SANDIA REPORT
SAND2007-3166
Unlimited Release
Printed May 2007

Incorporation of a Risk Analysis Approach for the Nuclear Fuel Cycle Advanced Transparency Framework

Virginia D. Cleary[a], Naoko Inoue[b], Takuya Kitabata[b], Carmen M. Mendez[c], Gary E. Rochau[a], Eric D. Vugrin[a], Kay W. Vugrin[a] and David L. York[a]

Prepared by
[a]Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

[b] Japan Atomic Energy Agency
4-49 Muramatsu, Tokai-mura, Naka-gun, Ibaraki, 319-1184

[c] Sociotecnia Solutions, LLC
Weston, FL 33331

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.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from

U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.osti.gov/bridge

Available to the public from

U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd.
Springfield, VA 22161

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2007-3166
Unlimited Release
Printed May 2007

Incorporation of a Risk Analysis Approach for the Nuclear Fuel Cycle Advanced Transparency Framework

Virginia D. Cleary, Gary E. Rochau, Eric D. Vugrin, Kay W. Vugrin and David L. York
Sandia National Laboratories
P. O. Box 5800
Albuquerque, New Mexico 87185-0748

Carmen M. Méndez
Sociotecnia Solutions, LLC

Naoko Inoue, Takuya Kitabata
Japan Atomic Energy Agency

ABSTRACT

Proliferation resistance features that reduce the likelihood of diversion of nuclear materials from the civilian nuclear power fuel cycle are critical for a global nuclear future. A framework that monitors process information continuously can demonstrate the ability to resist proliferation by measuring and reducing diversion risk, thus ensuring the legitimate use of the nuclear fuel cycle. The automation of new nuclear facilities requiring minimal manual operation makes this possible by generating instantaneous system state data that can be used to track and measure the status of the process and material at any given time.

Sandia National Laboratories (SNL) and the Japan Atomic Energy Agency (JAEA) are working in cooperation to develop an advanced transparency framework capable of assessing diversion risk in support of overall plant transparency. The "diversion risk" quantifies the probability and consequence of a host nation diverting nuclear materials from a civilian fuel cycle facility. This document introduces the details of the diversion risk quantification approach to be demonstrated in the fuel handling training model of the MONJU Fast Reactor.

ACKNOWLEDGEMENTS

The authors thank Tom Kirchner and Mitsutoshi Suzuki for providing valuable background on probability theory for the diversion risk model.

CONTENTS

TABLES

FIGURES

1.0 INTRODUCTION

A key objective to the global deployment of nuclear technology is maintaining transparency among nation-states and international communities to assure the safe and legitimate use of nuclear material and related technology. Proliferation resistance features that prevent theft or diversion of nuclear material and reduce the probability of proliferation are critical for a global nuclear future.

The automation of new nuclear facilities requiring minimal manual operation provides an opportunity to utilize the abundance of process information for monitoring proliferation risk. A framework that monitors process information continuously can lead to greater transparency of nuclear fuel cycle activities and can demonstrate the ability to resist proliferation associated with these activities.

Proliferation occurs in three stages: materials acquisition (with a focus on what occurs at the facility), materials transformation, and weapons fabrication. For the purpose of this document, diversion is defined as the process through which a host nation diverts fissile material from a declared fuel cycle facility with the intention of generating nuclear weapons; it refers only to the acquisition of nuclear materials. Facility misuse (undeclared production) is not taken into account in this document and is beyond the scope of the current project. Threats of acquisition of nuclear materials from a declared facility not conducted by the host nation are considered theft. Although the technology framework described in this document is designed to collect and analyze the facility data and should be capable of detecting undeclared movement of material regardless of who is the originator (i.e., host country or other groups), theft threats are not considered within the scope of this project.

Sandia National Laboratories and the Japan Atomic Energy Agency are working in cooperation to develop an advanced transparency framework capable of assessing proliferation or diversion risk in support of overall nuclear plant transparency. Within this framework, diversions of material from the facility can be detected as they occur. For demonstration purposes, we are calculating risk of diversion at a MONJU-style Fast Breeder Reactor.

The term "transparency" is used in many different applications. In the context of the nuclear fuel cycle, we define it as:

> "…a high-level concept, defined as a confidence building approach among political entities, possibly in support of multi-lateral agreements, to ensure civilian nuclear facilities are not being used for the development of nuclear weapons. Additionally, nuclear fuel cycle transparency involves the cooperative sharing of relevant nuclear material, process, and facility information among all authorized parties to ensure the *safe and legitimate use* of nuclear material and technology. A system is considered *transparent* when the parties involved feel that the *proliferation risk* is at an acceptable level. For this to occur, proliferation risk should be monitored in a continuous fashion." (Love et al., 2006)

Nuclear Fuel Cycle Transparency can be further categorized into four accumulating levels:

1. Bilateral or multilateral agreements on the operation, inspection, and verification of nuclear operations within a host country.
2. Added surveillance and remote monitoring of nuclear operations usually at random or without notification.
3. Direct monitoring of nuclear operations instantaneously.
4. Ability to remotely secure and inhibit operations.

The highest levels of transparency imply multilateral control of nuclear facilities and processes. This project represents the first attempt to implement a Level 3 Transparency System at any location, whether foreign or domestic. The present report introduces a methodology for analyzing the data obtained from a directly monitored advanced transparency system and their integration into the calculation of diversion risk for plant operations.

For a background and a holistic understanding of the project scope and goals, please refer to the conceptual framework of this methodology, documented in *SAND2006-0270: A Framework and Methodology for Nuclear Fuel Cycle Transparency (Love et al., 2006).* An extension of these transparency concepts is discussed in the above referenced document.

2.0 TRANSPARENCY FRAMEWORK: REVIEW AND DEFINITIONS

The Advanced Transparency Framework is comprised by secure technologies to be found in two different locations: (1) the host nuclear facility generating the information and (2) the remote site analyzing the data. Data is collected from the nuclear facility by a secure sensor signal database server located at the host facility. The data is then encrypted and transmitted through a Virtual Private Network (VPN) to the sensor signal database located at the remote site. The remote site hosts the Transparency Toolbox and the Transparency Analysis Software, which contain the core functionality for evaluating the signals, calculating the diversion risk and developing recommendations to support transparency of the facility.

The goal of the analysis is to assess the diversion risk instantaneously via analysis of continuously reported sensor information. Following the analysis, the values obtained can be used to recommend changes to reduce diversion risk and provide feedback to the site and other authorized parties. The framework is designed to monitor diversion risk levels in support of an acceptable level of proliferation risk. Figure 1 displays the framework of advanced nuclear fuel cycle transparency.

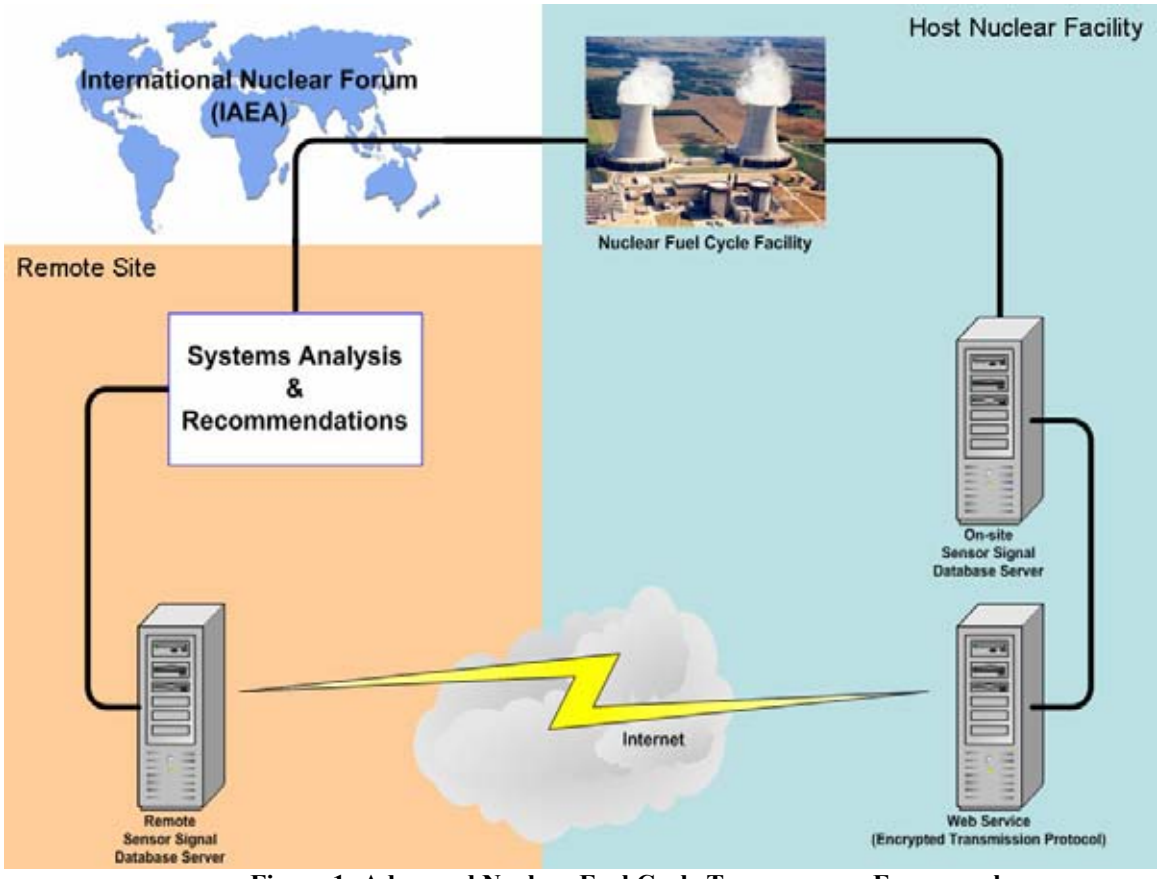

Figure 1: Advanced Nuclear Fuel Cycle Transparency Framework

In order to better understand the risk analysis model in context of this transparency framework, several definitions are required.

Proliferation Risk: Proliferation risk is often defined as the risk of acquisition, transformation and weapons fabrication. For the purpose of this document, "proliferation risk" is the risk that a facility can be used for proliferation by the host country. This risk is assumed to be an acceptable risk when the facility operates under normal conditions as declared by licensing and export control agreements.

Diversion Risk: The "diversion risk" is the risk of diverting nuclear material through the declared operations. This concept incorporates both the probability of a host nation diverting nuclear materials from a commercial facility and the consequences of such a diversion. Diversion risk is quantified, herein, in terms of significant quantities (SQs) of nuclear material potentially diverted within a specific period of time or cycle measurement (day, month, operation, process). For the purpose of this document, diversion risk will be calculated instantaneously (real-time) from process data.

