) • Neutron Detector (MSCS – ND) • ID Camera (MSCS (ID)	Divert MOX Canister from the MOX storage		• SA_{521}: • SA_{522}: • SA_{523}: • SA_{524}:
S5-3	UO_3 Bottle	KMP-7 [...]	• CdZnTe Detector (UBVS – GRS) • Flat Weighing Scale (UBVS – WI)	Divert UO_3 Bottle during the transfer to UOX Storage		• SA_{531}: • SA_{532}:
S5-4	UO_3 Bottle	KMP-I [...]	• Surveillance Camera (USCS – OS) • Metal Seal (USCS – SL)	Divert UO_3 Bottle from the UOX storage		• SA_{541}: • SA_{542}:

Diversion points at MBA5

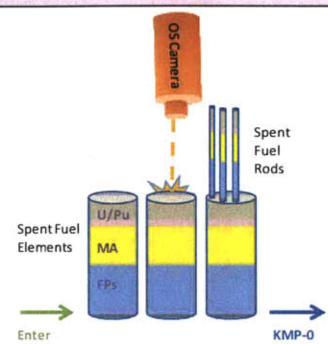
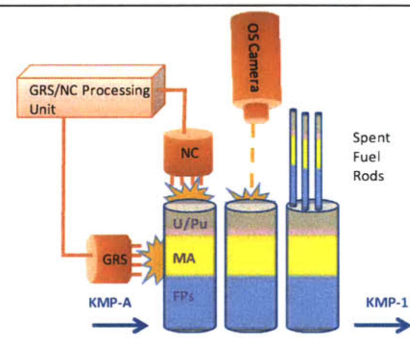
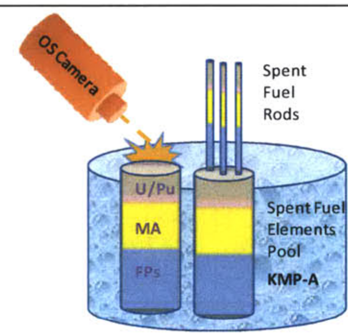
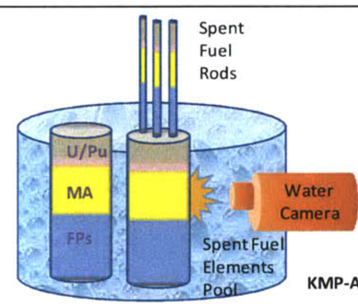
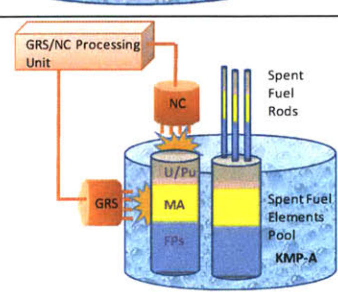


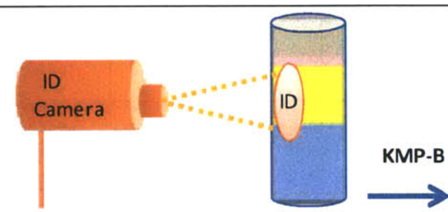
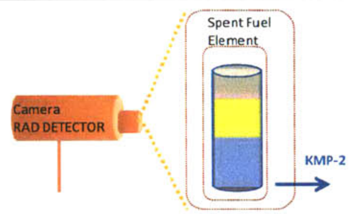
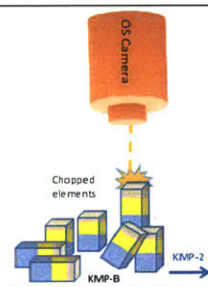
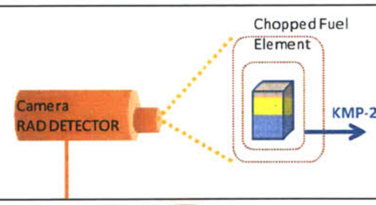
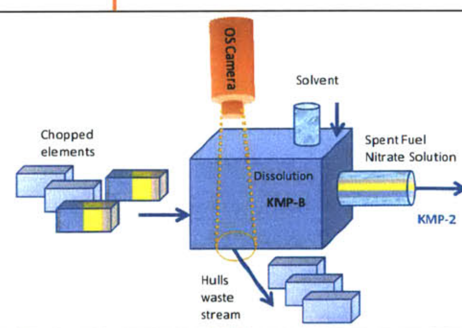
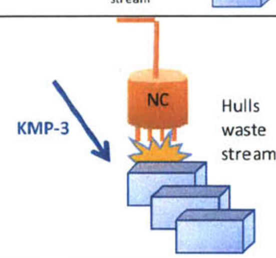
Safeguard Systems at MBA5

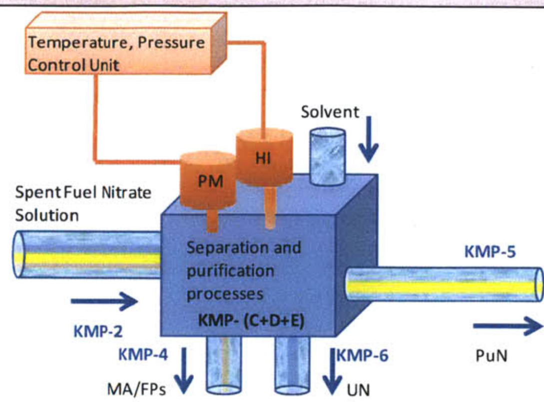
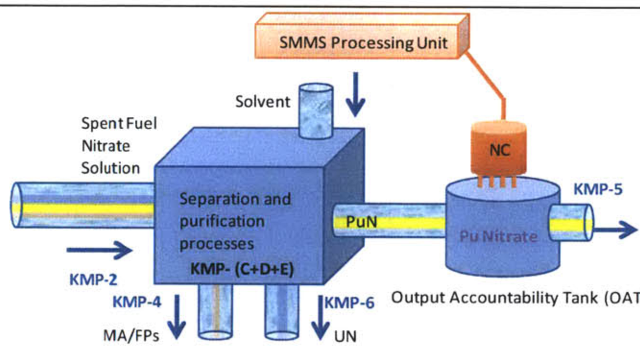
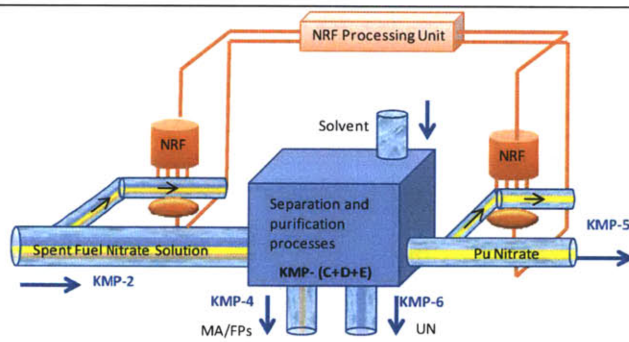
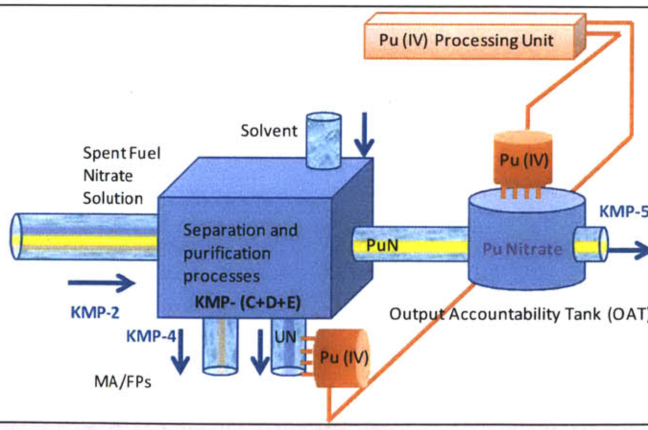


