Integrating Nuclear Resonance Fluorescence Safeguards into Nuclear Energy Systems using Non-proliferation Assessment Methods

E. Cavalieri d'Oro, et al. (DRAFT)
Massachusetts Institute of Technology
Nuclear Science and Engineering Department
77 Massachusetts Avenue
02139 Cambridge, MA
Tel: 617-852-5034, Email:edo@mit.edu

Abstract

A new detection technique, originally thought for the detection of explosives in cargo containers, is presented in this paper for the particular application of isotopic detection of nuclear materials in a Nuclear Energy System (NES). This technique is called Nuclear Resonance Fluorescence (NRF) and the reference fuel scheme to which it is applied is the Sodium Fast Reactor (SFR). The objective of this application is to safeguard nuclear fuel schemes from diversion of Special Nuclear Materials (SNM) in order to increase the proliferation resistance of the facilities exposed to these potential threats.

In this paper, first, we provide a description of a pre-experimental configuration accompanied by the changes in the NRF architecture to adapt it from the cargo to isotopic detection mode. Second, we study the experimental configuration to determine the critical parameters driving the probability of detection of SNM as a function of the economic resources employed by the virtual safeguarder of the plant. Finally, a method named ISTEM, currently under development at MIT, to assess the proliferation resistance of a nuclear energy system is presented and tested with NRF.

The results from a reference illustrative example simulated on the SFR fuel cycle, show the effective capability of NRF to safeguard the nuclear schemes and the potential to measure corresponding increases in the proliferation resistance of the selected scheme by means of the assessment method.

The conclusions discuss the needs to protect future nuclear fuel schemes with advanced NRF safeguards and to have adequate tools to measure the benefits of having such systems in place versus the cost devoted to their integration into the NES.

The use of assessment techniques to describe and measure the proliferation resistance of NES provides a fundamental tool to support the development of risk-informed and performance-based approaches.

I. INTRODUCTION

The current surge of interest in nuclear energy simultaneously calls to resolve the concerns about the appropriateness of the current nuclear non-proliferation regulatory framework for new threats challenging nuclear energy systems. Over the last decades, countries adhering to the Non-Proliferation Treaty (NPT) confronted the international community by building concealed facilities, by manipulating the configuration of their power plants, and by diverting material from their nuclear sites.

Strengthening the current non-proliferation regime, it is then needed to guarantee high standards of security for the sites that store, produce, or transform special nuclear materials (SNM). One way to achieve this goal is to avail of new tools and appropriate methods for evaluating the non-proliferation risk of nuclear energy systems (NES).

The call for the development of tools to evaluate the proliferation resistance (PR) of NES is ultimately coming from the society which demands appropriate protection from non-proliferation threats. The role to introduce new evaluation methods is played primarily by the scientific community, by the regulators, and by the industry.

The potential customers for a PR assessment method are the policy makers that can assist their decisions and support their arguments grounding them to quantitative evaluations.

This variety of stakeholders delineates an important peculiarity of the non-proliferation problem; a multi-dimensional connotation deriving from the assortment of the parties involved that adds to its well known multi-disciplinarily character. Therefore, the creation of a new tool for the quantitative PR assessment of NES is not a straightforward task not only because it has to satisfy criteria that belong to different disciplines, but also because it has to incorporate the different stakeholders' perspectives.

The PR evaluation method presented and tested in this paper has the precise objective to provide a method that can be approach from the all the stakeholders above mentioned. The particular focus of this paper is to test a specific feature of the PR assessment that is being developed, that is the inclusion of safeguards systems into PR modeling. Coupling safeguards' extrinsic barriers, such as safeguards, with the NES intrinsic barriers (i.e. the material properties and the plant characteristics), and demonstrating that the former increases the PR of the latter, are fundamental aspects required by PR evaluations.

A supporting example based on the physics of a specific safeguard, the Nuclear Resonance Fluorescence (NRF) detector, is used to illustrate the use of the method used to assess the PR of the selected NES.

An exploratory approach is being used to perfection the PR model: first an experimental set-up for NRF is described, then the knowledge derived from this description is being used to frame a PR model that models the NRF safeguard.

Risk-information and performance metrics are invoked to describe the systems. This is in line with the philosophy the regulator envision for the license of future NES.

II. RISK-INFORMING SECURITY AND INTRODUCING PERFORMANCE FOR SAFEGUARDS

The general scope of this work is the reinforcement of nuclear security by improving the proliferation resistance of nuclear energy systems. In order to defend NES and prevent malicious attempts aimed at the acquisition of strategic materials from sites or during transport, new safeguard systems can be introduced. However the rational with which safeguard schemes are implemented is the crucial aspect of the problem. In order to be effective the introduction of new safeguards into the NES has to be don two milestones: the effective improvement of the capability to safeguard the site and the effective reduction of the potential proliferation risks associated with the site. A safeguard system purpose has a dual connotation: to detect illicit movements of nuclear materials within and across the boundaries of locations where fissile materials are employed, and to count the material stockpiles present within system's boundaries. However, the cost allocation algorithm followed by the IAEA and by nuclear utilities to arrange safeguards on site, does not necessarily, and very often does not, follow performance principles.

This need is even more marked for sensitive facilities such as reprocessing plants which domestically do not have a dedicated licensing process in place and that internationally urge, for the sake of security, being regulated by norms favoring the highest performance possible

An outstanding example of this concept is provided by the recent cost burden in safeguards and monitoring systems placed for the Rokkasho-Mura reprocessing plant in Japan. Despite all the measures in place and the enormous amount of money spent to securitize the plant, an accidental leak occurred on August 2004. The leak was not detected until April 2005, eight months after it began, at which point about 83,000 liters, containing about 160 kg of plutonium, were released. Opportunities to detect the leak - cell sampling and level measurements - were missed[3].

The above considerations and this last example highlight the necessity of safeguard approaches being integrated with the plant design and driven by performance evaluations made in the conceptual design phase.

However, to establish approaches in favor of security and costs, methods for the evaluation and the assessment of safeguards' performance have to be developed.

II.A. Risk-Informed and performance based assessments for non-proliferation

The approach used in this paper is aligned with the most recent approaches introduced in the field of safety by the US Nuclear Regulatory Commission (NRC)[1].

The Integrated Success Tree Evaluation Methodology presented in this paper to measure the proliferation resistance of NESs can be used both to measure the performance of nuclear designs and to take decisions based on the risk associated with these designs. The measure of performance is defined by the metric Ps, measured in attempts succeeded over the total number of attempts potentially initiated. A Success Tree (ST), replicating the logic of the fault trees normally employed in the safety analyses, provides the structure to explore and perfect the vulnerabilities of a NES. The Ps metric is the top level metric obtained by the tree analysis and represents the probability of success of the potential proliferator attacking the NES. The complement to this metric (i.e., 1-Ps) measures the likelihood to defend the NES from any attack aimed at the acquisition of fissile materials. This complementary measure expresses the NES resilience from acquisition attacks, or in other words the proliferation resistance of the NES. In order to define the risk associated with a nuclear design, the concept of consequences has to be recalled. If Ps is the probability expressing the success to acquire the desired material from the NES, then the obtained material is the most immediate measurable consequence. Introducing the concept of significant quantity (SQ), which is the amount of fissile material necessary for a nuclear weapon device, then allows defining a risk space for the proliferation resistance problem. Each NES or design alternative can be associated with the pair defining the PR risk domain by means of which different NES can be evaluated {Ps, SQ%} probability to succeed in the acquisition attempt and fraction of material obtained.

Risk insights inform the decision process by helping selecting among different design alternatives whenever proper evaluation techniques are set and in place to evaluate the couple (Ps, SQ%). This paper tests an evaluation technique developed at MIT, focusing on performance aspects inherent to the introduction of proper safeguards in the NES scheme of a sodium fast reactor. The measure of performance Ps helps in taking cost-effective decisions, optimizing designs, and scaling the safeguards installed efficiently against the design basis threats.

II.B. The Integrated Success Tree Evaluation Methodology

The method to respond to the need of tools capable of measuring the PR of a particular NES is named as the Integrated Success Tree Evaluation Methodology (ISTEM). The core element of the method is the construction of a Success Tree (ST) measuring the PR for any given threat to the NES. The model allows for the measurement of the intrinsic proliferant features of the design, such as the use of degraded plutonium, as well as the extrinsic features (i.e., safeguards and detection systems). The ST effectively models potential acquisition scenarios and is coupled with an event tree (ET) that captures the physical transition from the point where the material is acquired to any point out of the attacked facility in question. The integration of ET and ST constitutes the ISTEM

The success tree model is a fault tree model that captures the proliferation resistance of a NES by means of a competition model between the two potential actors contending the security of the NES analyzed: the safeguarder on one hand defending the security of the NES and the proliferator on the other side trying to defeat the measures in place to protect the NES.

The tree is inspired from the fault trees used in the safety analysis with the major difference that the basic events forming the top event are driven by the intentions of two competing entities: the safeguarder, such as the IAEA, and the proliferator (e.g., the host state or a set of individual bribed by a terroristic organization)..

II.C. The Sodium Fast Reactor

The PR integrated methodology proposed in this paper is being applied to a specific NES, the sodium fast reactor (SFR). The present study is in fact part of a project promoted by the US Department of Energy to investigate new methods to address the economical feasibility, safety, and non-proliferation resistance of this fuel cycle concept.

The SFR is a promising nuclear design concept among the seven alternatives in the generation IV agenda. The SFR's potential success is due to its mature stage of development, its modularity and the relative affordable scale, and the fact that it comes coupled with a co-located fuel recycling facility.

Despite its potentials, the SFR ability to succeed in new markets depends on the engineers' and policy makers' ability to coordinate themselves in creating coherent "design-policy" systems. As of present, the export of nuclear technologies is in fact limited by the unresolved problem of designing, addressing, and regulating the PR of these fuel cycles.

It is worth mentioning that the SFR-DOE/NERI project scope is to generate valuable methods to guide the improvement of different metrics and that the SFR technology is being used as a platform where these new methods are tested regardless of the specific technology context. With this philosophy, the evaluation method proposed in this paper has been developed, for the sake of its generalization to other NES, with the highest effort to be technology neutral.

III. NUCLEAR RESONANCE FLUORESCENCE SAFEGUARDS

In order to safeguard the SFR plant a specific safeguard system has been selected and incorporated for testing within the proposed assessment method.

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

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

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

One major advantage of NRF technique is the gamma radiation generated and induced by the active Bremsstrahlung beam that is able to penetrate a fuel assembly envelope, or, for the example being set in this paper, the canister containing the separated Pu mix coming out from the electrorefiner; with the potential to accurately track the amounts of each isotope within a sample even at a great distance from its surface.

The NRF application for isotopic identification has other several advantages for the detection of Plutonium coming from spent fuel,[10] if compared to the twin atomic process X-ray Fluorescence Resonance (XRF) that does not allow to obtain clear signals from portions of material located in depth of the target (e.g. this does not permit to identify diversion of SNM within assemblies or canisters).

