A Framework for Nuclear Facility Safeguard Evaluation Using Probabilistic Methods and Expert Elicitation

By

Chonlagarn Iamsumang

Sc.B., Engineering and Physics (2006)
Brown University

SUBMITTED TO THE DEPARTMENT OF NUCLEAR SCIENCE AND ENGINEERING IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE IN NUCLEAR SCIENCE AND ENGINEERING

AT THE
MASSACHUSETTS INSTITUTE OF TECHNOLOGY
SEPTEMBER 2010

Signature of Author ....
Chonlagarn Iamsumang
Department of Nuclear Science and Engineering
August 19, 2010

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

Certified by ....
Richard C. Lanza
Senior Research Scientist in Nuclear Science and Engineering
Thesis Reader

Accepted by ....
Mujid S. Kazimi
TEPCO Professor of Nuclear Engineering
Chair, Department Committee on Graduate Students

A Framework for Nuclear Facility Safeguard Evaluation Using Probabilistic Methods and Expert Elicitation

By
Chonlagarn Iamsumang

Submitted to the Department of Nuclear Science and Engineering
on August 19, 2010 in Partial Fulfillment of the Requirements for
the Degree of Master of Science in Nuclear Science and Engineering

ABSTRACT

With the advancement of the next generation of nuclear fuel cycle facilities, concerns of the effectiveness of nuclear facility safeguards have been increasing due to the inclusion of highly enriched material and reprocessing capability into fuel cycles. Therefore, an extensive and quantitative safeguard evaluation is required in order for the decision makers to have a consistent measure to verify safeguards level of protection, and to effectively improve the current safeguard scheme.

The framework presented in this study provides a systematic method for safeguard evaluation of any nuclear facility. Using scenario analysis approach, a diversion scenario consists of target material, target location, diversion technique, set of tactics to help elude the safeguards, and the amount of material diverted per attempt. The success tree methodology and expert elicitation is used to construct logical models and obtain the probabilities of basic events. Then proliferator diversion success probabilities can be derived from the model for all possible scenarios in a given facility.

Using Rokkasho reprocessing facility as an example, diversion pathways, uncertainty, sensitivity, and importance measure analyses are shown. Results from the analyses can be used by the safeguarder to gauge the level of protection provided by the current safeguard scheme, and to identify the weak points for improvements. The safeguarder is able to further analyze the effectiveness of the safeguard scheme for different facility designs, and the cost effectiveness analysis will help the safeguarder allocate limited resources for maximum possible protection against a material diversion.

Thesis supervisor: Dr. Michael W. Golay
Title: Professor of Nuclear Science and Engineering

Acknowledgements

I would like to thank professor Golay for his guidance and support throughout the development of this study. I am deeply grateful for his patience and understanding during numerous discussions to help me with the production of this thesis. I also would like to thank Dr. Lanza and Dr. Kohse for providing many valuable comments and feedbacks, especially Dr. Lanza for being the thesis reader.

I am very thankful for the helps I received from Edo during this whole process. Without the countless discussions on those long days in his office, this thesis might never get completed.

I would like to thank the department of nuclear science and engineering friends, faculties and staffs for the supports throughout the years here at MIT.

I also thank all my Thai friends at MIT and in Boston areas. They make my time here enjoyable and memorable.

Finally, I would like to thank my family, who always understand and cheer me up every time we talk, even though they are on the other side of the world.

Table of Contents

List of Figures

List of Tables

Abbreviations

BE	Basic Events
C/S	Containment and Surveillance
CoK	Continuity of Knowledge
DA	Destructive Analysis
DIV	Design Information Verification
ES	Environmental Sampling
GRS	Gamma Ray Spectrometry
HI	Heat Inspection
IAEA	International Atomic Energy Agency
IAT	Input Accountability Tank
ID	ID Tracking
IIV	Interim Inventory Verification
KMP	Key Measurement Point
MA	Material Accountancy
MBA	Material Balance Area
MOX	Mixed Oxide Fuel
MPS	Minimal Patch Set
MR	Movement Recording
MUF	Material Unaccounted For
NC	Neutron Counting
NDA	Non-Destructive Analysis
NRTA	Near-Real-Time Accountancy
OAT	Output Accountability Tank
OM	Operation Monitoring
OS	Optical Surveillance
OSL	On-site Laboratory
PIV	Physical Inventory Verification
PM	Process Monitoring
PR	Proliferator Resistance
PTM	Portal Monitoring
SI	Safeguard by the Inspector
SL	Seal
SNM	Special Nuclear Material
SQ	Significant Quantity
WI	Weight Inspection

Chapter 1 Introduction

1.1 Nuclear Facility Safeguards

By definition, the nuclear safeguard system comprises of an extensive set of measures by which the safeguarder verifies the correctness and completeness of the declaration made by States about their nuclear material and activities (IAEA 2001). States, in this case, are the non-nuclear weapon states that have signed the Non-Proliferation Treaty (NPT), which includes the agreement not to manufacture or acquire a nuclear weapon by any mean. To ensure that States honor the agreement, they must accept safeguards on all source of special fissionable material in all peaceful nuclear activities within their territories by the International Atomic Energy Agency (IAEA). The goal of the IAEA safeguards is to detect the diversion of nuclear materials from civilian to military purposes (IAEA 2002).

There are three types of verification measures used by the IAEA: nuclear material accountancy tracks all inward and outward transfers and flows of material in a nuclear facility; physical security is used to restrict access to nuclear material at the site of use; and containment and surveillance detects unreported movements or tampering with the nuclear materials. The safeguard scheme is designed to maintain the continuity of knowledge (CoK) of nuclear material at all time inside a nuclear facility.

Nuclear safeguards of civilian nuclear technology is highly significant, since civilian nuclear technology potentially contributes to nuclear weapon proliferation in the many ways, such as supplying technologies used for weapon-grade material production, training technical experts with knowledge that can be misused, justifying reasons for nuclear activities that can be for both civilian and weapon programs, and providing sources of acquisition of weapon usable material and equipments required for weapon construction (Bunn 2001).

From the start of the development of next generation nuclear fuel cycle facilities, which includes production of highly enriched fuel and spent fuel reprocessing, there have been growing concerns that current safeguard schemes used by the IAEA will not be sufficiently effective in preventing proliferation(Barnaby 2002). The problem arises because of bulk reprocessing facilities handle large amount of nuclear material, such that only a fraction of which is needed for construction of nuclear weapon. When the daily throughputs of the material in these facilities are higher than the signification quantity (SQ), which is the amount needed to construct a nuclear weapon, it is difficult for the IAEA to detect the diversion in a timely manner. Therefore, the effectiveness of the safeguards is essential, and a good safeguard evaluation is required in order to verify the level of protection that they provide, and to effectively improve the current safeguard scheme.

1.2 Nuclear Safeguard Evaluation

As mentioned in the previous section, safeguard evaluation is a significant tool for verification and identification for improvements of a safeguard scheme. The evaluation is often a part of nonproliferation assessments because there are many factors that could be involved in nuclear proliferation. To reduce the complexity of the assessment, the problem must be decomposed into manageable elements. Therefore, a typical analysis includes definition of a finite set of threats, definition of barriers to proliferation, development of metrics, and segmentation of the system being evaluated (NNSA 2003).

There are two common approaches for nonproliferation assessments. The first one is the "attribute analysis". In this approach, the attributes of the system under evaluation are identified, then the effects that these attributes have on the potential of proliferation are estimated. Typically, these studies are qualitative and highly subjective. There are formal methods, such as the Multi-Attribute Utility (MAU) model, that helps assisting in decision making from the results of these studies.

The second approach is the "scenario analysis". The studies that use this approach usually investigate the possible proliferator diversion scenarios and the processes undertaken to overcome the barriers that prevent or detect the diversions. Results are the estimates of the probabilities that the proliferator will succeed with those scenarios or pathways. Typically, these studies use logical model and probability analysis to produce quantitative results. However, the accuracies of the results rely heavily on the accuracies of the expert judgments of the probabilities.

In either case, the goal of safeguard evaluation is to be able to qualitatively or quantitatively compare the effectiveness of the safeguard scheme to detect material diversion attempted by a proliferator for different nuclear facilities, safeguard setups, or diversion scenarios. The results of the evaluation will further be useful for the safeguarder to indentify where and how to improve the current safeguard systems.

1.3 Previous and Current Works

This section provides a summary of the previous and current works in the area of safeguard evaluation and proliferation resistance (PR).

The multi-attribute utility approach has been the most widely used among PR studies. In 2000, a key study on PR assessment (Taylor 2000) was comprehensively performed by the task force on Technological Opportunities to increase the Proliferation Resistance of Global Civilian Nuclear Power Systems (TOPS). They identified the principal barriers and attributes, based upon the measures determined in the earlier studies (National Science of Academy 1994) of the system against proliferation threats, and evaluated these attributes qualitatively.

Other studies use some other means to assess the safeguards, e.g. using a network model called "The Safeguards Network Analysis Procedure (SNAP)," which combines knowledge of the system, specific scenarios, and modeling objectives (Floyd H. Grant 1978); evaluating the diversion sensitivity of the nuclear material by decision analysis techniques (Shipley 1978); assessing proliferation risk by using weighted function of criteria for proliferation path ways (Silvennoinen 1982).

There are previous works that have utilized success tree model as a tool to obtain the measure of proliferation success probability, which is used as a mean for comparison between alternative fuel cycle concepts (Golay In preparation) (Sentell Jr. 2002). They characterized the features of a facility/fuel cycle that contributed to proliferation into material attractiveness, critical mass production rate, probability of nominal yield, relative cost ratio, resources devoted, material shielding/transport difficulty, and success probability of defeating the barriers. Subsequent work further investigates the method by introducing the concept of competition between the proliferator and the safeguarder into the proliferation assessment of a Modular Pebble Bed Reactor (MPBR) (Ham 2005). This study demonstrates the use of expert elicitation to derive the basic event probabilities as a function of proliferator level of effort for different material diversion pathways. Currently, there is an on-going work to extend and apply the previous developed methods to assess PR of the Sodium Fast Reactor Energy System by using risk-informed and performance-based regulatory framework (E. Cavalieri d'Oro 2009).

The framework introduced in this study is designed to improve and demonstrate the applications of the methodology used in previous works, focusing on the area of safeguard scheme evaluation and analyses for all possible proliferator diversion scenarios, which include tactics to elude safeguards and the amount of material diverted per attempt. The competition between the proliferator and the safeguarder is clearly distinguished into the proliferator's selection of diversion scenario that gives the highest diversion probability, and the safeguarder's facility design choices and resources devoted to safeguards that increase the effectiveness of the safeguard scheme.

1.4 Scope and Approach of this Framework

The objective of this study is to create a framework for an evaluation of a safeguard scheme in a nuclear facility. This includes the assessment of proliferator material diversion success probabilities, which are used to measure the effectiveness of the safeguards, for all of the possible diversion scenarios. These probabilities are computed by utilizing a success tree model, and the probabilities of the basic events are derived by the mean of expert elicitation.

The most important feature of the safeguard evaluation in this framework is the inclusion of scenarios where the proliferator attempts to use concealment tactics to help elude the safeguards. To accommodate this feature, the safeguards in this framework are separated into two types. The first type is the primary safeguard, which is used to detect a material diversion, and the second type is the supporting safeguard, which is used to detect any tactic that the proliferator might attempt to help elude the primary safeguard. The analyses then can be carried out for all possible set of tactics to find the set that gives the highest proliferator diversion success probability and identify which tactic provides the most contribution to the success probability.

The expert elicitation is also designed to derive probabilities of basic events as a function of the costs of the safeguards. This allows the safeguarder to evaluate the cost effectiveness of the safeguard scheme and better allocates the limited resources. In addition, the analyses of the same safeguard scheme for different facility designs can be done to compare which design choice gives higher safeguard effectiveness.

The evaluation demonstrated in this study is only for the effectiveness of the safeguards in detecting a material diversion, assuming that the proliferator decides to make an attempt. It does not include the probability that the proliferator will make an attempt. To evaluate the risk of having a successful material diversion by a proliferator, the results from this framework must be combined with the estimation of material attractiveness, which is the measure of the difficulty to transport and use the material for construction of nuclear weapons. It is expected that the safeguarder will devote more resources to the safeguard scheme of more attractive materials, thus the safeguards for these materials are more effective than the ones for less attractive materials.

The methodology of the framework is designed to be systematic to provide uniform procedures and analyses. Therefore, it can be easily applied for an evaluation of any safeguard system in any nuclear facility. It is also modular in terms of distinguishing a safeguard system in to various categories, thus the results from expert elicitation does not depend on any particular safeguard system or diversion scenario. Therefore, the results can be used in the analysis of another similar system without having to redo the expert elicitation.

The ultimate goal of this framework is to provide methodology of using probabilistic methods to evaluate the effectiveness of safeguard schemes and identify the strengths and weaknesses of the systems from material diversions and proliferator tactics, including analysis for the best way to improve the system. Note that the framework does not aim to derive an accurate diversion success probability for certain scenarios, but rather to use the probabilities to compare the effectiveness of the safeguards for different proliferator scenarios and safeguard setups.

1.5 Structure of the Document

Chapter 2 gives the description of the success tree methodology for a quantitative evaluation of a safeguard scheme. The details of each of the safeguard type and their sub-trees are shown. The tactics to elude the safeguards are also identified along with the supporting safeguards that are setup by the safeguarder to detect the tactics. Then the last section of the chapter shows how the safeguards are laid out in a nuclear facility. For material accountancy, a facility is separated in to material balance areas (MBAs), and the processes and material transferring between the MBAs are identified as key measurement points (KMPs), which are the places where a material diversion can occurs.

Chapter 3 provides the methods and the protocols for an expert elicitation to obtain the expert judgments of the probabilities of the basic events in the success tree model. The advantages and disadvantages of the organization of the elicitation are discussed in details. It also carried out the processes of converting the expert inputs to the desired probabilities of the basic events, and discusses the readiness of the results for various types of application and analyses.

Chapter 4 starts out showing the details of the Rokkasho reprocessing facility in order to use it as an example to explain the procedures to evaluate the safeguard scheme of a nuclear facility. The actual safeguard systems in the facilities are shown and categorized into different types of safeguards, which are discussed in Chapter 2. The locations and the functionalities of these safeguards are the important factors for the identification of safeguard systems to detect the possible scenarios. After the diversions scenarios have been indentified, the success tree model can be constructed based upon the definitions and description described in the previous chapters. Then the following sections show the analyses that can be done to evaluate the safeguard scheme, including diversion pathway analysis, uncertainty analysis, sensitivity analysis, and importance measure analysis. These analyses provide the methods to measure the effectiveness of the safeguards both as a system and as an individual safeguard. By going through the calculation of diversion success probability for every possible set of proliferator tactics, the ranking of the sets of tactics will indicate the strength and weak points of the safeguard scheme.

Chapter 5 extends the analysis of the results from expert elicitation to evaluate the available safeguards for different designs of a facility and the cost effectiveness of the resource devoted to the safeguards by the safeguarder. In contrast to the discussion in Chapter 4, where the analysis focuses on the scenario and tactics by the proliferator, this chapter presents the options for the safeguarder to improve the effectiveness of the safeguards. The limitation in this case is then the technical practicability of the designs and the safeguarder's available resources.

Chapter 6 summarizes the methodology of the entire framework and points out the factors that affect the effectiveness of the success tree model and the expert elicitation. Possible improvements of the safeguard evaluation processes are suggested and additional future works are discussed.

Chapter 2 Success Tree Model

2.1 Success Tree Methodology

The success tree methodology is introduced here as a tool to evaluate the safeguards by considering the probability that a proliferator will succeed in acquiring special nuclear material (SNM) and pathways for diversion scenarios. The success tree logic diagram has the same structure as the Fault Tree Analysis (FTA) used in safety analyses, such as Probabilistic Risk Assessment (PRA). However, in contrast of the top event being the failure of the system, the top event in a success tree analysis is a success. Therefore, in order for the top event to be successful, every event in the level below must also be successful.

In this case, for evaluation of a safeguard scheme, the top event of the success tree diagram is the event where a proliferator successfully diverts SNM according to the specific scenario. There are many possible diversion scenarios that the proliferator can use to divert material, depending on the design or the facility. For each scenario, the proliferator diversion attempts will succeed only when all of the safeguards that are designed to detect that specific attempt are eluded.

List of the types of safeguards

1. Material Accountancy (MA)
    - 1.1. Destructive Analysis (DA)
    - 1.2. Non-destructive Analysis (NDA)
        - 1.2.1. Gamma Ray Spectrometry (GRS)
        - 1.2.2. Neutron Counter (NC)
        - 1.2.3. Heat Inspection (HI)
        - 1.2.4. Weight Inspection (WI)
2. Containment and Surveillance (C/S)
    - 2.1. Optical Surveillance (OS)
    - 2.2. Seal (SL)
3. Operation Monitoring (OM)
    - 3.1. ID Tracking (ID)
    - 3.2. Movement Recording (MR)
    - 3.3. Process Monitoring (PM)
    - 3.4. Safeguard by the Inspector (SI)
4. Environmental Sampling (ES)
5. Portal Monitoring (PTM)

The schematic of the success tree diagram is shown in Figure 2-1. The figure shows the example of the tree for the case that every safeguard types is in place to detect the diversion. In the actual analysis, there will only be the safeguards that would detect the diversion under specific scenario. The box that is labeled "PROLIFERATOR ATTEMPTS TO DIVERT SNM" is the initiating event for the top event to occur. For the analysis concerning how likely that the top event will happen, the probability that the proliferator will attempt a diversion can be derived from the attractiveness of the material inside the facility as discussed in Chapter 1. It is expected that for the material that has high chance of being diverted by a proliferator, the probability to successfully elude all of the safeguards in place should be low.

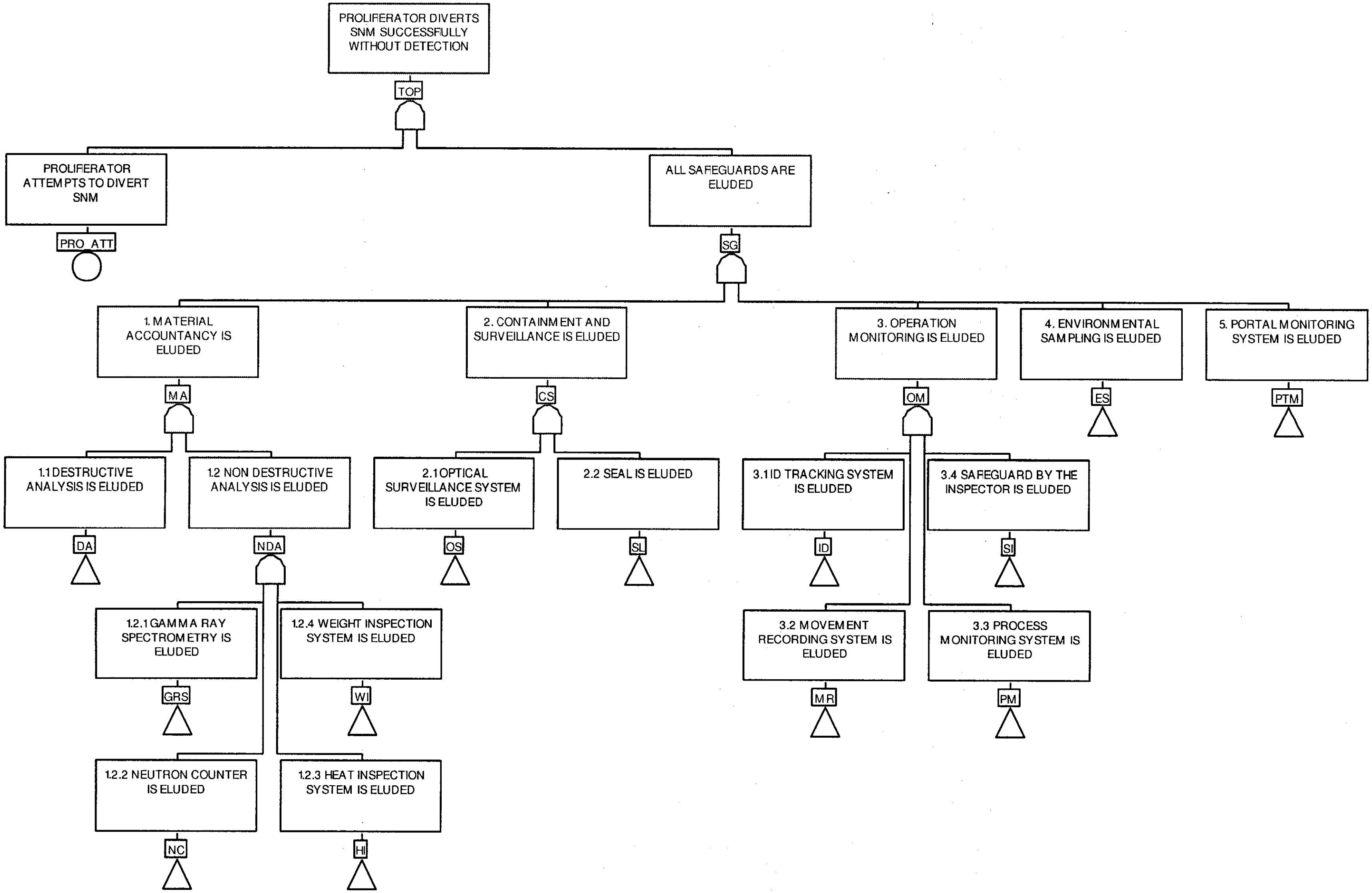

PROLIFERATOR DIVERTS SNM SUCCESSFULLY WITHOUT DETECTION
TOP
PROLIFERATOR ATTEMPTS TO DIVERT SNM
PRO_ATT
ALL SAFEGUARDS ARE ELUDED
SG
1. MATERIAL ACCOUNTANCY IS ELUDED
MA
2. CONTAINMENT AND SURVEILLANCE IS ELUDED
CS
3. OPERATION MONITORING IS ELUDED
OM
4. ENVIRONMENTAL SAMPLING IS ELUDED
ES
5. PORTAL MONITORING SYSTEM IS ELUDED
PTM
1.1 DESTRUCTIVE ANALYSIS IS ELUDED
DA
1.2 NON DESTRUCTIVE ANALYSIS IS ELUDED
NDA
2.1 OPTICAL SURVEILLANCE SYSTEM IS ELUDED
OS
2.2 SEAL IS ELUDED
SL
3.1 ID TRACKING SYSTEM IS ELUDED
ID
3.4 SAFEGUARD BY THE INSPECTOR IS ELUDED
SI
1.2.1 GAMMA RAY SPECTROMETRY IS ELUDED
GRS
1.2.4 WEIGHT INSPECTION SYSTEM IS ELUDED
WI
3.2 MOVEMENT RECORDING SYSTEM IS ELUDED
MR
3.3 PROCESS MONITORING SYSTEM IS ELUDED
PM
1.2.2 NEUTRON COUNTER IS ELUDED
NC
1.2.3 HEAT INSPECTION SYSTEM IS ELUDED
HI

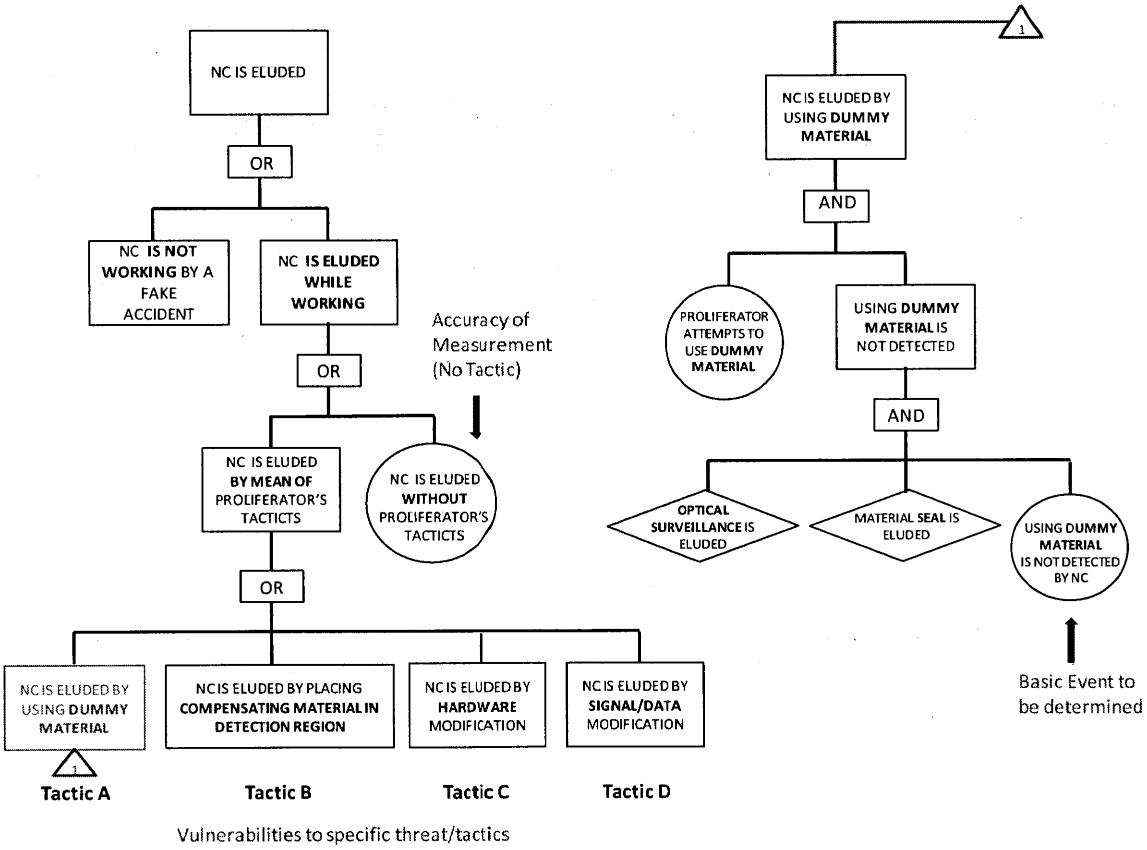
Figure 2-1 Success tree diagram showing the possible types of safeguard that the proliferator must elude in order to divert the material successfully

2.2 Nuclear Safeguard Success Tree Sub-Model

For a safeguard to be eluded, there are two types of diversion attempts that a proliferator can make.

1. The proliferator attempts to elude the safeguard as it is working by design. For an instance, the proliferator can divert small quantity of the material per each attempt, so that amount of missing material is still within the safeguard expected measurement error, or it is too small for the safeguard to detect.
2. The proliferator attempts to elude the safeguard by using concealment tactics to prevent the safeguard to work as intended. The tactics can be used to make modifications to the material under detection, the hardware, or the software of the system.

Figure 2-2 shows portions of the success tree diagram for a neutron counter safeguard. The top event labeled "NC IS ELUDED" refers to the case when the proliferator successfully eludes the neutron counter.



NC IS ELUDED
OR
NC IS NOT WORKING BY A FAKE ACCIDENT
NC IS ELUDED WHILE WORKING
OR
Accuracy of Measurement (No Tactic)
NC IS ELUDED BY MEAN OF PROLIFERATOR'S TACTICTS
NC IS ELUDED WITHOUT PROLIFERATOR'S TACTICTS
OR
NC IS ELUDED BY USING DUMMY MATERIAL
1
Tactic A
NC IS ELUDED BY PLACING COMPENSATING MATERIAL IN DETECTION REGION
Tactic B
NC IS ELUDED BY HARDWARE MODIFICATION
Tactic C
NC IS ELUDED BY SIGNAL/DATA MODIFICATION
Tactic D
Vulnerabilities to specific threat/tactics
1
NC IS ELUDED BY USING DUMMY MATERIAL
AND
PROLIFERATOR ATTEMPTS TO USE DUMMY MATERIAL
USING DUMMY MATERIAL IS NOT DETECTED
AND
OPTICAL SURVEILLANCE IS ELUDED
MATERIAL SEAL IS ELUDED
USING DUMMY MATERIAL IS NOT DETECTED BY NC
Basic Event to be determined

Figure 2-2 Portion of the success tree diagram for a neutron counter

The Success Tree diagram in Figure 2-2 describes the pathway that a proliferator has to follow in order to succeed in his acquisition attempt. The acquisition attempt depends on the Proliferator's capability to elude all the safeguards in place at a given location. Eluding the safeguard in this case means to elude all the measurements resulting from the safeguard scheme present in a selected location of the NES, or Material Balance Area (MBA). The top event, labeled "NC is eluded," represents the capability to elude a neutron counter (NC), which depends on two main factors. The first factor to consider is that, depending on the quantity of material subtracted, the safeguard might not be able to detect it even in the absence of additional tactics. This is the case when the proliferator acquires an amount of material that is below the threshold at which the instrument detects the presence of a given material (e.g. the amount of plutonium nitrate flowing in a pipe). The probability associated with this event, labeled as 'no tactic', can be inferred by knowing the accuracy of the safeguard. This means that the proliferator, assuming he knows the threshold of the instrument, does not need to produce an ad hoc tactic specifically intended for this safeguard.

In the case that the amount of material is within the range of detection of this instrument, the proliferator then needs to add an additional tactic selected from the four supportive tactics labeled from A to D in the left lower portion of the tree. Each one of these tactics represents a specific attack on the detection system or on the sample. Tactic A for an instance, expanded with a sub-tree on the right, depicts the situation where the proliferator adds dummy materials to the sample in order to elude the NC measurements and mask the illicit subtraction of material. In order to be undetected, the proliferator needs to support this strategy with further actions, such as eluding seals and optical surveillance (diamonds). These events in the success tree are shown as undeveloped events because they have to be expanded further into their own success trees and the probabilities of these events depend on the proliferator tactics to their supporting safeguards as well.

The determination of the basic event (circle) labeled "Using dummy material is not detected by NC" is the basic event that determines the potential vulnerability of the neutron counter to threat A.

Note that there is another choice of tactic for the proliferator to use to elude the neutron counter. This is shown as the event labeled "NC is not working by a fake accident". However, this tactic is not considered as the event relating directly to the neutron counter because the tactic simply breaks the functionality of the neutron counter and the only way that the tactic will be detected is by the supporting safeguards, not by the neutron counter itself.

In conclusion, there are 5 basic events probability relating directly to the neutron counter as shown in Table 2-1.

Table 2-1. Basic Event probabilities and tactics for a neutron counter

Tactic	*Basic Event Probability*	*Tactic Description*
No Tactic	Probability that a proliferator will successfully elude the neutron counter without any tactics	Depending on the neutron counter uncertainty of measurement, proliferator diverts the material for an amount that is within the expected error of measurement
Tactic A	Probability that a proliferator will successfully elude the neutron counter by using dummy material	Proliferator replaces missing material with another neutron source, such as minor actinides or fission products
Tactic B	Probability that a proliferator will successfully elude the neutron counter by placing compensating material in the detection region	Proliferator places compensating material with the same mass as those diverted in the detection region, such as on the surface of the pipe, or between the container and the detector.
Tactic C	Probability that a proliferator will successfully elude the neutron counter by modifying the detector/hardware	Proliferator modifies the detector to give more neutron count than normal, or modifies the electronic circuit to send more signals to the processing unit.
Tactic D	Probability that a proliferator will successfully elude the neutron counter by modifying the signal/data	Proliferator modifies the software to store the desired output or access the record to modify the data.

In addition, these basic events probabilities are not independent but a function of other variables, depending on the safeguard. The abbreviations of the safeguards are defined in Section 2.1

Table 2-2. Factor affecting the probability of the safeguard to detect the diversion

Factors	Safeguards												
	DA	GRS	NC	HI	WI	OS	SL	ID	MR	PM	SI	ES	PTM
Total mass of the material under detection	●	●	●	●	●	●						●	
Mass of the diverted material under detection	●	●	●	●	●	●	●	●	●	●		●	●
Cost of the safeguard	●	●	●	●	●	●	●	●	●	●	●	●	●
Material Form	●	●	●	●	●	●	●	●	●	●		●	●
Material Geometry under detection		●	●	●		●				●			
Detection Time		●	●	●		●				●	●		●
Background / Interference		●	●	●		●				●			

Since the material form, material geometry, detection time, and the background are given by the design of the facility. The main variables that are affecting the proliferator success probability are the mass under detection and the cost of the safeguard.

- The probability that the safeguard is eluded without tactic can be a function of the mass of the material that is being measured (M), and also a function of the resources devoted to the safeguard, or its final cost (C).
- The vulnerability measured in terms of the proliferator probability to succeed with tactics can be a function of the overall safeguard cost (C).

In this framework, there are two types of safeguard related to the proliferator tactics

1. Primary Safeguards: These safeguards are used to detect material diversion attempts. A proliferator will try to use tactics to elude these safeguards in order to divert the material without being detected. All primary safeguards that are in place to detect proliferator diversion attempts must be eluded for the proliferator to succeed.
2. Supporting Safeguards: These safeguards are used to detect tactics that a proliferator can use to elude the primary safeguards. Secondary safeguards that are in place to detect the proliferator tactics must be eluded for the proliferator to succeed. This type of safeguard is shown in diamond shape inside the success tree, indicating that this is an "undeveloped event" because the probability of this event also depends on the proliferator's choice to use any tactic on these supporting safeguards.

Table 2-3 contains the summary of proliferator tactics to elude primary and supporting safeguards.

Table 2-3. Summary of possible proliferator tactics that can be used to elude safeguards

Proliferator Tactics	Safeguards												
	DA	GRS	NC	HI	WI	OS	SL	ID	MR	PM	SI	ES	PTM
Avoid random sampling	●											●	
Modify the sample	●											●	
Use dummy material	●	●	●	●	●							●	
Modify detector/hardware		●	●	●	●	●		●	●	●			●
Modify signal/data		●	●	●	●	●		●	●	●			●
Placing compensating material in the detection region		●	●	●	●								
Repair/Replace the broken seal							●						
Use fake ID device								●					
Prevent physical inspection by the inspector											●		
Bribe the inspector											●		
Cleanup material traces												●	
Use shielding container													●
Faking an accident to break the safeguard		●	●	●	●	●	●	●	●	●			●

Table 2-4 shows the three supporting safeguards that are in place to detect proliferator tactics; Optical Surveillance (OS), Seal (SL), and Safeguard by the Inspector (SI). The table also shows specifically the type or the location of the safeguard for each tactic.

Table 2-4. Summary of the supporting safeguards that are used to detect proliferator tactics

Proliferator Tactics	Safeguards that are detecting the tactics		
	OS	SL	SI
Avoid random sampling			Random sampling
Modify the sample		Sample Seal	Sample Monitoring
Use dummy material	Material OS	Material Seal	
Modify detector/hardware	System OS	System Seal	
Modify signal/data	System OS	System Seal	
Placing compensating material in the detection region	System OS	System Seal	
Repair the broken seal	Seal OS	Seal	
Replace the broken seal	Seal OS	Seal	
Use fake ID device	Material OS		
Prevent physical inspection by the inspector	Facility OS		
Bribe the inspector			Inspector
Cleanup material traces	Facility OS		
Use shielding container	Facility OS		
Faking an accident to break the safeguard	Facility OS		Accident Inspection

Following this section are the details and the success tree model of each safeguard type (IAEA, Safeguards Techniques and Equipment 2003).

Destructive Analysis (DA)

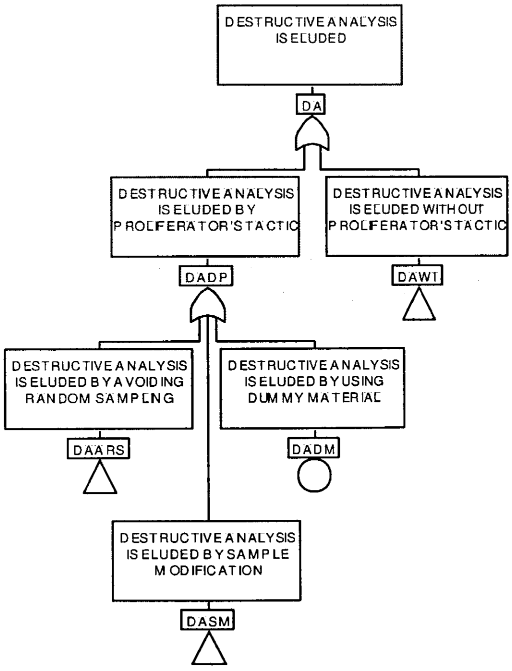

DESTRUCTIVEANALYSIS ISELUDED
DA
DESTRUCTIVEANALYSIS ISELUDEDBY PROLFERATOR'STACTIC
DESTRUCTIVEANALYSIS ISELUDED WITHOUT PROLFERATOR'STACTIC
DADP
DAWT
DESTRUCTIVEANALYSIS ISELUDEDBYAVOIDING RANDOM SAMPLNG
DESTRUCTIVEANALYSIS ISELUDEDBYUSING DUMMY MATERIAL
DAARS
DADM
DESTRUCTIVEANALYSIS ISELUDEDBYSAMPLE MODIFICATION
DASM

Figure 2-3. Destructive analysis success tree

The destructive analysis is used to determine elemental composition, elemental assay, or isotopic composition of the sample, which is randomly taken from the processes inside a facility. All part of the sample is consumed in the analysis, where the sample is irreversibly altered (dissolved, radiochemically purified). DA has better precision than Non-Destructive Analysis (NDA) because the effect of the matrix can be eliminated or corrected. There are two types of destructive analysis:
Elemental analysis: NBL Davies and Gray titration, MacDonald and Savage titration, Controlled potential coulometry, Ignition gravimetry, K-edge X ray densitometry, Wavelength dispersive X ray fluorescence spectrometry, Isotopic dilution mass spectrometry, Plutonium (VI) spectrophotometry,
Isotopic analysis: Thermal ionization mass spectrometry, High-resolution gamma ray spectrometry with Ge detector, Gamma ray spectrometry with NaI detector, Alpha spectrometry. Since DA requires the inspector to randomly collect samples and send them to a laboratory, a proliferator can attempt to elude DA by making the inspectors collect samples from certain areas, or modify the samples during the transportation.

Non-Destructive Analysis (NDA)

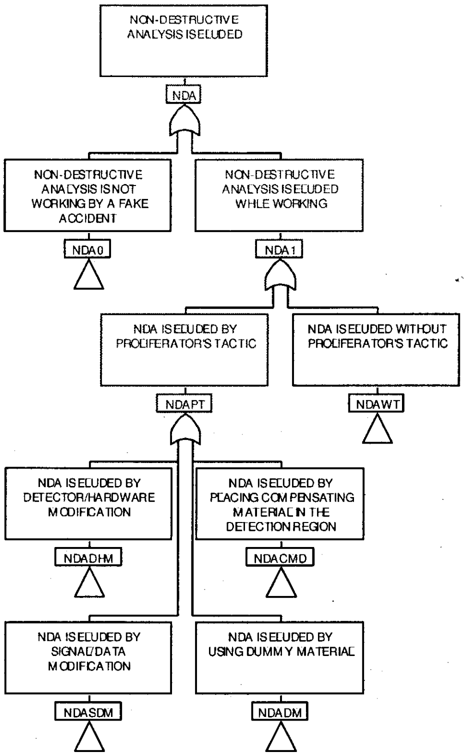

NON-DESTRUCTIVE ANALYSIS IS ELUDED
NDA
NON-DESTRUCTIVE ANALYSIS IS NOT WORKING BY A FAKE ACCIDENT
NDA0
NON-DESTRUCTIVE ANALYSIS IS ELUDED WHILE WORKING
NDA1
NDA IS ELUDED BY PROLIFERATOR'S TACTIC
NDAPT
NDA IS ELUDED WITHOUT PROLIFERATOR'S TACTIC
NDAWT
NDA IS ELUDED BY DETECTOR/HARDWARE MODIFICATION
NDADHM
NDA IS ELUDED BY PLACING COMPENSATING MATERIAL IN THE DETECTION REGION
NDACMD
NDA IS ELUDED BY SIGNAL/DATA MODIFICATION
NDASDM
NDA IS ELUDED BY USING DUMMY MATERIAL
NDADM

Figure 2-4. Non-destructive analysis success tree

NDA system measures nuclear material without alteration or direct contact with the item under analysis. Most NDA techniques measure radiation, spontaneous or stimulated, from nuclear material items. Comparing to destructive analysis, NDA is faster, cheaper and can perform in situ, however there is much higher uncertainty in the results. There are four main categories of non-destructive analysis; gamma ray spectrometry, neutron counter, heat inspection, and weight inspection. Proliferator tactics to elude all of the safeguards of this type are similar. There are four main tactics; hardware modification, software modification, using dummy material and placing compensating material in the detection region. The actual tactics are different because each type of NDA is detecting different property of the material and some tactics are easier for some types than the other.

Gamma ray spectrometry (GRS) measures the distribution of intensity of gamma radiation from the sample versus the energy of each photon. Gamma rays have well defined energies that are characteristic of the isotopes emitting them. When combined with a measurement of intensities, the gamma ray energies can provide quantitative information on the amount of material that is present. The basis of all gamma ray detector systems is the collection of liberated electrical charge to produce a voltage pulse whose amplitude is proportional to the gamma ray energy. GRS can be used to detect 186keV gamma ray from U-235 in enriched uranium, verify plutonium isotopes as well as decay products, and check the date of discharged of eradiated fuel by measuring 662keV gamma ray from Cs-137. There are two types of GRS; Attended mode such as Handheld Monitor System (HM-5), Inspector Multichannel Analyzer (IMCA), Spent Fuel Attribute Tester (SFAT), Improved Cerenkov Viewing Device (ICVD); and unattended mode such as Input Flow Verification System (CONS), Entrance Gate Monitor (ENGM), Spent Fuel Bundle Counter (VIFB), and Core Discharge Monitor (VIFC). There are three types of detector; NaI has higher efficiency, but low energy resolution, Ge has higher resolution, but must be operated at very low temperature, CdZnTe has highest detection efficiency and does not need cooling.

Neutron Counter (NC) measures the number of neutrons radiated from the sample that are passing through the detector. To know the amount of specific material, isotopic abundance must be known or verified, typically by means of high-resolution gamma ray measurement. There are many types of NC; Neutron Coincidence Counting is a passive detector system used to determine the mass of Pu based on spontaneous fission, Multiplicity Counting uses triple coincidence parameters to solve for mass, Active Neutron Assay is an active system that places a random neutron source in the cavity of a coincidence counter, and Active Delayed-Neutron Assay uses a sensitive detector to detect the delayed neutron after interrogating the sample with neutron source. The two most common types of neutron detector are He-3 and BF_3 gas filled proportional detectors.

Heat Inspection (HI) measures the heat radiated from the sample. Same as NC, the measurement must be combined with isotopic analysis to obtain mass of specific material. Plutonium and uranium emit heat from alpha-particle absorption in the sample. Plutonium produces 2-12 W/kg of heat, depending on the isotopic composition. For low burnup plutonium the principle heat source is Pu-239, but for high burn up plutonium, the major contribution comes from Pu-238 and Am-241. There are a few different types of HI: calorimetry, temperature sensor, and infrared camera.

Weight Inspection (WI) verifies and monitoring the gross weight of the material in any forms. Example of weight inspection safeguards are weighting scale, precision load cell, etc.

Optical Surveillance (OS)

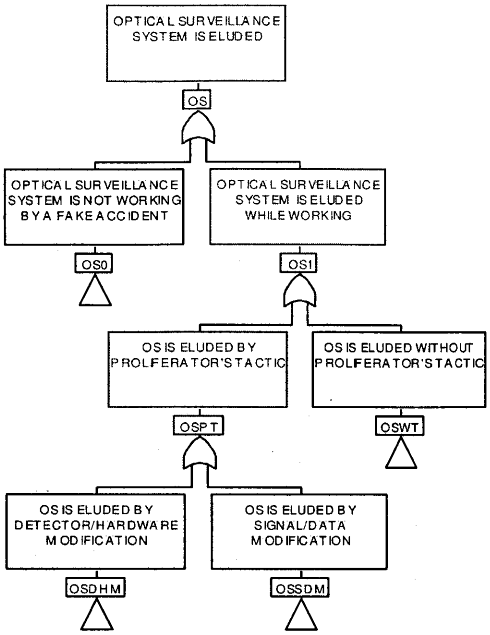

OPTICAL SURVEILLANCE SYSTEM IS ELUDED
OS
OPTICAL SURVEILLANCE SYSTEM IS NOT WORKING BY A FAKE ACCIDENT
OPTICAL SURVEILLANCE SYSTEM IS ELUDED WHILE WORKING
OS0
OS1
OS IS ELUDED BY PROLFERATOR'S TACTIC
OS IS ELUDED WITHOUT PROLFERATOR'S TACTIC
OSPT
OSWT
OS IS ELUDED BY DETECTOR/HARDWARE MODIFICATION
OS IS ELUDED BY SIGNAL/DATA MODIFICATION
OSDHM
OSSDM

Figure 2-5. Optical surveillance success tree

The main goal of optical surveillance is to provide continuity of knowledge about nuclear materials and other items of safeguards significance between on-site inspection visits. Optical surveillance is intrinsically an unattended technique that can be used to record images only, or it may be integrated with other unattended monitoring equipment to provide nuclear measurement, containment history and other data. Effective surveillance is achieved when a camera field of view covers the entire area of safeguards interest to capture the movement of safeguarded items. The following are the different types of optical surveillance; Single Camera: All-in-one surveillance, mains operated (ALIS) and portable battery operated (ALIP), Digital single camera optical surveillance (DSOS); Multi Camera: Server digital image surveillance (SDIS), Digital Multi- Camera Optical Surveillance (DMOS), FAST company surveillance system (FAST); Short Term Surveillance: All-in-one surveillance portable (ALIP), Surveillance for Remote Monitoring: Server digital image surveillance (SDIS); Underwater TV: Underwater TV (UWTV), Underwater viewing device (UWVD). To elude OS, a proliferator can generate fake images by modifying the cameras or falsify video data.

Seal (SL)

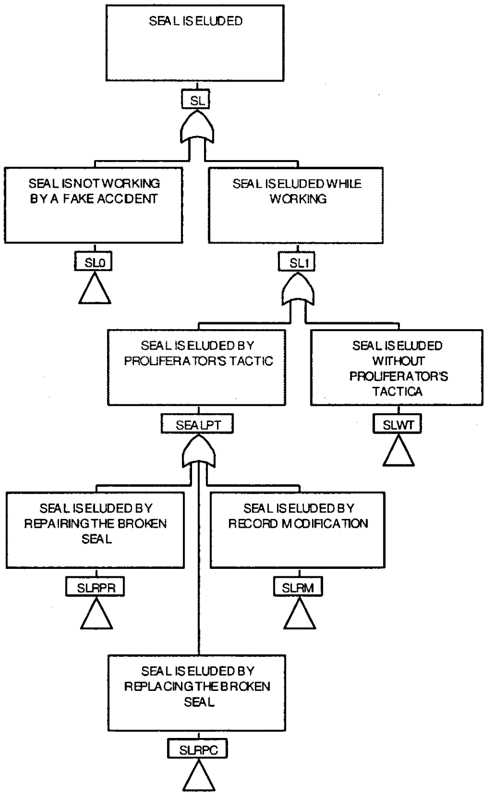

SEAL IS ELUDED
SL
SEAL IS NOT WORKING BY A FAKE ACCDENT
SEAL IS ELUDED WHILE WORKING
SL0
SL1
SEAL IS ELUDED BY PROLIFERATOR'S TACTIC
SEAL IS ELUDED WITHOUT PROLIFERATOR'S TACTICA
SEALPT
SLWT
SEAL IS ELUDED BY REPAIRING THE BROKEN SEAL
SEAL IS ELUDED BY RECORD MODIFICATION
SLRPR
SLRM
SEAL IS ELUDED BY REPLACING THE BROKEN SEAL
SLRPC

Figure 2-6. Seal success tree

Seal is used to secure materials, documents or any other important items in a tamper-proof containment. The purpose of the seals is to provide evidence of any unauthorized attempt to gain access to the secured material. Seals do not provide any kind of physical protection, nor were they designed to provide such protection. Seal types are separated into Single Use Seals: Metal cap seal (CAPS), Improved adhesive seal (VOID), which are traditionally used by the safeguarder. The other type is the In situ verifiable seals: Fiber Optic General Purpose Seal or COBRA seal (FBOS), Ultrasonic Seal (ULCS), Ultrasonic Sealing Bolt (USSB), and Variable Coding Seal System (VCOS). Possible locations to use seal: Material Container, Sample container, safeguard system container, MBA entrance and exit. To elude seal, a proliferator can break the seal and try to repair it to the original condition or replace the seal with an identical one to fool the inspectors. For seals that are digitally recorded, a proliferator can attempt to modify the records that show seals have been broken.

ID Tracking (ID)

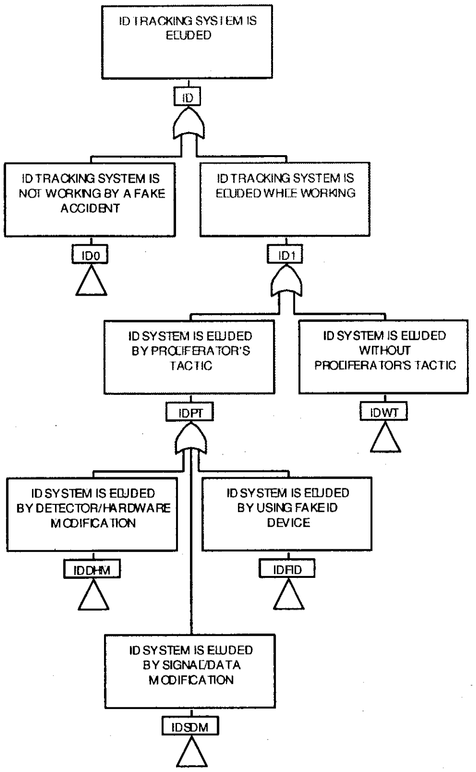

ID TRACKING SYSTEM IS ELUDED
ID
ID TRACKING SYSTEM IS NOT WORKING BY A FAKE ACCIDENT
ID0
ID TRACKING SYSTEM IS ELUDED WHILE WORKING
ID1
ID SYSTEM IS ELUDED BY PROLIFERATOR'S TACTIC
IDPT
ID SYSTEM IS ELUDED WITHOUT PROLIFERATOR'S TACTIC
IDWT
ID SYSTEM IS ELUDED BY DETECTOR/HARDWARE MODIFICATION
IDDHM
ID SYSTEM IS ELUDED BY USING FAKE ID DEVICE
IDFID
ID SYSTEM IS ELUDED BY SIGNAL/DATA MODIFICATION
IDSDM

Figure 2-7. ID Tracking success tree

The purpose of ID Tracking is to verify and keep track of the location of the container of material, such as cylinder, canister, glovebox, or assembly, at all time. ID tracking can be used to track the material both inside the facilities and outside during its transportation between facilities. The following are the most common types of ID Tracking; Barcode, Camera ID, Radio-frequency Identification (RFID), Laser Identification (Laser ID), and Global Positioning System (GPS). To elude ID tracking system, a proliferator can modify the hardware, including the detectors or the tracking device on the material container, or modify the signals/data in the processing system. For some systems, a proliferator can use faking devices to fool detectors from detecting that the material is missing.