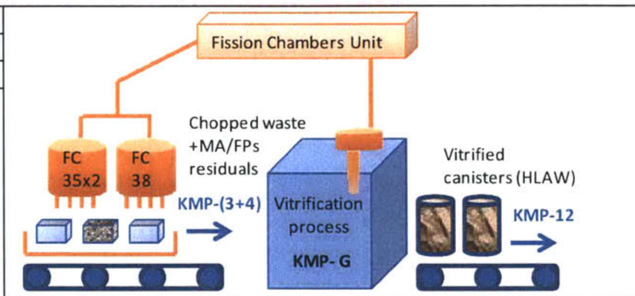
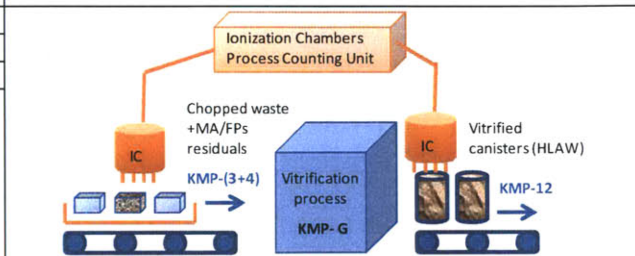
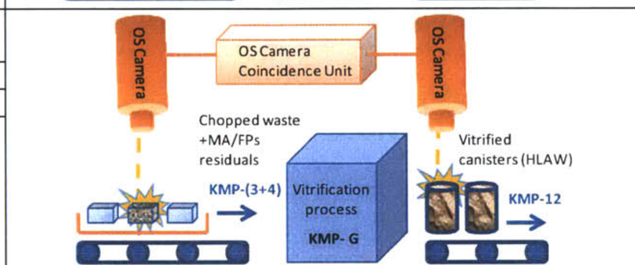
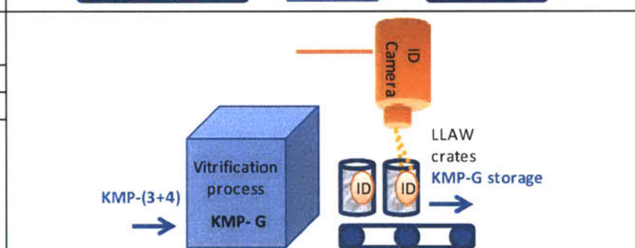
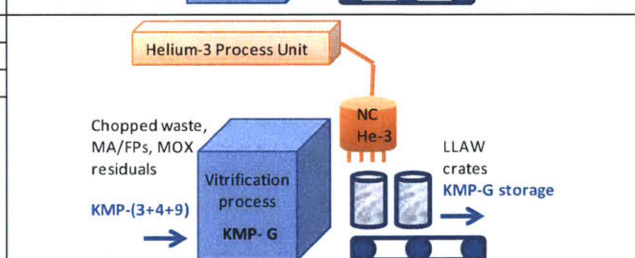
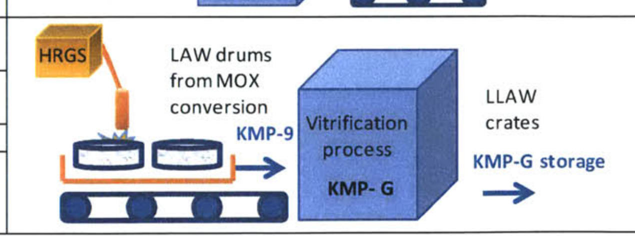
Nomenclature:

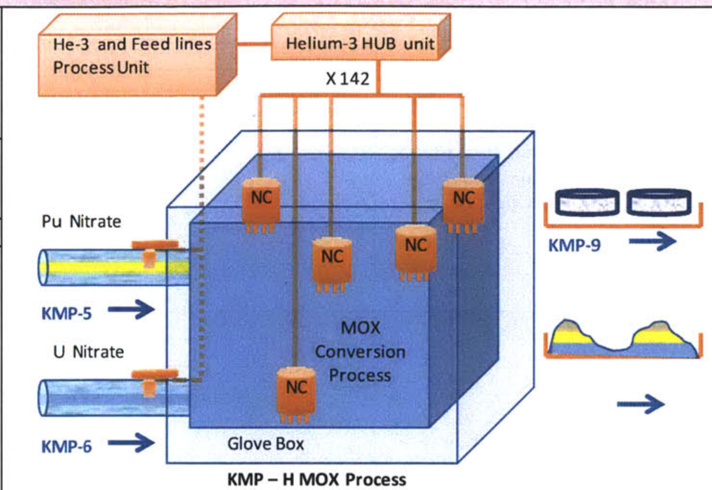
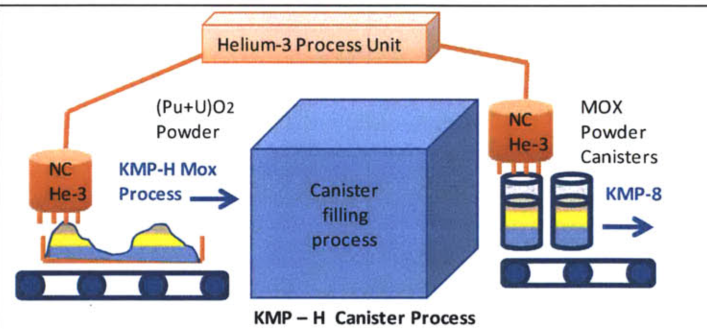
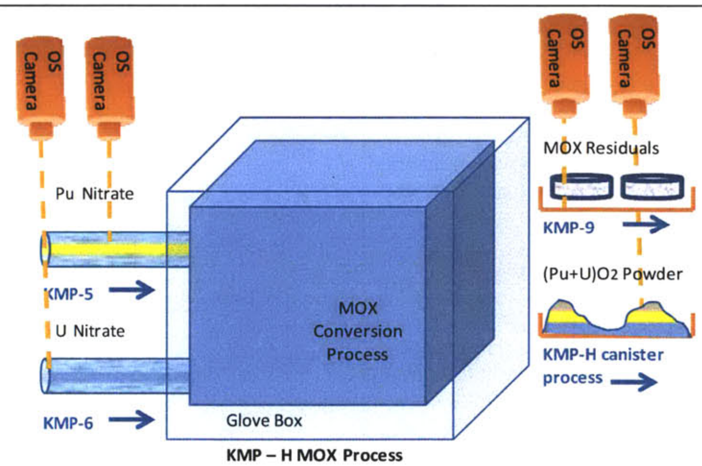
C.5 Safeguards and Samples Features at the Reprocessing Plant

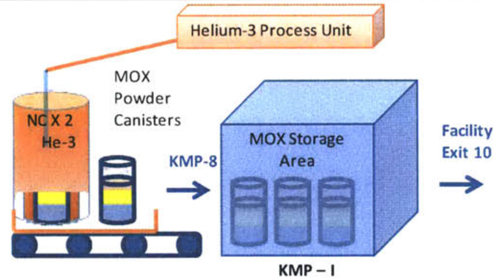
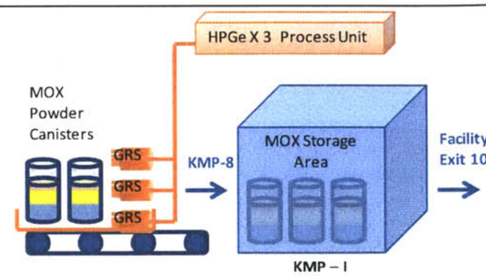
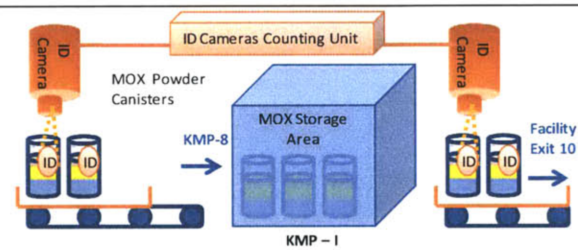
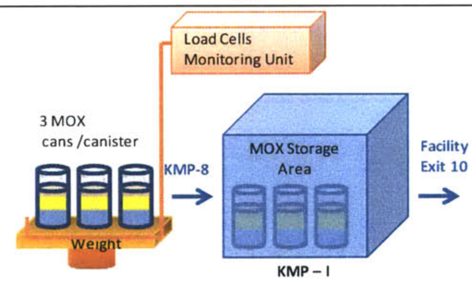
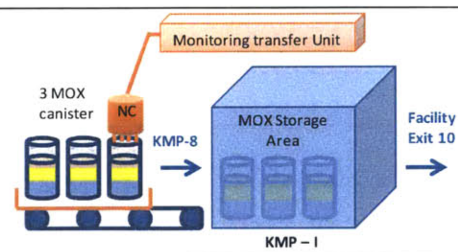
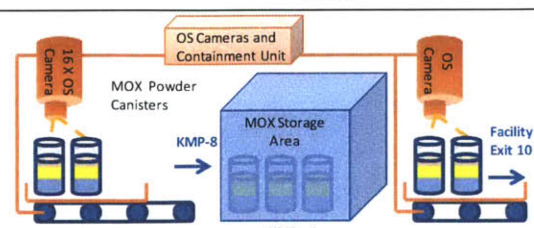
Sample ID and Function	Setup	Schematic Diagram
MBA 1		
SA_{111}: SFE/SFR items Surveillance Camera: ISVS_OSa Detecting SFE/SFR items before they enter the spent fuel pool	Resolution: high Time: real time Accuracy: no limitations if environment is lighted Sample phase: Spent fuel items in form of entire elements or rods	
SA_{112}: Pu neutrons in SFE/SFR Miniature Gamma & Neutron Detector: ISVS_GRS/NCa measuring the composition of the fuel elements coming into the facility	Geometry: SFE/SFR Time: any time (hours) Background: shielded by water but high radiation field Sample phase: Spent fuel items in forms of entire elements or rods	
SA_{121}: SFE/SFR items Surveillance Camera (ISVS_OSb) controlling the movements of fuel elements into the pool' s room	Resolution: high Time: real time Accuracy: limited by the visibility in the pool even if the environment is lighted Sample phase: Spent fuel items in form of entire elements or rods	
SA_{122}: SFE items Under Water Camera (ISVS_OSc) monitoring the movements of fuel elements in the pool	Resolution: high Time: real time Accuracy: no limitations if environment is lighted Sample phase: Spent fuel items in form of entire elements or rods	
SA_{123}: Pu radiation and neutrons in SFE/SFR	Geometry: SFE/SFR Time: any time (hours) Background: shielded by water but high radiation field Sample phase: Spent fuel items in forms of entire elements or rods	

