SAND2008-2054C

IMPLEMENTATION OF A RISK INFORMED ANALYSIS APPROACH TO OPTIMIZE SAFEGUARDS

Virginia D. Cleary
Gary E. Rochau
Sandia National Laboratories

Carmen M. Méndez
Sociotecnia Solutions

Sandia National Laboratories

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

Sociotecnia
life.systems.at.work™

Outline

- Risk Informed Decision-Making
- NRC Applications
- Applications to Safeguards
- Conclusion

Risk Informed Decision-Making

- Risk-informed decision-making uses risk insights, along with other important information, to assist in making decisions. (NRC)
- Traditionally, risk informed decision-making is primarily used by the nuclear industry to improve safety and reduce regulatory requirements.
- Risk informed decision-making is being utilized in other industries: chemical, aerospace, construction, financing and management planning.

NRC Applications

- 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.
- 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
  - what adverse events can occur,
  - what is the probability of these adverse events occurring, and
  - what are the consequences of the occurrence of an adverse event?

The Current Era of Nuclear Risk Informed Regulation

- In 1995 the NRC issued a policy statement on the “Use of Probabilistic Methods in Nuclear Regulatory Activities [1].”
  - “… 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 addition, the NRC said it expected that implementation of the policy would improve the regulatory process in three ways:
  - Incorporation of PRA insights in regulatory decisions
  - Conserving agency resources
  - Reducing unnecessary burdens on the licenses

- 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:
  - “explicitly considering a broader range of safety challenges;
  - prioritizing these challenges on the basis of risk significance, operating experience, and/or engineering judgment;
  - considering a broader range of countermeasures against these challenges;
  - explicitly identifying and quantifying uncertainties in analyses; and
  - testing the sensitivity of the results to key assumptions.”

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:
  - "…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]."
  - and "…the detection of undeclared nuclear material and activities in a state[4]"
- The IAEA is responsible for the design and implementation of a safeguards approach on all member states' civilian nuclear facilities.
- 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.

Application to Safeguards

- 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. month
  - By inference, an acceptable level of risk is the diversion of less than one SQ of material per month with a confidence level of 95%;
  - However, a lower level of risk can be utilized once defined.

Traditional PRA Practices

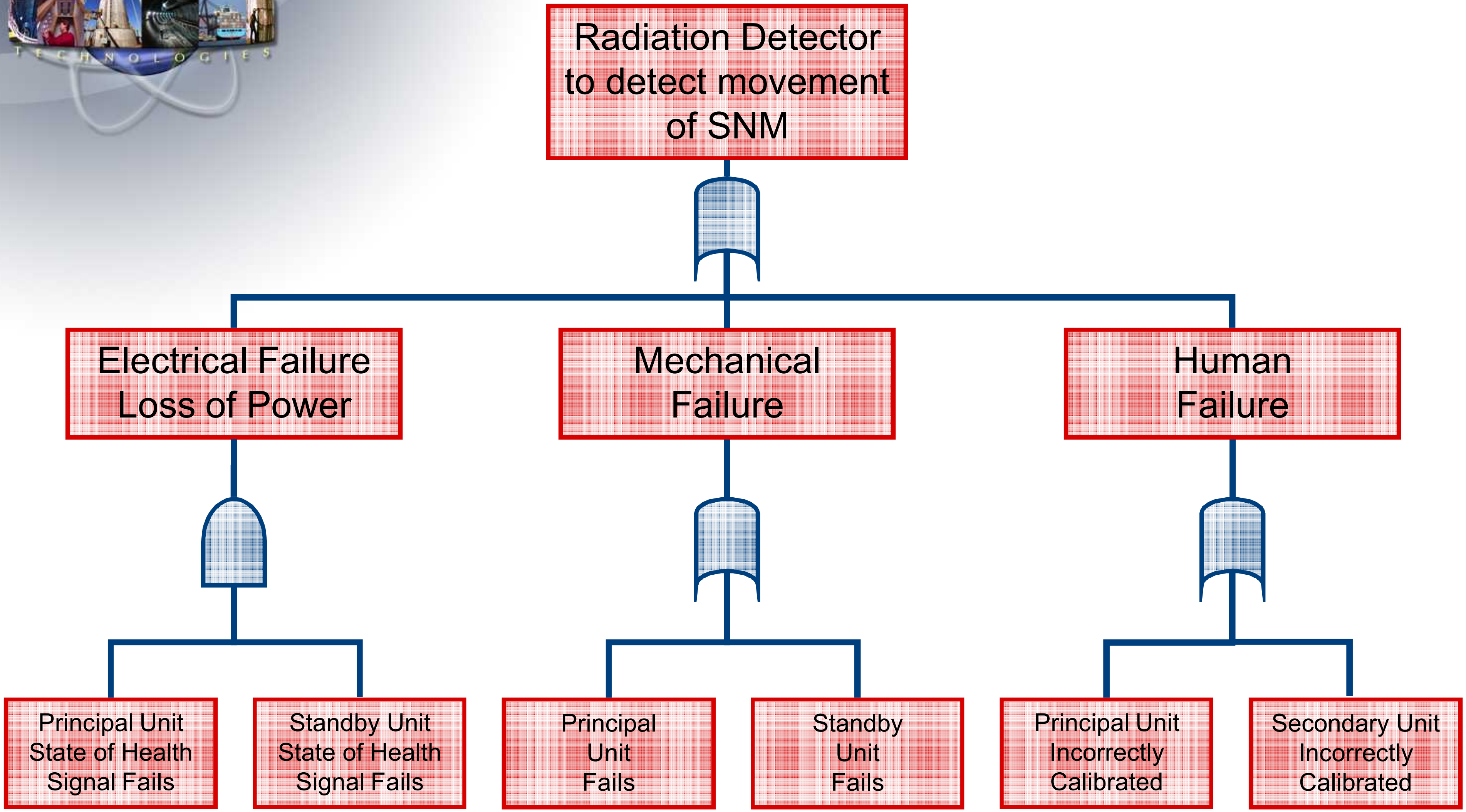
- The common methodology is the evaluation of fault trees and event trees.
- The use of fault trees and event trees provides an auditable and transparent analysis tool, which provides clear and precise documentation of not only the results but also the method of analysis.
- Fault trees use Boolean logic to analyze the various ways a component can fail.
- 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.