Movement Recording (MR)

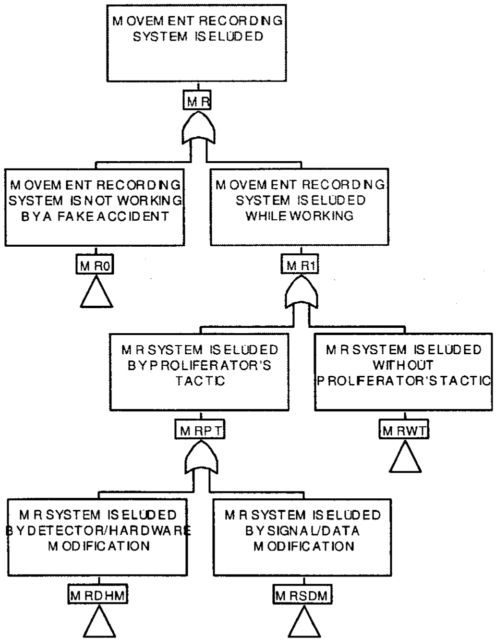

MOVEMENT RECORDING SYSTEM IS ELUDED
MR
MOVEMENT RECORDING SYSTEM IS NOT WORKING BY A FAKE ACCIDENT
MR0
MOVEMENT RECORDING SYSTEM IS ELUDED WHILE WORKING
MR1
MR SYSTEM IS ELUDED BY PROLIFERATOR'S TACTIC
MRPT
MR SYSTEM IS ELUDED WITHOUT PROLFERATOR'S TACTIC
MRWT
MR SYSTEM IS ELUDED BY DETECTOR/HARDWARE MODIFICATION
MRDHM
MR SYSTEM IS ELUDED BY SIGNAL/DATA MODIFICATION
MRSDM

Figure 2-8. Movement recording success tree

Movement Recording system is a sensor system used to record the movement of the material or equipments inside the facility. The common use is to detect that the material in the storage or in the reactor core does not move during the unscheduled time. The examples for movement recording system are Motion Sensor (MS) or Position Tracking System (PTS). To elude movement recording system, a proliferator can modify the sensor, or the software/data of the processing unit to not record any movement occurred during material diversion.

Process Monitoring (PM)

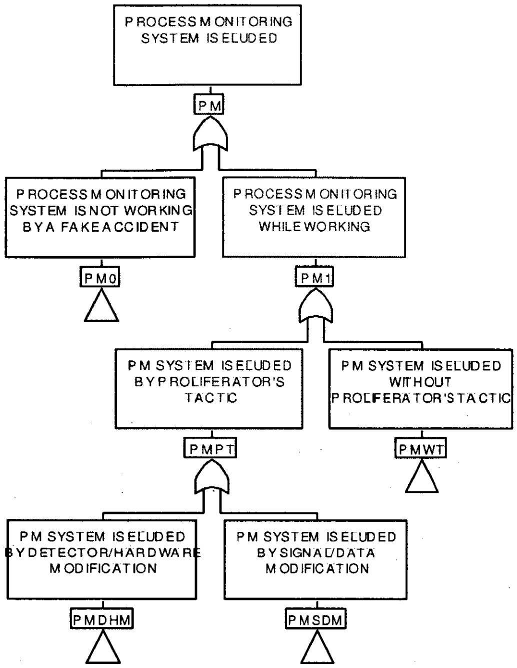

PROCESS MONITORING SYSTEM IS ELUDED
PM
PROCESS MONITORING SYSTEM IS NOT WORKING BY A FAKE ACCIDENT
PROCESS MONITORING SYSTEM IS ELUDED WHILE WORKING
PM0
PM1
PM SYSTEM IS ELUDED BY PROLIFERATOR'S TACTIC
PM SYSTEM IS ELUDED WITHOUT PROLFERATOR'S TACTIC
PMPT
PMWT
PM SYSTEM IS ELUDED BY DETECTOR/HARDWARE MODIFICATION
PM SYSTEM IS ELUDED BY SIGNAL/DATA MODIFICATION
PMDHM
PMSDM

Figure 2-9. Process monitoring success tree

Process monitoring system is used to monitor the processes in a nuclear facility to verify that the facility is operating as expected. There are many methods that a proliferator can do to change the processes in order to facilitate diversion scenarios, such as changing power of a nuclear reactor, modify the chemical separation process in a reprocessing facility, increase the enrichment of uranium in an enrichment facility, etc. There are three most commonly used process monitoring; Pressure Monitoring (Electromanometer), Flow Monitoring, and Power Monitoring. To elude process monitoring system, a proliferator can modify the sensors or detectors to give expected signals. Same as other safeguard systems with processing unit, a proliferator can also attempt to modify the recorded data or software of the system.

Safeguard by Inspector (SI)

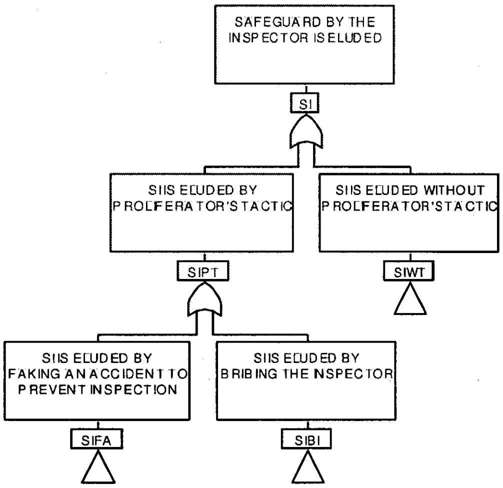

SAFEGUARD BY THE INSPECTOR IS ELUDED
SI
SI IS ELUDED BY PROLFERATOR'S TACTIC
SI IS ELUDED WITHOUT PROLFERATOR'S TACTIC
SIPT
SIWT
SI IS ELUDED BY FAKING AN ACCIDENT TO PREVENT INSPECTION
SI IS ELUDED BY BRIBING THE NSPECTOR
SIFA
SIBI

Figure 2-10. Safeguard by inspector success tree

Safeguard conducted by the inspectors including facility inspection, taking random sample for destructive analysis, verify the data of the unattended safeguard system, and monitor the facility operation, such as reactor refueling. Following are the list of SI:

- Routine Inspection: Physical Inventory Verification (PIV) and Design Information Verification (DIV)
- Safeguard System Inspection: Inspectors inspect the unattended safeguard system; seal, optical surveillance, non-destructive analysis system.
- Random Sampling: Inspectors collect random sample of the material for destructive analysis or swipe random surface for environmental sampling
- Sample Monitoring: Inspectors monitor the collected sample during the inspection and in transit from the site to the safeguarder's laboratory
- Accident Inspection. Examples of fake accidents are electrical accident, such as electrical circuit tripping, loss of power, short circuit, system overheat, fire accident, such as fire, explosion, and physical accident, such as accidental collision or facility operation mistake.

To elude SI, a proliferator can bribe the inspectors or create a situation where the inspectors cannot access the target areas to perform inspection.

Environmental Sampling (ES)

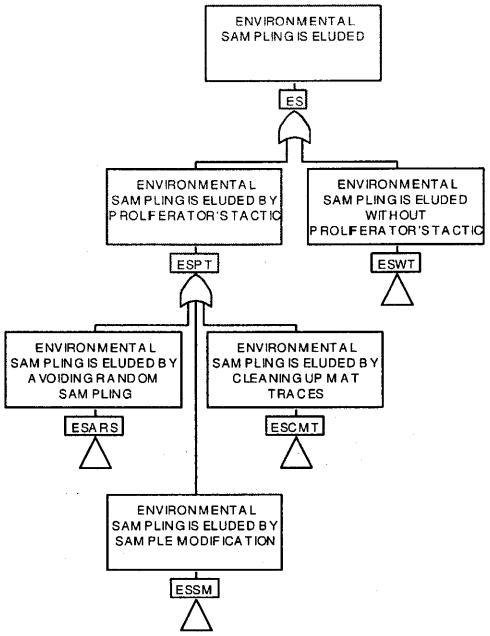

ENVIRONMENTAL SAMPLING IS ELUDED
ES
ENVIRONMENTAL SAMPLING IS ELUDED BY PROLFERATOR'S TACTIC
ENVIRONMENTAL SAMPLING IS ELUDED WITHOUT PROLFERATOR'S TACTIC
ESPT
ESWT
ENVIRONMENTAL SAMPLING IS ELUDED BY AVOIDING RANDOM SAMPLING
ENVIRONMENTAL SAMPLING IS ELUDED BY CLEANING UP MAT TRACES
ESARS
ESCMT
ENVIRONMENTAL SAMPLING IS ELUDED BY SAMPLE MODIFICATION
ESSM

Figure 2-11. Environmental sampling success tree

Collection of environmental samples at or near a nuclear site combined with ultrasensitive analytical techniques such as mass spectrometry, particle analysis, and low level radiometric techniques can reveal signatures of past and current activities in locations where nuclear material is handled. Environmental Sampling is designed to detect the unusual or unexpected activity inside the facility, such as movement of the SNM or extra processes that are not reported to the inspectors. Samples are analyzed in either bulk or particle mode, depending on the sampling objectives and the activity levels of the swipes. Types of ES; Screening of samples, such as low level gamma ray spectrometry, x-ray fluorescence spectrometry, alpha/beta counting; Isotopic and Elemental Analysis such as pulse counting thermal ionization mass spectrometry, scanning electron microscopy with electron probe analysis, fission track method, and secondary ion mass spectrometry. Besides the similar tactics to elude DA, a proliferator can attempt to clean up the traces of material along the diversion pathways.

Portal Monitoring (PTM)

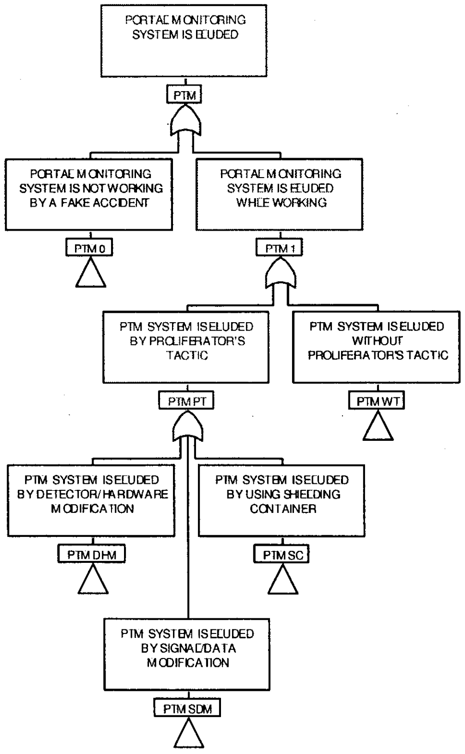

PORTAL MONITORING SYSTEM IS ELUDED
PTM
PORTAL MONITORING SYSTEM IS NOT WORKING BY A FAKE ACCIDENT
PORTAL MONITORING SYSTEM IS ELUDED WHILE WORKING
PTM0
PTM1
PTM SYSTEM IS ELUDED BY PROLIFERATOR'S TACTIC
PTM SYSTEM IS ELUDED WITHOUT PROLIFERATOR'S TACTIC
PTMPT
PTMWT
PTM SYSTEM IS ELUDED BY DETECTOR/HARDWARE MODIFICATION
PTM SYSTEM IS ELUDED BY USING SHIELDING CONTAINER
PTMDHM
PTMSC
PTM SYSTEM IS ELUDED BY SIGNAL/DATA MODIFICATION
PTMSDM

Figure 2-12. Portal monitoring success tree

Portal monitoring system is used to monitor the gates for everything that is going and out of the facility. The system is designed to record all of the properties of both the material and facility personnel that are crossing the boundaries of the facility to ensure that there is no extra material going in and no stolen material getting out. Besides attacking the hardware and software of the system, the proliferator can also use a shielding container to shield the radiation of the diverted material when passing through the portal monitoring system.
The following are the possible component of PTM X-Ray Spectrometry, Portal Gamma Ray, Spectrometry, Portal Neutron Detector, Infrared Camera, Temperature Sensor, Weight Scale. To elude portal monitoring system, a proliferator can modify the detector/hardware or signal/data of the system similar to other unattended system. One extra tactic that a proliferator can attempt is to place the diverted material inside a shielding container to prevent the system from detecting the radiations or properties of the material.

For complete descriptions and success trees for all types of safeguards, see Appendix A.

2.3 Nuclear Fuel Cycle Facilities

To identify the list of safeguards that are related to the possible diversion scenarios, the complete information about the safeguard scheme is needed. This section contains the information about the processes and possible safeguard setup for the major facilities inside the nuclear fuel cycle that are the likely targets of a material diversion. Figure 2-13 shows the nuclear fuel cycle with the material flow for both closed and open fuel cycle.

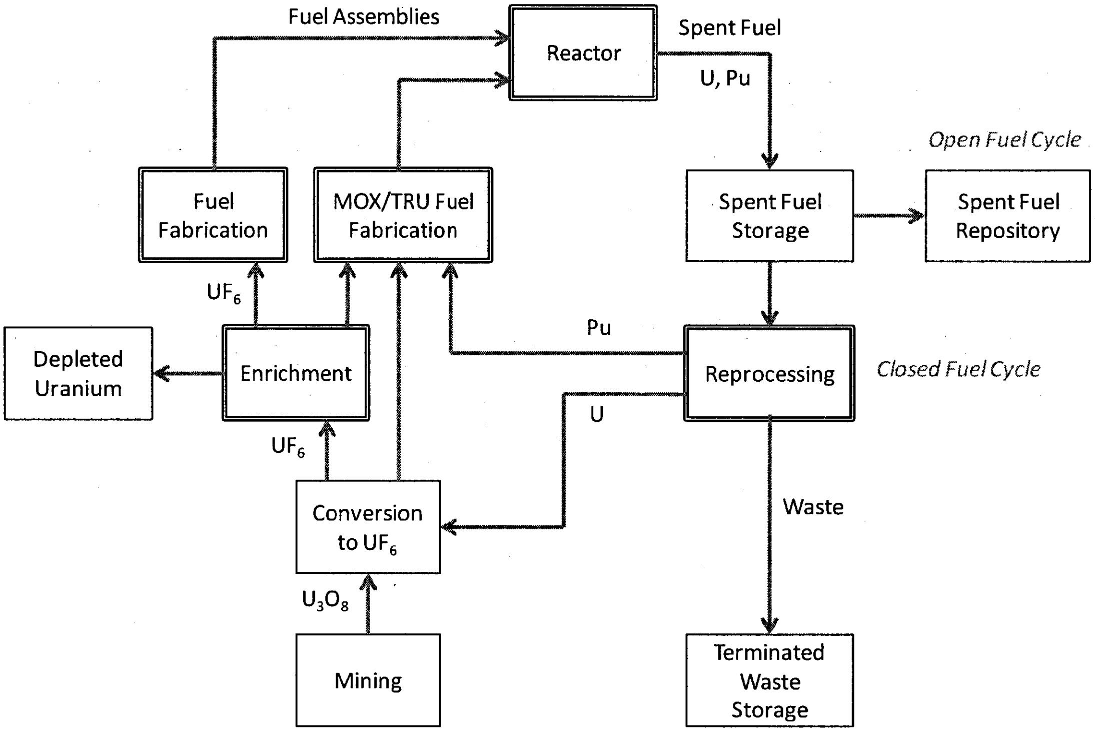


Figure 2-13. Nuclear fuel cycle and the material flow

There are four major facilities in the fuel cycle that are attractive for proliferation.

1. Nuclear Enrichment Facility
2. Nuclear Fuel Fabrication Facility
3. Nuclear Reactor
4. Nuclear Reprocessing Facility

Each facility is separated into several Material Balance Areas (MBAs) where the material flowing in and out will be accounted. For example, the list of current safeguards and possible safeguard setup in an aqueous reprocessing facility (Michael H. Ehinger 2009) are shown in Figure 2-14.

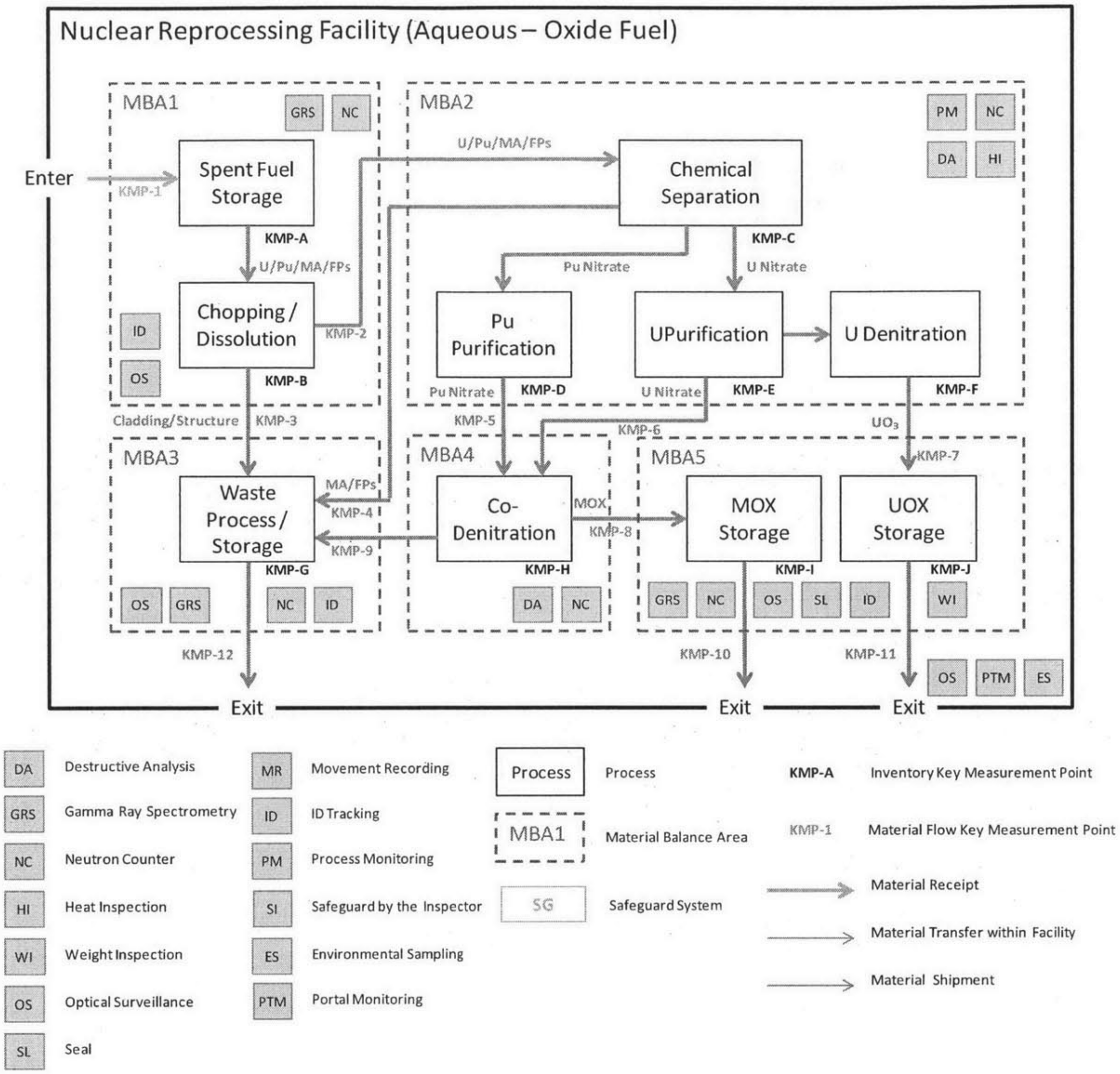


Figure 2-14. Aqueous reprocessing facility diagram

The scheme above shows the flow of the material and the safeguards scheme in an Aqueous Fuel Reprocessing Facility (ARF). The processes of this facility are separated into five material balance areas (MBA) where the material flows in and out of the areas are measured for material accountancy. Each MBA contains different types of safeguards that are suitable for the processes and form of the material within the area. The safeguards are located at the Key Measurement Points (KMP) throughout the facility. There are two types of KMP; one is Inventory Key Measurement Point (IKMP), where the safeguards monitor the material inside the process or storage. The other type is Flow Key Measurement Point (FKMP), where the safeguards monitor the amount of material transferring between two processes.

Table 2-5 and Table 2-6 show the details of the each material balance area and key measurement point in the facility.

Table 2-5. Material Balance Area (MBA) of an aqueous reprocessing facility

Material Balance Area	Nuclear Material	Safeguards
MBA1: Feed Storage & Disassembly Area	Spent Fuel Assembly Chopped Spent Fuel	Optical Surveillance Gamma Ray Spectrometry Neutron Counter ID Tracking
MBA2: Chemical Separation Area	Spent Fuel Pu Nitrate U Nitrate	Process Monitoring Neutron Counter Destructive Analysis Heat Inspection
MBA3: Waste Process & Storage Area	Solid Waste	Optical Surveillance Gamma Ray Spectrometry Neutron Counter ID Tracking
MBA4: Co-Denitration Area	Pu Nitrate U Nitrate	Neutron Counter Destructive Analysis
MBA5: Product Storage Area	MOX UOX	Optical Surveillance Seal Gamma Ray Spectrometry Neutron Counter Weight Inspection ID Tracking
Throughout Facility	Diverted Material	Optical Surveillance Environmental Sampling Portal Monitoring

Table 2-6. Key Measurement Point (KMP) of an aqueous reprocessing facility

Inventory KMP	**Flow KMP**
• KMP-A: Spent Fuel Storage • KMP-B: Chopping and Dissolution Process • KMP-C: Chemical Separation Process • KMP-D: Pu Purification Process • KMP-E: U Purification Process • KMP-F: U Denitration Process • KMP-G: Waste Process and Storage • KMP-H: Co-Denitration Process • KMP-I: MOX Storage • KMP-J: UOX Storage	• KMP-1: Receipt of Spent Fuel Assembly • KMP-2: Transfer of Spent Fuel from MBA1 to MBA2 • KMP-3: Transfer of Waste from MBA1 to MBA3 • KMP-4: Transfer of Waste from MBA2 to MBA3 • KMP-5: Transfer of Pu from MBA2 to MBA4 • KMP-6: Transfer of U from MBA2 to MBA4 • KMP-7: Transfer of UOX from MBA2 to MBA5 • KMP-8: Transfer of MOX from MBA4 to MBA5 • KMP-9: Transfer of Waste from MBA4 to MBA3 • KMP-10: Shipment of MOX • KMP-11: Shipment of UOX • KMP-12: Shipment of Waste

With this information, the list of safeguards needed for the elicitation and the possible diversion scenarios can be identified for safeguard evaluation. Chapter 4 explains the details and methodology of the analyses used to evaluate a reprocessing facility.

For full details and diagrams of all four facilities, please see Appendix B. Note that the safeguards shown in these facilities are the possible safeguard schemes. The actual safeguards in each facility type are varied.

Chapter 3 Expert Elicitation

3.1 Objective and Approach of the Elicitation Process

The objective of the elicitation is to obtain expert judgment estimates of basic events probabilities for the success tree model.

Approach of the elicitation

1. Design and distinguish sets of questions regarding the safeguards into different categories depending on the expertise of the experts.
2. The main elicitation process is conducted by a questionnaire, with prior phone interview for preparation, and the follow up phone interview for feedbacks.

There are two categories of questions for each safeguard.

1. Category I: Questions relating to the basic events probability for the case of no proliferator tactic. In this case, the safeguard is assumed to be working in the expected condition with expected environment.
2. Category II: Questions relating to the basic events probabilities for the case with proliferator concealment tactics. In this case, a proliferator attempts to attack the safeguard system, or modify the material or environment under the safeguard to help elude the safeguard from detecting the diversion.

Category I Questions:

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.

There are two types of safeguard functionality to be considered, see Figure 3-1.

1. Detection type: The safeguard is used to detect diverted material or a diversion activity by a proliferator. The conclusion from the outputs of the safeguard is a binary decision whether the safeguard detects a diversion or not. For examples, an optical surveillance detects some unusual activities, or a seal shows that it has been broken, etc.
2. Measurement type: The safeguards is used to measure and account for the amount of targeted material or verify the level of facility operations. The conclusion from the outputs of the measurement is whether or not some amount of material are missing, or the current level of processes matches well enough with the expected value. For example, a temperature sensor measures the heat coming from the material and verifies that the result of the measurement is in the range of acceptable values.

Detection Only	Both	Measurement Only
Optical Surveillance Seal ID Tracking Movement Recording	Gamma Ray Spectrometry Neutron Counter Destructive Analysis Environmental Sampling	Heat Inspection Weight Inspection Process Monitoring

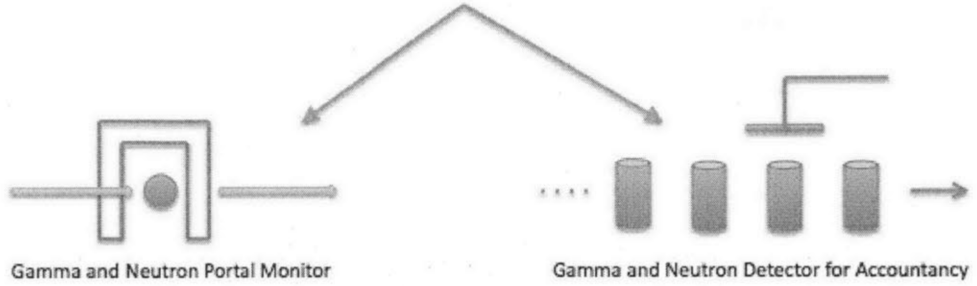

Gamma and Neutron Portal Monitor
Gamma and Neutron Detector for Accountancy

Figure 3-1. Difference between safeguard with detection and measurement functionality

For the safeguard of measurement type, the elicitation questions ask for the uncertainty of the measurement with 95% level of confidence as a function of the total material under detection. The uncertainty of measurement is expected to decrease when the total mass of material increases until it reaches saturation. See Figure 3-2 for an example plot.

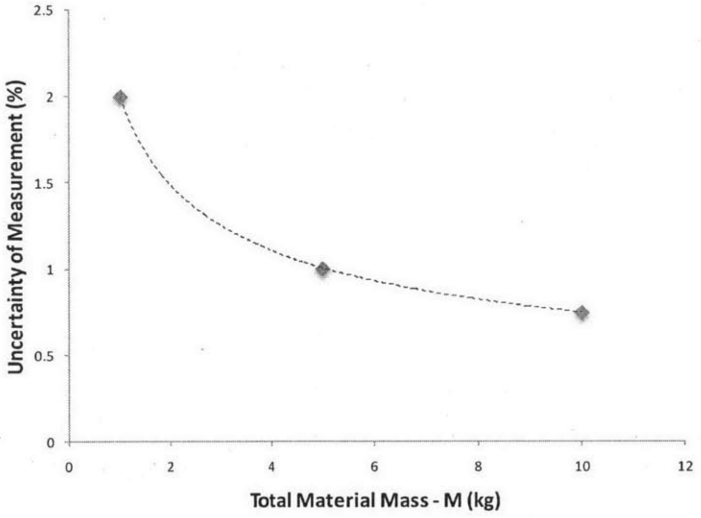


Figure 3-2. Example plot of material mass versus uncertainty of measurement

For the safeguard of detection type, the elicitation question only asks for the uncertainty of measurement with 95% level of confidence at the background level.

By asking the questions in term of the uncertainty of measurement, the expert can answer them more accurately and conveniently without much calculation required. The conversion of expert inputs to the proliferator diversion success probabilities will be described in Section 3.4

Category II Questions:

The questions ask for the probability that the proliferator tactic will successfully help elude the safeguard from detecting a material diversion, and its error with 95% level of confidence. The inputs from the experts are the probabilities of the basics event, thus they do not required any further calculation. Figure 3-3 shows the example inputs for this type of questions.

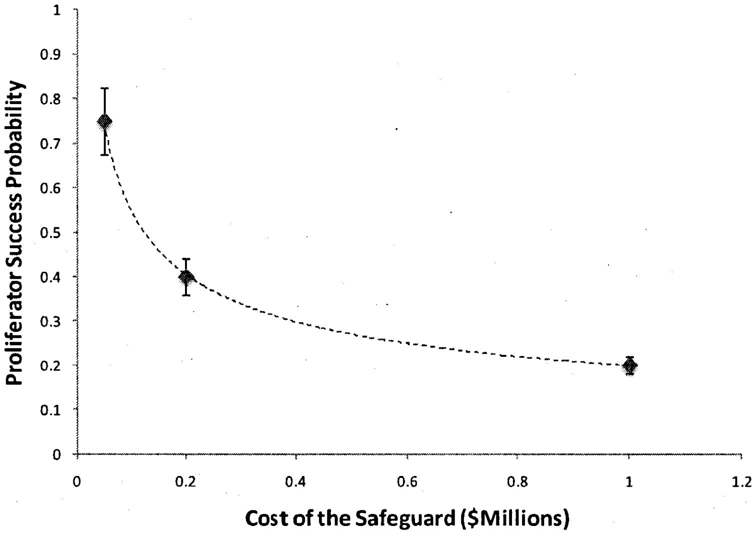


Figure 3-3. Plot of cost of safeguard (in $millions) versus proliferation success probability

The probabilities to elude the safeguard depend on the cost of safeguard setup. The cost that is associated to each tactic is the cost of safeguard modifications, equipments, components, and software that affects the proliferator success probability to elude the safeguard with the specific tactic.

3.2 Elicitation Protocols

The following list shows the steps for elicitation process used in this framework. It is adapted from ten steps process presented in NUREG-1150 (Hora 1989).

Step 1: Identification and selection of issues
Step 2: Selection of experts
Step 3: Provision of a uniform background database and preparation material
Step 4: Expert training and preparation for the elicitation
Step 5: Expert Elicitation
Step 6: Analyses based on aggregated expert inputs and feedbacks
Step 7: Finalizing expert inputs

Step 1: Identification and selection of issues

The goal of this elicitation process is to derive the success probabilities of the basic events in the safeguard evaluation success tree model. The questions to be answered by the experts are defined by the list of safeguards in the tree, the possible tactics that the proliferator can use to elude those safeguards, and the factors that will affect their detection failure probabilities.

Setup of the safeguards must be clearly defined along with identification of target material and design of the processes within the facility.

Step 2: Selection of experts

For each safeguard, the experts are chosen based on their expertise and experience in the area. Since there are different tactics that the proliferator can use to elude each safeguard, such as in the case of the non-destructive analysis; the proliferator can modify the hardware, software, using dummy material, or placing compensating material. For example, the experts who designed the safeguard will be able to provide their judgments for the uncertainty of measurement and the modification to the material under detection, while the experts who designed the software to run the safeguard will be able to provide their judgments for the probability that the proliferator will succeed in hacking the software or modify the stored data.

Step 3: Provision of a uniform background database and preparation material

The background material and the description, which explain the nature of the problem and the assessment being conducted, are prepared prior to contacting the experts. The document contains the structure of the framework, the success tree model, and the safeguard system description along with the details of the facility and material under studied. Example of results and calculation are also included. This process will ensure the uniform background and information among the experts.

Step 4: Expert training and preparation for the elicitation

This process is conducted by a telephone interview, in order to help the experts familiarize with the basic probability concept and success tree logic diagram. The interview also includes a discussion with the experts about the details of safeguard's functionality, components, and limitations. Specific safeguard setup will be defined, and all of the possible tactics to elude the safeguard will be listed, discussed, and categorized, to be used by every expert for the elicitation.

To ensure the quality and applicability of the inputs from the experts, the experts are asked to identify the safeguard detection range and the cost of the safeguard for different setup and components.

By considering the safeguard at specific material balance area of a facility, the main factors that will affect the uncertainty of measurement and the proliferator success probability are the mass of the material under detection, and the cost of the safeguard. Therefore, the applicable range of these factors, depending on the safeguard, will be derived from the discussion with the experts for use in the questionnaire. See Table 3-1 for the definitions of the reference points of the two factors.

Table 3-1. Factors affecting the variables in the elicitation and their reference points

Factor	Point on the detectable range	
	Point	Description
Total mass of the material under detection	M_{low}	Lowest total mass in the detectable range
	M_{bc}	Base case total mass, which is the regular mass of material under detection region in the facility
	M_{high}	Highest total mass in the detectable range
Cost of the safeguard	C_{min}	Minimum cost of the safeguard for it to operate
	C_{bc}	Base case cost, which is the regular cost of typical set up of the safeguard
	C_{opt}	Cost of the safeguard the will make it operate at the optimal efficiency

There are two types of the cost of the safeguard regarding the proliferator diversion success probability. First is the cost of the safeguard setup that affects the efficiency of the system. The other is the cost of safeguard setup that affects the vulnerability of the safeguard to proliferator tactics. For the latter case, these costs will be different depending on the type of tactics that proliferator will attempt to use.

Since the setup of the safeguard, such as the position of the detector, the distance between the detector and the material, the number of the detectors etc., affects the safeguard geometric efficiency, and thus affect the inputs from expert judgment. It is important that these are clearly defined and consistent between experts. In addition, by specifically defining the ranges of the factors, it ensures that the experts will provide probability estimates at the same reference points for further analyses.

Step 5: Expert Elicitation

The individual elicitation is completed by a questionnaire. The questionnaire contains questions asking for expert judgments of the uncertainties of measurement and the success probabilities of the proliferator tactics. For each variable, the questions will ask for the inputs at three different reference points that were derived in the last step of the elicitation process.

The following three tables show examples of questions to be filled in the questionnaire

Table 3-2. Questions for the uncertainty of measurement for detection type safeguard

Safeguard Estimated Cost	Uncertainty of Measurement (%) with 95% confidence level
	Point Estimate at the background level
$C_{min} = \$_{min}$	
$C_{bc} = \$_{bc}$	
$C_{opt} = \$_{opt}$	

Table 3-3. Questions for the uncertainty of measurement for measurement type safeguard

Safeguard Estimated Cost	Uncertainty of Measurement (%) with 95% confidence level		
	Total Mass $= M_{low}$	Total Mass $= M_{bc}$	Total Mass $= M_{high}$
$C_{min} = \$_{min}$			
$C_{bc} = \$_{bc}$			
$C_{opt} = \$_{opt}$			

Table 3-4. Questions for a proliferator success probability of a tactic that will elude the safeguard

Safeguard Estimated Cost	Proliferator success probability of tactic $\bar{A}$	
	Point Estimate	± Error with 95% Level of Confidence
$C_{A,min} = \$_{min}$		
$C_{\bar{A},bc} = \$_{bc}$		
$C_{\bar{A},opt} = S_{opt}$		

Along with the questionnaire, the expert will receive a supporting document that includes the full details of the safeguard setup, information of the material under detection, the definition and list of possible proliferator tactics in each category, and the details of the safeguard system at different costs.

Step 6: Analyses based on aggregated expert inputs and feedbacks

This step includes the analysis the questionnaire results from the experts, following by a phone interview with the experts to discuss about the issues that may arise and confirm the results of the elicitation. The uncertainties of measurement are converted to the detection failure probabilities, which are the basic events in the success tree model. A sensitivity analysis is then performed to check the affect of the inputs from each expert to the final results.

The inputs from different experts are aggregated by a linear opinion pool approach with equal weight, shown by Clemen and Winkler (Robert T. Clemen 1999). The result is the average of the values from all experts.

$$p(C_s) = \sum_{i=1}^{n} w_i p_i(C_s) \qquad (3\text{-}1)$$

p = the proliferator success probability
C_s = the safeguard cost
w_i = the weighting factor; in this case $w_i = 1$

Because the reference points on the range of the variable M and C have been defined prior the questionnaire during the first interview, the estimates of uncertainty of measurement and proliferator success probabilities are at the same reference points of the variables. Therefore, it provides a better comparison and aggregation of the inputs.

The second telephone interview will then be conducted to present the results to the experts along with the questions regarding some interesting issues from the analysis. The experts will either confirm the results or have an opportunity to adjust their inputs to better estimate the system.

Step 8: Finalizing expert inputs

The adjustments and final calculations will be made in this step for the results which are the basic event probabilities for the safeguard success tree as a function of the relevant factors for the safeguard system under study.

3.3 Example of the Elicitation Process

Here is the example of the expert elicitation with fictitious results for a neutron counter inside the MBA2 of an aqueous reprocessing facility.

Safeguard Setup

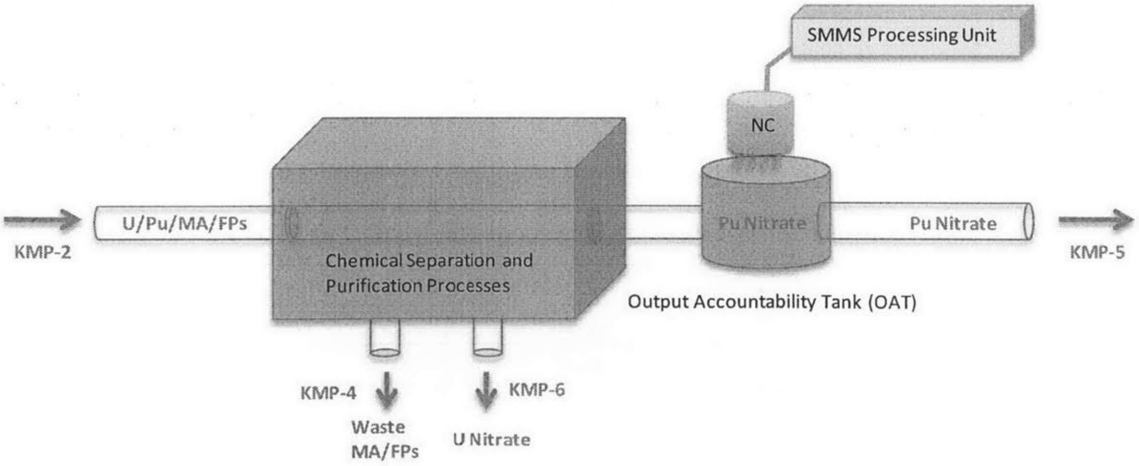


Figure 3-4. Setup on the neutron counter at the Output Accountability Tank (OAT)

Figure 3-4 and Table 3-5 show the setup and the information about the neutron detector as part of SMMS in Material Balance Area 2. The neutron detector is used to account for the amount of neutron radiation from plutonium nitrate in the Output Accountability Tank after the chemical separation and purification processes. The data from the detector is then compared with the reference signature and raises alarms in case of differences. This will effectively detect the proliferator' attempts to divert some amount of plutonium during the earlier processes since the amount of the plutonium under the detection will not match will the expected value.

Table 3-5. Information about the neutron detector in MBA2 as part of SMMS.

Type:	Helium-3 proportional detectors
System:	Solution Measurement and Monitoring System (SMMS)
Location:	Output Accountability Tank
Material Under Detection:	Plutonium in the plutonium nitrate solution

The material under detection by the neutron detector is the plutonium in plutonium nitrate solution. The approximation of plutonium isotope composition and neutron radiation is shown in the table below. Please note that the total mass the material under detection (M) in the questionnaire is the total mass of plutonium inside the detection region.

Table 3-6. Plutonium isotope composition and neutron radiation for a sample at MBA2.

Plutonium Isotope	% Isotope Composition	Neutron Radiation (N/kg.s)	Neutron Radiation of 1kg of Plutonium (N/s)
Pu-238	2.50%	2.67E+06	6.68E+04
Pu-239	55.00%	2.30E+01	1.27E+01
Pu-240	24.00%	1.03E+06	2.47E+05
Pu-241	14.00%	4.94E+01	6.92E+00
Pu-242	4.50%	1.73E+06	7.79E+04
Total	100.00%	5.43E+06	3.92E+05

Interview Questions

The following table shows the example questions and inputs for the neutron counter.

Table 3-7. Example of estimates of the three reference points for the total material mass under detection.

Factor	*Point on the detectable mass range*	
	Point	*Value (kg)*
Total mass of the material under detection	M_{low}	1
	M_{bc}	5
	M_{high}	10

The cost of the safeguard for the scenario without proliferator tactic is the cost of different safeguard set-ups that affect the safeguard uncertainty of measurement.

Table 3-8. Example of estimates of the three reference points for the cost of safeguard for no tactic

Tactics	*Safeguard Estimated Cost*	*Value*	*Safeguard modifications (e.g., equipment changes, component additions, quality improvements, software interfaces, etc.)*
No tactic: Uncertainty of Measurement	C_{min}	\$0.05M	Basic He-3 detector tube
	C_{bc}	\$0.2M	Larger detector, charge amplifier
	C_{opt}	\$1M	Multiple highest sensitivity detectors

The cost of the safeguard for the scenario with proliferator tactic is the cost of different safeguard set-ups that affect the proliferator success probability to elude the safeguard for each specific tactic.

Table 3-9. Example of estimates of the three reference points for the cost of safeguard for each tactic

Tactics	*Safeguard Estimated Cost*	*Value*	*Safeguard modifications (e.g., equipment changes, component additions, quality improvements, software interfaces, etc.)*
Tactic A: Dummy material	$C_{A,min}$	\$0.05M	Basic He-3 detector tube
	$C_{A,bc}$	\$0.2M	Larger detector, charge amplifier
	$C_{A,opt}$	\$1M	Multiple highest sensitivity detectors
Tactic B: Compensating material	$C_{B,min}$	\$0.05M	Basic He-3 detector tube
	$C_{B,bc}$	\$0.2M	Larger detector, charge amplifier
	$C_{B,opt}$	\$1M	Multiple highest sensitivity detectors
Tactic C: Hardware modification	$C_{C,min}$	\$0.05M	Basic detector and cable setup
	$C_{C,bc}$	\$0.5M	Detector and cable shielding
	$C_{C,opt}$	\$2M	Movement and tampering sensor
Tactic D: Software manipulation	$C_{D,min}$	\$0.05M	Basic software setup
	$C_{D,bc}$	\$0.1M	Software and data encryption
	$C_{D,opt}$	\$0.5M	Real time authentication and remote central server

Questionnaire

Here are the example of inputs and plots of the questionnaire for a neutron counter.

Question I: The neutron counter uncertainty of measurement

The question in the table is asking for the uncertainty of measurement with 95% level of confidence at three different points of total mass of material under detection (M) and cost of the safeguard (C). The safeguard cost and the material mass reference points are provided in the table both for M and C. The following figure shows the plots of the estimates for a comparison.

Table 3-10. Example of inputs of the uncertainty of measurement as a function of mass and safeguard cost

Safeguard Estimated Cost	Uncertainty of Measurement (%) with 95% confidence level		
	Total Mass M_{low} = 1kg	Total Mass M_{bc} = 5kg	Total Mass M_{high} = 10kg
C_{min} = \$0.05M	10	4	2.5
C_{bc} = \$0.1M	4	2	1.5
C_{opt} = \$1M	2	1	0.75

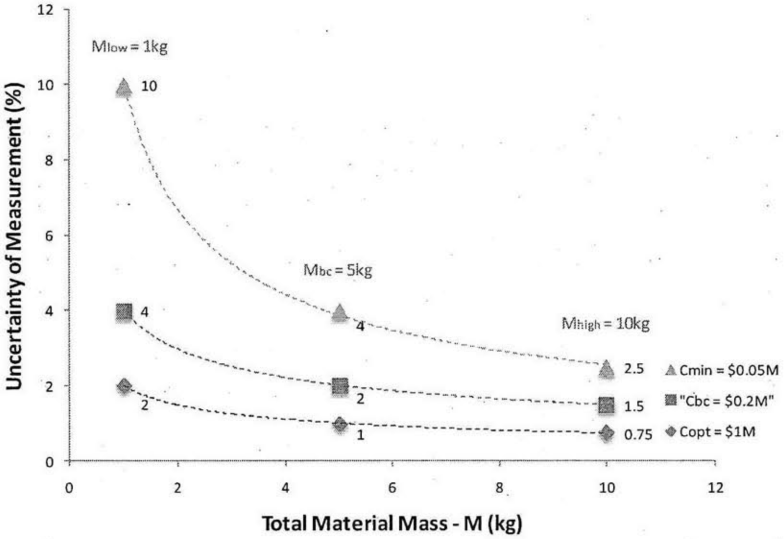


Figure 3-5. Example plot of total material mass versus uncertainty of measurement at three different costs of safeguard setups for a neutron counter.

Question II: Probability that the proliferator tactics will successfully elude the neutron counter

Tactic A: Using Dummy Material

The question in the table is asking for the proliferator success probability point estimate and the error with 95% level of confidence at three different points of the cost of the safeguard. The cost range and the base case estimates are provided in the table. The following figure shows the plots of the estimate as a function of the cost of the safeguard.

Table 3-11. Example of inputs of the proliferator success probabilities as a function of safeguard cost

Safeguard Estimated Cost	Proliferator success probability of tactic A	
	Point Estimate	± Error with 95% Level of Confidence
$C_{A,min}$ = \$0.05M	0.75	0.1
$C_{A,bc}$ = \$0.2M	0.4	0.05
$C_{A,opt}$ = \$1M	0.2	0.02

The expected trend of the proliferator success probability versus the cost of the safeguard is decreasing until it reaches the saturation point where increasing the cost of the safeguard will not anymore decrease the success probability of the proliferator.

Figure 3-6 shows the example plot of proliferator success probabilities versus the cost of the safeguard for different proliferator tactics. This plot shows the cost effectiveness of the set up of the safeguard to prevent the proliferator from eluding the safeguard by each tactic. Note that the actual comparison of the proliferator success probability will include the probability to elude the supporting safeguard, such as surveillance camera, seal, etc., as show in the success tree diagram for the safeguard.

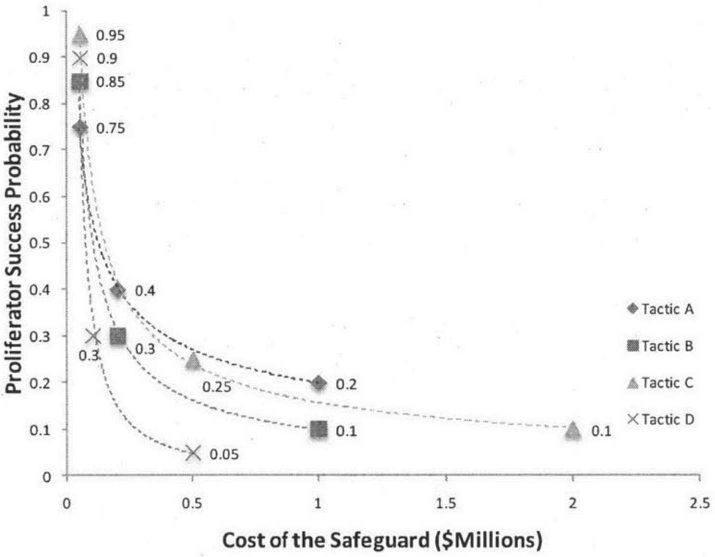


Figure 3-6. Example plot of proliferator success probabilities for different tactics to elude a neutron counter

Then, Figure 3-7 shows the example plot of uncertainty of measurement from different inputs and the aggregated values using the methods discussed in the earlier section.

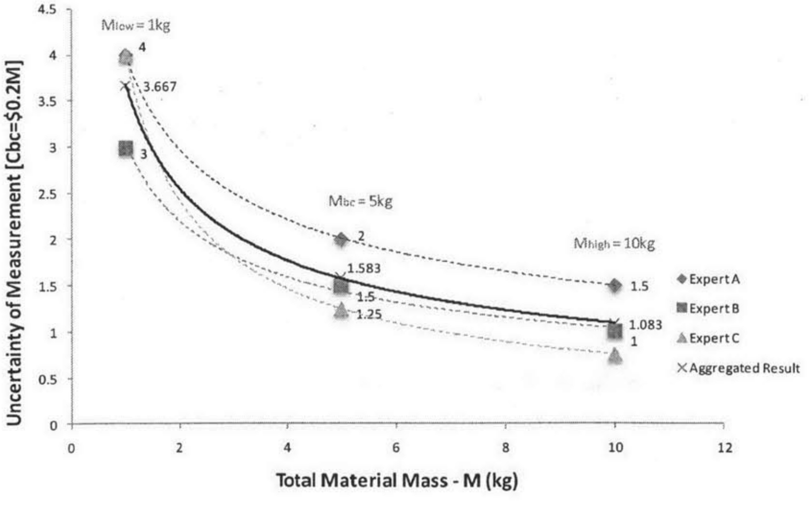


Figure 3-7. Example plot of the aggregated inputs for the uncertainty of measurement at base case NC cost

3.4 Applications of Results from Expert Elicitation

This section contains discussions of the calculations required to convert of the expert elicitation results to be used in success tree analyses and possible applications. The methods of transforming the expert inputs to the probability of the basic events in the success tree are shown in detail.

There are two types of inputs from the expert elicitation. The first one is related to category I questions, which are for the cases when a proliferator does not attempt any concealment tactic. The other is related to category II questions, which are for the cases when a proliferator attempts to use concealment tactics to help elude the safeguard.

1. Uncertainty of Measurement

This input related to the basic event where a proliferator is attempting to elude a safeguard without any concealment tactic. The uncertainty of measurement must be transformed into the safeguard probability of failing to detect a diversion for a given amount of diverted mass.

First, a "measurement" type safeguard, such as a neutron counter for material accountancy, is considered. For the simplest set up, the measurement system consists of a detector and a processing unit. The system is used to count the total radiation from material inside an accountability tank for a certain period of time.