Specifically for this study, a strategic positioning of the NRF equipment within a plant can accurately monitor material streams continuously almost in real time (i.e. a lag of about 2 hours has been demonstrated for cargo applications[12]). Destructive Assays (DA) techniques take longer times to identify the material sampled. In the case of the US SFR pilot plant EBR-II, a regular verification of the isotopic composition via DA (i.e. sampling and comparing to burn-up code simulations) took between 2 and 3 weeks, a period under which the facility might be arrested if the interrogation of the sample is being caused by suspects on the activities running on site[13].

Regarding the NRF maturity for its possible application as a safeguard for nuclear fuel detection, a set of preliminary tests using Passport Systems' test bed at the 4 MeV MIT accelerator, collaborative research with Pacific Northwest and LLNLs, revealed that strong NRF signature lines are present in the ^{239}Pu, ^{235}U isotopic elements and they can be effectively detected with a transmission method as it was verified at MIT[11].

Finally, the amount of information available for this technology makes it possible to include safeguards efficiency considerations into the ST method. The methods to incorporate this technology within the ST can be generalized and extended to other safeguards.

III.A. Applying the NRF technology to NMA problems

The original application of NRF technology in detection has been in the area of cargo inspections[12]. This section highlights the principles that have been followed in the adaptation process from cargo inspection to nuclear isotopic identification. TABLE 1 summarizes the highlighted principles followed in the adaptation phase from cargo to isotopic identification for nuclear facilities.

When making the transition from cargo inspections to nuclear material accountancy (NMA), some critical aspects had to be considered. One key difference between cargo inspection and NMA is the material that is being inspected. In cargo containers, the material that is being detected is primarily low Z. This allows for a greater volume of material to be inspected. Entire cargo containers can be inspected in a single pass[12], while in the NMA case, only grams of nuclear material can be inspected due to its high Z nature. While this may initially make the nuclear case seem daunting, there is the benefit that when determining the isotopic composition of nuclear materials, the outcome is known. If there is any deviation from the expected outcome, it is a sign of diversion. In the cargo case, the contents of the container are entirely unknown. Anticipating the outcome of the measurement in the nuclear case allows measurements to be made quickly and accurately. A final important difference between the NRF cargo case and the NRF nuclear case is the existence of background radiation in the nuclear case. The material being analyzed is radioactive by itself, but any additional fission products add a great deal more radiation to the system. For this reason, the detectors must be shielded, the beams collimated, and the interrogated photons backscattered to reduce the effects of the background radiation.

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

TABLE 1

Nuclear resonance fluorescence adaptability

Problem specifics	*Cargo Application*	*Isotopic identification in ER*
Material to detect	Partially unknown	Expected with uncertainties
Material form	Any type	SFE, chopped, ingots, powder, pins, liquid
Shielding	Unknown and masked	Cladding, crucible, ER walls, salt
Excitation technique	Photon beam at high En.	Photon beam or spontaneous fission
Target	High and low Z	High Z (U, Pu) and medium Z (FPs)
Mapping type	One unique scan	Multi-scan in different streams + mapping
Operating atmosphere	Air	Air, Argonne or inert gas
Barriers to detection	Materials	Radiation, spontaneous fission, background
Elements	Nitrogen, fertilizer, U238, and other expolives	U235, Pu239, FPs , Actinides (Np, Am, ..)
Z separation in the target	Very distinct and not isotopes	Very similar Z (all the actinides series), FPs

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

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

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

For this reason, given the hostile environment of the hot cell hosting where the electro-refiner equipment operates, the NRF safeguard system, which includes also delicate parts of the equipment, can be positioned at the exit of the cell as shown in the configuration of Figure 10.

III.B. NRF configuration for isotopic detection within a reprocessing facility

Based on the experience matured at the MIT Physics department with this technology, a simplified configuration for isotopic within a reprocessing facility has been virtually set up during a series of meeting held last summer. Due to the change of application for the NRF detector, modifications were made to address the new environment and sample. The high Z nature of the material and the high background radiation requires that a large number of incident photons be used to penetrate the sample and reduce the effects of the background radiation. The background radiation also necessitates the transmission method of detection using a reference scatterer. The transmission method consists of the incident photons attenuating throughout the sample. There is attenuation at all energies, but within the NRF ranges a greater number of photons are attenuated. The resulting beam passes through a collimator to the reference scatterer. The scatterer absorbs the photons within the NRF energy ranges, and then back scatters photons which are captured by the detector. These photons reveal the nature of the sample. The use of the reference scatterer is made possible by knowing the contents of the sample, which is a key difference between the original cargo container application and the NMA application.

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

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

The experiment that was designed has four main components: the creation of the incident beam, the fuel sample being measured, the reference scatterer, and the germanium detector. Figure 8 gives a schematic drawing of what the experimental configuration looks like. An accelerator creates the electrons that are assumed to have an energy of 3MeV. These electrons then are absorbed in the radiator which in turn, releases a beam of photons that range in energy from 3MeV down to 0MeV. The intensity of the beam that is being tracked is then reduced with the use of collimators. Following this initial reduction of intensity, the photons then pass through the sample of separated nuclear material.

The experiment is described by showing the intensities calculated in correspondence with the primary areas in which the photons can be tracked. The division in beam zones was also done to help understand the main vulnerabilities of the apparatus in parallel with the parameters, zones, or part of equipment determining the NRF detection efficiency. Figure 9 shows the findings of this analysis by means of vulnerable points in the experimental configuration.

The following section describes the vulnerabilities and the critical efficient point identified in the NRF configuration selected.

III.D. Efficiency-vulnerability analysis

The rationale used for this approach is that the technical/policy systems introduced to increase the proliferation resistance of the NES (i.e. extrinsic barrier) are not sufficient to guarantee the protection from potential threats unless it their capability proves to operate reliably also when directly exposed to the threat.

When the safeguarder improves his defense strategies by introducing new detection systems, such as the NRF, the potential proliferator consequently readapts his strategies elaborating new tactics to include in the overall strategic threat. This twisted mechanism is indeed the fundamental principle under which the competition between the two potential actors occurs and therefore needs to be accounted for the PR assessment model.

In order to qualify the performance of the NRF apparatus, an analysis to determine the equipment's weak points has been conducted. A set of experts in the area of detection physics were consulted and asked to identify physical vulnerable points and potential improvements in the efficiency of the machines. In a second phase, they were asked to propose a solution to mitigate the weaknesses and, by mean of a questionnaire, to address the resources that had to be devoted to improve the actual NRF configuration.

In order to facilitate these multiple interactions, the NRF configuration, illustrated in Figure 9, was divided into six physical regions which were associated with six corresponding threats. The threats were identified by running a sensitivity analysis on the parameters of the NRF configuration to measure variations in its efficiency, and in parallel by identifying the parts of the equipment most sensitive to physical attacks.

TABLE 2 summarizes the result of the investigation conducted on the NRF configuration.

TABLE 2

NRF efficiency-vulnerability table

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

The following discusses some of the physical regions into which the NRF configuration has been divided and some of the insights provided by this approach.

The first physical region into which the NRF apparatus has been decomposed, region 1, includes the entire system (i.e., NRF equipment, monitoring systems, and power supply). The threat analyzed is a failure of the system originated from a stochastic failure of the machine or by an unintentional initialization of the system. This eventuality differs from the remaining five regions since it does not consider a vulnerability due to an external agent. The inclusion of this event has a dual explanation: first, that the reliability of the system from a safety point of view allows the analyst to reference the security performance to its expected malfunctioning rate. This notion is informative and helps the analyst to scale the dimension of the problem based on his knowledge. Since methods like the one proposed in this paper are not yet part of the current practice and not included in the body of knowledge of security sciences, it is reasonable to expect that new users for these tools will have a background in safety and that they will be referencing new notions to their previous experience.

The second motivation is that the literature recognizes the need to integrate the security and safety dimensions. Some authors in the area of cyber security, in fact, highlight that in order to capture both the probabilistic and semantic meaning of an attack process, it is necessary to assess both the critical chains caused by random events and by malicious events. Even though we recognize the use of hybrid tree structures as fundamental to address the security of a target system, the logic used to construct the ISTM differs from the approach of these authors[21].

These different perspectives are imputable to the different context in which cyber security operates with respect to nuclear security: the semantic of software reliability and hacking security share the source of the system failure which is either the software developer or a potential hacker. In that case, the nature of the basic events in the trees are per se human-driven, therefore hybrid representations merging safety and security aspects are plausible, if not mandatory. In the nuclear case, the safety of the infrastructure analyzed is in most cases driven by the realization of stochastic events, which collide with the agent-based nature of the security aspect. Therefore, the hybrid representation in this context seems less preferable and it has been chosen to minimize the hybrid representation to the reliability of each safeguard system considered. These events have been labeled as NRT, not related to tactics and treated separately from the main body of the ST construction.

An extra motivation in support of the inclusion of a reference reliability value is that it is important to know when a particular safeguard might not be able to operate. A probability changing with the operating condition can be inserted to determine its effective level of functionality. For example, the machine may not be employed during maintenance cycles or might not be able to detect material under special environmental conditions.

In the particular application analyzed in this paper the reliability of the NRF detector is multiplied by the efficiency of the machine as a function of the sample mass. A threshold of 50 grams has been set as the minimum amount being detected by the machine. This value is based on previous experiments[11] showing NRF lines of ^{235}U and ^{238}U for this sample size. Despite no data for Pu are available at this time, an increasing functional relation between sample size and detection efficiency was assumed and included in the BE.

The other five physical regions analyze agent-based events following the same logic illustrated in the example that follows. Region 2 is characterized by the parameters describing the accelerator's electron beam. The equipment on site is the accelerator, the target radiator(s), and shielding materials. The accelerator cooler could be sabotaged to generate a decrease in the beam intensity that in turn could cause a shift in the end-point of the generated spectra. In order to exclude this from occuring, or to reduce the probability of cooling misuse, the safeguarder could invest more resources to protect the cooling system or to monitor the fluctuations in power at the electron beam source. A range for the financial expenditures required to contain the problem has been estimated to be a minimum of zero, corresponding to the situation where no precautions are taken to mitigate the problem, and a maximum value beyond which additional expenses would have no impact on the mitigation strategy adopted. The experts were also asked, in the final phase of the elicitations' process, to answer a written questionnaire by providing a probability curve relating the expected NRF performance with the monetary expenses required to improve the performance. The curves obtained by means of the experts' judgment protocol mentioned are key for the determination of the basic event probabilities of the success tree. In the same way, the entire analysis presented is key for the construction of the ST structure, since it helps in determining proliferator's plausible tactics to defeat the safeguards positioned in the NES, or in the selected location.

The vulnerabilities and inefficiencies revealed by this analysis were subsequently incorporated into the ST as described by the example in the next section.

Another region that offers interesting insight is the region of the cables and circuitry which connects the NRF equipment to the monitoring stations where signals are interpreted by an operator or appropriate software. The experts suggested that this is a very likely event, and the probability estimates they provided reflect this general opinion. The initial solution provided has been to monitor the output coming from the accelerator, to encrypt the data generated by the detector, and to store the data before they are sent to the console where a operator interprets the NRF responses. In addition, to avoid manipulation of the storage unit collecting the encrypting data, it was suggested to cover and seal all the experimental apparatus.

