SAND2008-2051C

IMPLEMENTATION OF A RISK INFORMED ANALYSIS APPROACH TO OPTIMIZE SAFEGUARDS

Virginia Cleary[1], Gary Rochau[1], Carmen M. Méndez[2]

[1]Sandia National Laboratories - P.O. Box 5800 MS0748, Albuquerque, NM 87185
[2]Sociotecnia Solutions, LLC - 4581 Weston Rd #174, Weston, FL 33331

ABSTRACT

In light of the planned growth and expansion of nuclear fuel cycle facilities (including reactors) throughout the international community, the resources of the International Atomic Energy Agency (IAEA) will need to be optimized to ensure the successful implementation of safeguards at civilian nuclear facilities at the lowest possible cost. The use of risk informed analysis for decision making is a widely accepted methodology in the safety community. The U.S. Nuclear Regulatory Commission has utilized a risk informed methodology to optimize their resources, time and effectiveness successfully. The use of Probabilistic Risk Assessment (PRA) to evaluate risk systematically, comprehensively, and methodically is the foundation for the NRC risk informed decision-making process.

The authors believe that the use of a risk informed analysis approach can also be applied to safeguards successfully. The use of such a methodology can help define the appropriate balance between process monitoring and material accountability measures. Equipment, inspectors, cost, effectiveness, accuracy, data analysis and time can all be optimized by identifying the key areas of risk. In addition, the application of a risk informed analysis approach will result in an auditable and transparent method for developing safeguard approaches. This paper will introduce the key components to successful implementation of a risk analysis approach for use in the safeguards community.

Key Words: *Safeguards, Risk Informed, Decision-making*

INTRODUCTION

Risk in PRA is defined as the probability of an event occurring multiplied by the consequence of such an event occurring. PRA answers the fundamental questions of

(a) what adverse events can occur,
(b) what is the probability of these adverse events occurring, and
(c) what are the consequences of the occurrence of an adverse event?

Once an acceptable quantitative risk metric is defined (i.e. fatalities per year, core damage frequency), it is possible to then utilize risk informed decision making as a tool to evaluate the design of a facility or changes to a facility (in terms of design, operation, etc) and the effect of the changes on the safety of a system and its components. When the established risk threshold is not surpassed, the change to the system is deemed acceptable.

The current era of risk informed regulation began in 1995 when the NRC issued a policy statement on the "Use of Probabilistic Methods in Nuclear Regulatory Activities [1]." This policy stated:

> "… an overall policy on the use of PRA methods in nuclear regulatory activities should be established so that many potential activities of PRA can be implemented in a consistent and predictable manner that would promote regulatory stability and efficiency."

In the policy statement, the NRC said it expected that implementation of the policy would improve the regulatory process in three ways: "by incorporating PRA insights in regulatory decisions, by conserving agency resources, and by reducing unnecessary burden on licensees."

In 1998, the NRC formally defined risk informed regulation as "an approach to regulatory decision-making that uses risk insights as well as traditional considerations to focus regulatory and licensee attention on design and operational issues commensurate with their importance to health and safety [2]."

The NRC further stated in "Use of Risk in Nuclear Regulations" that the traditional approach to safety is improved by utilizing a risk informed approach by:

(a) "explicitly considering a broader range of safety challenges;
(b) prioritizing these challenges on the basis of risk significance, operating experience, and/or engineering judgment;
(c) considering a broader range of countermeasures against these challenges;
(d) explicitly identifying and quantifying uncertainties in analyses; and
(e) testing the sensitivity of the results to key assumptions.[3]"

The use of PRA by the NRC has substantially increased since the first issued NRC policy in 1995. In addition, use of PRA for risk informed decision-making is being utilized in other industries: chemical, aerospace, construction, financing and management planning. The application of risk-informed decision making in all these areas suggests that a risk-based approach could also be successfully applied to safeguards.

APPLICATION TO SAFEGUARDS

According to the International Atomic Energy Agency's (IAEA) Safeguards glossary, "safeguards are applied by the IAEA to verify that commitments made by States under safeguards agreements with the IAEA are fulfilled [4]." In addition, it states that the objectives of the IAEA safeguards are:

(a) "…to verify a State's compliance with its undertaking to accept safeguards on all nuclear material in all its peaceful nuclear activities and to verify that such material is not diverted to nuclear weapons or other nuclear explosive devices [4]."
(b) and "…the detection of undeclared nuclear material and activities in a state[4]"

Thus, the IAEA is responsible for the design and implementation of a safeguards approach on all member states' civilian nuclear facilities. The IAEA defines safeguards approach as "a set of safeguards measures chosen for the implementation of safeguards in

a given situation in order to meet the applicable safeguards objectives [4]." The IAEA recommends developing model (generic) facility safeguards approaches, but note in their glossary, application at a specific facility requires "adapting the model approach (where such exists) to account for actual conditions at the facility as compared with the reference plant [4]." In addition, the IAEA develops a state level safeguard approach which encompasses "all nuclear material, nuclear installations and nuclear fuel cycle related activities in that state… and location outside (of the nuclear) facilities in the state… that would enable the IAEA to draw and maintain a conclusion of the absence of undeclared nuclear material and activities…[4]." The responsibilities of the IAEA are far-reaching and ever expanding; thus, resulting in a potential strain on the available resources and time of the Agency.