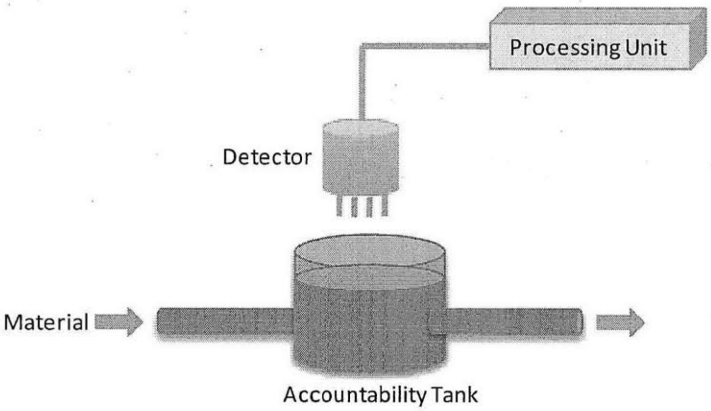


Figure 3-8. "Measurement" type safeguard and material flowing in/out of accountability tank

Let M be the total mass of material inside the accountability tank, and N_M be the number of counts recorded by the measurement system. The relationship between M and N_M is the following.

$$N_M = M \cdot \alpha \cdot f \cdot \varepsilon \cdot T$$

α is the number of activities per unit mass of material

f is the radiation yield per disintegration/fission

ε is the absolute detection efficiency

T is the counting time

Absolute detection efficiency consists of intrinsic efficiency and geometric efficiency. Intrinsic efficiency of the detector is the probability that the detector registers a count when a particle hit the detector. Geometric efficiency is the probability that a particle radiated from the material will reach the detector. Geometric efficiency depends on the relative location of the material to the detector, geometry, and form of the material.

Because of counting statistical fluctuation and other instrumental variations, the value of N_M is normally distributed with standard deviation σ_{NM}, assuming the counting time is long enough.

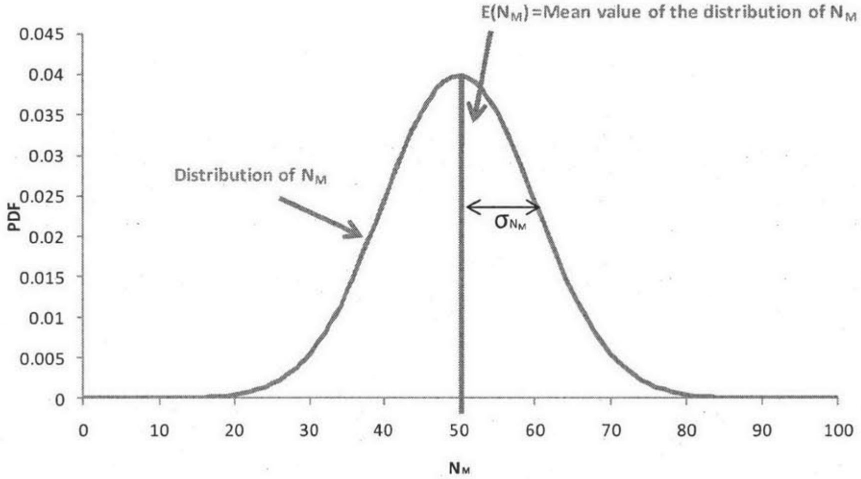


Figure 3-9. PDF Plot of the number of radiation counts from material mass M

Let N_m be the measured number of counts from a measurement, such that $N_m < E(N_M)$. $E(N_M)$ is the expected value or the mean value of N_M. And $\delta_m = E(N_M) - N_m$

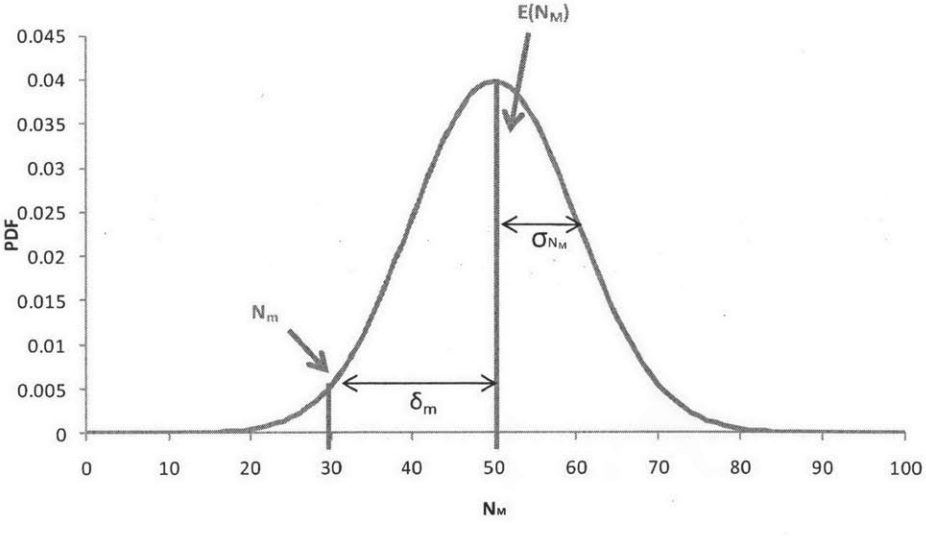


Figure 3-10. PDF Plot of the number of radiation counts from material mass M and a measurement N_m

Using statistical test of significant, the p-value of N_m is the probability that the measurement is outside of $E(N_M) \pm \delta_m$ range. For a normal distribution, this probability can be calculated using the following formula. *erf* is the error function.

$$p(N_m) = 1 - erf(\frac{\delta_m}{\sigma_{N_M}\sqrt{2}})$$

For numerical example, if $E(N_M)$ is 50 counts, and $\sigma_{NM} = 10$, p-value of $N_m = 30$ counts is equal to 0.05, by plugging in $\delta_m = E(N_M) - N_m = 20 = 2\ \sigma_{NM}$ in the above equation.

The significant level, or the critical p-value, is the value used to determine whether the measurement is "statistically significant," or in another word, having a very low probability of occurring given that the assumption that the known information about the system is correct. Let this value be denoted by α. If the p-value of the measurement is less than α, then the result of the measurement is statistically significant, otherwise, it is not. Have a statistically significant means that there is a high probability that the assumption of the system is incorrect. In the context of the study, it means that there is a high chance that the amount of material is not equal to the expected value, and a material diversion has occurred. The popular value of α is 0.05 or 5%.

For example, if α for this case is 0.05 and the measurement result is 10 counts, then the p-value is 0.0027, which is less than 0.05. Therefore, this measurement is statistically significant and indicates that there is a high probability that some material has been diverted.

Then the question is "what is the probability that a diversion of a certain amount of material or more has occurred" for a given result of measurement. For this case, the following figure show the distribution of number of counts when a diversion of M_D amount of material has occurred. Let $D = M - M_D$, and N_D is the record counts for material mass D.

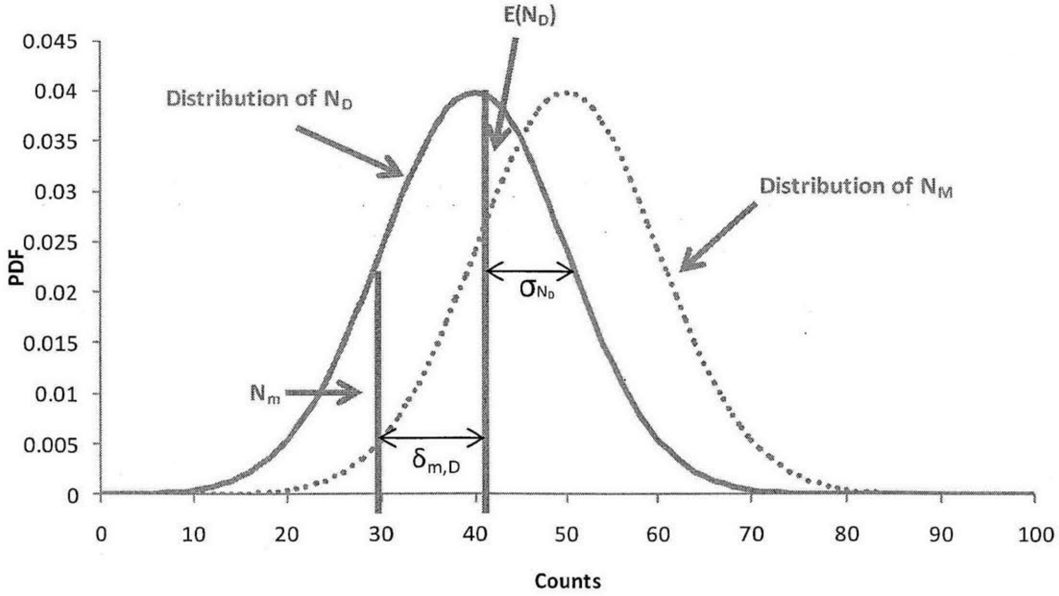


Figure 3-11. PDF Plot of the number of radiation counts from the material when a diversion has occurred

With the same measurement result as before, N_m, the p-value for this case can be calculated. Since $\delta_{m,D}$ is smaller than δ_m, therefore, the p-value is higher, which means that there is higher probability of having a measurement outside of $E(N_D) \pm \delta_{m,D}$ range, assuming that the standard deviation of measurement remain constant.

If consider the cases where more amount of material has been divert, $M_{D'} > M_D$. By following the calculation, the p-value is higher. In another word, there is higher probability of having a measurement of N_m. Therefore, the conclusion can be made that the probability of having M_D amount of material or more diverted is $1 - p(N_D)/2$, only when $N_M < E(N_D)$, for a given result of measurement, N_m.

For example, if $E(N_D) = 40$ counts for the case that M_D amount of material has been diverted, and result of measurement $N_m = 30$ counts, then $\delta_{m,D} = 10 = \sigma_{ND} \approx \sigma_{NM}$. The p-value for this case is 0.32. Therefore, the probability of having a measurement less than 30 counts and more than 50 counts is 32%. Following the above explanation, given the result of measurement N_m, the probability of having M_D or more amount of material diverted is $1 - (0.32/2) = 0.84$, or 84%.

From the above discussion, the probability of having a significant quantity (SQ) or more of material diverted can be derived as a function of the result of measurement. If the goal of the safeguard is to detect a diversion when there is 95% or more chance that a diversion of one SQ amount of material has occurred, then the safeguard should be set to signal an alarm with the measurement is lower than the amount of measurement corresponding to having 95% or more SQ quantity diverted.

Using the prior example, if the number of counts when an SQ amount of material has been diverted is N_{SQ} and $E(N_{SQ}) = 30$ counts. Then the plot of the probability that more than one SQ quantity of material has been diverted versus the result measurement can be calculated.

$$\Pr(M_i > M_{SQ} \mid N_{m,i} < N_{SQ}) = 1 - p(N_{m,i})/2 = erf(\frac{\delta_{m,i,SQ}}{\sigma_{N_{SQ}}\sqrt{2}})/2$$

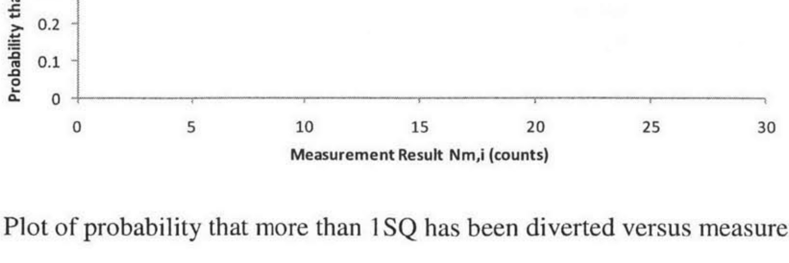


Figure 3-12. PDF Plot of probability that more than 1SQ has been diverted versus measurement result N_m

From the plot, the corresponding point where the probability of more than 1SQ has been diverted is 95%, or 0.95, is when the measurement result is between 13 and 14 counts. Therefore, if the result of a measurement is lower or equal to 13 counts then there is 95% or more chance that 1SQ amount of material has been diverted.

The above discussion provides a method to identify the significant level or the limit of measurement at which a safeguard will signal an alarm. This limit then can be used to derive the probability of detecting a diversion for a given diverted amount per attempt.

Using the prior notations, where a proliferator attempts to divert M_D amount of material from the total mass M, the amount left after the diversion is $D = M - M_D$ and the expected number of counts is $E(N_D)$. The standard deviation of N_D distribution is derived from the expert judgments of the percentage uncertainty of measurement with 95% level of confidence. Since N_D is normally distributed, 95% level of confidence corresponds to 2 standard deviations. Therefore, σ_{ND} is equal to a half of the uncertainty. Let U be the percentage of uncertainty given by the experts, and u be the uncertainty of N_D.

$$u = U \cdot E(N_D)$$

Then,

$$\sigma_{N_D} = \frac{u}{2}$$

If the significant level is 0.05, then the limit in the unit of number of counts is $N_L = E(N_M) - 2\sigma_{NM}$.

Finally, the probability of failing to detect the diversion is the probability that the measurement is higher than the limit value. The p-values in the following equation are for the distribution of N_D.

$$\Pr\text{ (fail to detect a diversion of } M_D) = 1 - \frac{p(N_L)}{2}; \qquad \text{if } N_L \leq E(N_D)$$

$$= \frac{p(N_L)}{2}; \qquad \text{if } N_L > E(N_D)$$

The second type of safeguard is the "detection" type, such as a portal monitor system. The simplest detection system is considered, it contains a detector and a processing unit. The system is used to detect and count the total radiation of interest from a sample or a person going through this detection system for a certain period of time.

The analysis for this type of safeguard is similar to the one in the earlier discussion. However, the number of counts by the detector when there is no material diversion is the counts of background radiation. When there is a diversion attempt, the total amount of radiation is the sum of radiations from the background and the material.

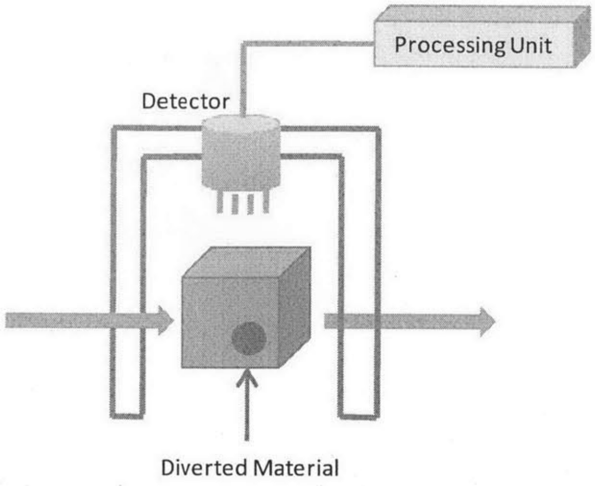


Figure 3-13. "Detection" type safeguard and diverted material going through the detection region

Let N_D be the number of counts for the radiation from diverted material and N_B be the number of counts for the background radiation. Assuming that the background radiation is constant for the period during the calibration and the actual detection, the total number of counts is $N_T = N_B + N_D$.

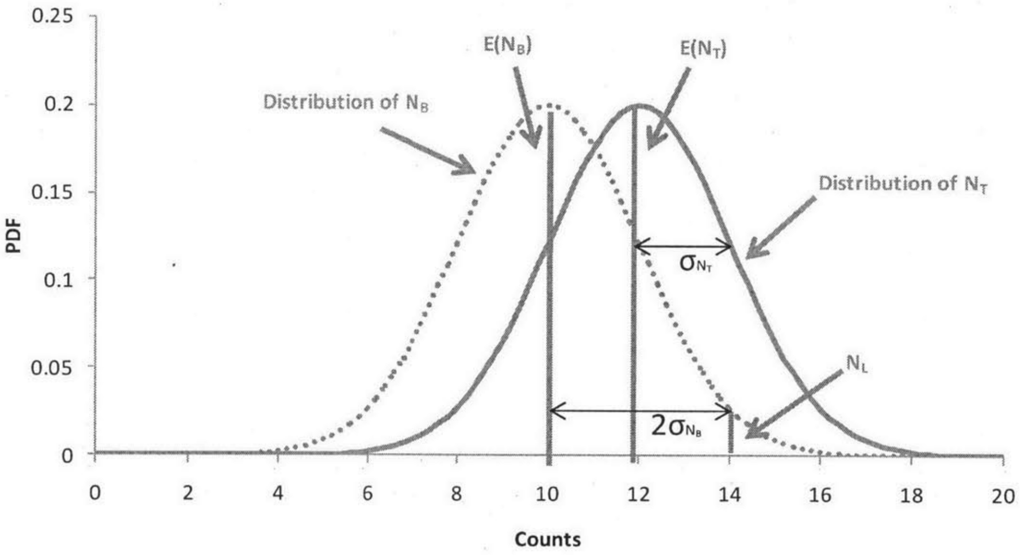


Figure 3-14. PDF Plot of the number of radiation counts from the diverted material and background

The standard deviation of N_T, σ_{NT}, can be approximate from the expert judgments of the uncertainty of measurement with 95% confidence level at the background level of radiation, assuming that N_D is low compared to N_B.

If the significant level is 0.05 then the limit in the unit of number of counts is $N_L = E(N_B) + 2\sigma_{NB}$.

The probability of failing to detect the diversion is the probability that the measurement is lower than the limit value. The p-values in the following equation are for the distribution of N_T.

$$\begin{aligned}
\text{Pr (fail to detect a diversion of } M_D) &= 1 - \frac{p(N_L)}{2}; && \text{if } N_L \geq E(N_T) \\
&= \frac{p(N_L)}{2}; && \text{if } N_L < E(N_T)
\end{aligned}$$

2. Proliferator diversion success probability

This input related to the basic event where a proliferator is attempting to elude a safeguard by using some concealment tactics. Proliferator diversion success probability is already in the form of the basic event probability and does not require any transformation. Depending on tactic choice, this probability depends on the cost of the components of the safeguard that help prevent the tactic to succeed.

Chapter 4 Facility Safeguard Evaluation

For this chapter, the Rokkasho reprocessing plant is used for a demonstration of the procedures and methodology of safeguard scheme evaluation presented in this framework.

4.1 Rokkasho Reprocessing Facility

The Rokkasho reprocessing facility is a nuclear reprocessing plant owned by Japan Nuclear Fuel Limited located in the village of Rokkasho in northeast Aomori Prefecture, Japan. Since this is the only operating commercial reprocessing plant outside of nuclear weapon state, the IAEA has been using this facility as a test site for the advance safeguard instrumentations and schemes.

Table 4-1. Specifications of Reference Industrial-scale Reprocessing Plants in Japan (IAEA 1980)

Topic	Value
Process	Chop/leach solvent extraction
Design capacity	2x3 t/d
Plant availability	200-300 d/a
Commercial program	1000-1500 t U/a
Maximum fuel burnup	40 GW d/t
Fuel cooling time	1 a (minimum)
Mode of operation	Continuous on shift
Spent fuel reception buffer storage	2000 t U
Uranyl nitrate buffer	100 m^3a(at 450 g U/l)
Plutonium nitrate buffer storage	2 m^3 (at 250 g Pu/l)
HA waste concentration storage	3600 m^3 (5 a)
MA aqueous waste storage	10000 m^3 (5 a)
MA organic waste interim storage	350 m^3
Cladding and structural material	0.5 m^3 /t U
Ion exchange resins and iodine absorbers	1.5 m^3/a
Off-gas and exhaust air filter	500 m^3 /a
Pu-contaminated material, engineering wastes and decontamination materials	1 m^3 /t U

Table 4-2 shows the list of different types of material inside the reprocessing facility separated by material balance areas.

Table 4-2. Material flow in each material balance area

MBA1	MBA2	MBA3	MBA4	MBA5
Spent LWR Fuel Assemblies, Chopped, and Solvent	Spent Fuel Solvent, Pu Nitrate, U Nitrate, UO_3	Hulls, Cladding, Waste from Chemical Separation Process and Denitration	Pu Nitrate, U Nitrate, MOX	MOX, UO_3

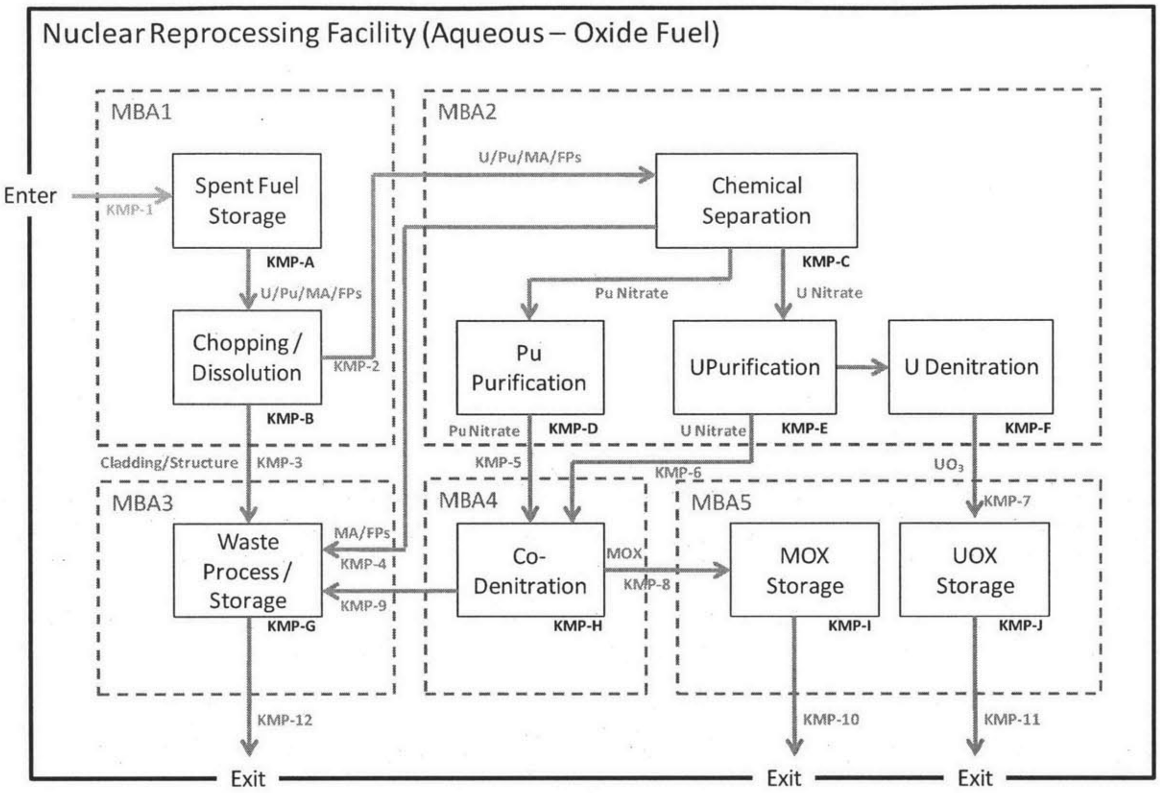


Figure 4-1. Diagram showing the processes and material flow inside Rokkasho reprocessing facility (PNNL 2007)

MBA1 Spent Fuel Storage Area

Material: Spent LWR Fuel

Isotopic Composition of Uranium in 4 Percent Enriched Fresh Fuel and in Spent Light Water Reactor Fuel, Burnup 45 MWd/kgHM, in percentage.

Table 4-3. Isotope composition of fresh and spend fuel (IAEA-TECDOC-1535 2007)

Isotope	Fresh Fuel	Spent Fuel
Trace U	0.04	0.02
U-235	4	0.68
U-236	0	0.52
U-238	96	93.05
Pu isotopes	0	0.99
FP	0	4.62
Non-PU TRU	0	0.095

MBA2 Reprocessing Area

Material: Spent Fuel Solvent, Plutonium Nitrate, Uranium Nitrate

The PUREX (Plutonium Uranium Recovery by EXtraction) solvent extraction process separates the uranium and plutonium from the fission products. After adjustment of the acidity, the resultant aqueous solution is equilibrated with an immiscible solution of tri-n-butyl phosphate (TBP) in refined kerosene. The TBP solution preferentially extracts uranium and plutonium nitrates, leaving fission products and other nitrates in the aqueous phase. Then, chemical conditions are adjusted so that the plutonium and uranium are re-extracted into a fresh aqueous phase. Normally, two solvent extraction cycles are used for the separation; the first removes the fission products from the uranium and plutonium, while the second provides further decontamination. Uranium and plutonium are separated from one another in a similar second extraction operation. The plutonium composition is shown below (IAEA 1980).

Table 4-4. Isotope composition of plutonium in the chemical separation area

Plutonium Isotope	Isotope Percentage
Pu-238	2.5%
Pu239	55%
Pu240	24%
Pu241	14%
Pu242	4.5%

MBA3 Waste Process and Storage Area

Material: Spent High Level Waste (HLW) and Low Level Waste (LLW)

Highly radioactive liquid waste, containing undissolved particles from the head-end process, concentrated fission products, and medium activity liquid waste are received in the waste-treatment area. They are further concentrated by evaporation and may be mixed together prior to being introduced to a vitrification process in which they are mixed into molten glass.

The LLW is the waste from the co-denitration process and it does not contain the radioactive materials, which are fission products and minor actinides.

MBA4 Co-denitration Area

Material: Spent MOX Powder, MOX Canister

Plutonium nitrate and Uranium nitrate are mixed and go through co-denitration to produce mixed oxide (MOX) powder. These powder is then stored in canisters.

MBA5 Product Storage Area

Material: MOX Canister, UOX Bottle

MOX canisters and UOX bottles from earlier process are stored in this area for shipment.

4.2 Safeguard Details of the Facility

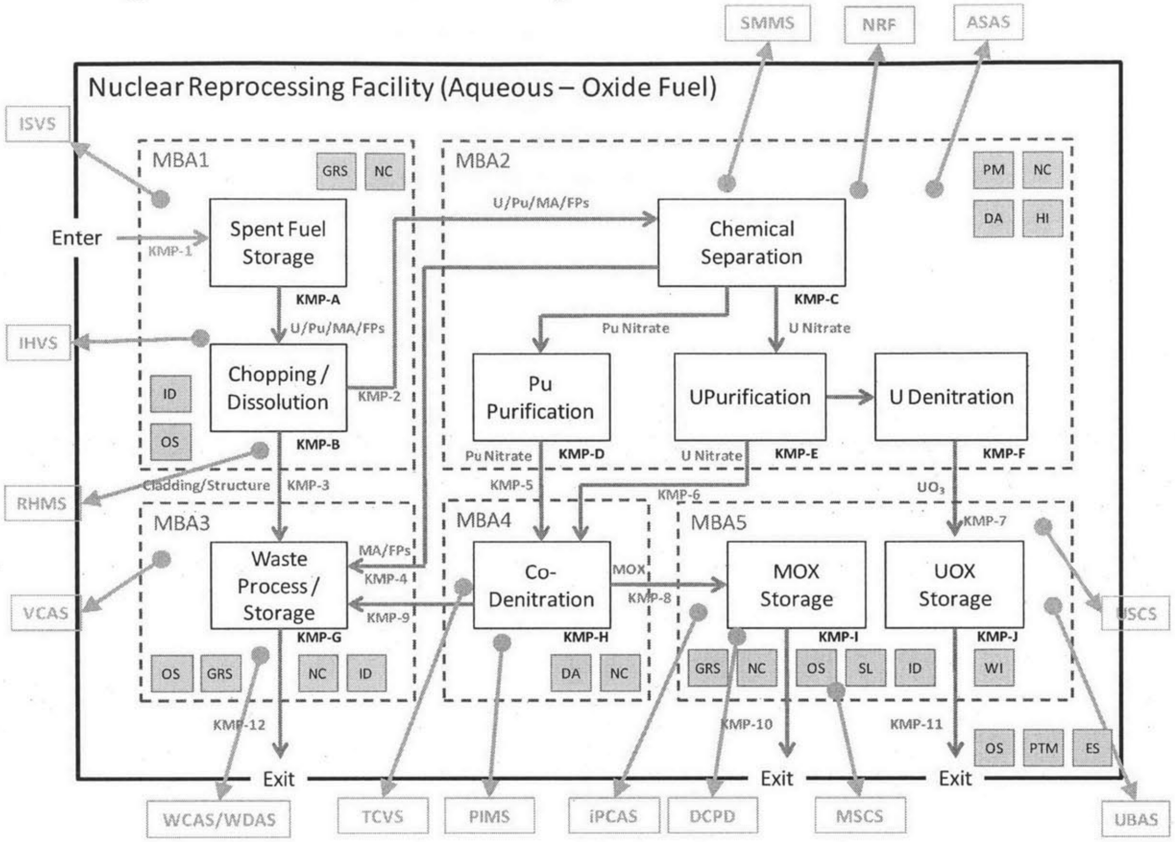


Figure 4-2. Diagram showing the safeguard systems inside Rokkasho reprocessing facility (S. J. Johnson 2001)

The safeguard systems shown in Figure 4-2 and in the following discussions are the actual safeguard systems inside Rokkasho reprocessing facility (PNNL 2007).

MBA1: Feed Storage & Disassembly Area

This is the area where the spent fuel assemblies arrive at the facility. The fuel assemblies are transport in a cask to the spent fuel pool. The transferring process and monitoring the spent fuel pool is done by the Integrated Spent Fuel Verification System (ISVS). Within MBA1, the transferring of the fuel elements to the fuel chopper is monitoring by Integrated Head-end Verification System (IHVS). Then the left over material such as hulls and cladding are verified for nuclear material by Rokkasho Hulls Measurement System (RHMS).

Integrated Spent Fuel Verification System (ISVS)

ISVS verifies the unloading and receipt of spent fuel assemblies and maintains continuity of knowledge of the inventory using aerial surveillance and radiation monitoring of passages.

Components	Type of Safeguard	Location	Material	Functionality
Surveillance Camera	OS	Walls above the storage ponds	Spent fuel assembly	Ensure the surveillance of spent fuel storage
Underwater Camera	OS	Unloading bays	Spent fuel assembly	Ensure that the cask are leaving empty and the radiation detectors are not being shielded
Miniature Gamma Ray and Neutron Detector (MiniGRAND) – Ionization Chamber/Plastic Scintillator	GRS	Unloading canals	Spent fuel assembly	Provide differentiation of whether the spent fuel is going in or out and if it is a shipment of poison rods and channel boxes (only gamma but no neutron)
Miniature Gamma Ray and Neutron Detector (MiniGRAND) – He-3 Tubes	NC	Unloading canals	Spent fuel assembly	Provide differentiation of whether the spent fuel is going in or out and if it is a shipment of poison rods and channel boxes (only gamma but no neutron)

Integrated Head End Verification System (IHVS)

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.

Components	Type of Safeguard	Location	Material	Functionality
Surveillance Camera	OS	Spent fuel mechanical cell lines	Spent fuel assembly	Ensure the surveillance of spent fuel assemblies as they move through the mechanical feeding cells to the shearing cells
ID Camera	ID	Spent fuel mechanical cell lines	Spent fuel assembly	Provide spent fuel IDs as they are brought into feeding cells
Camera Radiation Detector (CRD) – Xenon Ionization Chamber	GRS	Spent fuel mechanical cell lines	Spent fuel assembly	Monitor the passage of the spent fuel assemblies in feeding cells and shearing cells
Camera Radiation Detector (CRD) – 4atm He3 Neutron Detector	NC	Spent fuel mechanical cell lines	Spent fuel assembly	Monitor the passage of the spent fuel assemblies in feeding cells and shearing cells

Rokkasho Hulls Measurement System (RHMS)

RHMS provides semi-quantitative assay of the nuclear material content in the leached hulls and end pieces of the spent fuel assemblies.

Components	Type of Safeguard	Location	Material	Functionality
Neutron Detector	NC	Hulls line	Leached hulls and end pieces	Detects the passive neutrons from curium in the hulls to approximate the material content using Cm/Pu/U ratio in the dissolver solution

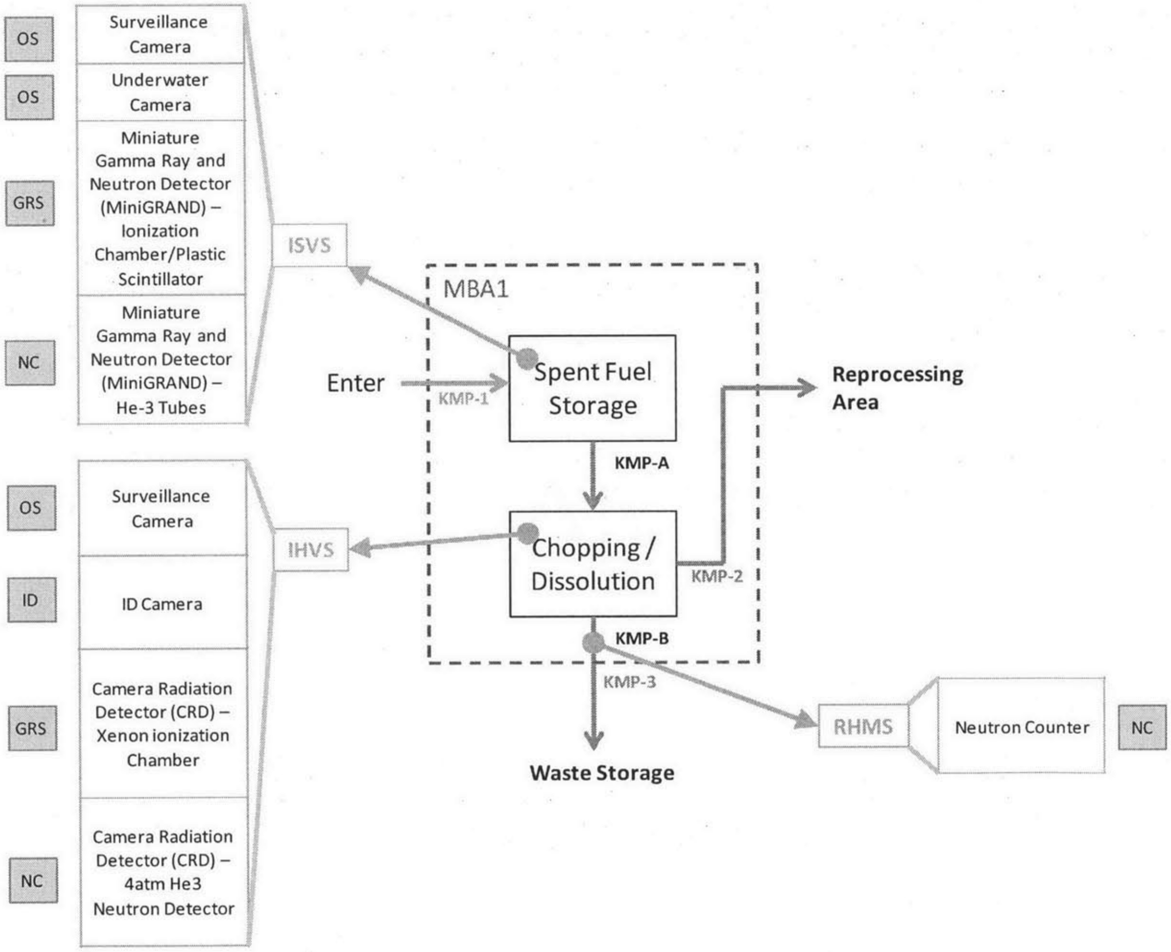

OS
Surveillance Camera
OS
Underwater Camera
GRS
Miniature Gamma Ray and Neutron Detector (MiniGRAND) – Ionization Chamber/Plastic Scintillator
NC
Miniature Gamma Ray and Neutron Detector (MiniGRAND) – He-3 Tubes
ISVS
MBA1
Enter
KMP-1
Spent Fuel Storage
KMP-A
Reprocessing Area
OS
Surveillance Camera
ID
ID Camera
GRS
Camera Radiation Detector (CRD) – Xenon ionization Chamber
NC
Camera Radiation Detector (CRD) – 4atm He3 Neutron Detector
IHVS
Chopping / Dissolution
KMP-2
KMP-B
KMP-3
Waste Storage
RHMS
Neutron Counter
NC

Figure 4-3. Diagram showing the safeguard systems inside MBA1

MBA2: Reprocessing Area

In this area, the material solution from MBA1 is verified by the Solution Measurement and Monitoring System (SMMS), which is the main system for verifying solution level, volume and density in most of the solution processes in the MBA2. Both the waste stream and Plutonium Nitrate stream are randomly verified by Automatic Sampling Authentication System (ASAS)

In the Rokkasho Reprocessing Plant, the separated uranium is purified and concentrated, and then approximately 99% of the uranyl nitrate is transferred to a conversion process – all within MBA2. After conversion to UO_3, it is transferred to a product- storage area in MBA5. The remaining uranyl nitrate is routed directly to the co-denitration process, which is the uranium- plutonium mixed-oxide (MOX) powder-production process in MBA4.

Solution Measurement and Monitoring System (SMMS)

SMMS is an in-tank measurement system used for the determination of solution level, volume and density. The technology is based on the bubbling of a controlled stream of gas through dip tubes installed at various depths within the solution and in the vapor space above the solution. The solution measurement data is obtained by determining the differential pressure between dip tubes and a specified time, and applying a tank calibration equation.

There are two types of SMMS. Type 1(SMMS-1) is used to measure and monitor the solution levels, volumes and densities in the most safeguards significant vessels in the main process. SMMS-1 uses high-accuracy, independent, and authenticated pressure measurement devices in the 12 most important process vessels. A volume measurement uncertainty of ±0.05% was achieved during commissioning. Type 2(SMMS-2) is used to measure and monitor the levels, volumes and densities in vessels of less safeguards significance in the main process. SMMS-2 uses mainly industrial pressure measurement devices in 80 process vessels. These can be pressure or temperature sensors, as well as neutron detectors mounted on the extractors in the main process.

The data collected from the detector are sent to the main processing unit which uses Solution Monitoring Software (SMS). SMS is a highly developed piece of software used routinely by the IAEA inspectors in the on-site inspector office, and includes configuration, preprocessing and evaluation functions. It automatically analyzes the data from the sensors (pressure, temperature, neutron detectors).

Components	Type of Safeguard	Location	Material	Functionality
Electromanometer	PM	Process vessels / Accountancy tanks	Material Solution	Measure and monitor solution levels, volume, and density
Temperature Sensor	HI	Process vessels / Accountancy tanks	Material Solution	Measure material solution temperature for accountancy
Neutron Detector	NC	Process vessels / Accountancy tanks	Material Solution	Measure material solution neutron radiation for accountancy

Automatic Sampling Authentication System (ASAS)

ASAS is an automatic system that authenticates the random taking and transferring of the sample from operator process sampling benches to the joint use of IAES/State Inspector On-site Laboratory (OSL). The sample of plutonium nitrate going to MBA4 is verified via Hybrid K-Edge Densitometry (HKED). On the other hand, the sample of High Active Liquid Waste (HALW) from the chemical separation process is analyzed via Pu(VI) Spectrophotometric method for plutonium and Isotope Dilution Mass Spectroscopy (IDMS) for uranium.

Components	Type of Safeguard	Location	Material	Functionality
Hybrid K-Edge Densitometry (HKED)	DA	Pu Nitrate Stream to MBA4	Pu Nitrate	Destructive analysis to verify the amount and isotope composition of plutonium in the solvent stream
Pu(VI) Spectrophotometric	DA	Waste Stream	High Active Liquid Waste	Destructive analysis to verify the amount of plutonium in the waste stream
Isotope Dilution Mass Spectroscopy (IDMS)	DA	Waste Stream	High Active Liquid Waste	Destructive analysis to verify the amount of uranium in the waste stream

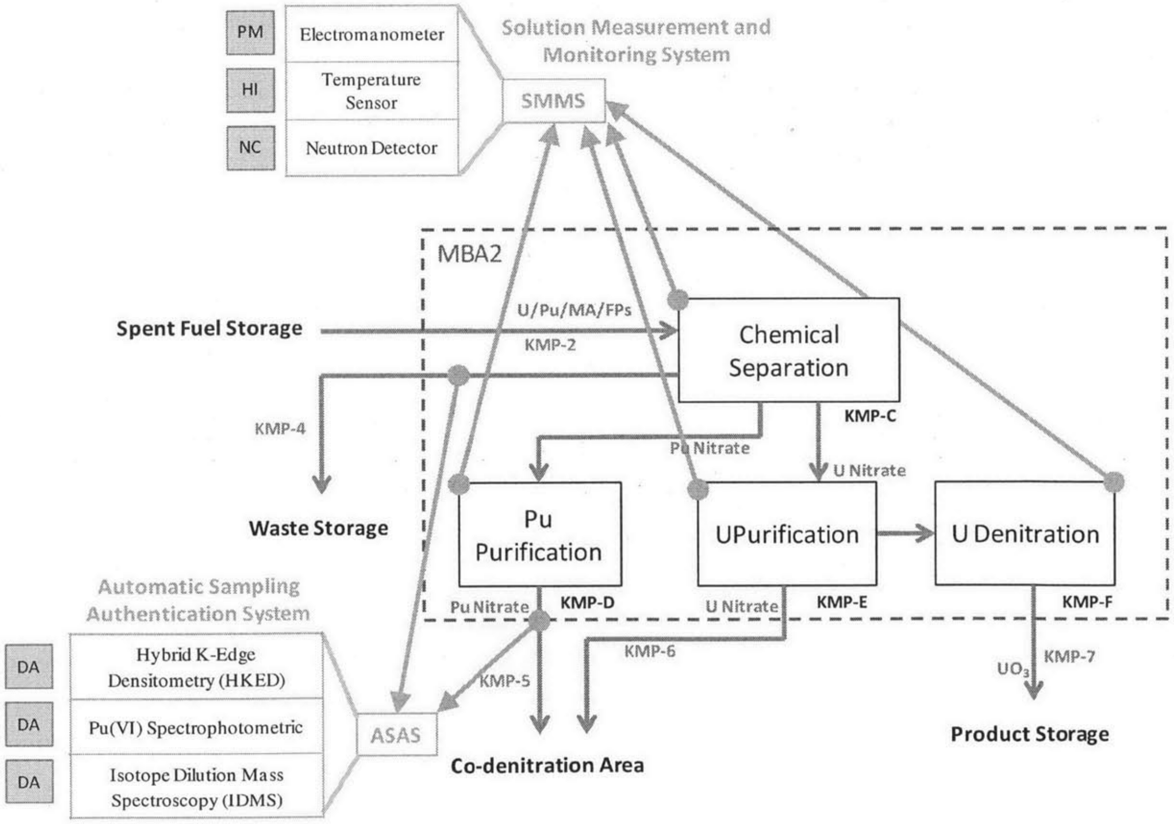


Figure 4-4. Diagram showing the safeguard systems inside MBA2

MBA3: Waste Storage Area

Highly radioactive liquid waste, containing undissolved particles from the head-end process, concentrated fission products, and medium activity liquid waste are received in the waste-treatment area. They are further concentrated by evaporation and may be mixed together prior to being introduced to a vitrification process in which they are mixed into molten glass. After accountancy measurements have been completed for consideration of termination of safeguards, canisters of solidified vitrified waste are transferred to a long-term storage area.

The total quantity of plutonium going into waste in a reprocessing plant is typically less that 0.5 percent of the total throughput, with concentrations in the milligram per liter (parts per million) range.

Vitrified Canister Assay System (VCAS)

VCAS provides semi-quantitative assay of the nuclear material content in the vitrified waste before being transferred to measured discards for termination of safeguards, and verifies that the nuclear material has been effectively vitrified and practically irretrievable.

Components	Type of Safeguard	Location	Material	Functionality
Fission Chambers	NC	After Vitrification Cell	Vitrified Waste Canister	Verify the amount of Pu and U from collecting neutron emitted by Curium-244 calculated with the composition ratio and the ratio of thermal/fast neutrons provides verification that the canister does not contain aqueous solution
Ionization Chambers	GRS	Route to and from the Vitrification Cell	Waste Canister	Confirm the direction of transferring of the canister
Surveillance Camera	OS	Route to and from the Vitrification Cell	Waste Canister	Ensure the surveillance of the waste canister transfer to and from the vitrification cell
ID Camera	ID	Route to and from the Vitrification Cell	Waste Canister	Provide ID of the waste canister

Waste Crate Assay System (WCAS)

WCAS provides semi-quantitative assay of the nuclear material content in the low active waste crates.

Components	Type of Safeguard	Location	Material	Functionality
He-3 Detector*	NC	Waste Storage	Waste Crate	Verify the amount of Pu and U from collecting neutron emitted by Curium-244 calculated with the composition ratio based on the building origin of the waste crate
Surveillance Camera	OS	Waste Storage	Waste Crate	Ensure the surveillance of the waste crate transfer
ID Camera	ID	Waste Storage	Waste Crate	Provide ID of the waste crate

He-3 Detector*: The detectors are distributed in different arrays (thermal, fast, shielded, and not shielded). This distribution allows for the estimation of the thermal effect of the matrix of the waste, and the measurement of wastes containing fission products.

Waste Drum Assay System (WDAS)

WDAS provides semi-quantitative assay of the nuclear material content in the Low Active Waste Drums from the mixed oxide (MOX) conversion process, having no fission products.

The system is based on the IAEA standard gamma spectrometry verification system (HRGS with portable Inspector Multichannel Analyzer). The system includes a high-resolution germanium detector, mounted on a trolley; a portable IMCA; and FRAM and ISOCS software.

Measurement time is around 15 minutes and the expected detection limit is below 1 g of plutonium.

Components	Type of Safeguard	Location	Material	Functionality
HPGe Detector	GRS	Low Active Waste Drums	Waste Crate	Verify the material content in the Low Active Waste Drums from MOX Conversion Process

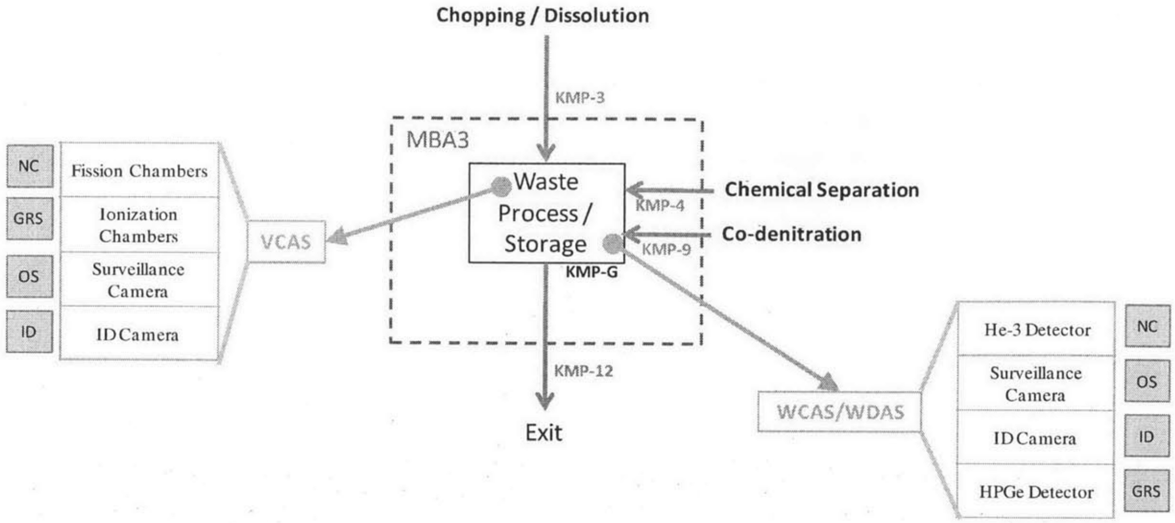


Figure 4-5. Diagram showing the safeguard systems inside MBA3

MBA4: Co-Denitration Area

The process of producing uranium-plutonium mixed-oxide powder at the Rokkasho Reprocessing Plant starts with the mixing of uranyl and plutonium-nitrate solutions. The resulting mixture is dried and calcined to produce oxide powder that is then milled to a uniform particle size. Processes used in other countries convert the uranium and plutonium solutions to oxide powders separately prior to mixing. The ASAS takes the solution and power sample for a verification by destructive analysis as explained in MBA3 section.

Plutonium Inventory Measurement System (PIMS)

PIMS provides continuous monitoring of the flow of MOX powder and measurement of plutonium in the glove boxes through the process lines to ensure that the operations are as declared.

Up to 8 detectors/amplifier units are connected to a "hub unit." There are 30 hubs linked by a high-speed fiber optic loop to the data acquisition computer (DAC) which timestamps the data. The DAC calculates the count rate information and transmits that data to a data processing computer (DPC), which calculates the plutonium and uranium distribution throughout the glove boxes.

Components	Type of Safeguard	Location	Material	Functionality
Helium-3 Neutron Detector	NC	MOX Process Glove Boxes	MOX Powder	Monitor plutonium and uranium distribution throughout the gloved boxes and provide the total inventory using isotopic composition from the feed solution

Temporary Canister Verification System (TCVS)

TCVS provides inventory measurements of the plutonium in the MOX Temporary Canister Storage. The system is designed to determine the number of MOX temporary containers that are present "left," "mid," and "right" and the amount of plutonium mass by "**known alpha**" analysis in the 3 storage pits in each glove box of lines A and B. The isotopic composition is provided by the operator, and later verified by comparison to analyses of samples taken from the solution feed.

Components	Type of Safeguard	Location	Material	Functionality
Neutron coincidence based system (He-3 detectors)	NC	MOX Temporary Canister Storage	MOX Powder	Monitor plutonium in the MOX temporary canister storage

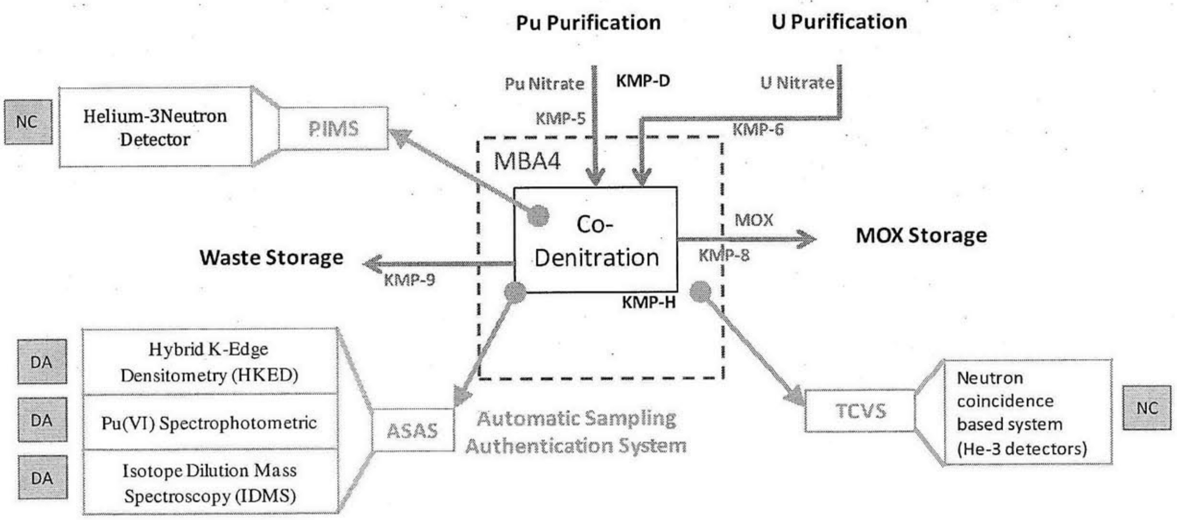

Pu Purification
U Purification
Pu Nitrate
KMP-D
U Nitrate
KMP-5
KMP-6
NC
Helium-3Neutron Detector
PIMS
MBA4
Co-Denitration
MOX
MOX Storage
KMP-8
Waste Storage
KMP-9
KMP-H
DA
Hybrid K-Edge Densitometry (HKED)
DA
Pu(VI) Spectrophotometric
DA
Isotope Dilution Mass Spectroscopy (IDMS)
ASAS
Automatic Sampling Authentication System
TCVS
Neutron coincidence based system (He-3 detectors)
NC

Figure 4-6. Diagram showing the safeguard systems inside MBA4

MBA5: Product Storage Area

In the Rokkasho Reprocessing Plant, canisters of uranium-oxide product are received for storage from the Conversion Process in MBA2 and canisters of MOX product are received from the MOX conversion process in MBA4.