However, this technical solution, also requires the parallel development of coherent policies that allow monitoring the safeguard installed into the facilities. Delivering a safeguard, assembling it, setting it online, sealing it, and then leaving to monitor operations in real time from an off-site control room is a technical solution that might encounter serious policy barriers. This serves as a reminder that the development of tools and technical solutions must often be coupled with consistent and policy solutions, and that as in this case, the two aspects often merge and call for each other.

IV. THE EXAMPLE

IV.A. Success Tree Structure

A numerical example showing the capabilities of the method is presented in this section. The success tree structure built to represent a theft attack of the outlet of an electrorefiner positioned in the hot cell of a pyro-reprocessing facility is shown in Figure 8.

The facility is protected by mean of traditional safeguard systems including surveillance with camera, sampling points, and it is monitored via periodic visits from IAEA inspectors. Additionally, the facility is equipped with a NRF detection machine located at the outlet of the hot cell. Other standard instrumentations to detect individual material properties such as radiation field, weight, or decay heat are not included in this example. A portal for gamma detection to detect possible contamination of the operators is located at the entrance of the facility. A 3D sketch of the equipment and safeguard available in the facility is portrayed in Figure 10.

The success tree shown in Figure 8 is made of 25 events out of which 16 are basic events. The basic event probabilities represent the probability of success for a proliferator attacking the facility's safeguards located in the chosen location. The location that is being chosen is the electrorefiner outlet, where, as indicated by a preliminary analysis, an inventory of about 130 kg is present during normal operations [1].

To complete the tree, the values for the basic event probabilities have to be inserted in its lower branches.

The discussion that follows represents how to measure the probabilities of the basic events constituting the minimal cut sets of the tree. The minimal cut sets (MCS) which are minimal sets of events that cause system success of the top event, ultimately determine the proliferation pathways followed by the proliferator when he combines his tactics. The cut sets and the pathway are determined using the CAFTA software[6]. In this case, there are a total of 72 MCS in the success tree. Every MCS has seven members such as { B, D, E, U, X, Q, R}, of which the first tree B, D, and E are common to all the sets as dictated by the AND logic port that includes all these factors and that asks for the simultaneous realization of the six different detection systems used to detect diversion in the location selected for this example.

The structure of the tree reflects the difficulty of defeating all the systems placed in vicinity of the diversion point: the proliferator success probability depends his capability to defeat all the detection systems in place and for each round (i.e., at each of the N attempts required to acquire a SQ).

Once the basic event probabilities are quantified, the top event probability can be calculated utilizing the structure function. The values of the basic event probabilities are evaluated using two different methods. One is to calculate the probability values utilizing the measures and the other way is to obtain the values of the basic event probabilities directly from the subjective judgments of selected experts.

IV.B. The Theft Scenario: Assumptions and definitions

The malicious attempt to which we refer to is theft, or interchangeably, diversion of special nuclear materials (SNM) such as ^{235}U, ^{233}U, and Pu . The Nuclear Regulatory Commission divides these materials into three main categories, according to their risk, the potential for their direct use in a clandestine fissile explosive where they can be transformed into weapon usable fissile material.

The selected location ER, it's of particular strategic significance within the SFR fuel cycle, and following the NRC criteria it falls within category I since it abundantly contains more than 2 kg of Plutonium.

The SFR REPROCESSING FACILITY has been selected as the place where the malicious attempt(s) occur.

- The THEFT POINT being selected is the outlet of the electrorefiner (ER), where considerable amounts of SNM stocked, such as in the molten salt, or are transiting contained into crucibles at the ER outlet. The electrorefiner is located within a hot cell hosted by the facility.
- MBA: the perimeter of the hot cell area is the material balance area analyzed (MBA), where both standard operations and malicious actions take place.
- THREAT: the repeated diversion or theft of a small quantity of SNM.
- AMOUNT PER ATTEMPT (daily): 16 g/day.
- MATERIAL TYPE: pure Plutonium (or mixed with ER salt).
- TIME REQUIRED TO OBTAIN A SQ: 8000 g / 16g / 365 day/year = 1.37 years (1 year 4 months and 15 days, or 500 days).
- COUNTRY HOSTING THE FACILITY: developed or undeveloped State adhering to the Non-Proliferation Treaty (NPT) and under safeguard agreement.
- CONSEQUENCES: acquisition of 16 g of Pu per day, or of 8 kg of Pu in 1.27 years. It is worth noting that in this scenario the consequences are evaluated in terms of acquisition of SNM and not by radiological effects on individuals. This distinction is being made to remark that the current scenario refers to the proliferation risk which is the potential risk deriving from the acquisition of weapon usable material by mean of concealed tactics and not by means of violent actions or sabotages exposing individuals to the risk of radiation. The misuse of these concepts very often, and as noted by other authors[16], conveys a misleading message with respect to the potential consequences[24] associated with the scenario and lead to the misinterpretation of the two distinguished design concepts of proliferation resistance and physical protection.

- NUMBER OF ACTORS: 2 to 5 actors, depending on the supporting tactics in place that are required to succeed in the daily SNM theft. This action might be driven by the host state or by an external organization bribing the operators within the facility.

The reference scenario being set is the repetition of N attempts. All the attempts, needs to be successful and therefore lead to the realization of the top event in the tree of Figure 2. This, following the tree logic, requires to succeed with at least one of the tactics, and not to fail in each of the N attempts. The overall success probability considering all the N scenarios, then means to succeed to acquire a Significant Quantity (SQ) of Pu from the selected location (i.e., 8 kg of Pu).

The attempts are not identical since the detection systems rely on different detection times and also because the proliferator might improve its strategies over time. No learning factor is considered at this time in the model to count for the plausible increase of confidence in the proliferator’s tactics over time. The time dependency is accounted for by considering different situations or competition schemes.

The first situation reflects the fact that some of the protection systems (i.e., S&C verifications and IAEA inspections) are typically employed to protect the NES periodically while the proliferator acts on a daily basis.

In the second situation, the proliferator faces the introduction of S&C techniques, either because suspects are raised or because the procedures in the facility demand to periodical comparisons of the NRF data with laboratory examinations. The third situation adds the periodical inspectors visit to the site.

Sequencing these situations gives the overall scenario which is characterized, from a proliferator’s perspective, by cyclical increases of the risk of being detected. As a consequence, the proliferator has to readapt his supporting tactics in order to defeat the safeguards systems as they come into play within the facility, and this is reflected in the tree structure.

The safeguard scheme on site can then be classified by looking at the characteristic detecting times of the four individual safeguard/surveillance systems used to protect the NES.

SG I: characterized by 6 months] time windows corresponding to the interval of time between consecutive visits by IAEA inspectors;

SG II: characterized by 3 weeks time windows corresponding to the average interval of time required to set up a sampling and comparing procedure (i.e., pick up a material sample, send it to a lab, and compare it to burn-up code calculations in order to determine the isotopic composition);

SG III: characterized by 2 hours time windows corresponding to the average interval of time required to screen the isotopic composition, via nuclear resonance fluorescence equipment installed at the electrorefiner outlet, to monitor the outcoming batches/flux;

SG IV: characterized by 1 second time windows corresponding to the almost instantaneous time required to visualize suspect movements within the material balance area with cameras and surveillance systems.

IV.C. Features of the safeguard scheme

Once the proliferator decides to attempt a diversion, he must circumvent a series of security systems. If a diversion attempt is made within the reprocessing facility to divert a small quantity of material, the proliferator must confront four main security systems. First he must defeat the containment and surveillance systems. The NRF detector must then be disabled or modified to hide the diversion. These sub-trees will not change significantly overtime. In the longer term however, sampling and comparing must be defeated, and finally on a bi-annual basis, inspectors must be fooled or bribed. These sections of the tree will change with time. The fault tree takes these systems into account and represents the competition that exists between the proliferator and safeguarder in these systems.

The NRF portion of the fault tree demonstrates the weaknesses of the system and highlights potential tactics that could be used to disable the NRF systems’ accountancy benefits. There are three possible tactics that the proliferator can use to beat the NRF without physically modifying the detection portion of the NRF system. The overall system could be disabled via sabotage which could be hidden by staging an accident. The signal coming from the detection system could either be disabled or altered in a way that masks the diversion attempt, and software could be modified that would allow for a diversion but would also mask the results that the safeguarder see. The proliferator can also attempt to disrupt the measurements themselves. This could be achieved by adding material to the sample, or by shielding the bean path to disrupt the counts that the detectors make.

The sub-trees that change over time are the inspections and sampling and comparing. Unlike the NRF and the Containment and Surveillance system (C/S), inspectors and S&C do not happen on a daily basis. For his daily attempts, the proliferator doesn’t need to address these systems. When these security systems are activated, the proliferator must attempt to disable them. Every 3 months, S&C will occur and will force the proliferator to take on different tactics and will greatly reduce his chance of success. Similarly, the proliferator must also change his tactics when inspectors come to the facility. During these two occurrences, the chance of success for the proliferator greatly decreases.

IV.D. Basic Event Probabilities

D.1. Initiating Event

The basic event, Event ER_INIT in Figure 8, is concerned with whether theft is attempted at the electrorefiner outlet, and therefore defined as an initiating event. SNM diversion is of major interest to a proliferator acquiring nuclear weapon capability because such material is essential for manufacturing a nuclear weapon. Since diversion can be attempted at several diversion points, several initiating events, describing diversion events being attempted in a diversion point of the SFR, should be considered in order to assess the overall diversion risk. However, this paper analyzes a single diversion point located at the outlet of one of the electrorefiners hosted in the hot cell of a fuel reprocessing facility. In principle, other locations might be suitable for SNM theft but such a comprehensive evaluation is out of the scope of this paper.

For the determination of the likelihood of the basic event describing the occurrence of a diversion attempt at the selected diversion point, three important factors affecting the basic events were identified and further quantified: material attractiveness (MA), facility attractiveness (FA), and material handling/transport difficulty (HT). These factors define the initiating event ER_INIT, representing the likelihood that the proliferator attempts a theft attack at the selected location, ER. ER_INIT is defined as a top-level intrinsic PR measure, since various sublevel measures determine the factors MA, FA, and HT. A detailed description of how these three factors have been formulated can be found in a parallel paper in the proceedings of the PSAM 2010 Conference[9].

The reason for selecting these factors is that the risk of SNM theft from any facility or during transport operations depends on several risk factors[19] that, using the classification of risk provided by a preliminary study to this assessment[8], can be summarized as:

- The quality, the quantity, and other properties that make the material appealing to a potential proliferator, favoring his decision to illicitly acquire it;
- The level of accessibility to these materials given the operations and the typology of the facility, or means of transport, where these are located;
- The capability to transport the acquired material out of the facility or out of the radar controlling the area where the material was originally used, stocked, or transiting.

The overall risk of SNM theft depends on the balance among these factors, and their aggregation by mean of any mathematical formulation is an indicator of whenever a theft threat is going to be attempted or not at a given location. Assuming that the factors are independent, after an appropriate transformation into a probability value, they can be combined into an multiplicative probability factor expressed by the equation:

$$\Pr(BE)_{INIT\_LOC} = \Pr(BE)_{MA} \times \Pr(BE)_{FA} \times \Pr(BE)_{HT} \qquad (1)$$

where the LOC subscript stands for location and expresses the variability of the measured probability with respect to the location.