The rapidly approaching "Nuclear Renaissance" will further stretch the available resources of the IAEA. Thus, a systematic, comprehensive and methodical approach to safeguard implementations will be a valuable tool for the IAEA. The application of this tool will ensure that each member state's nuclear fuel cycle program will have a similar metric for measuring risk.

One goal of IAEA Safeguards is the timely detection of material diversion. In order to apply the risk informed decision-making methodology to safeguards, an acceptable level of risk must be identified for safeguards applications. An example might be: to detect with 95% confidence that a significant quantity (SQ) of material has not been diverted within a country's nuclear program during one year. Thus, by inference, an acceptable level of risk is the diversion of less than one SQ of material per year with a confidence level of 95%; however, a lower level of risk can be utilized once defined.

IAEA is charged with verifying both the correctness and completeness of declarations provided by a state within the safeguards regime [5]. In order to successfully achieve these objectives, the Agency must implement safeguards systems that are both comprehensive (to verify the completeness of information) and reliable (to verify correctness).

DESCRIPTION

As previously defined, risk is the probability of an event occurring multiplied by the consequences of such an event occurring. In traditional safety PRA practices, the common methodology is the evaluation of fault trees and event trees. The use of fault trees and event trees provides an auditable and transparent analysis tool, which provides clear and precise documentation of not only the results but also the method of analysis. Fault trees use Boolean logic to analyze the various ways a component can fail. For example, a valve's failure can be the result of a mechanical, electrical, or human error. Fault trees aide the analyst in looking at all failure modes and associating a probability of failure with each mode. Event trees are used to systematically evaluate all of the events that can occur in a system. For example, a loss of coolant accident can be initiated by a pipe break. However, the ability of all the safety related components to mitigate the initiating event will determine the accident progression state.

For applications to safeguards, fault trees can be utilized to determine all the failure modes for the extrinsic sensors and monitors utilized in the facilities safeguard design. Event trees can be systematically utilized to evaluate all the different types of diversion that can occur.

In order for fault trees to be constructed, an analysis of all detectors, monitors and sensors utilized in safeguards will have to be conducted to determine their probability of failure. For example, video cameras are consistently used in safeguard approaches to monitor the events at a civilian nuclear facility. A breakdown of video camera equipment can hinder the IAEA's ability to timely verify the correctness of information. Building in contingencies for data collection to avoid delays due to breakdowns can become extremely costly, especially given the number of video cameras that would need to be implemented to ensure the continuity of data availability. This is where a PRA approach can help optimize the safeguards solution: breakdowns of video camera equipment can be traced to a mechanical failure (a component of the machine breaks), an electrical failure (power for the video camera is lost), human failure (the analyst watching the video could fail to detect the diversion), etc. Fault trees can be constructed after all of the various failures for each detector are determined and probabilities for each type of failure calculated. Figure 1 shows a simplified, high-level example of what a safeguard's fault tree for a radiation detector could look like. The fault tree shown in Figure 1 details all the potential events that could cause a radiation detector to fail.