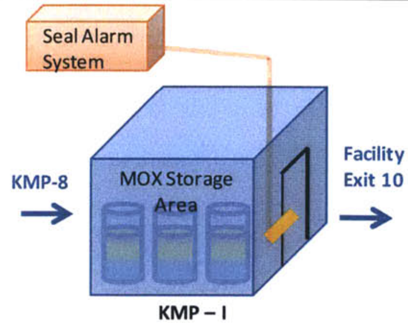
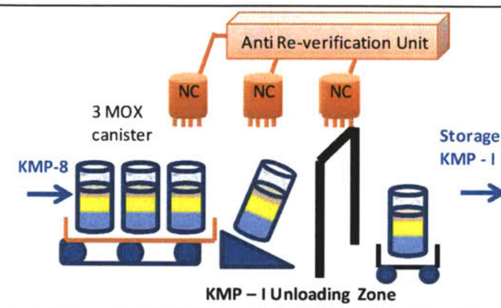
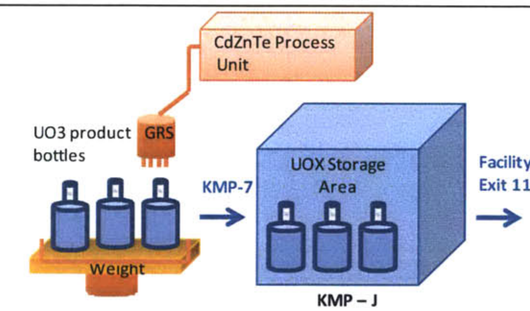
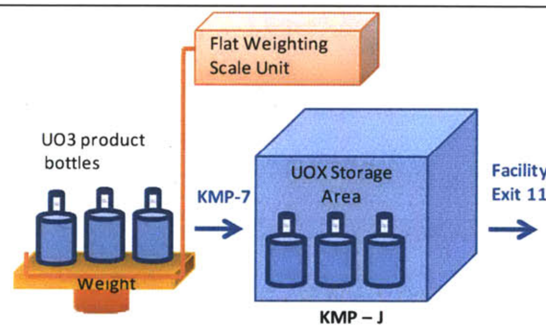
Sample ID and Function	Setup	Schematic Diagram
SA_{131}: SFE/SFR items	Same as SA_{111}	Same as SA_{111}
Surveillance Camera (IHVS_OSd)	Same as SA_{111} Same as SA_{111} Same as SA_{111}	
SA_{132}: SFE/SFR items	Resolution: high	
ID Camera (IHVS_ ID)	Time: real time Accuracy: no limitations if environment is lighted Sample phase: Spent fuel items in form of entire elements or rods	
SA_{133}: Pu radiation in SFE/SFR	Geometry: SFE/SFR	
Camera Radiation Detector (CRD) (IHVS_ GRS/NCc): monitoring the SFE in transit by detecting the neutrons emitted	Time: real time Background: high as due to the transit of others SFE Sample phase: SFE	
SA_{141}: CFE items	Resolution: high	
Surveillance Camera (IHVS_OSe)	Time: real time Accuracy: no limitations if environment is lighted Sample phase: CFE	
SA_{142}: Pu radiation in SFE/SFR	Geometry: CFE varying in size	
Camera Radiation Detector (CRD) (IHVS_GRS/NCd): monitoring the CFE in transit by detecting the neutrons emitted	Time: real time Background: high as due to the transit of others CFE Sample phase: CFE	
SA_{151}: CFE items	Resolution: high	
Surveillance Camera (IHVS_OSf): preventing CFE to be diverted in to the hulls line	Time: real time Accuracy: no limitations if environment is lighted Sample phase: Spent fuel items in form of entire elements or rods	
SA_{152}: Pu neutrons in CFE	Geometry: CFE varying in size	
Neutron Detector (RHMS_NC): determines the passive neutrons from curium in the hulls to approximate the material content using Cm/Pu/U ratio	Time: real time Background: high as due to the transit of others CFE Sample phase: CFE	

Sample ID and Function	Setup	Schematic Diagram
MBA 2		
SA_{211} and SA_{212}: liquid SFE **SA_{221} and SA_{222}: liquid SFE** **SA_{231} andSA_{232}: liquid MA/FSs** **SA_{241} and SA_{242}: liquid PuN** **SA_{251} and SA_{252}:liquid UN** **SA_{261} and SA_{262}: liquid PuN**	Geometry:	
Electromanometer ($SMMS\_PM_{i\text{-}th}$) and Temperature Sensor ($SMMS\_HI_{i\text{-}th}$): controlling the thermodynamic conditions/properties of the flows in pipes and processes	Time: real time Background: Sample phase:	
SA_{213}: liquid SFE **SA_{223}: liquid SFE** **SA_{233}: liquid MA/FSs** **SA_{243}: liquid PuN** **SA_{263}: liquid PuN**	Geometry:	
Neutron Detector ($SMMS\_NC_{i\text{-}th}$): in support of the PM and HI systems provides density and liquid level information about the processes	Time: real time Background: Sample phase:	
SA_{214}: liquid SFE **SA_{224}: liquid SFE** **SA_{234}: liquid MA/FSs** **SA_{244}: liquid PuN** **SA_{264}: liquid PuN**	Geometry:	
Nuclear Resonance Fluorescence (NRF_GRS): controlling the presence of Pu-239 and Pu-240 in the PuN mix	Time: real time Background: Sample phase:	
SA_{235}: liquid MA/FSs **SA_{245}: liquid PuN** **SA_{265}: liquid PuN**	Geometry:	
Pu(VI) Spectrophotometric Method ($ASAS\_ D_{i\text{-}th}$): monitoring the Pu abundance within the two main product streams	Time: real time Background: Sample phase:	

Sample ID and Function	Setup	Schematic Diagram
MBA 3		
SA_{311}: ^{244}Cm in the MA mix Fission Chambers (VCAS – NC): two U235 and a U238 fission chambers provide the position, U/Pu compositions and check that no aqueous solution is present	Geometry: Time: real time Background: Sample phase:	
SA_{312}: HLAW items Ionization Chambers (VCAS – GRS): used in conjunction with cameras to count objects in the pipeline	Geometry: Time: real time Background: Sample phase:	
SA_{313}: HLAW items **SA_{322}: LLAW items** Surveillance Camera (VCAS – $OS_{i\text{-}th}$): used to check that canisters are not resubmitted for measurement	Geometry: Time: real time Background: Sample phase:	
SA_{314}: ID bottle image **SA_{323}: ID LLAW crates** ID Camera (VCAS – $ID_{i\text{-}th}$): count the LLAWs crates before they go into storage (2 camera)	Accuracy: digital camera Time: real time Background: low Sample phase:	
SA_{321}: ^{244}Cm in the MA mix He-3 Detector (WCAS – NC):244Cm neutrons provide semi-quantitative info about the presence of U/Pu. This depends on info provided by the operator	Geometry: Time: real time Background: Sample phase:	
SA_{324}: Low Active Waste Drums from MOX with no FPs HPGe Detector (WDAS – GRS):	Geometry: portable Time: 15 minutes for 1 g of Pu detection limit Background: Sample phase: solid	