Application 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.

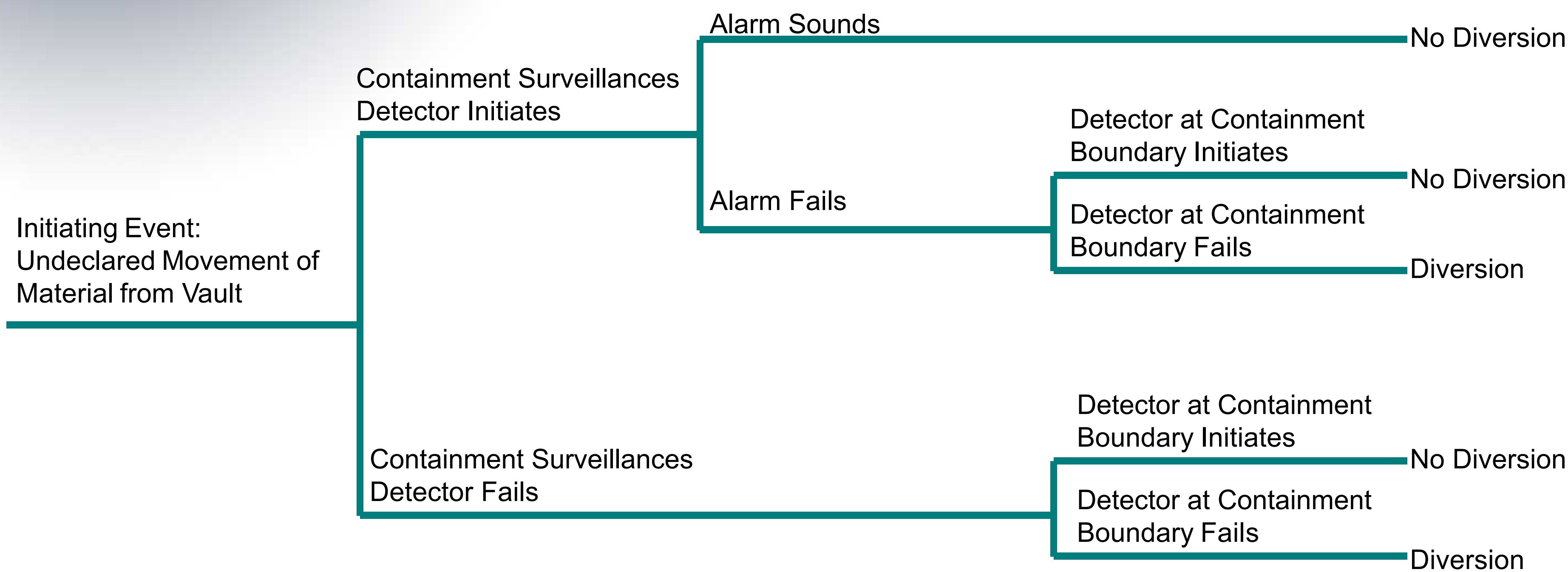
Fault Trees

- An analysis of all detectors, monitors and sensors utilized in safeguards will have to be conducted to determine their probability of failure.
- Fault trees can be constructed after all of the various failures for each detector are determined and probabilities for each type of failure calculated.