Transparency Database1 (webservice): The Transparency Database1/webservice stores information collected from the Monju Model and provides a communication protocol for transferring that data to the Transparency Toolbox. The database consists of XML formatted sensor signal files collected during activity of the model. The webservice operates as a client-server system allowing data transfer queries to pass through SOAP communication protocol. The data is encrypted at the server, located at the site of the facility, and transferred to the client, or remote site making the query request, where the information is decrypted. This information is transferred through a Virtual Private Network (VPN).

Secure communications: During the information transfer process, encryption algorithms are provided to encrypt or scramble information being requested from the remote site, or client of the webservice.

Transparency Database2: After information is transferred from the Server to the Client, an XML Controller parses through the information and populates the Transparency Database2 into the proper format for use in an analysis. The database consists of the primary data coming from the model and secondary data identifying specific attributes about each signal.

Transparency Toolbox: The Transparency Toolbox is the main Graphical User Interface (GUI) at the remote site. The Toolbox is used to display information transferred via the webservice. The minute amount of processing at the Toolbox level involves time constraints and signal order-of-operation evaluations. For instance, if a sensor is activated outside of a particular time constraint, or if a sensor is activated out of order, an error indicator is activated with an error description at the Transparency Toolbox level.

Transparency Software: The Transparency Analysis Software conducts the operational verification and calculates the proliferation risk of a nuclear facility. The software incorporates analysis tools in the form of a risk model to quantitatively evaluate the process data, using information from the Transparency Toolbox to calculate the expected and observed risk parameters. The continuous stream of information provided by the software will yield a timely proliferation assessment. This analysis is necessary to design, support, and maintain transparent systems.

Plant Process and Plant/Operational Process Data: "Plant process" refers to the collection of physical events that take place during normal plant operations. An example is using a crane to move material from one location to another. The term "plant process data" or "operational process data" is used to represent operational data normally generated by the plant independent of any advanced transparency requirements or efforts. A basic assumption in the development of the transparency framework is that the plant process is automated and that the abundance of plant process data generated during operations is immediately available for analysis. (We assume, for this study, that plant data is secure and tamper resistant.)

Process Flow: "Process flow" refers to the movement, activity, or any processes associated with the nuclear material in the fuel handling cycle at a specific facility. Process flow information is crucial for the analysis because it provides the foundation for the development of expected signals from the facility, based on a facility activity manifest. This information is well defined, structured, organized, and placed into the secure facility database. Implementation of the transparency framework at any location requires examining process flow information for each nuclear facility type on a plant-wide basis. This specificity and flexibility of the framework allows for ease of implementation in all aspects of the nuclear fuel cycle.

Sensors and Monitors: Sensors and monitors convey specific information about the operational processes of the facility. A "sensor" detects the status of the various conditions of the plant, whether it is temperature, motion, position, et cetera, and does not require interpretation. A sensor can provide either binary information (e.g., on/off) or analog information (e.g., temperature).

There are two types of sensors: intrinsic and extrinsic. An "intrinsic sensor" is a sensor that transmits signals inherent to the system (for example, identifies the binary plant process events by following voltage during plant operations) and generates what was previously defined as "plant process data." The information gathered by the intrinsic sensors is part of the existing operation system, without transparency in place.

An "extrinsic sensor" is an added sensor that is not needed for plant operations and monitors material properties such as mass, temperature, et cetera, which may be needed to calculate the diversion risk. This sensor is added to the system solely for advanced transparency measurements as an additional verification device to manage the risk. Extrinsic sensors are not currently incorporated into the risk model, as diversion risk will be first calculated with information intrinsic to the facility. In the future, the location of extrinsic sensors should be determined to further support the calculation of diversion.

A "monitor" is a data-gathering tool that is also added to the system for transparency purposes. However, in contrast to extrinsic sensors, information transmitted by monitors is subject to interpretation by the analyst. Monitors, such as video cameras and inspectors, allow the analyst to observe an operation. Monitors are not currently incorporated into the risk model, as diversion risk will be first calculated with information intrinsic to the facility. In the future, the location of monitors should be determined to further support the calculation of diversion risk.

Significant Quantity: A "significant quantity" (SQ) of a specific material is the minimum amount of that material needed to develop a nuclear weapon. This measurement presents a means for addressing the material attractiveness or quality of a specific fissile isotope and will be used in the development of a quantitative risk approach as a measure of the consequence of successful diversion.

3.0 PLANT DESIGN AND SENSOR USAGE

Plant design has a significant impact on the risk modeling process and the calculation of diversion risk for a specific facility. Once the required plant operations are detailed in a process flow diagram, sensor placement must be addressed. Every plant operation is assumed to have as many associated sensors as are necessary to (1) verify that the remote operation took place and (2) provide feedback to the associated automation systems. These intrinsic sensors will verify movement of plant equipment and yield data in a binary form (i.e., operating or not operating). The length of time between readings and sequence of operations of intrinsic sensors will be part of the process flow diagram and will also be collected as input to the transparency toolbox.

4.0 RISK MODEL

It has previously been stated by Love et al. (2006) that proliferation risk, and ultimately fuel cycle transparency, is a function of material attractiveness, a static (baseline) risk, and a dynamic (changing) risk. For simplicity and comprehensiveness, we will now redefine the terminology proposed in that document.

The calculation of proliferation risk from a process step is assumed to be directly related to the risk of a host nation diverting material from the process. Hereafter, the risk model addresses this specific calculation as diversion risk.

A fundamental component of the "diversion risk model" is the comparison of "expectations" and "observations." Declared plant operations have an expected sequence of events, and when these events are conducted in the expected manner, a set of signals are generated for these events by the sensors. This set of signals is referred to herein as the set of expectations or expected signals. The expectations are based on the detailed process flow, declared operations, and diversion routes. Expectations account for the diversion risk under normal operations. The observations are the set of sensor signals recorded by the same monitoring sensors during actual operations at the facility.

An instantaneous comparison between expectations and observations provides the foundation for the calculation of diversion risk. A deviation from expectations (a discrepancy between expected and observed signals) represents an opportunity for diversion of radioactive materials. When a deviation occurs, the transparency system detects the discrepancy and adjusts the risk calculation according to the model proposed in this document.

This document defines diversion as the action of "diverting nuclear material through the declared operations," whereas deviation is solely a "discrepancy between expected and observed signals" as detected by the sensors. Deviations are specific and limited to the information generated by the sensors and can occur under several circumstances, such as an unexpected time delay in the process or a sensor malfunction. A deviation is a flag to indicate that diversion might be occurring; it is not an indicator of diversion certainty. However, although sensor failures and time delays can be considered within the normal range of automated systems events, they are anomalies in the declared process and can increase the chances of successful diversion (e.g., a sensor that malfunctions would not detect a diversion, a time delay provides opportunity for manipulating the automated system). For this reason, all detected deviations will trigger an adjustment in the diversion risk calculation that will likely increase the diversion risk for that operation.

The "diversion risk model" introduced in this document considers two types of risk: expected and observed risk. We suggest that the concepts of "static" and "dynamic" risk that were discussed in Love et al. (2006) are instead "expected" and "observed" risk. These concepts are further developed in Sections 4.1 and 4.2. We outline the diversion risk model in the following subsections.

4.1 Expected Risk

The "expected risk" is the risk introduced by the existence of the facility based on planned and declared operations. This risk represents the normal baseline risk and is dependent upon plant design and processing capabilities. The plant design should have the goal of making this amount as small as possible. All planned activities from a facility are communicated to the risk analysts before operations begin. Risk analysts use this information to develop a set of "expected signals" that will be generated by the model prior to the execution of declared operations.

While the expected risk can never be equal to zero, due to uncertainties and the possibility of overlooking possible routes for diversion during the design of the plant, a careful and comprehensive plant design will minimize this risk. The value of expected risk will be expressed in terms of the rate of significant quantities per unit of time or process (e.g., SQs/process) and represents the amount of material that may be diverted without detection over a predetermined amount of time or during the completion of a specific process. The expected risk is calculated for individual process steps based on the technologies, sensors, and plant design, including considerations for materials type and event consequences. The plant expected risk will be calculated by aggregating the calculated expected risk at every plant step, including transition points from one-step to another.

4.2 Observed Risk

The "observed risk" is measured instantaneously when the plant is operating and is based on the signals transmitted by sensors during the completion of declared operations. Observed risk is calculated at every process step via a comparison of actual operations to planned and declared operations (the foundation for expected risk). Real-time raw data from sensors is aggregated in the transparency toolbox to detect deviations. A baseline risk file containing the calculated expected risk based on declared operations will be compared to an alternate working file being fed by real-time process data, evaluating the status of the sensors according to estimated operation times and predicted timetags. This information is transmitted to the risk analysis software where a value of observed risk for each process step is calculated. The observed risk will accumulate over the same span of time as the expected risk.

4.3 Expectations and Observations

The Advanced Transparency Framework assumes that all planned operations from a facility are communicated to the risk analysts before they begin. These declarations are used to develop a set of "expectations" or "expected signals" that represent what the facility sensors should transmit if the operation goes according to plan, without any deviation. During operations, expectations are the binary status [on/off] expected from each sensor according to the declaration. "Observations" or "observed signals" are the binary status [on/off] signals actually transmitted by sensors while operations are taking place.

When the information is being transmitted, the risk analysis software performs a comparison between the expectations and observations to determine if they match. The software then determines if the operation has occurred as expected (expected = observed) or if a deviation has been reported (expected ≠ observed).

4.4 Components of Risk

For the purposes of this document, the risk of an event occurring has two components: the probability that the event will happen and the consequences of such an event if it did occur. The risk is calculated by taking the product of the probability and the consequence. The diversion risk model presented herein assesses the probability that a diversion has occurred by interpreting the set of observed signals for an operation. For simplicity in the risk calculation, we will utilize a "significant quantity" (SQ) as the measure of consequence. Diversion risk will be based on the fraction or total number of SQs that may be diverted from the facility within a specified timeframe or process.

4.4.1 Probability

The diversion risk model compares the set of observed signals with the expected signals to calculate the probability component of the diversion risk. This section discusses the concepts used to estimate the probability that a diversion has occurred (P), conditional on the observed sensor data. Because this probability calculation is dependent upon the sensor data, it is a conditional probability. For the sake of brevity, later uses of the term "probability that a diversion has occurred, conditional on sensor data" will omit the phrase "conditional on sensor data."