Since this MBA is a storage area containing previously verified containers of product material, there is no need for new measurements. The integrity of the measurements performed in MBA4 is maintained by surveillance and radiation monitoring systems to detect movements of containers and materials within and out of the facility. In other plants, containers used for long-term storage could be sealed with tamper- indicating seals.

Uranium Bottle Verification System (UBVS)

UBVS verifies the transfer of the UO3 product before it is placed under C/S in the UO3 product storage. It comprises of CdZnTe detector connected to a standard IMCA with MGAU software (IMCC), rack (provided by the operator) for holding the bottle during measurement, and flat weighing scale.

After weighing, the operator stores the UO_3 bottles in one of the storage bays. These bays are under Uranium Storage Containment and Surveillance (USCS) surveillance. Periodically, and after a sufficient number of bottles have been produced and stored, an IAEA verification is scheduled.

Components	Type of Safeguard	Location	Material	Functionality
CdZnTe Detector	GRS	Before UO_3 Product Storage	UO_3 Bottle	Verify UO_3 enrichment before it is placed in the product storage
Flat Weighing Scale	WI	Before UO_3 Product Storage	UO_3 Bottle	Verify UO_3 bottle weight before it is placed in the product storage

Uranium Storage Containment and Surveillance (USCS)

USCS applies dual C/S on the uranium product storage, in order to reduce or eliminate the requirements for re-verification of UO3 bottles at the PIV.

Components	Type of Safeguard	Location	Material	Functionality
Surveillance Camera	OS	Entrance of UO_3 Storage Bay	UO_3 Bottle	Ensure the surveillance of UO_3 bottles from the exit of the measurement room to the entrance of each storage bay
Metal Seal	SL	Entrance of UO_3 Storage Bay	UO_3 Bottle	Seal is applied on the transfer machine rail when a storage bay is full or no longer in use

Improved Plutonium Canister Assay System (iPCAS)

iPCAS provides quantitative verification of the MOX product in canisters, before they are placed in the MOX storage under dual containment and surveillance (C/S).

Components	Type of Safeguard	Location	Material	Functionality
Array of He-3 Tubes*	NC	Before MOX Product Storage	MOX Canister	Verify the quantity of nuclear material using isotopic composition of MOX product
HPGe detector	GRS	Before MOX Product Storage	MOX Canister	Verify the isotopic composition of MOX product
ID Camera	ID	Before MOX Product Storage	MOX Canister	Provide MOX canister ID
Precision Load Cell	WI	Before MOX Product Storage	MOX Canister	Verify the weight of the MOX canister. IPCL has accuracy better than ±0.042%.

He-3 tubes*: 2 concentric arrays of helium-3 tubes, one under-moderated, the other over-moderated, provide correction for the moisture content.

Directional Canister Passage Detectors (DCPD)

DCPD monitors the transfer of the MOX product canisters, after they have been verified with the iPCAS and until they reach the MOX storage where they are put under dual C/S.

Components	Type of Safeguard	Location	Material	Functionality
Neutron Detector	NC	Path from iPCAS to the MOX Storage	MOX Canister	Verify nuclear material inside MOX canister before it is placed in the storage
Surveillance Camera	OS	Path from iPCAS to the MOX Storage	MOX Canister	Provide the surveillance of MOX canister transfer carts in the corridors leading to each of the MOX storages

MOX Storage C/S System (MSCS)

MSCS applies dual C/S on the MOX product storage area after verification by iPCAS and transfer under DCPD monitoring, in order to reduce or eliminate re-verification at the PIV.

Components	Type of Safeguard	Location	Material	Functionality
Surveillance Camera	OS	Above Storage Pits and Cart Unloading Position	MOX Canister	Ensure the surveillance of MOX canister in the storage pits
Metal Seal	SL	Transfer Cart Door	MOX Canister	Seal is applied to the transfer cart back door
Neutron Detector	NC	Transfer Cart Unloading Position	MOX Canister	Verify nuclear material in MOX canister before it is unloaded into the storage
ID Camera	ID	Transfer Cart Unloading Position	MOX Canister	Provide MOX canister ID

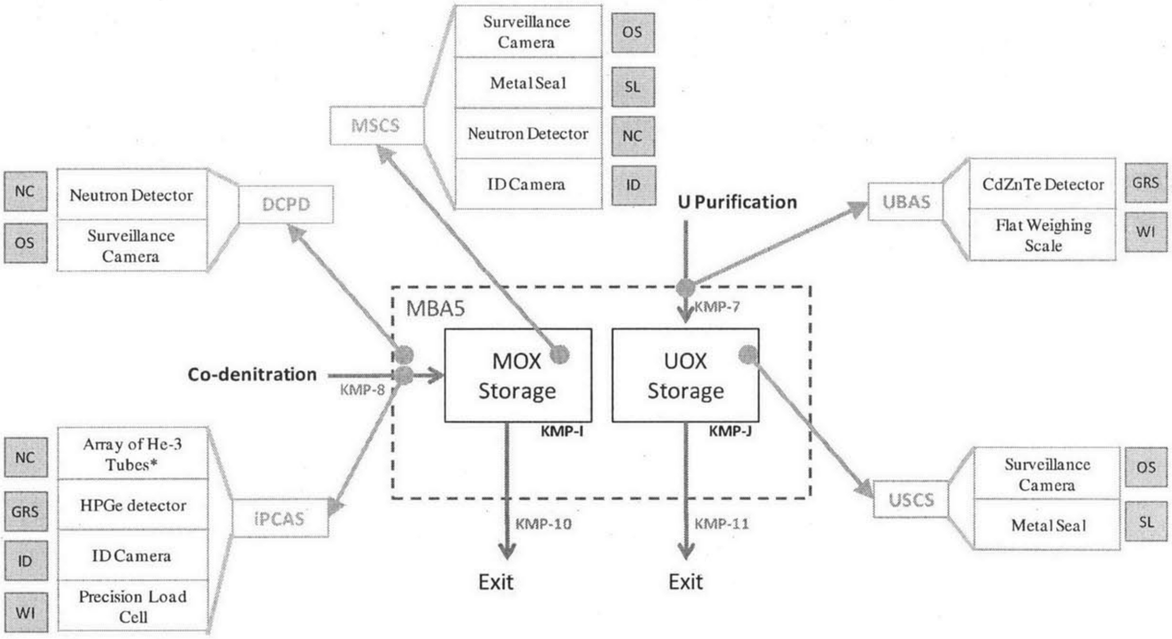


Figure 4-7. Diagram showing the safeguard systems inside MBA5

4.3 Diversion Scenarios

After the safeguard scheme for each material balance area has been identified, then the list of all of the possible diversion scenarios can be derived by checking the key measurement points inside the facility.

For a proliferator to succeed diverting SNM, the following must be accomplished.

1. Remove the material from the process without detection
2. Take the diverted material out of the facility

In the following section, the possible diversion scenarios in each MBA are identified along with the type material being diverted and the safeguard in place to detect these diversions. All of the key measurement points are considered. Each diversion will be given specific diversion scenario ID for use in analyses following this section. The diagram helps providing the clarification of where the diversion scenarios can occur.

Action 1: Obtain material within the facility

For this action, there are two types of methods that the proliferator can do.

1. Direct diversion of material from a specific location in the facility
2. Indirect diversion where the proliferator modify the facility processes in order to redirect the flow of material in the facility to the location where diversion is easier

The first method can be done at all of the processes and transfer points inside the facilities depending on the accessibility of the location of the process. The second method must be done at the processes where there is a change of form of the material of there are more than one different streams of products out of the processes.

MBA1

This is the first area of the reprocessing facility. The material in this area is the spent fuel assemblies, which contain radioactive materials. Therefore, these materials are more difficult for the proliferator to handle. Also the spent fuel assemblies can be easily counted, thus the proliferator is required to use more sophisticated tactics in order to divert these fuel assemblies. For the location options, the proliferator can choose to divert the material during the transfer and storage in the spent fuel pool. One additional tactic that can be done is to modify the dissolution process or leave some of the fuel assemblies out of the dissolution process to send extra amount of spent fuel down the waste stream and then make the diversion attempt there.

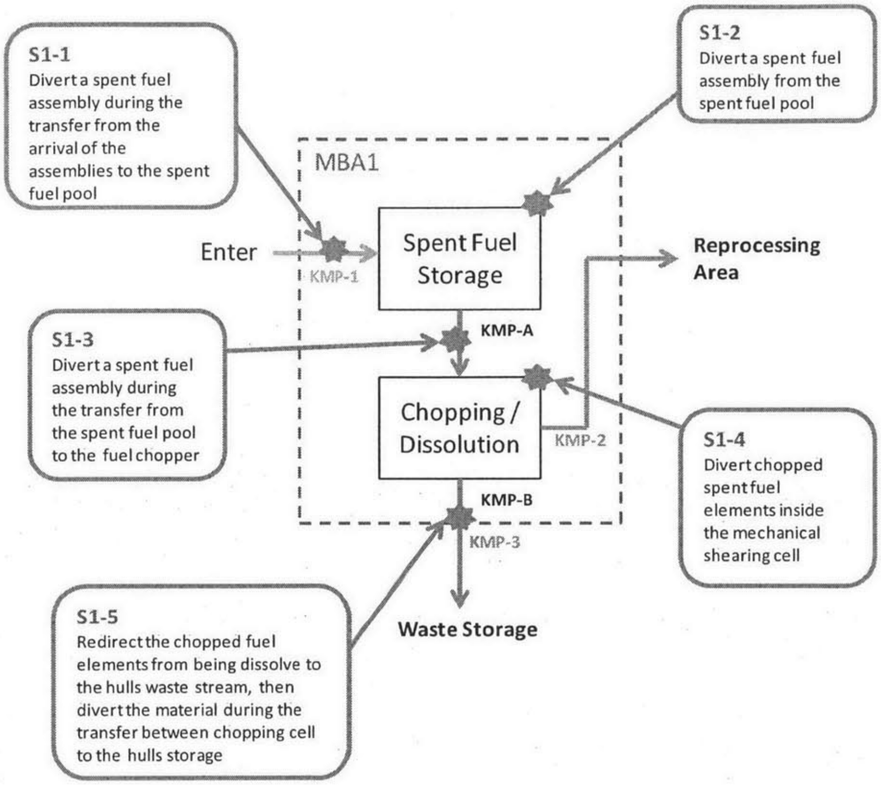

S1-1
Divert a spent fuel assembly during the transfer from the arrival of the assemblies to the spent fuel pool
S1-2
Divert a spent fuel assembly from the spent fuel pool
MBA1
Enter
KMP-1
Spent Fuel Storage
Reprocessing Area
KMP-A
S1-3
Divert a spent fuel assembly during the transfer from the spent fuel pool to the fuel chopper
Chopping / Dissolution
KMP-2
S1-4
Divert chopped spent fuel elements inside the mechanical shearing cell
KMP-B
KMP-3
S1-5
Redirect the chopped fuel elements from being dissolve to the hulls waste stream, then divert the material during the transfer between chopping cell to the hulls storage
Waste Storage

Figure 4-8. Diagram showing the possible diversion scenarios in MBA1

Table 4-5. List of possible material diversion scenarios in MBA1

Scenario ID	Scenario	Material	Preventing Safeguards
S1-1	Divert a spent fuel assembly during the transfer from the arrival of the assemblies to the spent fuel pool	Spent fuel assembly	Surveillance Camera (ISVS – OS) Miniature Gamma Ray and Neutron Detector (ISVS – GRS/NC)
S1-2	Divert a spent fuel assembly from the spent fuel pool	Spent fuel assembly	Surveillance Camera (ISVS – OS) Under Water Camera (ISVS – OS) Miniature Gamma Ray and Neutron Detector (ISVS – GRS/NC)
S1-3	Divert a spent fuel assembly during the transfer from the spent fuel pool to the fuel chopper	Spent fuel assembly	Surveillance Camera (IHVS –OS) ID Camera (IHVS – ID) Camera Radiation Detector (CRD) (IHVS – GRS/NC)
S1-4	Divert chopped spent fuel elements inside the mechanical shearing cell	Chopped spent fuel element	Surveillance Camera (IHVS –OS) Camera Radiation Detector (CRD) (IHVS – GRS/NC)
S1-5	Redirect the chopped fuel elements from being dissolve to the hulls waste stream, then divert the material during the transfer between chopping cell to the hulls storage	Chopped spent fuel element	Surveillance Camera (IHVS –OS) Neutron Detector (RHMS – NC)

MBA2

This is the main process of the facility and since the material inside this MBA is in form of liquid, it is easier for the proliferator to divert at any desired amount. After the separation process, the products are in the form of plutonium and uranium nitrate, which are easier to handle and more attractive in term of nuclear weapon construction.

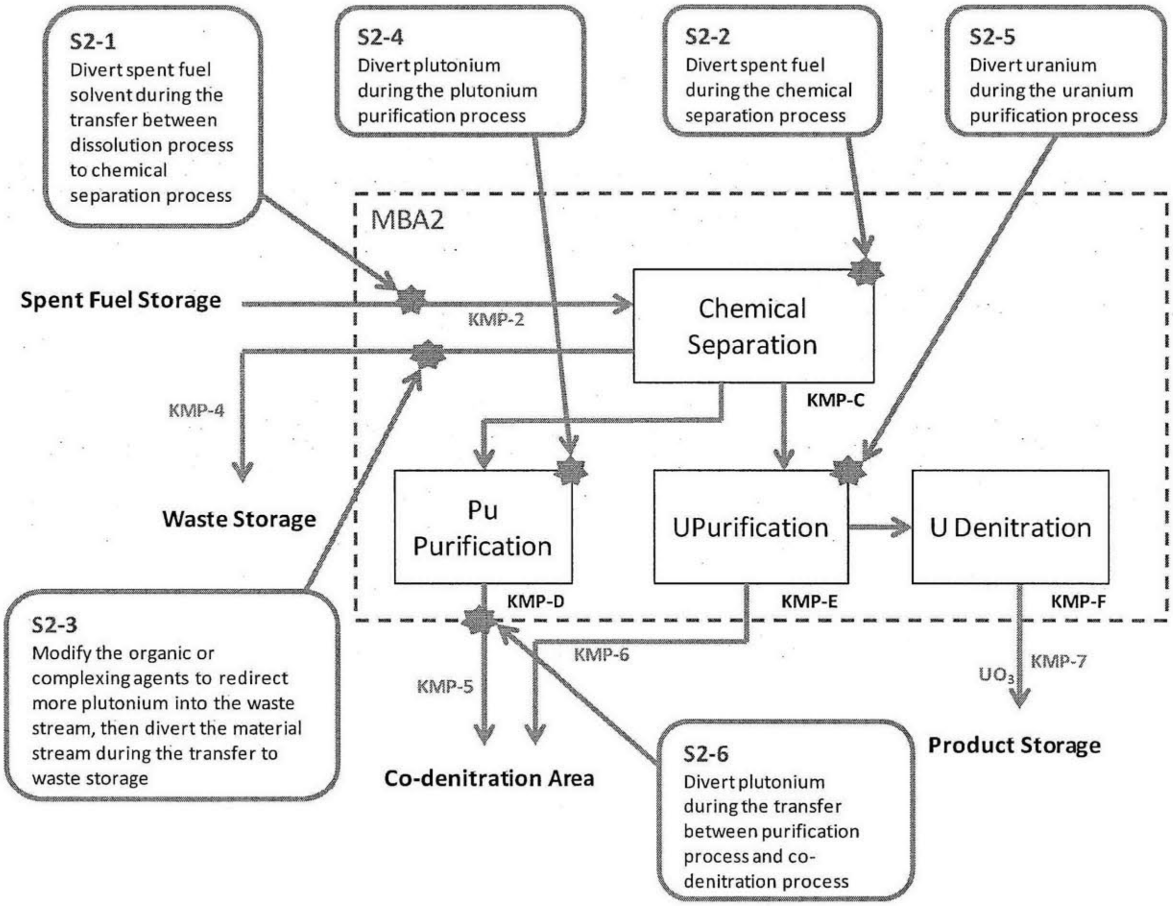

S2-1
Divert spent fuel solvent during the transfer between dissolution process to chemical separation process
S2-4
Divert plutonium during the plutonium purification process
S2-2
Divert spent fuel during the chemical separation process
S2-5
Divert uranium during the uranium purification process
MBA2
Spent Fuel Storage
KMP-2
Chemical Separation
KMP-4
KMP-C
Waste Storage
Pu Purification
UPurification
U Denitration
KMP-D
KMP-E
KMP-F
S2-3
Modify the organic or complexing agents to redirect more plutonium into the waste stream, then divert the material stream during the transfer to waste storage
KMP-6
KMP-5
UO_3
KMP-7
Product Storage
Co-denitration Area
S2-6
Divert plutonium during the transfer between purification process and co-denitration process

Figure 4-9. Diagram showing the possible diversion scenarios in MBA2

Table 4-6. List of possible material diversion scenarios in MBA2

Scenario ID	Scenario	Material	Preventing Safeguards
S2-1	Divert spent fuel solvent during the transfer between dissolution process to chemical separation process	Spent fuel solvent	Electromanometer (SMMS – PM) Temperature Sensor (SMMS –HI) Neutron Detector (SMMS – NC)
S2-2	Divert spent fuel during the chemical separation process	Spent fuel solvent	Electromanometer (SMMS – PM) Temperature Sensor (SMMS –HI) Neutron Detector (SMMS – NC)

Scenario ID	Scenario	Material	Preventing Safeguards
S2-3	Modify the organic or complexing agents to redirect more plutonium into the waste stream, then divert the material stream during the transfer to waste storage	Pu Nitrate in waste stream (MA, FPs)	Electromanometer (SMMS – PM) Temperature Sensor (SMMS –HI) Neutron Detector (SMMS – NC) Pu(VI) Spectrophotometric (ASAS – DA)
S2-4	Divert plutonium during the plutonium purification process	Pu Nitrate	Electromanometer (SMMS – PM) Temperature Sensor (SMMS –HI) Neutron Detector (SMMS – NC) Hybrid K-Edge Densitometry (ASAS – DA)
S2-5	Divert uranium during the uranium purification process	U Nitrate	Electromanometer (SMMS – PM) Temperature Sensor (SMMS –HI)
S2-6	Divert plutonium during the transfer between purification process and co-denitration process	Pu Nitrate	Electromanometer (SMMS – PM) Temperature Sensor (SMMS –HI) Neutron Detector (SMMS – NC) Hybrid K-Edge Densitometry (ASAS – DA)

MBA3

This MBA contains the waste processes and storage. The materials in here are mostly structure/cladding and waste from the separation processes. This is the least attractive place for a diversion unless the proliferator modifies the process to divert more plutonium into the waste stream.

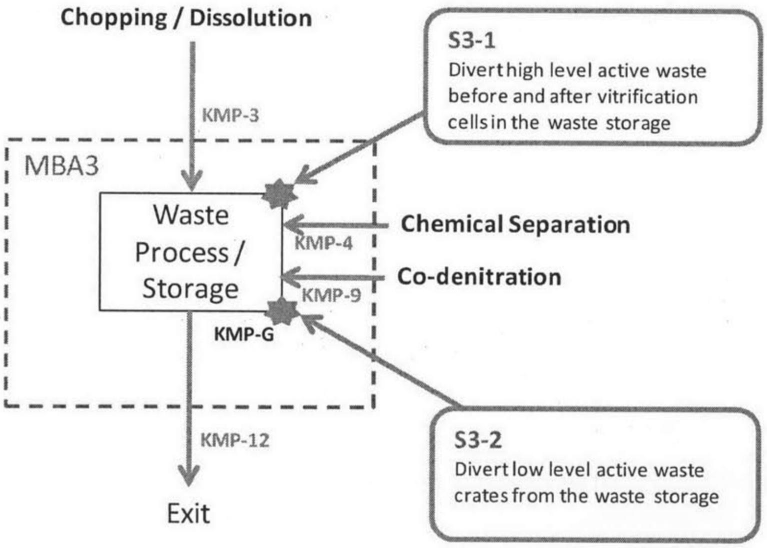

Chopping / Dissolution
KMP-3
MBA3
Waste Process / Storage
KMP-4
KMP-9
KMP-G
KMP-12
Exit
Chemical Separation
Co-denitration
S3-1
Divert high level active waste before and after vitrification cells in the waste storage
S3-2
Divert low level active waste crates from the waste storage

Figure 4-10. Diagram showing the possible diversion scenarios in MBA3

Table 4-7. List of possible material diversion scenarios in MBA3

Scenario ID	Scenario	Material	Preventing Safeguards
S3-1	Divert high level active waste before and after vitrification cells in the waste storage	High level active waste	Fission Chambers (VCAS – NC) Ionization Chambers (VCAS – GRS) Surveillance Camera (VCAS – OS) ID Camera (VCAS – ID)
S3-2	Divert low level active waste crates from the waste storage	Low level active waste	He-3 Detector (WCAS – NC) Surveillance Camera (WCAS – OS) ID Camera (WCAS – ID) HPGe Detector (WDAS – GRS)

MBA4

This MBA contains the co-denitration process to create the MOX fuel. There are various processes that change the form of the material and combining plutonium and uranium from different stream. This provides an opportunity for a diversion, since the uncertainty for material accountancy will be high.

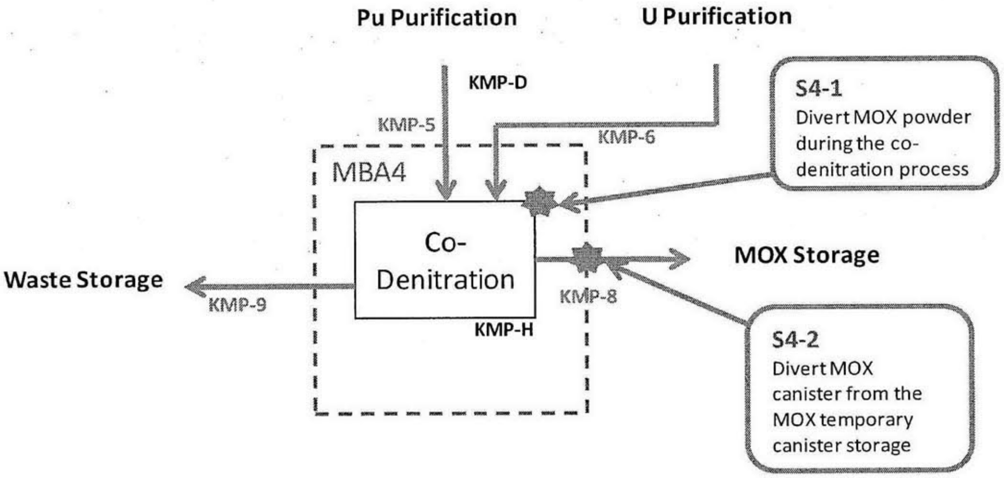

Pu Purification
U Purification
KMP-D
KMP-5
KMP-6
MBA4
Co-Denitration
Waste Storage
KMP-9
KMP-H
KMP-8
MOX Storage
S4-1
Divert MOX powder during the co-denitration process
S4-2
Divert MOX canister from the MOX temporary canister storage

Figure 4-11. Diagram showing the possible diversion scenarios in MBA4

Table 4-8. List of possible material diversion scenarios in MBA4

Scenario ID	Scenario	Material	Preventing Safeguards
S4-1	Divert MOX powder during the co-denitration process	MOX powder	He-3 Neutron Detector (PIMS – NC)
S4-2	Divert MOX canister from the MOX temporary canister storage	MOX Canister	He-3 Neutron Detectors (TCVS – NC)

MBA5

This is the last area of the facility before shipping the product out of the facility. The MBA contains the storage of MOX canisters and UOX bottles.

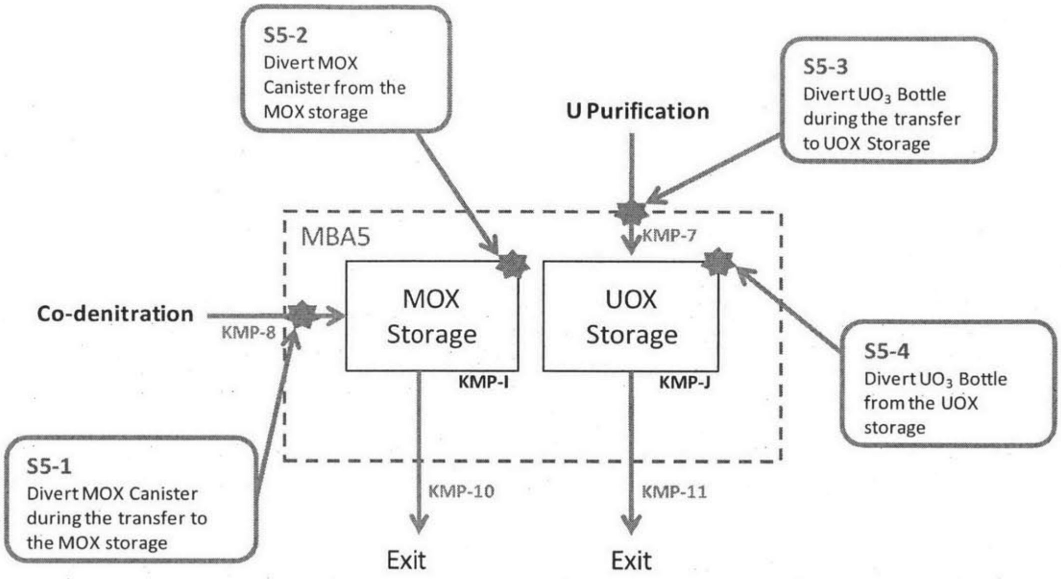

S5-2
Divert MOX Canister from the MOX storage
U Purification
S5-3
Divert UO_3 Bottle during the transfer to UOX Storage
MBA5
KMP-7
Co-denitration
KMP-8
MOX Storage
UOX Storage
KMP-I
KMP-J
S5-4
Divert UO_3 Bottle from the UOX storage
S5-1
Divert MOX Canister during the transfer to the MOX storage
KMP-10
KMP-11
Exit
Exit

Figure 4-12. Diagram showing the possible diversion scenarios in MBA5

Table 4-9. List of possible material diversion scenarios in MBA5

Scenario ID	Scenario	Material	Preventing Safeguards
S5-1	Divert MOX Canister during the transfer to the MOX storage	MOX Canister	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)
S5-2	Divert MOX Canister from the MOX storage	MOX Canister	Surveillance Camera (MSCS – OS) Metal Seal (MSCS – SL) Neutron Detector (MSCS – NC) ID Camera (MSCS (ID)
S5-3	Divert UO_3 Bottle during the transfer to UOX Storage	UO_3 Bottle	CdZnTe Detector (UBVS – GRS) Flat Weighing Scale (UBVS – WI)
S5-4	Divert UO_3 Bottle from the UOX storage	UO_3 Bottle	Surveillance Camera (USCS – OS) Metal Seal (USCS – SL)

Action 2: Take the diverted material out of the facility

For this action to be success the proliferator must elude the surveillance system, environmental sampling and the portal monitoring system. The success probability depends on the type of the material.

Table 4-10. List of possible material diversion scenarios to take diverted material out of the facility

Scenario ID	Scenario	Material	Preventing Safeguards
STO-1	Take the diverted material out of the facility	Spent Fuel	Optical Surveillance (Facility – OS) Environmental Sampling (ES) Portal Monitoring (PTM)
STO-2		Pu Nitrate	
STO-3		U Nitrate	
STO-4		MOX Powder	
STO-5		MOX Canister	
STO-6		U Bottle	
STO-7		HALW	
STO-8		LALW	

With the list of the possible scenarios and the associated safeguards, this is the background information needed for the expert elicitation of the probability of the basic events that will be used in the success tree model analysis.

4.4 Probabilistic Analysis

For each scenario in Section 4.3 , the success tree can be built depending on the safeguards that are in place to detect that diversion and the tactics that the proliferator will try to use. From an expert elicitation process shown in Chapter 3, the basic event probabilities in the tree can be derived for the set of safeguards in the facility.

There are three variables for a material diversion attempt

1. The scenario: the proliferator must choose the scenario of the diversion, which contains the type of material to be diverted, the location of the attempt, and the method of obtaining the material.
2. The tactic: the proliferator must decide on the tactics that he/she will use to help elude the safeguards in place to detect the diversion attempt.
3. The amount of material diverted per attempt: the proliferator must select the amount of material that will be diverted during one of the attempts. The goal of the proliferator is to choose a large enough amount to reach the significant quantity in acceptable time frame, while small enough to have high percentage chance of eluding the safeguards.

Since there are many scenarios and safeguards inside Rokkasho reprocessing facility, all of the analyses in this section will focus only on the diversion scenarios of plutonium inside MBA2 to show the methods and the examples of the results. Using the same processes, a complete evaluation of the whole facility can be accomplished.

4.4.1 Success Tree Path Sets and Diversion Pathways

Consider the scenario where the proliferator is trying to obtain the plutonium nitrate during the transfer from plutonium purification process and co-denitration process, using the notation in the previous section, this is scenario S2-6. In order to succeed with the diversion, the proliferator must elude the following safeguards: Electromanometer (SMMS – PM), Temperature Sensor (SMMS – HI), Neutron Detector (SMMS – NC), and Hybrid K-Edge Densitometry (ASAS – DA).

A path set is a set of basic events that must be true in order for the top event to be true. In this case the top event is the event that proliferator succeed in diverting special nuclear material (SNM). For this to be true, the proliferator must make an attempt to divert SNM, which is the initiator event in this case, and the proliferator must elude all of the safeguards in place to detect the diversion.

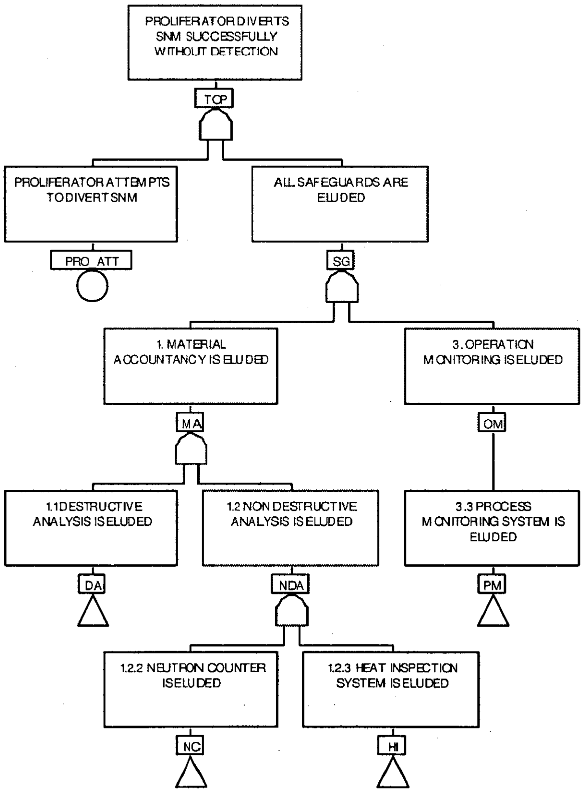

PROLIFERATOR DIVERTS SNM SUCCESSFULLY WITHOUT DETECTION
TOP
PROLIFERATOR ATTEMPTS TO DIVERT SNM
PRO ATT
ALL SAFEGUARDS ARE ELUDED
SG
1. MATERIAL ACCOUNTANCY IS ELUDED
MA
3. OPERATION MONITORING IS ELUDED
OM
1.1 DESTRUCTIVE ANALYSIS IS ELUDED
DA
1.2 NON DESTRUCTIVE ANALYSIS IS ELUDED
NDA
3.3 PROCESS MONITORING SYSTEM IS ELUDED
PM
1.2.2 NEUTRON COUNTER IS ELUDED
NC
1.2.3 HEAT INSPECTION SYSTEM IS ELUDED
HI

Figure 4-13. Success tree of the diversion scenario S2-6

Each of the safeguard has its own success tree as shown in Chapter 2. The diversion pathway is the set the events in the tree that will make the top event success. The Minimal Path Set (MPS), which is the set of events that cause the success of the top event, not containing another path set as a subset.

Using the probability of the top event as the measurement to compare the effectiveness of the diversion pathways, there are two variables. First one is the mass of material that is being diverted per attempt, and the second one is the choice of tactics by the proliferators to attack the safeguard.

The equation for the calculation of the event probability in the success tree is shown below.

$$\Pr(TOP) = \prod_{i=1}^{n} \Pr(MPS_i) \tag{4-1}$$

Therefore,

$$\text{Pr(TOP)} = \text{(Pr(PM)) (Pr(HI)) (Pr(NC)) (Pr(DA))} \tag{4-2}$$

Pr(TOP): Probability that proliferator divert SNM successfully without detection
Pr(PM): Probability that processing monitoring system (electromanometer) is eluded
Pr(HI): Probability that heat inspection system (temperature sensor) is eluded
Pr(NC): Probability that neutron counter (He-3 neutron detector) is eluded

Equation 4-1 is only true when the events within the minimal path set are independent. Depending on the choice of tactics by the proliferator, the probability to elude each safeguard will be different. Consider the success tree of a neutron counter, shown in Figure 4-14.

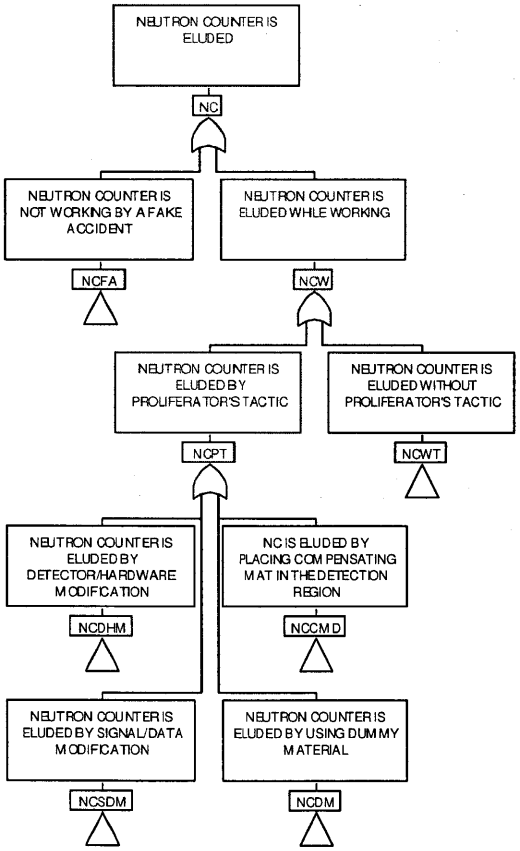

NEUTRON COUNTER IS ELUDED
NC
NEUTRON COUNTER IS NOT WORKING BY A FAKE ACCIDENT
NEUTRON COUNTER IS ELUDED WHILE WORKING
NCFA
NCW
NEUTRON COUNTER IS ELUDED BY PROLIFERATOR'S TACTIC
NEUTRON COUNTER IS ELUDED WITHOUT PROLIFERATOR'S TACTIC
NCPT
NCWT
NEUTRON COUNTER IS ELUDED BY DETECTOR/HARDWARE MODIFICATION
NC IS ELUDED BY PLACING COMPENSATING MAT IN THE DETECTION REGION
NCDHM
NCCMD
NEUTRON COUNTER IS ELUDED BY SIGNAL/DATA MODIFICATION
NEUTRON COUNTER IS ELUDED BY USING DUMMY MATERIAL
NCSDM
NCDM

Figure 4-14. Success tree of a neutron counter

Table 4-11. Proliferator tactics to elude a neutron counter and the sub-tree events for each tactic

Safeguard	Proliferator Tactic to Elude the Safeguard	Tactic Sub-tree Events
Neutron Counter (NC)	Without tactic (NCWT)	Neutron counter is eluded by design (NC_DS)
	Breaking NC by a fake accident (NCFA)	System optical surveillance is eluded (OS_E_SYS), Accident inspection is eluded (SI_E_AI)
	Detector/hardware modification (NCDHM)	Detector/hardware modification is not detected by NC (NC_DHM_D), System optical surveillance is eluded (OS_E_SYS), System seal is eluded (SL_E_SYS)
	Signal/data modification (NCSDM)	Signal/data modification is not detected by NC (NC_SDM_D), System optical surveillance is eluded (OS_E_SYS), System seal is eluded (SL_E_SYS)
	Use dummy material (NCDM)	Use of dummy material is not detected by NC (NC_DM_D), System optical surveillance is eluded (OS_E_MAT), System seal is eluded (SL_E_MAT)
	Placing compensating material in the detection region (NCCMD)	Placing compensating material in the detection region is not detected NC (NC_CMD_D), System optical surveillance is eluded (OS_E_SYS), System seal is eluded (SL_E_SYS)

If one of the tactics by the proliferator is successful, then the proliferator succeeds in eluding the neutron counter. Therefore, the probability of eluding neutron counter is calculated by the following equation.

$$\Pr(NC) = 1 - \prod_{j=1}^{m} (1 - \Pr(MPS_j)) \qquad (4\text{-}3)$$

$$\begin{aligned}\Pr(\mathrm{NC}) = 1 - (1 - \Pr(\mathrm{NCFA}))\ (1 - \Pr(\mathrm{NCDHM}))\ (1 - \Pr(\mathrm{NCSDM}))\\ (1 - \Pr(\mathrm{NCDM}))\ (1 - \Pr(\mathrm{NCCMD}))\ (1 - \Pr(\mathrm{NCWT}))\end{aligned} \qquad (4\text{-}4)$$

Pr(NCFA): Probability that neutron counter is not working by a fake accident
Pr(NCDHM): Probability that neutron counter is eluded by detector/hardware modification
Pr(NCSDM): Probability that neutron counter is eluded by signal/data modification
Pr(NCDM): Probability that neutron counter is eluded by use of dummy material
Pr(NCCMD): Probability that neutron counter is eluded by placing compensating material in the detection region
Pr(NCWT): Probability that neutron counter is eluded without proliferator tactic

For an example, if the proliferator chooses to use dummy material in order to elude the neutron detector, the probability of eluding neutron detector is the probability that neutron detector does not detect the use of dummy material and the material optical surveillance and seal does not detect the attempt. Figure below shows the success tree of the event when a neutron counter is eluded by the use of dummy material

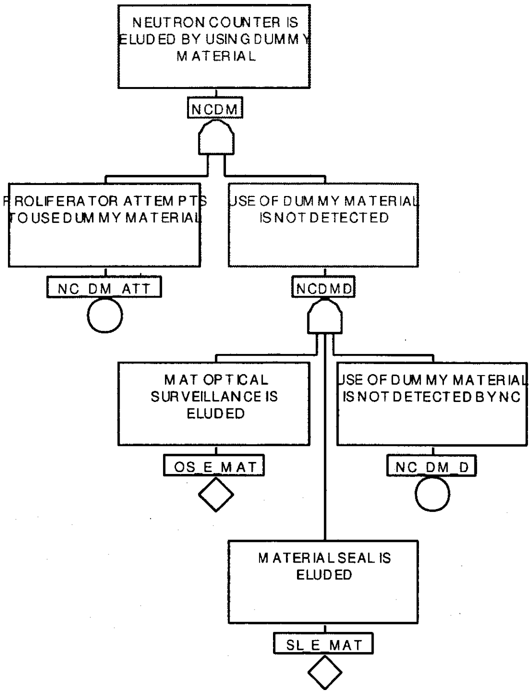

NEUTRON COUNTER IS ELUDED BY USING DUMMY MATERIAL
NCDM
PROLIFERATOR ATTEMPTS TO USE DUMMY MATERIAL
USE OF DUMMY MATERIAL IS NOT DETECTED
NC_DM_ATT
NCDMD
MAT OPTICAL SURVEILLANCE IS ELUDED
USE OF DUMMY MATERIAL IS NOT DETECTED BY NC
OS_E_MAT
NC_DM_D
MATERIAL SEAL IS ELUDED
SL_E_MAT

Figure 4-15. Success tree of a neutron counter for case that proliferator attempts to use dummy material

Therefore,

$$\Pr(NC\_DM) = (\Pr(NC\_DM\_D)) (\Pr(OS\_E\_MAT)) (\Pr(SL\_E\_MAT)) \qquad (4\text{-}5)$$

Pr(NC_DM_D): Probability that use of dummy material is not detected by NC
Pr(OS_E_MAT): Probability that material optical surveillance is eluded
Pr(SL_E_MAT): Probability that material seal is eluded

Each of the probability of eluding the supporting safeguard can still be expanded depending on the proliferator tactic to those safeguards, using the same method as for a neutron counter. The table below shows the possible choices of tactics the proliferator can use to elude the supporting safeguards of a neutron counter.

Table 4-12. Proliferator tactics to elude material optical surveillance and seal and their sub-tree events

Supporting Safeguard	Proliferator Tactic to Elude the Safeguard	Tactic Sub-tree Events
Material Optical Surveillance (OS_E_MAT)	Without tactic (OSWT)	Optical surveillance is eluded by design (OS_DS)
	Breaking OS by a fake accident (OSFA)	Accident inspection is eluded (SI_E_AI)
	Detector/Hardware Modification (OSDHM)	Detector/Hardware modification is not detected by OS (OS_DHM_D), System seal is eluded (SL_E_SYS)
	Signal/Data Modification (OSSDM)	Signal/Data modification is not detected by OS (OS_SDM_D) , System seal is eluded (SL_E_SYS)

Supporting Safeguard	Proliferator Tactic to Elude the Safeguard	Tactic Sub-tree Events
Material Seal (SL_E_MAT)	Without tactic (SLWT)	Seal is eluded by design (SL_DS)
	Breaking SL by a fake accident (SLFA)	System optical surveillance is eluded (OS_E_SYS), Accident inspection is eluded (SI_E_AI)
	Repairing the broken seal (SLRPR)	Repairing broken seal is not detected by seal inspection (SL_RPR_D), System optical surveillance is eluded (OS_E_SYS)
	Replacing the broken seal (SLRPC)	Replacing broken seal is not detected by seal inspection (SL_RPC_D), System optical surveillance is eluded (OS_E_SYS)
	Seal record modification (SLRM)	Seal record modification is not detected by seal inspection (SL_RM_D), Seal inspector is eluded (SI_E_SLI)

To calculate the probability of eluding these two safeguards for all possible tactics, more tactics choices to elude system optical surveillance, system seal, accident inspection, and seal inspector must be considered.

For a set of proliferator tactics chosen for primary and supporting safeguard, the proliferator success probability can be calculated. For an example, a proliferator attempts to divert SNM using scenario S2-6, while using dummy material to replace the material that has been diverted and modifying the images recorded by the optical surveillance camera. The proliferator is also required to repair the material seal and optical surveillance system seal to avoid detection. The following is the summary of tactics.

Primary Safeguards:

Electromanometer (PM): Without tactic (PMWT)
Temperature Sensor (HI): Use dummy material (HIDM)
He-3 Neutron Detector (NC): Use dummy material (NCDM)
Hybrid K-Edge Densitometry (DA): Use dummy material (DADM)

Supporting Safeguards:

Material Optical Surveillance (OS_E_MAT): Signal/Data modification (OSSDM)
Safeguard System Optical Surveillance (OS_E_MAT): Without tactic (SIWT)
Material Seal (SL_E_MAT): Repair broken seal (SLRPR)
Safeguard System Seal (SL_E_SYS): Repair broken seal (SLRPR)

Using the equations described before, the proliferator success probability to divert the material for scenario S2-6 is the following. Bold face shows the events that will be expanded in the next step.

Pr(TOP) = **(Pr(PM)) (Pr(HI)) (Pr(NC)) (Pr(DA))**
= (Pr(PM_DS)) **(Pr(HIDM)) (Pr(NCDM)) (Pr(DADM))**
= (Pr(PM_DS)) (Pr(HI_DM_D)) (Pr(NC_DM_D)) (Pr(DA_DM_D)) **(Pr(OS_E_MAT)) (Pr(SL_E_MAT))**

$$\begin{aligned}\text{Pr(TOP)} = {} & (\text{Pr(PM\_DS)})\,(\text{Pr(HI\_DM\_D)})\,(\text{Pr(NC\_DM\_D)})\,(\text{Pr(DA\_DM\_D)}) \\ & (\text{Pr(OS\_SDM\_D)}_{\text{mat}})\,\mathbf{(Pr(SL\_E\_SYS))}\,(\text{Pr(SL\_RPR\_D)}_{\text{mat}})\,\mathbf{(Pr(OS\_E\_SYS))} \\ = {} & (\text{Pr(PM\_DS)})\,(\text{Pr(HI\_DM\_D)})\,(\text{Pr(NC\_DM\_D)})\,(\text{Pr(DA\_DM\_D)}) \\ & (\text{Pr(OS\_SDM\_D)}_{\text{mat}})\,(\text{Pr(SL\_RPR\_D)}_{\text{sys}})\,(\text{Pr(SL\_RPR\_D)}_{\text{mat}})\,(\text{Pr(OS\_SDM\_D)}_{\text{sys}})\end{aligned} \tag{4-6}$$

When applying probability calculation into success tree, the set of event must be a minimal path set, therefore, when expanding the event into sub-tree, if the sub-tree contains an event that has already exists, then it will not reappear into the equation.

By varying the mass of the material being diverted and the proliferator tactics, the proliferator success probability of each set of tactics can be calculated and compared.

To demonstrate quantitative results, the following tables contain a fictitious example of basic event probabilities for the base case cost of all the safeguards related to scenario S2-6. The point estimates of the basic event probabilities are for three different mass of diverted material per attempt; $m_1 = 0.05$kg, $m_2 = 0.5$kg, $m_3 = 5$kg. Let Pr be the probability of success of that event. See the success trees in Appendix A for the full diagrams and names/IDs of the basic events.

Please note that the numbers in the following tables are made up by the author. They do not represent any real safeguard system.

Primary Safeguards

Process Monitoring (PM)	Probability that process monitoring is eluded by design (PM_DS)			Probability that detector/hardware modification is not detected by PM (PM_DHM_D)	Probability that signal/data modification is not detected by PM (PM_SDM_D)
	m_1	m_2	m_3		
Electromanometer (SMMS)	0.5	0.2	0.05	0.8	0.75

Heat Inspection (HI)	Probability that heat inspection is eluded by design (HI_DS)			Probability that detector/ hardware modification is not detected by HI (HI_DHM_D)	Probability that signal/data modification is not detected by HI (HI_SDM_D)	Probability that use of dummy material is not detected by HI (HI_DM_D)	Probability that placing compensating material in the detection region is not detected by HI (HI_CMD_D)
	m_1	m_2	m_3				
Temperature Sensor (SMMS)	0.6	0.4	0.2	0.8	0.75	0.8	0.9

Neutron Counter (NC)	Probability that neutron counter is eluded by design (NC_DS)			Probability that detector/ hardware modification is not detected by NC (NC_DHM_D)	Probability that signal/data modification is not detected by NC (NC_SDM_D)	Probability that use of dummy material is not detected by NC (NC_DM_D)	Probability that placing compensating material in the detection region is not detected by NC (NC_CMD_D)
	m_1	m_2	m_3				
He-3 Neutron Detector (SMMS)	0.4	0.15	0.1	0.8	0.75	0.6	0.7

Destructive Analysis (DA)	Probability that destructive analysis is eluded by design (DA_DS)			Probability that avoiding random sampling is not detected by DA (NC_ARS_D)	Probability that sample modification is not detected by DA (DA_SM_D)	Probability that use of dummy material is not detected by DA (DA_DM_D)
	m_1	m_2	m_3			
Hybrid K-Edge Densitometry (ASAS)	0.3	0.1	0.01	0.95	0.9	0.25

Supporting Safeguards

Optical Surveillance (OS)	Probability that optical surveillance is eluded by design (OS_DS)			Probability that detector/hardware modification is not detected by OS (OS_DHM_D)	Probability that signal/data modification is not detected by OS (OS_SDM_D)
	m_1	m_2	m_3		
Material OS	0.5	0.2	0.1	0.4	0.6
Safeguard System OS	0.1	0.1	0.1	0.4	0.6
Facility OS	0.6	0.4	0.2	0.4	0.6

Seal (SL)	Probability that seal is eluded by design (SL_DS)			Probability that repairing broken seal is not detected by seal inspection (SL_RPR_D)	Probability that replacing broken seal is not detected by seal inspection (SL_RPC_D)	Probability that seal record modification is not detected by seal inspection (SL_RM_D)
	m_1	m_2	m_3			
Material Seal	0.05	0.05	0.05	0.3	0.2	0.9
Safeguard System Seal	0.05	0.05	0.05	0.4	0.3	0.9
Sample Seal	0.05	0.05	0.05	0.3	0.2	0.9

Safeguard by the Inspector (SI)	Probability that safeguard by the inspector is eluded by design (SI_DS)			Probability that faking an accident to prevent inspection is not detected by the inspector (SI_FA_D)	Probability that bribing the inspector is not detected (SI_BI_D)
	m_1	m_2	m_3		
Random Sampling	0.02	0.02	0.02	0.3	0.3
Sample Monitoring	0.05	0.05	0.05	0.2	0.3
Seal Recording	0.01	0.01	0.01	0.3	0.3
Accident Inspection	0.1	0.1	0.1	0.1	0.3

First, by varying the choices of proliferator tactics to the supporting safeguards, the probability of eluding a primary safeguard for a certain tactic choice can be calculated. Table 4-13 shows the probability of eluding a neutron counter by using a dummy material for every possible set of tactics to the supporting safeguards for three different amount of material diverted per attempt.

