**SANDIA REPORT**
SAND2007-6429
Unlimited Release
Printed October 2007

# Framework for Integrating Safety, Operations, Security, and Safeguards in the Design and Operation of Nuclear Facilities

John Darby, Karl Horak, Jeffrey LaChance, Keith Tolk, and Donnie Whitehead

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

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.

Approved for public release: further dissemination unlimited.

Sandia National Laboratories

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

**NOTICE:** This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof, or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof, or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

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
5825 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

SAND2007-6429
Unlimited Release
Printed October 2007

# Framework for Integrating Safety, Operations, Security, and Safeguards in the Design and Operation of Nuclear Facilities

John Darby, Karl Horak, Jeffrey LaChance, Keith Tolk, and Donnie Whitehead

Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185-MS1373

## Abstract

The US is currently on the brink of a nuclear renaissance that will result in near-term construction of new nuclear power plants. In addition, the Department of Energy's (DOE) ambitious new Global Nuclear Energy Partnership (GNEP) program includes facilities for reprocessing spent nuclear fuel and reactors for transmuting safeguards material. The use of nuclear power and material has inherent safety, security, and safeguards (SSS) concerns that can impact the operation of the facilities. Recent concern over terrorist attacks and nuclear proliferation led to an increased emphasis on security and safeguard issues as well as the more traditional safety emphasis. To meet both domestic and international requirements, nuclear facilities include specific SSS measures that are identified and evaluated through the use of detailed analysis techniques. In the past, these individual assessments have not been integrated, which led to inefficient and costly design and operational requirements. This report provides a framework for a new paradigm where safety, operations, security, and safeguards (SOSS) are integrated into the design and operation of a new facility to decrease cost and increase effectiveness. Although the focus of this framework is on new nuclear facilities, most of the concepts could be applied to any new, high-risk facility.

# Table of Contents

**Acronyms** ..... **7**
**1.0 Introduction** ..... **9**
**1.1** Need for Integration ..... 9
**1.2** Framework Overview ..... 10
**1.3** Benefits ..... 11
**1.4** Report Content ..... 11
**2.0 Background** ..... **12**
**2.1** Typical Design Process ..... 12
**2.2** Operational Considerations ..... 13
**2.3** Nuclear Facility Licensing Processes ..... 13
**2.4** Safety Analysis/Design Process for Nuclear Facilities ..... 15
**2.5** Security Analysis/Design Process for Nuclear Facilities ..... 16
**2.6** Safeguard Analysis/Design Process for Nuclear Facilities ..... 19
**2.7** Information Technology ..... 23
**3.0 Integration Framework** ..... **25**
**3.1** Elements of Proposed Framework ..... 26
**3.2** Regulatory Requirements ..... 29
**3.3** Identify SOSS Expectations and Performance Measures ..... 29
**3.4** Design Analysis Process ..... 30
**4.0 Enabling Tools and Techniques for ISOSS** ..... **39**
**4.1** SOSS IT Integration ..... 39
**4.2** Integrated Risk Analysis Tools ..... 44
**4.3** Cross-Training in SSS ..... 45
**4.4** Formalized Design/Operation Review Process Enabling IT ..... 45
**5.0 Required Developments to Effectively Integrate SOSS** ..... **47**
**5.1** Integrated Risk-Informed SOSS Regulations for New Nuclear Facilities ..... 47
**5.2** Performance Measures ..... 47
**5.3** Threats and Challenges ..... 51
**5.4** Integrated Risk Analysis Methods ..... 51
**6.0 Summary** ..... **72**
**References** ..... **74**

## Figures

Figure 1. Framework for integrating SOSS during the design process. ..... 25
Figure 2. Steps in Vital Area Identification ..... 36
Figure 3. Example of the Sabotage Portion of a Fault Tree ..... 36
Figure 4. Notional Data Collection Infrastructure ..... 40
Figure 5. Belief/Plausibility as Bounds on Probability ..... 54
Figure 6. Evidence for Intervals and Probabilities for Values for Variable "Dow Jones Industrials Close on Dec. 31, 2007" ..... 55
Figure 7. Fuzzy Sets for Consequence (Deaths) ..... 56
Figure 8. Adversary and Defender: Different Consequences of Concern ..... 58
Figure 9. Overall Adversary-Defender Model for Risk ..... 59
Figure 10. Overall Adversary-Defender Model for Risk in LinguisticBelief Software ..... 59
Figure 11. Adversary Model ..... 60
Figure 12. Defender Model ..... 60
Figure 13. Fuzzy Sets for Numeric and Non-Numeric Variables ..... 61
Figure 14. An Approximate Reasoning Rule Base for Expected Consequence ..... 62
Figure 15. Belief/Plausibility for Evidence on Numeric Variable ..... 62
Figure 16. Belief/Plausibility for Evidence on Linguistic Variable ..... 63
Figure 17. Evaluation in LinguisticBelief ..... 63
Figure 18. Ranking of Scenario CBRNE_1B ..... 64
Figure 19. Ranking of Scenario CBRNE_2B ..... 65
Figure 20. Ranking of Scenario CBRNE_3B ..... 65
Figure 21. Ranking of Scenario CBRNE_4B ..... 66
Figure 22. Ranking of Scenario CBRNE_5B ..... 66
Figure 23. Evidence from Four Experts for Adversary Level of Technical Training ..... 68
Figure 24. Evidence Entered into PoolEvidence ..... 68
Figure 25. Pooled Evidence for Example ..... 69

## Table

Table 1. Example Documentation of Performance Measures Considered During the Design of a Facility ..... 30

## Acronyms

| | |
|---|---|
| CDP | critical detection point |
| CFR | Code of Federal Regulations |
| DA | destructive assay |
| DBA | design basis accident |
| DBT | design basis threat |
| DOE | Department of Energy |
| DPA | diversion path analysis |
| DPA | Diversion Path Analysis |
| FFF | fuel fabrication facility |
| FMEA | Failure, Modes, and Effects Analysis |
| FTP | file transfer protocol |
| GNEP | Global Nuclear Energy Partnership |
| IAEA | International Atomic Energy Agency |
| IC | inspectorate cabinet |
| ID | Inventory Difference |
| ISA | Integrated Safety Assessment |
| ISOSS | safety, operations, security, and safeguards |
| IT | Information Technology |
| JCATS | Joint Conflict and Tactical Simulation |
| JSGO | Japanese Safeguards Office |
| kg | kilogram |
| LC | local cabinet |
| LOCA | Loss of Coolant Accident |
| MBA | material balance area |
| MC&A | material control and accounting |
| MOX | mixed oxide |
| NDA | non-destructive assay |
| NDAS | non-destructive assay system |
| NRC | Nuclear Regulatory Commission |
| NTK | need to know |
| NTP | network time protocol |
| PMS | process monitoring system |
| PPS | physical protection system |

| | |
|---|---|
| PRA | probabilistic risk assessment |
| Pu | plutonium |
| PUREX | plutonium and uranium recovery by extraction |
| RDB | Raw Database |
| SEID | standard error of inventory difference |
| SnF | Sign and Forward |
| SNL | Sandia National Laboratories |
| SNM | special nuclear material |
| SOSS | safety, operations, security, and safeguards |
| SQ | significant quantity |
| SSC | structures, systems, and components |
| SSS | safety, security, and safeguards |
| STIE | sealed tamper indicating enclosure |
| URA | uncertainty risk assessment |
| VA | vulnerability assessment |
| VPN | virtual private network |

# 1.0 Introduction

The US is currently on the brink of a nuclear renaissance that will result in near-term construction of new nuclear power plants. In addition, the Department of Energy's (DOE) ambitious new Global Nuclear Energy Partnership (GNEP) program includes facilities for reprocessing spent nuclear fuel and reactors for transmuting safeguards material. The use of nuclear power and material has inherent safety, security, and safeguards (SSS) concerns that can impact the operation of the facilities. Recent concern over terrorist attacks and nuclear proliferation has led to an increased emphasis on security and safeguard issues as well as the more traditional safety emphasis. To meet both domestic and international requirements, nuclear facilities include specific SSS measures that are identified and evaluated through the use of detailed analysis techniques. In the past, these individual assessments have not been integrated, which led to inefficient and costly design and operational requirements. This report provides a framework for a new paradigm where safety, operations, security, and safeguards (SOSS) are integrated into the design and operation of a new facility to decrease cost and increase effectiveness. Although the focus of this framework is on new nuclear facilities, most of the concepts could be applied to any new, high-risk facility.

## 1.1 Need for Integration

The need for integrated safety, operations, security, and safeguards (ISOSS) is being stressed in new DOE orders and proposed Nuclear Regulatory Commission (NRC) licensing approaches. SOSS (including real-time process information management) must be coherently integrated into the design and operation of a facility in order for the facility to meet the applicable regulatory requirements in a cost-effective manner. Sandia National Laboratories (SNL) has long been a proponent of this concept in the nuclear weapons field, where it is referred to as surety.

The design of nuclear facilities is primarily driven by the operational needs of the facility. For nuclear power plants, the operational requirement is to generate electrical power, while fuel cycle facilities typically manufacture fuel (under the GNEP concept, these facilities would reprocess fuel). Operational and safety issues are often given higher priority than security and safeguard features.[1] While safety is typically incorporated into the design and operation of a nuclear facility, security and safeguard features are generally considered add-ons, and are often done after the facility has been constructed. As a result, the design features and procedures identified to meet the requirements for SOSS can be contradictory if the individual groups have not worked together to provide a single solution meeting all SOSS requirements (e.g., requiring the same door to be locked for security and unlocked for safety). In addition, new SOSS concerns and resulting requirements are often identified after a facility is built, which sometimes requires costly back-fits. Although the back-fits may improve one SOSS element, they can adversely affect other elements. For example, increases in security to confront changing

[1] Security focuses on the physical security system which protects the facility from attack by adversaries; safeguards is the material control and accounting system and the international safeguards system (if any) which focuses on ensuring that nuclear materials are not stolen or diverted. The complexity of the safeguards system depends on the nature of the facility. A nuclear reactor that does not have plutonium-bearing fresh fuel has a much simpler safeguards system than a nuclear fuel reprocessing facility.

“insider” threat requirements can impose significant restrictions on the movement of personnel throughout the facility, negatively impacting normal operations.

The stove-piped design of a facility may not effectively allow for the full utilization of available systems and information for addressing SOSS requirements. In particular, there is the potential for better use of information systems to address multiple aspects of SOSS. Safeguards-related measurements that indicate a loss of material, for example, may actually occur because of a component malfunction and should be reviewed to identify potential concerns related to operations and safety. Interaction between the groups that evaluate and design the facility can also lead to better understanding of the facility with regard to each SOSS element; this, in turn, could lead to recognition of risks that may have otherwise been overlooked.

Fortunately, because the concepts used to evaluate the safety and security of a facility are closely related and have sufficient similarity, it is possible to integrate these aspects. Despite the possibility of integration, it is not clear that this would be desirable, which is why this aspect is not discussed in the framework documented in this report. However, it is desirable to reconcile conflicting SOSS requirements. Thus, a major aspect of integration discussed in this framework deals with harmonizing the results of separate SOSS analyses into a cost-effective and optimal set of design and operational features. This set of features can be created using several enabling tools and techniques discussed in this framework (some of which will require further development).

## 1.2 Framework Overview

SNL has developed a preliminary framework for ISOSS, beginning at the facility design level and extending into the facility operation. The integration framework uses a systems engineering approach to combine the results of the individual—quantitative and qualitative—SOSS analyses to identify the structures, systems, and components (SSC) (including facility operations monitoring systems, such as process control information); limits on operation; and procedures required for each of the four disciplines.

The framework considers and addresses the commonalities and differences among the different SOSS elements. For example, both safety and security affect operations; use SSCs; and focus on preventing or mitigating similar consequences. Safety and security have a set of “design events” that drive the design and are concerned with events outside this set. However, safety is concerned with random acts, while security is concerned with intentional malevolent acts. Consequently, the “intensity” of the initiating event that must be addressed is much more uncertain for security than for safety. Also, the set of events of concern for safety are less subject to drastic change than the set of events of concern for security.

The framework also addresses consideration of a “design” set of events, and a risk-based consideration of events outside the design space. The risk process uses probabilistic risk assessment (PRA) for safety and uncertainty risk assessment (URA) for security. The URA approach considers the considerable epistemic uncertainty associated with intentional acts.

The framework addresses areas where safety and security have common benefits, such as use of barriers and access control of personnel, and areas where safety and security are in conflict, such as the tradeoff between allowing rapid emergency egress and the need to maintain the integrity of physical security barriers. The framework also discusses incorporating security into the design of operations to lessen security’s impact on operations.

The integrated framework addresses:

- the high-level SSS requirements and interactions among disciplines,
- effective management and utilization of the process information collected for each discipline,
- areas of subtle inter-disciplinary interactions,
- integration of the response procedures for safety and security personnel, and
- harmonization of the results of the various discipline analyses to achieve cost-effective facility design and operation (innovative methods may be required to meet all concerns).

## 1.3 Benefits

The benefits of incorporating an integrated approach into the design and operation of nuclear facilities using this framework are as follows:

- providing increased security at reduced cost,
- using complementary aspects of safety systems for security systems,
- decreasing impact on operations,
- addressing both “design events” and events outside the design space,
- extending safety-based PRA to security-based URA to evaluate events outside the design space using a risk measure,
- reducing personnel costs associated with security,
- rendering the security system robust to changes in the threat,
- incorporating intelligence gathering to improve security, and
- incorporating safety measures for mitigating consequences into security measures for mitigating consequences.

## 1.4 Report Content

The process of identifying a viable framework for integrating SOSS begins with a clear understanding of the typical design process, required regulations, and analysis techniques used in each SOSS element. Thus, Section 2 provides background material on the typical design process for a nuclear facility, focusing on licensing requirements for SSS systems. Section 3 presents an integration framework based on background information. This section also addresses the elements of the proposed framework, including regulatory requirements, performance measures, and an actual process for harmonizing the results of the various SOSS analyses. Section 4 discusses some enabling tools and techniques that could be used to facilitate integrating SOSS. Finally, Section 5 addresses areas where further development is required to fully implement the integration framework.