The risk model presented herein assumes that each process step has as many associated sensors as are necessary to verify that the remote operation took place. This assumption leads to the following set of four scenarios for a single process step:

Scenario 1: If no diversion occurs and the sensor is functioning correctly (i.e., no malfunction), the sensor will not report a deviation from expected operations.

Scenario 2: If a diversion occurs and the sensor functions correctly, the sensor will report a deviation from expected operations.

Scenario 3: If no diversion occurs but the sensor malfunctions, the sensor will report a deviation from expected operations. This scenario is termed a "false positive."

Scenario 4: When a diversion occurs but the sensor malfunctions, the sensor will not report a deviation from expected operations. This scenario is termed a "miss" and represents why the diversion risk is not equal to zero even if a sensor does not report a deviation from expected operations.

Figure 2 illustrates these scenarios.

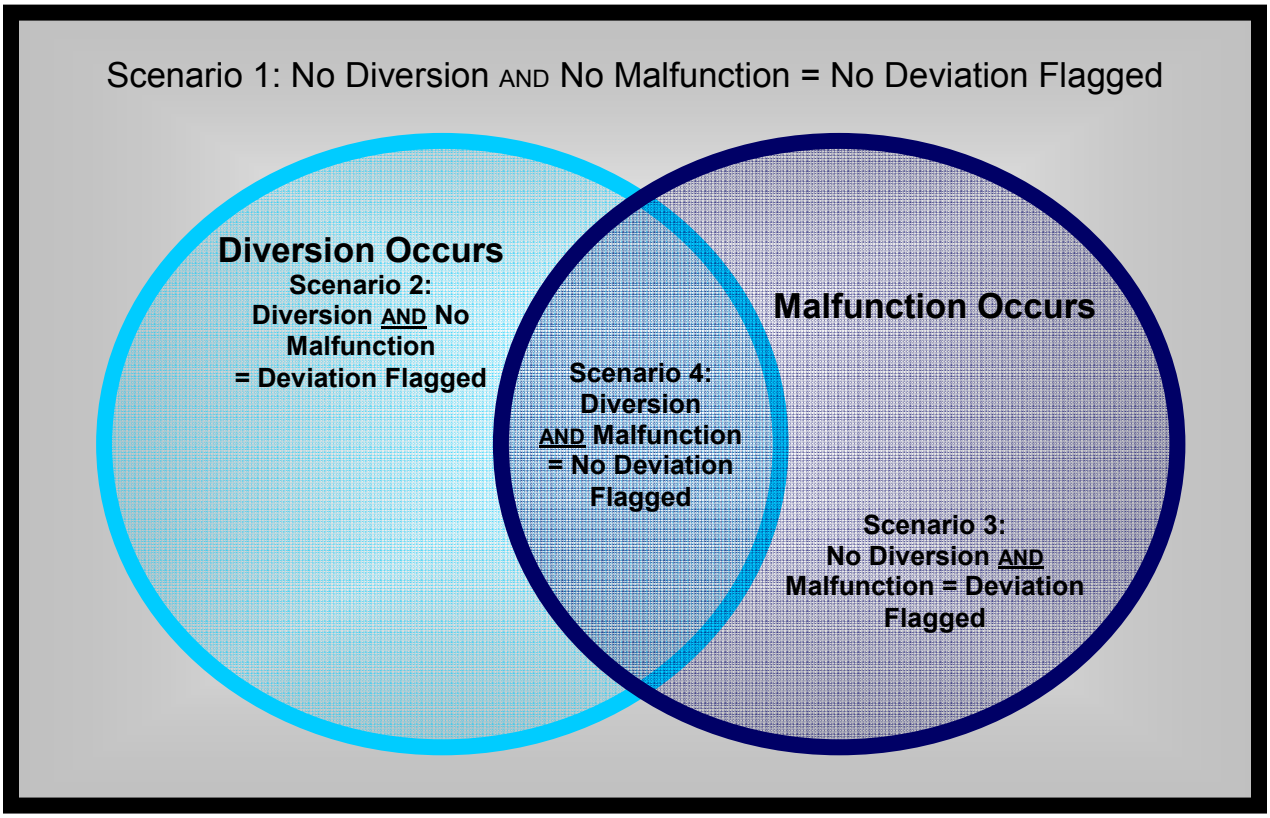

Figure 2: Sensor Malfunction and Diversion Scenarios

The model used to calculate the probability that a diversion has occurred, *P*, for an individual process step involves two factors: 1) the probability that a diversion will occur during that step (*PD*) and 2) the probability that the sensor monitoring that process step will malfunction and report incorrect data (*PM*). Appendix A provides the mathematical details of how these probabilities are used to calculate *P*.

Several factors such as design, location/environment, and function impact the frequency of sensor malfunction. These factors have not been evaluated yet for the MONJU facility, so the method for calculating *PM* is not discussed in this document. However, it should be noted that the sensors used in this calculation are intrinsic to the plant and are required to successfully operate the plant; the reliability of these sensors is extremely high. Thus, it is expected that *PM* will be exceedingly low. This is because plant equipment will be designed with reliability as a primary concern. In addition, most of the equipment will have state of health signals that will indicate the likely failure of any equipment.

The method of calculating *PD* for a process step has not been fully matured, but several contributing factors have been identified. They include the location of the process step, the attractiveness of the materials being processed, and situational factors.

The location at which diversion begins must be considered when determining the possibility of diversion. It takes into account the ease of diverting material out of the facility given a starting point. It considers the physical barriers to removal of the diverted material: thus, the less physical barriers to exiting the facility the higher the location factor and the more physical barriers, the lower the location factor.

Material attractiveness considers the usefulness of a material to a potential diverter, thus the term attractiveness. It considers why a diverter would be more inclined to take a material with a small quantity of high purity plutonium over a larger quantity of lesser quality plutonium. Thus, it considers the last two components of proliferation: processing and fabrication.

A situation factor is used to supply a weighting factor for the probability of diversion. A series of questions are asked, and depending on the answer, a weighting factor is considered. For example, if a deviation in the process is reported, the first question asked is "Is material present in the room." If the answer is no a weighting factor of one is applied to indicate there is no change in the probability of diversion. However, if the answer is yes, the questions are continued until a weighting factor is assigned. The purpose of these questions is to assess the situations occurring at the reactor and determine if the situations affect the probability of diversion.

Figure 3 summarizes the questions to be asked and corresponding weighting factors to assess material accessibility based on the situation.

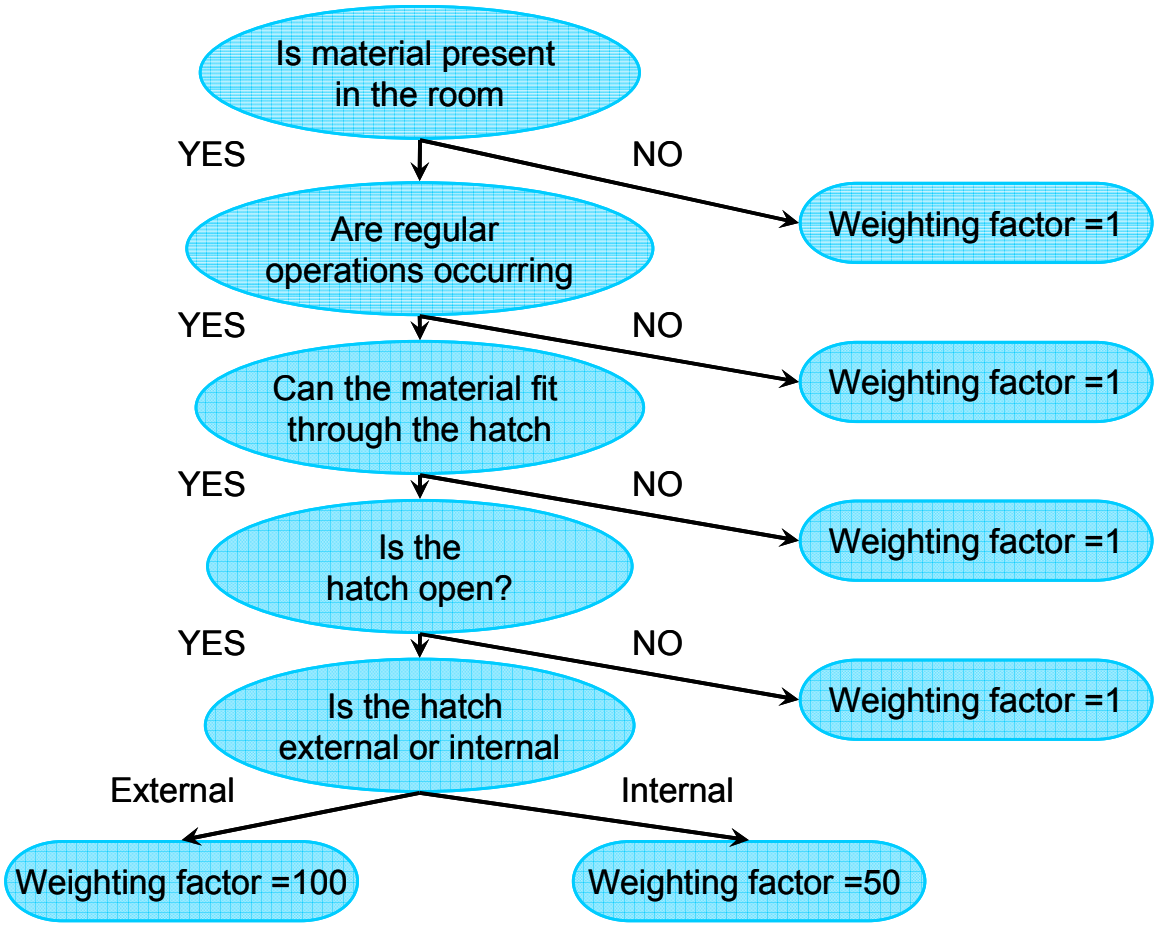

Figure 3: Questions and Weighting Factors to Assess Material Accessibility Based on Situational Factors

The locations, materials, and situational factors were qualitatively assessed, and a numerical weighting factor was assigned to each of these factors. These numerical values will be used to scale the base rate of diversion to develop PD for a process step. Table 1 lists the various locations in the MONJU plant in which process steps occur, and a proposed numerical quantification of these locations is given. Table 2 provides the material classes for MONJU and their proposed corresponding material attractiveness values. These tables were developed so that higher values indicate greater ease of diversion and greater attractiveness level, respectively.