Table 4-13. Proliferator success probability for all possible sets of tactics for NCDM event

Case No.	Pr(NCDM)	NC_DM_D	OS_DHM_D	OS_SDM_D	OS_DS (m1)	OS_DS (m2)	OS_DS (m3)	SL_RPR_D	SL_RPC_D	SL_RM_D	SL_DS	SI_BI_D	SI_DS
1	0.009	●									●	●	
2	0.003	●									●		●
3	0.0006	●	●								●		
4	0.0009	●		●							●		
5	0.015	●			●						●		
6	0.006	●				●					●		
7	0.003	●					●				●		
8	0.0162	●										●	
9	0.0006	●											●
10	0.0024	●	●										●
11	0.0036	●		●									●
12	0.015	●			●								●
13	0.0024	●				●							●
14	0.0006	●					●						●
15	0.0162	●						●				●	
16	0.0018	●						●					●
17	0.0216	●	●					●					
18	0.0324	●		●				●					
19	0.045	●			●			●					
20	0.0072	●				●		●					
21	0.0018	●					●	●					
22	0.0108	●							●			●	
23	0.0012	●							●				●
24	0.0096	●	●						●				
25	0.0144	●		●					●				
26	0.03	●			●				●				
27	0.0048	●				●			●				
28	0.0012	●					●		●				
29	0.0486	●								●		●	
30	0.0054	●								●			●
31	0.017496	●	●							●			
32	0.026244	●		●						●			
33	0.081	●			●					●			
34	0.0324	●				●				●			
35	0.0162	●					●			●			

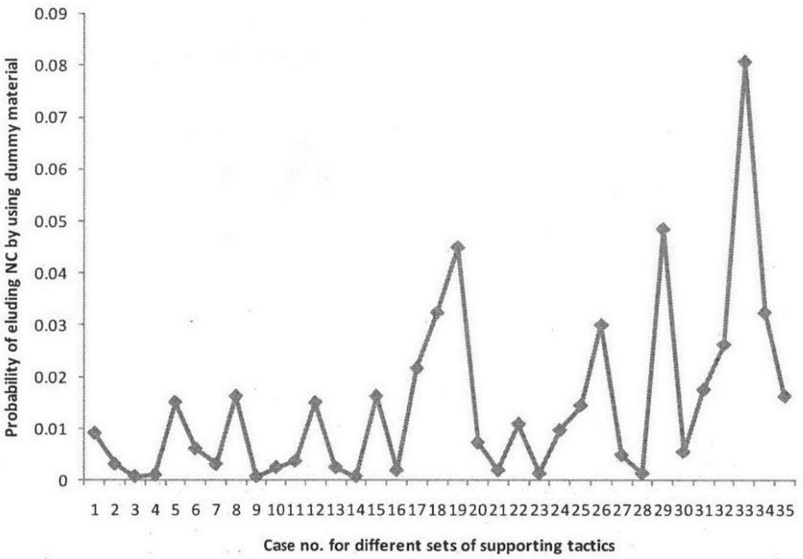


Figure 4-16. Probability of eluding neutron counter by using a dummy material for different sets of proliferator tactics to supporting safeguards

Figure 4-16 shows the plots of probabilities from Table 4-13. The spikes with high probabilities are for the cases when the proliferator attempt to divert very small amount of material without any tactic to the optical surveillance system. The high spike on the far right side of the plot is when the proliferator attempt to modify the seal record. This results show that, for this example, the effectiveness of the optical surveillance system to detect small amount of material and the seal protection from record modification must be improved.

Figure 4-17 shows the comparison of the probability plots between different proliferator tactics to elude a neutron counter for different material mass per diversion attempt, assuming proliferator attempt the same set of tactic to the supporting safeguards. The solid lines are the probability of eluding neutron counter without any tactic.

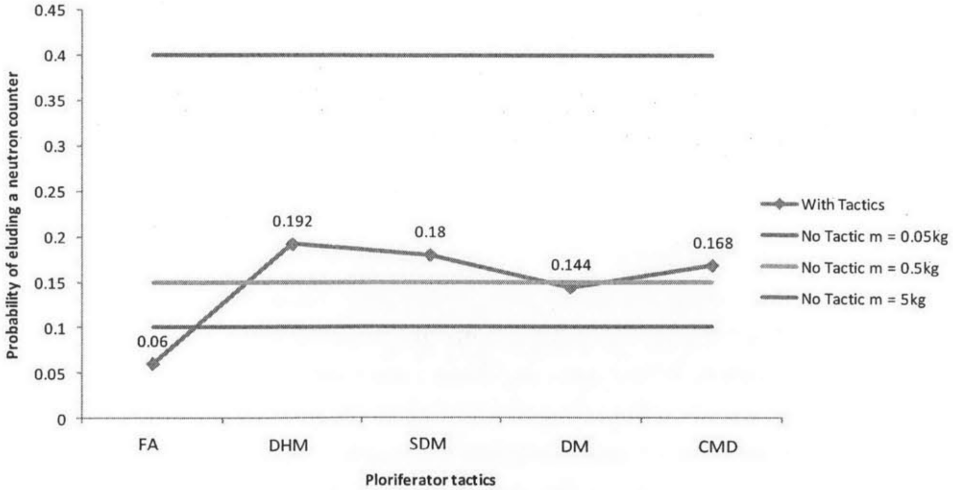


Figure 4-17. Probability of eluding neutron counter for different tactics

The relative proliferator success probabilities to elude a neutron counter for different tactics is shown for this example. They are fairly comparable, except the case where the proliferator attempts a fake accident, which mean no tactic is significantly better than the others. The solid lines showing the probabilities to elude a neutron counter without any tactic display a comparison for the proliferator choices whether or not a concealment tactic is required.

Following the same method, the proliferator success probability to elude the safeguards in place to detect the scenario S2-6 can be calculated for different sets of proliferator tactics and derived the set of tactics that give the highest proliferator success probability to elude each safeguard. Then by varying both the tactics to the primary safeguard and the tactics to the supporting safeguard, the top sets of tactic that give the highest proliferator success probability to divert the material by the scenario can be derived.

Besides the scenarios and set of tactics that provide the highest proliferator success probabilities, the analysis should also be carried out to compare the suggested or most likely diversion path way that the experts recommend during the elicitation process.

4.4.2 Uncertainty Analysis

The uncertainty analysis technique has been extensively developed and applied in the area of Probabilistic Risk Assessment (PRA). Since the proliferation assessment relies on incomplete information, there are uncertainties in the judgment of the expert. These uncertainties are provided by the experts when they give the point estimates of the probabilities.

There are two types of uncertainties: aleatory and epistemic. Aleatory uncertainty is the model uncertainty, which is the variability of the model that predicts the quantity. In this case, the aleatory uncertainty is the success tree model. The epistemic uncertainty is the parameter uncertainty, which is the uncertainty due to the incomplete knowledge of the value of the parameter of the aleatory model. In this case, the epistemic uncertainty is the uncertainty of the inputs from the expert's judgment.

The point estimates of the model parameter and the epistemic uncertainties vary from different experts depending on their state-of-knowledge of the system. The expert who is experienced with the system and have high confidence with his/her state-of-knowledge will be able to estimate the probabilities with less uncertainties than the expert who is less familiar with the system.

The basic events probabilities derived from expert elicitation are assumed to be normally distributed. The experts provide the uncertainty of the point estimate by giving the 95% confidence intervals. Then the standard deviations of the distributions of the basic events probabilities can be obtained. When inserting these values into the success tree model, the uncertainty of the basic events will propagate through to the probability of the TOP event. The calculation is done by the Monte Carlo sampling technique. For demonstration of the calculation, the example in the prior discussion for the case with scenario S2-6 and the set of proliferator tactics is used.

$$\Pr(TOP) = (\Pr(PM\_DS))\,(\Pr(HI\_DM\_D))\,(\Pr(NC\_DM\_D))\,(\Pr(DA\_DM\_D))\,(\Pr(OS\_SDM\_D)_{mat})\,(\Pr(SL\_RPR\_D)_{sys})\,(\Pr(SL\_RPR\_D)_{mat})\,(\Pr(OS\_SDM\_D)_{sys}) \tag{4-7}$$

The following table shows the fictitious example results with uncertainties of the related parameters from the elicitation process.

Table 4-14. Example of basic event probabilities point estimates and standard deviations

Basic Events Probabilities	Point Estimate	Standard Deviation
Pr(PM_DS)	0.2	0.02
Pr(HI_DM_D)	0.8	0.05
Pr(NC_DM_D)	0.6	0.03
Pr(DA_DM_D)	0.25	0.01
$\Pr(OS\_SDM\_D)_{mat}$	0.6	0.04
$\Pr(SL\_RPR\_D)_{sys}$	0.4	0.03
$\Pr(SL\_RPR\_D)_{mat}$	0.3	0.01
$\Pr(OS\_SDM\_D)_{sys}$	0.6	0.05

Using Monte Carlo sampling technique with 10000 sample points, the following show the result or the TOP event probability with propagated uncertainties from the basic events.

Event Probability	Point Estimate	Standard Deviation
Pr(TOP)	1.0368E-3	1.579E-4

When integrated the uncertainty analysis into the diversion pathway analysis, the results provide complete information to compare the proliferator success probability between scenarios and tactics. The proliferator success probabilities and uncertainties of different scenarios in MBA2 for the set tactics that give the highest proliferator success probability can be derived.

4.4.3 Sensitivity Analysis

The sensitivity analysis provides a systematic and visualized way to see the effect of the inputs or the basic events to the outcome. By changing the values of the inputs one by one, while keeping the rest constant, the change in the outcome indicates the amount of effect each input has on the outcome.

There are two goals for the sensitivity analyses. The first one is investigation of the effect upon which experts have estimated the basic event probabilities. This analysis tests how much the different beliefs of an expert would affect the output. This can be accomplished by determining how much the proliferator success probability changes according to changes of the values of the input variables.

Two cases will be considered. For the first case, the inputs from the experts are divided by half, representing the estimate of lower proliferator success probability. The second case, the inputs from the experts are set to twice the original values, representing the estimate of higher success probability. The original inputs from the experts will be called "base case".

For an example, Table below shows fictitious inputs from 4 different experts for the probability that a neutron counter does not detect the use of dummy material by the proliferator (NC_DM_D) and the values of the each input for the two cases.

Table 4-15. Example of probabilities estimates from four expert for base case and case I and II

Expert	Pr(NC_DM_D)		
	Base Case	Case I (Base Case/2)	Case II (Base Case*2)
Expert A	0.65	0.325	1
Expert B	0.45	0.225	0.9
Expert C	0.5	0.25	1
Expert D	0.8	0.4	1

The following plot shows the probability of the TOP event resulting from each case

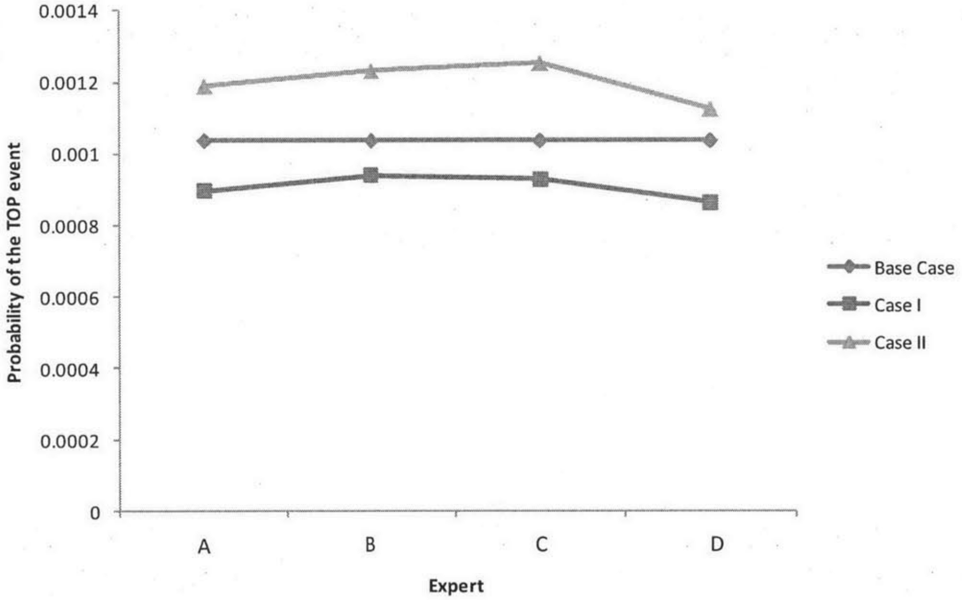


Figure 4-18. Probability of the TOP event for different cases, Expert.

The second goal is to perform a sensitivity analysis of the basic events to the TOP event, which involves varying each basic event probability in turn, while the rest of the probabilities remain at the values of the base case, this is done in order to see how the variation in the basic event affects the variation in the output.

4.4.4 Importance Measure Analysis

The importance measure is the method to identify the effect of the basic event probabilities to the top events. In this case, the importance measure will be use to rank the importance of the primary and supporting safeguard to the proliferator diversion success probability for each scenarios.

There are three commonly used importance measures: Risk Achievement Worth (RAW), Risk Reduction Worth (RRW), and Fussell-Vesely (FV)(Michael C. Cheok 1998). In this case, the risk is the proliferator success probability. The definitions below are modified to suit with the success tree model.

Risk Achievement Worth $a_i = \frac{R_i^+}{R_0}$

Risk Reduction Worth $r_i = \frac{R_0}{R_i^-}$

Fussel – Vesely $FV_i = \frac{R_0 - R_i^-}{R_0} = 1 - \frac{R_i^-}{R_0}$

R_i^+ = overall model success probability with the success probability of event i set to 1

R_i^- = overall model success probability with the success probability of event i set to 0;

R_0 = base case of overall model success probability

The RAW presents a measure of the worth of the basic event in achieving the TOP event success probability and indicates the importance of maintaining the level of probability of that basic event at the current level. The RRW presents maximum decrease of the TOP event success probability if event i never succeed, in the other word, the maximum improvement of safeguard related to event i. The Fussel-Vesely importance is a measure of the fraction contribution of the basic event to the TOP event success probability when the basic event success probability is changed from its base value to zero. The RRW and FV importance measure are related and the relative importance of the basic events from both measures is identical.

Using the example set of tactics in the prior discussion for scenario S2-6, the table below show the values of RAW importance measure for each of the basic events.

Table 4-16. Example of basic event probabilities estimates and importance measures

Basic Event (BE)	Probability of the Basic Event Pr(BE)	Importance Measure [Rank]
		RAW
PM_DS	0.2	5 [1]
HI_DM_D	0.8	1.25 [8]
NC_DM_D	0.6	1.67 [5]
DA_DM_D	0.25	4 [2]
OS_SDM_D_{mat}	0.6	1.67 [5]
SL_RPR_D_{sys}	0.4	2.5 [4]
SL_RPR_D_{mat}	0.3	3.3 [3]
OS_SDM_D_{sys}	0.6	1.67 [5]

From the table, the most important basic event for this set of tactics is the probability that the proliferator will elude processing monitoring by its design. The second is the tactic where proliferator attempt to use dummy material to elude destructive. These show that these two are strong safeguard, while the last one which is the probability to elude the heat inspection by dummy material could be improved.

For further analysis, the importance measure of the same basic event can also be compare for different scenario, to find the different of amount of the effect each safeguard has on different scenarios.

Chapter 5 Facility Design and Safeguards Scheme Analyses

In Chapter 4, the evaluation of existing safeguard schemes have been shown for different scenarios of proliferator diversion attempts. This chapter contains how the evaluation will help with design a facility and safeguard scheme.

5.1 Design and Cost of a Reprocessing Facility

There are two methods to increase proliferation resistance.

1. Design the processes and the forms of the materials inside the facility such that the materials are self-protected. In another word, the materials are in the forms that are difficult to handle, such as emitting high radiation, and difficult to be used for weapon construction, such as being very low enriched in U-235 or Pu-239. The limitation is the technology current available for the facility designers.
2. Improve the safeguard scheme of the facility by the safeguarder, such that the detection probabilities of all possible diversion scenarios are very high. The limitation is the amount of resource of the safeguarder.

This is one of the biggest challenges for the nuclear fuel cycle to be widely used commercially. As long as the material in the reprocessing facility can be quickly used to construct a nuclear weapon and easily enough to be diverted without detection by the safeguarder, the risk will remains too high for justification to build recycling facilities in non-nuclear weapon states.

The current safeguarder for the nuclear facilities in the non-nuclear weapon states is the International Atomic Energy Agency (IAEA). It is operating under tight budget and even though half of the annual budget goes to nuclear safeguard and verification, there are 1,131 facilities under safeguards or at least containing safeguarded material, as of 31 December 2008 (IAEA, Annual Report 2008). Therefore, the IAEA must allocate the funds effectively to achieve the best protection against possible proliferation.

There are 4 common layers of protection against a material diversion in a nuclear facility

1. The type of the material, such as the isotope composition from the design of the processes
2. The form of the material, such as the physical container and the state the material
3. The safeguard scheme to detect the diversion attempts
4. The physical barrier security, such as facility boundary, walls, security guards.

5.2 Safeguard Evaluation for Different Facility Designs

There are many variables in facility design that affect the effectiveness of the safeguards

Table 5-1. Variables that affect the effectiveness of the safeguards and methods to increase the value

Variable	Design Factor	Method to Increase the Effectiveness of the Safeguards
Material Composition	Facility processes, Input material, Output material, Burnup time	Remove the background material, increase the radioactivity of the material to increase the difficulty to handle and the diversion attempt is easier to be detected by the surveillance cameras
Material Form and Geometry	Facility processes, Material container	Put material into a form of countable unit, such as a canister or a bottle, do not have material flow in big chunk to avoid the effect of the self shielding effects, Use a uniform material for less error in material accountancy
Material Flow Rate	Size of the facility, Size of the processes, Annual throughput, capacity factor	Choose smaller plant design for smaller mass flow rate and less material unaccounted for (MUF)
Material Accessibility by the Personnel	Facility building design, Automatic processes	Use automatic process in the area where the material is highly attractive for proliferation, so the diversion attempt is easier to be detected

By varying this design variable the change in the top event probability can be obtained and ranked to find which variable affect the effectiveness of the safeguard the most. These factors then can be emphasized during the facility design process in order to maximize the proliferation protection by the safeguards.

For example, considering the MBA2 of Rokkasho reprocessing facility, an analysis can compare the effectiveness of a neutron counter for two different material flow rates through the Output Accountability Tank (OAT). If the uncertainties of measurements for both flow rates are approximately at the same value of percentage, i.g. 1% of the flow rates, then the probabilities of detecting the diversion for 1% of material from both flow rates are equal. Therefore, a proliferator has the same probability of success to divert more amount of material for the design with higher flow rate than the design with lower flow rate. Results from the analysis will show the comparison of safeguard effectiveness between the two facility designs and provide quantitative information for the safeguarder to regulate the plant operations that affect the flow of the material in MBA2.

5.3 Cost Effectiveness of the Safeguard Scheme

By evaluating the efficiency of the safeguard for different setups and costs, the safeguarder can determine the best resource allocation to particular safeguards that will greatly decrease the proliferator success probability.

There are two types of cost effectiveness analysis to consider; analysis of the existing safeguards in the facility, and analysis or effectiveness of adding a new safeguard.

5.3.1 Existing Safeguard Cost Effectiveness Analysis

First type is the analysis of the cost effectiveness of the current safeguard in a facility. From the results of the expert elicitation, the proliferator success probability can be derived for the range of the cost of safeguard setups to increase the safeguard effectiveness and prevent proliferator tactics. By vary the cost of the safeguard and calculate the success probability to elude the safeguard, the percentage change of the probability versus the amount of difference in cost will show the most effective way to put in resource to increase the safeguard efficiency and protection.

The results from the expert elicitation contain the information of the proliferator success probability in terms of the cost of the safeguard related to the possible tactics by the proliferator. The total cost of the safeguard is the sum of all of the cost to prevent all the tactics.

For example, the table below shows fictitious results from a neutron counter expert elicitation. The experts provide the estimate of the proliferator success probabilities at three different costs of the safeguard setups to detect each of the proliferator tactics.

Table 5-2. Example results of the proliferator success probabilities to elude NC a function of safeguard cost

Proliferator Tactic to Elude NC		Low Cost Setup	Base Case Setup	High Cost Setup
NC_DS	Safeguard Cost ($M)	0.05	0.2	1
	Probability for m_1	0.9	0.4	0.25
	Probability for m_2	0.3	0.15	0.1
	Probability for m_3	0.2	0.1	0.05
NC_DHM_D	Safeguard Cost ($M)	0.05	0.3	1
	Probability	0.95	0.8	0.4
NC_SDM_D	Safeguard Cost ($M)	0.05	0.1	0.5
	Probability	0.9	0.75	0.2
NC_DM_D	Safeguard Cost ($M)	0.05	0.2	1
	Probability	0.85	0.6	0.2
NC_CMD_D	Safeguard Cost ($M)	0.05	0.2	1
	Probability	0.9	0.7	0.15

The cost of a neutron counter is the sum of the component costs to protect from each type of the proliferator tactics.

$$C_{NC} = C_{DS} + C_{DHM} + C_{SDM} + C_{DM} + C_{CMD} \tag{5-1}$$

Consider the cases where the proliferator uses the same set of tactics for the supporting safeguard, Figure 5-1 shows improvement to the safeguard effectiveness by adding or decreasing the component of the safeguards that helps detecting the tactic of using dummy material to elude a neutron counter.

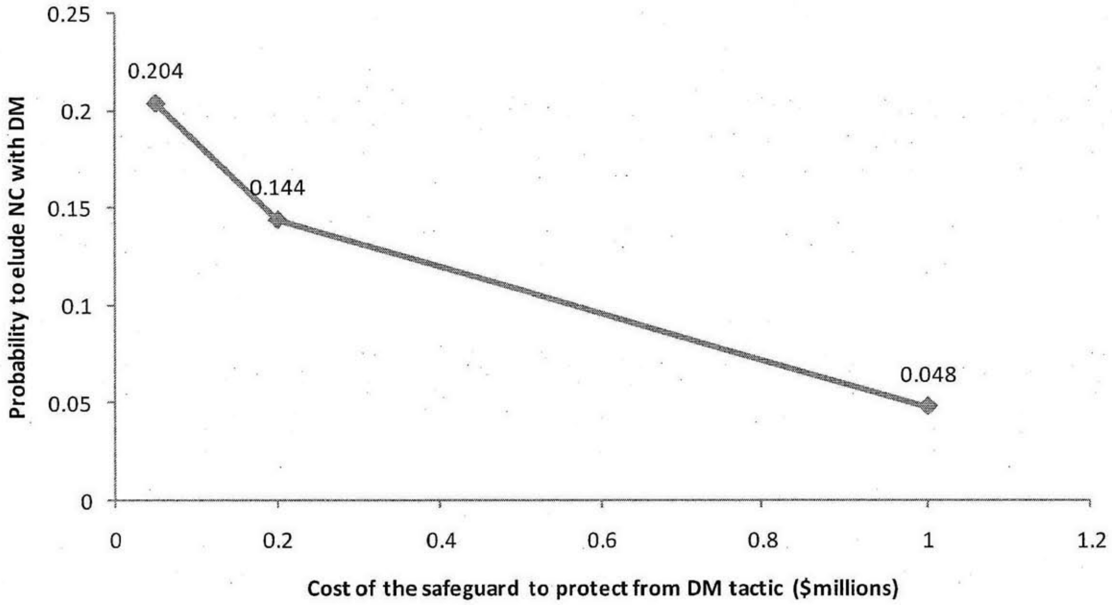


Figure 5-1. Probability to elude NC with DM for different cost of the safeguard

The result shows that by increasing the cost to protect NC from DM for $0.8 million, the probability to elude the NC by DM decreases by 0.096, which is not much significant comparing to the decrease of the success probability from the low cost to the base case cost which reduce for 0.06 for only $0.15 million more. This justify that the investment for the base case protection components is fairly cost effective.

Figure 5-2 shows the probability to elude NC versus costs of the safeguards with different proliferator tactics, considering that the proliferator uses the same set of tactics for the supporting safeguards. The results show that in order for the safeguarder to reach the same safeguard effectiveness to prevent each type of tactic, the safeguarder must devote more resources to protect the safeguard from DHM than DM and CDM, and more than SDM.

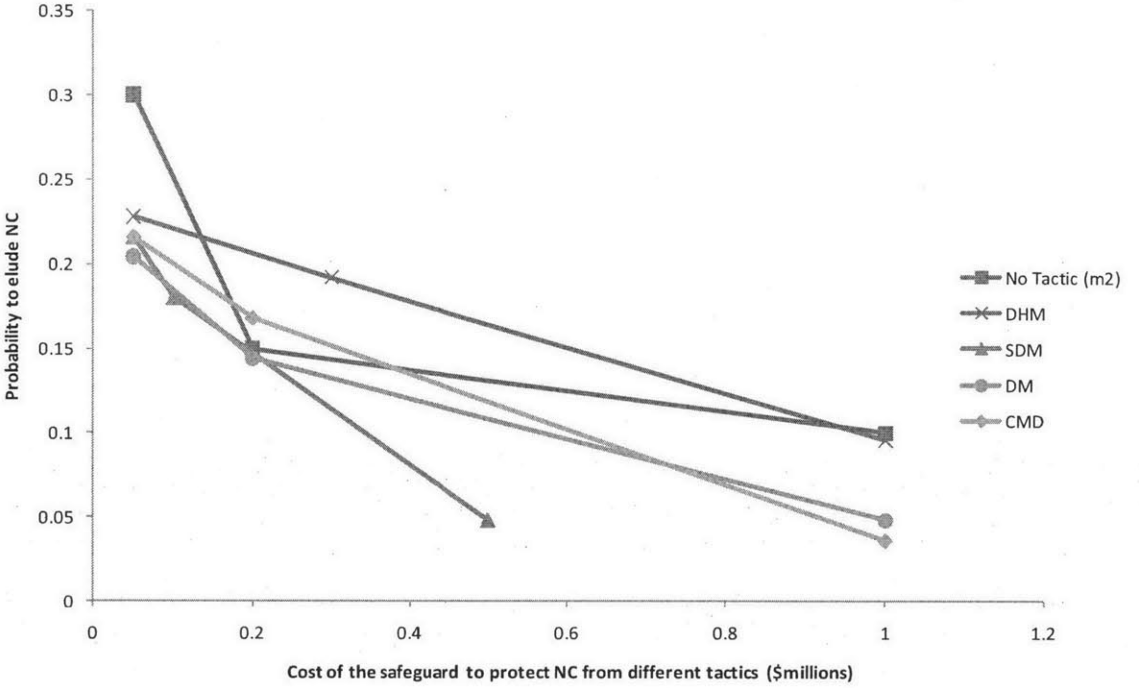


Figure 5-2. Probability to elude NC versus costs of the safeguard for different tactics

Moreover, by comparing the percentage changes of success probabilities between the changes of the cost of different safeguards, the safeguarder can decide on the priority of safeguards which to allocate the limited funding.

5.3.2 Additional Safeguard Cost Effectiveness Analysis

The section contains the analysis of cost effectiveness of adding a new safeguard into the scheme.

Considering scenarios in MBA2 as in the analysis in Chapter 4 with a new safeguard introduced to the system. The new safeguard system is the Nuclear Resonance Fluorescence (NRF).

NRF is an active interrogation technique. Excitation of nuclides is caused by an incident Bremsstrahlung beam. When the excited state decays, the characteristic photons are radiated into all directions with respect to the incident beam, leading to unique photon energies of resonance fluorescence. The radiated photons can be detected by a detector and used to identify the nucleus of the material by the unique energy spectrum of the radiated photons.

The advantage of NRF technique is due to the gamma radiation generated and induced by the active Bremsstrahlung beam that is able to penetrate the fuel assembly envelope and eventually the cask holding it.

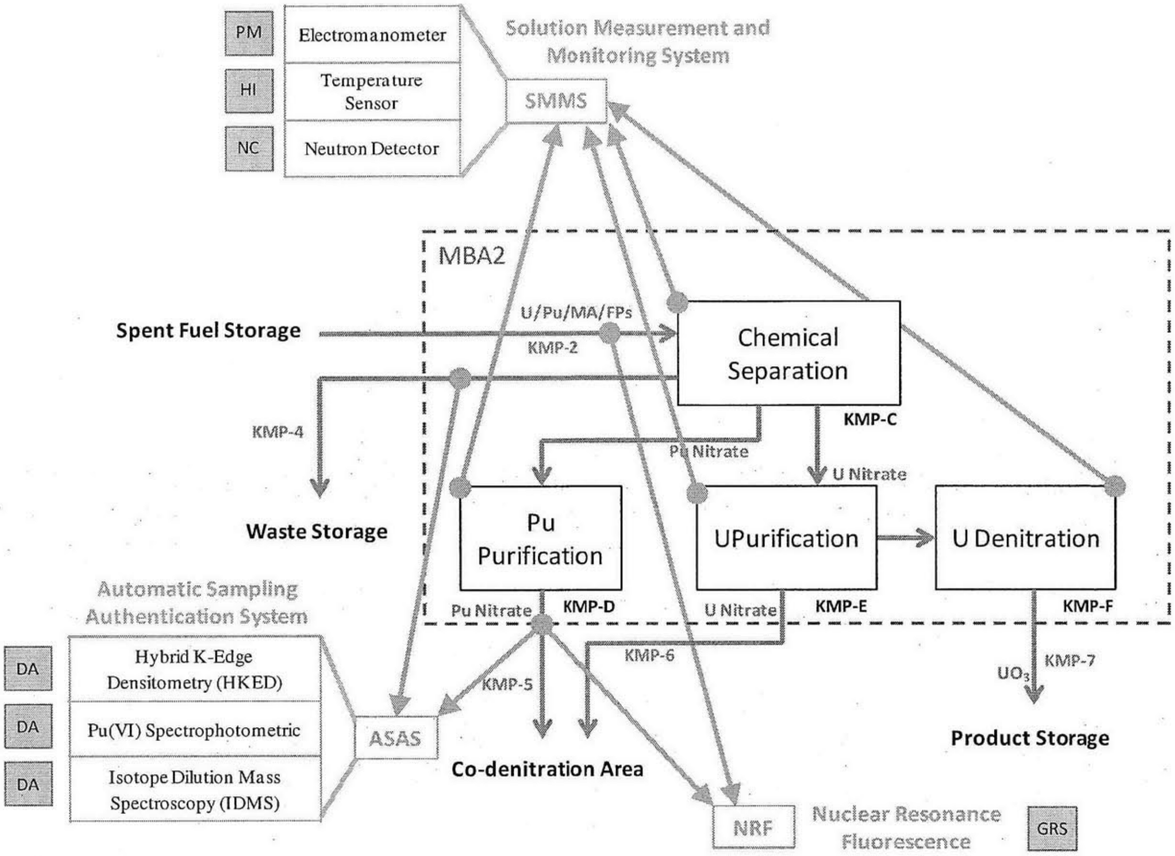


Figure 5-3. Diagram of safeguard system in MBA2 with NRF

Components	Type of Safeguard	Location	Material	Functionality
NRF	GRS	Before and after chemical separation Process	Material Solution	Determine the composition of the material solution going in and out of the chemical separation process for material accountancy

Then the list of safeguards and possible scenarios is changed to the following.

Table 5-3. List of possible material diversion scenario for MBA2 with NRF system

Scenario ID	Scenario	Material	Preventing Safeguards
S2-1	Divert spent fuel solvent during the transfer between dissolution process to chemical separation process	Spent fuel solvent	Electromanometer (SMMS – PM) Temperature Sensor (SMMS –HI) Neutron Detector (SMMS – NC)
S2-2	Divert spent fuel during the chemical separation process	Spent fuel solvent	Electromanometer (SMMS – PM) Temperature Sensor (SMMS –HI) Neutron Detector (SMMS – NC)
S2-3	Modify the organic or complexing agents to redirect more plutonium into the waste stream, then divert the material stream during the transfer to waste storage	Pu Nitrate in waste stream (MA, FPs)	Electromanometer (SMMS – PM) Temperature Sensor (SMMS –HI) Neutron Detector (SMMS – NC) Pu(VI) Spectrophotometric (ASAS – DA)
S2-4	Divert plutonium during the plutonium purification process	Pu Nitrate	Electromanometer (SMMS – PM) Temperature Sensor (SMMS –HI) Neutron Detector (SMMS – NC) Nuclear Resonance Fluorescence (NRF – GRS) Hybrid K-Edge Densitometry (ASAS – DA)
S2-5	Divert uranium during the uranium purification process	U Nitrate	Electromanometer (SMMS – PM) Temperature Sensor (SMMS –HI)
S2-6	Divert plutonium during the transfer between purification process and co-denitration process	Pu Nitrate	Electromanometer (SMMS – PM) Temperature Sensor (SMMS –HI) Neutron Detector (SMMS – NC) Nuclear Resonance Fluorescence (NRF – GRS) Hybrid K-Edge Densitometry (ASAS – DA)

The same analysis as in Chapter 4 can be carried out to find the proliferator success probabilities for different proliferator choices of tactics. The results can be used to justify whether the addition of the NRF system is worth the extra cost added.

For an example, considering the scenario 2-6 with the sets of tactics as discussed in the earlier sections. Assume that the proliferator also attempt to use dummy material to elude the NRF system. Here is the list of the updated set of tactics.

Primary Safeguards:

Electromanometer (PM): Without tactic (PMWT)
Temperature Sensor (HI): Use dummy material (HIDM)
He-3 Neutron Detector (NC): Use dummy material (NCDM)

Hybrid K-Edge Densitometry (DA): Use dummy material (DADM)
Nuclear Resonance Fluorescence (NRF): Use dummy material (NRFDM)

Supporting Safeguards:

Material Optical Surveillance (OS_E_MAT): Signal/Data modification (OSSDM)
Safeguard System Optical Surveillance (OS_E_MAT): Without tactic (SIWT)
Material Seal (SL_E_MAT): Repair broken seal (SLRPR)
Safeguard System Seal (SL_E_SYS): Repair broken seal (SLRPR)

The TOP event probability is then

$$\Pr(\text{TOP}) = (\Pr(\text{PM\_DS}))\,(\Pr(\text{HI\_DM\_D}))\,(\Pr(\text{NC\_DM\_D}))\,(\Pr(\text{DA\_DM\_D}))\,(\Pr(\text{NRF\_DM\_D}))\,(\Pr(\text{OS\_SDM\_D})_{\text{mat}})\,(\Pr(\text{SL\_RPR\_D})_{\text{sys}})\,(\Pr(\text{SL\_RPR\_D})_{\text{mat}})\,(\Pr(\text{OS\_SDM\_D})_{\text{sys}})$$

With the example of result for the NRF from the expert elicitation, the following table shows the results comparing between the safeguard scheme with and without the NRF.

Event	NRF_DM_D	TOP without NRF	TOP with NRF
Probability	0.15	0.001037	0.0001555

Adding the NRF decrease the proliferator success probability by almost an order of magnitude.

Comparing cost effectiveness of improving the current safeguard and the cost of adding NRF to the safeguard scheme. From this example, the cost of the NRF will be $1M for the base case. Comparing the improvement to the safeguards in prior discussion, adding an NRF is much more cost effective. Therefore, this justifies the significant of adding NRF into the safeguard scheme.

Chapter 6 Conclusion

6.1 Summary of the Framework

This framework presents a complete and systematic method for a safeguard evaluation in a nuclear facility. The complete procedures to identify safeguard systems and possible diversion scenarios are shown for the Rokkasho reprocessing facility. Then discussions and examples of success tree analyses are presented with fictitious results in the format derived from the introduced expert elicitation process.

The success tree methodology is used as a tool to evaluate proliferator diversion success probability of a safeguard scheme by dividing the scheme into safeguard systems categorized by safeguard types. Proliferator success probability to elude a safeguard depends on the amount of material diverted per attempt and the sets of concealment tactics used by the proliferator to help elude the safeguards. The tactics can range from attacking the safeguard system itself to modifying the material under detection. However, by attempting extra tactics to help elude the safeguards, the attempts can also be detected by the supporting safeguards that are in place to detect these tactics.

The basic event probabilities in the success tree are functions of many variables depending on the diversion scenario of the proliferator and the safeguard scheme set up by the safeguarder. Analyses of these factors capture the competition between the two actors where the proliferator is trying to choose a scenario that gives the highest diversion success probability, and the safeguarder is trying to setup a safeguard scheme that minimizes the diversion success probabilities for all possible scenarios. A diversion scenario consists of target material, target location, diversion technique, set of tactics to help elude the safeguards, and the amount of material diverted per attempt. The safeguard scheme can vary depending on resources devoted to the safeguards by the safeguarder. Its effectiveness also depends on the designs of the facility. With these variables embedded in the design of the model, results can be extensively analyzed for many applications.

Expert elicitation is used to derive the probabilities of the basic events via expert judgments. The framework provides a systematic approach for the processes of inquiring the expert judgments by having qualitative discussions with the experts to obtain the optimal safeguard setups and its vulnerabilities, prior of a quantitative questionnaire. Questions for the experts are conveniently tailored for them to answer with minimal calculation required. An example of a fully prepared document for the expert elicitation is provided in Appendix A.

Finally, the diversion pathways analysis to evaluate the safeguard scheme with the uncertainties is shown along with sensitivity and importance measure analyses. Results of the analyses can be used by the safeguarder to gauge the level of protection provided by the current safeguard scheme, and to identify the weak points for further improvements. The safeguarder is also able to further analyze the effectiveness of the safeguard scheme for different facility designs to suggest the best designs for proliferation resistance of new facilities. Finally, the cost effectiveness analysis will help the safeguarder allocate the limited resources for maximum possible protection against a material diversion attempt.

6.2 Effectiveness of the Model

This section contains a discussion about the effectiveness of the success tree model and the use of expert elicitation to acquire the probabilities of basic events.

The effectiveness of the model depends heavily on the accuracy of expert judgments. Therefore, the elicitation process must be properly conducted to obtain the best estimations of the probabilities. The selected experts must be fairly familiar with the safeguard system under study. Higher number of experts per safeguard and more diversity of expert backgrounds will greatly improve accuracy of the results. For the questionnaire, the conductor of the elicitation must ensure that the safeguard setup, which the experts use to provide the estimates, is consistent among the experts. The definitions of the proliferator tactics must be clear and contain a complete list of possible actions. These steps are important for the validity of the aggregation of expert inputs and eventually the effectiveness of the model.

In order to obtain accurate and insightful results from the analyses, complete information of target facility and safeguard scheme is required. This can be a limitation of the study because most of the detailed information is classified and there are small numbers of experts who have experiences with the actual systems. For this reason, an open study must be conducted with approximate safeguard setups and facility designs, or a close study must be done carefully by a government entity or the IAEA to avoid leaking security information that could compromise the safeguard systems to a proliferator.

With complete information and careful expert elicitation, one more approach to improve the effectiveness of the model is to create higher number of proliferator scenarios with higher level of details, and distinguish the proliferator tactics into several specific ones. This provides better accuracy of estimations from the experts and more in-depth analyses. However, complexity of the analyses will increase, along with the number of basic events for which the expert must provide probability estimates.

6.3 Future Additional Work

The framework presented here is complete and ready to be used as a part of nuclear facility proliferation resistance evaluation. For direct comparison of proliferation resistances between different diversion scenarios, results of the analyses in this framework must be combined with the material attractiveness, as discussed in Chapter 1. While only the evaluation for a reprocessing facility is shown, the framework can be used for any facility in the nuclear fuel cycle, and can also be extended to evaluate the safeguard scheme for fuel transportation between facilities by defining suitable material balance areas. Further comparison of the effectiveness of the safeguard scheme between facilities will provide the safeguarder quantitative information to identify the strengths and weaknesses of their safeguard policies and resource allocations.

References

Barnaby, Dr Frank. *Planning for failure – International nuclear safeguards and the Rokkasho-mura reprocessing plant.* Oxford Research Group; Shaun Burnie, Greenpeace International, 2002.

Bunn, M. *Civilian Nuclear Energy and Nuclear Weapons Programs: The Record.* Draft for Discussion, 2001.

Currie, L. A. *Anal. Chem.*, 1968: 40 (3), 586.

E. Cavalieri d'Oro, M. Golay. "Proliferation Resistance Assessment of the Sodium Fast Reactor Energy System Using a Risk-Informed and Performance-Based Regulartory Framework." *Proc. Global 2009.* American Nuclear Society, 2009.

Floyd H. Grant, Robin J. Miner, Dennis Engi. *A Network Modeling and Analysis Technique for the Evaluation of Nuclear Safeguards Effectiveness.* NlIREG/CR-0616, Nuclear Regulartory Commissioner, 1978.

Golay, Michael. "Measures of Safeguards, Barriers and Nuclear Reactor Concept/Fuel Cycle Resistance to Nuclear Weapons Proliferation." *Nuclear Science and Engineering*, In preparation.

Ham, Hyeongpil. *An Integrated Methodology for Quantitative Assessment of Proliferation Resistance of Advanced Nuclear Systems Using Probabilistic Methods.* MIT Ph.D. Thesis, 2005.

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

IAEA. "IAEA: Safeguards Stemming the Spread of Nuclear Weapons." *IAEA Annual Report "Nuclear Security & Safeguards," IAEA Bulletin, Vol. 43, No. 4*, 2001.

—. "Safeguard Glossary." *International Nuclear Verification Series No. 3*, 2002.

IAEA. *Reprocessing, Plutonium Handling, Recycle.* Report of INFCE Working Group 4, Vienna: IAEA, 1980.

IAEA, International Atomic Energy Agency. *Annual Report.* IAEA, 2008.

IAEA, International Atomic Energy Agency. "Safeguards Techniques and Equipment." Vienna, 2003.

IAEA-TECDOC-1535. "Nuclear Fuel Cycle Simulation System (VISTA)." (IAEA) 2007.

Knoll, Glenn F. *Radiation Detection and Measurement 3rd Edition.* John Wiley & Sons, Inc., 2000.

Michael C. Cheok, Gareth W. Parry, Richard R. Sherry. "Use of importance measures in risk-informed regulartory applications." *Reliability Engineering and System Safety 60*, 1998: 213-226.

Michael H. Ehinger, Shirley J. Johnson. *Lessons Learned in International Safeguards—Implementation of Safeguards at the Rokkasho Reprocessing Plant.* ORNL/TM-2010/23, Oak Ridge National Laboratory, 2009.

National Science of Academy. *Management and Disposition of Excess Weapons Plutonium.* Washington D.C.: National Academy Press, 1994.

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

PNNL. *Advanced Safeguards Approaches for New Reprocessing Facilities.* Pacific Northwest National Laboratory, U.S. Department of Energy, 2007.

Robert T. Clemen, Robert L. Wrinkler. "Combining Probability Distribuitions From Experts in Risk Analysis"." *Risk Analysis*, 1999: Vol.19, No.2.

S. J. Johnson, H. Higuchi, K. Fujimaki. *Development of Safeguard Approach for the Rokkasho Reprocessing Plant.* IAEA-SM-367/8/01, 2001.

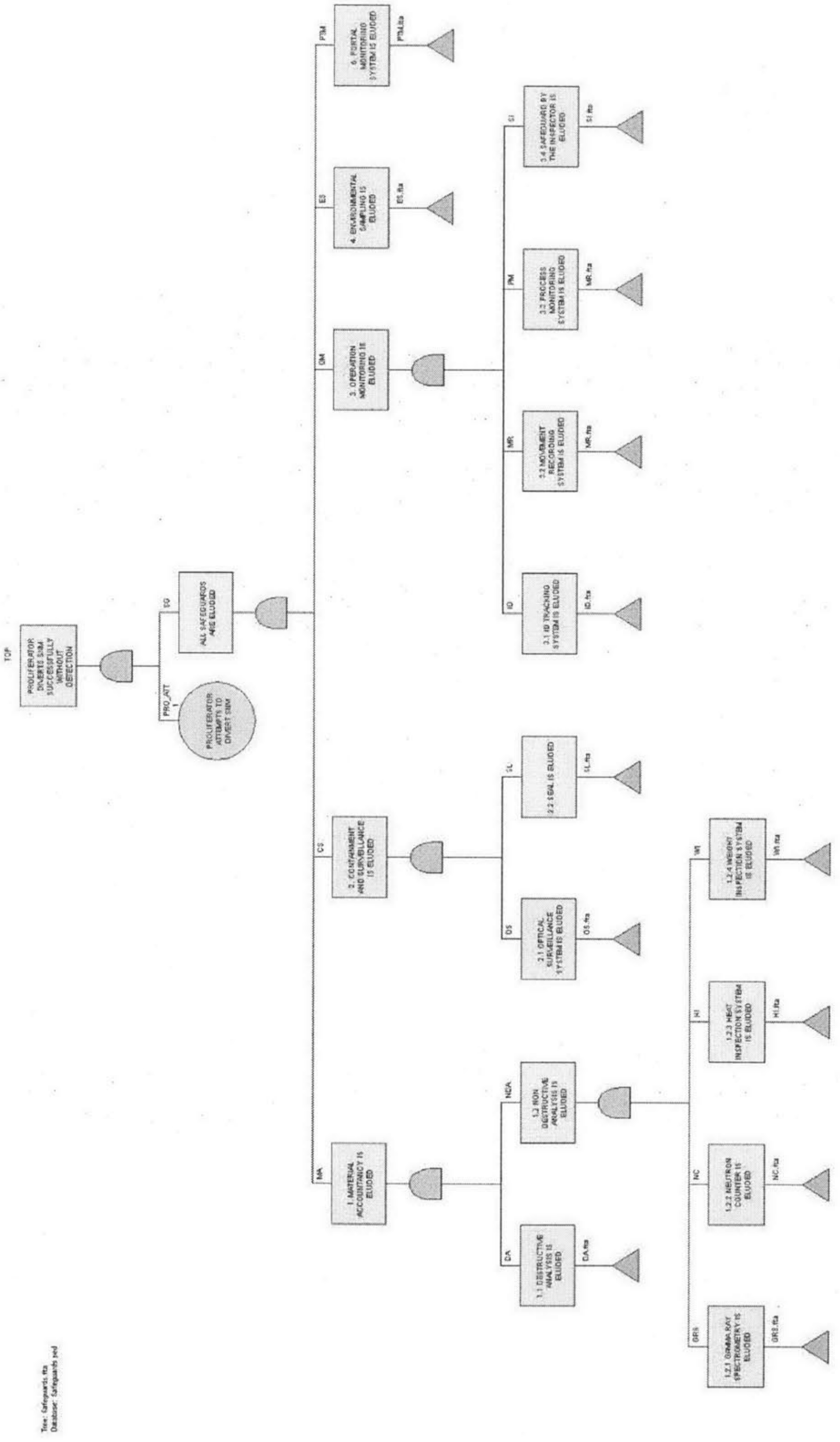
Sentell Jr., D. S. *A Quantitative Assessment of Nuclear Weapons Proliferation Risk Utilizing Probabilistic Methods.* MIT MS Thesis, 2002.

Shipley, James P. "Decision Analysis for Nuclear Safeguards." In *Nuclear Safeguard Analysis Nondestructive and Analytical Chemical Techniques*, by E. Arnold Hakkila, 34. 1978.

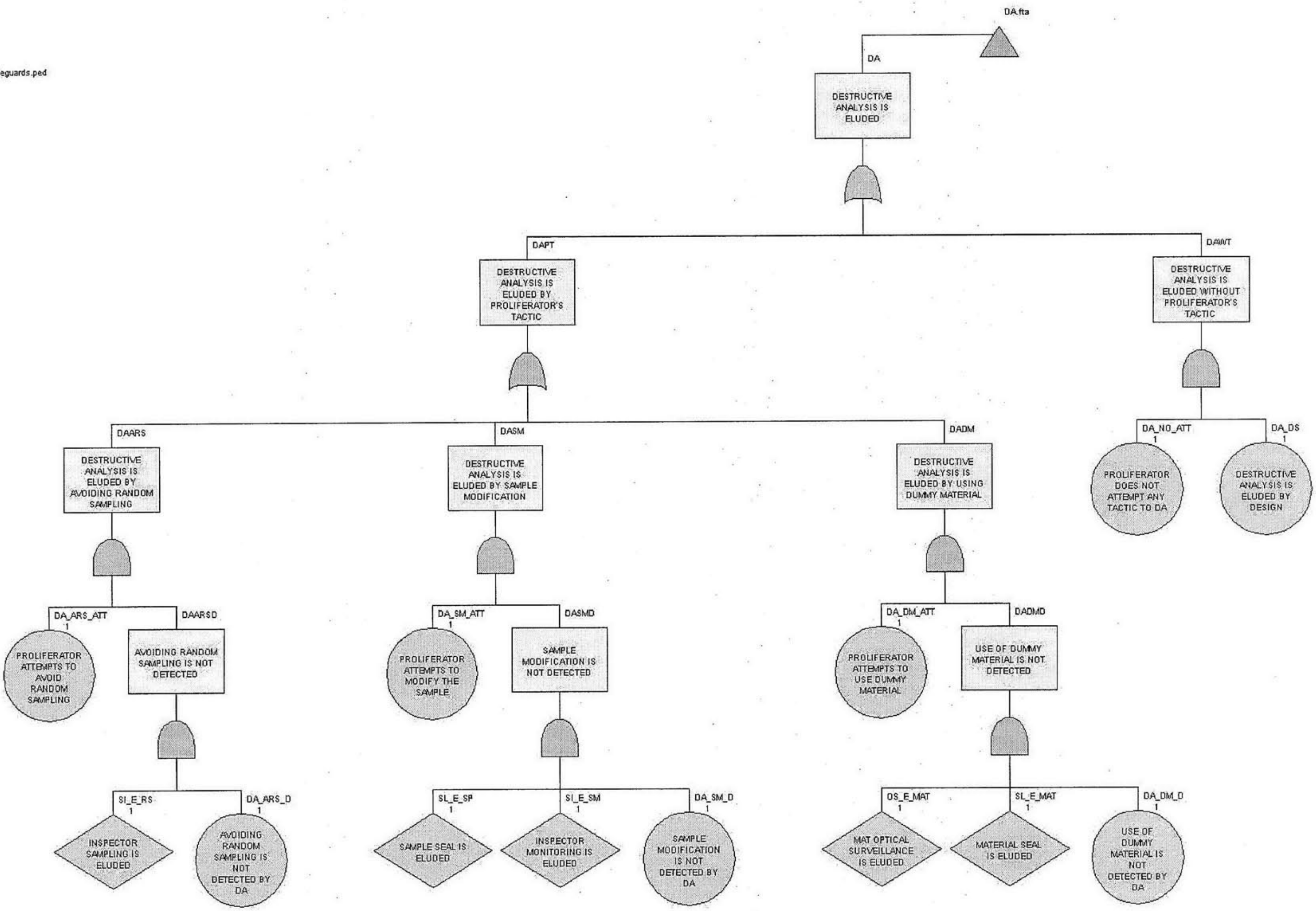
Silvennoinen, P. *Nuclear Fuel Cycle Optimization Methods and Modelling Techniques.* Technical Research Centre of Finland, Helsinki, Finland: Pergamon Press, 1982.