# 2.0 Background

This section focuses on the design process for nuclear facilities under the cognizance of the NRC and the DOE. Department of Defense facilities are not addressed.

Safety and security have many similarities, which the framework proposes to consider in the design of a new facility. For instance, both safety and security use SSCs as system elements (e.g., a radiation barrier can serve as a delay element in the security system), and both require access control systems. Safety uses access control to prevent entry into hazardous areas and to account for personnel during an emergency egress. Security uses access control to address the insider problem and to address deceit modes of outsider attack scenarios. Also, both safety and security are concerned with similar consequences, such as the release of radionuclides, and both have measures to mitigate such consequences. Safety and security must each address a set of "design events," and both must consider events outside the design space to ensure robustness of the systems.

Other similarities include requiring information technology (IT) for monitoring and communication, and being concerned with cyber threats. Typically, designers build in IT reliability through redundancy, such as hot backup network servers, on-site and off-site hard drive backups, uninterruptible power supplies, and so forth. However, different design phases of nuclear facilities present additional requirements.

## 2.1 Typical Design Process

The traditional design process for a nuclear facility is divided into four steps:

- pre-conceptual planning
- conceptual design
- preliminary design
- final design

The major input going into the pre-conceptual design phase is the purpose and need for the facility. It is during this phase that the facility project team is formed, which includes representatives from safety, operations, security, and safeguards. The most important milestone in this phase is the identification of high-level functions and requirements that cover not only the operational considerations but also include SSS requirements. Alternative studies can be performed at this stage to evaluate different designs.

It is during the conceptual design phase that the functional requirements for the facility are translated into an initial design. Although the main focus at this stage is on designing the facility to meet the operational requirements, some initial SSS reviews are typically performed as part of this effort. Sufficient operational analysis is performed to ensure that the proposed design can meet the required product outputs. Some form of preliminary safety analysis is generally performed to identify the hazards associated with the facility and needed preventive and mitigation features. Similarly, preliminary security and safeguard assessments are also needed at this stage to identify systems and features needed to meet the associated requirements. These preliminary assessments are generally qualitative in nature (e.g., Failure Modes and Effects Analysis), are performed in isolation, and may not be effectively integrated at this stage.

The preliminary design should refine the facility design to a greater level of detail based on more detailed analyses. The analysis techniques to evaluate the adequacy of the facility SOSS features can be more quantitative in nature and can include both deterministic and probabilistic analyses. The deterministic analyses provide the proof that the facility is designed to meet selected safety-related design basis accidents (DBAs) and security-related design basis threats (DBTs). Probabilistic approaches, such as PRA, can be used to evaluate the safety aspects of the facility for a full range of accidents, including those that are greater or lesser in magnitude than the DBA, and thus identify the important contributors to risk. Other techniques include vulnerability analysis (VA), which can be used to determine the adequacy of the security design, and diversion path analysis (DPA), which can be used to address material control and accountability. Although there is an opportunity to more fully integrate the SOSS features at this stage, the operational and safety requirements generally are the dominant features that impact the facility design.

The final design reflects the results of final detailed analyses and includes modifications that are needed to meet the functional and system design requirements. The final design also includes procedures for addressing normal, abnormal, and emergency situations. Technical specifications that address allowed outage times and inspection intervals for critical systems are also included as part of the final design submittal.

## 2.2 Operational Considerations

Facilities, by necessity, are designed to perform a specific function or set of functions. These functions are the reason for the facility's existence. As such, a facility must be designed to perform its operational activities such that these functions are conducted effectively and efficiently. Thus, for this reason, operational considerations are typically the main driver in determining a facility's design requirements.

For example, a commercial nuclear power plant that plans to sell electricity must generate that electricity at a cost that allows the owner to compete with other generating sources while making an adequate profit. The requirement that costs be competitive will influence the design of the facility, including its size (i.e., how many megawatts of electricity it produces), its reliability (i.e., how much of the time it can produce electricity), and the ease and ability to perform required maintenance (e.g., while operating).

Accurate and timely information forms the basis for many operational decisions in any nuclear facility. In addition, due to the complexity of the facility, many decisions are made automatically by mechanisms and information systems. As with the design process, a significant effort is placed on safe and reliable power, network infrastructure, server capacity, integration with embedded processors and monitoring systems, usable desktop environments, control displays/systems, and overall communications efficiency.

## 2.3 Nuclear Facility Licensing Processes

Most of the future commercial nuclear facilities in the US will be licensed by the NRC. This will include GNEP facilities that are operated by commercial enterprises. The NRC is responsible for ensuring both the safety and security of these commercial nuclear facilities.

The NRC is also responsible for licensing and regulating the operation of commercial nuclear power plants and material production and utilization facilities in the US. Currently, such facilities have been licensed under a two-step process described in Title 10 of the Code of

Federal Regulations (CFR) under Part 50. This process requires both a construction permit and an operating license.

In order to construct or operate a nuclear power plant, an applicant must submit a safety analysis report. This document contains the design information and criteria for the proposed reactor and comprehensive data on the proposed site. It also discusses various hypothetical accident situations and the safety features of the plant that prevents accidents or, if accidents should occur, lessens their effects. In addition, the application must contain a comprehensive assessment of the environmental impact of the proposed plant. A prospective licensee must also submit information for antitrust reviews of the proposed plant.

When an application to construct a nuclear plant is received, the NRC staff determines whether it contains sufficient information to satisfy commission requirements for a detailed review. If the application is accepted, the NRC holds a public meeting near the proposed site to familiarize the public with the safety and environmental aspects of the proposed application, including the planned location and type of plant, the regulatory process, and the provisions for public participation in the licensing process. Numerous public meetings of this type are held during the course of the reactor licensing process.

In an effort to improve regulatory efficiency and add greater predictability to the process, in 1989 the NRC established alternative licensing processes in 10 CFR Part 52 that included a combined license. This process, although not used to date, combines a construction permit and an operating license with conditions for plant operation.

Other licensing alternatives under Part 52 include early site permits that allow an applicant to obtain approval for a reactor site without specifying the design of the reactor(s) that could be built there, and certified standard plant designs that can be used as pre-approved designs.

In either process (10 CFR Part 50 or Part 52), before a nuclear power plant or nuclear material production facility can be built and operated, approval must be obtained from the NRC. In both licensing processes, the NRC maintains oversight of the construction and operation of a facility throughout its lifetime to assure compliance with the commission's regulations for the protection of public health and safety, the common defense and security, and the environment.

Nuclear safeguards are primarily concerned with accounting for nuclear materials (rather than activities or operations, for example). The safeguards regulatory regime for future US nuclear facilities may be complicated, as discussed below.

The safeguards licensing process and requirements will depend upon facility ownership and US Government policy. Privately owned commercial facilities are regulated by the NRC. Facilities that may be part of a national demonstration program, such as GNEP, may be owned by the DOE, and would normally be under the jurisdiction of the DOE safeguards requirements. However, the actual location of the facilities, the materials processed by these facilities, and the intended purpose of the facilities can all influence their regulatory environment. These facilities may process commercial spent fuel and all may have the intended purpose of commercial fuel cycle development. For these reasons, it is possible that these facilities would fall under NRC licensing and safeguards regulation and may be subject to international safeguards. It is possible that DOE would retain control of the security programs for those facilities located on DOE property, as is the case for the DOE Plutonium Disposition Program's Mixed Oxide (MOX) Fuel Fabrication Facility (FFF).

The most difficult safeguards challenges are presented by spent fuel reprocessing plants. If DOE facilities process commercial spent fuel and are intended for the commercial fuel cycle, they could be on the "Eligible Facilities List" of the US Voluntary Offer for the Application of International Atomic Energy Agency (IAEA) Safeguards. In that case, the US' obligations as a designated Nuclear Weapons State must be considered under the Treaty on the Non-Proliferation of Nuclear Weapons. From its Agreement for the Application of Safeguards with the IAEA, the US has committed to "…permit the Agency to apply its safeguards to all nuclear activities in the United States—excluding only those with direct national security significance …." Furthermore, the US and Agency have agreed to cooperate to "…facilitate the implementation of the safeguards provided for in …" the Agreement. The purpose of the US in entering into this agreement is to encourage "widespread adherence to the Treaty by demonstrating to non-nuclear weapon States that they would not be placed at commercial disadvantage by reason of the application of safeguards pursuant to the Treaty."[2] Under the Agreement, the US places facilities not intended for defense purposes on an "Eligible Facilities List." The IAEA may elect to apply safeguards to any facility on this list. There have been very few US facilities that have been put under IAEA safeguards thus far due to limited expected value from the required resource expenditure. The US Government has stated, however, that the GNEP facilities will demonstrate and support advanced international safeguards. Therefore, it is expected that some form of international safeguards requirements will be in effect.

## 2.4 Safety Analysis/Design Process for Nuclear Facilities

Commercial nuclear facilities must be licensed before they can be built and operated. One of the requirements in the licensing process is that the facility design must be able to withstand a set of specified upset or accident conditions. This set of conditions is typically referred to as the DBAs for the facility. These DBAs ensure that for a specified set of upset or off-normal conditions, the facility will function in a predictable and safe manner. This functioning may result from the use of active systems and components (e.g., electrically driven pumps and valves), passive features (e.g., gravity injection, natural circulation), or some combination of active and passive equipment or features.

Typically, the safety challenges to nuclear facilities generally include random failure of equipment leading to accident initiators, internal hazards such as fire and flood, and external events such as natural phenomena and accidents at nearby facilities. While DBAs are typically used to *establish* the safety-related accident mitigation features that must be present in a facility for it to be licensed, other methods may be needed to establish that a facility's design is adequate to handle all credible accidents (e.g., those with frequencies greater than 1E-7/yr) including those beyond the design basis. One such technique is a PRA.

In addition to demonstrating that a particular facility design meets the regulatory (i.e., licensing) requirements for a specific type of facility, a PRA may also be used in the actual design of a facility. Such use provides facility designers with a tool that can be used to ascertain the impact that specific design changes (or options) have on a facility's safety. These changes can then be examined to determine which are the most cost effective (i.e., have the least initial capital cost and subsequent operating cost).

---

[2] INFCIRC 288

## 2.5 Security Analysis/Design Process for Nuclear Facilities

In the past, the design and analysis of security systems for nuclear facilities have been performed after the facility was constructed. This led to expensive and less-than-optimal security features. In this era of terrorism, it is essential to consider a wider variety of threats in the design of security systems. This section discusses the pitfalls of the current practice for designing security systems and suggests a new paradigm for installing and operating systems that can adapt to the changing security threats.

### 2.5.1 Current Practice

Nuclear facilities have not been able to integrate changing security requirements into the design process since no nuclear facilities have been built in the US in more than 20 years. However, existing facilities have implemented new security requirements in response to changing threats, especially since September 11, 2001. The modifications required to meet an escalating threat are costly and/or manpower-intensive in terms of response force personnel.

Section 3.1 summarizes the regulatory requirements for physical security for both NRC-regulated facilities and DOE-owned and regulated facilities.

The physical security requirements are driven by the DBT for NRC and DOE facilities. The details of the DBT are classified (DOE) or safeguards information (NRC). Since September 11, 2001, there have been significant changes to the DBT in terms of adversary numbers and resources that must be protected against. The upgrading of security systems and the evaluation of the effectiveness of these upgrades are evaluated using the DBT to establish the threat that must be defeated.

A security system must meet the functional requirements of detection and assessment, delay, and response. An effective system detects and assesses the adversary, delays the adversary until effective response arrives, and provides sufficient response to neutralize the adversary. A security system is typically implemented at three layers—the perimeter, access to buildings, and access to areas within buildings.

The effectiveness of the security system depends on the scenario used by the adversary. The scenario includes the adversary group, adversary resources, the target, and the attack plan. Adversary resources include attributes (such as numbers, equipment, or weapons) and adversary knowledge (such as information gained from publicly available materials, reconnaissance, or insider assistance).

To evaluate the effectiveness of the system against the DBT, various scenarios within the DBT are postulated, and the system is evaluated under these scenarios. Evaluations are performed using modeling/simulation tools (e.g., path evaluation using Analytic System and Software for Evaluating Safeguards and Security [ASSESS], and response force evaluation using Joint Conflict and Tactical Simulation [JCATS]), table top exercises, and field exercises (force-on-force exercises). [3] [4]

With the increase in the DBT since September 11, 2001, the cost is high to back-fit existing facilities to provide improved security to counter the DBT. Therefore, for new facilities, integration of security into the design process is needed to provide improved security at lower cost, and to be less brittle to increases in the DBT.

Using traditional security to protect an existing facility against an ever-increasing threat results in:

- costly modifications,
- high costs for significant numbers of response force personnel, and
- major impact on operations.

### 2.5.2 Security for New Facilities

A new facility should have security integrated into the design along with operations and safety considerations. This integrated approach is referred to as "Assured Security by Design." [5] This approach has the following principles, all of which should be part of a new facility's design process.

- intrinsic physical security
- integrated physical security
- dynamic physical security
- integrated risk management

#### 2.5.2.1 Intrinsic Security

Intrinsic physical security refers to security that is intrinsic to the design process for the facility during all phases of the design—conceptual to final—and during construction. Intrinsic security incorporates security as an overall design requirement for the facility. For example, for safety, commercial reactors must meet the site criteria of 10 CFR 100; similarly, for security, the location of the site regarding the ease of implementing extended detection and the ability to provide effective response, onsite and offsite, should be part of the evaluation criteria.