Sample ID and Function	Setup	Schematic Diagram
MBA 4		
SA_{411}:	Geometry: 142 detectors in the glove box (GB) to detect U and Pu distribution in the GB	
He-3 Neutron Detector (PIMS_ $NC_{i\text{-}th}$): the signal from each detector is compared with the isotopic composition from the feed solutions (possible threats) to obtain the Pu and U inventories*	Time: real time (30 hubs in a fiber optic loop) Background: Sample phase: powder	
SA_{421}:..		
He-3 Neutron Detectors in coincidence (TCVS_ $NC_{i\text{-}th}$) : provide inventory of the Pu in the MOX temporary canister storage and monitor flows in and out from this area**		
		

Sample ID and Function	Setup	Schematic Diagram
MBA 5 – A		
SA$_{511}$: MOX Canister Array of He-3 Tubes (iPCAS – NC)	Geometry: Time: real time Background: Sample phase:	
SA$_{512}$: MOX Canister HPGe Detector (iPCAS – GRS)	Geometry: Time: real time Background: Sample phase:	
SA$_{513}$: MOX Canister **SA$_{524}$: MOX Canister** ID Camera (iPCAS – ID)	Geometry: Time: real time Background: Sample phase:	
SA$_{514}$: MOX Canister Precision Load Cells (iPCAS – WI)	Geometry: Time: real time Background: Sample phase:	
SA$_{515}$: MOX Canister Neutron Detector (DCPD –NC)	Geometry: Time: real time Background: Sample phase:	
SA$_{516}$: MOX Canister **SA$_{521}$: MOX Canister** **SA$_{541}$: UO_3 Bottle** Surveillance Camera (DCPD – OS)	Geometry: Time: real time Background: Sample phase:	
Sample ID and Function	**Setup**	**Schematic Diagram**
MBA 5– B		

SA_{522}: MOX Canister **SA_{542}: UO_3 Bottle** Metal Seal (MSCS – SL)	Geometry: Time: real time Background: Sample phase:	
SA_{523}: MOX Canister Neutron Detector (MSCS – ND)	Geometry: Time: real time Background: Sample phase:	
SA_{531}: UO_3 Bottle CdZnTe Detector (UBVS – GRS)	Geometry: Time: real time Background: Sample phase:	
SA_{532}: UO_3 Bottle Flat Weighing Scale (UBVS – WI)	Geometry: Time: real time Background: Sample phase:	

C.6 3D View of the Material Balance Areas of the Reprocessing Facility

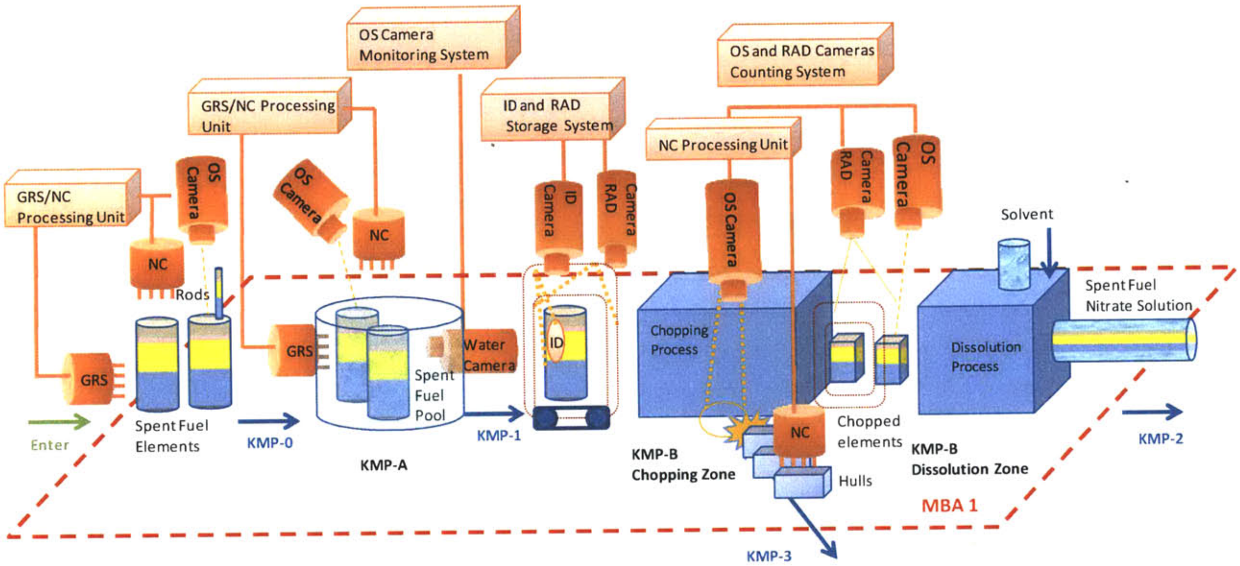


Figure 63. Safeguards and Processes within the Material Balance Area 1 – 3D Representation.

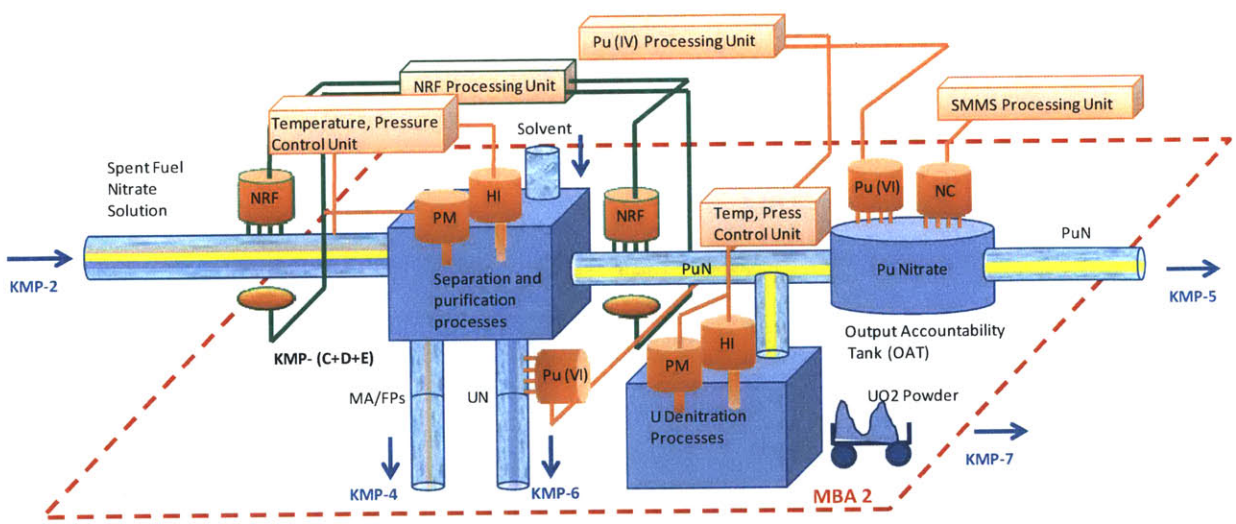


Figure 64. Safeguards and Processes within the Material Balance Area 2 – 3D Representation.

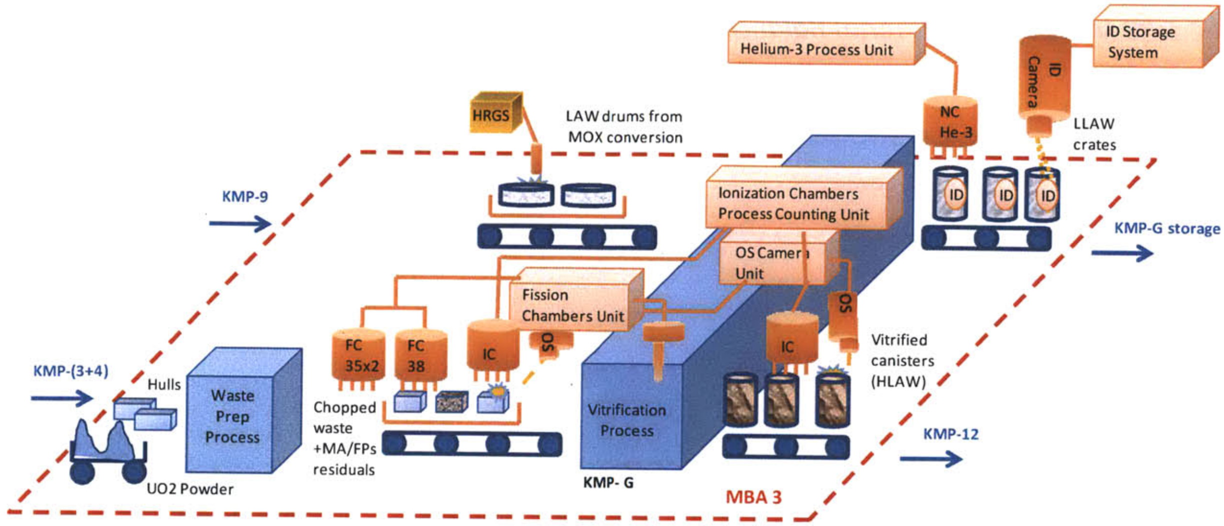


Figure 65. Safeguards and Processes within the Material Balance Area 3 – 3D Representation.