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.

Appendix A: Safeguards Success Trees


Tree: Safeguards.fta
Database: Safeguards.sed
TOP
PROLIFERATOR DIVERTS SNM SUCCESSFULLY WITHOUT DETECTION
PRO_ATT 1
PROLIFERATOR ATTEMPTS TO DIVERT SNM
SG
ALL SAFEGUARDS ARE ELUDED
MA
1. MATERIAL ACCOUNTANCY IS ELUDED
CS
2. CONTAINMENT AND SURVEILLANCE IS ELUDED
OM
3. OPERATION MONITORING IS ELUDED
ES
4. ENVIRONMENTAL SAMPLING IS ELUDED
ES.fta
PTM
5. PORTAL MONITORING SYSTEM IS ELUDED
PTM.fta
DA
1.1 DESTRUCTIVE ANALYSIS IS ELUDED
DA.fta
NDA
1.2 NON DESTRUCTIVE ANALYSIS IS ELUDED
OS
2.1 OPTICAL SURVEILLANCE SYSTEM IS ELUDED
OS.fta
SL
2.2 SEAL IS ELUDED
SL.fta
ID
3.1 ID TRACKING SYSTEM IS ELUDED
ID.fta
MR
3.2 MOVEMENT RECORDING SYSTEM IS ELUDED
MR.fta
PM
3.3 PROCESS MONITORING SYSTEM IS ELUDED
MR.fta
SI
3.4 SAFEGUARD BY THE INSPECTOR IS ELUDED
SI.fta
GRS
1.2.1 GAMMA RAY SPECTROMETRY IS ELUDED
GRS.fta
NC
1.2.2 NEUTRON COUNTER IS ELUDED
NC.fta
HI
1.2.3 HEAT INSPECTION SYSTEM IS ELUDED
HI.fta
WI
1.2.4 WEIGHT INSPECTION SYSTEM IS ELUDED
WI.fta

Tree: DA.fta
Database: Safeguards.ped

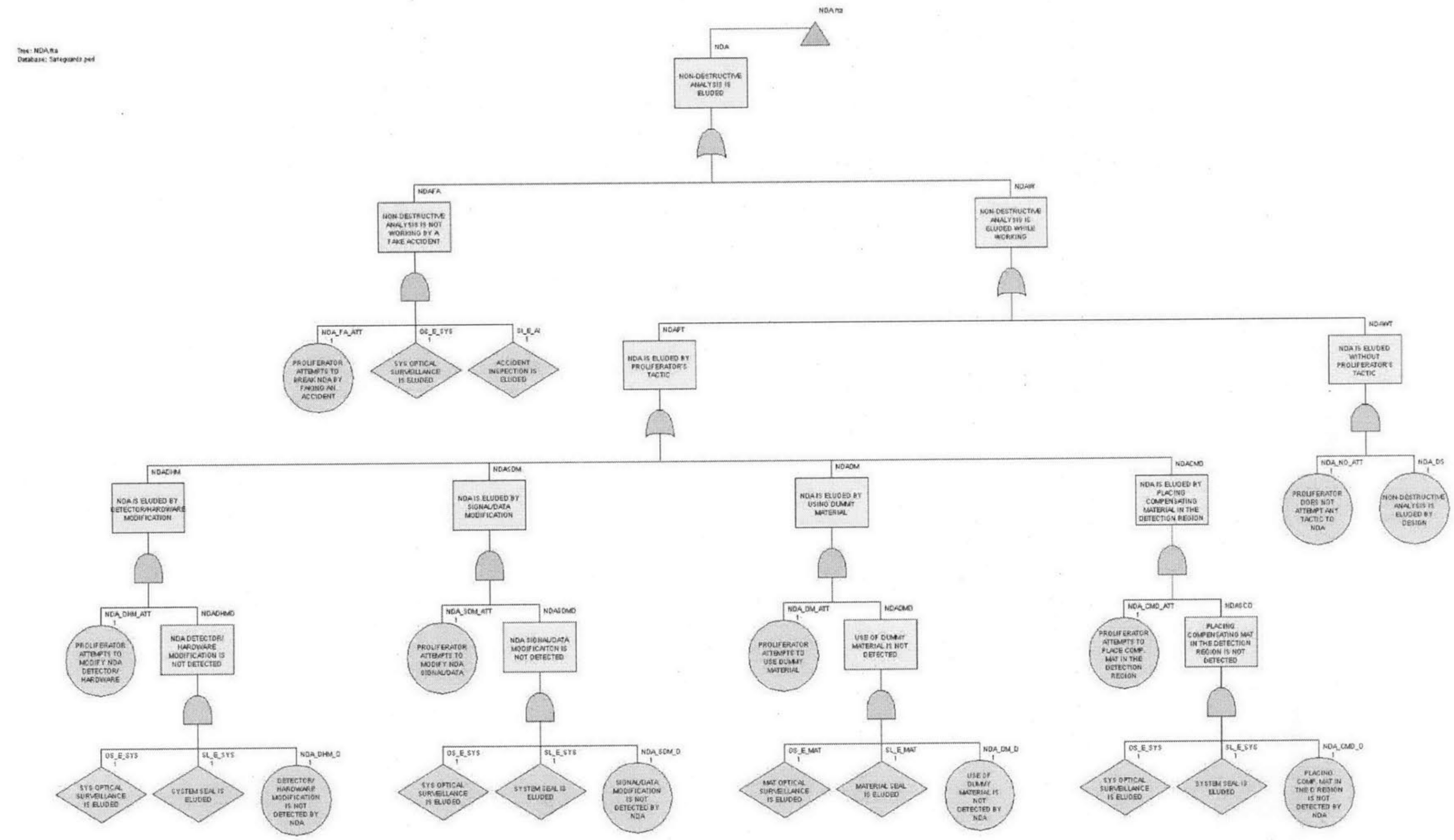

DA.fta
DA
DESTRUCTIVE ANALYSIS IS ELUDED
DAPT
DESTRUCTIVE ANALYSIS IS ELUDED BY PROLIFERATOR'S TACTIC
DAWT
DESTRUCTIVE ANALYSIS IS ELUDED WITHOUT PROLIFERATOR'S TACTIC
DAARS
DESTRUCTIVE ANALYSIS IS ELUDED BY AVOIDING RANDOM SAMPLING
DASM
DESTRUCTIVE ANALYSIS IS ELUDED BY SAMPLE MODIFICATION
DADM
DESTRUCTIVE ANALYSIS IS ELUDED BY USING DUMMY MATERIAL
DA_NO_ATT
1
PROLIFERATOR DOES NOT ATTEMPT ANY TACTIC TO DA
DA_DS
1
DESTRUCTIVE ANALYSIS IS ELUDED BY DESIGN
DA_ARS_ATT
1
PROLIFERATOR ATTEMPTS TO AVOID RANDOM SAMPLING
DAARSD
AVOIDING RANDOM SAMPLING IS NOT DETECTED
DA_SM_ATT
1
PROLIFERATOR ATTEMPTS TO MODIFY THE SAMPLE
DASMD
SAMPLE MODIFICATION IS NOT DETECTED
DA_DM_ATT
1
PROLIFERATOR ATTEMPTS TO USE DUMMY MATERIAL
DADMD
USE OF DUMMY MATERIAL IS NOT DETECTED
SI_E_RS
1
INSPECTOR SAMPLING IS ELUDED
DA_ARS_D
1
AVOIDING RANDOM SAMPLING IS NOT DETECTED BY DA
SL_E_SP
1
SAMPLE SEAL IS ELUDED
SI_E_SM
1
INSPECTOR MONITORING IS ELUDED
DA_SM_D
1
SAMPLE MODIFICATION IS NOT DETECTED BY DA
OS_E_MAT
1
MAT OPTICAL SURVEILLANCE IS ELUDED
SL_E_MAT
1
MATERIAL SEAL IS ELUDED
DA_DM_D
1
USE OF DUMMY MATERIAL IS NOT DETECTED BY DA

1. Material Accountancy

1.1Destructive Analysis (DA)

Basic events descriptions of destructive analysis success tree

Proliferator Tactic	Specific Tactic Examples	Sub-tree Events
Proliferator does not attempt any tactic to DA (DA_NO_ATT) Proliferator does not attempt any tactic to prevent DA from detecting the diversion	• Proliferator diverts the material with small enough amount per attempt such that DA has low probability of detecting the diversion	• **Destructive analysis is eluded by designed (DA_DS)** Destructive analysis does not detect the material diversion because of its detection efficiency
Proliferator attempts to avoid random sampling (DA_ARS_ATT) Proliferator attempts to prevent the part of material, where some has been diverted, from being randomly collect by the inspector	• Proliferator prevent the inspector to collect a sample from the area where the material is diverted • Proliferator prepared a sample or have a designated area for the inspector to collect a sample	• **Inspector sampling is eluded (SI_E_RS)** The inspector does not randomly collect sample from all parts of the material inside the MBA • **Avoiding random sampling is not detected by DA (DA_ARS_D)** Destructive analysis does not detect that the sample is not randomly collected
Proliferator attempts to modify the sample (DA_SM_ATT) Proliferator attempts to replace or modify the sample after it has been randomly collected by the inspector	• Proliferator swap the sample during the site inspection after it has been randomly collected by the inspector • Proliferator swap the sample during its transit from the site to the inspection agency laboratory	• **Sample seal is eluded (SL_E_SP)** Seal of the sample container does not show that it has been opened • **Inspector monitoring is eluded (SI_E_SM)** The inspector who monitor the sample does not detect the sample modification • **Sample modification is not detected by DA (DA_SM_D)** Destructive analysis does not detect that the sample has been modified
Proliferator attempts to use dummy material (DA_DM_ATT) Proliferator replace the diverted material with a dummy material that could avoid detection by the destructive analysis	• Proliferator replace the diverted material with the material that has the same elemental or isotopic properties	• **Material optical surveillance is eluded (OS_E_MAT)** Optical surveillance does not detect that the proliferator replace the diverted material with a dummy material • **Material seal is eluded (SL_E_MAT)** Seal of the material container does not show that it has been opened • **Use of dummy material is not detected by DA (DA_DM_D)** Destructive analysis does not detect that the material is a dummy material


Tree: NDA.fta
Database: Safeguards.psd
NDA.fta
NDA
NON-DESTRUCTIVE ANALYSIS IS ELUDED
NDAFA
NON-DESTRUCTIVE ANALYSIS IS NOT WORKING BY A FAKE ACCIDENT
NDAIW
NON-DESTRUCTIVE ANALYSIS IS ELUDED WHILE WORKING
NDA_FA_ATT
1
PROLIFERATOR ATTEMPTS TO BREAK NDA BY FAKING AN ACCIDENT
OS_E_SYS
1
SYS OPTICAL SURVEILLANCE IS ELUDED
SL_E_AI
1
ACCIDENT INSPECTION IS ELUDED
NDAPT
NDA IS ELUDED BY PROLIFERATOR'S TACTIC
NDAWT
NDA IS ELUDED WITHOUT PROLIFERATOR'S TACTIC
NDA_NO_ATT
1
PROLIFERATOR DOES NOT ATTEMPT ANY TACTIC TO NDA
NDA_DS
1
NON-DESTRUCTIVE ANALYSIS IS ELUDED BY DESIGN
NDADHM
NDA IS ELUDED BY DETECTOR/HARDWARE MODIFICATION
NDA_DHM_ATT
1
PROLIFERATOR ATTEMPTS TO MODIFY NDA DETECTOR/ HARDWARE
NDADHMD
NDA DETECTOR/ HARDWARE MODIFICATION IS NOT DETECTED
OS_E_SYS
1
SYS OPTICAL SURVEILLANCE IS ELUDED
SL_E_SYS
1
SYSTEM SEAL IS ELUDED
NDA_DHM_D
1
DETECTOR/ HARDWARE MODIFICATION IS NOT DETECTED BY NDA
NDASDM
NDA IS ELUDED BY SIGNAL/DATA MODIFICATION
NDA_SDM_ATT
1
PROLIFERATOR ATTEMPTS TO MODIFY NDA SIGNAL/DATA
NDASDMD
NDA SIGNAL/DATA MODIFICATON IS NOT DETECTED
OS_E_SYS
1
SYS OPTICAL SURVEILLANCE IS ELUDED
SL_E_SYS
1
SYSTEM SEAL IS ELUDED
NDA_SDM_D
1
SIGNAL/DATA MODIFICATION IS NOT DETECTED BY NDA
NDADM
NDA IS ELUDED BY USING DUMMY MATERIAL
NDA_DM_ATT
1
PROLIFERATOR ATTEMPTS TO USE DUMMY MATERIAL
NDADMD
USE OF DUMMY MATERIAL IS NOT DETECTED
OS_E_MAT
1
MAT OPTICAL SURVEILLANCE IS ELUDED
SL_E_MAT
1
MATERIAL SEAL IS ELUDED
NDA_DM_D
1
USE OF DUMMY MATERIAL IS NOT DETECTED BY NDA
NDACMD
NDA IS ELUDED BY PLACING COMPENSATING MATERIAL IN THE DETECTION REGION
NDA_CMD_ATT
1
PROLIFERATOR ATTEMPTS TO PLACE COMP. MAT IN THE DETECTION REGION
NDASCD
PLACING COMPENSATING MAT IN THE DETECTION REGION IS NOT DETECTED
OS_E_SYS
1
SYS OPTICAL SURVEILLANCE IS ELUDED
SL_E_SYS
1
SYSTEM SEAL IS ELUDED
NDA_CMD_D
1
PLACING COMP. MAT IN THE D REGION IS NOT DETECTED BY NDA

1.2Non-Destructive Analysis (NDA)

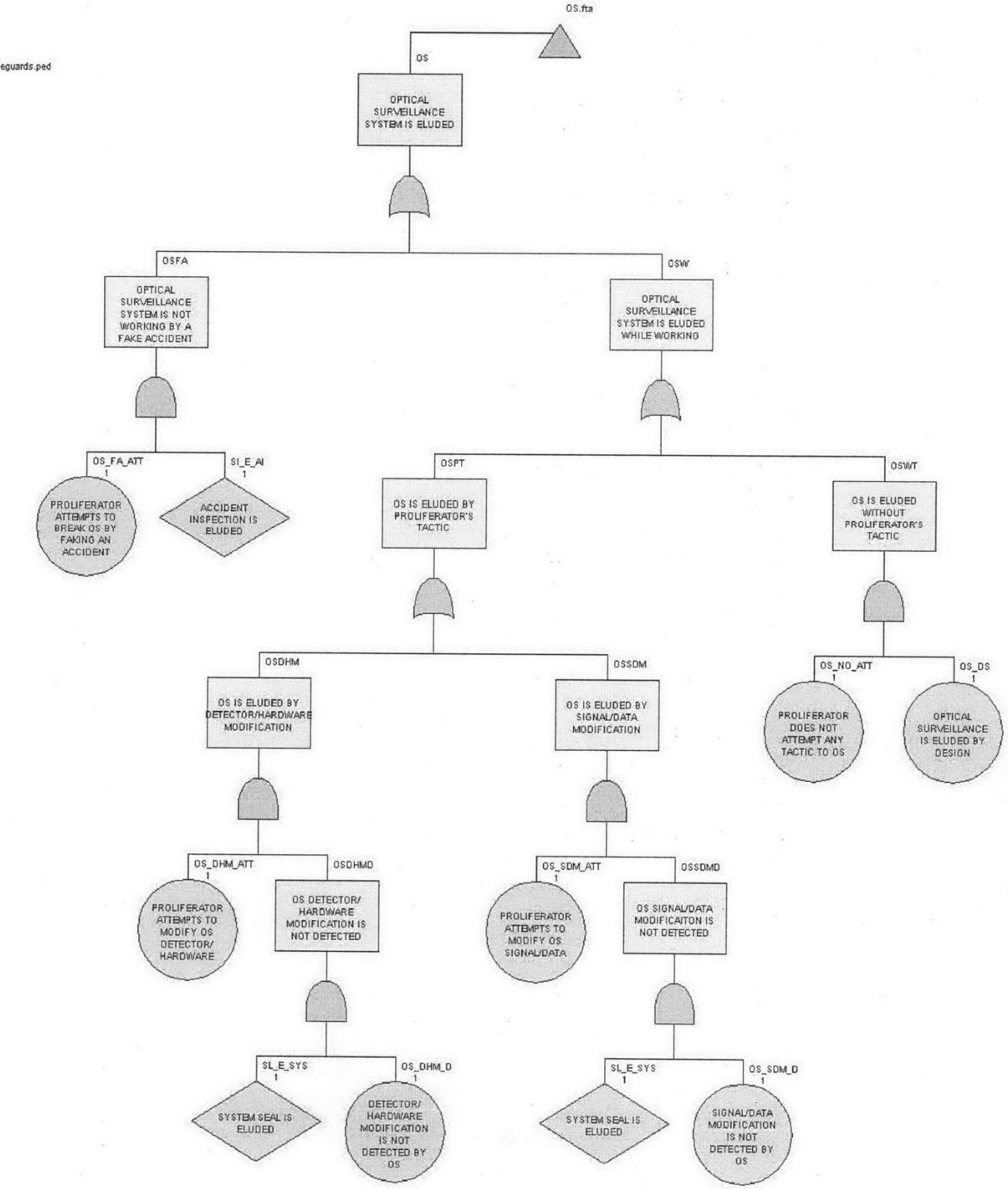
All of these tactics apply to each type of the NDA (Gamma Ray Spectrometry, Neutron Counter, Heat Inspection, Weight Inspection, and Nuclear Resonance Fluorescence)

Basic events descriptions of non-destructive analysis success tree

Proliferator Tactic	Specific Tactic Examples	Sub-tree Events
Proliferator does not attempt any tactic to NDA (NDA_NO_ATT) Proliferator does not attempt any tactic to prevent NDA from detecting the diversion	• Proliferator diverts the material with small enough amount per attempt such that NDA has low probability of detecting the diversion	• **Non-destructive analysis is eluded by designed (NDA_DS)** Non-destructive analysis does not detect the material diversion because of its detection efficiency
Proliferator attempts to break NDA by faking an accident (NDA_FA_ATT) Proliferator attempts to stage a fake accident that will break the functionality of the NDA	• Proliferator stages a fake electrical system that cut the power to the NDA system • Proliferator stages a fake fire accident that breaks NDA system hardware	• **Optical surveillance is eluded (OS_E_SYS)** Optical surveillance does not detect that the proliferator stages a fake accident • **Accident inspection is eluded (SI_E_AI)** The accident inspection by the inspector cannot detect that it has been staged
Proliferator attempts to modify NDA detector/ hardware (NDA_DHM_ATT) Proliferator attempts to modify the detector or hardware of the NDA system, preventing it from detecting the missing material	• Proliferator modify the NDA detector to give larger signal compensating for the diverted material	• **System optical surveillance is eluded (OS_E_SYS)** Optical surveillance does not detect that the proliferator tampers with the NDA detector/hardware • **System seal is eluded (SL_E_SYS)** Seal of the NDA system does not show that it has been opened • **Detector/Hardware modification is not detected by NDA (NDA_DHM_D)** Non-destructive analysis system does not detect that its detector/hardware has been modified
Proliferator attempts to modify NDA signal/data (NDA_SDM_ATT) Proliferator attempts to modify the signal between NDA detector and the processing unit or modify the record data to remove the detection signal	• Proliferator feed a fake detector signal to the processing unit • Proliferator hacks the NDA system software to always display and store expected data • Proliferator access and modifies the stored data before the inspection	• **System optical surveillance is eluded (OS_E_SYS)** Optical surveillance does not detect that the proliferator tampers with the NDA cables or processing system to modify the signal/data • **System seal is eluded (SL_E_SYS)** Seal of the NDA system does not show that it has been opened • **Signal/data modification is not detected by NDA (NDA_SDM_D)** Non-destructive analysis signal and data encryption does not detect that its signal/data has been modified

Proliferator Tactic	Specific Tactic Examples	Sub-tree Events
Proliferator attempts to use dummy material (NDA_DM_ATT) Proliferator attempts to replace the diverted material with a dummy material to avoid the detection by the NDA system	• Proliferator replaces the diverted material with a material that has the same NDA detecting properties	• **Material optical surveillance is eluded (OS_E_MAT)** Optical surveillance does not detect that the proliferator replace the diverted material with a dummy material • **Material seal is eluded (SL_E_MAT)** Seal of the material container does not show that it has been opened • **Use of dummy material is not detected by NDA (NDA_DM_D)** Non-destructive analysis does not detect that the material is a dummy material
Proliferator attempts to place compensating material in the detection region (NDA_CMD_ATT) Proliferator attempts to place compensating amount of material for the diverted material in the NDA detection region.	• Proliferator places the same amount of material as the diverted material in the detecting region to fool the NDA system	• **Material and System optical surveillance is eluded (OS_E_SYS)** Optical surveillance does not detect that the proliferator places compensating material in the detection region • **System seal is eluded (SL_E_SYS)** Seal of the NDA system, which prevent the access to the detecting region, does not show that it has been opened • **Placing compensating material in the detection region is not detected by NDA (NDA_CMD_D)** Non-destructive analysis does not detect that the proliferator put compensating material in the detecting region

Tree: OS.fta
Database: Safeguards.ped

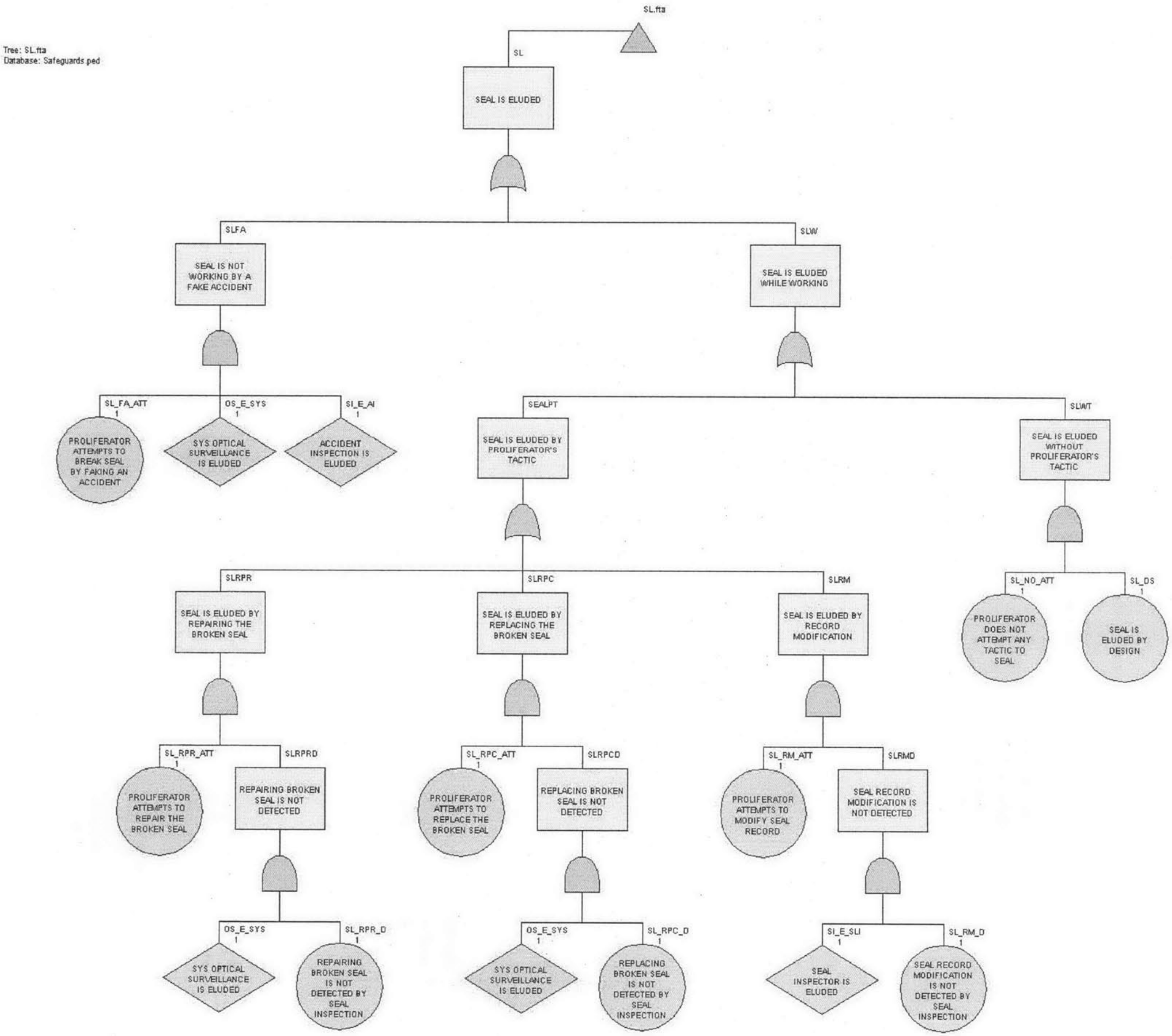

OS.fta
OS
OPTICAL SURVEILLANCE SYSTEM IS ELUDED
OSFA
OPTICAL SURVEILLANCE SYSTEM IS NOT WORKING BY A FAKE ACCIDENT
OSW
OPTICAL SURVEILLANCE SYSTEM IS ELUDED WHILE WORKING
OS_FA_ATT
1
PROLIFERATOR ATTEMPTS TO BREAK OS BY FAKING AN ACCIDENT
SI_E_AI
1
ACCIDENT INSPECTION IS ELUDED
OSPT
OS IS ELUDED BY PROLIFERATOR'S TACTIC
OSWT
OS IS ELUDED WITHOUT PROLIFERATOR'S TACTIC
OSDHM
OS IS ELUDED BY DETECTOR/HARDWARE MODIFICATION
OSSDM
OS IS ELUDED BY SIGNAL/DATA MODIFICATION
OS_NO_ATT
1
PROLIFERATOR DOES NOT ATTEMPT ANY TACTIC TO OS
OS_DS
1
OPTICAL SURVEILLANCE IS ELUDED BY DESIGN
OS_DHM_ATT
1
PROLIFERATOR ATTEMPTS TO MODIFY OS DETECTOR/ HARDWARE
OSDHMD
OS DETECTOR/ HARDWARE MODIFICATION IS NOT DETECTED
OS_SDM_ATT
1
PROLIFERATOR ATTEMPTS TO MODIFY OS SIGNAL/DATA
OSSDMD
OS SIGNAL/DATA MODIFICAITON IS NOT DETECTED
SL_E_SYS
1
SYSTEM SEAL IS ELUDED
OS_DHM_D
1
DETECTOR/ HARDWARE MODIFICATION IS NOT DETECTED BY OS
SL_E_SYS
1
SYSTEM SEAL IS ELUDED
OS_SDM_D
1
SIGNAL/DATA MODIFICATION IS NOT DETECTED BY OS

2. Containment and Surveillance

2.1 Optical Surveillance (OS)

Basic events descriptions of optical surveillance success tree

Proliferator Tactic	Specific Tactic Examples	Sub-tree Events
Proliferator does not attempt any tactic to OS (OS_NO_ATT) Proliferator does not attempt any tactic to prevent OS from detecting the diversion	• Proliferator diverts the material with small enough amount per attempt such that OS has low probability of detecting the diversion	• **Optical Surveillance is eluded by designed (OS_DS)** Optical surveillance does not detect the material diversion because of its detection efficiency
Proliferator attempts to break OS by faking an accident (OS_FA_ATT) Proliferator attempts to stage a fake accident that will break the functionality of the OS	• Proliferator stages a fake electrical system that cut the power to the OS system • Proliferator stages a fake fire accident that breaks OS system hardware	• **Accident inspection is eluded (SI_E_AI)** The accident inspection by the inspector cannot detect that it has been staged
Proliferator attempts to modify OS detector/ hardware (OS_DHM_ATT) Proliferator attempts to modify the detector or hardware of the OS system, preventing it from detecting material diversion activity	• Proliferator modifies the digital OS camera to avoid displaying and storage of material diversion images • Proliferator moves the camera to another location that it will give the same images	• **System seal is eluded (SL_E_SYS)** Seal of the OS system does not show that it has been opened • **Detector/Hardware modification is not detected by OS (OS_DHM_D)** Optical surveillance system does not detect that its detector/hardware has been modified
Proliferator attempts to modify OS signal/data (OS_SDM_ATT) Proliferator attempts to modify the signal between OS camera and the processing unit or modify the record data to remove the detection images	• Proliferator feed a fake images to the processing unit • Proliferator hacks the OS system software to always display and store expected images • Proliferator access and modifies the stored data before the inspection	• **System seal is eluded (SL_E_SYS)** Seal of the OS system does not show that it has been opened • **Signal/data modification is not detected by OS (OS_SDM_D)** Optical surveillance software system and data encryption does not detect that its signal/data has been modified

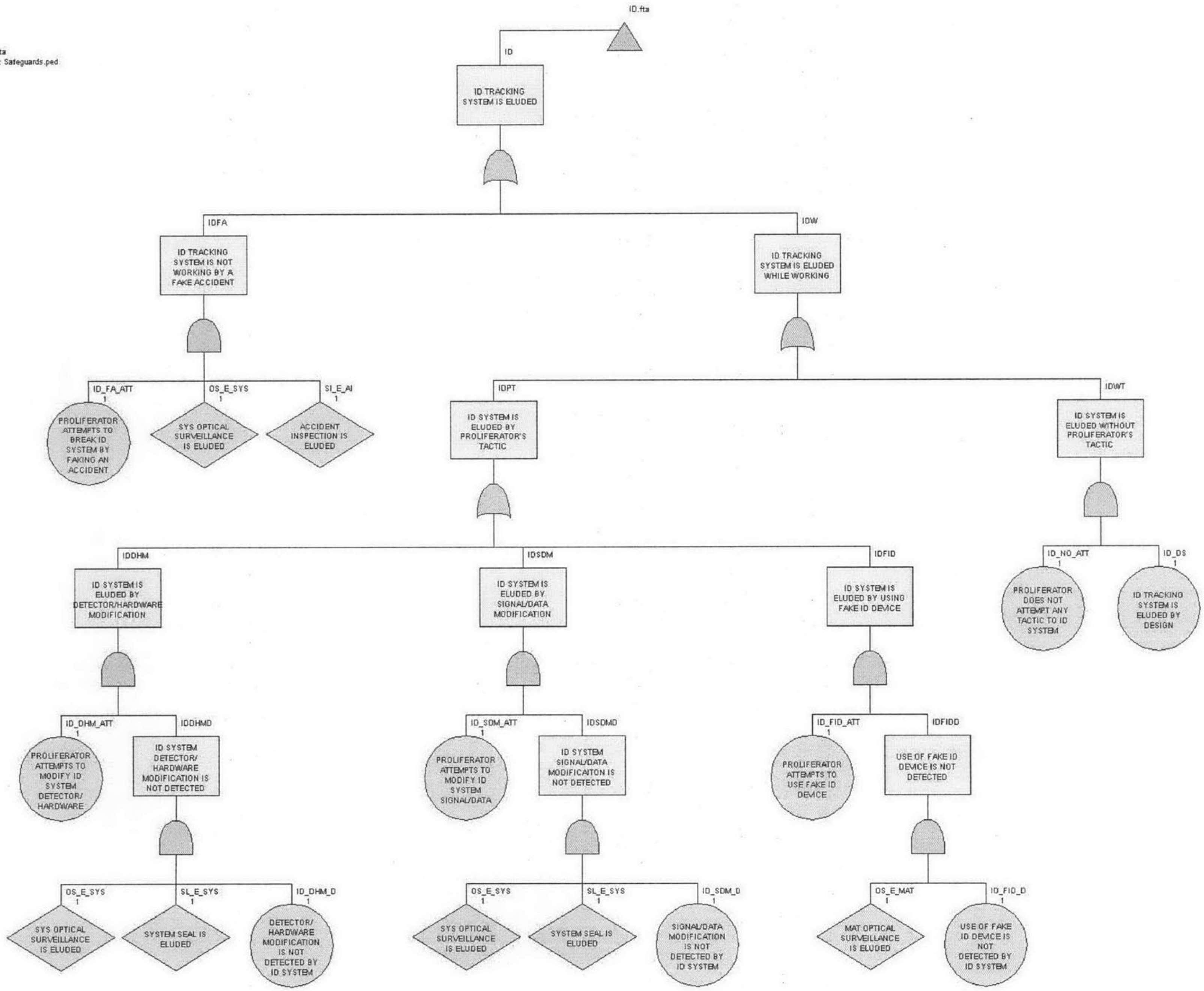

Tree: SL.fta
Database: Safeguards.ped
SL.fta
SL
SEAL IS ELUDED
SLFA
SEAL IS NOT WORKING BY A FAKE ACCIDENT
SLW
SEAL IS ELUDED WHILE WORKING
SL_FA_ATT
1
PROLIFERATOR ATTEMPTS TO BREAK SEAL BY FAKING AN ACCIDENT
OS_E_SYS
1
SYS OPTICAL SURVEILLANCE IS ELUDED
SI_E_AI
1
ACCIDENT INSPECTION IS ELUDED
SEALPT
SEAL IS ELUDED BY PROLIFERATOR'S TACTIC
SLWT
SEAL IS ELUDED WITHOUT PROLIFERATOR'S TACTIC
SLRPR
SEAL IS ELUDED BY REPAIRING THE BROKEN SEAL
SLRPC
SEAL IS ELUDED BY REPLACING THE BROKEN SEAL
SLRM
SEAL IS ELUDED BY RECORD MODIFICATION
SL_NO_ATT
1
PROLIFERATOR DOES NOT ATTEMPT ANY TACTIC TO SEAL
SL_DS
1
SEAL IS ELUDED BY DESIGN
SL_RPR_ATT
1
PROLIFERATOR ATTEMPTS TO REPAIR THE BROKEN SEAL
SLRPRD
REPAIRING BROKEN SEAL IS NOT DETECTED
SL_RPC_ATT
1
PROLIFERATOR ATTEMPTS TO REPLACE THE BROKEN SEAL
SLRPCD
REPLACING BROKEN SEAL IS NOT DETECTED
SL_RM_ATT
1
PROLIFERATOR ATTEMPTS TO MODIFY SEAL RECORD
SLRMD
SEAL RECORD MODIFICATION IS NOT DETECTED
OS_E_SYS
1
SYS OPTICAL SURVEILLANCE IS ELUDED
SL_RPR_D
1
REPAIRING BROKEN SEAL IS NOT DETECTED BY SEAL INSPECTION
OS_E_SYS
1
SYS OPTICAL SURVEILLANCE IS ELUDED
SL_RPC_D
1
REPLACING BROKEN SEAL IS NOT DETECTED BY SEAL INSPECTION
SI_E_SLI
1
SEAL INSPECTOR IS ELUDED
SL_RM_D
1
SEAL RECORD MODIFICATION IS NOT DETECTED BY SEAL INSPECTION

2.2 Seal (SL)

Basic events descriptions of seal success tree

Proliferator Tactic	Specific Tactic Examples	Sub-tree Events
Proliferator does not attempt any tactic to SL (SL_NO_ATT) Proliferator does not attempt any tactic to prevent SL from detecting the diversion	• Proliferator diverts the material without having to break the seal or the probability that the seal inspection will detect that that seal has been broken is low	• **Seal is eluded by designed (SL_DS)** Seal does not detect the material diversion because of its detection efficiency
Proliferator attempts to break seal by faking an accident (SL_FA_ATT) Proliferator attempts to stage a fake accident that will break the seal	• Proliferator stages a fake fire or collision accident that breaks the seal	• **Optical surveillance is eluded (OS_E_SYS)** Optical surveillance does not detect that the proliferator stages a fake accident • **Accident inspection is eluded (SI_E_AI)** The accident inspection by the inspector cannot detect that it has been staged
Proliferator attempts to repair the broken seal (SL_RPR_ATT) Proliferator attempts to repair the seal that has been broken by them to access the material/system	• Proliferator reattach the wire of the E-cup seal • Proliferator reset the VACOSS seal	• **Optical surveillance is eluded(OS_E_SYS)** Optical surveillance does not detect that the proliferator repairs the broken seal • **Repairing broken seal is not detected by seal inspection (SL_RPR_D)** Seal inspection does not detect that the seal was broken and has been repaired
Proliferator attempts to replace the broken seal (SL_RPC_ATT) Proliferator attempts to replace the broken seal that has been broken with a new similar seal	• Proliferator replace E-cup or VACOSS seal with a new similar unit	• **Optical surveillance is eluded (OS_E_SYS)** Optical surveillance does not detect that the proliferator replace the broken seal • **Replacing broken seal is not detected by seal inspection (SL_RPC_D)** Seal inspection does not detect that the seal was broken and has been replaced
Proliferator attempts to modify seal record (SL_RM_ATT) Proliferator attempts to modify the record of the state of the seal during the inspection	• The seal inspector does not report the correct record of the state of the seal	• **Seal inspector is eluded (SI_E_SLI)** Seal inspector does not report that the seal has been broken • **Seal record modification is not detected by seal inspection (SL_RM_D)** Seal inspection does not detect that the seal record has been modified

Tree: ID.fta
Database: Safeguards.ped


ID.fta
ID
ID TRACKING SYSTEM IS ELUDED
IDFA
ID TRACKING SYSTEM IS NOT WORKING BY A FAKE ACCIDENT
IDW
ID TRACKING SYSTEM IS ELUDED WHILE WORKING
ID_FA_ATT
1
PROLIFERATOR ATTEMPTS TO BREAK ID SYSTEM BY FAKING AN ACCIDENT
OS_E_SYS
1
SYS OPTICAL SURVEILLANCE IS ELUDED
SI_E_AI
1
ACCIDENT INSPECTION IS ELUDED
IDPT
ID SYSTEM IS ELUDED BY PROLIFERATOR'S TACTIC
IDWT
ID SYSTEM IS ELUDED WITHOUT PROLIFERATOR'S TACTIC
IDDHM
ID SYSTEM IS ELUDED BY DETECTOR/HARDWARE MODIFICATION
IDSDM
ID SYSTEM IS ELUDED BY SIGNAL/DATA MODIFICATION
IDFID
ID SYSTEM IS ELUDED BY USING FAKE ID DEVICE
ID_NO_ATT
1
PROLIFERATOR DOES NOT ATTEMPT ANY TACTIC TO ID SYSTEM
ID_DS
1
ID TRACKING SYSTEM IS ELUDED BY DESIGN
ID_DHM_ATT
1
PROLIFERATOR ATTEMPTS TO MODIFY ID SYSTEM DETECTOR/ HARDWARE
IDDHMD
ID SYSTEM DETECTOR/ HARDWARE MODIFICATION IS NOT DETECTED
ID_SDM_ATT
1
PROLIFERATOR ATTEMPTS TO MODIFY ID SYSTEM SIGNAL/DATA
IDSDMD
ID SYSTEM SIGNAL/DATA MODIFICAITON IS NOT DETECTED
ID_FID_ATT
1
PROLIFERATOR ATTEMPTS TO USE FAKE ID DEVICE
IDFIDD
USE OF FAKE ID DEVICE IS NOT DETECTED
OS_E_SYS
1
SYS OPTICAL SURVEILLANCE IS ELUDED
SL_E_SYS
1
SYSTEM SEAL IS ELUDED
ID_DHM_D
1
DETECTOR/ HARDWARE MODIFICATION IS NOT DETECTED BY ID SYSTEM
OS_E_SYS
1
SYS OPTICAL SURVEILLANCE IS ELUDED
SL_E_SYS
1
SYSTEM SEAL IS ELUDED
ID_SDM_D
1
SIGNAL/DATA MODIFICATION IS NOT DETECTED BY ID SYSTEM
OS_E_MAT
1
MAT OPTICAL SURVEILLANCE IS ELUDED
ID_FID_D
1
USE OF FAKE ID DEVICE IS NOT DETECTED BY ID SYSTEM

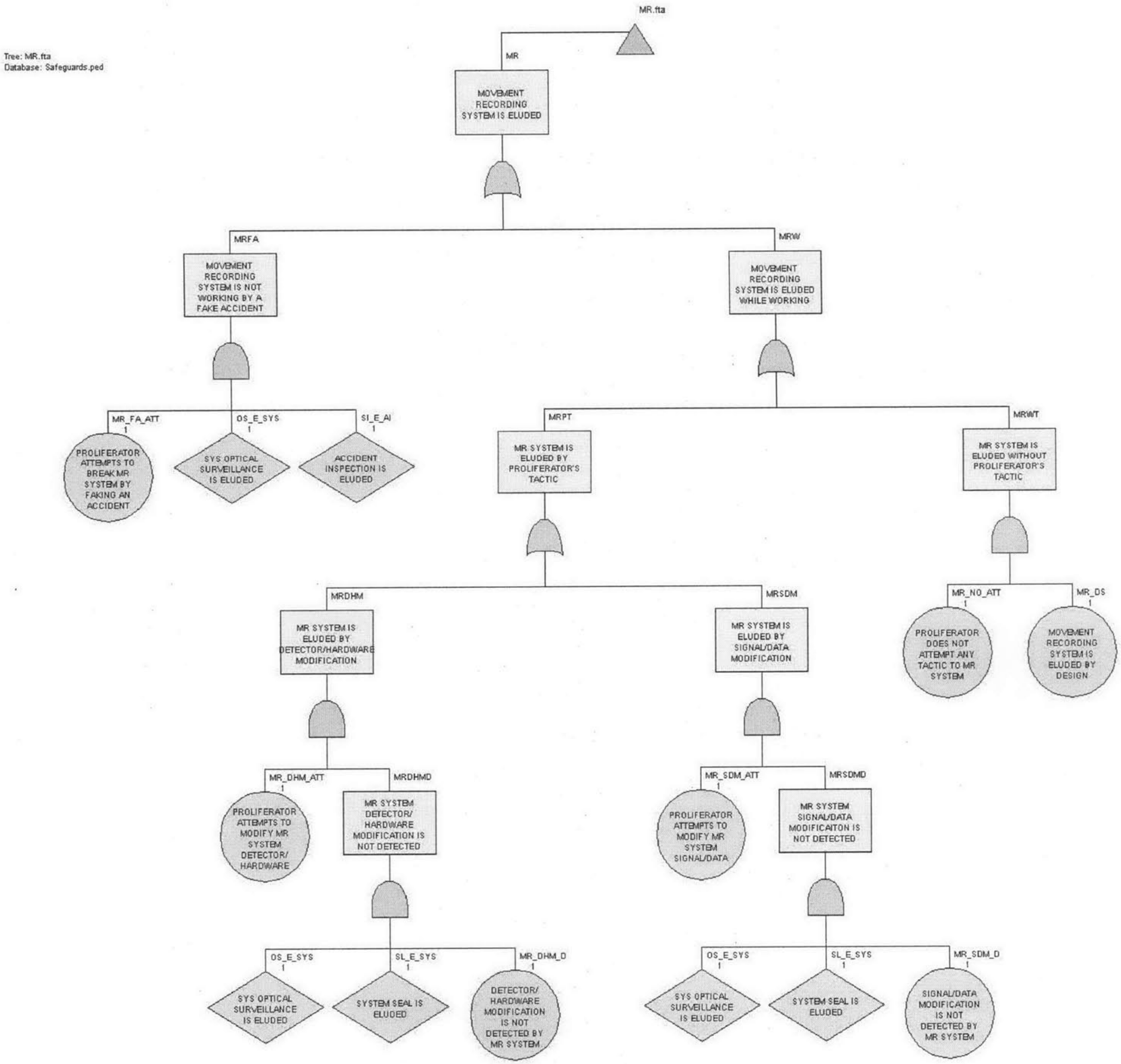
3. Operation Monitoring

3.1 ID Tracking (ID)

Basic events descriptions of ID tracking success tree

Proliferator Tactic	Specific Tactic Examples	Sub-tree Events
Proliferator does not attempt any tactic to ID tracking (ID_NO_ATT) Proliferator does not attempt any tactic to prevent ID tracking from detecting the diversion	• Proliferator diverts the material with small enough amount per attempt such that ID tracking has low probability of detecting the diversion	• **ID tracking is eluded by designed (DA_DS)** ID tracking does not detect the material diversion because of its detection efficiency
Proliferator attempts to break ID system by faking an accident (ID_FA_ATT) Proliferator attempts to stage a fake accident that will break the functionality of the ID tracking system	• Proliferator stages a fake electrical system that cut the power to the ID tracking sensor • Proliferator stages a fake fire accident that break the ID tracking device	• **Optical surveillance is eluded (OS_E_SYS)** Optical surveillance does not detect that the proliferator stages a fake accident • **Accident inspection is eluded (SI_E_AI)** The accident inspection by the inspector cannot detect that it has been staged
Proliferator attempts to modify ID system detector/ hardware (ID_DHM_ATT) Proliferator attempts to modify the detector or hardware of the ID system, preventing it from detecting material diversion activity	• Proliferator modifies the ID detector to send a tracking signal without actually detecting the actual device	• **System optical surveillance is eluded (OS_E_SYS)** Optical surveillance does not detect that the proliferator tampers with the ID system detector/hardware • **System seal is eluded (SL_E_SYS)** Seal of the ID system does not show that it has been opened • **Detector/Hardware modification is not detected by ID system (ID_DHM_D)** ID tracking system does not detect that its detector/hardware has been modified
Proliferator attempts to modify ID system signal/data (ID_SDM_ATT) Proliferator attempts to modify the signal between ID detector and the processing unit or modify the record data to change the detection signal	• Proliferator feed a fake detector signal to the processing unit • Proliferator modifies ID system software to add or remove ID tracking record • Proliferator access and modifies the stored ID tracking data before the inspection	• **System optical surveillance is eluded (OS_E_SYS)** Optical surveillance does not detect that the proliferator tampers with the ID tracking processing system to modify the signal/data • **System seal is eluded (SL_E_SYS)** Seal of the ID system does not show that it has been opened • **Signal/data modification is not detected by ID system (ID_SDM_D)** ID tracking system signal and data encryption does not detect that its signal/data has been modified

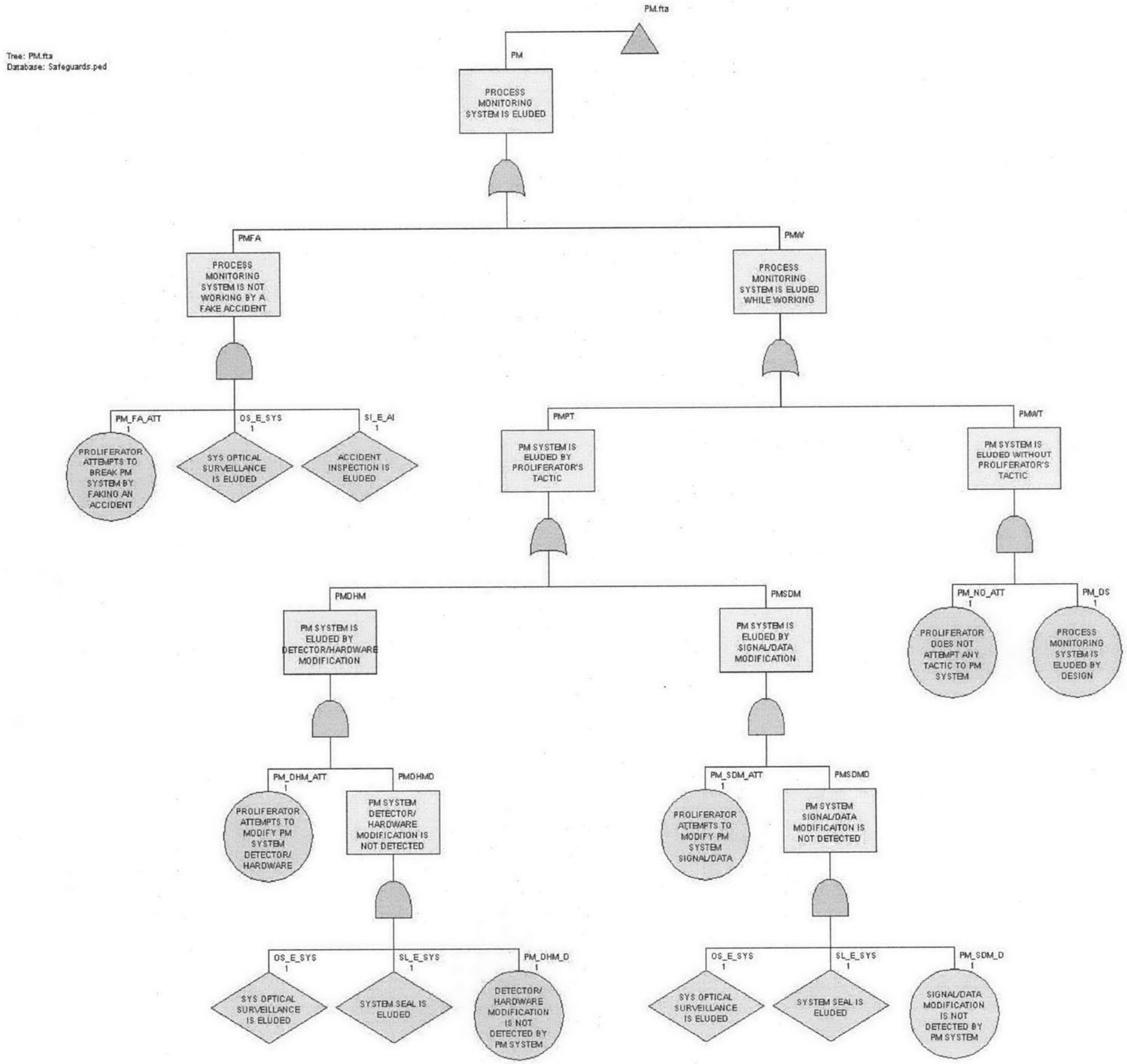
Proliferator Tactic	Specific Tactic Examples	Sub-tree Events
Proliferator attempts to use fake ID device (ID_FID_ATT) Proliferator attempts to use a fake ID device to fool the ID tracking system	• Proliferator creates a fake ID device and put it through the detector to fool the system that the it is the actual device attach to the material	• **Material optical surveillance is eluded (OS_E_MAT)** Optical surveillance does not detect that the proliferator use a fake ID device • **Use of fake ID device is not detected by ID system(ID_FID_D)** ID tracking system does not detect that the ID device is fake one