Intrinsic security can complement traditional security. Improved detection, including early detection beyond the traditional site perimeter, can provide extra time for response. Delay can be incorporated at the correct layer of the facility (delay too deep inside a facility can be used by an adversary to hold off effective response). New active denial systems can be used. The number of onsite response force personnel can be reduced through better design to allow force multiplication for the responders, and more delay to allow time for offsite response to arrive.

#### 2.5.2.2 Integrated Security

Integrated physical security combines physical security with other functions in the design phase. Safety integrates with physical security to resolve conflicting requirements; for example, safety requires uninhibited emergency egress during an emergency, but security requires maintaining the delay afforded by a barrier, and the opening of an emergency exit could compromise a barrier. Security and safety can be integrated to synergistically provide a common means for reducing consequence. The facility operations group integrates with physical security personnel to address the insider threat without imposing onerous, costly impediments to operations. For example, if the design can be such that sabotage can be achieved in only a few areas, then two-person control can perhaps be restricted to only those areas, and operations in the other areas can be less affected by insider security requirements.

Cyber security is integrated with physical security in two ways. First, there are cyber characteristics of the physical security system itself. These include databases for access control and data transmission (e.g., from perimeter sensors to the central alarm station). Threats to these

cyber characteristics can degrade the physical security system. Second, physical security is necessary for cyber systems that handle sensitive information, such as the need to control access to servers.

Material control and accounting (MC&A) integrates with physical security on many levels. For piece-part materials, such as fuel assemblies for a nuclear power plant, security is necessary to ensure the integrity of the items so that MC&A can focus on counting the items rather than verifying the contents of the items have not changed. For facilities with materials in flow, such as a nuclear fuels reprocessing plant, physical security is necessary to ensure that the material to be accounted for is not diverted from the measurement systems. For international safeguards accounting of materials, portions of the physical security system (such as structures) can be considered part of the containment and surveillance system that complements the accounting system.

#### 2.5.2.3 Dynamic Physical Security

Dynamic physical security adapts the state of physical security during three phases: before the attack, during the attack, and after the attack [19-21]. Before the attack, dynamic security is proactive readiness. The facility state, both security posture and operations, changes based on current threat information from national, regional, and local intelligence sources. The more specific the threat information, the greater the state of readiness.

During the attack, dynamic security can incorporate active denial systems that are not part of the normal state of the facility. Active denial can augment expensive static structures to provide significant delay to an adversary. Also, dynamic physical security can incorporate last-resort options. A last-resort option is used to negate the attractiveness of the target (e.g., foaming-in a room with an asset to be protected). The last-resort option is based on the strong link–weak link safety strategy used in nuclear weapons [22]. The strong links perform their safety function reliably in certain environments, but cannot be guaranteed to remain safe in all environments. Weak links are designed into the weapon; when strong links are in environments they are unable to handle, they may experience undesired failures. In these cases, the weak links fail irreversibly before the strong links in order to render the weapon immune to these failures. For security, the last-resort option is a weak link that is used when the threat is above that which the traditional security system (the strong links) can defeat.

After the attack, dynamic security focuses on mitigating consequences through the use of contingency plans coordinated with safety mitigation measures. Also, for certain scenarios such as those that cause loss of production (e.g., loss of electrical power production from a nuclear power plant), dynamic security addresses protecting redundant facilities that can replace the services lost.

#### 2.5.2.4 Integrated Risk Management

Integrated risk management expands the traditional evaluation of physical security effectiveness from an evaluation against scenarios within the DBT to a risk-based evaluation. A major issue to be addressed is how to accommodate changes to the DBT.

The DBT for security is similar to the set of DBAs for safety. Both establish a set of criteria for design: safety systems address the initiating events in the DBA, security systems address the adversary scenarios in the DBT. Similar to the resources ascribed to the adversary for the DBT, safety evaluations have certain prescriptive rules associated with the DBAs, such as the single-

failure criteria. The DBT and the DBA are necessary, as they provide guidance required for the design of security and safety systems, respectively.

For safety evaluations, PRA is an accepted methodology for evaluating risk. PRA addresses accidents outside the DBA with the goal of identifying any that have risk sufficiently high to be of concern. Also, PRA is used to identify accidents that should be part of the DBA but that are complex and could be missed without the systematic PRA process. These include reactor coolant pump seal loss of coolant accidents (LOCA) and interfacing system LOCAs in commercial nuclear power plants.

Similar to the way the PRA enhances the DBA for accident evaluations, a process for assessing the risk for adversary acts is needed to enhance the DBT for security evaluations. The difficulty is that the risk from an intentional act has considerably more uncertainty than the risk from a "dumb" random event. Section 5.4 discusses a process for evaluating the risk for intentional acts called uncertainty risk analysis (URA) that is an extension of PRA to address the considerable epistemic uncertainty associated with evaluating the risk from an intentional act. This process addresses the three variables in the risk equation: likelihood of event, likelihood of failure of protective systems, and consequence of failure of protective systems. In the terminology of security evaluations, these three terms are called threat, vulnerability, and consequence, respectively.

For security, the current practice is to evaluate the vulnerability as the likelihood of failure of protective systems given specific scenarios within the DBT. The risk-based approach expands this practice to also address the likelihood of the threat (within and outside the DBT) and the different consequence of concern. As discussed in Section 5.4, the consequences desired by the adversary may differ from the consequences perceived as important by the defender, and this difference is captured in the evaluation process. The adversary consequences influence the threat, in that targets with desired consequences are more likely to be chosen. The defender consequences are part of the consequence term in the risk equation in that these are the consequences of concern for risk for the defender.

Evaluation of security with a risk approach allows all possible security improvement strategies to be evaluated. The current evaluation practice is based on the "fort mentality" used to design current security systems, which is hardening the fort to defeat the adversary when an attack occurs. The effectiveness is a measure of the ability of the fort to defeat the attack. An important part of security is the effectiveness of intelligence-gathering efforts to detect the adversary-gathering resources, both attributes and information. The risk-based evaluation approach allows for the evaluation of the effectiveness of intelligence-gathering as part of the threat (the likelihood of the initiating event).

## 2.6 Safeguard Analysis/Design Process for Nuclear Facilities

Safeguards systems and practices are used to ensure that special nuclear material (SNM) is not diverted from nuclear facilities and is accounted for. Intentional diversion is a key function that is addressed to some extent in the security requirements from insider threats. MC&A is also a critical aspect of safeguards. This section presents these and other basic concepts of safeguards and identifies differences between international and domestic requirements.

### 2.6.1 Safeguards Essentials

The three safeguards systems have many elements in common, including terminology. The terms MC&A, measurement requirements for material unaccounted for (an international term), and material balance or inventory difference (ID) (US terms) refer to the same quantity. This quantity is the difference between the book inventory and physical inventory, assuming all receipts and shipments have been addressed. Here, the term ID will be used.

Focusing on the ID and its error allows us to evaluate whether the goals and requirements for the three agencies can be met with current safeguards approaches and measurement techniques and their associated uncertainties.

The ID is calculated for each of possibly several material balance areas (MBA) over a material balance period using the material balance equation. The IAEA commonly writes this equation as:

$$ID = PB + X - Y - PE$$

where PB is the beginning physical inventory, X is the sum of additions to inventory (receipts), Y is the sum of withdrawals from inventory (shipments), and PE is the ending physical inventory. From the scientist's perspective, this is the "conservation of mass" equation for the closed system of the MBA; that is, the mass of material must balance or be conserved. From the accountant's perspective, the MBA starts with a book inventory of the records. Next, the records are adjusted for receipts and shipments throughout the material balance period. Finally, a physical inventory is taken at the close of the period. The material balance becomes the difference between the records (the book inventory) and the actual material present (the physical inventory).

Reconciliation takes place once the physical inventory is completed, and then the ID is evaluated. If the ID is determined not to be statistically significant, a new book inventory is established based on the physical inventory, and a new inventory period starts.

### 2.6.2 Safeguards Measurements

Two general types of material measurements are used in a bulk facility for MC&A purposes: destructive assay (DA) and non-destructive assay (NDA). DA requires a sample of the material to be measured; some, if not all, of the sample is consumed in the measurement. The sample must be taken from homogenous material to be representative. DA results in a lower measurement uncertainty, that is, a higher-quality measurement. However, DA generally requires more material handling and a longer turn-around time for results. NDA, on the other hand, is performed without taking a sample and can be utilized on homogeneous or heterogeneous materials. Although NDA provides quicker measurements, it results in a higher uncertainty.

Measurements are estimates of the quantity of material based on quantification of some observable attribute of the material. Every measurement is associated with an error or uncertainty. This error provides statistical uncertainty about which a measurement will fluctuate or a fixed bias while operating in a controlled state. Decisions about safeguards physical inventory are based on ID, which are, in turn, based on measurements of material and an assessment of measurement uncertainties.

In large, complex facilities that require many measurement systems, errors from multiple measurements and techniques are combined to determine the uncertainty of the ID. The ID uncertainty determines the loss detection capability of a safeguards system. Since uncertainties are typically expressed as a percentage of the ID, the absolute uncertainty of ID may increase directly as the throughput of the facility increases. As the throughput for the same measurement instrumentation increases, so does the uncertainty about the ID as the individual errors are propagated through the ID calculation. This results from existing measurement errors that cannot be reduced further through calibration or bias correction. This is the inherent, irreducible uncertainty of any measurement technique.

### 2.6.3 Domestic versus International Safeguards

Although the safeguard systems of the IAEA, NRC, and DOE have much in common, they focus on different threats. Domestic safeguards (NRC and DOE) protect against sabotage, theft, and other threats of direct concern to the government and the operators of the facility. Physical protection is a key element of domestic safeguards, along with traditional tracking of nuclear materials and other measures. In contrast, international safeguards, as applied by the IAEA, have a goal to detect diversion of significant amounts of fissile nuclear materials by the State/facility operator through verification of the State's declaration. Thus, in scenarios of concern in international safeguards, threats are posed by the State/facility operator, whereas in domestic safeguards scenarios, the threat is posed to the operator. Consequently, the safeguards measures required to meet domestic and international safeguards objectives have very different technical approaches. However, many of the techniques are useful for either safeguards system.

A second difference is that domestic criteria are requirements that must be met, while international criteria are goals. If these goals cannot be met, they can be supplemented with additional measures. This issue is addressed further below.

#### 2.6.3.1 IAEA Safeguards Criteria

The IAEA verifies the State's declaration to assure, in a timely fashion, that fissile material is not diverted during operations, transport, or storage. The IAEA must detect abrupt and protracted diversion of a significant quantity (SQ) of fissile material within a defined conversion time and with a false-alarm rate of no more than 5 percent. A significant quantity is defined to be 8 kg of unirradiated plutonium (Pu) or 75 kg of uranium 235, which is the amount of material that the IAEA estimates a diverter would need in order to manufacture a single nuclear weapon. The conversion time is based on the weaponization of the fissile material.

The IAEA must detect abrupt diversion (the removal of a large amount of material all at once) at a reprocessing facility within one month. Detection of protracted diversion (the removal of small amounts of material over a long period of time) of an SQ from a reprocessing facility must occur within one year. Therefore, the nuclear material balance must be closed monthly to meet the abrupt diversion timeliness goal and annually to meet the protracted goal.

Protracted diversion accounting requires plant shutdown and inventory clean-out. Ideally, detection of abrupt diversion accounting would also be based on a shutdown inventory; however, the facility may utilize process instrumentation for the inventory estimate.

### 2.6.3.2 NRC Safeguards Criteria

The NRC has not licensed a reprocessing facility since April 7, 1977, when President Jimmy Carter prohibited commercial reprocessing in the US as part of his non-proliferation policy. President Reagan lifted the indefinite ban that previous administrations had placed on commercial reprocessing activities in the US in an October 8, 1981, nuclear energy policy statement; however, no private sector entity has submitted a license application to the NRC for the licensing of a reprocessing plant.

Fortunately, one modern facility has recently been granted a construction authorization by the NRC, which gives an indication of the requirements that the NRC may use to license Advanced Fuel Cycle Initiative facilities. This facility is the Savannah River Site MOX FFF, which has a reprocessing component. Although this facility will be built on a DOE site, the DOE requested NRC regulation of this facility because it will be run by a commercial entity. The MOX FFF Plutonium and Uranium Recovery by Extraction (PUREX) processing component removes impurities from surplus weapons' Pu (which has been converted to oxide form), which will eventually be converted to MOX reactor fuel.

The construction authorization for this facility utilizes the newer NRC safeguards regulation, Part 74. Part of the approval process for this facility involved identifying and approving an MC&A requirement of a standard error of inventory difference (SEID) of 0.1% of the active inventory.[3] (The SEID is defined in 10 CFR Part 74.4 as "the standard deviation of an inventory difference that takes into account all measurement error contributions to the components of the ID.") When the NRC licenses another new reprocessing facility, this same requirement may apply.

### 2.6.3.3 DOE Safeguards Criteria

DOE MC&A requirements are based on the attractiveness level and category of the material as defined in Table I-4, reproduced in Appendix 3: Graded Safeguards, from the "Manual for Control and Accountability of Nuclear Materials," DOE M 470.4-6. The most conservative DOE inventory difference control limits, which are for Category I material, are as follows:[4] (a) For Category I and II MBAs, limits-of-error must not exceed 2 percent of the active inventory during the inventory period or a Category II quantity of material.

IT systems for IAEA Safeguards are driven as much by treaty compliance as by any other requirement. Due to the need for separate IT systems to support (a) plant declarations and (b) IAEA verification, there has been a long history of independent systems design and implementation. The IAEA has recently drafted a policy on joint-use technology[5] that is relevant to the design, construction, and operation of shared information assets.

---

[3] 10CFR74.59e5

[4] DOE manual 470.4-6, 8/26/05, "Nuclear Material Control and Accountability," p. I-14-15

[5] IAEA Policy Paper 20: Joint Use of Safeguards Equipment between the IAEA and an External Party. SMR 2.20, April 2004.