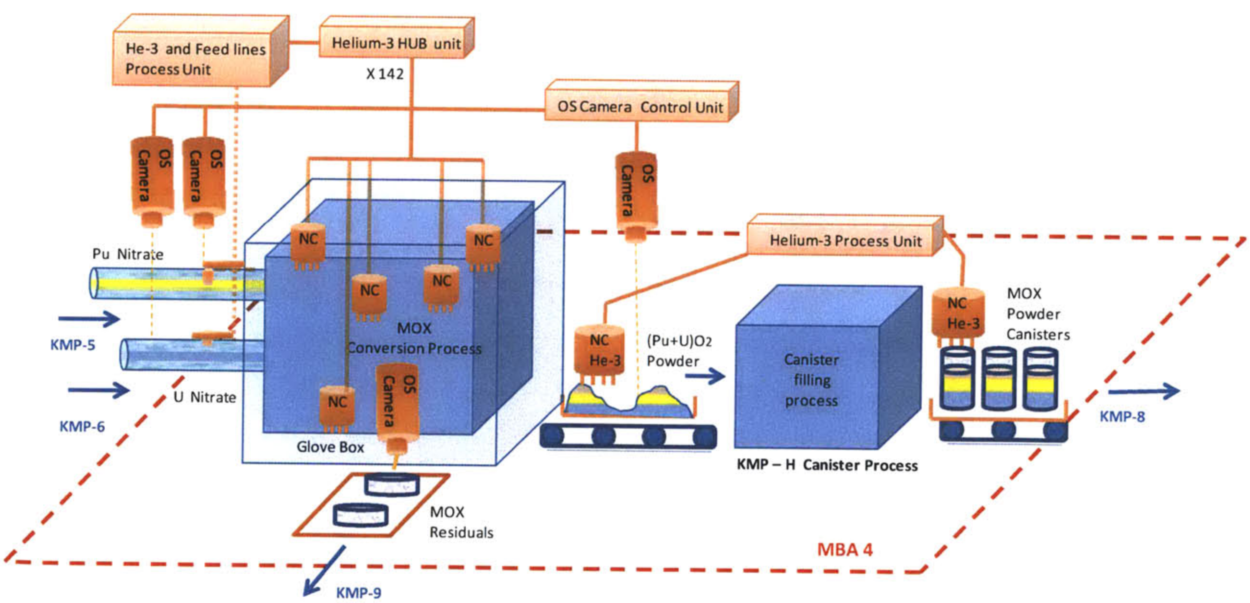


Figure 66. Safeguards and Processes within the Material Balance Area 4 – 3D Representation.

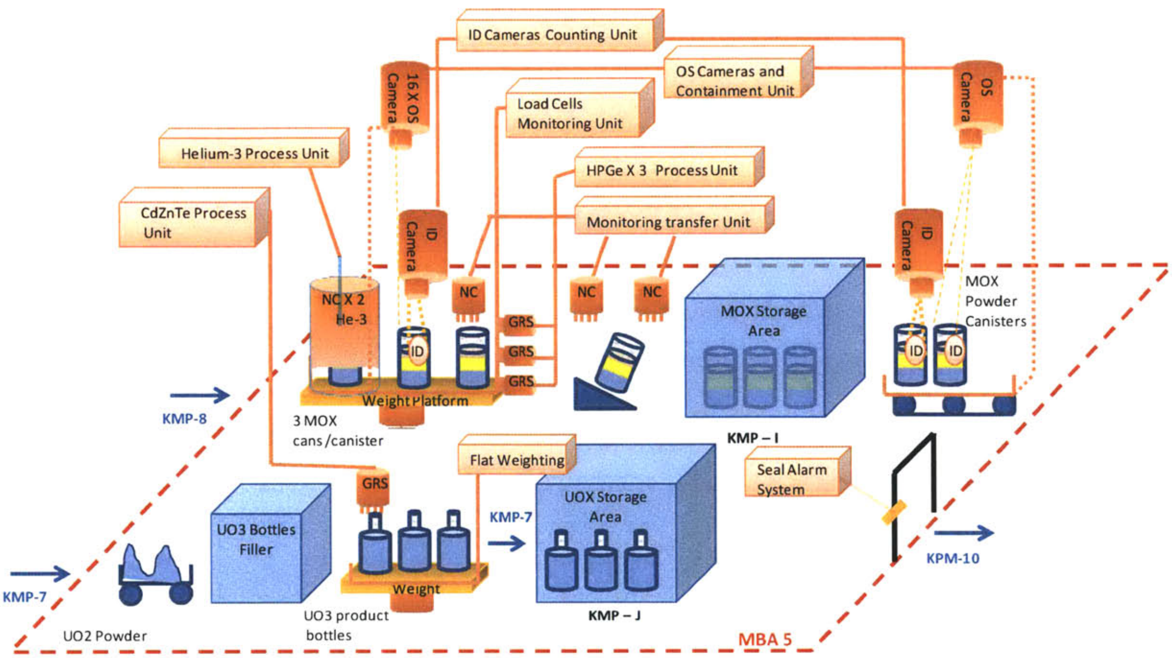


Figure 67. Safeguards and Processes within the Material Balance Area 5 – 3D Representation.

REFERENCES

[1] Michael H. Ehinger, Shirley J. Johnson: *"Lessons Learned in International Safeguards—Implementation of Safeguards at the Rokkasho Reprocessing Plant"*. Oak Ridge National Laboratory, ORNL/TM-2010/23 (December 2009).

[2] S. J. Johnson et al.,: *"Development of the safeguards approach for the Rokkasho Reprocessing Plant"*. IAEA-SM-367/8/01.

[3] Y. Yokota et al., : *"Integrated Monitoring and Reviewing Systems for The Rokkasho Spent Fuel Receipt and Storage Facility"*. Los Alamos National Laboratories, 1998 INMM Naples, FL USA, July 26-30, 1998. LA-UR-98-3004 (July, 1998).

[4] T. Iwamoto: *"Hold-up Measurement in a Reprocessing Facility"*. Japan Nuclear Fuel Limited (JNFL).