Table 1: Locations of Process Steps in the MONJU Facility and Their Ease of Diversion Values

Location*	Ease of Diversion
Reactor Building	0⬩
Reactor Vessel	1
Fuel Handling Machine	1
In-vessel Transfer Machine	1
EVST	1
EVTM	10
Underwater Transporter	10
Underfloor Transporter	20
Spent Fuel Inspection	20
Spent Fuel Cleaning System	20
Spent Fuel Canning Station	20
PIE Cask Pit	50
Fresh Fuel Handling Room	90
Shipping Cask Receiving and Shipping Station	100

* Location is defined as an initiating point to begin diversion

⬩ Reactor Building is not an initiating point for diversion

Table 2: Material Classes for the MONJU Facility and Their Attractiveness Levels

Material Class	Attractiveness Level	Material Description
Irradiated Blanket Material	100	anything greater than 10 full operational days
Fresh fuel	10	anything with a burnup less than 40MW
Spent Fuel	5	material with a burnup equal to or greater than 40MW
Blanket Material	1	depleted uranium
Control Rods	1	boron control rods
Instrumentation Tubes	1	neutron detectors, etc

4.4.2 Consequence

For the purposes of this document, the consequence of diversion will be measured in terms of Significant Quantities (SQs). SQs are defined by the International Atomic Energy Agency (IAEA) as the mass needed to manufacture a nuclear weapon. Table 3 is a proposed relationship of items to SQs. The information in this table will likely evolve with time as more information becomes available.

Table 3: SQ Consequence Measures Associated with Specific Items

Item	# SQ/Item
Control Rods & Instrumentation Tubes	0.0
Fresh Blanket Assembly	0.0
Spent Reactor Fuel Assembly	0.2
Fresh Reactor Fuel Assembly	0.6
Irradiated Blanket Assembly	0.6

4.5 Risk Calculations

The diversion risk for an individual process step is the product of the probability that a diversion has taken place during that step and the consequences (in SQs) of a diversion occurring during that step. To calculate the diversion risk of a process that is comprised of individual process steps, the risks for the individual steps are aggregated. The diversion risk for the entire plant operation can be assessed by totaling the risks for the individual steps and processes. Figure 4 illustrates the risk hierarchy for a hypothetical plant operation consisting of three processes.

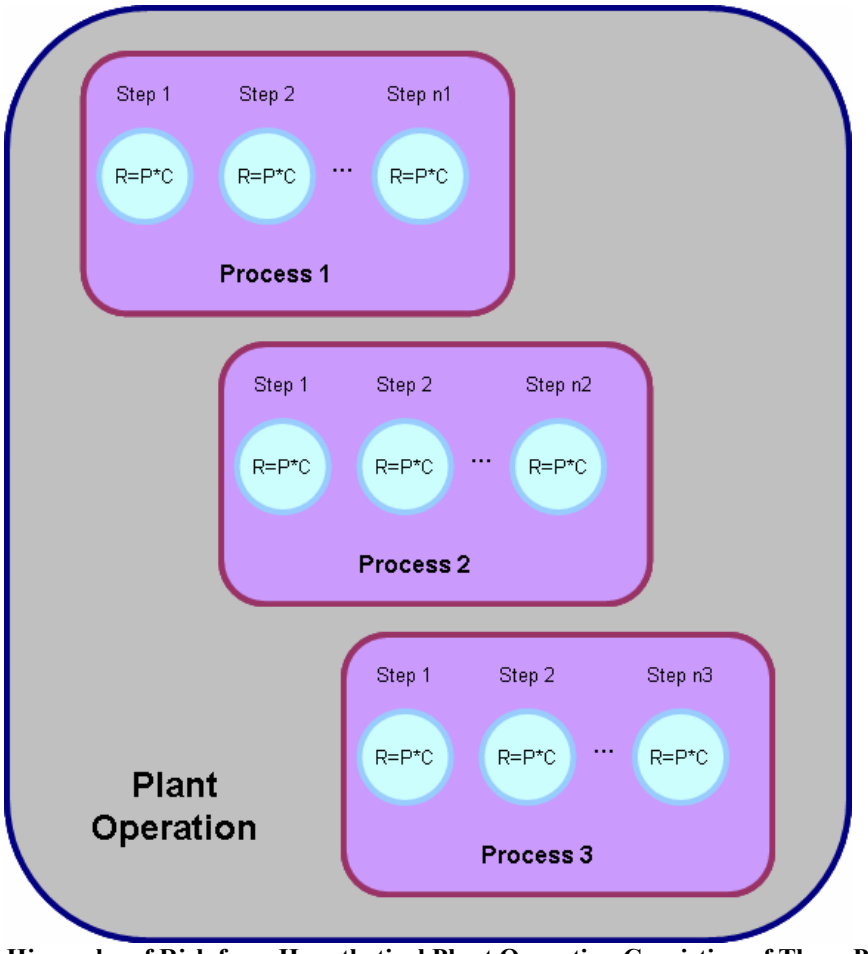

Figure 4: Hierarchy of Risk for a Hypothetical Plant Operation Consisting of Three Processes

4.6 Format of Reported Data

The numerical values reported by the transparency software will either be 1) the difference between the expected diversion risk and the observed diversion risk when point probabilities are used to model *PM* and *PD* or 2) the difference between the mean expected diversion risk and the mean observed diversion risk and the uncertainty associated with this difference when probability distributions are used to model *PM* and *PD*.

See Appendix A for a discussion of when PM and PD should be modeled with a point probability or probability distribution.

See Appendix B for a demonstration of how the risk model can be applicable to a MONJU-Style Fast Reactor based on the types of signals and information that is collected by the automated process.

5.0 FUTURE WORK

5.1 Extrinsic Sensor and Monitor Placement

An actual application of the advanced transparency system at a facility will also include extrinsic sensor placement. Extrinsic sensors will be designed to measure material quantity either directly or indirectly. The process flow diagram will be analyzed to identify locations where extrinsic sensors may be needed. The extrinsic sensors will be used to verify the amount and type of material at strategic points within the facility, including storage rooms and receiving areas.

5.2 Process Deviations and Their Effect on the Risk Calculation

When deviations from expected process steps are detected, the model will incorporate the evaluation of correlations between intrinsic sensors. The correlation between intrinsic sensors will rely on analyzing signal order and time relationships to determine if a deviation in the declared operation has actually occurred. In addition, future work may involve the use of supplemental extrinsic sensors and monitors to verify declared operations versus observed operations in the event that a deviation in process steps was reported. For example, if an intrinsic sensor detects an anomaly and sensor signal order cannot verify that no deviation has occurred, an extrinsic monitor or sensor may be able to determine whether the anomaly was triggered by equipment malfunction, safety override, or other circumstances. The extrinsic sensors and monitors will also make it possible to verify if the material is still in the system, or if a diversion occurred. This system of balance and checks will allow the risk analyst to make informed decisions when an increase in diversion risk is observed and will eliminate unnecessary interruptions of operations in the event that a deviation occurred but no diversion was verified by intrinsic signal order and time, extrinsic monitors, or extrinsic sensors.

5.3 Signal Optimization

The number of signals received for operations at a plant is large. The massive amounts of data received for even small processes can bog down the transparency software. It will be necessary to rank signal importance to minimize the number of signals that must be analyzed to sufficiently determine the diversion risk. Signals with a high importance will primarily make up the data used in the risk calculation; whereas, signals with a medium or low ranking will be used as supplemental data that can be used when needed to ensure the accuracy of the risk calculation. A diversion pathway analysis will be completed to identify areas where signals have a greater importance.

5.4 Diversion Pathway Analysis

A diversion pathway analysis will identify areas where material can be removed from the system and the pathway a diverter must follow to remove the material from the plant. Areas that are identified as having a direct exit pathway would have a higher importance, and would potentially be areas where extrinsic sensors and monitors could be used to reduce diversion risk. For areas that do not have a direct exit, the path the divertor must follow to leave the plant should be identified. Extrinsic sensors and monitors could be installed along the possible diversion pathways to provide a surveillance method to detect material movement. If material is found to be moving along a diversion pathway, the diversion risk would immediately indicate to the analysts that inspectors and regulators should be notified. The transparency software would be

able to follow the movement of material along the diversion pathway and identify areas where inspectors should look to find the diverted material.

5.5 Development of PM and PD

The methods for calculating the probability of sensor failure (PM) and the probability that a diversion will occur at a process step (PD) have not been fully matured. These calculations will be developed for implementation in the transparency software.

5.6 Additional Risk Considerations

The risk analysis framework is being developed for evaluating proliferation risk as a basis of any nuclear fuel cycle independent of country, political sensitivities and other factors that may be considered relevant for a comprehensive evaluation of the risk environment. Such considerations may later be included in the model in a customized module that may allow the risk analyst to increase or decrease diversion risk as necessary based on other factors that would affect the probability of diversion.

6.0 CONCLUSIONS/PROGRESS

The natural progression of the transparency framework suggests that the development and demonstration of qualitative and quantitative risk analysis methods should be preceded by a demonstration of the secure communications and data transfer from the two sites involved in the analysis. A demonstration of secure communications between the location generating the data and the location analyzing it will guarantee the integrity of the data in support of neglecting the risk associated from remote communications and data interference from the calculation of proliferation risk.

Once secure communications are established, a demonstration of the quantitative risk concept and its qualitative interpretation can be documented for specific operations of the fuel cycle. These operations will later be integrated into a demonstration of the total fuel cycle proliferation risk concept.

7.0 REFERENCES

Love, T., McClellan, Y., Rochau, G., York, D., and Inoue, N. (2006) "A Framework and Methodology for Nuclear Fuel Cycle Transparency." Sandia National Laboratories, Albuquerque, NM. SAND2006-0270.

Related Presentations

Mendez, C., Rochau, G., York, D., Inoue, N., "A Demonstration of Nuclear Fuel Cycle Transparency", Proceedings 47th INMM Annual Meeting, July 2006.

Rochau, G., Mendez, C., York, D. "Advanced Remote Monitoring for Reprocessing Systems", Proceedings 47th INMM Annual Meeting, July 2006.

APPENDIX A: MATHEMATICAL DETAILS FOR THE DIVERSION RISK MODEL

For the purposes of this document, the risk of an event is the product of the probability of the occurrence of the event and the consequences of such an event. This appendix provides the mathematical model for the calculation of the probability component of diversion risk.

A.1 Risk Notation

The process step level is the basic level at which risk is calculated in the risk model. The diversion risk from individual steps can be accumulated to report a risk for an individual plant process or for plant operations. However, the following discussion of risk will focus on calculating risk at the process step level.