## 2.7 Information Technology

A common feature to SOSS is the presence of IT. As discussed in Section 5.5, integrating the IT systems utilized by each discipline is one means of integration. This section briefly discusses some key considerations regarding IT systems needed for each discipline.

### 2.7.1 Cyberthreats

Any information system, even one completely isolated by airgaps, is susceptible to a host of cyberthreats: viruses, unauthorized access, malicious ware, denial-of-service attacks, insider threat, and others.

NRC classifies nuclear facility information systems into "safety" and "non-safety," with different security criteria for each. In 2005, the NRC completed an official manual ("Criteria for Use of Computers in Safety Systems of Nuclear Power Plants") to guide plant operators in evaluating their cybersecurity posture. This manual is not directive and does not establish a minimum level of security. It replaces a three-page 1996 guide, which does not mention cybersecurity.

> "Increasingly, as a means of reducing costs, increasing efficiencies or making better use of technology investments, organizations are integrating physical security devices for access control, monitoring and process control into the IT infrastructure. This collision of two different technology worlds, each coming from a separate management approach and protection philosophy, does not always come together easily. The differences in design, functionality, implementation, maintenance and management can present conflicts, possibly resulting in a security breach involving the IT systems, the security systems or both."[6]

In 2005, the IAEA prepared new guidelines on "Security of Information Technology Related Equipment and Software Based Controls Against Malevolent Acts" aimed at combating the danger of computerized attacks by outside intruders or corrupt insiders.

### 2.7.2 Authentication

Actionable information requires that it be actually and exactly what is claimed, fully trustworthy in accordance with the facts, and of definite origin from a given, known source. The process of authentication performs this guarantee and must be integral with any operational, safety, security or safeguards information system. Typically, for externally transmitted data, it is encrypted using public-key technology and may only be successfully decrypted by the recipient when using the authentic, corresponding private key. International safeguards data is also protected from alteration or substitution using digital signatures or other cryptographic authentication. Information restricted to internal systems may be unencrypted, but this assumes fool-proof firewalls and an absence of insider threat.

---

[6] *Convergent Security Risks in Physical Security Systems and IT Infrastructures*. The Alliance for Enterprise Security Risk Management.

### 2.7.3 Verification

Verification refers to the requirement that authenticated data must establish its correspondence with the actual facts or details subsumed in the original output, measurement, or sensor activity. Systems must be designed to transmit correct, full, and complete information. Often, this includes periodic sending of state-of-health messages to indicate that the system is operating correctly even in the absence of alarms, sensor hits, or other transmissions.

### 2.7.4 Validation

Validation in the IT sense is the attestation of the correctness of a system. This involves examining and testing hardware and software components to determine that they correctly perform their designed functions and nothing more. Importantly, they must not include extraneous code that could, for example, clandestinely transmit sensitive information or provide a backdoor login for unauthorized access.

# 3.0 Integration Framework

A proposed framework for integrating and harmonizing SOSS elements into the design process is illustrated in Figure 1. The elements of this framework are briefly described below. More detailed descriptions are provided in the subsequent sections of this chapter.

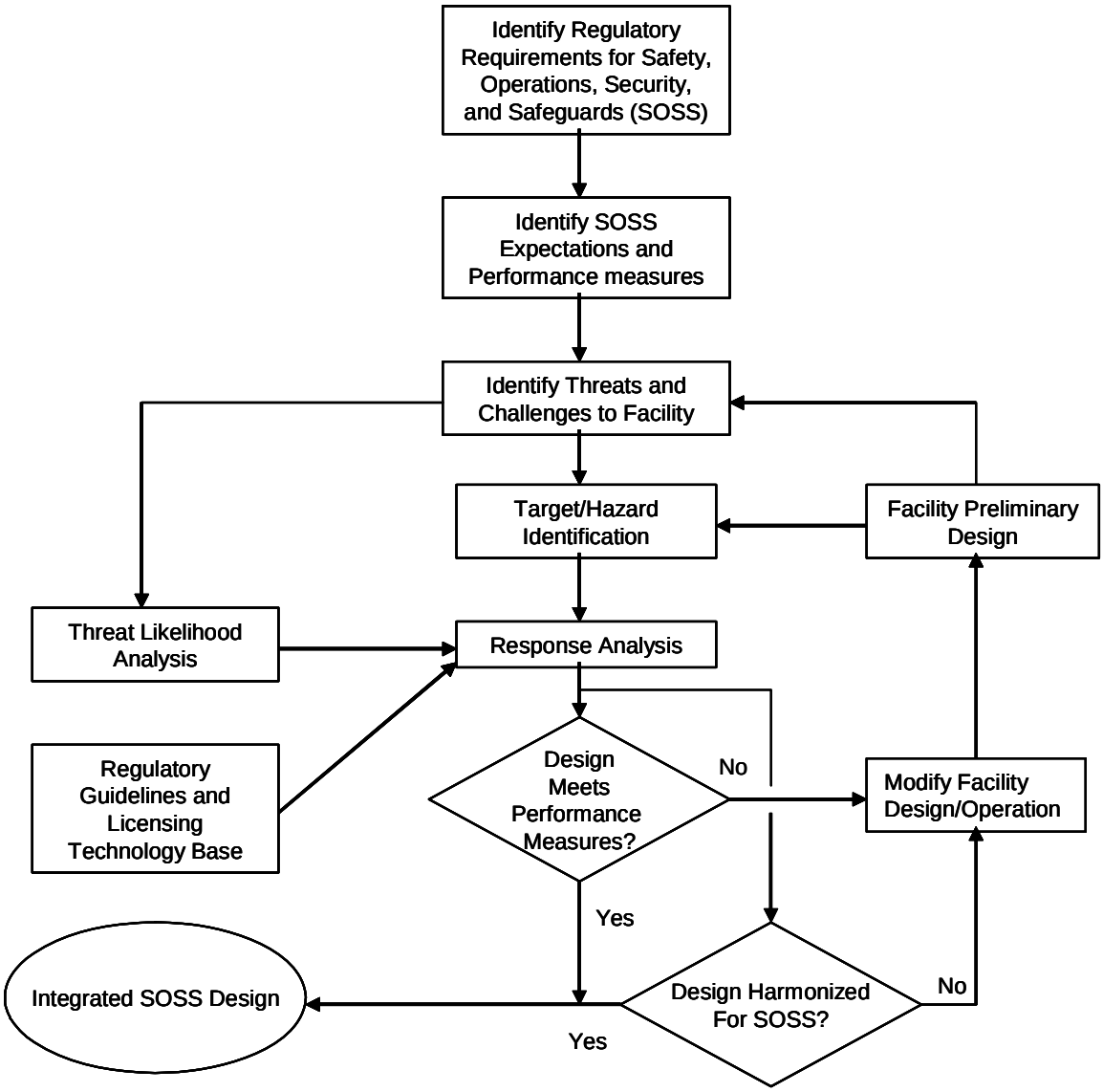



**Figure 1. Framework for integrating SOSS during the design process.**

## 3.1 Elements of Proposed Framework

### 3.1.1 Identify Regulatory Requirements for Safety, Security, and Safeguards

The first step in integrating SOSS into the design process is to clearly identify the regulatory requirements for each of the three elements. The NRC will be the regulatory body charged with licensing future nuclear facilities. The NRC requirements for future nuclear facilities are evolving and may contain a combination of prescriptive, risk-informed, and performance-based regulations. This aspect is discussed further in Section 3.2.

### 3.1.2 Identify SOSS Expectations and Performance Measures

The adequacy of a facility's design is ultimately determined by whether it meets the regulations. The regulations, particularly risk-informed and performance-based regulations, will likely utilize a set of performance measures and expectations in determining the adequacy of a design. Both deterministic and probabilistic criteria can be utilized to ensure defense-in-depth. For example, the NRC's safety goal policy combined with the expectation that advanced reactors will have enhanced margins of safety provides the current NRC expectation related to the safety of reactors. In addition, high-level performance measures can be used in the evaluation of a preliminary design with regard to each SSS element. For example, the performance of a facility's security systems could include measures such as delay time or detection time as well as the overall probability of interrupting an adversary. Different high-level criteria may be utilized to evaluate different levels of design (e.g., qualitative criteria such as having redundancy could be used during a conceptual design phase as an operational requirement, but functional reliability values could be used to evaluate the final design). Performance measures are discussed further in Section 3.3.

### 3.1.3 Facility Preliminary Design

The initial conceptual design for a new nuclear facility will likely be focused on meeting a set of functional requirements (e.g., producing X metric tons of transuranic fuel). However, the facility design must also address accident prevention and mitigation. In many instances, redundancy provided in a facility to improve the operability of the facility will also provide a safety benefit. Similarly, safety-related design features can also benefit the security of the facility (e.g., a structure designed to withstand tornados also is beneficial for withstanding some security threats). Similarly, the physical separation of required safety systems can also be beneficial from a security aspect. However, design features required for safety can also be detrimental to security concerns (e.g., a door that is required to be unlocked for safety reasons could have a negative impact on security). The task of ensuring that SSS are integrated into each step of the design process is the goal of the *Design Analysis Process*. It is an iterative process that strives to harmonize the design to meet all SOSS requirements, expectations, and performance measures in a cost-effective manner. Section 3.3 provides a discussion on the different steps in this process, which are outlined below.

### 3.1.4 Design Analysis Process

The analytical process for evaluating SSS involves several common steps. Both qualitative and quantitative analyses can be effectively utilized and include Failure, Modes, and Effects Analysis

(FMEA), PRA, and vulnerability assessment (VA). The degree to which qualitative and quantitative methods are used can vary depending on the stage of the facility design (e.g., qualitative methods may be the focus during early design stages) and the type of facility (e.g., a PRA would be required for a reactor but an integrated safety assessment may suffice for a fuel reprocessing facility). Although individual SSS analyses can be performed, the analysis groups are required to identify interactions between the resulting facility design features.

#### 3.1.4.1 Identify Threats and Challenges to the Facility

The first step in the evaluation of the SSS needs in a facility is to identify the potential threats or challenges to the facility. With regard to safety, the challenges generally include random failure of equipment leading to accident initiators, internal hazards such as fire and flood, and external events such as natural phenomena and accidents at nearby facilities. DBAs are typically used to establish the safety-related accident mitigation features. PRAs can be used to establish that the facility design is adequate to handle all reasonable accidents (e.g., those with frequencies greater than 1E-7/yr), including those beyond the design basis. For security, a facility is typically designed and evaluated against a DBT. However, in the new era of security concerns, VAs can be performed to ensure security systems can effectively address a full spectrum of threats, including some beyond the DBT. The evaluation of safeguards systems and operations is focused on insider threats diverting material.

#### 3.1.4.2 Target/Hazard Identification

The targets or hazards that are of concern will be a function of the type of facility. For reactors, the hazardous material is contained in the reactor core and the spent fuel pool. Accidents that can lead to reactivity insertions or disrupt the cooling of the material in these areas are the primary safety concern. From a security perspective, both of these sources also represent sabotage concerns. In addition, theft of the hazardous material should also be considered (including that of unirradiated fuel that contains SNM). Accident mitigation equipment and support structures can also be potential targets. Fuel reprocessing facilities can have similar radioactive hazards and targets, as well as significant chemical hazards. Theft of material, whether by an external or internal threat, is of concern in reprocessing facilities where SNM is present. Developing a systematic process for identifying targets and hazards would benefit the SSS evaluations.

#### 3.1.4.3 Response Analysis

Separate analyses should be performed to determine the necessary features required to respond to SSS threats, since a single analysis may not be feasible. However, analyzing the plant to each threat determines the SSCs required in the facility to respond to DBAs and other accidents and the DBT and other threats, prevent diversion of material, and reduce the risk of operation to an acceptable level. The analyses also identify the operational requirements (e.g., emergency response procedures and limits of operation) necessary to satisfactorily respond to threats and hazards. The plant response analyses should be increasingly more detailed as the design progresses from conceptual to final. For conceptual designs, qualitative or semi-quantitative analyses such as FMEAs may be adequate for identifying the required preventive and mitigation features for responding to SSS threats. However, as the design progresses, detailed quantitative assessment of the design is required using techniques such as PRA and VA. When design or operational information is not yet available, assumptions should be made in the design

evaluation. These assumptions can be translated into design and operational requirements in later versions of the facility design.

To some extent, the different evaluation methods used for safety and security are complementary. Both require the evaluation of the response to similar scenarios, whether they are initiated by random events, external events, or security threats. The use of PRA models is an example of how the same tool can be used in both safety and security assessments. PRA events and fault trees identify which components must fail in order for a particular end state (e.g., core damage in a nuclear reactor) to occur. The same models, when transformed from component failures to component locations, can identify the critical areas that must be protected to prevent that end state from occurring.

To support the facility design evaluation, deterministic analyses are required to evaluate the response of the plant to the different threats. These deterministic analyses can include structural, thermal-hydraulic, criticality, reactor kinetics, and environmental evaluations. Integration of the SSS requirements includes identifying which element is the driver for the deterministic design of a facility (e.g., is the structural strength of a building determined by the design basis earthquake or by the DBT). Establishing the process for integrating the different evaluations required at different design phases is critical to comprehensively designing a facility to address all SOSS concerns in a cost-effective manner.

Alternative features can be identified and evaluated at any phase of facility design. However, in order to provide for an effective design process, the evaluation of alternatives should be performed as early in the design process as possible. Cost-benefit analysis is recommended as one means to evaluate alternative design/operational features.

#### 3.1.4.4 Regulatory Guidelines and Licensing Technology Base

A licensing technology base (both experimental and simulation) is needed to support the response analyses in confirming the safety and security of GNEP facilities. The technology base includes development of computer codes that provide realistic assessments of the facilities to different accidents. It also includes development of advanced security and safeguard technologies for addressing security threats.