It is worth noting that the probability of the event described by Eq. (1) is conditional to the proliferator’s willingness to attempt a SNM theft at that segment of the fuel cycle where the particular material is located. Despite this constitutes a potentially unquantifiable probability, since it depends on an individual actor that might rely his decision on several unknown factors, this probability can be extrapolated by looking at the rate of theft attempts occurring in the past decades and notified to the IAEA’s information system[20]. Over the past 15 years, about 100 states reported 1340 incidents dealing with nuclear materials, 303 of these involving unauthorized acquisition (i.e., by theft) which correspond to about 21 attempts/year. Considering that exactly two thirds of the cases the materials reported lost or stolen either from a specific location or during transportation, were not recovered, this mean the success rate of these malicious acts is of 14 successes/year . Despite the target of these attempts were most of the time radiological sources of various nature and not fissile materials, exception for ^{241}Am, these numbers reveal that the frequency of these events is very high and also potentially measurable.

D.2. Factors formulation

The top PR intrinsic measures, MA, FA, and HT consist of a variety of intermediate and basic metrics; the basic metrics, each of which resembles a different intrinsic feature of the NES, ultimately influences the corresponding top-measure.

The MA measure is an overall indicator of the qualities of materials that relate to the inherent value of the material for a potential proliferator. This concept was first introduced to address the attractiveness of reactor or fuel cycle concepts[15], then changed to address the attractiveness of the material located in the fuel cycle, and most recently it has been replaced by the more comprehensive concept of figure of merit (FOM)[16] considering the weapon capabilities of the actors involved.

The FA factor is constructed in a similar fashion to the MA factor, but it measures the level of attractiveness of a plausible diversion point. There are less quantitative applications of the FA and HT factors in the literature, but the intermediate metrics that affect these factors have been qualitatively described in several compendia published by the PR&PP group[18]. The FA factor is an overall measure of the attractiveness of a diversion point, which describes the extent to which diversion can be covertly undertaken without any detection. In order for an area within the system to be attractive to a potential proliferator, easy access to the facility, sufficient mass of weapon material available to the facility, and minimal modifications to the facilities for diversion are needed.

Finally, the HT factor is an overall measure of the structural requirements imposed by the need for radiation shielding, a device requirement to cooling the internal decay heat of the materials to be diverted, and for the total amount of mass of the material of interest transported. The structural requirements, the cooling system load, and large mass and bulk may impose high costs and inconvenience in handling and transporting the material of interest clandestinely, thereby rendering it easier to detect diversion or forcing the proliferator to desist from his malicious attempt.

After determining factors affecting the basic events using sub-level metrics, it is necessary to convert the calculated values into corresponding probability values required for calculation of the ultimate basic event measure. This probabilistic model is defined as a modulating function, which was determined from expert judgments. A modulation function represents the conditional probabilities that the basic events occur given a factor affecting the basic events as shown in Equation (2).

$$\Pr(BE)_{MA} = Z(MA): \text{ MA modulating function} \qquad (2)$$

where, Z is a function.

A questionnaire is being designed to obtain expert opinions on the conditional probability of a diversion attempt given a factor affecting the basic event. This method is a convenient way to translate measured values into probability values and it seemed to work adequately in a previous simplified example[8] of the framework presented in this paper. For instance, assuming that a value of material attractiveness is measured for a particular diversion point, and by applying this value to the modulating function, an exact conditional probability that a target event would occur can be determined given particular value of the MA measure. An illustrative example of the subjective probability assessment of two domain experts, who were asked to convert the likelihood judgment into a numerical probability value, is illustrated in Figure 3.

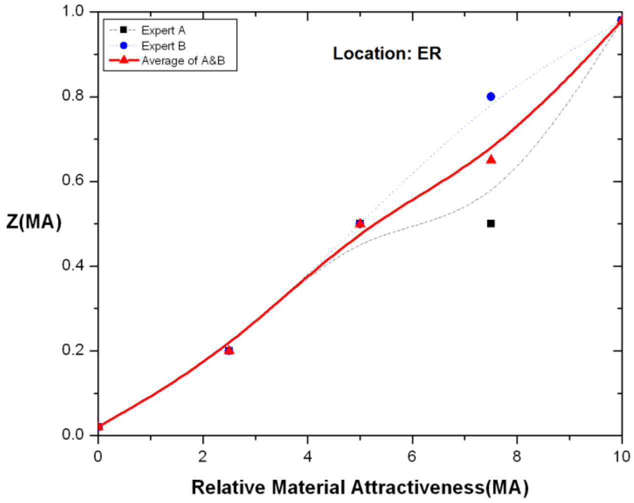

Figure 1. MA Modulating Function at the ER.

The average of each point estimate, reported in TABLE 3, is computed to determine the overall success probability value, and the extremes expressed by the experts serve as the range of the uniform distribution used for the simulations.

TABLE 3

Initiating event and initiating event factors

BE	Event	Estimate	range
B	Pr(ER_INIT)	0.729	0.6735-0.752
B1	Pr(ER_MA)	0.9	0.87 -0.93
B2	Pr(ER_FA)	0.9	0.87 -0.93
B3	Pr(ER_HT)	0.9	0.87 -0.93

The Pr(ER_INIT | Pa) or initiating event probability conditional to the proliferator's intention to set off a theft threat of SNM, Pa, relative to the ST structure shown in Figure 8, has been described in this section. The probability is created starting with measures on the material of interest, the location hosting these materials, and their capability to be handled and transported out of the facility. It is finally worth mentioning that the obtained probability is in principle a function of the resources that the proliferator avails of in his malicious attempt. The inclusion of these resources within the probability estimates is not employed in this branch of the ST but it is incorporated in the part involving the use of safeguards to mitigate eventual threats which is described next.

D.3. Basic event probabilities related to the safeguarder-proliferator competition

The three risk factors expressing the intention and the decision at the basis of a malicious attack, and used to formulate the ST initiating event, can be balanced by:

- The security measures in place to protect the materials;
- The threats those security measures must protect against.

The overall risk of nuclear theft depends on the balance among these factors; the intersection between the three initiating factors and the these new factors related to the capability to effectively safeguard the NES, dominate the global risk of nuclear theft[19]. The property of efficiently safeguarding a particular location, or transportation system, will be referred from now on as safeguardability function (SGB). The SGB allows including into the NES design a safeguard system capable to strengthen the proliferation metric PR, and to also incorporate a measure of its efficiency relative to its ability to strengthen the PR of the NES considered.

This property, that in other contexts is being referred as "safeguard by design[1]", is the property that dominates the competition model embedded in the ST. The proliferator's perspective, in fact, implies to defeat the safeguard systems by eluding their measures and therefore bypassing the safeguardability function built to strengthen the vulnerabilities present on site. In order to capture the "safeguard by design" concept and the already-defined concept of safeguardability, the NRF detector was decomposed into sub-regions and analyzed in its behaviors as discusse in Section III.D. The events emphasized from the vulnerability-efficiency analyses conducted on the pre-design configuration shown in Figure 9 were logically embodied into the tree structure shown in Figure 2.

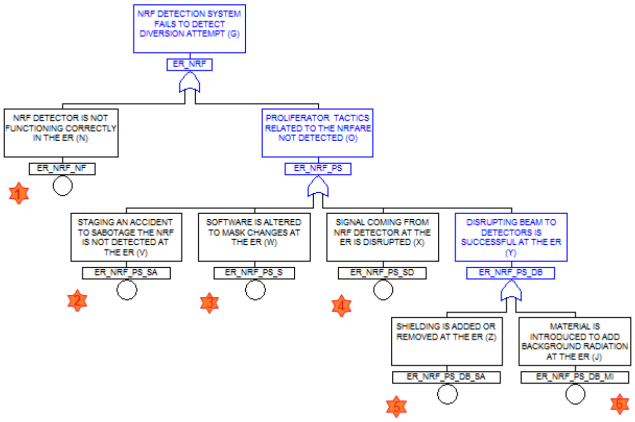
NRF DETECTION SYSTEM FAILS TO DETECT DIVERSION ATTEMPT (G)
ER_NRF
NRF DETECTOR IS NOT FUNCTIONING CORRECTLY IN THE ER (N)
ER_NRF_NF
1
PROLIFERATOR TACTICS RELATED TO THE NRFARE NOT DETECTED (O)
ER_NRF_PS
STAGING AN ACCIDENT TO SABOTAGE THE NRF IS NOT DETECTED AT THE ER (V)
ER_NRF_PS_SA
2
SOFTWARE IS ALTERED TO MASK CHANGES AT THE ER (W)
ER_NRF_PS_S
3
SIGNAL COMING FROM NRF DETECTOR AT THE ER IS DISRUPTED (X)
ER_NRF_PS_SD
4
DISRUPTING BEAM TO DETECTORS IS SUCCESSFUL AT THE ER (Y)
ER_NRF_PS_DB
SHIELDING IS ADDED OR REMOVED AT THE ER (Z)
ER_NRF_PS_DB_SA
5
MATERIAL IS INTRODUCED TO ADD BACKGROUND RADIATION AT THE ER (J)
ER_NRF_PS_DB_MI
6

Figure 2. Success tree measuring the NRF safeguardability

The above figure shows each of the possible threats the NRF detector is exposed to. Each of them is represented by a basic event. The entire threat set, in this case composed of 5 tactics and 1 reference event, constitutes the set of tactics that support the primary proliferator's strategy counted by the initiating event.

By inserting the probability values that the experts provide in the elicitation process, it is then possible to quantitatively estimate the success probability, Ps(SGB_X), of the safeguard X considered.

In other words, the role of the ST is to assemble the event obtained in the decomposition process (i.e. the vulnerability-efficiency assessment) and to provide an overall estimate which includes all the realizations of the supportive tactics used by the proliferator to defeat the X system, assuming these are independently pursued.

The measured metric is a function of the level of expenditure that the safeguarder foresees to use in reaction to a potential proliferator's threat. Implicitly in this process, the safeguarder is assumed to know the proliferator's capabilities. In principle, the competition between the two agents should be asymmetric in the information that each actor can deduce from the opponent. This is because the probability SGB depends on the level of monetary effort that both parties devote to succeed in their respective goals. For the theft scenario considered in this paper, this aspect is left out since the proliferator's resources devoted to succeed are modeled as a constant and hypothesized sufficient in relation to the proliferator's goal (i.e. the diversion of considerably low amounts of material does not require special monetary efforts).

Refined versions of this framework should consider this dependency on the resources of the two competitors.

A similar structure can be replicated for any safeguard or extrinsic barrier of the system. However, in this only the assessment of the NRF safeguard has been evaluated in detail to prove the concept.