The diversion risk for a specific process step is calculated as the product of the probability of diversion of nuclear materials during that step and the consequences of that diversion:

$$R_{i,j,k} = P_{i,j,k} \times C_{i,j,k}$$

$R_{i,j,k}$ denotes the risk of diversion for the i^{th} step of the j^{th} process of the k^{th} plant operation. For the same step, process, and operation combination, $P_{i,j,k}$ denotes the conditional probability that a diversion has occurred, given the data reported by the sensors for that step (see Section 4.4.1). The term $C_{i,j,k}$ denotes the consequence for the same step, process, and plant combination.

A.2 Inputs to the Probability Model

As discussed in Section 4.4.1, the diversion risk model assumes that every process step is assumed to have as many associated sensors as are necessary to verify that the remote operation took place. Under this assumption, the probability of diversion for a specific process step can be calculated. The fundamental question that the probability model answers is as follows:

> *Given the data reported by the sensors, what is the probability that nuclear materials have been diverted from a single process step?*

That is, we need to calculate the probability that a diversion has occurred, conditional upon the data reported by the sensors for a single step. To do so, the probability model requires three sets of inputs:

1. S_h: the result from comparing the expected signal and the observed signal of the h^{th} intrinsic sensor associated with a process step. When $S_h = 0$, the observed signal matches the expected signal, and no deviation is logged by the transparency software. When $S_h = 1$, the observed signal does not match the expected signal, and the transparency software logs a deviation from expected operations.
2. PD: the probability that a diversion will occur at the process step. This probability is a function of several factors and is discussed in Section 4.4.1.
3. PM_h: the probability that the h^{th} sensor will malfunction. This probability is also described in Section 4.4.1.

The two events (diversion and sensor malfunction) are assumed to be independent in all risk calculations. If PD and PM_h are known with precision, they can be taken to be point probabilities. If it is necessary to incorporate uncertainty in these probabilities, they can be

considered random variables that have associated probability distributions. The probability model has been developed so that either approach can be used.

A.3 Background Results

Before detailing the probability calculations, it is necessary to state a theorem and lemma that are used in the calculations. The diversion risk model requires the conditional probability that a diversion has occurred, given the data reported by the sensors (Section 4.4.1). Consequently, the following results involve the calculation of conditional probabilities.

Theorem 1 (Bayes' Theorem; Bayes 1764)[†]: *If* $B_1, B_2, \ldots, B_k$ *constitute a partition of the sample space* U *and* $P(B_i) \neq 0$ *for* $i = 1, 2, \ldots, k$, *then for any event* A *in* U *such that* $P(A) \neq 0$

$$P(B_r \mid A) = \frac{P(B_r)P(A \mid B_r)}{\sum_{i=1}^{k} P(B_i)P(A \mid B_i)}.$$

Lemma 1[‡]: *If A, B, and C are independent events and* $P(C) \neq 0$, *then*

$$P(A \cap B \mid C) = P(A \mid C)P(B \mid C).$$

These results are used in the development of the probability model.

A.4 Probability Calculation: Single Sensor

Consider the example of a single process step that is monitored by a single sensor. In this example, it is assumed that *PD* and *PM* are known with precision, and we model them as point probabilities. We omit the subscript "*h*" on *PM* and *S* in this section because we are assuming that only one sensor monitors the process step.

Let *P* denote the conditional probability that a diversion has occurred during this step, given the data reported by the sensor. Using standard notation for conditional probabilities, we write $P = P(D \mid S)$, where the variable D is used to denote the event in which a diversion takes place. *S* is 1 when the transparency software identifies a deviation from expected operations and 0 when no deviation is identified.

To calculate *P*, we apply Bayes' Theorem. The sample space that we consider is partitioned by two events, D and D^C, the complement of *D*. (D^C is the event in which no diversion takes

[†] The notation *P*(*A*|*B*) is used to denote the conditional probability of *A* relative to the sample space *S*, or as it is more commonly stated "the probability of *A* given *B*."
[‡] The notation $A \cap B$ is used to denote the "intersection" of the sets A and B.

place.) Additionally, review of Scenarios 1-4 and Figure 2 in Section 4.4.1 leads to the following probabilities that will be used to calculate $P(D \mid S)$:

$$\begin{aligned} P(S=1 \mid D) &= 1-PM \\ P(S=0 \mid D^C) &= 1-PM \\ P(S=0 \mid D) &= PM \\ P(S=1 \mid D^C) &= PM. \end{aligned} \tag{1}$$

We are interested in calculating the probability that a diversion occurs, conditional upon the data reported by the sensor. The probability that a diversion has occurred when a deviation is identified ($S = 1$) is calculated by application of Bayes' Theorem:

$$\begin{aligned} P(D \mid S=1) &= \frac{P(D)P(S=1 \mid D)}{P(D)P(S=1 \mid D)+P(D^C)P(S=1 \mid D^C)} \\ &= \frac{PD(1-PM)}{PD(1-PM)+(1-PD)PM}. \end{aligned}$$

When no deviation is identified ($S = 0$), the probability that a diversion has taken place is

$$\begin{aligned} P(D \mid S=0) &= \frac{P(D)P(S=0 \mid D)}{P(D)P(S=0 \mid D)+P(D^C)P(S=0 \mid D^C)} \\ &= \frac{PD(PM)}{PD(PM)+(1-PD)(1-PM)}. \end{aligned}$$

These equations are appropriate when a process step is monitored by a single sensor and *PD* and *PM* are modeled as point probabilities.

A.5 Probability Calculation: Multiple Sensors

The equations presented in the previous section can be generalized for a process step with multiple sensors. Consider a process step with n_s sensors. The variable S_h, h=1,2,…, n_s, is 1 when the h^{th} intrinsic sensor sends a signal that does not match the expected signal, and S_h is 0 when the signal matches the expected signal. The probability that the h^{th} sensor will malfunction is denoted by the term PM_h, and it is assumed that the occurrence of a sensor malfunction is independent of any other sensor malfunctioning. Furthermore, we represent all PM_h and *PD* as point probabilities in this example. Thus, given any set of sensor data $S_1, S_2, \ldots, S_{n_s}$, the probability that a diversion of nuclear material has occurred during this operation is

$$P(D \mid S_1 \cap S_2 \cap \ldots \cap S_{n_s}) = \frac{P(D)P(S_1 \cap S_2 \cap \ldots \cap S_{n_s} \mid D)}{P(D)P(S_1 \cap S_2 \cap \ldots \cap S_{n_s} \mid D)+P(D^C)P(S_1 \cap S_2 \cap \ldots \cap S_{n_s} \mid D^C)}.$$

This result is a simple application of Bayes' Theorem. Because the events S_h, h=1, …, n_s, and D are independent, application of Lemma 1 to the numerator in the above equation yields equation (2)*:

$$P\left(D \mid S_1 \cap S_2 \cap \ldots \cap S_{n_s}\right) = \frac{P(D)\prod_{h=1}^{n_s} P(S_h \mid D)}{P(D)\prod_{h=1}^{n_s} P(S_h \mid D) + P\left(D^C\right)\prod_{h=1}^{n_s} P\left(S_h \mid D^C\right)}. \tag{2}$$

Finally, the terms in (1) can be combined into the following expressions:

$$\begin{aligned} P(S_h \mid D) &= \left\{ \begin{matrix} PM,\ S_h = 0 \\ 1-PM,\ S_h = 1 \end{matrix} \right\} = (PM)^{1-S_h}(1-PM)^{S_h},\ i = 1,\ldots,n_s \\ P\left(S_h \mid D^C\right) &= \left\{ \begin{matrix} 1-PM,\ S_h = 0 \\ PM,\ S_h = 1 \end{matrix} \right\} = (1-PM)^{1-S_h}(PM)^{S_h},\ i = 1,\ldots,n_s. \end{aligned} \tag{3}$$

Replacement of the terms $P(S_h \mid D)$ and $P\left(S_h \mid D^C\right)$ with terms on the right-hand side of equation (3) results in equation (4).

$$P\left(D \mid S_1 \cap S_2 \cap \ldots \cap S_{n_s}\right) = \frac{PD\prod_{h=1}^{n_s}(PM_h)^{(1-S_h)}(1-PM_h)^{S_h}}{PD\prod_{h=1}^{n_s}(PM_h)^{1-S_h}(1-PM_h)^{S_h} + (1-PD)\prod_{h=1}^{n_s}(PM_h)^{S_h}(1-PM_h)^{(1-S_h)}}. \tag{4}$$

This equation is appropriate when a process step is monitored by multiple sensors and PD and PM_h are modeled as point probabilities.

A.6 Risk Calculation

The risk of the diversion of nuclear material during a process step is calculated with the following equation:

$$R_{i,j,k} = P_{i,j,k} \times C_{i,j,k}\,. \tag{5}$$

The term $R_{i,j,k}$ denotes the diversion risk for the i^{th} process step of the j^{th} process in the k^{th} plant operation. $P_{i,j,k}$ and $C_{i,j,k}$ denote the conditional probability and consequence of diversion, respectively, for that same process step. When point probabilities are used to calculate $P_{i,j,k}$, the cumulative diversion risk for the j$^{\text{th}}$ process can be calculated by summing the risks from the process's individual process steps:

---

* The notation $\prod_{i=1}^{k} A_i$ is used to denote the product $A_i \times A_i \times \cdots \times A_i$.

$$R_{j,k} = \sum_i R_{i,j,k} \ . \tag{6}$$

The diversion risk for the k[th] plant operation is calculated by summing the risks from all of the plant's processes:

$$R_k = \sum_j R_{j,k} = \sum_{i,j} R_{i,j,k} \ . \tag{7}$$

A.7 Modeling PM and PD with Probability Distributions

It is reasonable to consider that the probabilities PM and PD will not be known with great precision. In this case, it is appropriate to consider them as random variables with probability distributions, and these variables have means and standard deviations (uncertainties). Rather than calculating a single value for the conditional probability *P*, a mean probability and associated standard deviation can be calculated.

The following theorems can be utilized to calculate the mean and standard deviation for the probability that a diversion has occurred at a process step (conditional upon the sensor data).

Theorem 2 **(Mood et al. 1974)***: Let X and Y be two random variables with means* μ_X *and* μ_Y*, respectively. If* $Z = X \pm Y$*, then* $\mu_Z = \mu_X \pm \mu_Y$.

Theorem 3 **(Mood et al. 1974)***: Let X and Y be two random variables with means* μ_X *and* μ_Y*, respectively. If* $Z = X \times Y$*, then* $\mu_Z = \mu_X \mu_Y + \mathrm{cov}[X,Y]$.