Tree: MR.fta
Database: Safeguards.ped
MR.fta
MR
MOVEMENT RECORDING SYSTEM IS ELUDED
MRFA
MOVEMENT RECORDING SYSTEM IS NOT WORKING BY A FAKE ACCIDENT
MRW
MOVEMENT RECORDING SYSTEM IS ELUDED WHILE WORKING
MR_FA_ATT 1
PROLIFERATOR ATTEMPTS TO BREAK MR SYSTEM BY FAKING AN ACCIDENT
OS_E_SYS 1
SYS OPTICAL SURVEILLANCE IS ELUDED
SI_E_AI 1
ACCIDENT INSPECTION IS ELUDED
MRPT
MR SYSTEM IS ELUDED BY PROLIFERATOR'S TACTIC
MRWT
MR SYSTEM IS ELUDED WITHOUT PROLIFERATOR'S TACTIC
MR_NO_ATT 1
PROLIFERATOR DOES NOT ATTEMPT ANY TACTIC TO MR SYSTEM
MR_DS 1
MOVEMENT RECORDING SYSTEM IS ELUDED BY DESIGN
MRDHM
MR SYSTEM IS ELUDED BY DETECTOR/HARDWARE MODIFICATION
MRSDM
MR SYSTEM IS ELUDED BY SIGNAL/DATA MODIFICATION
MR_DHM_ATT 1
PROLIFERATOR ATTEMPTS TO MODIFY MR SYSTEM DETECTOR/ HARDWARE
MRDHMD
MR SYSTEM DETECTOR/ HARDWARE MODIFICATION IS NOT DETECTED
MR_SDM_ATT 1
PROLIFERATOR ATTEMPTS TO MODIFY MR SYSTEM SIGNAL/DATA
MRSDMD
MR SYSTEM SIGNAL/DATA MODIFICAITON IS NOT DETECTED
OS_E_SYS 1
SYS OPTICAL SURVEILLANCE IS ELUDED
SL_E_SYS 1
SYSTEM SEAL IS ELUDED
MR_DHM_D 1
DETECTOR/ HARDWARE MODIFICATION IS NOT DETECTED BY MR SYSTEM
OS_E_SYS 1
SYS OPTICAL SURVEILLANCE IS ELUDED
SL_E_SYS 1
SYSTEM SEAL IS ELUDED
MR_SDM_D 1
SIGNAL/DATA MODIFICATION IS NOT DETECTED BY MR SYSTEM

3.2 Movement Recording (MR)

Basic events descriptions of movement recording success tree

Proliferator Tactic	Specific Tactic Examples	Sub-tree Events
Proliferator does not attempt any tactic to MR (MR_NO_ATT) Proliferator does not attempt any tactic to prevent MR from detecting the diversion	• Proliferator diverts the material with small enough amount per attempt such that MR has low probability of detecting the diversion	• **Movement recording is eluded by designed (MR_DS)** Movement recording does not detect the material diversion because of its detection efficiency
Proliferator attempts to break MR system by faking an accident (MR_FA_ATT) Proliferator attempts to stage a fake accident that will break the functionality of the MR system	• Proliferator stages a fake electrical system that cut the power to the MR system • Proliferator stages a fake fire accident that break the MR system hardware	• **Optical surveillance is eluded (OS_E_SYS)** Optical surveillance does not detect that the proliferator stages a fake accident • **Accident inspection is eluded (SI_E_AI)** The accident inspection by the inspector cannot detect that it has been staged
Proliferator attempts to modify MR system detector/ hardware (MR_DHM_ATT) Proliferator attempts to modify the detector or hardware of the MR system, preventing it from detecting material diversion activity	• Proliferator modifies the MR sensor to not send the movement signal • Proliferator relocates the sensor, preventing it from detecting the material movement	• **System optical surveillance is eluded (OS_E_SYS)** Optical surveillance does not detect that the proliferator tampers with the MR system detector/hardware • **System seal is eluded (SL_E_SYS)** Seal of the MR system does not show that it has been opened • **Detector/Hardware modification is not detected by MR system (MR_DHM_D)** MR tracking system does not detect that its detector/hardware has been modified
Proliferator attempts to modify MR system signal/data (MR_SDM_ATT) Proliferator attempts to modify the signal between MR detector and the processing unit or modify the record data to change the detection signal	• Proliferator feed a fake detector signal to the processing unit • Proliferator modifies MR system software to add or remove movement record • Proliferator access and modifies the stored MR data before the inspection	• **System optical surveillance is eluded (OS_E_SYS)** Optical surveillance does not detect that the proliferator tampers with the MR tracking processing system to modify the signal/data • **System seal is eluded (SL_E_SYS)** Seal of the MR system does not show that it has been opened • **Signal/data modification is not detected by MR system (MR_SDM_D)** MR system signal and data encryption does not detect that its signal/data has been modified

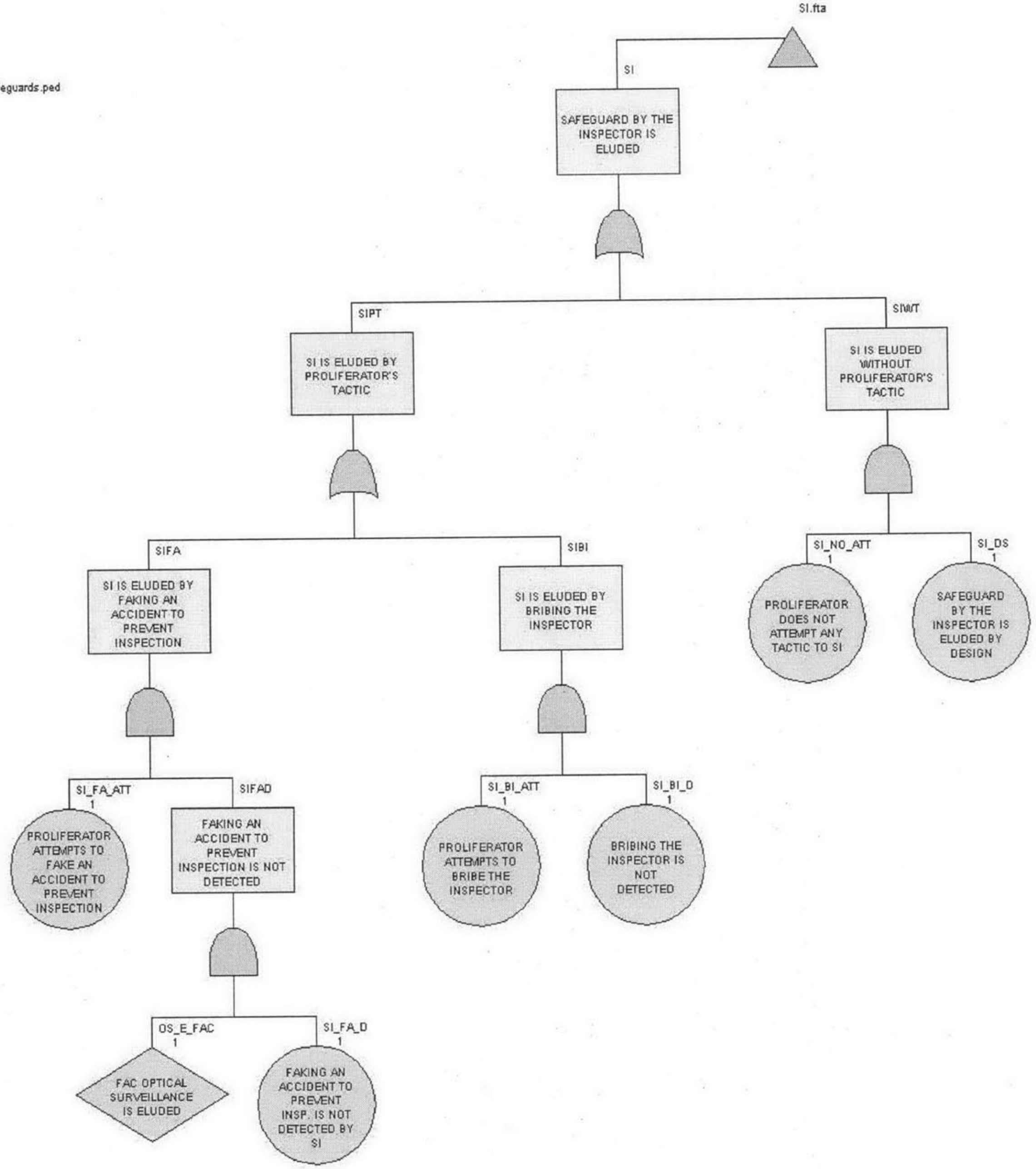

Tree: PM.fta
Database: Safeguards.ped
PM.fta
PM
PROCESS MONITORING SYSTEM IS ELUDED
PMFA
PROCESS MONITORING SYSTEM IS NOT WORKING BY A FAKE ACCIDENT
PMW
PROCESS MONITORING SYSTEM IS ELUDED WHILE WORKING
PM_FA_ATT
1
PROLIFERATOR ATTEMPTS TO BREAK PM SYSTEM BY FAKING AN ACCIDENT
OS_E_SYS
1
SYS OPTICAL SURVEILLANCE IS ELUDED
SI_E_AI
1
ACCIDENT INSPECTION IS ELUDED
PMPT
PM SYSTEM IS ELUDED BY PROLIFERATOR'S TACTIC
PMWT
PM SYSTEM IS ELUDED WITHOUT PROLIFERATOR'S TACTIC
PM_NO_ATT
1
PROLIFERATOR DOES NOT ATTEMPT ANY TACTIC TO PM SYSTEM
PM_DS
1
PROCESS MONITORING SYSTEM IS ELUDED BY DESIGN
PMDHM
PM SYSTEM IS ELUDED BY DETECTOR/HARDWARE MODIFICATION
PMSDM
PM SYSTEM IS ELUDED BY SIGNAL/DATA MODIFICATION
PM_DHM_ATT
1
PROLIFERATOR ATTEMPTS TO MODIFY PM SYSTEM DETECTOR/ HARDWARE
PMDHMD
PM SYSTEM DETECTOR/ HARDWARE MODIFICATION IS NOT DETECTED
PM_SDM_ATT
1
PROLIFERATOR ATTEMPTS TO MODIFY PM SYSTEM SIGNAL/DATA
PMSDMD
PM SYSTEM SIGNAL/DATA MODIFICAITON IS NOT DETECTED
OS_E_SYS
1
SYS OPTICAL SURVEILLANCE IS ELUDED
SL_E_SYS
1
SYSTEM SEAL IS ELUDED
PM_DHM_D
1
DETECTOR/ HARDWARE MODIFICATION IS NOT DETECTED BY PM SYSTEM
OS_E_SYS
1
SYS OPTICAL SURVEILLANCE IS ELUDED
SL_E_SYS
1
SYSTEM SEAL IS ELUDED
PM_SDM_D
1
SIGNAL/DATA MODIFICATION IS NOT DETECTED BY PM SYSTEM

3.3 Process Monitoring (PM)

Basic events descriptions of process monitoring success tree

Proliferator Tactic	Specific Tactic Examples	Sub-tree Events
Proliferator does not attempt any tactic to PM (PM_NO_ATT) Proliferator does not attempt any tactic to prevent PM from detecting the diversion	• Proliferator diverts the material with small enough amount per attempt such that PM has low probability of detecting the diversion	• **Process monitoring is eluded by designed (PM_DS)** Process monitoring does not detect the material diversion because of its detection efficiency
Proliferator attempts to break PM system by faking an accident (PM_FA_ATT) Proliferator attempts to stage a fake accident that will break the functionality of the PM system	• Proliferator stages a fake electrical system that cut the power to the PM system • Proliferator stages a fake fire accident that break the PM system hardware	• **Optical surveillance is eluded (OS_E_SYS)** Optical surveillance does not detect that the proliferator stages a fake accident • **Accident inspection is eluded (SI_E_AI)** The accident inspection by the inspector cannot detect that it has been staged
Proliferator attempts to modify PM system detector/ hardware (PM_DHM_ATT) Proliferator attempts to modify the detector or hardware of the PM system, preventing it from detecting material diversion activity	• Proliferator modifies the PM sensor to send the expected signal for current monitored processes	• **System optical surveillance is eluded(OS_E_SYS)** Optical surveillance does not detect that the proliferator tampers with the PM system detector/hardware • **System seal is eluded (SL_E_SYS)** Seal of the PM system does not show that it has been opened • **Detector/Hardware modification is not detected by PM system (PM_DHM_D)** PM tracking system does not detect that its detector/hardware has been modified
Proliferator attempts to modify PM system signal/data (PM_SDM_ATT) Proliferator attempts to modify the signal between PM detector and the processing unit or modify the record data to change the detection signal	• Proliferator feed a fake detector signal to the processing unit • Proliferator modifies PM system software to record expected process monitoring data • Proliferator access and modifies the stored PM data before the inspection	• **System optical surveillance is eluded (OS_E_SYS)** Optical surveillance does not detect that the proliferator tampers with the PM processing system to modify the signal/data • **System seal is eluded (SL_E_SYS)** Seal of the PM system does not show that it has been opened • **Signal/data modification is not detected by PM system (PM_SDM_D)** PM system signal and data encryption does not detect that its signal/data has been modified

Tree: SI.fta
Database: Safeguards.ped

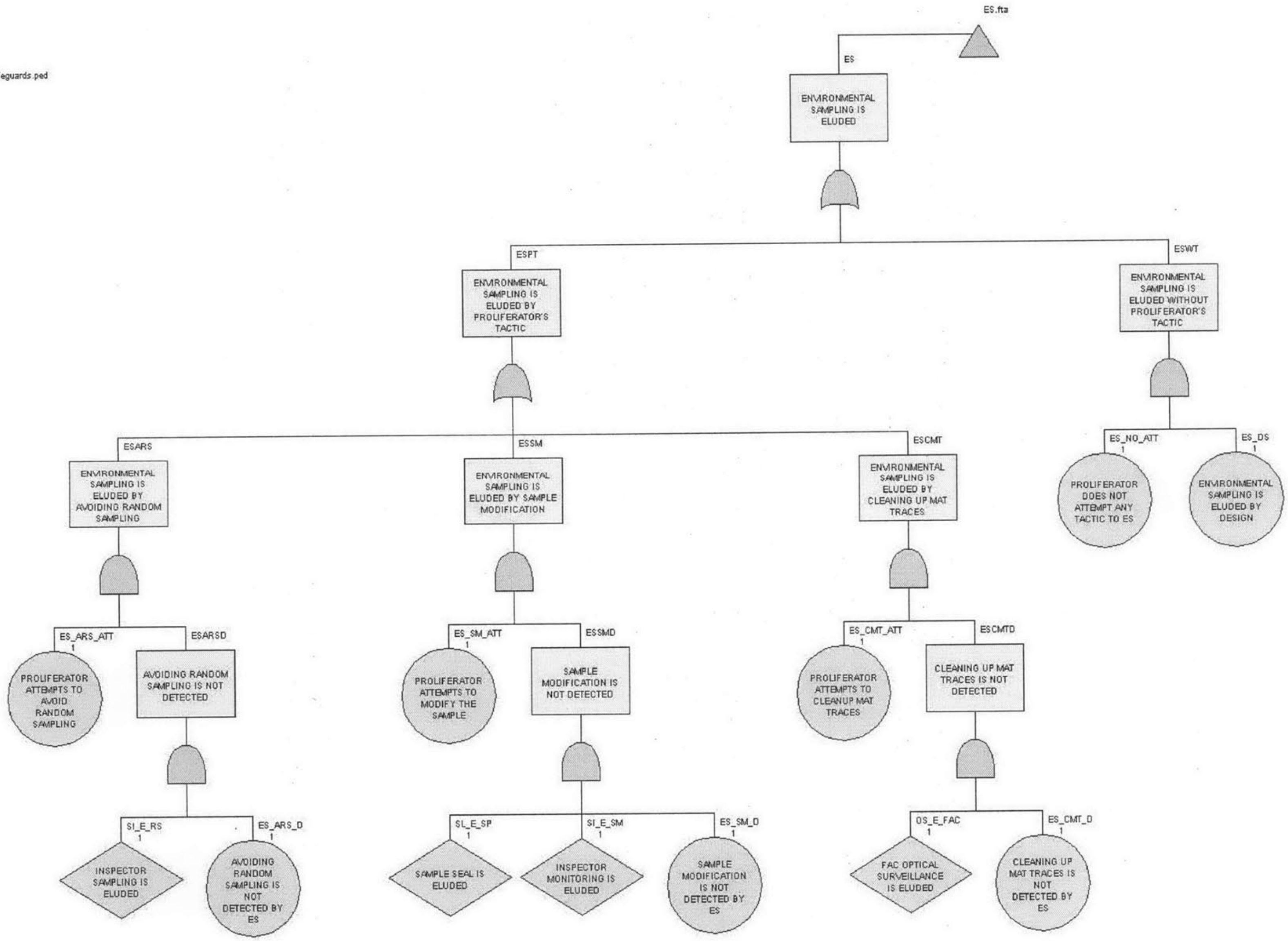

SI.fta
SI
SAFEGUARD BY THE INSPECTOR IS ELUDED
SIPT
SI IS ELUDED BY PROLIFERATOR'S TACTIC
SIWT
SI IS ELUDED WITHOUT PROLIFERATOR'S TACTIC
SIFA
SI IS ELUDED BY FAKING AN ACCIDENT TO PREVENT INSPECTION
SIBI
SI IS ELUDED BY BRIBING THE INSPECTOR
SI_NO_ATT
1
PROLIFERATOR DOES NOT ATTEMPT ANY TACTIC TO SI
SI_DS
1
SAFEGUARD BY THE INSPECTOR IS ELUDED BY DESIGN
SI_FA_ATT
1
PROLIFERATOR ATTEMPTS TO FAKE AN ACCIDENT TO PREVENT INSPECTION
SIFAD
FAKING AN ACCIDENT TO PREVENT INSPECTION IS NOT DETECTED
SI_BI_ATT
1
PROLIFERATOR ATTEMPTS TO BRIBE THE INSPECTOR
SI_BI_D
1
BRIBING THE INSPECTOR IS NOT DETECTED
OS_E_FAC
1
FAC OPTICAL SURVEILLANCE IS ELUDED
SI_FA_D
1
FAKING AN ACCIDENT TO PREVENT INSP. IS NOT DETECTED BY SI

3.4 Safeguard by the Inspector (SI)

Basic events descriptions of safeguard by the inspector success tree

Proliferator Tactic	Specific Tactic Examples	Sub-tree Events
Proliferator does not attempt any tactic to SI (SI_NO_ATT) Proliferator does not attempt any tactic to prevent SI from detecting the diversion	• Proliferator diverts the material with a scenario such that the probability of detecting the diversion by SI is low	• **Safeguard by the inspector is eluded by designed (SI_DS)** Safeguard by the inspector does not detect the material diversion because of its detection efficiency
Proliferator attempts to fake an accident to prevent inspection (SI_FA_ATT) Proliferator attempts to stage a fake accident that prevents the inspector to access and inspect certain areas	• Proliferator stages a radioactive material leak accident where the material has been diverted to prevent the inspector to collect a sample or does an inspection	• **Facility optical surveillance is eluded (OS_E_FAC)** Facility optical surveillance does not detect that the proliferator stages a fake accident • **Faking an accident to prevent inspection is not detected by SI (SI_FA_D)** Inspector does not detect that the preventing accident is staged by the proliferator
Proliferator attempts to bribe the inspector (SI_BI_ATT) Proliferator attempts to bribe the inspector	• Proliferator bribes the inspector to not report the material diversion detection • Proliferator bribes the inspector to collect sample from certain area • Proliferator bribes the inspector to modify safeguard detection record	• **Bribing the inspector is not detected (SI_BI_D)** Bribe is accepted by the inspector and the inspection agency does not detect that the inspector has been bribed

Tree: ES.fta
Database: Safeguards.ped



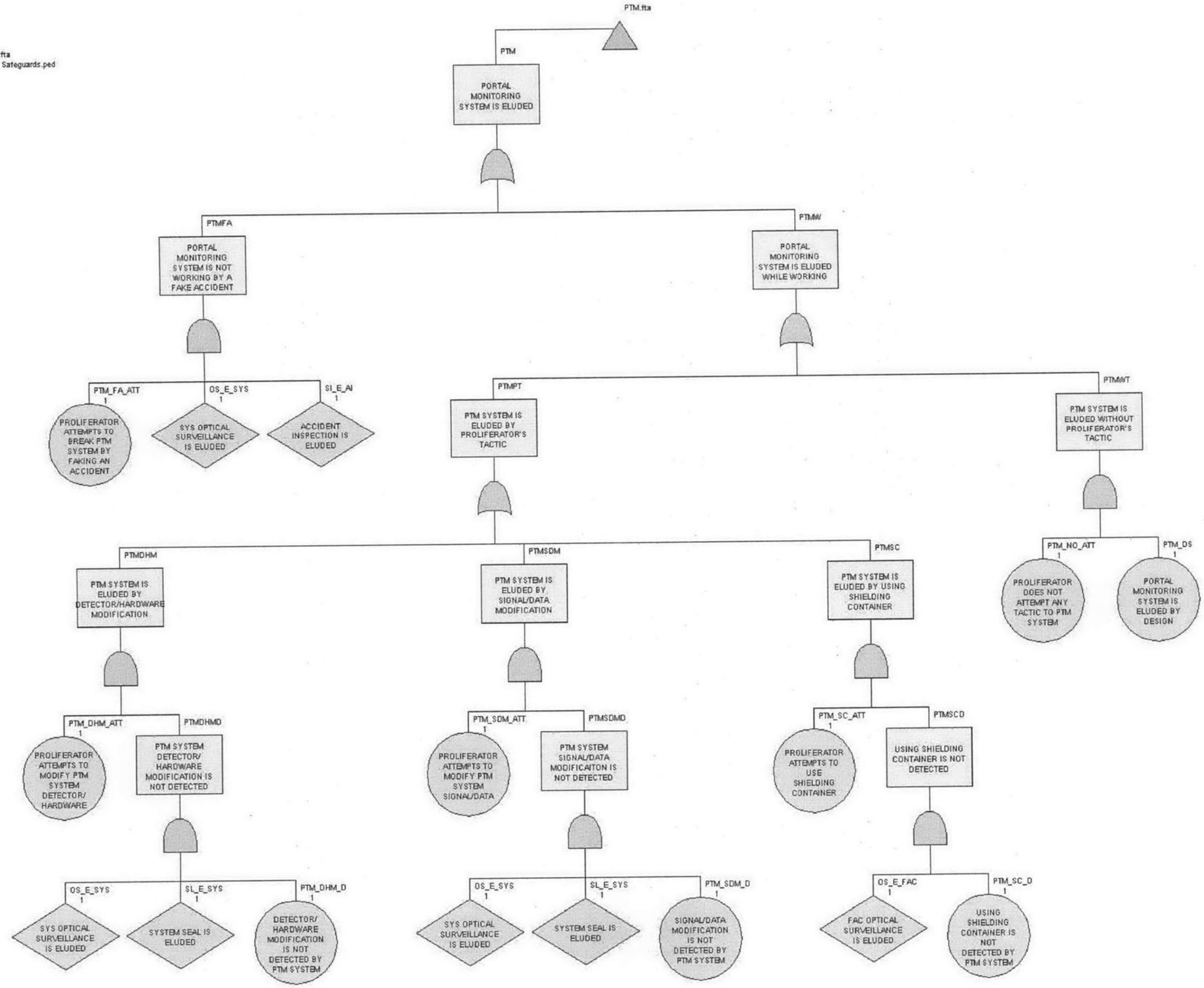
ES.fta
ES
ENVIRONMENTAL SAMPLING IS ELUDED
ESPT
ENVIRONMENTAL SAMPLING IS ELUDED BY PROLIFERATOR'S TACTIC
ESWT
ENVIRONMENTAL SAMPLING IS ELUDED WITHOUT PROLIFERATOR'S TACTIC
ESARS
ENVIRONMENTAL SAMPLING IS ELUDED BY AVOIDING RANDOM SAMPLING
ESSM
ENVIRONMENTAL SAMPLING IS ELUDED BY SAMPLE MODIFICATION
ESCMT
ENVIRONMENTAL SAMPLING IS ELUDED BY CLEANING UP MAT TRACES
ES_NO_ATT
1
PROLIFERATOR DOES NOT ATTEMPT ANY TACTIC TO ES
ES_DS
1
ENVIRONMENTAL SAMPLING IS ELUDED BY DESIGN
ES_ARS_ATT
1
PROLIFERATOR ATTEMPTS TO AVOID RANDOM SAMPLING
ESARSD
AVOIDING RANDOM SAMPLING IS NOT DETECTED
ES_SM_ATT
1
PROLIFERATOR ATTEMPTS TO MODIFY THE SAMPLE
ESSMD
SAMPLE MODIFICATION IS NOT DETECTED
ES_CMT_ATT
1
PROLIFERATOR ATTEMPTS TO CLEANUP MAT TRACES
ESCMTD
CLEANING UP MAT TRACES IS NOT DETECTED
SI_E_RS
1
INSPECTOR SAMPLING IS ELUDED
ES_ARS_D
1
AVOIDING RANDOM SAMPLING IS NOT DETECTED BY ES
SL_E_SP
1
SAMPLE SEAL IS ELUDED
SI_E_SM
1
INSPECTOR MONITORING IS ELUDED
ES_SM_D
1
SAMPLE MODIFICATION IS NOT DETECTED BY ES
OS_E_FAC
1
FAC OPTICAL SURVEILLANCE IS ELUDED
ES_CMT_D
1
CLEANING UP MAT TRACES IS NOT DETECTED BY ES

4. Environmental Sampling (ES)

Basic events descriptions of environmental sampling success tree

Proliferator Tactic	Specific Tactic Examples	Sub-tree Events
Proliferator does not attempt any tactic to ES (ES_NO_ATT) Proliferator does not attempt any tactic to prevent ES from detecting the diversion	• Proliferator diverts the material with small enough amount per attempt such that ES has low probability of detecting the diversion	• **Environmental sampling is eluded by designed (ES_DS)** Environmental sampling does not detect the material diversion because of its detection efficiency
Proliferator attempts to avoid random sampling (ES_ARS_ATT) Proliferator attempts to prevent the parts of facility that are in the material diversion pathway from being randomly collect by the inspector	• Proliferator prevent the inspector to collect a sample from the areas that are in the material diversion pathway • Proliferator prepared a sample or have a designated area for the inspector to collect a sample	• **Inspector sampling is eluded (SI_E_RS)** The inspector does not randomly collect sample from all parts of the facility inside the MBA • **Avoiding random sampling is not detected by ES (ES_ARS_D)** Environmental sampling analysis does not detect that the sample is not randomly collected
Proliferator attempts to modify the sample (ES_SM_ATT) Proliferator attempts to replace or modify the sample after it has been randomly collected by the inspector	• Proliferator swap the sample during the site inspection after it has been randomly collected by the inspector • Proliferator swap the sample during its transit from the site to the inspection agency laboratory	• **Sample seal is eluded (SL_E_SP)** Seal of the sample container does not show that it has been opened • **Inspector monitoring is eluded (SI_E_SM)** The inspector who monitor the sample does not detect the sample modification • **Sample modification is not detected by ES (ES_SM_D)** Environmental sampling analysis does not detect that the sample has been modified
Proliferator attempts to clean up material traces (ES_CMT_ATT) Proliferator attempts to clean up the traces of material diversion activities	• Proliferator remove the radiation traces of the diverted material in the diversion pathway	• **Optical surveillance is eluded (OS_E_FAC)** Optical surveillance does not detect that the proliferator tries to clean up the material traces • **Cleaning up material traces does is not detected by ES (ES_CMT_D)** Environmental sampling analysis does not detect that the proliferator tries to clean up the material traces

Tree: PTM.fta
Database: Safeguards.ped


PTM.fta
PTM
PORTAL MONITORING SYSTEM IS ELUDED
PTMFA
PORTAL MONITORING SYSTEM IS NOT WORKING BY A FAKE ACCIDENT
PTMW
PORTAL MONITORING SYSTEM IS ELUDED WHILE WORKING
PTM_FA_ATT
1
PROLIFERATOR ATTEMPTS TO BREAK PTM SYSTEM BY FAKING AN ACCIDENT
OS_E_SYS
1
SYS OPTICAL SURVEILLANCE IS ELUDED
SI_E_AI
1
ACCIDENT INSPECTION IS ELUDED
PTMPT
PTM SYSTEM IS ELUDED BY PROLIFERATOR'S TACTIC
PTMWT
PTM SYSTEM IS ELUDED WITHOUT PROLIFERATOR'S TACTIC
PTMDHM
PTM SYSTEM IS ELUDED BY DETECTOR/HARDWARE MODIFICATION
PTMSDM
PTM SYSTEM IS ELUDED BY SIGNAL/DATA MODIFICATION
PTMSC
PTM SYSTEM IS ELUDED BY USING SHIELDING CONTAINER
PTM_NO_ATT
1
PROLIFERATOR DOES NOT ATTEMPT ANY TACTIC TO PTM SYSTEM
PTM_DS
1
PORTAL MONITORING SYSTEM IS ELUDED BY DESIGN
PTM_DHM_ATT
1
PROLIFERATOR ATTEMPTS TO MODIFY PTM SYSTEM DETECTOR/ HARDWARE
PTMDHMD
PTM SYSTEM DETECTOR/ HARDWARE MODIFICATION IS NOT DETECTED
PTM_SDM_ATT
1
PROLIFERATOR ATTEMPTS TO MODIFY PTM SYSTEM SIGNAL/DATA
PTMSDMD
PTM SYSTEM SIGNAL/DATA MODIFICAITON IS NOT DETECTED
PTM_SC_ATT
1
PROLIFERATOR ATTEMPTS TO USE SHIELDING CONTAINER
PTMSCD
USING SHIELDING CONTAINER IS NOT DETECTED
OS_E_SYS
1
SYS OPTICAL SURVEILLANCE IS ELUDED
SL_E_SYS
1
SYSTEM SEAL IS ELUDED
PTM_DHM_D
1
DETECTOR/ HARDWARE MODIFICATION IS NOT DETECTED BY PTM SYSTEM
OS_E_SYS
1
SYS OPTICAL SURVEILLANCE IS ELUDED
SL_E_SYS
1
SYSTEM SEAL IS ELUDED
PTM_SDM_D
1
SIGNAL/DATA MODIFICATION IS NOT DETECTED BY PTM SYSTEM
OS_E_FAC
1
FAC OPTICAL SURVEILLANCE IS ELUDED
PTM_SC_D
1
USING SHIELDING CONTAINER IS NOT DETECTED BY PTM SYSTEM

4. Portal Monitoring (PTM)

Basic events descriptions of portal monitoring success tree

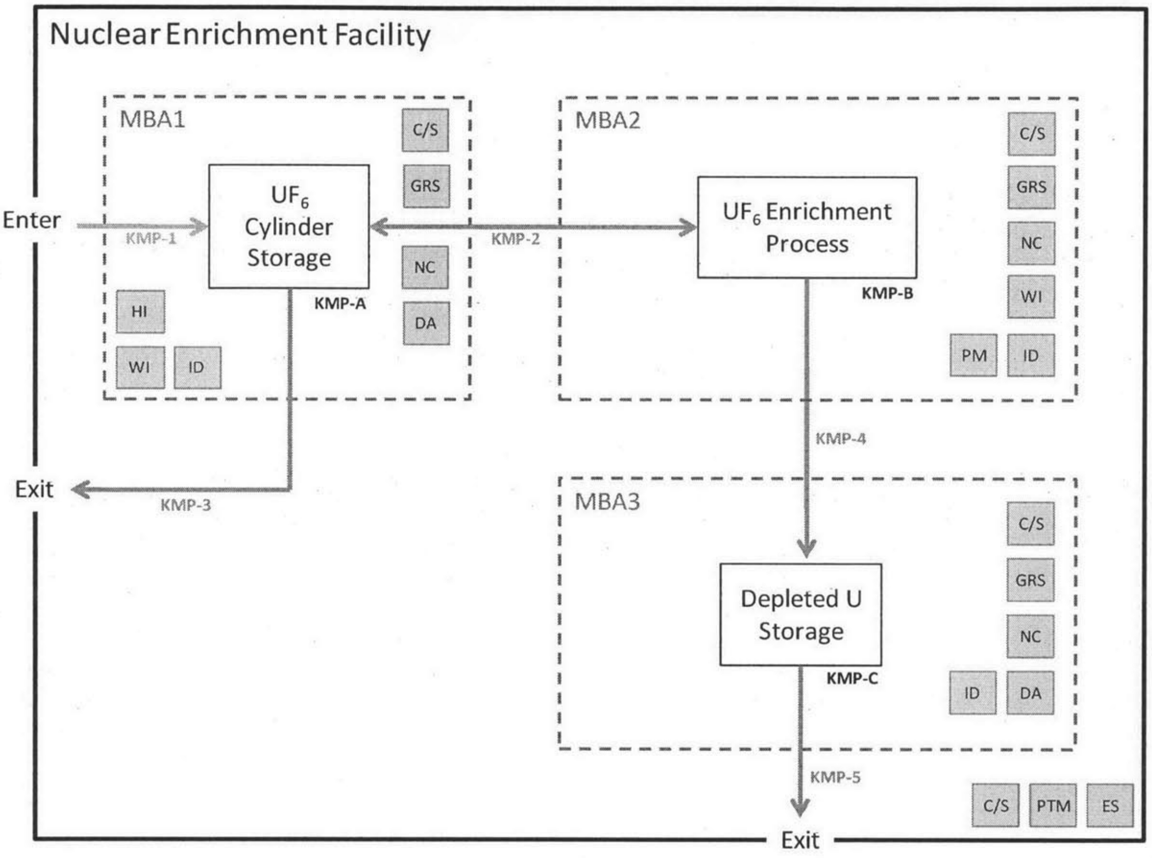
Proliferator Tactic	Specific Tactic Examples	Sub-tree Events
Proliferator does not attempt any tactic to PTM (PTM_NO_ATT) Proliferator does not attempt any tactic to prevent PTM from detecting the diversion	• Proliferator diverts the material with small enough amount per attempt such that PTM has low probability of detecting the diversion	• **Portal Monitoring is eluded by designed (PTM_DS)** Portal monitoring does not detect the material diversion because of its detection efficiency
Proliferator attempts to break PTM system by faking an accident (PTM_FA_ATT) Proliferator attempts to stage a fake accident that will break the functionality of the PTM system	• Proliferator stages a fake electrical system that cut the power to the PTM system • Proliferator stages a fake fire accident that break the PTM system hardware	• **System optical surveillance is eluded (OS_E_SYS)** Optical surveillance does not detect that the proliferator stages a fake accident • **Accident inspection is eluded (SI_E_AI)** The accident inspection by the inspector cannot detect that it has been staged
Proliferator attempts to modify PTM system detector/ hardware (PTM_DHM_ATT) Proliferator attempts to modify the detector or hardware of the PTM system, preventing it from detecting material diversion activity	• Proliferator modifies the PTM sensor to send the expected signal for current monitored processes	• **System optical surveillance is eluded(OS_E_SYS)** Optical surveillance does not detect that the proliferator tampers with the PTM system detector/hardware • **System seal is eluded (SL_E_SYS)** Seal of the PTM system does not show that it has been opened • **Detector/Hardware modification is not detected by PM system (PTM_DHM_D)** PTM tracking system does not detect that its detector/hardware has been modified
Proliferator attempts to modify PTM system signal/data (PTM_SDM_ATT) Proliferator attempts to modify the signal between PTM detector and the processing unit or modify the record data to change the detection signal	• Proliferator feed a fake detector signal to the processing unit • Proliferator modifies PTM system software to record expected portal monitoring data • Proliferator access and modifies the stored PTM data before the inspection	• **System optical surveillance is eluded (OS_E_SYS)** Optical surveillance does not detect that the proliferator tampers with the PTM processing system to modify the signal/data • **System seal is eluded (SL_E_SYS)** Seal of the PTM system does not show that it has been opened • **Signal/data modification is not detected by PTM system (PTM_SDM_D)** PTM system signal and data encryption does not detect that its signal/data has been modified

Proliferator Tactic	Specific Tactic Examples	Sub-tree Events
Proliferator attempts to use shielding container (PTM_SC_ATT) Proliferator attempts to use shielding container to shield the diverted material from being detected by the portal monitoring system	• Proliferator places the diverted material inside a iron, carbon steel, or stainless steel container to shield the gamma ray and neutron radiation from the diverted material • Proliferator places the diverted material with a heat sink to absorb the heat from the material	• **Facility optical surveillance is eluded (OS_E_FAC)** Facility optical surveillance does not detect that the proliferator place the diverted material inside a shielding container before going through PTM system • **Using shielding container is not detected by PTM system (PTM_SC_D)** PTM system does not detect that the proliferator use a shielding container to prevent detection of the diverted material

Appendix B: Safeguard Schemes in Nuclear Facilities

Nuclear Enrichment Facility

Fuel Enrichment Facility Type: Gas Centrifuge Enrichment Plant (GCEP), Gaseous Diffusion, and Electromagnetic Isotope Separation (EMIS). Material: 3-5% U-235 in the form of UF_6.



Material Balance Area (MBA)

Material Balance Area	Nuclear Material	Safeguards
MBA1:Feed Storage Area	UF_6 Cylinder	Containment and Surveillance Gamma Ray Spectrometry Neutron Counter Destructive Analysis ID Tracking Weight Inspection Heat Inspection
MBA2:Enrichment Process Area	UF_6 Cylinder	Containment and Surveillance Gamma Ray Spectrometry Neutron Counter ID Tracking Weight Inspection Process Monitoring

Material Balance Area	Nuclear Material	Safeguards
MBA3:Product Storage Area	Depleted U	Containment and Surveillance Gamma Ray Spectrometry Neutron Counter Destructive Analysis ID Tracking
Throughout Facility	Diverted Material	Containment and Surveillance Environmental Sampling Portal Monitoring

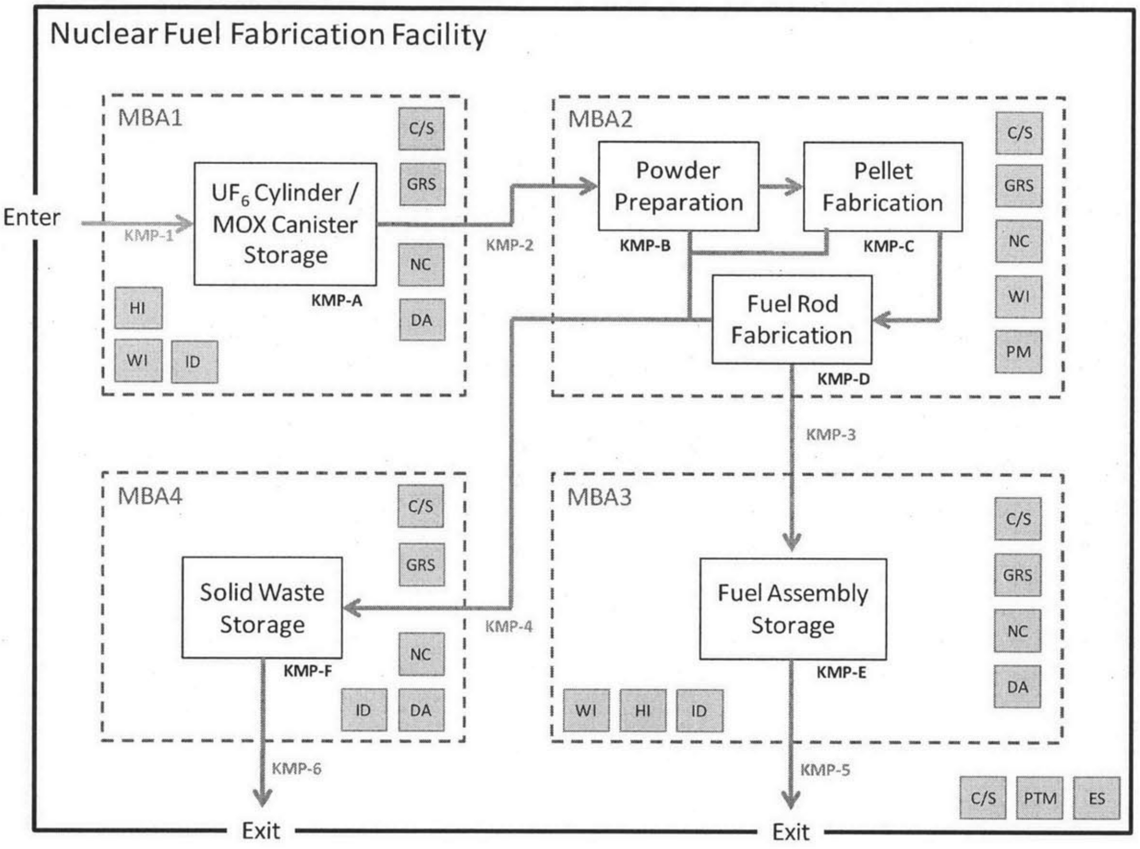
Key Measurement Point (KMP)

Inventory KMP	**Flow KMP**
• KMP-A: UF_6 Cylinder Storage • KMP-B: UF_6 Enrichment Process • KMP-C: Depleted U Storage	• KMP-1: Receipt of Feed UF_6 Cylinder • KMP-2: Transfer of UF_6 Cylinder between MBA1 and MBA2 • KMP-3: Shipment of Product UF_6 Cylinder • KMP-4: Transfer of Depleted U between MBA2 and MBA3 • KMP-5: Shipment of Depleted U

Nuclear Fuel Fabrication Facility

Fuel Fabrication Facility Type:

- Low Enriched Uranium (LEU) Fuel
  Material: 3-5% U-235 in the form of UF_6cylinder, fuel pellet, rod and assembly
- Mixed Oxide (MOX) /Transuranic (TRU)
  Material: MOX/TRU in the form of MOX/TRU canister, fuel pellet, rod and assembly



Material Balance Area (MBA)

Material Balance Area	Nuclear Material	Safeguards
MBA1:Feed Storage Area	UF_6 Cylinder MOX/TRU Canister	Containment and Surveillance Gamma Ray Spectrometry Neutron Counter Destructive Analysis ID Tracking Weight Inspection Heat Inspection
MBA2:Fuel Fabrication Process Area	UO_3/MOX/TRU Powder Fuel Pellet Fuel Rod Fuel Assembly	Containment and Surveillance Gamma Ray Spectrometry Neutron Counter Weight Inspection Process Monitoring

Material Balance Area	Nuclear Material	Safeguards
MBA3:Product Storage Area	Fuel Assembly (LEU/MOX/TRU)	Containment and Surveillance Gamma Ray Spectrometry Neutron Counter Destructive Analysis ID Tracking Weight Inspection Heat Inspection
MBA4:Waste Storage Area	Solid Waste	Containment and Surveillance Gamma Ray Spectrometry Neutron Counter ID Tracking Destructive Analysis
Throughout Facility	Diverted Material	Containment and Surveillance Environmental Sampling Portal Monitoring

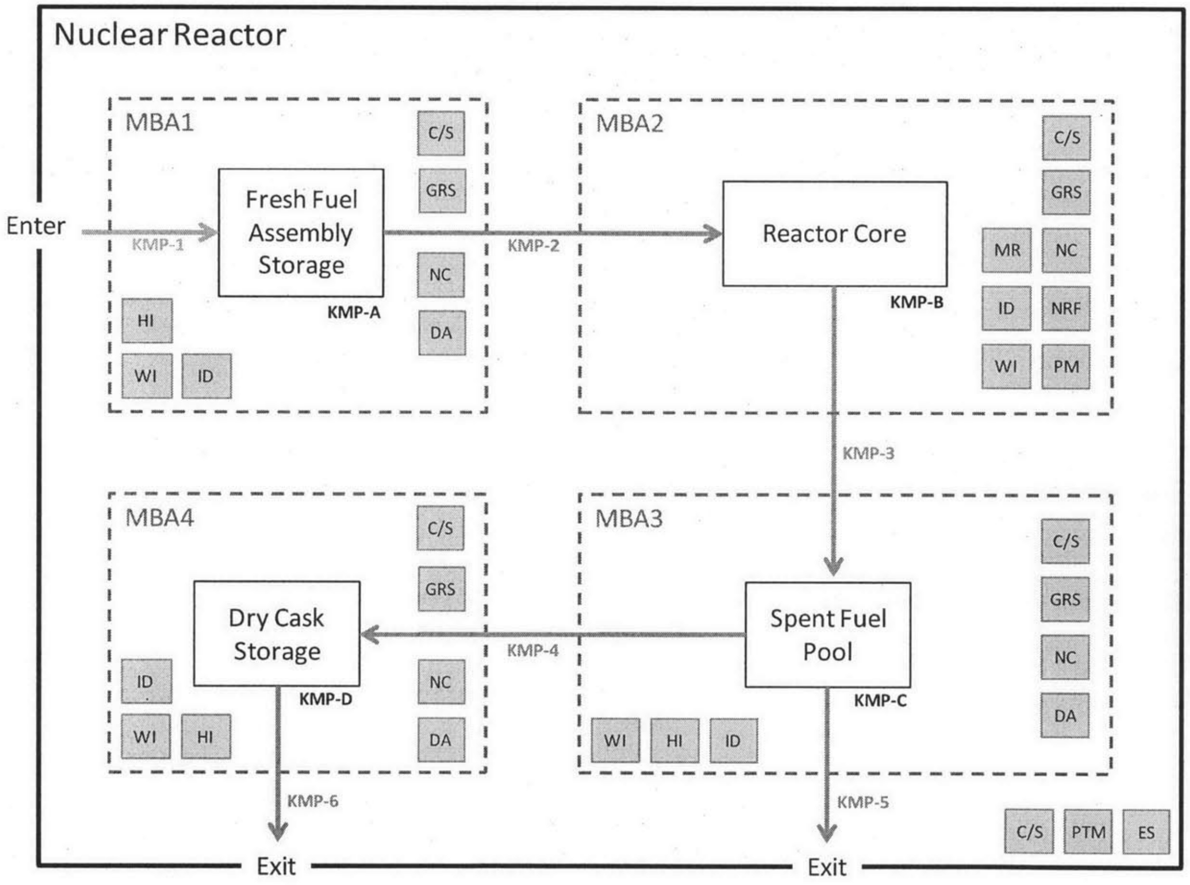
Key Measurement Point (KMP)

Inventory KMP	**Flow KMP**
• KMP-A: UF_6 Cylinder/MOX Canister Storage • KMP-B: Powder Preparation Process • KMP-C: Pellet Fabrication Process • KMP-D: Fuel Rod Fabrication Process • KMP-E: Fuel Assembly Storage • KMP-F: Solid Waste Storage	• KMP-1: Receipt of Feed UF_6 Cylinder/MOX Canister • KMP-2: Transfer of UF_6 Cylinder/MOX Canister between MBA1 and MBA2 • KMP-3: Transfer of Fuel Assembly between MBA2 and MBA3 • KMP-4: Transfer of Solid Waste between MBA2 and MBA4 • KMP-5: Shipment of Fuel Assembly • KMP-6: Shipment of Solid Waste

Nuclear Reactor

Reactor Type

- Light Water Reactor (LWR)
  Material: 3-5% U-235 fuel assembly, Pu in the spent fuel assembly
- Heavy Water Reactor (HWR)
  Material: Low or un-enriched U-235 fuel assembly, Pu in the spent fuel assembly
- Fast Breeder Reactor (FR)
  Material: MOX or Metal (U-Pu-Zr) fuel assembly and spent fuel
- Research Reactor (RR)
  Material: Highly enrich U-235 fuel assembly, Pu in the spent fuel assembly



Material Balance Area (MBA)

Material Balance Area	Nuclear Material	Safeguards
MBA1:Feed Storage Area	Fresh Fuel Assembly (LEU or MOX)	Containment and Surveillance Gamma Ray Spectrometry Neutron Counter Destructive Analysis ID Tracking Weight Inspection Heat Inspection

Material Balance Area	Nuclear Material	Safeguards
MBA2:Reactor Core Area	Fuel Assembly	Containment and Surveillance Gamma Ray Spectrometry Neutron Counter Nuclear Resonance Fluorescence Movement Recording Process Monitoring ID Tracking Weight Inspection
MBA3:Spent Fuel Storage Area	Spent Fuel Assembly	Containment and Surveillance Gamma Ray Spectrometry Neutron Counter Destructive Analysis ID Tracking Weight Inspection Heat Inspection
MBA4:Dry Cask Storage Area	Spent Fuel Assembly	Containment and Surveillance Gamma Ray Spectrometry Neutron Counter Destructive Analysis ID Tracking Weight Inspection Heat Inspection
Throughout Facility	Diverted Material	Containment and Surveillance Environmental Sampling Portal Monitoring

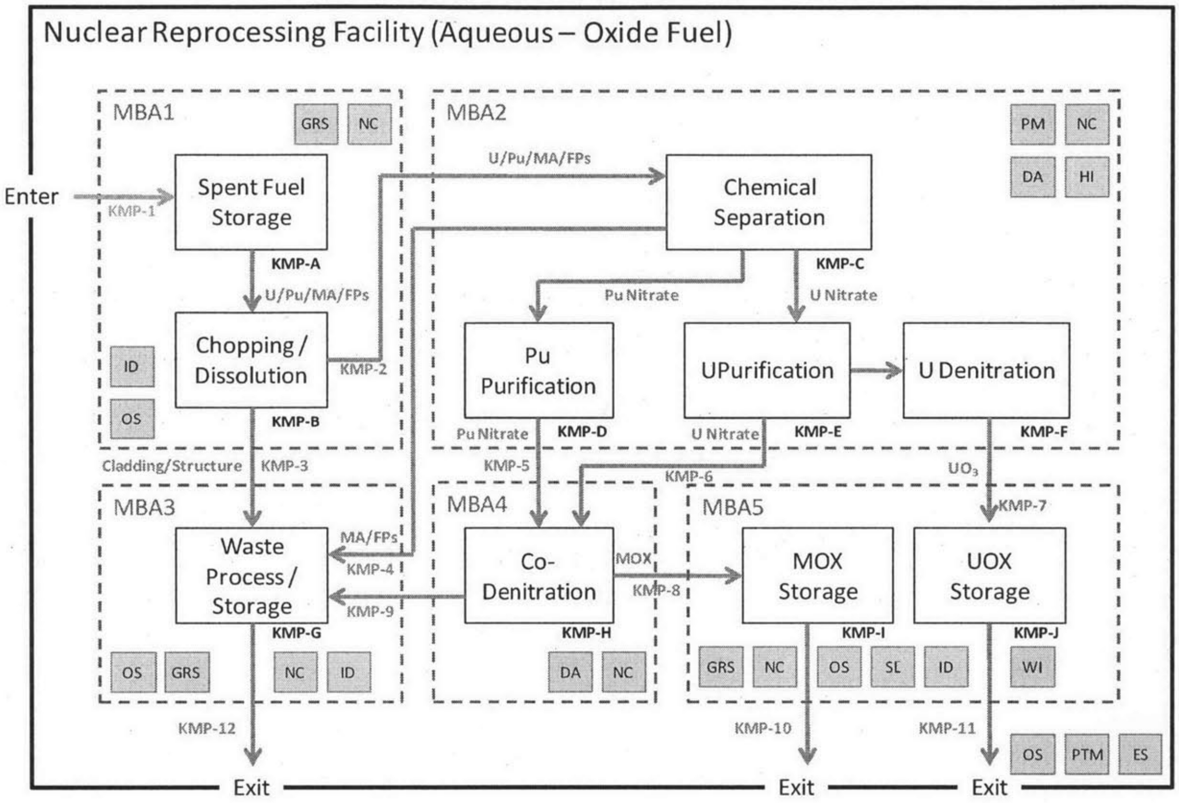
Key Measurement Point (KMP)