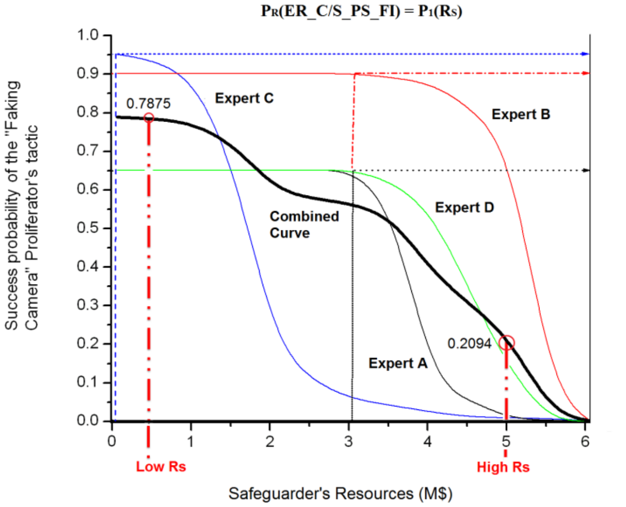

Figure 3. Cumulative combined probability curve for the basic event ER_C/S_PS_FI.

The evaluation of the three extrinsic PR features inserted in the tree, were modeled by putting less effort in their decomposition and using estimates obtained from a previous work [20].

To illustrate the method, Figure 3 shows the estimates from four experts who expressed their opinion on the probability to fool the cameras placed out of the hot cell shown in the scenario cartoon of Figure 10.

The experts were asked to address the success probability as a function of the resources available to protect the location with cameras. The amount of resources devoted in surveillance and containment, measure via experts’ judgment, the efficiency of this safeguard. A lower and an upper bound were chosen to represent the two cases of inadequate and adequate resources to guarantee the C/S function. In this case, the two Pr(BE) values corresponding to 0.5 M$ and 5M$ were used to express the performance of the C/S system for these two distinct cases.

The aggregation of the four experts’ opinion were respectively conducted using the simple equal weighting principle. This approach was taken from the SSHAC study[22] where equal weighting is seen as reasonable since it avoid to determining how to assess who the best expert is, if any, and it provides a decomposition in which different evaluations can be explicitly compared.

The uncertainties associated with the cumulative aggregate probability distribution, $Pr(ER\_C/S)=P_1(Rs)$, were accounted by building a distribution with point estimate, equal to the cumulative curve and ranges equal to the lowest and highest expert estimates.

TABLE 4 reports the data collected from the elicitation process conducted on the NRF, and combines it with the data obtained from previous work for other safeguards.

TABLE 4

Pr(BE) related to tactics obtained from experts

BE	Legend	Low Res	High Res
T	ER_C/S_PS_FI	0.7875	0.2094
U, X	ER_C/S_PS_FS, ER_NRF_PS_SD	0.8	0.0407
R	ER_INSP_TS	0.8625	0.6625
S, Q	ER_INSP_BP, ER_S&C_BP	0.82	0.2983
V, P	ER_NRF_PS_S, ER_S&C_RF	0.01	0.01
W	ER_NRF_PS_SA	0.5	0.5
J	ER_NRF_PS_DB_MI	0.7875	0.1655
Z	ER_NRF_PS_DB_SA	0.659	0.211

D.4. Basic Event Probabilities non related to the Proliferator’s Tactics

The success tree structure also integrate events that have stochastic nature. The basic events D, E, L, and N in Figure 8 describe events that to realize do not need human intervention as it is the case of most of the events belonging to the completion between the safeguarder and the proliferator. However the realization of these events, such as the incorrect calibration of the NRF, or a false alarm at the C/S might bring to light the proliferator’s tactics.

The probability values of the basic events, which are not related to the proliferator’s tactics, or NRT, are evaluated from the subjective assessment of one expert.

In this process, an expert is asked to assign a numerical values to the basic events according to his degree of belief, which reflects states of knowledge. A normal distribution, with a 10% standard deviation was set to describe the epistemic uncertainty of the NRT basic events, as shown in TABLE 5.

TABLE 5

Pr(BE) non related to proliferator’s tactics

BE	Legend	μ	σ
D	ER_AD	0.99	±10%
E	ER_EI	0.5	±10%
L	ER_C/S_NF	0.001	±10%
N	ER_NRF_NF	0.01	±10%

IV.E. Probability calculations

Once the probabilities obtained in the three different ways explained in the previous sections are obtained, the software combines them and provides a measure of the top tree metric Ps, or Pr(NEWTOP), using the labeling of Figure 8, for each of the opposed monetary efforts.

Ps represents the conditional probability to acquire the SNM for each theft attempt, *k*, in an amount that has been *a piori* settled by the proliferator. In order to calculate the proliferation risk corresponding to the acquisition of 1 SQ, the probability to transport the material out of the facility has to be assigned to each scenario as shown by Eq. (3). Then, the obtained value has to be multiplied for the N times the scenario is repeated in order to acquire a full SQ.

$$Pr(SCENARIO|\ Pa)_K = Pr(NEWTOP|\ Pa)_K \times Pr(PT=1) \quad (3)$$

Where Pr(PT=1) represents the probability to successfully transport the acquired material out of the facility, for simplicity assumed equal to the chance of success in passing throughout the gamma detector portal located at the entrance of the facility, as shown in Figure 10 and reported in the event tree of Figure 8.

However, since not all scenarios are identical (i.e. when inspectors visit the plant and when samples are examined with DA techniques, such as S&C), the final formulation for the probability referring to a successful execution of all the attempts, assuming they are all independent, should be given in the form expressed by Eq. (4). For simplicity, we assume that all scenarios are identical and therefore obtained as shown in Eq. (5).

$$\Pr(\text{Acquire 1 SQ}) = [\Pr(\text{SCENARIO}|\ \text{Pa})_K]^{(N-M)} \times [\Pr(\text{SCENARIO}|\ \text{Pa})_J]^{M} \qquad (4)$$

where M is the number of scenarios including S&C verifications and the visits of IAEA inspectors, and
N-M is the number of attempts that have to defeat only C/S and NRF instrumentations.

$$\Pr(\text{Acquire 1 SQ}) = [\Pr(\text{SCENARIO}|\ \text{Pa})_K]^{N} \qquad (5)$$

IV.F. Results

The results obtained from the ST are summarized in this section. The model was simulated with CAFTA and calculations were benchmarked with the uncertainty analysis simulated with the Crystal Ball software[7]. The calculation were set up using the estimates obtained via experts' elicitation, and uncertainties were associated with the estimates following as reported below:

- NRT: Normal distribution with a 10% deviation from the estimated value;
- BE associated with proliferator's tactics and obtained via experts' judgment: uniform distribution with range set up by the extreme values given to the point estimate from the different experts;
- BE associated with the initiating event: uniform distribution with a 10% variability between the point estimate value and the extreme values.

The model was run to test its capabilities under different sets of assumptions. The following list summarizes the key features of the success tree (STi) structures used to simulate the scenarios explored.

ST 1: calculate the top measure Ps without the involvement of S&C and INSP verifications on site;
ST 2: calculate the top measure Ps counting all four safeguards with a low commitment in terms of the safeguarder resources devoted to prevent the proliferator success;
ST 3: as ST 2 above but with high resources devoted (high commitment);
ST 4: calculate the top measure Ps with all the safeguards but not the NRF.

The SNM theft scenario of interest is calculated by combining (N-M) repeated realizations of ST 1, simulating a consecutive set of daily attempts, and with M simulations of ST 2 or 3, depending on the resources considered, providing the case of safeguards additional to the NRF.
ST 4 is used to set the reference condition corresponding to the situation where isotopic measurements are taking place by mean of traditional standard sampling techniques, without NRF expenditures and the related PR benefits.

Figure 4 shows the distribution of the success probability Ps of the top event Pr(NEWTOP) in the two cases where low and high effort in terms of resources are used to safeguard the NES.

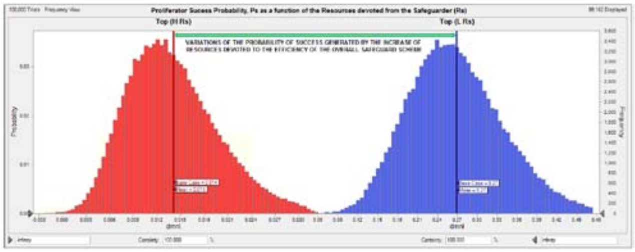

Figure 4. Probability changes obtained by varying the resources devoted to the overall safeguard scheme.

The blue right curve corresponds to the situation where low resources are used to safeguard the scheme, while the red curve represents the same scheme when potentiated by mean of monetary efforts. The graph therefore confirm the model's capability to capture the inefficiencies of the safeguard scheme as well as to reveal the changes in performance when the individual systems are further protected from the proliferator's tactics.

The proliferator's success probability measured at each attempt results to be 0.27 in the low resources case, and 0.014 when the four safeguards are improved. The corresponding monetary expenses in the two cases are correspondingly of 0.258 M$ and 2.61 M$.

Given the provisional value of these numbers at this stage of the project, it is however worth to note that their order of magnitude is relatively low compared to the cost estimates of a reprocessing facility serving a 1800 MWe SFR plant is about 800 M$ considering contingencies, and that the cost of the basic equipment of a NRF detecting device with a 3 MeV accelerator is in the order of 2 M$.

Therefore, it seems that the relative cost of introducing performance changes, in the entire safeguard scheme provides a benefit/cost positive gain in favor of taking the decision to introduce the changes.

Regarding the adoption of NRF technology, the variation measured between the low and high resources case, is equal to 1.8 – 0.21 = 1.57 M$. The high resources evaluation provide by the model, implies to almost double the costs of the NRF machine in a standard configuration (i.e. 1.8M$/2M$ = 90%). Then the introduction of additional systems to protect the NRF equipment should be motivated by a corresponding high gain the measured performance Ps.

Figure 5 summarizes these findings and reports the impact generated by the introduction of NRF safeguards in the scheme. The figure suggests that the introduction of NRF significantly reinforces the robustness of the entire scheme. The proliferator's probability of success is considerably high when the NRF technique is not employed and then falls down of about one order of magnitude when NRF is included in the system. The use of performance measures in the tree made possible to run this evaluation.

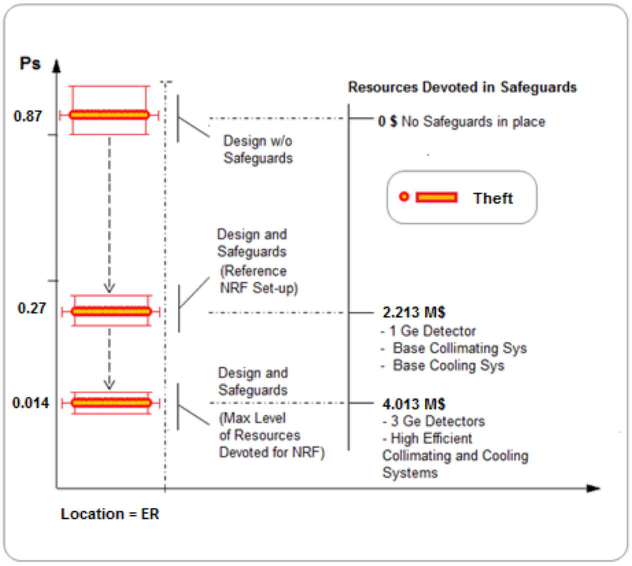
Ps
0.87
0.27
0.014
Resources Devoted in Safeguards
0 $ No Safeguards in place
Design w/o Safeguards
Theft
Design and Safeguards (Reference NRF Set-up)
2.213 M$
- 1 Ge Detector
- Base Collimating Sys
- Base Cooling Sys
Design and Safeguards (Max Level of Resources Devoted for NRF)
4.013 M$
- 3 Ge Detectors
- High Efficient Collimating and Cooling Systems
Location = ER

Figure 5. Efficiency of the NRF detector as a function of the resources devoted from the safeguarder.