#### 3.1.4.5 Comparison of the Design to Performance Measures

At every stage of the facility design, the results of the qualitative or quantitative SSS evaluations are compared against the established regulatory and performance criteria. If it is determined that the facility design or operational features do not meet a specific SSS requirement or performance measure, the facility design must be modified. If the design does meet the individual SSS requirements and performance measures, the facility should be reviewed to determine if the design for each SSS element is harmonized with respect to the other elements.

#### 3.1.4.6 SOSS Design Harmonization

To the extent practical, the teams evaluating SSS should be in constant communication, particularly with respect to the design and operational features each is imposing on the facility. This would allow for the identification of potential conflicts in the design (e.g., door unlocked for safety consideration versus locked for security reasons) and possible solutions. Reviewing the analysis of one team by another can also potentially lead to cross-fertilization of ideas to solve common problems (e.g., physical separation of mitigation systems can address both safety and security concerns) or to utilize common information (e.g., utilize information technology

outputs for multiple applications). In addition, the communication between groups may identify interactions between systems or operations that present risks, which would otherwise be overlooked.

## 3.2 Regulatory Requirements

As mentioned above, the first step in integrating SOSS into the design process is to clearly identify the regulatory requirements for each of the four elements. The NRC will be the regulatory body charged with licensing future nuclear facilities. This section summarizes the requirements associated with physical security for NRC and DOE nuclear facilities.

For NRC facilities, 10 CFR 73 addresses physical protection. Title 10 of CFR 74 addresses MC&A. There are various regulatory guides to assist in meeting the requirements. For current reactors, the major concern is radiological sabotage. Fresh fuel is low enriched uranium and spent fuel is somewhat self-protecting. New reactors that have Pu in the fresh fuel will have significantly more concern related to the theft of fresh fuel.

The subparts of 10 CFR 73 of major interest are as follows:

- 73.1 Design Basis Threat for Theft and Radiological Sabotage
- 73.21 Safeguards Information
- 73.37 Irradiated Fuel in Transit
- 75.51 Stored Spent Nuclear Fuel and High Level Waste
- 73.55 Physical Protection for Reactors against Radiological Sabotage
- 73.56 Access Authorization.

The DOE addresses the DBT in the Design Basis Threat Policy (U) document, which is classified [6]. The DOE DBT specified for a specific type of facility is based on the potential magnitude of consequences at the facility. DOE has numerous regulations for physical security systems, such as the Physical Protection manual [7].

## 3.3 Identify SOSS Expectations and Performance Measures

A basic determination of the adequacy of a facility design is whether it meets applicable regulations (i.e., safety-, safeguards-, and security-related regulations as defined by the appropriate governing authorities) and operational expectations (i.e., those expectations placed on the facility by the facility owner or owners). The SSS regulations, particularly those that are risk-informed and/or performance-based, will likely utilize a set of performance measures and expectations in determining the adequacy of a design. For those regulations that identify specific performance measures, the performance measures contained in the regulations must be identified and the facility must be designed such that it meets or exceeds those performance measures. For the applicable regulations that only include general expectations (rather than specific performance measures), specific performance measures must be identified and agreed to by all relevant organizations. For operational expectations, the facility's owner must first define what those expectations are and then define what performance measures will be tracked to ensure that the facility is meeting its operational expectations.

Both deterministic and probabilistic criteria can be utilized to ensure defense-in-depth for both types of performance measures (i.e., those defined by the appropriate governing authorities and those defined by the facility's owner). For example, the NRC's safety goal policy combined

with the expectation that advanced reactors will have enhanced margins of safety provides the current NRC expectation related to the safety of advanced reactors, such as the Advanced Burner Reactor. Table 1 provides an example of how to document the performance measures that must be considered during the design of a facility.

**Table 1. Example Documentation of Performance Measures Considered During the Design of a Facility**

| Performance Measure Basis | Performance Measure | Discussion/Description of Performance Measure |
|---|---|---|
| **Applicable "Regulations"** | | |
| NRC Safety Goal Policy Statement | The *qualitative* safety goals are as follows:<br><br>-Individual members of the public should be provided a level of protection from the consequences of nuclear power plant operation such that individuals bear no significant additional risk to life and health.<br><br>-Societal risks to life and health from nuclear power plant operation should be comparable to or less than the risks of generating electricity by viable competing technologies and should not be a significant addition to other societal risks. | *Quantitative* objectives are to be used in determining achievement of the *qualitative* safety goals:<br><br>-The risk to an average individual in the vicinity of a nuclear power plant of prompt fatalities that might result from reactor accidents should not exceed one-tenth of one percent (0.1 percent) of the sum of prompt fatality risks resulting from other accidents to which members of the US population are generally exposed.<br><br>-The risk to the population in the area near a nuclear power plant of cancer fatalities that might result from nuclear power plant operation should not exceed one-tenth of one percent (0.1 percent) of the sum of cancer fatality risks resulting from all other causes.<br><br>Quantitative estimates of risk may be generated using various techniques (e.g., a probabilistic risk assessment). |
| **Operational Expectations** | | |
| Plant Electrical Generation Goal | Unit 1 Capacity Factor<br>Unit 2 Capacity Factor | If Units 1 and 2 capacity factors are greater than or equal to 90%, then Electrical Generation Goal will be achieved. |

## 3.4 Design Analysis Process

Both qualitative and quantitative analyses can be effectively utilized in the SOSS design analysis process. Examples include FMEA, Integrated Safety Assessment (ISA), PRA, diversion path

analysis (DPA), and VA. The degree to which qualitative and quantitative methods are used can vary depending on the stage of the facility design (e.g., qualitative methods may be the focus during early design stages) and the type of facility (e.g., a PRA would be required for a reactor, but an ISA may suffice for a fuel reprocessing facility). The ultimate goal of the integrated design analysis process is to move to a risk-informed approach for all disciplines. This would provide a common base for evaluating the design across each discipline and would allow for a more simplified approach to decision making when considering design trade-offs, since a common basis would exist for comparing different designs.

### 3.4.1 Identify Threats and Challenges to Facility

For security evaluations, the current practice is to evaluate the security system for threat scenarios based on the DBT. This is similar to a safety evaluation based on the set of DBAs. That is, the likelihood of the DBT (or DBA) is not addressed, but the ability of the systems to prevent consequences given the DBT (or DBA) is evaluated. Section 2.5 discussed techniques used to evaluate the effectiveness of a security system.

To date, the likelihood of threat scenarios has not been addressed in a complete way. The threat for security is analogous to the initiating event for safety: both specify the likelihood of the event of concern and both can be evaluated using a risk-based approach as discussed in Section 5.4. However, the risk-based approach for security differs from the PRA approach used for safety (also discussed in Section 5.4). Using the approach in Section 5.4, both safety initiating events and threat scenarios are quantified as a frequency, and can therefore be compared; however, the evaluation must include uncertainty, and uncertainty of the likelihood of a threat scenario (an intentional, malevolent act with large epistemic uncertainty) is significantly larger than the uncertainty of a random event, such as an earthquake.

### 3.4.2 Target/Hazard Identification

When performing a SOSS evaluation of a nuclear facility, it is necessary to use a systematic process to identify targets and hazards. This section describes a process for identifying the targets and hazards pertinent to each SOSS discipline and how they interact. The targets or hazards of concern will be a function of the type of facility (e.g., power reactor, fuel reprocessing facility, or FFF).

Both qualitative and quantitative analyses can be effectively utilized to identify targets or hazards. Analysis techniques include FMEA, ISA, PRA, DPA, and VA.

#### 3.4.2.1 Safety-Related Target/Hazard Identification

For reactors, the hazardous material of primary concern is the radioactive material contained in the reactor core and spent fuel storage locations (e.g., spent fuel pool).[7] The primary safety concerns are accidents that can lead to reactivity insertions or disrupt the cooling of the material in these areas. Additional safety concerns involve any materials (e.g., gases and chemicals) that could adversely affect the equipment or humans that provide cooling or reactivity control for the radioactive material in the reactor core or spent fuel storage locations.

[7] Radioactive material may be located in water or air filters; however, these locations usually do not contain sufficient quantities of material to be of concern. This should be verified for each facility design.

Given the complex nature of reactors and the potential for substantial consequences resulting from accidents, a PRA is typically employed to determine the frequency of accident sequences and to identify the specific SSCs that comprise the accident sequences. These accident sequences represent specific paths through the event trees[8] that are used in a PRA. Fault trees[9] are used to identify the specific combinations of undesired events that comprise those events that make up the accident sequences.

Information obtained from the accident sequences analyzed using event trees and fault trees, along with any information from the analysis of materials that could adversely affect equipment and humans (such as those that provide cooling and reactivity control) constitute safety-related targets that, if attacked, would lead to unacceptable safety-related consequences. This information is one of the necessary inputs to ensuring that security understands what must be protected (from a safety-related viewpoint).

For fuel reprocessing and fuel fabrication facilities, a PRA may be used to identify potential safety-related targets and hazards. If a PRA is not used, then a consequence approach similar to that utilized in DOE safety basis analyses may be employed.[10] This approach identifies the risk drivers at the facility at the design phase and ensures that sufficient safeguards are in place to reduce the risk from the facility to acceptable levels. The approach used to identify targets may be dictated by the licensing authority. Regardless of the approach used, the safety-related information obtained by the analysis provides the security system design team with a list of items that need protecting.

#### 3.4.2.2 Operations-Related Target Identification

Currently, the process of identifying operations-related targets is somewhat less defined than the process for identifying safety-related targets.[11] Before operations-related targets can be identified, the facility owner must create a list of unacceptable operations-related events (e.g., process flow must not be interrupted for more than one hour or generation of electrical power must not be lost for more than 24 hours). To generate this list, the facility owner must understand the impacts associated with either the loss of the facility or the degradation of some aspect of the facility's function with regard to financial considerations, public confidence, potential for additional regulatory oversight, etc. Once this list of unacceptable operations-related events has been identified, a structured approach should be employed to identify the set of targets that, if attacked, would result in the unacceptable operations-related events. As with

---

[8] An event tree is an inductive logic diagram. It begins with an initiating event or condition and progresses through a series of branches that represent expected system or operator performance that either succeeds or fails. Each path (through the tree) represents a single scenario that ultimately arrives at either a successful or failed end state.

[9] A fault tree is a deductive logic diagram. If depicts how a particular undesired event can occur as a logical combination of other undesired events.

[10] 10 CFR Part 830, *Nuclear Safety Management*, requires contractors and operators of DOE nuclear facilities to develop and maintain a Safety Basis. There are several orders, standards, and guidance documents that are used in developing the safety basis. In particular, DOE-STD-1189-2006, *Integration of Safety into the Design Process*, provides the guidance for integrating safety into the design process of a nuclear facility.

[11] Regulatory agencies typically have very specific unacceptable consequences that must be prevented. Unacceptable operational consequences are typically not specifically enumerated. Their definition (if they are defined) is typically left to the facility owner.

safety-related targets, these operations-related targets are another necessary input to ensuring that security understands what must be protected.

#### 3.4.2.3 Safeguards-Related Target Identification

The identification of safeguards-related targets (either domestic or international) involves the following:

1) the characterization of SNM (e.g., determining category [I, II, III, or IV] and attractiveness [A, B, C, D] of all SNM items at the facility based on type, quantity, and attractiveness level) at the facility;

2) an SNM roll-up characterization (e.g., from the container level to the facility level);

3) a description of the locations at which SNM is stored the majority of time; where it is moved and how often; whether it is removed from its primary container; and how, when, and where it is removed and stored for shipments and receipts;

4) a description of the SNM size and portability, including material state (powder, liquid, metal versus non-metallic, etc.); and

5) the physical systems (e.g., cameras and sensors) and administrative processes (e.g., two-person rule) used to ensure that SNM is always where it is supposed to be.

With this information, safeguards-related targets can be identified. It should be noted that safeguards-related targets may be either the SNM itself or the physical systems and administrative process that, if defeated, could allow the uninhibited removal of SNM. These safeguards-related targets are another of the necessary inputs to ensuring that security understands what must be protected.

#### 3.4.2.4 Security-Related Target Identification

Security-related target identification is the process of identifying specific safety-, operations-, and safeguards-related areas or components that must be protected to prevent undesirable consequences. There are three steps in the identification of targets: specifying undesirable consequences,[12] selecting a technique for security-related target identification,[13] and using the technique identified in step 2 to identify the actual targets (i.e., the protection set or sets) that are to be protected.

---

[12] This step is actually accomplished as part of the safety-, operations-, and safeguards-related target identification process. Undesired consequences are typically specified by the regulatory authority (e.g., US NRC, DOE, or Environmental Protection Agency), but may need to be defined by the facility owner for undesirable operations-related consequences (e.g., unexpected loss of bulk processing cannot exceed 8 hours).

[13] Given the complex nature of commercial nuclear power plants, one technique that may be employed to identify the security-related targets is to use logic diagrams to identify vital areas (vital area identification or analysis) [1] [2]. Vital area identification is a structured approach based on using fault trees (i.e., logic diagrams) to identify the areas containing structures, systems, and components that, if destroyed or damaged by sabotage, result in the release of sufficient radioactive material such that the undesired safety-related consequence occurs. This technique can be modified to include the identification of areas that contain operations- and safeguards-related targets.

Other nuclear fuel cycle facilities could employ the same vital area identification technique or could use some comparable identification process.

Because protecting everything is neither possible nor practical, effective security protects a minimum, yet complete, set of items necessary to prevent the undesired consequences as defined in step 1. Safety-related undesirable consequences generally fall into two categories: those from radioactive material theft[14] and those from radiological sabotage. Operations-related undesirable consequences may have several categories. Safeguards-related undesirable consequences are typically associated with theft of material. Thus, all undesirable consequences should be considered during the design and evaluation of a physical protection system (PPS).