Inventory KMP	**Flow KMP**
• KMP-A: Fresh Fuel Assembly Storage • KMP-B: Reactor Core • KMP-C: Spent Fuel Pool • KMP-D: Dry Cask Storage	• KMP-1: Receipt of Feed Fresh Fuel Assembly • KMP-2: Transfer of Fresh Fuel Assembly between MBA1 and MBA2 • KMP-3: Transfer of Spent Fuel Assembly between MBA2 and MBA3 • KMP-4: Transfer of Spent Fuel Assembly between MBA3 and MBA4 • KMP-5: Shipment of Spent Fuel Assembly • KMP-6: Shipment of Spent Fuel Assembly

Nuclear Reprocessing Facility

Fuel Reprocessing Facility Type: Aqueous (PUREX), Pyroprocessing

Material: U/Pu/MOX spent fuel, Plutonium, Uranium, Uranium Oxide and MOX



Material Balance Area (MBA)

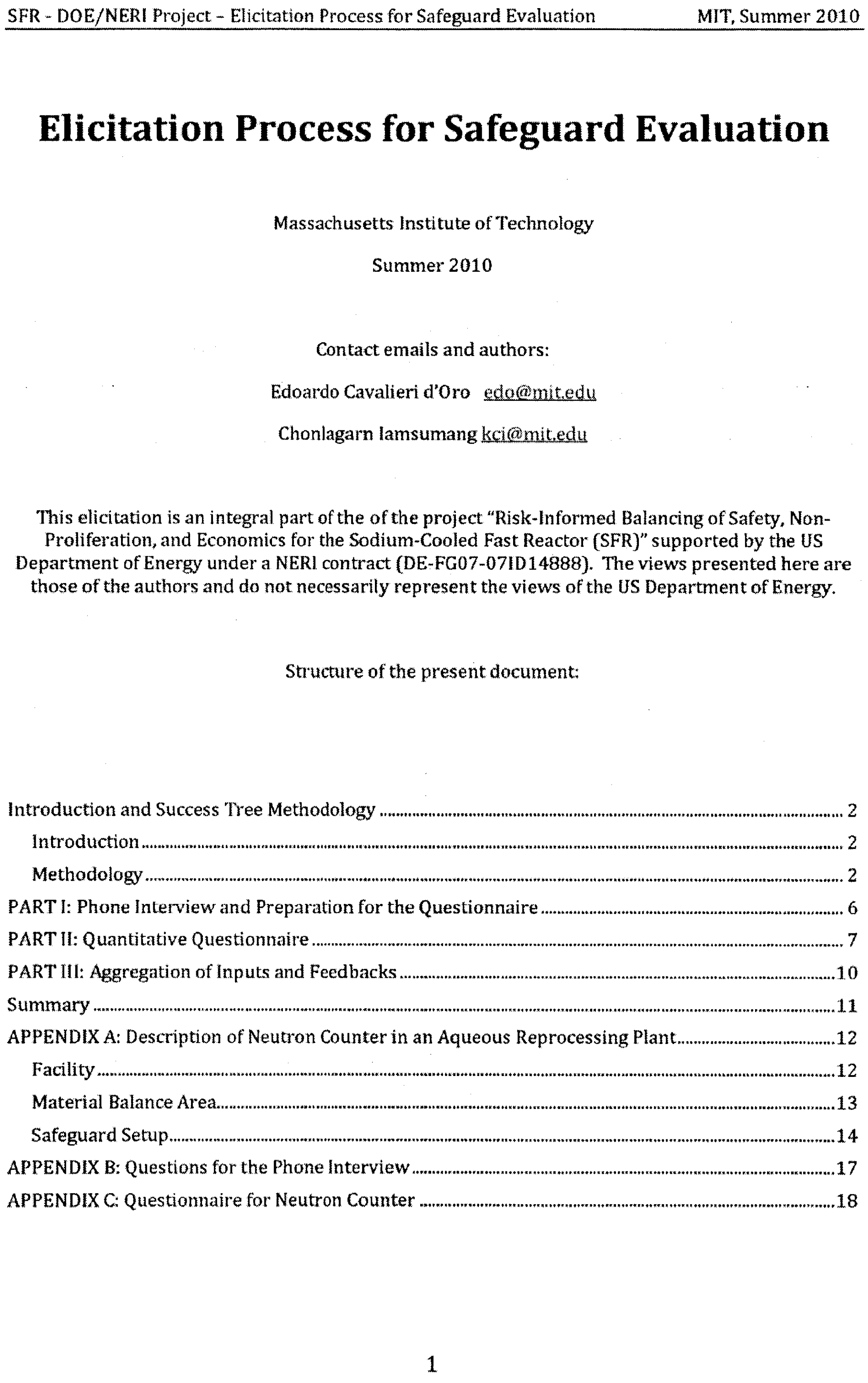
Material Balance Area	Nuclear Material	Safeguards
MBA1: Feed Storage & Disassembly Area	Spent Fuel Assembly Chopped Spent Fuel	Optical Surveillance Gamma Ray Spectrometry Neutron Counter ID Tracking
MBA2: Chemical Separation Area	Spent Fuel Pu Nitrate U Nitrate	Process Monitoring Neutron Counter Destructive Analysis Heat Inspection
MBA3: Waste Process & Storage Area	Solid Waste	Optical Surveillance Gamma Ray Spectrometry Neutron Counter ID Tracking
MBA4: Co-Denitration Area	Pu Nitrate U Nitrate	Neutron Counter Destructive Analysis

Material Balance Area	Nuclear Material	Safeguards
MBA5: Product Storage Area	MOX UOX	Optical Surveillance Seal Gamma Ray Spectrometry Neutron Counter Weight Inspection ID Tracking
Throughout Facility	Diverted Material	Optical Surveillance Environmental Sampling Portal Monitoring

Key Measurement Point (KMP)

Inventory KMP	**Flow KMP**
• KMP-A: Spent Fuel Storage • KMP-B: Chopping and Dissolution Process • KMP-C: Chemical Separation Process • KMP-D: Pu Purification Process • KMP-E: U Purification Process • KMP-F: U Denitration Process • KMP-G: Waste Process and Storage • KMP-H: Co-Denitration Process • KMP-I: MOX Storage • KMP-J: UOX Storage	• KMP-1: Receipt of Spent Fuel Assembly • KMP-2: Transfer of Spent Fuel from MBA1 to MBA2 • KMP-3: Transfer of Waste from MBA1 to MBA3 • KMP-4: Transfer of Waste from MBA2 to MBA3 • KMP-5: Transfer of Pu from MBA2 to MBA4 • KMP-6: Transfer of U from MBA2 to MBA4 • KMP-7: Transfer of UOX from MBA2 to MBA5 • KMP-8: Transfer of MOX from MBA4 to MBA5 • KMP-9: Transfer of Waste from MBA4 to MBA3 • KMP-10: Shipment of MOX • KMP-11: Shipment of UOX • KMP-12: Shipment of Waste

Appendix C: Elicitation Questionnaire



Elicitation Process for Safeguard Evaluation

Massachusetts Institute of Technology

Summer 2010

Contact emails and authors:

Edoardo Cavalieri d'Oro edo@mit.edu

Chonlagarn Iamsumang kci@mit.edu

This elicitation is an integral part of the of the project "Risk-Informed Balancing of Safety, Non-Proliferation, and Economics for the Sodium-Cooled Fast Reactor (SFR)" 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.

Structure of the present document:

Introduction and Success Tree Methodology

Introduction

We have developed a three-part elicitation process that can be used to estimate the probabilities of the events populating typical diversion scenarios, in order to evaluate the safeguards in a nuclear facility.

A typical diversion scenario is driven by an actor that we are going to call the proliferator. His goal is the concealed acquisition of attractive nuclear materials from the plant's site. In order to succeed, or successfully complete the scenario he envisions, he is in general required to simultaneously complete two actions: acquiring the material and avoiding detection. While the first action requires that the proliferator is a person working within the plant and with knowledge about the plant's procedures, the second action requires the proliferator to elude the safeguards that are designed to prevent his acquisition attempt. The probabilities associated with this second type of action are the focus of the present elicitation process. In order to determine these probabilities, it is necessary to interview personnel familiar with the safeguards and this is where we ask for your contribution.

Before describing in detail the probabilities and the characteristics of the safeguard that we would like to estimate with you, we ask you to first familiarize with some basic probability concepts and in particular the methodology that has been developed in order to simulate the proliferation pathways within a given Nuclear Energy System (NES).

Methodology

The diagram in the next page shows the details of the methodology that has been developed in order to capture the attempt of a proliferator trying to acquire weapon usable materials (WUM) from a given location within the boundaries of a nuclear facility. The method is called "Success Tree" and it adopts the topology of the fault trees commonly used for safety analyses (i.e. Probabilistic Risk Assessment). The tree decomposes the actions required to acquire the WUM by combining the probabilities of single events assuming they are independent. To each event, portrayed in the diagram as a box, is then associated a probability. Such a probability is obtained by combining the Basic Event (BE) probabilities, portrayed as circles in the lowest level of the diagram. The top event in the upper part of the diagram is thus finally calculated by simple math, once all the basic events in the lowest part of the diagram have been determined. However, no experimental data are available for the basic events, and their value can only determined by an estimation based on the judgment of a person that is familiar with each of the detection systems in the selected NES.

The following page shows the structure of the success tree for the example case of a Neutron Counter (NC)[1] used to determine the amount of plutonium within a solvent circulating at a given location of the selected NES.

[1] We will use this example throughout the document to explain our elicitation process in detail. The appendices at the end of the document contain all the information and questionnaire related to the safeguard of current interest

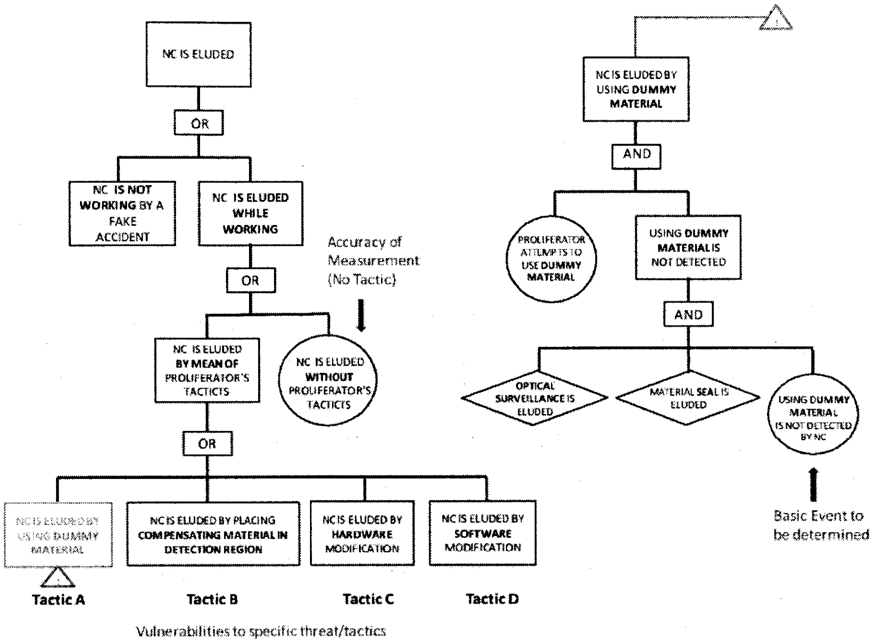

NC IS ELUDED
OR
NC IS NOT WORKING BY A FAKE ACCIDENT
NC IS ELUDED WHILE WORKING
OR
Accuracy of Measurement (No Tactic)
NC IS ELUDED BY MEAN OF PROLIFERATOR'S TACTICTS
NC IS ELUDED WITHOUT PROLIFERATOR'S TACTICTS
OR
NC IS ELUDED BY USING DUMMY MATERIAL
NC IS ELUDED BY PLACING COMPENSATING MATERIAL IN DETECTION REGION
NC IS ELUDED BY HARDWARE MODIFICATION
NC IS ELUDED BY SOFTWARE MODIFICATION
Tactic A
Tactic B
Tactic C
Tactic D
Vulnerabilities to specific threat/tactics
NC IS ELUDED BY USING DUMMY MATERIAL
AND
PROLIFERATOR ATTEMPTS TO USE DUMMY MATERIAL
USING DUMMY MATERIAL IS NOT DETECTED
AND
OPTICAL SURVEILLANCE IS ELUDED
MATERIAL SEAL IS ELUDED
USING DUMMY MATERIAL IS NOT DETECTED BY NC
Basic Event to be determined

Figure 1. Portion of the success tree method referring to the probability to elude a neutron counter.

The Success Tree diagram in the above figure describes the pathway that a proliferator has to follow in order to succeed in his acquisition attempt. The acquisition attempt depends on the Proliferator's capability to elude all the safeguards in place at a given location. Eluding the safeguard in this case means to elude all the measurements resulting from the safeguard scheme present in a selected location of the NES, or Material Balance Area (MBA). The top event, labeled "NC is eluded," represents the capability to elude a neutron counter (NC), which depends on two main factors. The first factor to consider is that, depending on the quantity of material subtracted, the safeguard might not be able to detect it even in the absence of additional tactics. This is the case when the proliferator acquires an amount of material that is below the threshold at which the instrument detects the presence of a given material (e.g. the amount of plutonium nitrate flowing in a pipe). The probability associated with this event, labeled as 'no tactic', can be inferred by knowing the accuracy of the safeguard. This means that the proliferator, assuming he knows the threshold of the instrument, does not need to produce an ad hoc tactic specifically intended for this safeguard.

The determination of the basic event (circle) labeled as "NC is eluded without proliferator's tactics" is the first basic event that has to be determined by our elicitation process. Thus, the first question is asking you to determine the uncertainty of measurement of the detector.

In the case that the amount of material is within the range of detection of this instrument, the proliferator then needs to add an additional tactic selected from the four supportive tactics labeled from A to D in the left lower portion of the tree. Each one of these tactics represents a specific attack on the detection system, a portion of it, or on the sample. Tactic A for instance, expanded with a sub tree on the right, depicts the situation where the proliferator adds dummy materials to the sample in order to elude the NC's measurements and mask the illicit subtraction of material. In order to be undetected, the proliferator needs to support this strategy with further actions covering this extra action, such as eluding seals and optical surveillance (diamonds).

The determination of the basic event (circle) labeled as "using dummy material is not detected by NC" is the second basic event that has to be determined by our elicitation process. This second question is asking you to determine the potential vulnerability of the detector to the threats from A to D. Note that the four threats, or tactics, listed in the above diagram are specific for eluding a neutron counter. The list of tactics will be different depending on the type of safeguard.

In conclusion, there are 5 basic event probabilities that need to be derived from the elicitation as summarized by Table 1.

Table 1. Basic Event probabilities and tactics for a neutron counter

Tactic	*Basic Event Probability*	*Tactic Description*
No Tactic	Probability that the proliferator will successfully elude the neutron counter without any tactics	Depending on the neutron counter uncertainty of measurement, proliferator diverts the material in an amount that is within the expected error of the measurement
Tactic A	Probability that the proliferator will successfully elude the neutron counter by using dummy material	Proliferator replaces the missing material with another neutron source, such as minor actinides or fission products
Tactic B	Probability that the proliferator will successfully elude the neutron counter by placing compensating material in the detection region	Proliferator places compensating material with the same mass as that diverted in the detection region, such as on the surface of the pipe, or between the container and the detector.
Tactic C	Probability that the proliferator will successfully elude the neutron counter by modifying the hardware	Proliferator modifies the detector to give more neutron counts than normal, or modifies the electronic circuit to send more signals to the processing unit.
Tactic D	Probability that the proliferator will successfully elude the neutron counter by modifying the software	Proliferator modifies the software to store the desired output or access the record to modify the data.

In some cases, it is possible that your expertise might be more useful to address the first three items presented in the above diagram. In general it is expected that a person dealing with a specific safeguard might not be aware of software related problems or he might not have been personally involved in the definition of counter measures to protect 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, or people in your company that might have a specific capability to address these issues.

Factors affecting the probabilities and the uncertainty estimates

At this point it should be clear that the scope of the elicitation process is to determine the probabilities of the boxes labeled "no tactic" which refers to the accuracy of the safeguard system and the four remaining probabilities, labeled tactics "A", "B", "C", and "D", which refer to the probabilities to elude the detection system in question via its vulnerabilities to four types of threats, or tactics.

The uncertainty of measurement and the probabilities values expressing the vulnerability of a safeguard to the four threats are all expressed by means of a point estimate and a judgment about your uncertainty in providing that estimate. So in the second part of the elicitation process you will be asked to quantitatively provide estimates of these values accompanied by the level of confidence of your subjective evaluation.

In addition, these estimates in the framework we have envisioned are not independent but a function of other variables:

- The uncertainty of measurement is a function of the mass of the material that is being measured (M), and also a function of the resources that you devote to your safeguard, or its final cost (C).
- The vulnerability measured in terms of the proliferator's probability to succeed with tactics is a function of the overall safeguard cost (C).

The scope of the first part of the elicitation process is to determine the plausible ranges of the variables on which uncertainty and vulnerability depend. In this first part of the elicitation process[2] you are asked to provide a range for the dependent variables M and C, while in the second part you will be asked to provide estimates of the probabilities and uncertainty associated with these ranges. Within the range, the base case of M, which is the regular mass flow of the material at the safeguard location, will be determined from the facility design. On the other hand, the base case of C, which is the expected regular cost of the safeguard, will be defined with you during the phone interview. The definitions of the upper and lower limits, and base cases for the two dependent variables M, and C, are provided in the following table.

Table 2. Factors affecting the probabilities and the uncertainty estimates.

Factor	*Point on the detectable range*	
	Point	*Description*
Total mass of the material under detection	M_{low}	Lowest total mass in the detectable range
	M_{bc}	Base case total mass, which is the regular mass of material under detection region in the facility
	M_{high}	Highest total mass in the detectable range
Cost of the neutron counter	C_{min}	Minimum cost of the safeguard for it to operate
	C_{bc}	Base case cost, which is the regular cost of typical set up of the safeguard
	C_{opt}	Cost of the safeguard the will make it operate at the optimal efficiency

Following this section, the document will show the elicitation process separated into three parts using a neutron counter as the example safeguard. For specific details of the safeguard of current interest, please see Appendix A[3].

[2] The reason for not having these two phases of the elicitation process together is that in order to establish a comparison between your estimates and the estimates provided from other people who have expertise in the same safeguard, we have to define a range that is the same for all the interviewees.

[3] Appendix A contains the description of the safeguard and facility that have been selected, including all the details regarding potential diversion scenarios occurring at the safeguard location of that facility.

PART I: Phone Interview and Preparation for the Questionnaire

The objective of this first part of the elicitation process is to discuss with you the details of the safeguard's functionality, its components, and its limitations. The information provided by you during a phone interview will help us to prepare for the second part of the elicitation process, which is going to be in the form of a written questionnaire. During the conversation we will ask you to help us determine some characteristics of the safeguard relative to the specific application we are looking at (i.e. acquisition of materials from a given location within a pre-selected facility). Specifically these characteristics are: the safeguard detection range, such as the amount of material that it can detect, and the cost of the safeguard for different setup and components.

In this first part of the elicitation process, you are asked to provide a range for the dependent variables, mass of the material under detection (M) and the cost of the safeguard (C) for scenarios with and without proliferator tactics.

The total time for the phone interview is estimated to be approximately 30 minutes.

The following table shows the example questions and inputs for the neutron counter. For the specific questions relating to the safeguard of current interest, please see Appendix B.

Factor	*Point on the detectable mass range*	
	Point	*Value (kg)*
Total mass of the material under detection	M_{low}	0.1
	M_{bc}	0.5
	M_{high}	1

The cost of the safeguard for the scenario without proliferator's tactic is the cost of different safeguard set-ups that affect the uncertainty of measurement.

Tactics	*Safeguard Estimated Cost*	*Value*	*Safeguard modifications (e.g., equipment changes, component additions, quality improvements, software interfaces, etc.)*
No tactic: Uncertainty of measurement	C_{min}	$0.05M	Basic He-3 detector tube
	C_{bc}	$0.2M	Larger detector, charge amplifier
	C_{opt}	$1M	Multiple highest sensitivity detectors

The cost of the safeguard for the scenario with proliferator's tactic is the cost of different safeguard set-ups that affect the proliferator success probability to elude the safeguard for each specific tactic.

Tactics	*Safeguard Estimated Cost*	*Value*	*Safeguard modifications (e.g., equipment changes, component additions, quality improvements, software interfaces, etc.)*
Tactic A: Dummy material	$C_{A,min}$	$0.05M	Basic He-3 detector tube
	$C_{A,bc}$	$0.2M	Larger detector, charge amplifier
	$C_{A,opt}$	$1M	Multiple highest sensitivity detectors
Tactic B: Compensating material	$C_{B,min}$	$0.05M	Basic He-3 detector tube
	$C_{B,bc}$	$0.2M	Larger detector, charge amplifier
	$C_{B,opt}$	$1M	Multiple highest sensitivity detectors
Tactic C: Hardware modification	$C_{C,min}$	$0.05M	Basic detector and cable setup

Tactics	*Safeguard Estimated Cost*	*Value*	*Safeguard modifications (e.g., equipment changes, component additions, quality improvements, software interfaces, etc.)*
	$C_{C,bc}$	\$0.5M	Detector and cable shielding
	$C_{C,opt}$	\$2M	Movement and tampering sensor
Tactic D: Software manipulation	$C_{D,min}$	\$0.05M	Basic software setup
	$C_{D,bc}$	\$0.1M	Software and data encryption
	$C_{D,opt}$	\$0.5M	Real time authentication and remote central server

PART II: Quantitative Questionnaire

The objective of the second part of the assessment is to acquire the estimates of the probabilities that the proliferator will succeed in eluding the safeguard.

As shown by the Success Tree method, there are two ways to elude the safeguard:

- Without recourse to supportive tactics:
  - The probability is inferred through the uncertainty of measurement of the safeguard.
  - The uncertainty of measurement is a function of the material mass (M), and of the amount of resources spent for the safeguard, or cost (C).
- With the use supportive tactics:
  - The probability is directly expressed in terms of probability of success for the proliferator attempting the attack.
  - These probabilities are functions of the amount of resource spent for the safeguard, or cost (C).

You might recall that in the first part of the assessment you were asked to provide ranges for the two variables M, and C. At the same time we asked other professionals to provide the same ranges and we averaged the values provided by you with the value provided by these other experts. Therefore in the tables that you are asked to complete, you will not find exactly the range values that you provided in the first part of the elicitation process. However, the new values won't differ much from the values you gave us and therefore you should be able to proceed with this assessment.

In this part you will be asked to estimate the uncertainty of measurement and the probabilities to elude the safeguard system that you are familiar with and also provide the level of confidence for your estimates.

The total time for the questionnaire is estimated to be approximately 1 hour.

Two preliminary examples are provided below so that you can familiarize yourself with the assessment. The two examples show how the probability and uncertainty of measurement curves are built based on the estimates and confidence levels provided by a hypothetical interviewee. The questionnaire is designed specifically for a neutron counter. For the questionnaire relating to the current safeguard of interest, please see Appendix C.

Question I: The neutron counter uncertainty of measurement

The question in the table is asking for the uncertainty of measurement with 95% level of confidence at three different points of total mass under detection and cost of the safeguard. The cost and mass ranges and the base case estimates are provided in the table both for M and C. The following figure shows the plots of the estimates for comparison.

Safeguard Estimated Cost	Uncertainty of Measurement (%) with 95% confidence level		
	Total Mass M_{low} = 1kg	Total Mass M_{bc} = 5kg	Total Mass M_{high} = 10kg
C_{min} = $0.05M	10	4	2.5
C_{bc} = $0.1M	4	2	1.5
C_{opt} = $1M	2	1	0.75

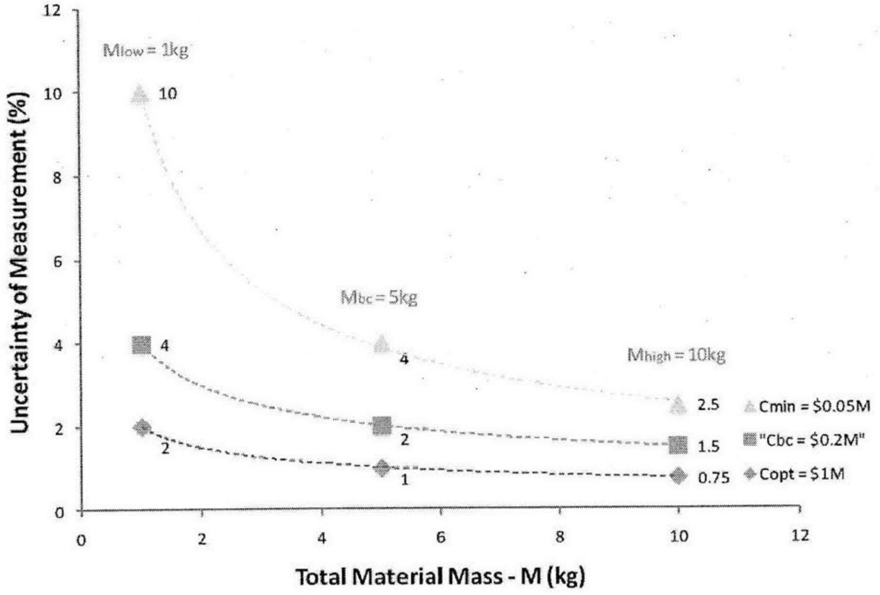


Figure 2. Example plot of total material mass versus uncertainty of measurement at three different costs of safeguard setups for a neutron counter.

Question II: Probability that the proliferator's tactics will successfully elude the neutron counter

Tactic A: Using Dummy Material

The question in the table is asking for the proliferator success probability point estimate and the error with 95% level of confidence at three different points of the cost of the safeguard. The cost range and the base case estimates are provided in the table. The following figure shows the plots of the estimate as a function of the cost of the safeguard.

Safeguard Estimated Cost	Proliferator success probability of tactic A	
	Point Estimate	± Error with 95% Level of Confidence
$C_{A,min} = \$0.05M$	0.75	0.1
$C_{A,bc} = \$0.2M$	0.4	0.05
$C_{A,opt} = \$1M$	0.2	0.02

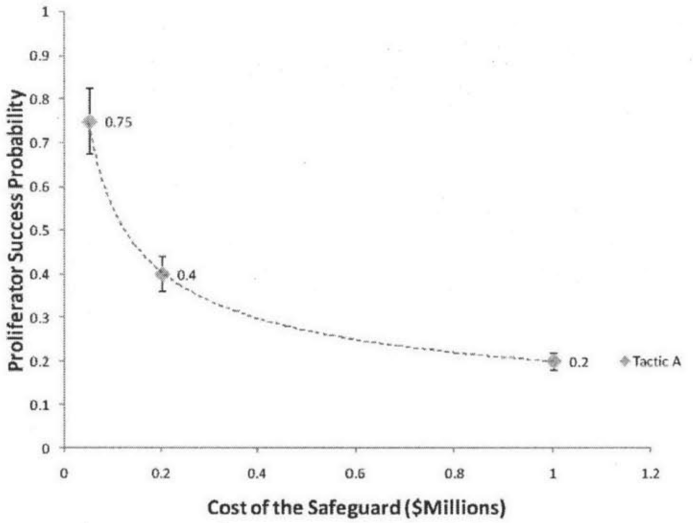


Figure 3. Example plot of the proliferator success probability versus the cost of the safeguards.

The expected trend of the proliferator success probability versus the cost of the safeguard is decreasing until it reaches the saturation point where increasing the cost of the safeguard will no longer anymore decrease the success probability of the proliferator.

Following the same template, the rest of the questionnaire for the other tactics will have similar format as the one shown for tactic A.

PART III: Aggregation of Inputs and Feedbacks

The objective of the third part of the assessment is to analyze and aggregate the inputs from the questionnaires, and then show these results to you before the final interview to receive your feedback.

The total time for the phone interview is estimated to be approximately 30 minutes.

The main analysis of the inputs is to compare the proliferator success probabilities for the different tactics that can be used to elude the safeguard. Figure 4 shows the example plot of proliferator success probabilities versus the cost of the safeguard for different proliferator's tactics. This plot shows the cost effectiveness of the set up of the safeguard to prevent the proliferator from eluding the safeguard by each tactic (Please note that the actual comparison of the proliferator success probability will include the probability of eluding the supporting safeguard, such as surveillance camera, seal, etc., as show in the success tree diagram in Figure 1)

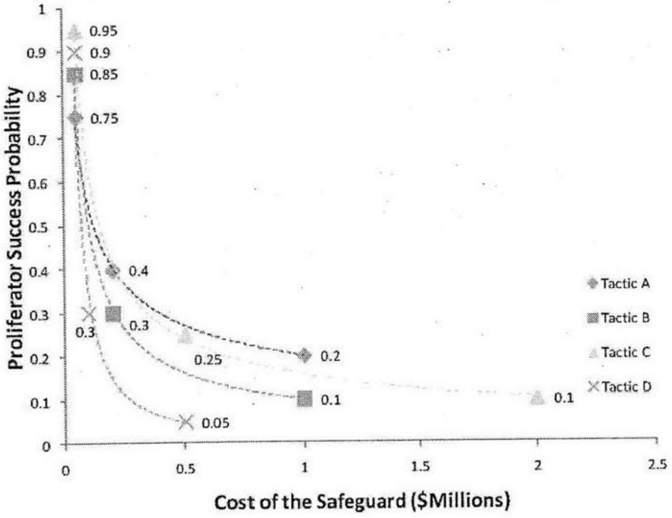


Figure 4. Example plot of comparison of proliferator success probabilities of different tactics

Next, the inputs from different sources are aggregated. We are using the linear opinion pool approach with equal weight, shown by Clemen and Winkler[4], the result is the average of the values from all experts.

$$p(C_s) = \sum_{i=1}^{n} w_i p_i(C_s)$$

p = the proliferator success probability
C_s = the safeguard cost
w_i = the weighting factor; in this case w_i = 1

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

Because we have defined the points on the range of the variable M and C prior to the questionnaire during the first interview, the estimates of the uncertainty of measurement and the proliferator success probabilities are at the same value of the factors. This provides better comparison and aggregation of the inputs from different sources.

Figure 5 shows an example plot of uncertainty of measurement from different inputs and the aggregated values using this method.

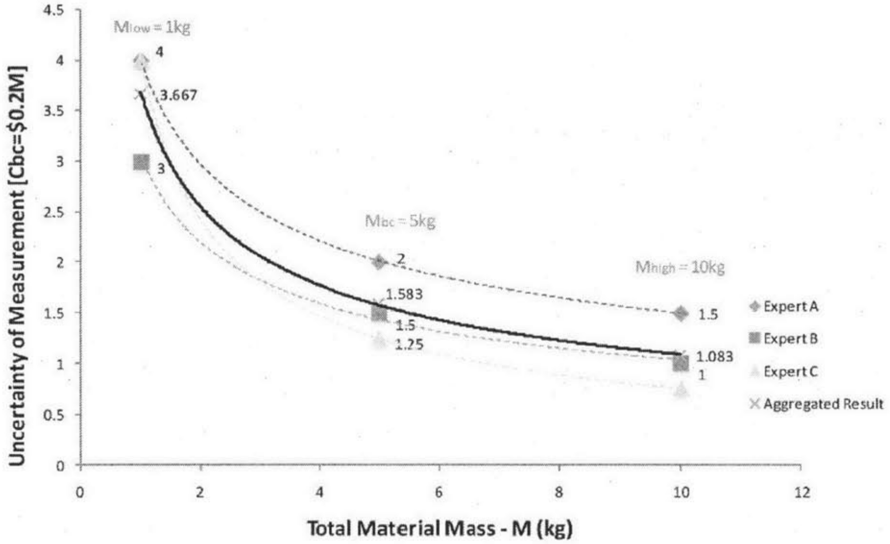


Figure 5. Example plot of the aggregated inputs for the uncertainty of measurement with C = $0.2M

The results from the analysis will be sent to you, prior the phone interview for a discussion about the issues that may come up and to receive your feedbacks of the outcome of the assessment. You will also have an opportunity to adjust your inputs if you found necessary during the interview.

Summary

In summary, this document demonstrates the step-by-step procedures and example inputs of our elicitation process using neutron counter as the example safeguard. We would like to thank you for reading through the document and we hope that this document provides enough information and explanation for you to complete our interview and questionnaire. In the appendices, you will find the descriptions and the questionnaire for the safeguard of current interest.

If you have any questions or if you are ready to set up a time for the phone interview please contact: kci@mit.edu

APPENDIX A: Description of Neutron Counter in an Aqueous Reprocessing Plant

The following description is provided for the estimation of the probability that the proliferator will succeed in eluding the neutron counters in the chemical separation process area of an aqueous reprocessing plant.

Facility

The scheme below shows the flow of the material and the safeguards scheme in an Aqueous Fuel Reprocessing Facility (ARF). The processes of this facility are separated into five material balance areas (MBA) where the material flows in and out of the areas are measured for material accountancy. Each MBA contains different types of safeguards that are suitable for the processes and form of the material within the area. The safeguards are located at the Key Measurement Points (KMP) throughout the facility. There are two types of KMP; one is Inventory Key Measurement Point (IKMP), where the safeguards monitor the material inside the process or storage. The other type is Flow Key Measurement Point (FKMP), where the safeguards monitor the amount of material transferring between two processes.

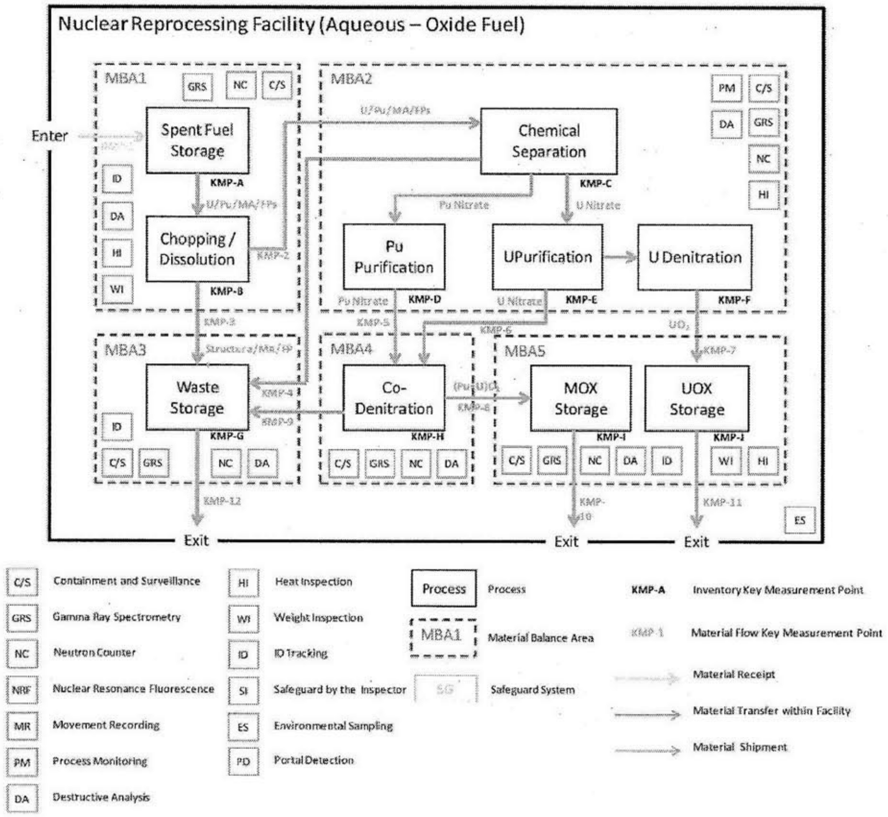


Figure 6. Schematic of the processes and safeguards schemes in an aqueous reprocessing plant.

Facility Data (based on Rokkasho Reprocessing Plant[5])

- Reprocessing capacity for light water reactor (LWR) spent fuel: 800 tons/year
- Expected operating days per year: 200
- Normal daily operation throughput: 4 tons/day
- Plutonium product in the form of MOX powder: 8 tons/year (40kg/day)
- The main process employs a PUREX type separation process for the removal of fission products and the partitioning and purification of uranium and plutonium.
- Approximate contents of the spent fuel at 50GWd/MTIHM burnup are given below[6]

Table 3. Spent fuel composition from a LWR.

50 GWd/MTIHM irradiated oxide fuel	% of Content
Uranium	93.4% (1.1% U-235)
Plutonium	1.33%
Minor Actinides	0.12%
Fission Products	5.15%

Material Balance Area

The details of the safeguards in the chemical separation area (MBA2) are shown in Figure 7.

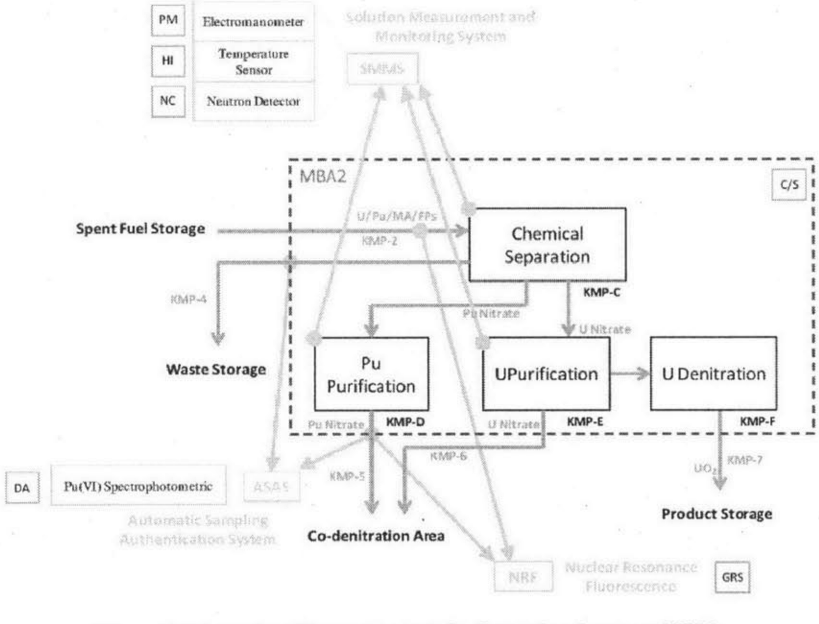


Figure 7. Schematic of the processes and safeguards schemes at MBA2.

[5] S. J. Johnson, H. Higuchi, K. Fujimaki, "Development of the Safeguards Approach for the Rokkasho Reprocessing Plant", International Atomic Energy Agency, IAEA-SM-367/8/01.

[6] Xu, Zhiwen, "Design Strategies for Optimizing High Burnup Fuel in Pressurized Water Reactors", MIT Department of Nuclear Engineering doctoral thesis, January 2003.

There are three major safeguard systems within the MBA2.

1. Solution Measurement and Monitoring System (SMMS): SMMS is an in-tank measurement system used for the determination of solution level, volume and density, from a combination of data of pressure measurement device (Electromanometer), temperature sensor, and neutron detector.
2. Automatic Sampling Authentication System (ASAS): ASAS authenticates the sampling jug and the taking and transferring of samples from the operator's process sampling benches to the inspector's On-Site Laboratory (OSL) for sample analysis.
3. Nuclear Resonance Fluorescence (NRF): NRF is a new active interrogation technique that is currently proposed to be used for material accountancy before and after the chemical separation process. The technique relies on the detection of unique photon energies of resonance fluorescence from excited nuclides.

On top of these systems the area is monitored by containment and surveillance (C/S) systems.

Safeguard Setup

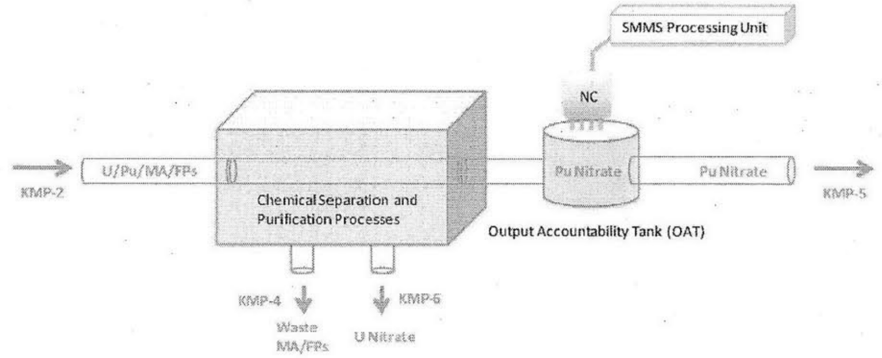


Figure 8. Setup of the neutron counter at the Output Accountability Tank (OAT)

Figure 8 and Table 4 show the setup and the information about the neutron detector as part of SMMS in Material Balance Area 2. The neutron detector is used to account for the amount of neutron radiation from plutonium nitrate in the Output Accountability Tank after the chemical separation and purification processes. The data from the detector is then compared with the reference signature and raises alarms in case of differences. This will effectively detect the proliferator's attempts to divert some amount of plutonium during the earlier processes, since the amount of the plutonium detected will not match the expected value within the allowable tolerance.

Table 4. Information about the neutron detector in MBA2 as part of SMMS.

Type:	Helium-3 proportional detectors
System:	Solution Measurement and Monitoring System (SMMS)
Location:	Output Accountability Tank
Material Under Detection:	Plutonium in a plutonium nitrate solution

The material detected by the neutron detector is the plutonium in plutonium nitrate solution. The approximate plutonium isotope composition and neutron radiation is shown in the table below. Please note that the total mass the material under detection (M) in the questionnaire is the total mass of plutonium inside the detection region.

Table 5. Plutonium isotope composition and neutron radiation for a sample at MBA2.

Plutonium Isotope	% Isotope Composition	Neutron Radiation (N/kg.s)	Neutron Radiation of 1kg of Plutonium (N/s)
Pu-238	2.50%	2.67E+06	6.68E+04
Pu-239	55.00%	2.30E+01	1.27E+01
Pu-240	24.00%	1.03E+06	2.47E+05
Pu-241	14.00%	4.94E+01	6.92E+00
Pu-242	4.50%	1.73E+06	7.79E+04
Total	100.00%	5.43E+06	3.92E+05

The following figure shows the portion of the success tree model for a neutron counter (as explained by the example in the first section of the document, see Figure 1).

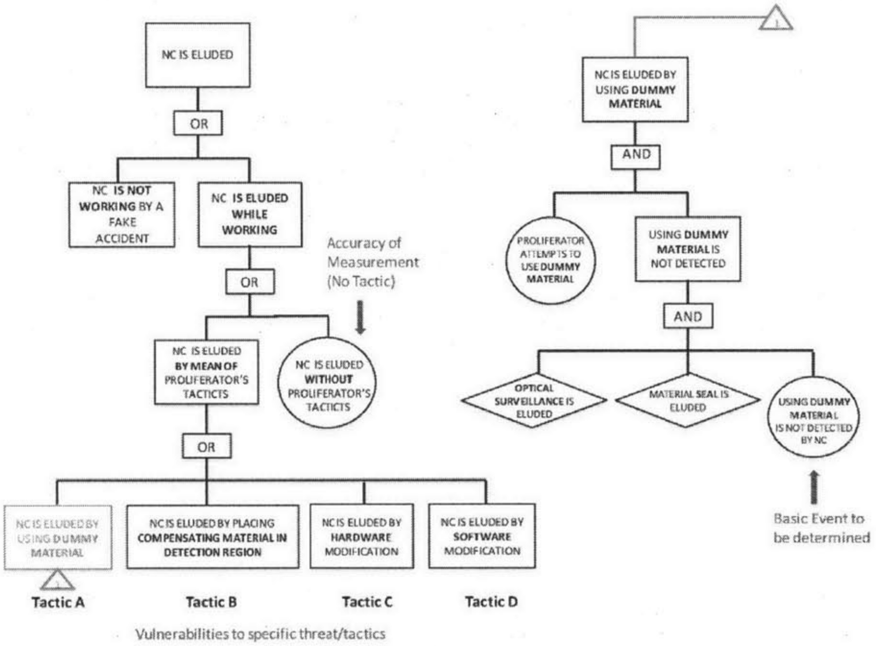

NC IS ELUDED
OR
NC IS NOT WORKING BY A FAKE ACCIDENT
NC IS ELUDED WHILE WORKING
Accuracy of Measurement (No Tactic)
OR
NC IS ELUDED BY MEAN OF PROLIFERATOR'S TACTICTS
NC IS ELUDED WITHOUT PROLIFERATOR'S TACTICTS
OR
NC IS ELUDED BY USING DUMMY MATERIAL
NC IS ELUDED BY PLACING COMPENSATING MATERIAL IN DETECTION REGION
NC IS ELUDED BY HARDWARE MODIFICATION
NC IS ELUDED BY SOFTWARE MODIFICATION
Tactic A
Tactic B
Tactic C
Tactic D
Vulnerabilities to specific threat/tactics
NC IS ELUDED BY USING DUMMY MATERIAL
AND
PROLIFERATOR ATTEMPTS TO USE DUMMY MATERIAL
USING DUMMY MATERIAL IS NOT DETECTED
AND
OPTICAL SURVEILLANCE IS ELUDED
MATERIAL SEAL IS ELUDED
USING DUMMY MATERIAL IS NOT DETECTED BY NC
Basic Event to be determined

Figure 9. Portion of the success tree method referring to the probability to elude a neutron counter.

The following table contains the description of the basic events and proliferator's tactic to elude the safeguard for a neutron counter (as explained by the example in the first section of the document, see Table 1).

Table 6. Basic Event probabilities and tactics for a neutron counter

Tactic	*Basic Event Probability*	*Tactic Description*
No Tactic	Probability that the proliferator will successfully elude the neutron counter without any tactics	Depending on the neutron counter uncertainty of measurement, proliferator diverts the material in an amount that is within the expected error of the measurement
Tactic A	Probability that the proliferator will successfully elude the neutron counter by using dummy material	Proliferator replaces the missing material with another neutron source, such as minor actinides or fission products
Tactic B	Probability that the proliferator will successfully elude the neutron counter by placing compensating material in the detection region	Proliferator places compensating material with the same mass as that diverted in the detection region, such as on the surface of the pipe, or between the container and the detector.
Tactic C	Probability that the proliferator will successfully elude the neutron counter by modifying the hardware	Proliferator modifies the detector to give more neutron counts than normal, or modifies the electronic circuit to send more signals to the processing unit.
Tactic D	Probability that the proliferator will successfully elude the neutron counter by modifying the software	Proliferator modifies the software to store the desired output or access the record to modify the data.

APPENDIX B: Questions for the Phone Interview

The following tables show the values that will be acquired from the discussion during the phone interview for Part I of the elicitation process for neutron counter. The details of the neutron counter setup and the material under detection are shown in the "Safeguard Setup" Section of Appendix A.

Factor	*Point on the detectable mass range*	
	Point	*Value*
Total mass of the material under detection	M_{low}	
	M_{bc}	
	M_{high}	

For the cost of the safeguard, please provide the details of the physical changes that correspond to each of the following points of each proliferator's tactic scenarios. The cost of the safeguard for the scenario without proliferator's tactic is the cost of different safeguard set-ups that affect the uncertainty of measurement.

Tactics	*Safeguard Estimated Cost*	*Value*	*Safeguard modifications (e.g., equipment changes, component additions, quality improvements, software interfaces, etc.)*
No tactic: Uncertainty of measurement	C_{min}		
	C_{bc}		
	C_{opt}		

The cost of the safeguard for the scenario with proliferator's tactic is the cost of different safeguard set-ups that affect the proliferator success probability to elude the safeguard for each specific tactic

Tactics	*Safeguard Estimated Cost*	*Value*	*Safeguard modifications (e.g., equipment changes, component additions, quality improvements, software interfaces, etc.)*
Tactic A: Dummy material	$C_{A,min}$		
	$C_{A,bc}$		
	$C_{A,opt}$		
Tactic B: Compensating material	$C_{B,min}$		
	$C_{B,bc}$		
	$C_{B,opt}$		
Tactic C: Hardware modification	$C_{C,min}$		
	$C_{C,bc}$		
	$C_{C,opt}$		
Tactic D: Software manipulation	$C_{D,min}$		
	$C_{D,bc}$		
	$C_{D,opt}$		

APPENDIX C: Questionnaire for Neutron Counter

Based on your experience and your judgment, please complete the following tables. The details of the neutron counter setup and the material under detection are shown in the "Safeguard Setup" Section of Appendix A.

(Please note that the following questions are shown as an example. The actual questionnaire will contain specific values of M and C derived from Part I of the elicitation)

Question I: The neutron detector uncertainty of measurement (no tactic)

Safeguard Estimated Cost	Uncertainty of Measurement (%) with 95% confidence level		
	Total Mass = M_{low}	Total Mass = M_{bc}	Total Mass = M_{high}
C_{min}			
C_{bc}			
C_{opt}			

Question II: Probability that the proliferator's tactics will successfully elude the NC

- **Tactics A: using dummy material**

Safeguard Estimated Cost	Proliferator success probability of tactic A	
	Point Estimate	± Error with 95% Level of Confidence
$C_{A,min}$		
$C_{A,bc}$		
$C_{A,opt}$		

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

Safeguard Estimated Cost	Proliferator success probability of tactic B	
	Point Estimate	± Error with 95% Level of Confidence
$C_{B,min}$		
$C_{B,bc}$		
$C_{B,opt}$		

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

Safeguard Estimated Cost	Proliferator success probability of tactic C	
	Point Estimate	± Error with 95% Level of Confidence
$C_{C,min}$		
$C_{C,bc}$		
$C_{C,opt}$		

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

Safeguard Estimated Cost	Proliferator success probability of tactic D	
	Point Estimate	± Error with 95% Level of Confidence
$C_{D,min}$		
$C_{D,bc}$		
$C_{D,opt}$		