Radiation Detector to detect movement of SNM
Electrical Failure Loss of Power
Mechanical Failure
Human Failure
Principal Unit State of Health Signal Fails
Standby Unit State of Health Signal Fails
Principal Unit Fails
Standby Unit Fails
Principal Unit Incorrectly Calibrated
Secondary Unit Incorrectly Calibrated

Event Trees

- 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]"
- 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.

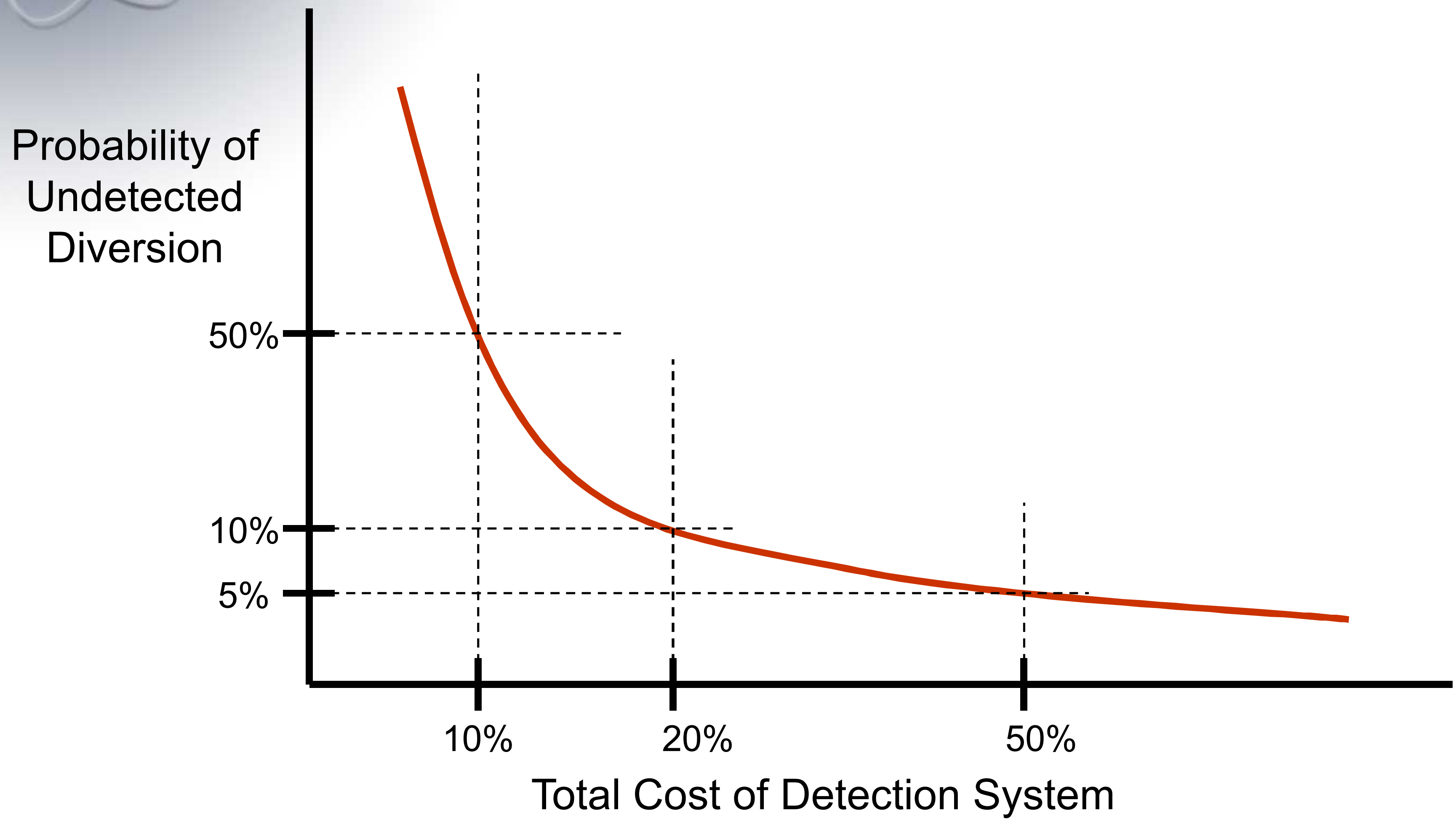

Alarm Sounds
No Diversion
Containment Surveillances Detector Initiates
Detector at Containment Boundary Initiates
No Diversion
Alarm Fails
Detector at Containment Boundary Fails
Initiating Event: Undeclared Movement of Material from Vault
Diversion
Detector at Containment Boundary Initiates
No Diversion
Containment Surveillances Detector Fails
Detector at Containment Boundary Fails
Diversion

Results of PRA

- 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.
- Events, which result end states with an extremely low risk can also be modified.
- Changes to the design, process, etc can all be updated in the analysis to determine a new risk baseline

Optimizing Resources

- 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.


Probability of Undetected Diversion
50%
10%
5%
10%
20%
50%
Total Cost of 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.