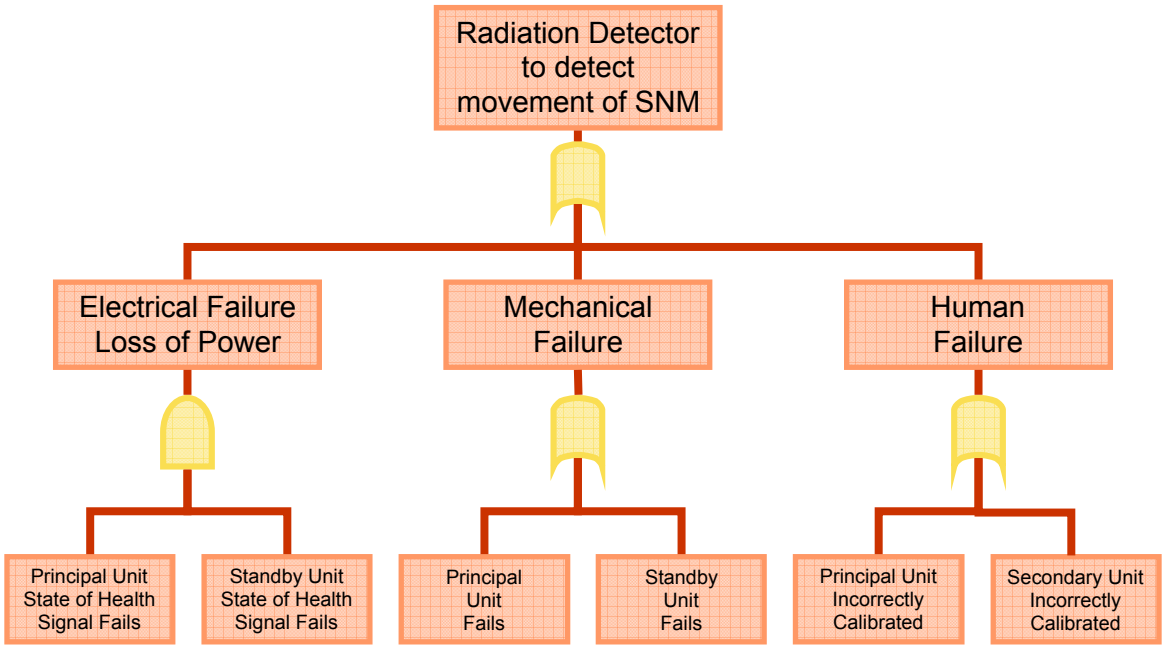

Figure 1: Sample fault tree for a radiation detector that would indicate failure modes of the detector. Probabilities would be determined for each type of failure; thus, providing an estimated failure rate for the system.

According to Proliferation Resistance and Physical Protection Evaluation Methodology Expert Group, proliferation "…targets are nuclear material, equipment, and processes to be protected from threats of diversion and misuse. Pathways are potential sequences of

events and actions followed by the actor to achieve objectives. For each target, individual pathways are divided into segments through a systematic process, and analyzed at a high level. [6]" Thus, event trees can be developed by starting with a detailed diversion pathway analysis of the nuclear facility. Once all paths of diversion have been identified, results from the fault tree analysis can be applied to the event tree analysis. The entire nuclear fuel cycle facility can be systematically evaluated. Figure 2 shows a simplified example of what a safeguard's event tree for a diversion scenario could look like. The event tree shown in Figure 2 outlines all the means of detecting undeclared material movement from the initiating point to the containment boundary. For example purposes, the end states are restricted to diversion or no diversion.

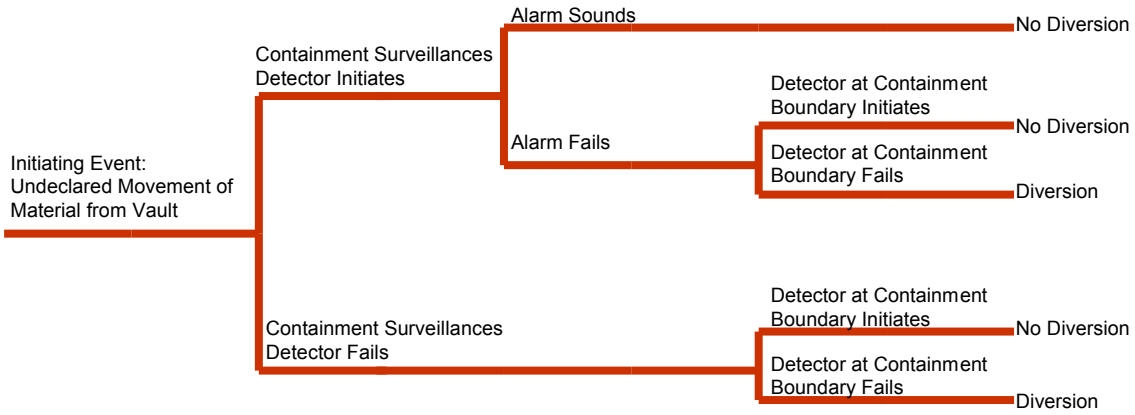

Figure 2: Sample event tree for a diversion scenario initiating in a vault storage room. The event tree is constructed from all barriers between the vault and the containment boundary. Probability failures from fault trees would be incorporated for each branch of the event tree; thus, resulting in determining the likelihood of reaching a successful diversion endpoint.