Theorem 4 **(Mood et al. 1974)***: Let X and Y be random variables with respective means* μ_X *and* μ_Y*. If Z=X/Y, then*

$$\mu_Z \approx \frac{\mu_X}{\mu_Y} - \frac{1}{\mu_Y^2}\mathrm{cov}[X,Y] + \frac{\mu_X}{\mu_Y^3}\mathrm{var}[Y].$$

Theorem 5 **(Mood et al. 1974)***: Suppose X and Y are measured with uncertainties* σ_X *and* σ_Y*, and the measured values are used to compute* $Z = X \pm Y$*. If the uncertainties in X and Y are known to be independent and random, then the uncertainty in Z,* σ_Z*, is*

$$\sigma_Z = \sqrt{(\sigma_X)^2 + (\sigma_Y)^2} \ .$$

In any case,

$$\sigma_Z \le \sigma_X + \sigma_Y \ .$$

Theorem 6 **(Taylor 1982)***: Suppose X and Y are measured with uncertainties* σ_X *and* σ_Y*, and the measured values are used to compute* $Z = X \times Y$ *and* $W = X/Y$. *If the uncertainties in X and Y are known to be independent and random, then the fractional uncertainties in Z and W,* $\frac{\sigma_Z}{|Z|}$ *and* $\frac{\sigma_W}{|W|}$*, are*

$$\frac{\sigma_Z}{|Z|} = \frac{\sigma_W}{|W|} = \sqrt{\left(\frac{\sigma_X}{|X|}\right)^2 + \left(\frac{\sigma_Y}{|Y|}\right)^2}\ .$$

In any case,

$$\frac{\sigma_Z}{|Z|} \le \frac{\sigma_X}{|X|} + \frac{\sigma_Y}{|Y|}$$

and

$$\frac{\sigma_W}{|W|} \le \frac{\sigma_X}{|X|} + \frac{\sigma_Y}{|Y|}.$$

Theorems 2-4 can be applied to equation (4) to calculate the mean conditional probability, denoted μ_p, and Theorems 5 and 6 must be applied to equation (4) to calculate the standard deviation on the conditional probability, denoted σ_p. It is evident from these theorems that only the means and standard deviations of PM and PD are required to calculate μ_p and σ_p. It is not necessary to know the PM and PD distributions.

The mean risk for a process step is calculated by simply multiplying the consequence for that step by μ_p. Similarly, the standard deviation for the risk of a process step is calculated by multiplying the consequence for that step by σ_p. The mean risk for a process or plant operation is calculated by summing the mean risks of all of the individual process steps associated with that process or plant operation. The standard deviation of the risk for a process or operation must be calculated using Theorem 5.

A.8 References

Bayes, T. 1764. An Essay Towards Solving a Problem in the Doctrine of Chances. *Phil. Trans.*, 53, 370. (Reproduced in *Biometrika*, 45, 293(1968), edited and introduced by G. A. Barnard.)

Mood, A. M., F. A. Graybill and D. C. Boes. 1974. Introduction to the Theory of Statistics. McGraw-Hill, New York, NY.

Taylor, J. R. 1982. An Introduction to Error Analysis: The Study of Uncertainties in Physical Measurements. University Science Books, Mill Valley, CA.

APPENDIX B: EXAMPLE DEMONSTRATION OF DIVERSION RISK CALCULATION USING POINT PROBABILITIES

This Appendix introduces a demonstration of how the risk model can be applicable to a MONJU-Style Fast Reactor based on the types of signals and information that are collected by the automation of the process.

B.1 Defining Expected Signals and Observed Signals

Declarations of facility operations are used to develop a set of "expected signals" that represent what the facility sensors should transmit if the operation goes according to plan, without any deviation. An example of expected signals defining a process step is shown in the table below, where **"No.**" is the sensor number, and "**Signal**" is the binary status [0 or 1] expected from the sensor during the step according to the declared operation.

This example represents Step 10000, where the New Fuel Transfer Machine –NFTM– gripper descends to the new fuel storage rack in a path to attain a new fuel assembly. In this example, when a facility declares that Step 10000 will take place, the risk analysis software develops a set of expected signals where each sensor in the list returns the signal identified in the table.

These expected signals can be simultaneous or sequential depending on the time standard for each activity. Simultaneous signals are grouped and expected to start at exactly the same time, tracking multiple sensors that together describe an event in the process. Sequential signals are expected to start immediately after the preceding signals are completed. (By design, it is possible for some sequential signals to overlap with one or more of the sensors in the preceding step if those preceding sensors are still active.) The time standard represents how much time is required or allotted for each event of the step and is developed in accordance to a time standard analysis for the automated activity.

For example, in Table B1[1], it is expected that when Sensor 7506 signals 1 it indicates that Step 10000 has begun and the pulse motor driver of the NFTM gripper has started. To successfully fulfill the declared step, it is expected that exactly one second after this signal is received, Sensors 7002, 7003, 7506, 7511, and 8908 will report the signals shown in the table during a total 21 seconds. After 21 seconds, Sensors 7002 and 7511 are then expected to report a change in their binary status, indicating the completion of Step 10000.

[1] Data from the MONJU Fuel Handling Transparency Model.

Table B1

Time Standard	No.	Signal	Comment
	7506	1	NFTM gripper - hoisting - pulse motor driver start
Sequential	7002	1	NFTM gripper - hoisting - pulse motor driver - busy
1 second past 7506			
Simultaneous with 7002	7003	0	NFTM gripper - hoisting - mechanical origin sensor - home position
Simultaneous with 7002	7506	0	NFTM gripper - hoisting - pulse motor driver start
Simultaneous with 7002	7511	1	NFTM Indicating Lamp
Simultaneous with 7002	8908	1	
Sequential	7002	0	NFTM gripper - hoisting - pulse motor driver - busy
21 seconds past 8908			
Simultaneous with 7002	7511	0	NFTM Indicating Lamp

"Observed signals" are the binary status [0, 1] transmitted by the sensor while the operation is taking place. During a real-time step, the time standard is measured by the time stamp transmitted by the observed signal.

When the information is being transmitted, the risk analysis software performs a comparison between the expected and observed signals, using "**S**" to determine if they are equal or not. When S=0, the operation has occurred as expected (expected = observed). When S=1, the sensor has reported a deviation from expectations (expected ≠ observed).

Table B2 summarizes an example of this comparison. Where S = 1, for Sensors 7003 and 7506, indicates that these sensors failed to transmit the expected binary status during actual operations. "S = 1" represents a flag where observations do not meet the expectations. The risk analysis software uses this information to initiate the risk calculation algorithm. Physically, the sensors track the progress of the step in the model, providing insight into and considering the potential diversion pathway. The failed sensors in the example indicate that the model NFTM gripper was not in the original position (7003) and the motor driver failed to shut down (7506).

Table B2

Time Stamp	No.	Expected Signal	Observed Signal	S	Comment
60726095356	7506	1	1	0	NFTM gripper - hoisting - pulse motor driver start
60726095357	7002	1	1	0	NFTM gripper - hoisting - pulse motor driver - busy
60726095357	7003	0	1	1	NFTM gripper - hoisting - mechanical origin sensor - home position
60726095357	7506	0	1	1	NFTM gripper - hoisting - pulse motor driver start
60726095357	7511	1	1	0	NFTM Indicating Lamp
60726095357	8908	1	1	0	
60726095418	7002	0	0	0	NFTM gripper - hoisting - pulse motor driver - busy
60726095418	7511	0	0	0	NFTM Indicating Lamp

B.2 Diversion Risk for Single Sensor Process Steps

The diversion risk can be calculated for any step, process and operation in the system, including those defined by a single sensor. This is the simplest case, where the consequence of diversion is defined by the number of SQ's handled during the step, and the probability of diversion at the step is calculated by comparing the expectations and observations of that single sensor.

Figure 5 introduces the algorithm for evaluating the signals during practical application, when a step is defined by a single sensor.

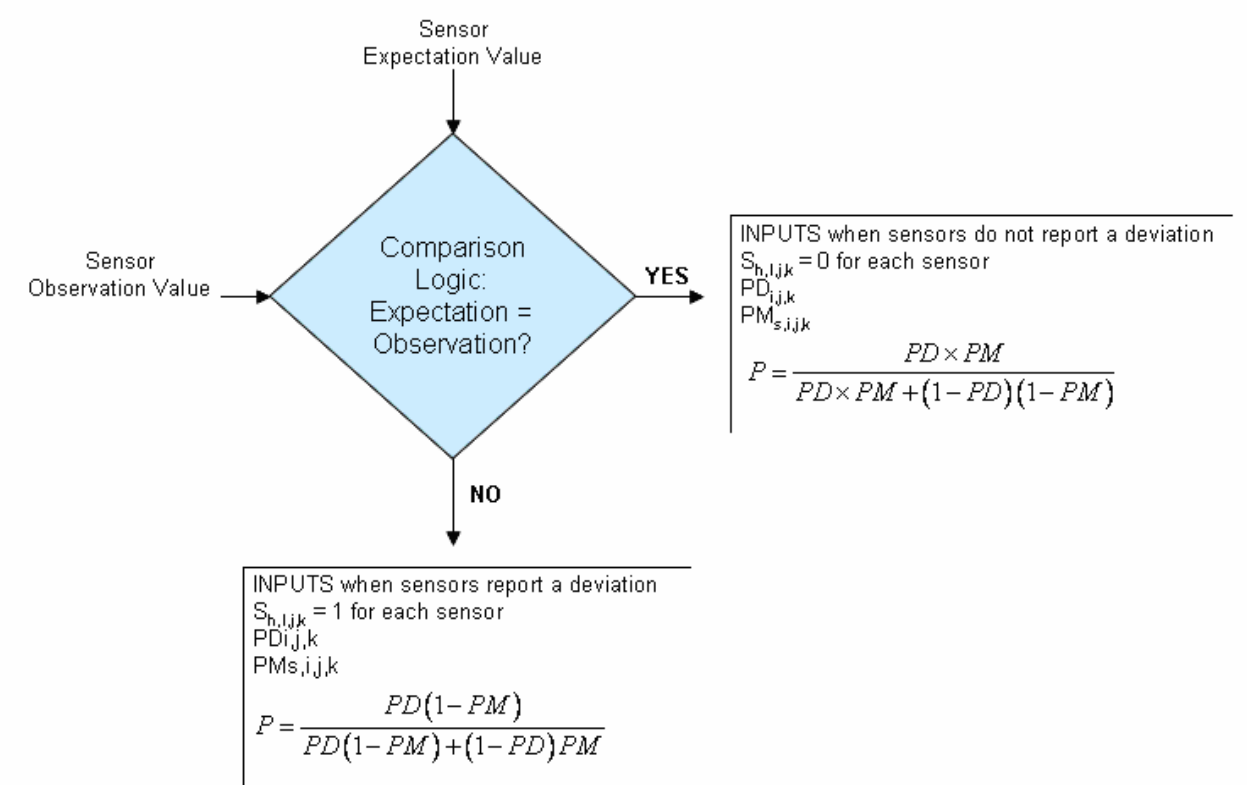

Figure 5: Calculating P for a Process Step with a Single Sensor

The following example shows both the comparison between expected and observed signals and the formula used for risk calculation in each of the possible outcomes (i.e., "expectations meet observations" and "expectations do not meet observations"). Although there is no step in the MONJU model that is solely defined by a single sensor, for the purpose of this example, we will consider the case of a step defined by the NFTM gripper latching to new fuel (Step 10001, Sensor 7005).