The lowest portion of the figure shows the relative merit deriving from the introduction of additional systems to defend the NRF from the proliferator's tactics for 1 attempt. The improvement in the Ps performance factor does not seem significant when compared to the cost gain above commented. However, the importance of having more resources devoted to protect the NES becomes important when the entire scenario leading to the acquisition of 1 SQ with N attempts is considered, as shown by the next figures.

Figure 6 refers to the overall probability, P(scenario), to succeed in all the scenarios required to acquire a significant quantity of SNM. The relation between P(scenario) and Ps is expressed by Eq. 5. The figure reports P(scenario) on the y-axis. The x-axis reports the number of attempts *N* required to obtain 1 SQ, assuming that the configuration of the safeguard scheme is invariant to the mass diverted per attempt (i.e. this happens when the tactic fooling the camera with images is employed). The graph is in logarithmic scale to contain the large variation of P(scenario) due to the high variation of N, from 500 attempts (i.e., 16 g/attempt) in the reference case to 1 (i.e., 8,000 g/attempt).

The two cases of high and low resources are compared. The figure shows that while the trend of the curves is identical, a difference of several orders of magnitude, empathized for the scenarios targeting lower SQ fraction, differentiates the two cases. With respect to the previous analysis, where only one attempt is considered (i.e., SQ %=1 in the figure below), the analysis considering the entire sequence shows the importance to devote high resources devoted the safeguard scheme.

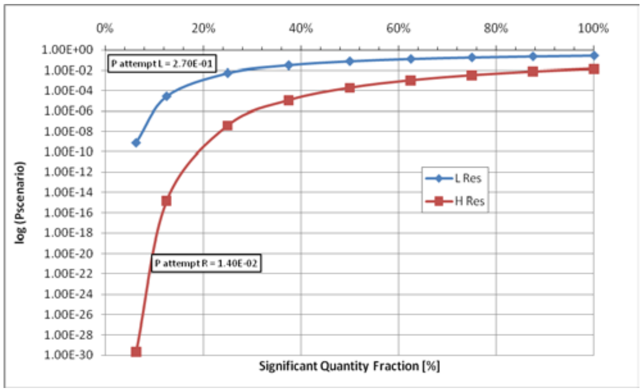

Figure 6. P(scenario) function of SQ – mass independent.

However the behavior on the right side of the curve is not realistic because the probability to acquire 1 SQ in a single attempt is too high. This is because the safeguard scheme analyzed is the C/S system that in our assumptions is not sensitive to the mass of material acquired at each attempt. Figure 7 consider the entire scheme, including NRF and shows that, when the mass assumption is released (i.e., detection efficiency of the NRF is a function of mass), P(scenario) decreases after an optimal point, OPT. The best mass is 8.8% corresponding to 700 g and N=11 attempts.

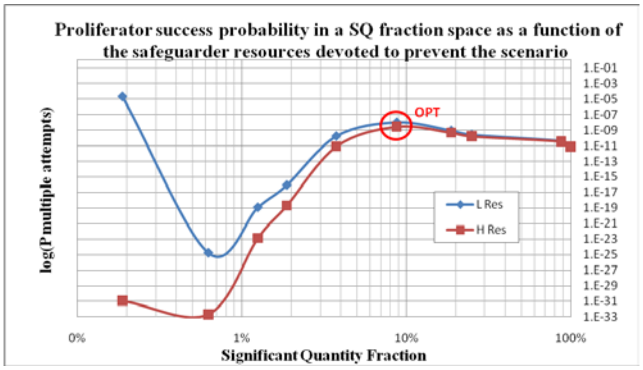

Figure 7. P(scenario) function of SQ – mass dependent.

To conclude, the figure below summarizes the insights that can be obtained from the ISTEM.

It is worth reminding that the goal of the PR assessment method under development is to provide insights and evaluations to assist decision makers in their decisions. For example, the information needed from a regulatory authority responsible for the licensing of a NES in the US, have to be risk-informed. This requires to evaluate the NES in terms of probabilities, Pi, and consequences, Ci, or, in terms of the pairs {Pi, Ci} since the product of the two defines the risk.

In figure below the risk is represented by the pair {P(scenario), SQ%}. The y-axis provides an estimate of the probability that a sequence of *N* theft attempts, which are identical, independent, and conducted on a daily basis, is being conducted successfully by the proliferator. The scenarios are independent because no learning factor from two consecutive attempts is considered. The scenarios are identical because once the proliferator decides how much material he would subtract in a daily attempt, he will day by day subtract always this amount. The x-axis portrays the fraction of SNM material that is being acquired in each attempt. This fraction is calculated over the amount of SNM considered adequate to build a nuclear weapon device with that material. Therefore SQ is a material property that in our case is pure Plutonium (Pu). The value of 1 SQ of Pu is provided by the IAEA and is equal to 8,000 grams. Given that each scenario is made of identical attempts, then when de decides how much material is going to acquire per day, he also knows how many attempts are required to obtain 1 SQ. For this reason the x-axis also include the number of attempts *N* which is inversely proportional to the grams acquired in each attempt. Finally, since the attempts are conducted on a daily basis his initial decision will also dictate the duration of the entire scenario, which is also inversely proportional to *SQ%*. This explain why on the axis are reported the quantities *N*, *SQ%*, and why the same representation can also include time measurements.

The bottom part of the figure portrays the initial decision: collecting 1 SQ with 500 tiny pieces of material on one side (i.e., the reference scenario) or to acquire it in one single attempt on the other extreme. Thus, a point in the plane, or a pair {P, SQ} represents the risk involved in a multiple attempt sequence where the ultimate consequence is always to obtain 1 SQ with *N* subtractions SQ%. Two sets of points, or curves, are represented in this plane. The upper curve shows the results obtained with the ISTEM model, using the experts estimates for the case of low resources devoted to the safeguard scheme. The lower

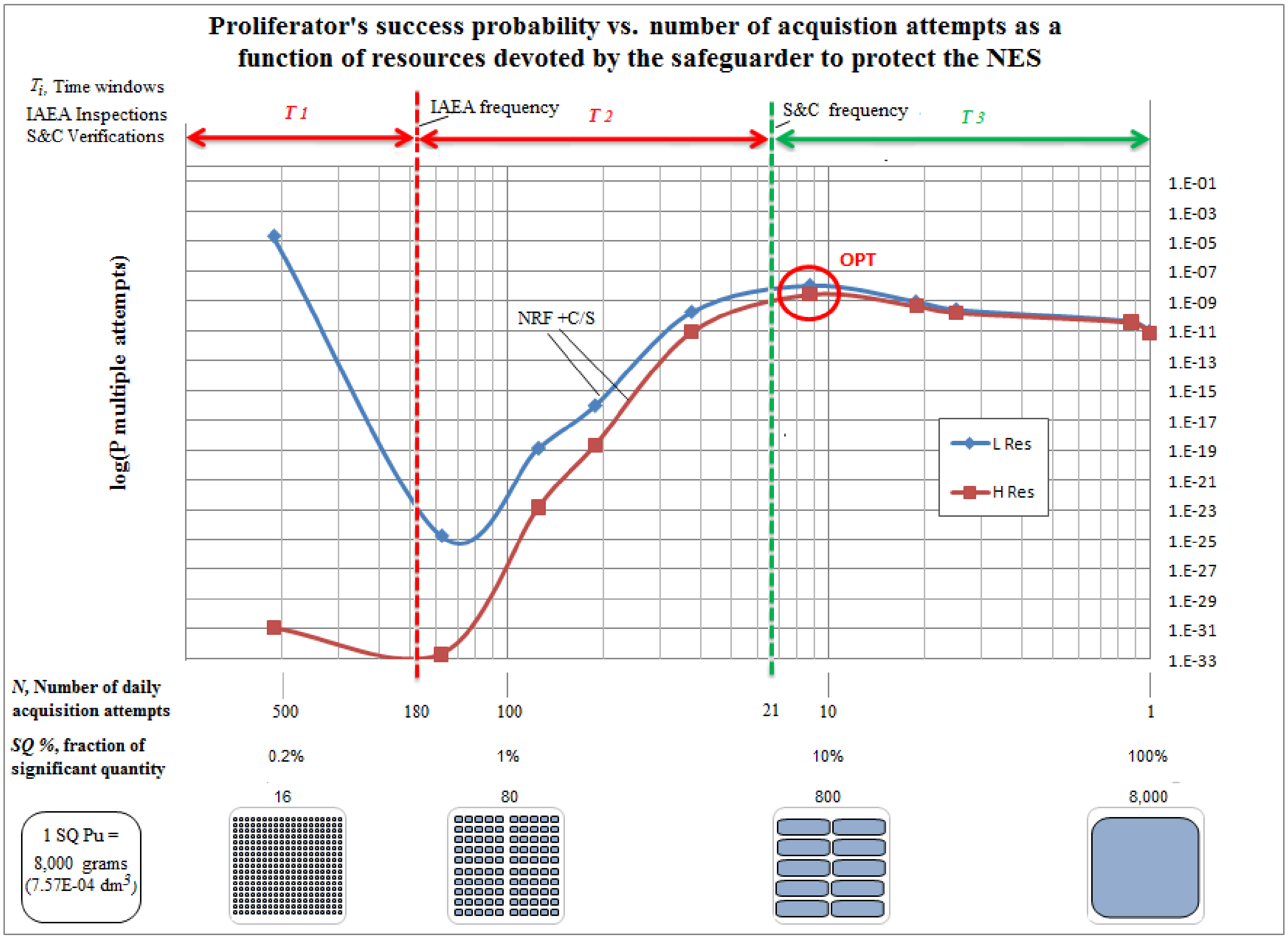

Figure. Results generated by the model

curve represents the other extreme condition where high resources are employed. Since the NRF detection efficiency is sensitive to mass, the behaviors of the two sets is varying with the SQ fraction. The diagram is finally divided in three time windows. The first, T1, shows the frequency at which the IAEA inspectors come to visit the plant. All the scenarios between 500 days and 180 days (i.e., the inspectors visit the plant every 6 months) it is likely that are going to be detected at day 180 when the inspectors, unless bribed, will observe that 180*16= 2,880 grams are missing. Therefore despite the high P to succeed in this region, the proliferator won’t pursue strategies involving more than 180 days, unless he knows that few resources have been devoted in the safeguard scheme. In the same way if S&C verifications are employed every 21 days, the proliferator will have to have a new tactic to defeat this additional safeguard. Every scenario below 21 days will then have to face only C/S and NRF systems. Given that C/S is invariant to mass, the proliferator would have to find the optimal mass to defeat the NRF in this time window. However the proliferator is only aware of the frequencies at which the IAEA visits and S&C verifications occur but he is not knowledgeable about the existence of any optimal point in region 3. Differently, policy makers, or designers know the results obtained from the analysis and consequently taking decisions with the support of risk-information and measures of performance.