After construction and analyzing all the fault trees for a safeguards approach a quantitative result is obtained for each fault tree. The quantitative results of the fault trees populate the event trees and provide a quantitative result for each end state of the event trees. Events, which result end states with a risk higher than deemed acceptable, can be modified. For example if the risk of an undetected movement of nuclear material from a vault is deemed unacceptable, additional sensors or monitors can be utilized to decrease the risk. Furthermore, areas where the risk is found to be exceptionally low can be re-evaluated to determine cost-cutting measures. Areas where extremely low risk is calculated have most likely been over protected resulting in unnecessary cost. The use of fault and event tree analysis coupled with a cost analysis measure can optimize resources. In addition, by utilizing a well-defined methodology for safeguards, lessons learned from one facility can be applied to other facilities. Figure 3 represents an example comparison between probability of an undetected diversion and cost.

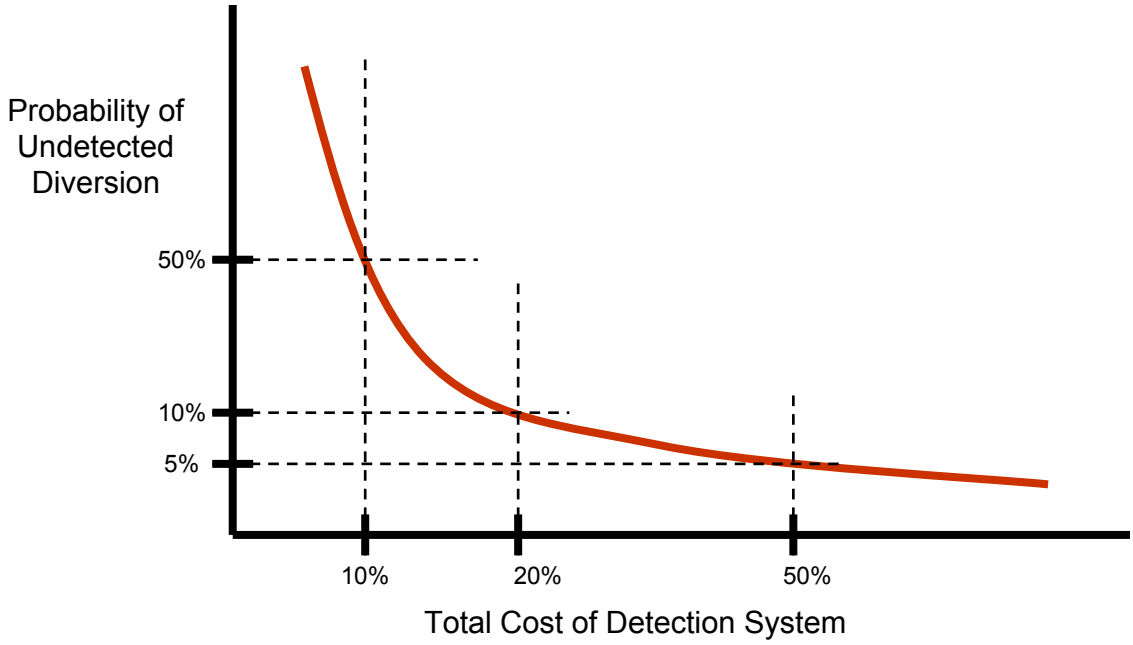

Figure 3: Sample comparison between probability that a diversion event goes undetected and the cost of the detection system.

CONCLUSION

The development of a framework for applying risk informed safeguards to nuclear fuel cycle facilities (including reactors) that is both auditable and transparent, will result in a systematic, comprehensive and methodical approach to safeguard implementations . Key aspects of this development process will include detailed system analysis, diversion pathway analysis and a review of applicable extrinsic sensors and monitors used in safeguards practices. The end result of our project will be the development a systematic, comprehensive and methodical framework to utilize risk informed safeguards for decision-making in the next generation of nuclear fuel cycle facilities.

ACKNOWLEDGEMENTS

Sandia National Laboratories is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under contract DE-AC04-94AL85000.

REFERENCES

1. NRC Policy Statement 60FR42622, 8/16/1995.
2. NRC SECY-98-144 (Letter to the Commissioners) "White Paper on Risk-Informed and Performance Based Regulation," June 1998.
3. http://www.nrc.gov/about-nrc/regulatory/rulemaking/risk informed.html "Use of Risk in Nuclear Regulation"
4. IAEA Safeguards Glossary 2001 Edition, International Nuclear Verification Series No. 3, International Atomic Energy Agency, Vienna Austria, 2002.
5. http://www.iaea.org/worldatom/Programmes/Safeguards/safeg_system.pdf "The Safeguards System of the International Atomic Energy Agency"

6. Proliferation Resistance and Physical Protection Evaluation Methodology Expert Group of the Generation IV International Forum, “Evaluation Methodology for Proliferation Resistance and Physical Protection of Generation IV Nuclear Energy Systems: Revision 5.” OECD Nuclear Energy Agency.