We will assume that the Probability of Diversion (PD) for this step is *known* as .9 and that the Probability of Malfunction(PM) for sensor 7005 is *known* as .001. Furthermore, we will assume that .5 SQ is handled during this step. Then, in Table B3:

Table B3

	EXAMPLE A If expectations meet observation[2]	EXAMPLE B If expectations do not meet observations[3]
1	Assumptions	
1.a	PD = .9	PD = .9
1.b	PM = .001	PM = .001
1.c	SQ = .5 SQ/step	SQ = .5 SQ/step
	Probability Calculation	
2	Sensor input	
2.a	Expectation Value = 0	Expectation Value = 0
2.b	Observation Value = 0	Observation Value = 1
3	Logical Test	
3.a	YES = No deviation is reported	NO = Deviation is reported
4	Inputs	
4.a	S = 0	S = 1
4.b	PD = .9	PD = .9
4.c	PM = .001	PM = .001
5	Formula	
5.1	$P = \frac{PD \times PM}{PD \times PM + (1-PD)(1-PM)}$	$P = \frac{PD(1-PM)}{PD(1-PM) + (1-PD)PM}$
6	Results: Probability of Diversion	
6.1	P = 8.9E-3	P = .99
	Diversion Risk	
7	Inputs	
7.1	P = 8.9E-3	P = .99
7.2	C = .5 SQ/step	C = .5 SQ/step
8	Formula	
8.1	$R_{i,j,k} = P_{i,j,k} \times C_{i,j,k}$	$R_{i,j,k} = P_{i,j,k} \times C_{i,j,k}$
9	Risk	
9.1	**R = 4.4E-3 SQ/step**	**R = .49 SQ/step**

[2] The calculation to be performed if "Expectations meet Observations" is the process to calculate the Expected Risk for each sensor.

[3] The calculation to be performed if "Expectations do not meet Observations" is the process to calculate the Observed Risk for each sensor.

B.3 Diversion Risk for Multi-Sensor Steps

The calculation of the risk of process steps that are defined and verified by multiple sensors is more complex than the previous case. While the consequence of diversion is still defined by the number of SQ's handled during the step, the probability of diversion at the step is calculated by comparing the expectations and observations for every single sensor.

Figure 6 introduces the algorithm for evaluating the signals during practical application, when a step is defined by multiple sensors.

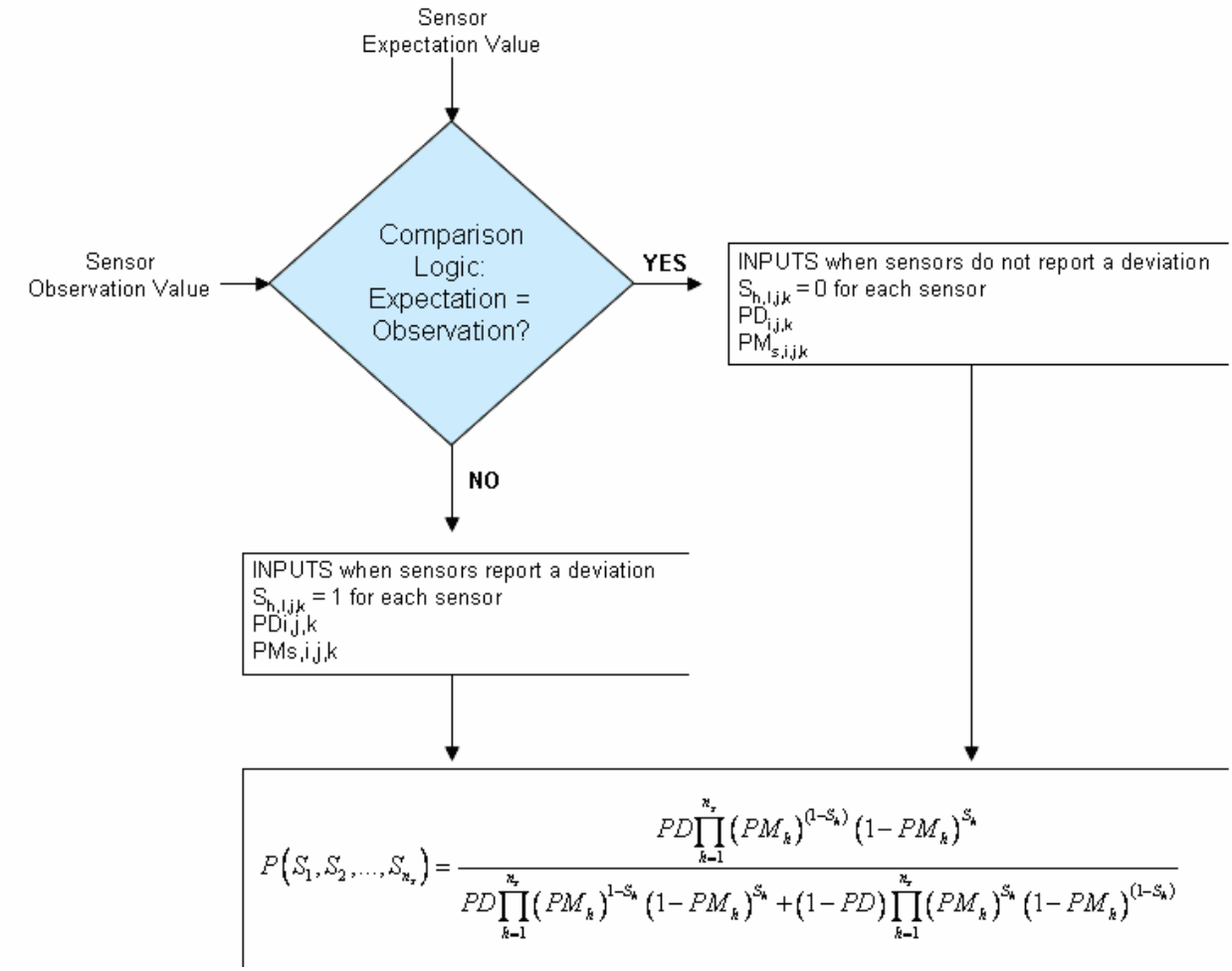

Figure 6: Calculating P for a Process Step with Multiple Sensors

The following examples show the practical application for calculating diversion risk for a step with multiple sensors.

EXAMPLE C: All observations meet expectations, *same* PM for *each* sensor.
For the purpose of this example, we will consider the NFTM gripper descent to new fuel storage rack (Step 10000) which is defined by sensors described in Table B4.

Table B4

h	Time/Date	No.	Signal	Comment
1	60726095356	7506	1	NFTM gripper - hoisting - pulse motor driver start
2	60726095357	7002	1	NFTM gripper - hoisting - pulse motor driver - busy
3	60726095357	7003	0	NFTM gripper - hoisting - mechanical origin sensor - home position
4	60726095357	7506	0	NFTM gripper - hoisting - pulse motor driver start
5	60726095357	7511	1	NFTM Indicating Lamp
6	60726095357	8908	1	
7	60726095357	8908	0	
8	60726095418	7002	0	NFTM gripper - hoisting - pulse motor driver - busy
9	60726095418	7511	0	NFTM Indicating Lamp

The time stamp field indicates the sensor signals that are received simultaneously, and those that are received sequentially, in the following format.

X	XX	XX	XX	XX	XX
year	month	day	hour	minute	second

As in the previous example, we will assume that the Probability of Diversion (PD) for this step is *known* as .9 and that the Probability of Malfunction for each sensor is *known* as .001. We will also assume that .5 SQ is handled during this step.

Then, the Probability of Diversion (P) can be calculated according to Table B5:

Table B5

h	No.	Expected Signal	Observed Signal	Test	S_h	PM_h	1-S_h	1-PM_h	PM_h^ (1-S_h)	(1-PM_h) ^S_h	PM_h^ (1-S_h)* (1-PM_h) ^S_h	PM_h ^S_h	(1-PM_h) ^(1-S_h)	PM_h^S_h* (1-PM_h) ^(1-S_h)
1	7506	1	1	YES	0	0.001	1	0.999	0.001	1	0.001	1	0.999	0.999
2	7002	1	1	YES	0	0.001	1	0.999	0.001	1	0.001	1	0.999	0.999
3	7003	0	0	YES	0	0.001	1	0.999	0.001	1	0.001	1	0.999	0.999
4	7506	0	0	YES	0	0.001	1	0.999	0.001	1	0.001	1	0.999	0.999
5	7511	1	1	YES	0	0.001	1	0.999	0.001	1	0.001	1	0.999	0.999
6	8908	1	1	YES	0	0.001	1	0.999	0.001	1	0.001	1	0.999	0.999
7	8908	0	0	YES	0	0.001	1	0.999	0.001	1	0.001	1	0.999	0.999
8	7002	0	0	YES	0	0.001	1	0.999	0.001	1	0.001	1	0.999	0.999
9	7511	0	0	YES	0	0.001	1	0.999	0.001	1	0.001	1	0.999	0.999

PD =	0.9
1-PD =	0.1
∏(PMh)^(1-Sh)*((1-PMh)^Sh) =	1E-27
∏((PMh)^Sh)*(1-PMh)^(1-Sh) =	0.991035916
PD∏(PMh)^(1-Sh)*((1-PMh)^Sh) =	9E-28
(1-PD)∏((PMh)^Sh)*(1-PMh)^(1-Sh) =	0.099103592

$$P(S_1,S_2,\ldots,S_{n_s}) = \frac{PD\prod_{k=1}^{n_s} PM_k^{(1-S_k)}(1-PM_k)^{S_k}}{PD\prod_{k=1}^{n_s} PM_k^{1-S_k}(1-PM_k)^{S_k} + (1-PD)\prod_{k=1}^{n_s} PM_k^{S_k}(1-PM_k)^{(1-S_k)}} = 9.08141E\text{-}27$$

Finally, the Diversion risk for Step 10000 is calculated in accordance to $R_{i,j,k} = P_{i,j,k} \times C_{i,j,k}$.