V. CONCLUSIONS

The research presented in this work has explored the applicability of a comprehensive methodology for the proliferation resistance assessment of the Sodium Fast Reactor (SFR), one of the Generation IV concepts. This comprehensive methodology is referred to as the Integrated Success Tree Evaluation Methodology (ISTEM). The methodology establishes the theft of SNM by mean of a competition model embedded into success tree and event tree logic diagrams. Most of the previous proliferation studies followed either the attribute approach or scenario approach. Either approach has not adequately reflected the competitive interactions between a host State (i.e., the proliferator) and safeguarders, such as the IAEA.

The key interest for the practical application of current proliferation assessments is competition between these two opponents. Accordingly, the ISTEM constitutes a hybrid method that combines multi-attribute measures, such as MA, with the scenarios formulated using event and success trees.

The expert judgment for the calculation of the BE probabilities’ competition structure, elaborated as a function of the resources devoted, establishes a direct relationship between the PR performance measured in terms of the success probability metric, Ps, and the costs associated with the implementation of improvements of the same performance.

The illustrative example, although oversimplified, confirms the ability of the model to provide adequate responses to the applied design changes in the safeguard scheme and the NES.

The SNM theft with repeated attempts, despite the use of numbers not coming from a formal elicitation process, confirmed the extreme difficulties encountered by a terrorist organization to acquire SNM, even though in small quantities from a reprocessing facility.

Further demonstrations of the method’s ability to provide risk information, will be included in the next products generated by the SFR-DOE/NERI project[9].

VI. FUTURE RECOMMENDATIONS

The ISTEM method has been framed and applied the problem of quantitatively analyzing the PR metric and taking the ER location in the SFR reprocessing facility as an example. The core structure within the evaluation method created so far, is the success tree. Its tree structure has the following major benefit: to host a competition model that generate scenarios of diversion and that can also include non agent-based realizations such as the efficiency of a safeguard. The tree structure has been used to test the impact of the addition of new safeguards in terms of PR. the same structure also easily can be used to evaluate the impact of intrinsic barriers such as the use of degraded Plutonium. One of the main difficulties encountered during the formulation of the example is the selection of proper probabilities for the basic events. This has been partially remediated by creating an expert’s elicitation process. Although, the opinion from experts in turn pose other issues such as how to choose the experts and how to weight their opinion, this approach allowed to test the model numerically. The probabilities obtained by the expert have been expresses as a function of the resources that potentially can be devoted to improve the performance of the safeguards protecting the NES. The advantage of this approach is to include into the tree the notions of vulnerability and efficiency. The first notion ask the experts to provide solutions to possible threats such as signal attacks, camera fooling, etc. The second notion, asks the experts to provide the probability to fail of a safeguard as a function of a form of the safeguard efficiency that can be expressed as number of false alarms, probability of a wrong initialization, etc. for the reference safeguard analyzed the efficiency was expressed as proportional to mass of the sample. The use of these notions also revealed satisfactory since it produced results that very meaningful and produced insights.

It is however recognized that the parameters and the experts estimates have not been accurately quantified, and that at this stage of development, the results provided by the ISTEM cannot certainly be regarded as an assessment of the SFR.

Future work will continue refining the model, testing the elicitation process with different pool of experts, and obtaining data for the efficiency curves.

Also in order to obtain more realistic scenarios data from real experiments of the NRF and data on the facility should be obtained.

All the above would allow to obtain more realistic insights and to let the method being regarded as a tool to assist policy making decision or investments and not just as a methodology development study.

ACKNOWLEDGMENTS

This work is a product 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.

NOMENCLATURE

NES = Nuclear Energy System
ER = electrorefiner
SFR = Sodium Fast Reactor
NRC = Nuclear Regulatory Commission
NPT = Non Proliferation Treaty
IAEA = International Atomic Energy Agency
LANL = Los Alamos National Labs
LLNL = Lawrence Livermore National Labs
NRT = Non-proliferation Related Tactics
NMA = Nuclear Material Accountancy
MBA = Material Balance Area
SQ = Significant Quantity
BE = Basic Event
FA = Facility Attractiveness
SGB = Safeguard Efficiency or safeguardability
SG = Safeguard System
MA = Material Attractiveness
HT = Handle Transportation difficulty
C/S = Containment and Surveillance
NRF = Nuclear Resonance Fluorescence
PPA = Pulsed Photon Accelerator
S&C = Sampling and Comparing
INSP = IAEA Inspectors
DA = Destructive Assay
NDA = Non Destructive Assay
MCS = minimal Cut Set
ST = Success Tree
ET = Event Tree
PR&PP = Physical Protection & Proliferation Resistance
ISTEM = Integrated Success Tree Evaluation Methodology

REFERENCES

1. Yue M., Cheng L., Bari R.A., *“A Markov Model Approach to Proliferation-Resistance Assessment of Nuclear Energy Systems,”* Nuclear Technology vol. 162 pp.26-44 (2008).

2. Bean R.S. et al., *“Safeguards-by-Design: An Element of 3S Integration,”* IAEA Symposium on Nuclear Safety, IAEA-CN-166/067 (2008).

3. A description of the accident with reasonable critics and comments can be found at http://www.japanfocus.org/site/view/103 (2005).

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

5. US NRC website, *“Classification of Special Nuclear Material and Safeguards”*. http://www.nrc.gov/security/snm.html

6. CAFTA Software. Electric Power Research Institute. Data systems and solutions 1994-2007. Version 5.3 educational edition (2009)

7. Crystal ball software Decisioneering, Inc., Professional Crystal Ball 11.1, educational Edition (2008).

8. Ham H. and Golay M. W.: *“An integrated Methodology for Quantitative Assessment of proliferation Resistance of Advanced Nuclear Systems Using Probabilistic Methods”*. CANES PhD Thesis, MIT-NFC-TR-084, (2006).

9. Cavalieri d’Oro E., Golay M.W., *“Risk-Informed and Performance Based Metrics and Regulatory Limits to Assess the Proliferation Resistance of Nuclear Energy Systems,”* Proceedings of the PSAM 2010 Conference, to be published (2010).

10. S. J. Tobin et al., *“Determination of plutonium content in spent fuel with NDA – why an integrated approach?”*. Los Alamos National Labs, 2008. LA-UR-08-03763 (2008).

11. W. Bertozzi et. al., *“Nuclear Resonance Fluorescence Excitations near 2 MeV in 235U and 239Pu,”* Physical Review C 78, 041601(R) (2008).

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

13. Personal communication with Prof. Michael Lineberry, MIT (2009).

14. Koji Sato et al., *"Conceptual Design on an Integrated Metallic Fuel Recycle System,"*, Takeshi Yokoo, Tadashi Inoue Pyro-Process Fuel Cycle Project, Komae Resesarch Laboratory, Central Research Institute of Electric Power Industry 2-11-1, Iwado Kita, Komae, Tokyo 201-8511 Japan (2001).

15. Galperin, A. et al., *"Thorium Fuel for LWR - Reducing Proliferation Potential of Nuclear Power Fuel Cycle,"* Science & Global Security, Volume 6, pp. 265-290, (1997).

16. Bathke C. G.. et al., *"The Attractiveness Of Materials In Advanced Nuclear Fuel Cycles For Various Proliferation And Theft Scenarios,"* Proceedings of Global 2009, Paris, France, September 6-11, paper 9543, (2009).

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

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

19. Bunn Matthew, "*Reducing the Greatest Risks of nuclear Theft & Terrorism,"* Harvard School of Government. Cambridge, MA January 2010 http://enews.belfercenter.org/ct.html?rtr=on&s=lj1i,k0zj,7oo,k28q,19gc,b18w,2i9t (2010).

20. IAEA Illicit Trafficking Database. Vienna, IAEA website last updated provided: 1 September 2008 http://www.iaea.org/NewsCenter/Features/RadSources/PDF/fact_figures2007.pdf (2008).

21. Fovino I. N., Masera M., De Cian A., "*Integrating Cyber Attacks within Fault Trees*," Reliability Engineering and System Safety vol. 94 pp. 1394-1402 (2009).

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

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

24. Cavalieri d'Oro E., Proceedings of the Fuel Cycle Research & Development (FCR&D) 2009 Annual Meeting Agenda, Albuquerque, NM 87110, October 20-22 (2009).