When target identification is concerned with safety-, operations-, and safeguards-related consequences, there may be choices of target sets to protect[15] (e.g., protection of selected components within selected systems that are redundant and/or diverse that may prevent loss of the function provided by the selected components even if other components of other systems are sabotaged). That is, safety, operations, and safeguards concerns may sometimes be addressed by protecting one set from among a number of sets of items. The selection of a set to be protected is determined by the ease of providing protection and the operational impact of providing protection.

The selection of a limited set of components to be protected is intended to minimize the difficulty of providing protection. The PPS is designed to protect a minimum number of components (or targets) to a high degree. This set of components (targets) must be complete; that is, protection of the minimum set must completely prevent the undesirable results regardless of what happens to the other components (targets) not included in this protection set. This selection process is typically accomplished in two phases: identifying vital areas within the plant, and then identifying the potential protection sets (i.e., the targets) and the subsequent selection of one (or more) set(s) to protect [1]. This selection of one (or more) protection set(s) allows the PPS designer to focus on providing protection to this set (of locations and subsequently components or activities within the locations). Such a focus should allow the designer to develop an effective and cost-efficient PPS.

The basic steps used to identify vital areas in a nuclear facility are summarized in Figure 2. The first step defines the levels of radioactive release or theft and operational impacts that are of concern.[16] These levels, in turn, determine the release, theft, or operational thresholds that must be considered and help to establish the required scope of the analysis. The second step identifies the sources of radioactive material in the plant from which a release in excess of the defined limit could occur and from which theft could occur. Additionally, the sources (i.e., the facility activities) that could impact operations must be determined. The third step identifies the facility operating states (e.g., for power reactors, the operating states include power operation, refueling

[14] Theft means unauthorized removal of material (e.g., radioactive or SNM) from the facility to an off-site location for later use. Thus, the targets to be protected are the material in various physical locations within the facility

[15] A target set is sometimes referred to as a protection, minimal target, minimal vital area, minimum critical location, or top event prevention set.

[16] The levels associated with release or theft that are of concern will be defined by the appropriate regulatory authority (e.g., the US NRC). The levels of operational impact must be defined by the facility owner.

outages, and all other intermediate operating states or conditions).[17] The fourth step identifies the actions by which significant amounts of material could be released[18] or stolen. Additionally, actions that can affect the facility's operation are identified. The functional and/or system failures that could lead to radioactive release, theft, or operational impacts must be determined in the fifth step.[19] To identify vital areas, it is necessary, in the sixth step, to determine all the locations in the plant at which each failure can be accomplished.[20] The final step in vital area identification involves solving the fault trees developed in step 5, having transformed each failure into its corresponding location or locations. The locations that form the solution of the sabotage fault tree constitute the vital areas for the plant (see Figure 3 for an example of the top part of the sabotage portion of the fault tree).

Identifying the possible protection sets may be accomplished by taking the Boolean complement of the fault tree, selecting one location from each of the cut sets making up the solution of the sabotage fault tree until all possible combinations have been identified, or some other technique that produces comparable results (e.g., *Top Event Prevention in Complex Systems* [2]). With these results (i.e., the sets of targets that must be protected), PPS designs can be developed, balancing desired protection effectiveness against the cost associated with protecting a particular target set.[21]

### 3.4.3 Response Analysis

**Deterministic Analysis.** Both safety and security concerns require deterministic analyses. For example, the fragility of a building as a function of the magnitude of an earthquake is of concern for a safety evaluation. The structural integrity of a building in response to explosives of varying types and sizes is of concern for a security evaluation. Both safety and security need deterministic analyses to support consequence evaluations.

---

[17] Some of the equipment necessary to prevent release of radioactive material during one operating state may not be required, or may not be available, during another; thus, it may be appropriate to identify different sets of vital areas for the different plant operational states.

[18] Three types of release mechanisms are considered: direct dispersal, induced criticality, and radioactive decay heating. It must be determined whether any of these mechanisms can cause an off-site release of radioactive material from any of the sources identified.

[19] This typically involves the development of a plant-specific sabotage fault tree, where the top event in the fault tree is release of (sufficient) radioactive material from the plant from each potential source for each plant operating state. Because of the redundant, safety-based design of nuclear power reactors, this step is the most complicated part of the process. However, because it is expected that any new power plant will have performed a probabilistic risk assessment for the particular reactor design, a substantial portion of the work necessary for this task may already have been completed.

[20] The identification of locations involves determining the physical location of each component (e.g., actual location of a pump) or theft target and the locations of all electrical and instrumentation/control cabling and other equipment that supports the operation of the component or prevent or monitor theft.

[21] It must be noted that if the design of the facility or operational parameters change, systems or components are added, or their locations change, then target set identification may need to be performed again to ensure that the changes have not affected the identification of the protection sets.

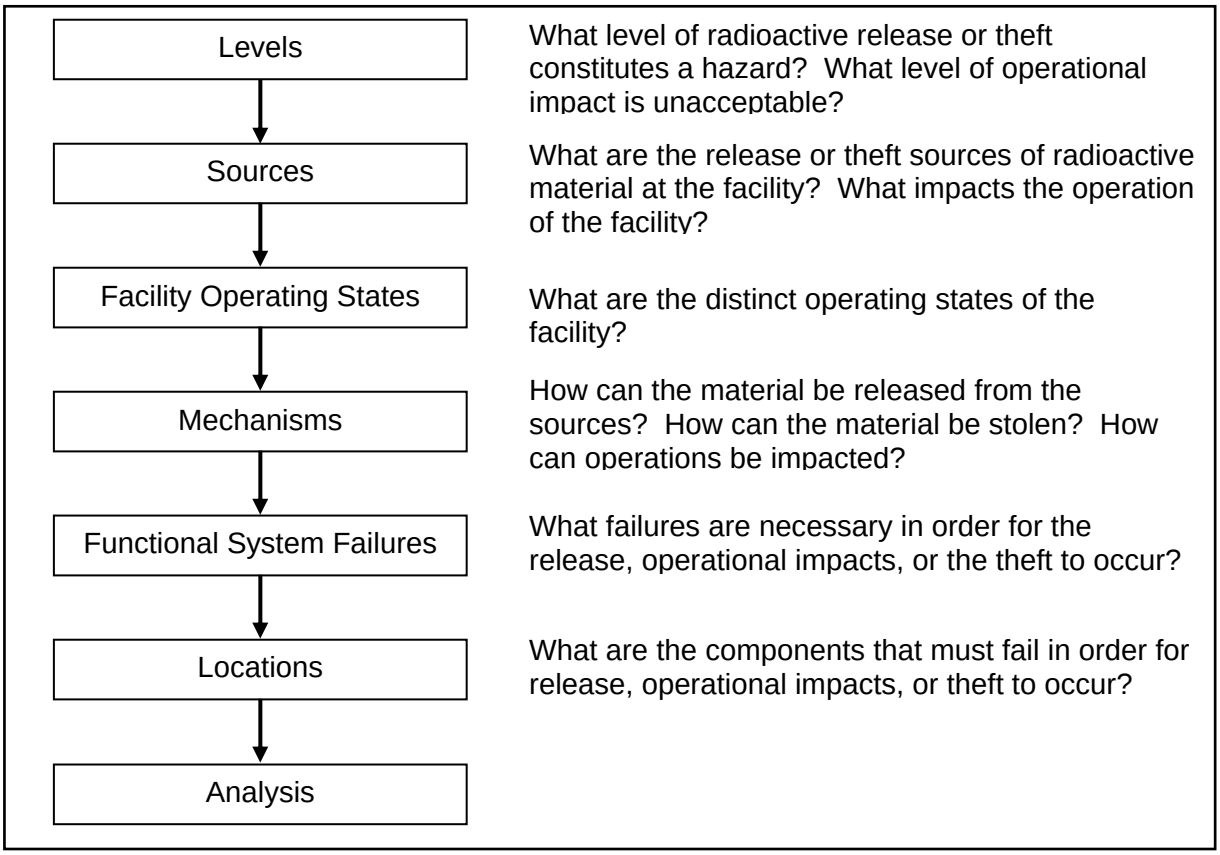



**Figure 2. Steps in Vital Area Identification**

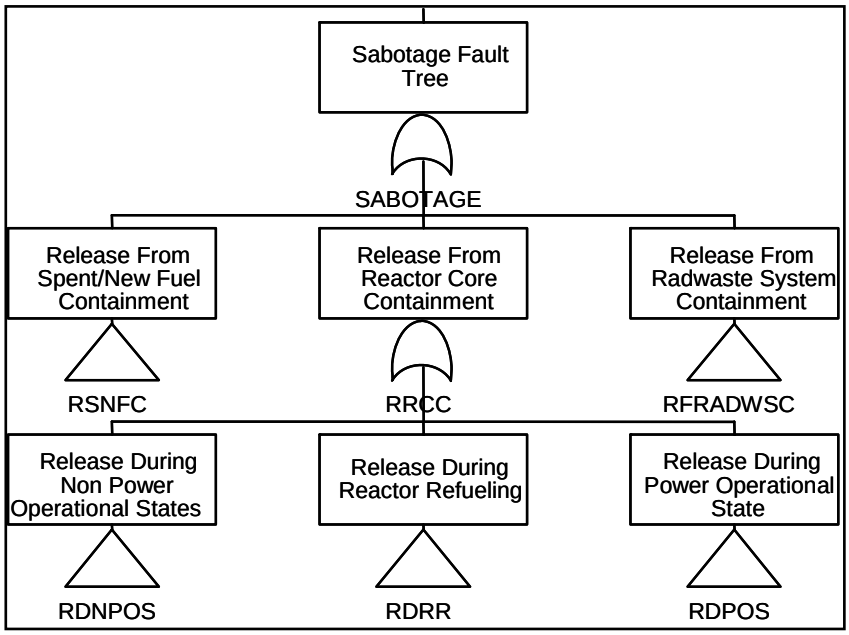



**Figure 3. Example of the Sabotage Portion of a Fault Tree**

**Data Needs.** Safety requires a database on the frequency of initiating events and the response of components (e.g., probability of failure) that comprise protection systems. Security requires a database on the performance of detection and delay elements to specific adversary attributes.

**Risk Analysis.** Both safety and security need an evaluation of risk to identify the initiating events of most concern and to evaluate the effectiveness of systems designed to prevent and reduce consequences. Risk analysis can be used to optimize the design of both safety and security systems to complement the consideration of only DBAs and DBTs.

As discussed elsewhere in this report, safety uses PRA to evaluate risk, but security requires an extension of PRA to address epistemic uncertainty to evaluate risk. This is discussed further in Section 5.4.

### 3.4.4 Comparison of Design to Performance Measures

At every stage of the facility design, the results of the qualitative or quantitative SOSS evaluations are compared against the established regulatory and performance criteria. If it is determined the facility design or operational features do not meet a specific SOSS requirement or performance measure, the facility design must be modified. If the design does meet the individual SOSS requirements and performance measures, the facility should be reviewed to determine if the design for each SOSS element is harmonized with respect to the other elements.

### 3.4.5 SOSS Design Harmonization

Safety and security concerns have many similarities. Both are concerned with preventing similar severe consequences by designing systems to counter initiating events. Both utilize SSCs, as well as procedures and controls over personnel as part of the system to prevent severe consequences. Both interface with operations—safety interfaces with operations to address worker safety, and security interfaces with operations to address the insider threat. Both safety and security can be evaluated using a risk measure as discussed elsewhere in this report.

Conversely, there are differences between safety and security concerns. Safety-related design and evaluation requires details of the design, consequences of concern, and operations. These details, however, may actually make it easier for an adversary to gather information for an attack. Thus, the desire to provide open access to information for safety purposes can be at odds with the desire to prevent such information from being used for malevolent purposes.

The need for rapid, unimpeded egress of personnel during an emergency can conflict with the security need to prevent loss of control of personnel and opening of doors through barriers. An emergency can create a chaotic egress of personnel from areas, buildings, and through the access control posts to offsite locations. A false emergency could be part of an attack plan to degrade the security system and divert response.

During the design phases for a facility, consideration of security can take advantage of the similarities between safety and security. Since both are concerned with similar consequences, the criteria for siting the facility can include security considerations as well as safety considerations. For example, the seismicity of a region is an important criterion for siting from a safety perspective. The site characteristics that dictate the ease of detecting and assessing the adversary, and the response tactics for defeating the adversary should also be considered. Population density is another important consideration for both safety and security.

The layout of buildings, areas with buildings, and operations within buildings should consider security requirements in the design phase to lessen the impact of security elements for detection, delay, access control, and response. Also, the layout can be designed to optimize and reduce the cost of intrusion detection systems, and controls over entries and exits into buildings and areas of concern with buildings. Structures designed to contain radionuclides released during an accident can also be designed to withstand a blast from explosives. The shielding required to protect workers from exposure to radiation during normal operations can be designed for use as a delay barrier for the security system; care must be taken in the design to ensure that such barriers cannot be used by an adversary entrenched inside the facility to delay response. Strategies to mitigate consequences—such as sheltering and evacuation—can be coordinated and designed to address both intentionally caused consequences as well as similar consequences resulting from a safety-related initiating event. Access control for both safety and security can be coordinated with operational requirements in the design stage. The emergency egress system can be designed to safely channel evacuating personnel along secure pathways to secure locations within the site perimeter.

In the early part of the 20$^{th}$ century, safety considerations were incorporated into the design of manufacturing operations to improve worker safety. For new facilities, the challenge is to similarly integrate security considerations into the operations to address the insider threat. For facilities designed without consideration of the insider, the back-fit of controls directed at the insider can have a severe impact on operations. In the design phase, concepts for segregating operations can be considered. Also, the segregation of information is an important aspect of addressing the insider threat to make it more difficult for an adversary to gather sufficient information from one individual. Better screening and processing of potential employees can be used to make it more difficult for an adversary to plant a malicious insider as part of the facility staff.