C.9 Success Trees and 3D Visualizations at MBA 1

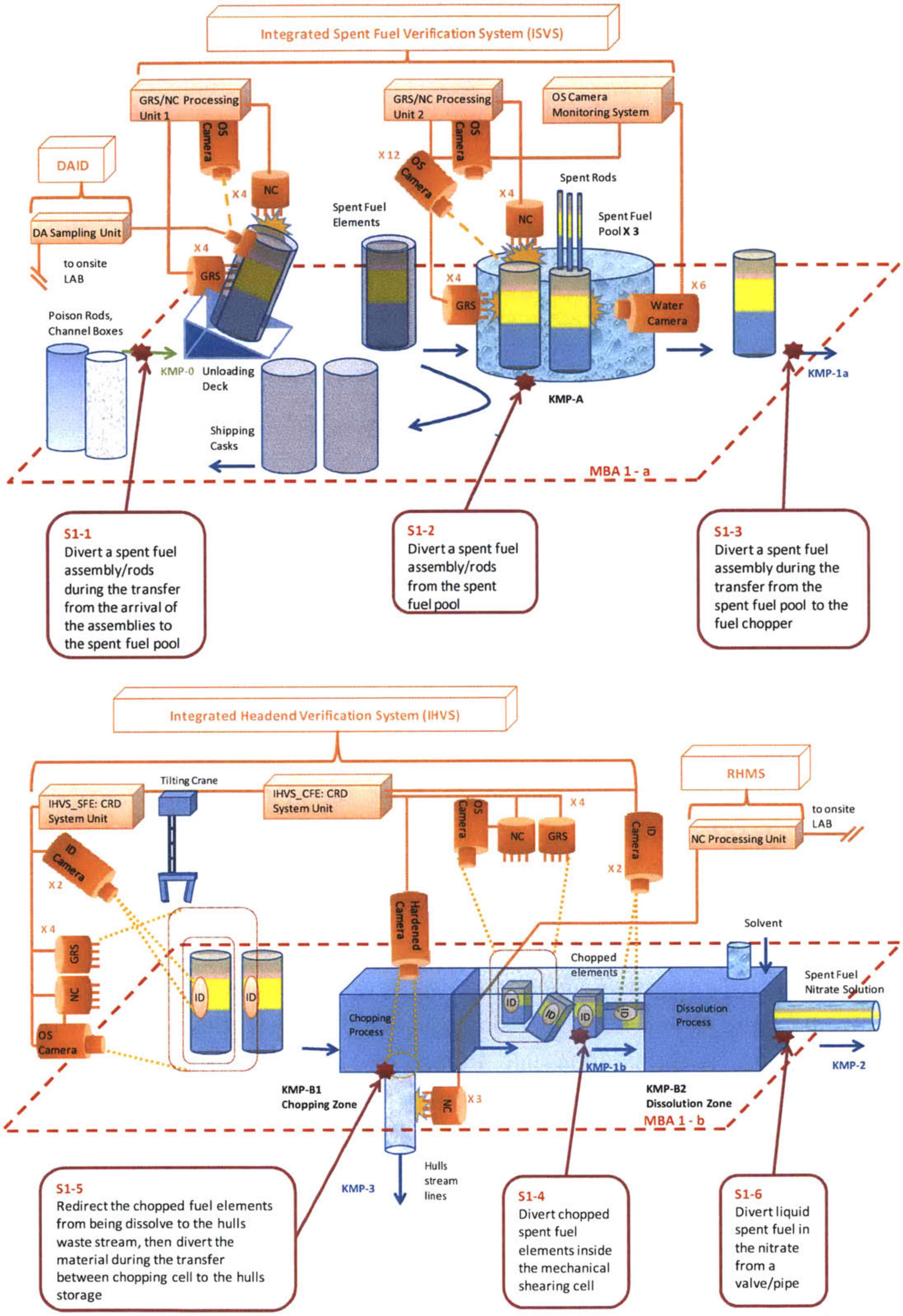


Figure 68. Diversion Scenarios and Safeguard Systems, and Operations at MBA 1 (3D View).

Figure 69, Figure 70, Figure 71, and Figure 72 show the success tree of the KMP at different sections of the first material balance area at an aqueous reprocessing facility.

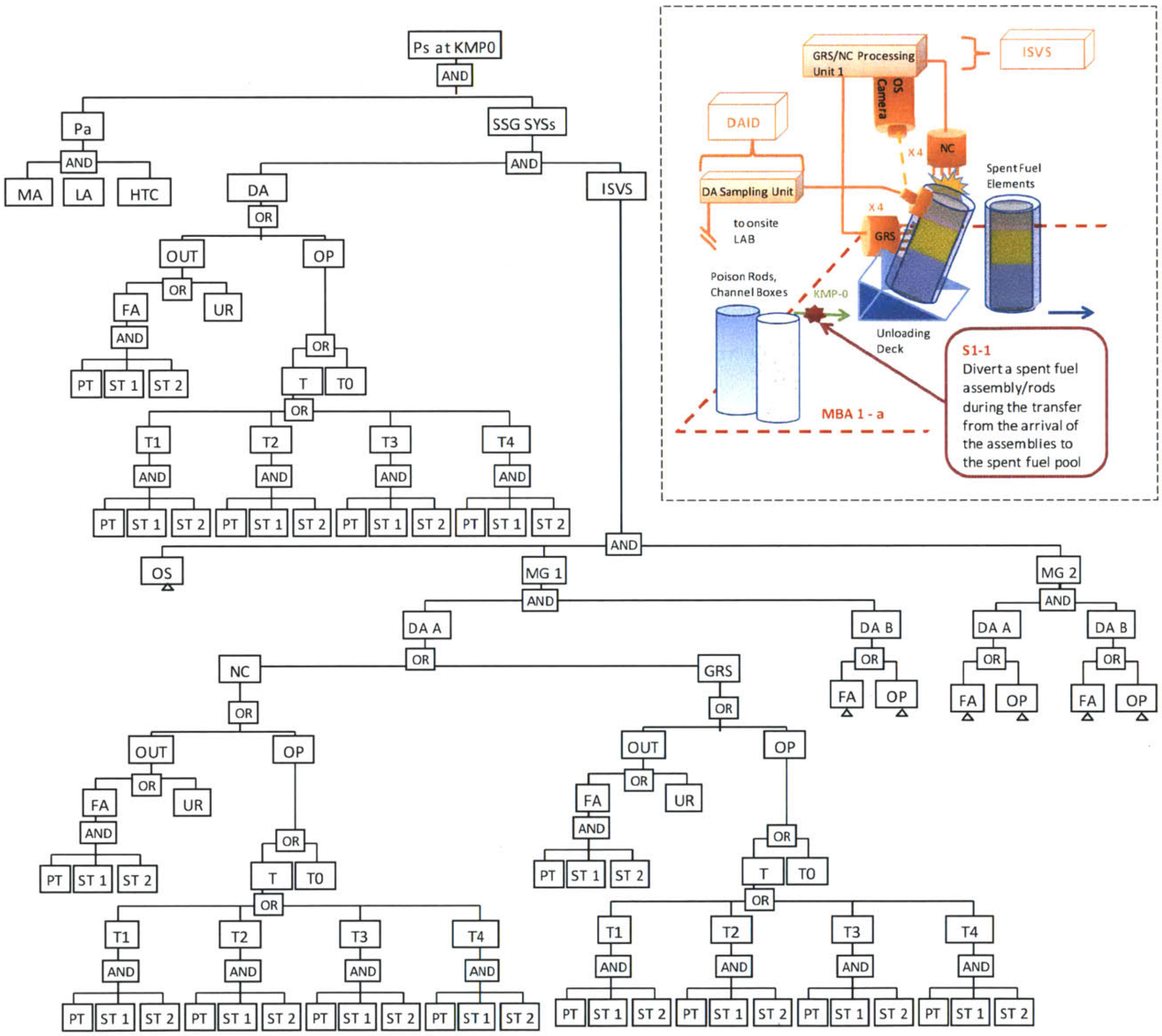


Figure 69. Diversion scenario and safeguards at the unloading deck area of MBA 1 - 3D View and Tree.

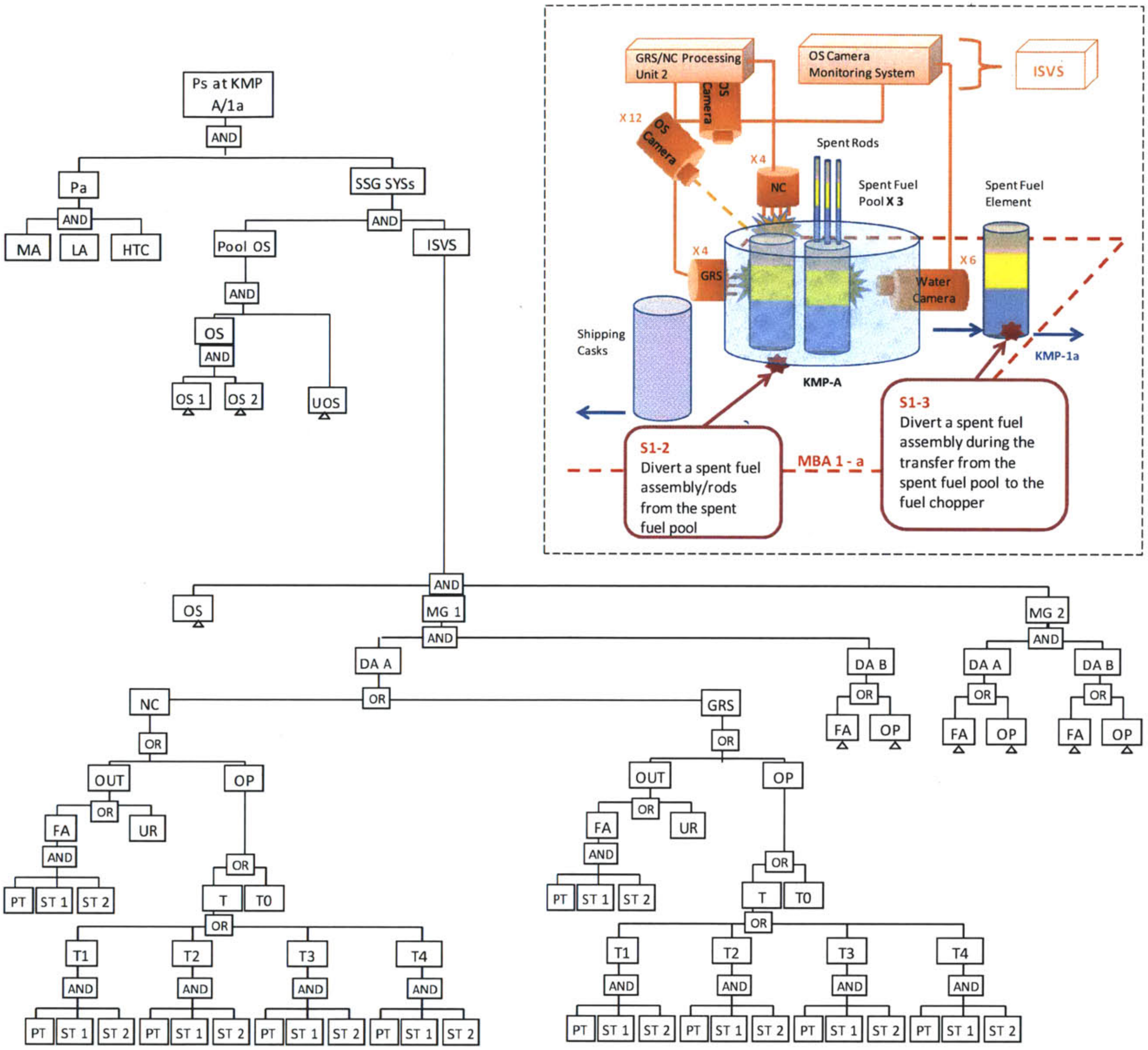


Figure 70. Diversion scenario and safeguards at the pool storage area of MBA 1 - 3D View and Tree.