Where P = 9.0E-27
C = .5 SQ

So, **R = 4.5E-27 SQ/step**
R = ~0

EXAMPLE D: All observations meet expectations, *different* PM for *various* sensors. For the purpose of this example, we will consider the NFTM gripper latch new fuel (Step 10001) which is defined by sensors described in Table B6.

Table B6

h	Time/Date	No.	Signal	Comment
1	60726095418	7510	1	NFTM gripper - DC motor - start
2	60726095418	7511	1	NFTM Indicating Lamp
3	60726095419	7004	1	NFTM gripper - delatch sensor
4	60726095421	7005	0	NFTM gripper - latch sensor
5	60726095421	7510	0	NFTM gripper - DC motor - start
6	60726095421	7511	0	NFTM Indicating Lamp

As in the previous examples, we will assume that the Probability of Diversion (PD) for this step is *known* as .9 and that that .5 SQ is handled during this step. The Probability of Malfunction for each sensor is *known* and the Probability of Diversion (P) can be calculated according to Table B7:

Table B7

h	No.	Expected Signal	Observed Signal	Test	S_h	PM_h	1-S_h	1-PM_h	PM_h^ (1-S_h)	(1-PM_h) ^S_h	PM_h^ (1-S_h)* (1-PM_h) ^S_h	PM_h^ S_h	(1-PM_h) ^(1-S_h)	PM_h^S_h* (1-PM_h) ^(1-S_h)
1	7510	1	1	YES	0	0.001	1	0.999	0.001	1	0.001	1	0.999	0.999
2	7511	1	1	YES	0	0.05	1	0.95	0.05	1	0.05	1	0.95	0.95
3	7004	1	1	YES	0	0.001	1	0.999	0.001	1	0.001	1	0.999	0.999
4	7005	0	0	YES	0	0.001	1	0.999	0.001	1	0.001	1	0.999	0.999
5	7510	0	0	YES	0	0.01	1	0.99	0.01	1	0.01	1	0.99	0.99
6	7511	0	0	YES	0	0.05	1	0.95	0.05	1	0.05	1	0.95	0.95

PD = 0.9

1-PD = 0.1

∏(PMh)^(1-Sh)*((1-PMh)^Sh) = 2.5E-14

∏((PMh)^Sh)*(1-PMh)^(1-Sh) = 0.890797255

PD∏(PMh)^(1-Sh)*((1-PMh)^Sh) = 2.25E-14

(1-PD)∏((PMh)^Sh)*(1-PMh)^(1-Sh) = 0.089079725

$$F(S_1,S_2,\ldots,S_n)=\frac{PD\prod_{h=1}^{n}(PM_h)^{(1-S_h)}(1-PM_h)^{S_h}}{PD\prod_{h=1}^{n}(PM_h)^{1-S_h}(1-PM_h)^{S_h}+(1-PD)\prod_{h=1}^{n}(PM_h)^{S_h}(1-PM_h)^{(1-S_h)}} = 2.52583E\text{-}13$$

Finally, the Diversion risk for Step 10001 is calculated in accordance to $R_{i,j,k} = P_{i,j,k} \times C_{i,j,k}$.

Where P = 2.5E-13
C = .5 SQ

So, **R = 1.2E-13 SQ/step**

EXAMPLE E: Some observations do not meet expectations.
For the purpose of this example, we will consider the NFTM ascent to starting point (Step 10002) which is defined by sensors described in the following table.

Table B8

h	Time/Date	No.	Signal	Comment
1	60726095422	7505	1	NFTM gripper - hoisting - pulse motor driver - changeover of operation mode
2	60726095422	7506	1	NFTM gripper - hoisting - pulse motor driver start
3	60726095422	7002	1	NFTM gripper - hoisting - pulse motor driver - busy
4	60726095422	7506	0	NFTM gripper - hoisting - pulse motor driver start
5	60726095422	7511	1	NFTM Indicating Lamp
6	60726095431	7204	0	
7	60726095443	7511	0	NFTM Indicating Lamp
8	60726095444	7002	0	NFTM gripper - hoisting - pulse motor driver - busy
9	60726095444	7003	1	NFTM gripper - hoisting - mechanical origin sensor - home position
10	60726095444	7505	0	NFTM gripper - hoisting - pulse motor driver - changeover of operation mode

In this example, several sensors observations do not meet expectations. Namely, all the sensors associated with the NFTM gripper-hoisting report a deviation from expectations.

As in the previous examples, we will assume that the Probability of Diversion (PD) for this step is *known* as .9 and that that .5 SQ is handled during this step. The Probability of Malfunction for each sensor is *known* and the Probability of Diversion (P) can be calculated according to Table B9:

Table B9

h	No.	Expected Signal	Observed Signal	Test	S_h	PM_h	1-S_h	1-PM_h	PM_h^(1-S_h)	(1-PM_h)^S_h	PM_h^(1-S_h)*(1-PM_h)^S_h	PM_h^S_h	(1-PM_h)^(1-S_h)	PM_h^S_h*(1-PM_h)^(1-S_h)
1	7505	1	1	YES	0	0.001	1	0.999	0.001	1	0.001	1	0.999	0.999
2	7506	1	1	YES	0	0.001	1	0.999	0.001	1	0.001	1	0.999	0.999
3	7002	1	0	NO	1	0.01	0	0.99	1	0.99	0.99	0.01	1	0.01
4	7506	0	1	NO	1	0.05	0	0.95	1	0.95	0.95	0.05	1	0.05
5	7511	1	1	YES	0	0.05	1	0.95	0.05	1	0.05	1	0.95	0.95
6	7204	0	0	YES	0	0.05	1	0.95	0.05	1	0.05	1	0.95	0.95
7	7511	0	0	YES	0	0.001	1	0.999	0.001	1	0.001	1	0.999	0.999
8	7002	0	1	NO	1	0.001	0	0.999	1	0.999	0.999	0.001	1	0.001
9	7003	1	0	NO	1	0.001	0	0.999	1	0.999	0.999	0.001	1	0.001
10	7505	0	1	NO	1	0.05	0	0.95	1	0.95	0.95	0.05	1	0.05

PD =	0.9
1-PD =	0.1
∏(PMh)^(1-Sh)*((1-PMh)^Sh) =	2.22922E-12
∏((PMh)^Sh)*(1-PMh)^(1-Sh) =	2.24949E-11
PD∏(PMh)^(1-Sh)*((1-PMh)^Sh) =	2.0063E-12
(1-PD)∏((PMh)^Sh)*(1-PMh)^(1-Sh) =	2.24949E-12

$$P(S_1,S_2,\ldots,S_{n_s}) = \frac{PD\prod_{k=1}^{n_s} PM_k^{(1-S_k)}(1-PM_k)^{S_k}}{PD\prod_{k=1}^{n_s} PM_k^{(1-S_k)}(1-PM_k)^{S_k} + (1-PD)\prod_{k=1}^{n_s} PM_k^{S_k}(1-PM_k)^{(1-S_k)}} = 0.471428571$$

Finally, the Diversion risk for Step 10002 is calculated in accordance to $R_{i,j,k} = P_{i,j,k} \times C_{i,j,k}$.

Where P = .47
C = .5 SQ

So, **R = .23 SQ/step**

B.4 Accumulation of Risk

Diversion Risk can be accumulated to account for all the steps in a process, processes in operations, and operations in a facility. The cumulative diversion risk can be calculated by summing the risks from the facility individual operations, processes and steps.

Taking as an example the Diversion Risk calculated in Examples C, D and E for steps 10000 to 10002, the Diversion Risk for the process comprising these three steps can be calculated as follows:

Step	**Diversion Risk**
10000	~0 SQ/step
10001	1.2E-13 SQ/step
10002	.23 SQ/step
$R_{j,k} = \sum_i R_{i,j,k}$	.23 SQ/process

B.5 Understanding the Range of Diversion Risk Results

The magnitude of diversion risk can vary greatly from one step, process or operation to the next, as seen in the summary tables below:

Single Sensor Example

Step	**Diversion Risk**	**Comments**
10000	4.4E-3 SQ/step	A. Operation meets expectations
10001	.49 SQ/step	B. Operation does not meet expectations

Multiple Sensors Example

Step	**Diversion Risk**	**Comments**
10000	4.5E-27 SQ/step	C. 9 sensors. Operation met expectations
10001	1.2E-13 SQ/step	D. 6 sensors. Operation met expectations
10002	.23 SQ/step	E. 10 sensors. Operation did not meet expectations on 5 sensors
$R_{j,k} = \sum_i R_{i,j,k}$	.23 SQ/process	Full process Risk of Diversion is governed by the risk of diversion at the step where sensors detected a diversion.

The result of the diversion risk algorithm is a factor of PD, PM, SQ and whether the sensors detect a deviation or not. The large variation in diversion risk values seen in the example (from 1E-2 to 1E-28) can be explained by two main factors:

- Number of sensors in the step
- Number of deviations detected in multi-sensor steps

For a single sensor step, as seen in examples A and B (where PM, PD and SQ were kept constant), the higher diversion risk was obtained when the step did not meet expectations. This indicates an increase in risk when deviations between expectations and observations are detected, which is compatible with the conceptual framework of the model. However, while an increase in risk is expected because there is only one opportunity (one sensor) to detect a deviation, there is also only one point for measurement. Therefore, when a deviation is detected, there are no mitigating measurements to mitigate the increase in risk (the difference in results between examples A and B changed from the order of 1E-3 when no deviation was detected to approximately .5 when deviation was detected).

For a multi-sensor step, as seen in examples C, D and E, the higher diversion risk was also obtained when steps did not meet expectations (in the order of 1E-2 with 5 deviations detected). However, in multi-sensor cases where steps met expectations, the diversion risk was lower when more sensors were available. This is because if the sensors are functioning properly there is more opportunity to detect a deviation and thus less chance that diversion will go undetected.

Finally, it is expected (as shown in the accumulation of risk results) that once diversion risk is summed for every step, process, and operation, the diversion risk value will be determined by the risk of diversion at the steps or processes where sensors detect a deviation since the risk at other steps or processes might be too small to be of significance in the summation.

DISTRIBUTION

2	MS9018	Central Technical Files	08944
2	MS0899	Technical Library	04536
1	MS0123	D. L. Chavez, LDRD Office	01011