The concepts of Assured Security previously discussed in Section 2.5 can be used to harmonize security with safety and operations for a new facility. The evaluation of safety and security concerns can be harmonized by a consistent evaluation of the two throughout the design process, not just as an add on activity at the end. For example, threat scenarios within the DBT serve the same purpose as the set of initiating events in the DBAs: both drive the basic requirements of the safety and security systems and lead to SSCs to prevent similar consequences. For an overall evaluation beyond the DBT and DBAs, risk assessment can be used.

For a new facility, risk assessment is important to systematically identify scenarios outside the DBT of concern, so that, in the future, changes to the security system in response to changes to the DBT can be accomplished in a more effective, less costly manner.

# 4.0 Enabling Tools and Techniques for ISOSS

This section identifies some enabling tools and techniques that can facilitate integrating SOSS. This includes multi-disciplinary use of IT systems, integrated risk analysis tools, cross-training in SOSS requirements, and a formalized design/operation review process. Additional techniques and tools may be possible.

## 4.1 SOSS IT Integration

As nuclear facilities become larger and more complex, distributed data collection systems must be used to monitor activities in the facility and to bring the resulting data to a central data repository for use by the operators, security personnel, and inspectors. This allows safety and security personnel to have timely and accurate data while domestic and international inspectors are better able to use their time on site reviewing data, rather than visiting the various monitoring systems to collect data storage media (as would be the case if several autonomous data collection systems were used at the facility).

Unfortunately, the data security issues with connecting these computers in a network are nontrivial. In order to ensure that the data is authentic, the system must be protected from possible attacks everywhere in the network. It is not practical to consider physically protecting the network cables and computers not owned by the IAEA from tampering. Also, the virtual private network (VPN) technology that is used for transferring the data over public networks is sometimes unsuitable for the network architectures inside operational facilities.

In 2006, the IAEA issued a new policy regarding sharing of equipment and data; details about how best to implement this new policy is still being worked. The introduction of this new policy and the evolution of the implementation guidance indicate that those working on systems that will be proposed for joint use among operators, States' regulatory authorities, and the IAEA must not assume that existing sharing agreements will serve as models for future agreements.

One of the driving factors for the new policy was the realization that if an operator had knowledge of the data that would be used to verify a declaration before that declaration is made, the declaration could be modified to take advantage of the small errors present in any measurement data to divert material. As processing plants become larger, exploiting these small measurement uncertainties can result in the diversion of large quantities of nuclear material.

The policy is also intended to raise awareness of the IAEA's requirement for authentication of the equipment and computers used to collect the data that will form the basis for safeguards conclusions. Simply stated, the IAEA must be assured that the data collection equipment gives accurate results that cannot be surreptitiously modified by the adversary, and the data from that equipment must also be protected from modification between the sensor and the data review station.

Figure 4 shows a notional data collection infrastructure that could be shared among the IAEA, the plant operator, and the State's regulatory authority. Data collected from the various measurement systems can be collected in the Inspectorates' Cabinet (IC), which can be shared between the IAEA and the State's authority. A typical processing facility might have several of these cabinets. The data may then be moved to the Raw Database (RDB), another shared computer. Both the IAEA and the State's authority can then retrieve the data from this database for review.

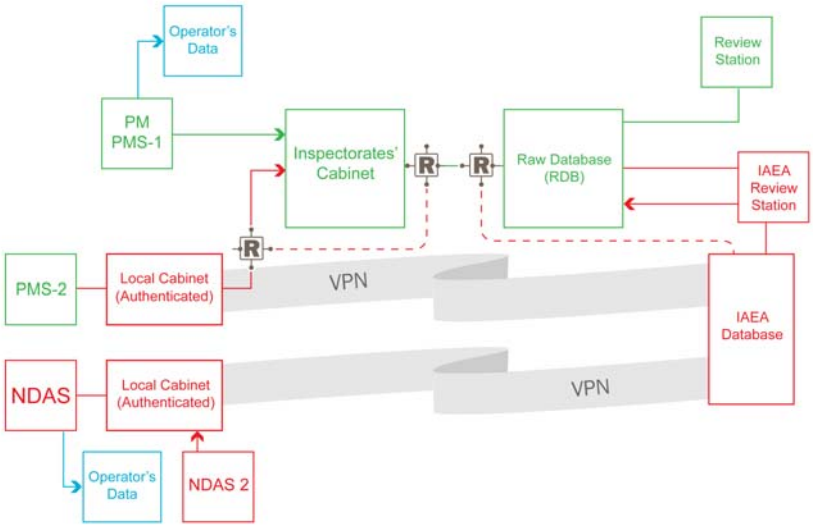



**Figure 4. Notional Data Collection Infrastructure**

Data that is considered sensitive by the IAEA would be protected from disclosure by encrypting it at the source. One means of accomplishing this is by employing virtual private network (VPN) technology to establish an encrypted tunnel on the network. For this to work, a means for bypassing both the ICs and the RDB must be provided. This can be done by installing routers at key locations as shown by the boxes labeled "R" in the diagram. In this way, all but a few meters of the shared data cabling in the facility can be employed without compromising the IAEA's security standards.

The process monitoring system (PMS) PMS-1 is a measurement system used and controlled by the operator for monitoring the plant process. Because the IAEA has no assurance of authenticity of the equipment or the data coming from the equipment, the data should be used with caution. However, inspectors could use the data to gain insight into the plant's operation, which can enhance confidence that the plant is operating as declared.

The PMS-1 system has no authentication measures implemented. The sensors and other system equipment are not protected with any tamper-indicating technologies, and the data itself bears no cryptographic authentication. As the data comes from the measurement system, it goes directly to both the operator and the IC.

PMS-2 is a system that has been authenticated by the IAEA and is protected inside the IAEA's sealed tamper indicating enclosures (STIE). The computer inside each STIE adds a cryptographic digital signature to each data packet before it is forwarded through the data collection system. The data from this system is shared between the IAEA and the State's authority and might be shared with the operator as well.

Non-destructive assay system (NDAS) hardware is similarly authenticated and sealed to ensure that the data collected from the system is authentic. The IAEA directly shares the data with the operator and the State's authority. The system has been augmented with other measurement

equipment, designated as NDAS-2, to provide enhanced accuracy. This data would be protected from disclosure by using VPN technology.

After the operator's declaration has been received by the IAEA, the IAEA may share some of the data that had been protected from disclosure by uploading it to the RDB.

The data collection system for the Rokkasho Reprocessing Plant is an example of the problems encountered in a large facility and a workable solution to these data security problems that generally follows the architecture described above. This facility is very large, with activities being monitored in several large buildings. The IAEA's approach to monitoring these activities was to install one or more "local cabinets" (LC) in each building. Each cabinet contained one or more computers collecting surveillance or nuclear measurements data. These LCs are connected to an IC, which is shared between the IAEA and the Japanese Safeguards Office (JSGO). There is one IC per building, each of which are supplied and maintained by JSGO and the Nuclear Material Control Center. Data is buffered at the IC before being forwarded to the RDB, which is also provided and maintained by the Japanese. The IAEA downloads the safeguards data from the RDB to IAEA computers in the IAEA inspectors' office for storage, review, and analysis.

Each LC is housed in a tamper indicating cabinet that is sealed with an IAEA seal. Since the network cables and computers in the network are not all under control of the IAEA, the LCs must be protected from the threat of attack over the network. The data must also be protected from alteration or other modifications while in transit through the network to the IAEA computers.

Network attacks are addressed by using a Netscreen VPN appliance inside each LC. The system architecture at this facility does not allow active connections between the computers inside the LC and the IAEA computers; using an encrypted VPN adds no security, so that functionality is not used. Instead, the devices are used as hardware firewalls and are configured to only allow very limited network traffic into or out of the cabinet. Currently, the only network traffic allowed into the cabinets is the network time protocol (NTP) to allow all of the computers to be synchronized to a central time source. Outbound traffic is limited to file transfers using file transfer protocol, with the transfer limited to being initiated by the local computer.

All data is cryptographically authenticated before it is sent out of the LC. Surveillance data from the cameras is authenticated by the DCM 14 camera modules, so no further authentication is required. All other data is digitally signed using the Sign and Forward (SnF) system. The cryptographic tokens used in the SnF system have an internal clock, which is used to verify that the time signals received from the NTP server have not been falsified.

### 4.1.1 Inputs

Data inputs for safety, operations, safeguards, and security share many common elements: video feeds, sensors (radiation, closure, motion, temperature, smoke, etc.), and plant monitoring equipment. Current designs require separate systems and lead to inefficient redundancies, such as a security video camera mounted adjacent to a safeguards monitoring camera.

Reduced installation costs can result from doing careful analysis during the design phase regarding where monitoring devices and sensors will be physically placed. Past experience has shown that retrofitting a completed facility with a new, secondary monitoring system can exceed the cost of the initial installation (such as at Kashiwazaki in Japan). In addition to reducing

installation costs, there will eventually be a reduced need for future maintenance, since redundant systems will be largely eliminated.

Since data security needs to be ensured from the moment of collection, advanced sensors and monitoring systems should provide on-board encryption and authentication. Tamper indicators need to be universally present, yet in an emergency they should be easily and verifiably releasable.

### 4.1.2 Processes

Operations, facility safety, and plant security require real-time access to data; safeguards needs only periodic access to data. The most economical solution to integrating these four processes is to use the data feeds for continuous monitoring (operations, safety, and security) as a source for a portion of the safeguards information. Additional data needed for verifying declarations would remain encrypted (but available in an emergency situation) until after IAEA verification activities have been completed.

Processes that determine system vulnerabilities (for example, network scans of open hardware ports) would have to remain restricted on a need-to-know basis to appropriate members of facility staff and national regulatory authority members. Such a process or the conclusions based on the process could never be shared with an external entity, such as the IAEA.

### 4.1.3 Storage and Transmission

The major hurdle to shared resources for SOSS is the requirement that plant declaration data be independent of information used for IAEA verification. This need implies that data streams used by plant operators to verify a declaration be encrypted after inspectors have verified those declarations. The data would also need to be authenticated at the point of use. Encryption would have to extend from the source instrument, over the facility network (whether secure Ethernet, wireless, or some combination), to the facility data storage and, if necessary, to any off-site information consumers.

It is essential that the data that will be used to draw safeguards conclusions is authentic. It must be known that the data originated from the intended source, that the data was not changed in transit, and that it is not a repeat or delayed copy of previous data. One approach to ensuring this authenticity is to maintain a secure physical boundary around the equipment taking the data and then to physically secure the data media until it can be loaded onto trusted equipment for review and evaluation. In other words, the equipment is sealed inside a tamper indicating enclosure until the inspector takes the data to his headquarters for review. As the number and complexity of sites being monitored increases, this approach becomes unwieldy—due to the labor costs involved and the difficulty in maintaining physical security on the large amounts of data an inspector has collected from multiple pieces of equipment. An alternative approach is to use cryptography to put a digital authentication code or digital signature on the data. Once this cryptographic data authentication has been applied, the security requirements for transporting the data to the review location are much less stringent.

The work done by Gus Simmons and Paul Stokes in the early 1970s on authentication for remote seismic monitoring systems[22] was quite likely the first time that cryptography had been applied to the problem of data authentication. Although their algorithm was not fielded in the Deployable Seismic Verification System, the concept of authentication that was used was the same.

From the beginning, however, the key management problems associated with this approach to data authentication were troublesome. These early systems were based on symmetric key cryptography, which required that the same key be used both for signing and for verifying the authentication. In a bilateral or multilateral situation, anyone who could verify the authentication could also generate bogus data that appeared to be authentic. There were also problems associated with maintaining the security on a large number of secret authentication keys as they were loaded into the equipment and as they were used by the inspectors in the field.

The development of public key cryptography in the late 1970s offered a solution to this key management problem. Using this cryptography, different keys are used for the signing and verifications processes. The private (secret) key only exists in the monitoring device, while anyone wishing to verify the authenticity of the data can have a copy of the public key without compromising the security of the private key. Unfortunately, the calculations involved were very complex and these public key algorithms could not be deployed in the seals and camera systems of the day because the microprocessors required to perform these calculations would quickly drain the batteries.

Recent developments in microprocessors and in cryptography are now allowing systems to be developed that will include public key signature technology. The Next Generation Surveillance System currently under development by Canberra Albuquerque and Dr. Neumann Consultants will employ public key cryptography. The new Secure Sensor Platform under development by SNL and Canberra Albuquerque will also use public key technology in a very low-power device.

The IAEA developed the SnF data authentication system to have a standardized approach to authentication for its unattended and remote monitoring systems where other authentication measures are not already built into the sensor platform. In this system, an extra layer of physical security is added by using dedicated cryptographic hardware tokens to store the keys and to perform all the cryptographic calculations. This system is currently being deployed worldwide.

VPN technology was developed to allow secure communications over public networks. This was very attractive to the safeguards community due to the high cost and questionable security of leased lines, satellite, and other approaches to collect data from remote monitoring sites.

The first implementation of a VPN to transfer safeguards data internationally was deployed by SNL to transfer data from Finland to Vienna in 1999. Since then, the IAEA has deployed VPN technology in Korea, Japan and several other locations worldwide.

The VPN technology was chosen to be deployed in dedicated hardware devices rather than to use software running on the data collection/data server computers. The use of these certified and tested modules simplifies installation and improves security while reducing the probability that

[22] G.J. Simmons, R.E.D. Stewart, P.A. Stokes, "Digital data authenticator." Patent Application SD2654, S42640, June 30, 1972.

the VPN configuration will be maliciously or accidentally modified by users or by other software running on the computer.

A single data transmission backbone (a "Modular Common-User Facility Information Infrastructure"[23]) will be needed for a truly integrated SOSS system. Such a universal data bus will need to transmit physical protection data, MPC&A information, Safeguards containment and surveillance data, and monitors for production processes and safety. In turn, the data bus will have to provide timely, secure, authenticated, validated, and accurate information to the security response force, IAEA inspectors, facility operators, and other vested information shareholders.