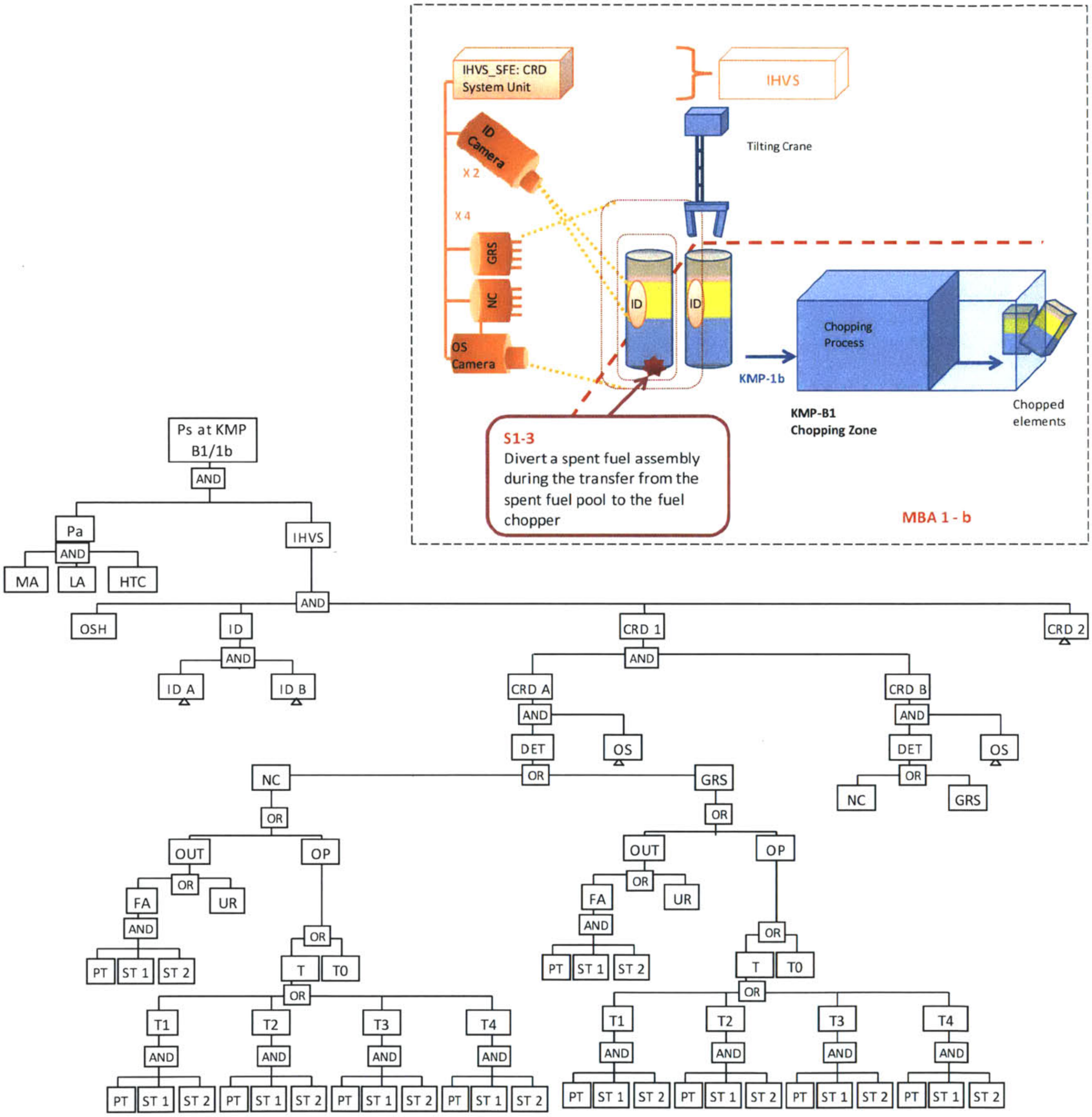


Figure 71. Diversion scenario and safeguards at the chopping area of MBA 1 - 3D View and Tree.