25. Picture courtesy of Alberto Soto Marín Industrial Design.

APPENDIX: DIAGRAMS AND FIGURES

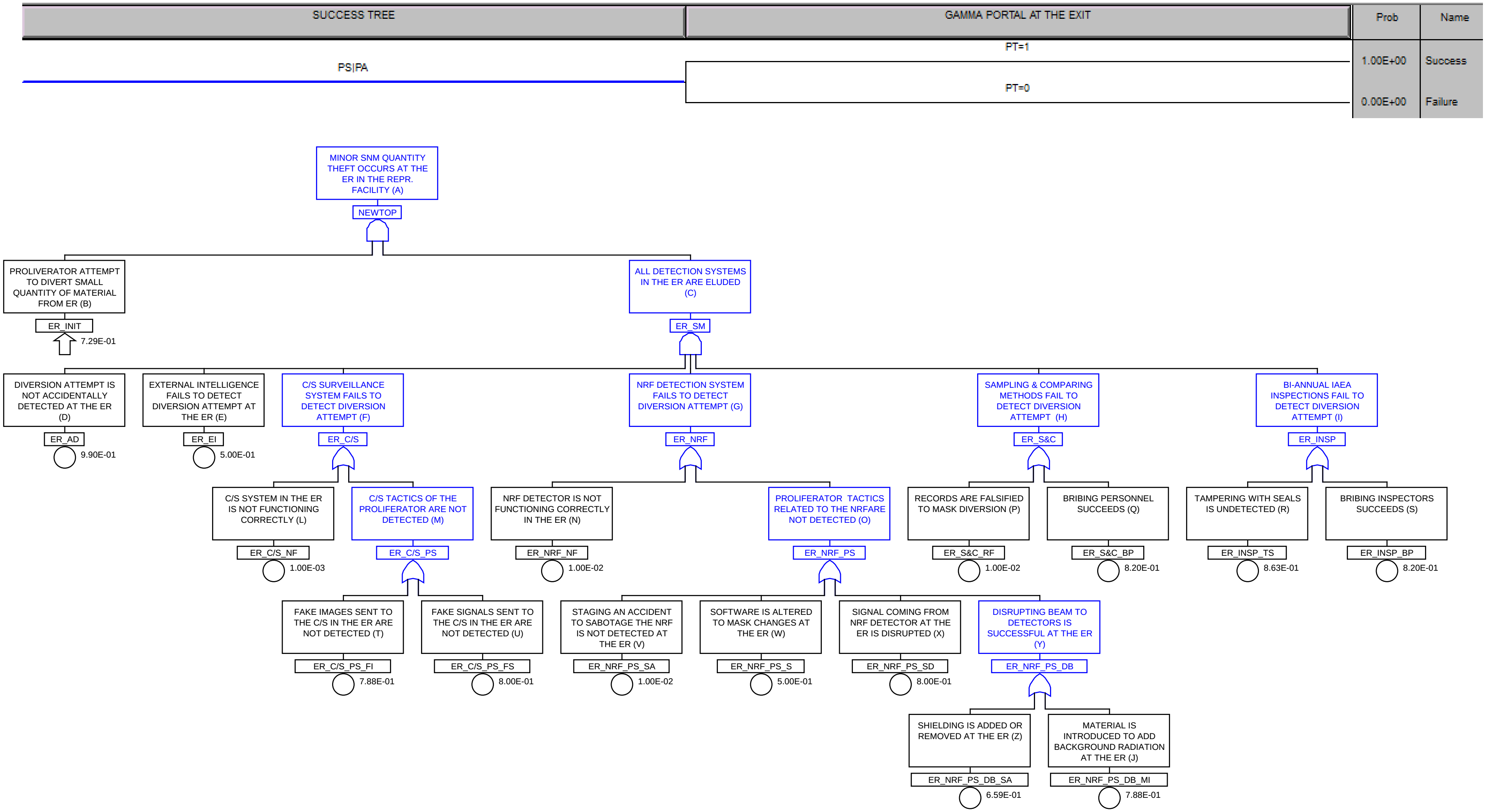
SUCCESS TREE
GAMMA PORTAL AT THE EXIT
Prob
Name
PS|PA
PT=1
PT=0
1.00E+00
Success
0.00E+00
Failure
MINOR SNM QUANTITY THEFT OCCURS AT THE ER IN THE REPR. FACILITY (A)
NEWTOP
PROLIVERATOR ATTEMPT TO DIVERT SMALL QUANTITY OF MATERIAL FROM ER (B)
ER_INIT
7.29E-01
ALL DETECTION SYSTEMS IN THE ER ARE ELUDED (C)
ER_SM
DIVERSION ATTEMPT IS NOT ACCIDENTALLY DETECTED AT THE ER (D)
ER_AD
9.90E-01
EXTERNAL INTELLIGENCE FAILS TO DETECT DIVERSION ATTEMPT AT THE ER (E)
ER_EI
5.00E-01
C/S SURVEILLANCE SYSTEM FAILS TO DETECT DIVERSION ATTEMPT (F)
ER_C/S
NRF DETECTION SYSTEM FAILS TO DETECT DIVERSION ATTEMPT (G)
ER_NRF
SAMPLING & COMPARING METHODS FAIL TO DETECT DIVERSION ATTEMPT (H)
ER_S&C
BI-ANNUAL IAEA INSPECTIONS FAIL TO DETECT DIVERSION ATTEMPT (I)
ER_INSP
C/S SYSTEM IN THE ER IS NOT FUNCTIONING CORRECTLY (L)
ER_C/S_NF
1.00E-03
C/S TACTICS OF THE PROLIFERATOR ARE NOT DETECTED (M)
ER_C/S_PS
NRF DETECTOR IS NOT FUNCTIONING CORRECTLY IN THE ER (N)
ER_NRF_NF
1.00E-02
PROLIFERATOR TACTICS RELATED TO THE NRFARE NOT DETECTED (O)
ER_NRF_PS
RECORDS ARE FALSIFIED TO MASK DIVERSION (P)
ER_S&C_RF
1.00E-02
BRIBING PERSONNEL SUCCEEDS (Q)
ER_S&C_BP
8.20E-01
TAMPERING WITH SEALS IS UNDETECTED (R)
ER_INSP_TS
8.63E-01
BRIBING INSPECTORS SUCCEEDS (S)
ER_INSP_BP
8.20E-01
FAKE IMAGES SENT TO THE C/S IN THE ER ARE NOT DETECTED (T)
ER_C/S_PS_FI
7.88E-01
FAKE SIGNALS SENT TO THE C/S IN THE ER ARE NOT DETECTED (U)
ER_C/S_PS_FS
8.00E-01
STAGING AN ACCIDENT TO SABOTAGE THE NRF IS NOT DETECTED AT THE ER (V)
ER_NRF_PS_SA
1.00E-02
SOFTWARE IS ALTERED TO MASK CHANGES AT THE ER (W)
ER_NRF_PS_S
5.00E-01
SIGNAL COMING FROM NRF DETECTOR AT THE ER IS DISRUPTED (X)
ER_NRF_PS_SD
8.00E-01
DISRUPTING BEAM TO DETECTORS IS SUCCESSFUL AT THE ER (Y)
ER_NRF_PS_DB
SHIELDING IS ADDED OR REMOVED AT THE ER (Z)
ER_NRF_PS_DB_SA
6.59E-01
MATERIAL IS INTRODUCED TO ADD BACKGROUND RADIATION AT THE ER (J)
ER_NRF_PS_DB_MI
7.88E-01

Figure 8. Success/Event trees structures used to describe the probability to acquire SNM from the electro-refiner located into the hot cell of a reprocessing facility.

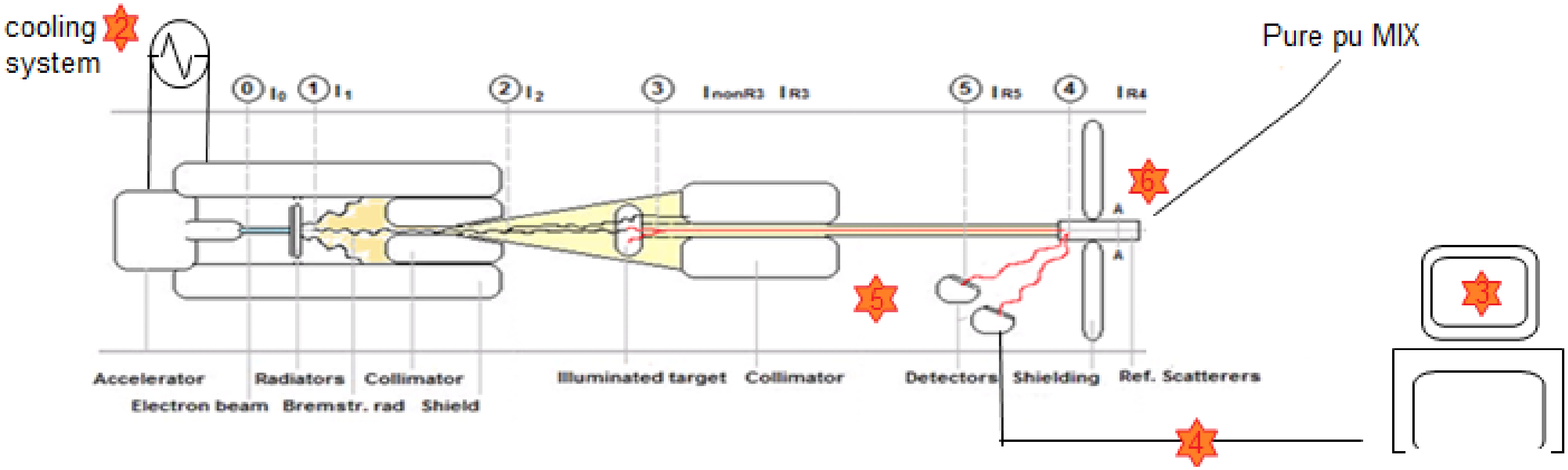

Figure 9. Schematic of the experimental pre-design created to study the NRF detection system showing the potential vulnerable points and beam zones.

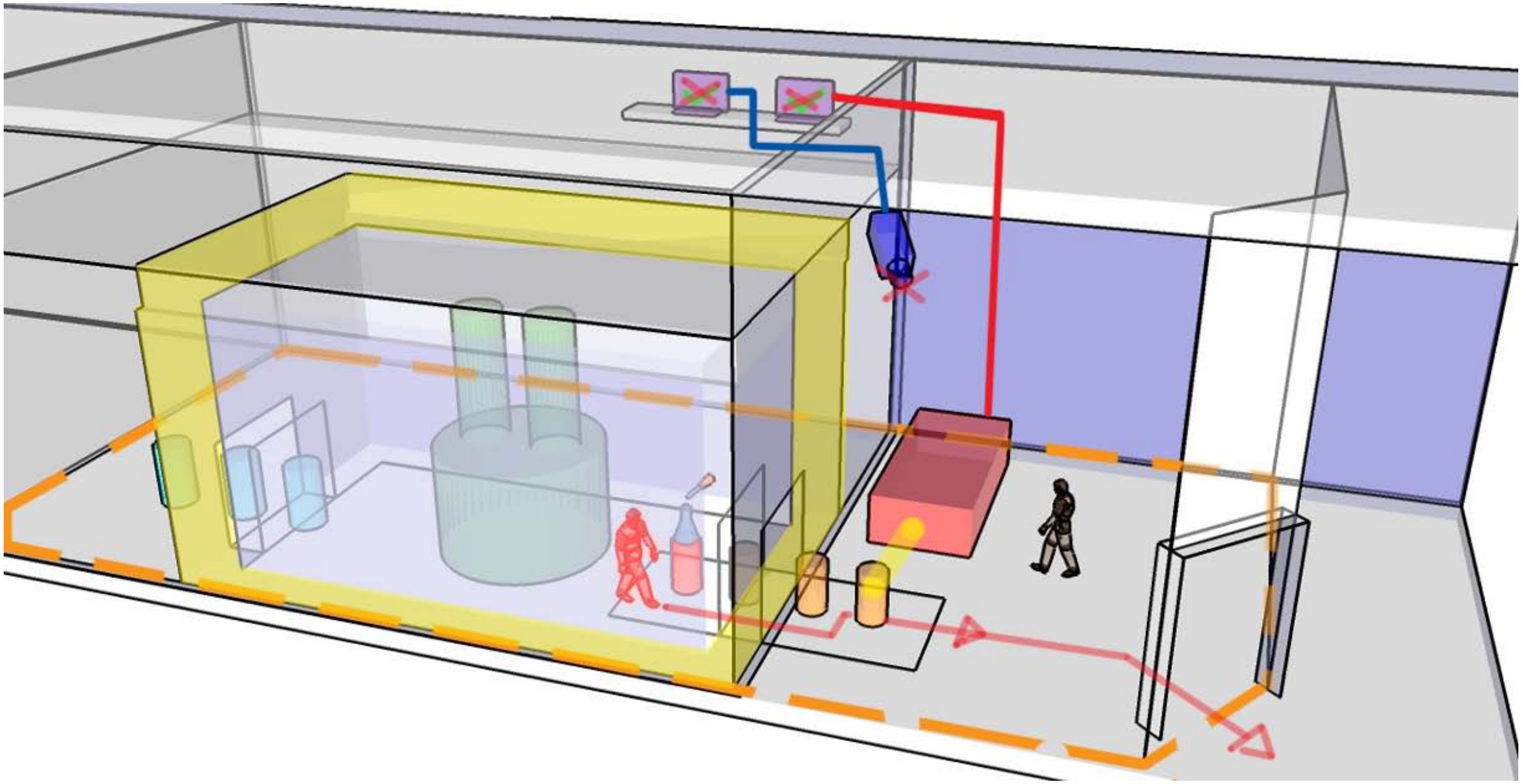

Figure 10. Pathway for theft of nuclear special materials and safeguard scheme elusion in the hot cell of a fuel reprocessing facility[25].