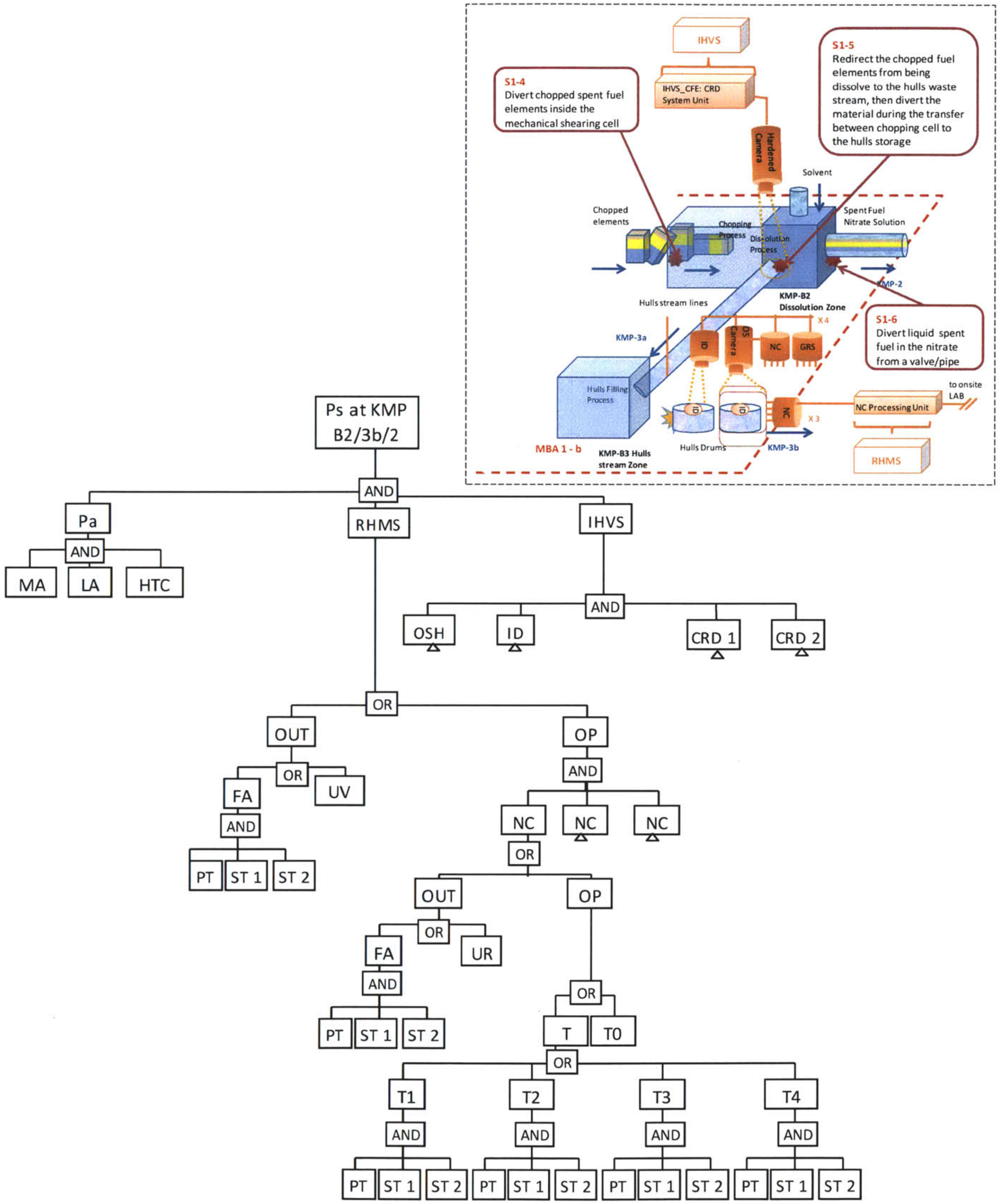
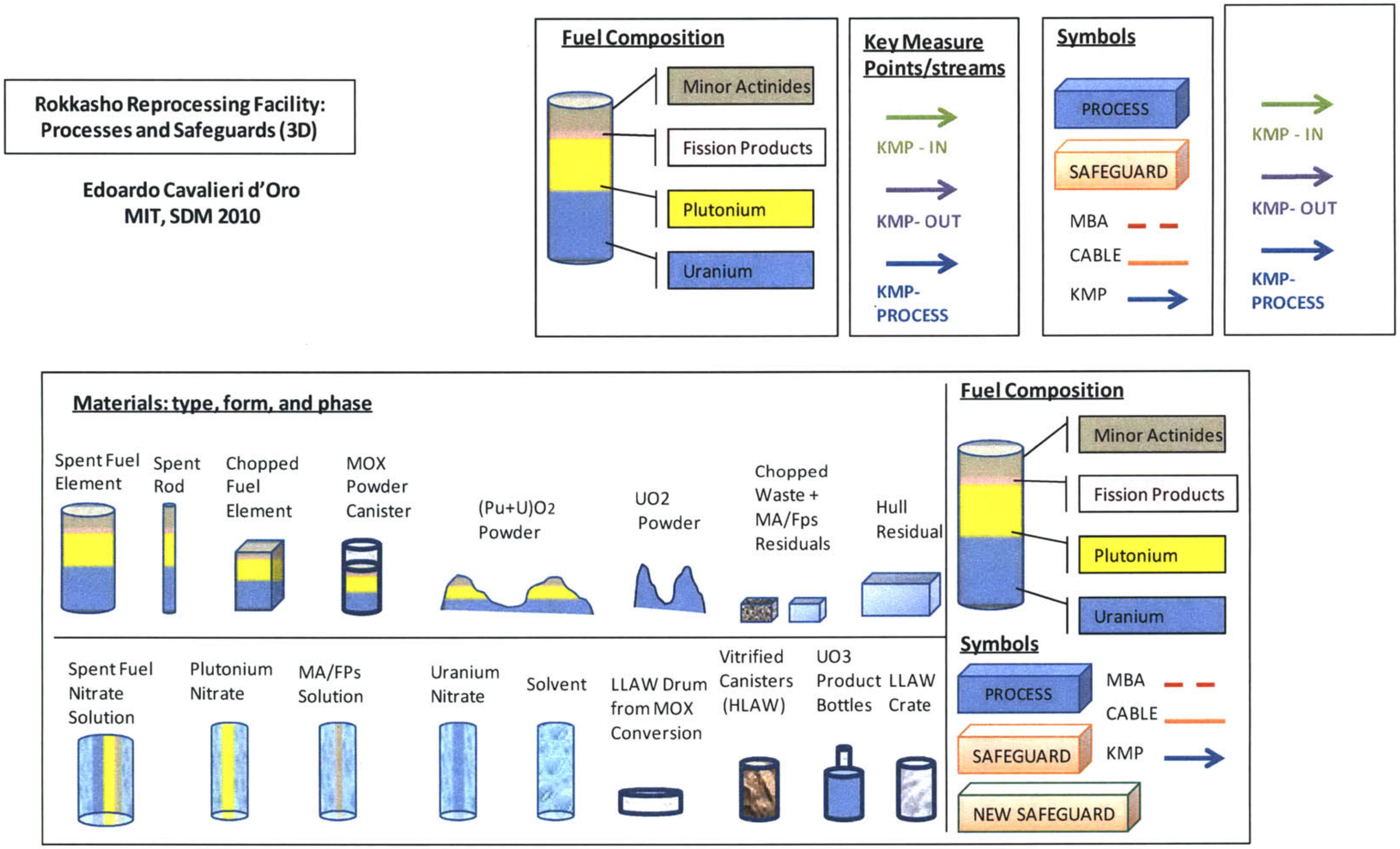


Figure 72. Diversion scenario and safeguards at the dissolution and hull drums filling areas of MBA 1 - 3D View and Tree.



KMP = Key Measurement Point
MBA = Material Balance Area

Figure 73. Agenda showing material types, forms, and phases and all the auxiliary symbols used to model the reprocessing plant.

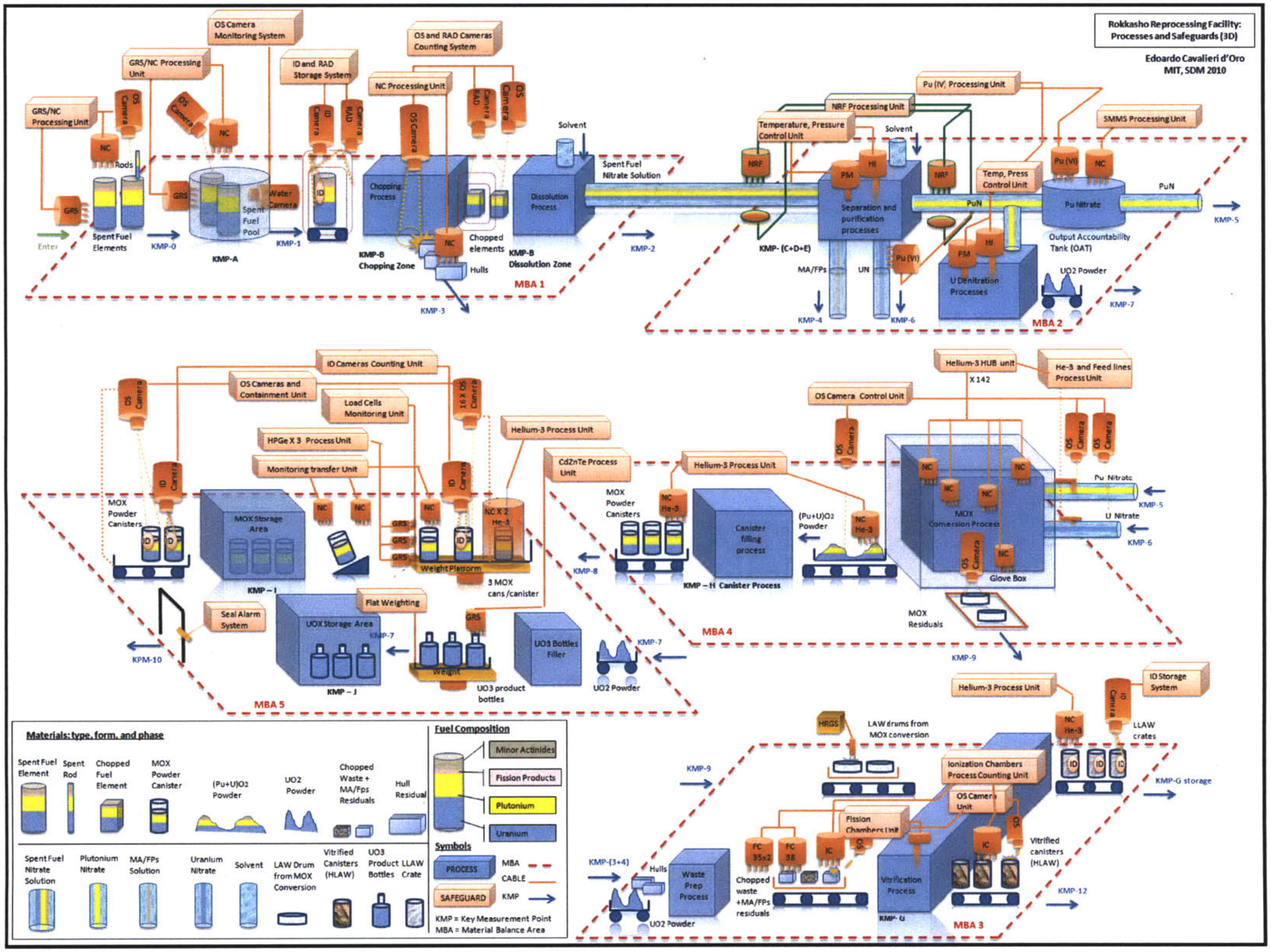


Figure 74. Rokkasho reprocessing plant 3d mapping showing systems' processes, material flows, and safeguards.