### 4.1.4 Data Security

Simple physical access to a computer can be exploited to gain access to an otherwise secure platform. Mechanisms to manage physical access to servers, network hardware, and backup media will need to be put in place to minimize opportunities for compromising data.

If a single centralized database management system is envisioned for data storage, careful attention should be paid to administration of users and their privileges. Typically a master database administrator account has access to all subsidiary user accounts. Use of the master administrator account will need to be tightly controlled. Modern database management systems allow for the control of data input, editing, deleting, and viewing at the individual record and field level. Careful design of the logical database structure will permit administrative separation of data that needs to be kept from certain audiences.

The entire information infrastructure of the facility will have to employ industry-standard best practices for network security: firewalls, password control, user training, administrative mechanisms, system security patches, etc. Safety systems will have to be carefully integrated with security protocols to avoid possible misuse of, for example, fire alarm pulls to create breaches in plant security or to allow adversaries to take advantage of authentic emergencies.

## 4.2 Integrated Risk Analysis Tools

For the evaluation of risk for safety, PRA is an accepted, proven technique. Numerous tools are available to assist in the performance of a PRA, such as Saphire and Crystal Ball [8] [9]. Important aspects of PRA are the consideration of uncertainty and dependence.

To date, few tools have been developed to evaluate the risk of a threat scenario, other than simple tools that evaluate point estimate values for threat, vulnerability, and consequence. Section 5.4 discusses new tools that have been developed to evaluate the risk of threat scenarios, including uncertainty. These tools address the considerable epistemic uncertainty for threat scenarios using a super set of probability called belief/plausibility.

The BeliefConvolution code evaluates algebraic combinations of numeric variables using the belief/plausibility measure of uncertainty; that tool also evaluates the belief/plausibility of fuzzy sets defined for numeric variables.

---

[23] "Enhanced Safeguards based on Expanded Information Availability in New Nuclear Facilities," Tom Sellers, June 2007. Sandia National Laboratories International Security News, SAND2007-2950 P.

Many of the variables of importance for the evaluation of threat scenarios cannot be easily evaluated numerically, as discussed in Section 5.4. The LinguisticBelief code evaluates combinations of purely linguistic variables with approximate reasoning using the belief/plausibility measure of uncertainty.

Risk for both safety and security can be quantified as a consequence per unit time. For safety, if PRA is used, risk can be expressed as a complementary cumulative probability distribution. For security, if the numerical model is used, risk can be expressed as two bounding curves: a complementary cumulative belief distribution and a complementary cumulative plausibility distribution. For security, if the linguistic model is used, risk can be expressed as two bounding curves: a complementary cumulative belief distribution and a complementary cumulative plausibility distribution over the purely linguistic fuzzy sets for risk.

## 4.3 Cross-Training in SSS

The simplest way to help integrate SOSS in a facility design is to cross-train the personnel involved in each discipline with a basic (i.e., general) understanding of the requirements for the other disciplines. For example, facility designers concerned with operational characteristics would receive cross-training in the areas of SSS. This cross-training would help ensure that as operational design decisions were made, they were made after considering the effects such decisions would have on the other disciplines. Similarly, providing training to SSS personnel on the basic aspects of the other disciplines will help alleviate potential conflicts in the overall facility design. This cross-training does not eliminate the need for experts in each discipline, but rather is envisioned as one means of integrating the SOSS design process.

## 4.4 Formalized Design/Operation Review Process Enabling IT

Information technologies form a substantial foundation that enables critical aspects of formalized design. Fairly mundane capabilities such as routine backup (and if necessary, restoration), version control, workflow routing, and electronic approvals are now expected to be a standard part of the design process. Electronic task tracking, e-mail, calendaring, messaging, scheduling, and project management are all elements of the overall design process toolset. IT and communications form an indispensable foundation to formal design methodologies regardless of whether they are carried out with separate applications or by means of integrated systems, or custom-built or commercial-off-the-shelf.

### 4.4.1 Sharing Design/Operation Information

Documents that provide highly detailed views of plant layout, infrastructure design, security system components, and critical safety mechanisms would have to remain closely controlled. Serious implications would result if architectural plans, wiring diagrams, as-built diagrams, and even interior photographs are released to an adversary. Means of designing in safeguards systems without compromising overall facility security will have to take into account the difficulty of physical design verification by foreign nationals working for the IAEA.

Enabling information technology methods such as the use of controlled CAD drawings can help the design and SOSS groups with the communication of information needed to integrate and harmonize the SOSS elements into the design.

### 4.4.2 Procedural Process for Design/Operation Approval

To ensure that an integrated SOSS design is achieved, all design features and operational requirements should be reviewed and approved by each discipline before it is incorporated into the facility. This should also include all maintenance considerations and limiting conditions of operation. Including this procedural requirement would provide a mechanism to force each discipline to review a proposed design or operational feature with regard to how it would influence the performance of their systems or operations. This action would provide the detailed evaluation of the design process by each discipline that can only be superficially addressed by the cross-training enabling process mentioned above.

# 5.0 Required Developments to Effectively Integrate SOSS

A framework for integrating SOSS elements in the design of a nuclear facility has been delineated in Chapter 3. Although the enabling tools and techniques identified in Chapter 4 will facilitate the integration process, additional developments are required. This chapter identifies those developmental needs.

## 5.1 Integrated Risk-Informed SOSS Regulations for New Nuclear Facilities

The current requirements for SSS that exist in NRC regulations do not explicitly address GNEP and other proposed nuclear facilities. For example, the current licensing requirements for reactors address light water reactors and not liquid metal reactors, and current safeguard requirements specifically exclude reprocessing facilities. The current requirements can be used as a basis, but ultimately, new guidance will be required. The NRC has begun work on establishing requirements for future GNEP facilities that may contain a combination of prescriptive, risk-informed, and performance-based regulations. As such, an opportunity exists to support the NRC in establishing the regulatory requirements and licensing framework necessary to license these facilities.

## 5.2 Performance Measures

High-level performance measures can be used in the effort to integrate SOSS elements into a preliminary facility design. For example, the performance of a facility's security systems could include measures such as delay time or detection time as well as the overall probability of interrupting an adversary. Different high-level criteria may be utilized to evaluate different levels of design (e.g., qualitative criteria, such as redundancy, could be used during the conceptual design phase as an operational requirement and functional reliability values could be used to evaluate the final design).

Both deterministic and risk criteria are currently used to measure safety. For security, the current process is to evaluate the conditional probability that a threat will not cause an undesired consequence. To harmonize safety and security features it is necessary to also establish risk measures for security. This section describes the performance measures that are currently utilized for measuring security and proposes a new process and associated measures for evaluating security-related risk.

### 5.2.1 Current Approach

For safety, the performance measure for the set of DBAs is an evaluation that shows that the protection systems prevent the consequence of concern given a DBA, with bounding assumptions, such as a single failure in the protection systems (active mechanical, active and passive electrical).

For security, the performance for each of a number of threat scenarios within the DBT is evaluated as $P_E \equiv P_I \cdot P_N$. $P_E$ is the security system effectiveness—the conditional probability that the threat scenario can be prevented from causing the undesired consequence, given the attack occurs. $P_I$ is the probability that the security system can interrupt (detect and delay) the threat scenario in time for response. $P_N$ is the probability that the response force can neutralize

the threat scenario. Typically, point estimates are used in the evaluation, but sometimes uncertainty can also be considered.

The conditional risk (CR) (the risk given the threat scenario) is evaluated as CR = (1 - $P_E$) · C where C is consequence. Traditionally, point estimates are used but uncertainty can also be considered.

#### 5.2.1.1 Traditional Equation for Conditional Risk

The traditional equation for conditional risk, CR, for a physical security system is:

$$CR = (1 - P_E) \times C \qquad \text{(Eqn. 1)}$$

where $P_E$ is the effectiveness of the security system in detecting and defeating a specific threat scenario and C is the consequence, given failure to defeat the threat scenario. The risk is conditional on the attack since CR assumes that the threat scenario will occur.

For a specific path for a specific threat scenario, $P_E$ is evaluated as:

$$P_E = \sum_{i=1}^{m} \left( \prod_{j=1}^{i-1} (1 - P_{D_j}) \right) P_{D_i} \, P_{N_i} \qquad \text{(Eqn. 2)}$$

where i ranges over the m layers of the security elements, $P_{Di}$ is the probability of detection at the $i^{th}$ layer, and $P_{Ni}$ is the probability of neutralization given detection at the $i^{th}$ layer.

#### 5.2.1.2 Evaluation of $P_E$

**Point Estimate of $P_E$ with Fixed $P_N$**

For some analyses of security systems, it is assumed that the probability of neutralizing the adversary is a constant, given sufficient time to respond; that is, the effectiveness of response is assumed to be independent of where the response force must respond to. With this assumption, and using point estimate values for the variables in equation 2, the concept of a Critical Detection Point (CDP) is useful. The CDP can be defined as that specific $k^{th}$ layer for which the guard force has sufficient time to interrupt the adversary, assuming the adversary minimizes delay from that point forward, but for layer k+1 the guard force does not have time to interrupt the adversary. Thus, $P_{Ni}$ is a constant for any layer i up to k and is zero for any layer i from k+1 to m. Detection at or before the $k^{th}$ layer is critical, as detection following that layer is useless since there is insufficient time to respond. Let $P_N$ denote the constant value of $P_{Ni}$ for i less than k+1. Using these assumptions equation 2 simplifies to:

$$P_E = \sum_{i=1}^{k} \left( \prod_{j=1}^{i-1} (1 - P_{D_j}) \right) P_{D_i} \, P_N \qquad \text{(Eqn. 3)}$$

where k is the CDP.

**Generalization of Equation for $P_E$**

To facilitate the extension of $P_E$ to more complicated cases, we need to model $P_{Ni}$ to greater detail. For effective neutralization (given detection), the guard force must:

- correctly assess the situation (decide that the detection is not a false/nuisance alarm or a diversion, etc.),

- have sufficient time to interrupt the adversary before the adversary completes the attack, and
- engage and defeat the adversary.

$P_{ASSESSi}$ is the probability that the guard force correctly assesses the threat scenario given detection at layer i. $P_{TDi}$ denotes the probability of timely detection at layer i, defined to be the probability that the guard force can respond in time given detection at layer i. $P_{TDi}$ is a function of $T_{ADVi}$ and $T_{GRi}$, where $T_{ADVi}$ is the time for the adversary to complete the scenario from layer i and $T_{GRi}$ is the time for the guards to respond given detection at layer i, including the time required for assessment. $P_{WINi}$ is the probability that the guard force defeats the adversary given they engage the adversary given detection at layer i. With these definitions, we can express $P_{Ni}$ as:[24, 25]

$$P_{N_i} = P_{ASSESS_i} \times P_{TD_i} \times P_{WIN_i} \qquad \text{(Eqn. 4)}$$

Equation 2 can be written as:

$$P_E = \sum_{i=1}^{m} \left( \prod_{j=1}^{i-1} (1 - P_{D_j}) \right) P_{D_i} \, P_{ASSESS_i} P_{TD_i} P_{WIN_i} \qquad \text{(Eqn. 5)}$$

If we use point value estimates for each variable, and assume that $P_{Ni}$ is a constant $P_N$, $P_{TDi}$ is 1.0 for any layer i at or before the CDP at layer k, and $P_{TDi}$ is 0.0 for any layer beyond the CDP.

**Point Estimate of $P_E$ with Variable $P_{Ni}$**

Let $P_{Ni}$ be allowed to vary at each layer i. For this case, the concept of a CDP is not meaningful since there may not be just one layer beyond which $P_{TDi}$ is non-zero. Using point estimates for the variables, Equation 5 is evaluated over all m layers with $P_{TDi}$ explicitly evaluated at each layer.

**Evaluation of $P_E$ with Uncertainty Modeled as Probability**

In general, all the variables in Equation 5 have uncertainty, and to consider uncertainty, $P_E$ should be evaluated by convoluting the uncertainty distributions for each variable.

Traditionally, probability has been used as a measure of uncertainty.[26] With this approach, a probability distribution is assigned to the variables of interest and Equation 5 is evaluated by probabilistic convolution of the probability distributions of the constituent variables. The convolution can be performed analytically in some cases or by Monte Carlo or Latin hypercube sampling techniques.

Using probability distributions to solve equation 5, $P_{TDi}$ requires special attention. Given probability distributions for $T_{ADVi}$ and $T_{GRi}$, we can form the probability distribution for

---

[24] Other terms can be added to $P_{Ni}$ if needed.

[25] Assessment of an alarm can be included in $P_D$ instead of $P_{Ni}$. Correctly responding based on that evidence to the correct location—that is, calling the correct "response plan" from the playbook—can be broken out separately.

[26] Probability used for a value, such as $P_E$, is probability in the objective sense, a frequency. Uncertainty in the probability value can be modeled as a probability measure, probability in the subjective sense. [Kaplan and Garrick]

$T_{REMAININGi} = T_{ADVi} - T_{GRi}$, where $T_{REMAININGi}$ is the extra time available for response at layer i. Since we are using probability distributions for $T_{ADVi}$ and $T_{GRi}$, the probability distribution for $T_{REMAININGi}$ can have negative values where the response time is insufficient. If $T_{REMAININGi}$ is negative, there is no neutralization. Therefore, to correctly evaluate $P_{TDi}$ in Equation 2, we want only the part of the distribution for which $T_{REMAININGi}$ is positive; that is, $P_{TDi}$ = Probability ($T_{REMAININGi} > 0$), or equivalently $P_{TDi}$ is the probability that $T_{REMAININGi}$ exceeds 0. For clarity, this value for $P_{TDi}$ will be denoted as $P_{TD\ POSITIVEi}$ For discrete probability distributions,

$$P_{TD\ POSITIVE_i} = \sum_{T_j \in T_{REMAINING_i}} p(T_j) \,|\, T_j > 0 \qquad \text{(Eqn. 6)}$$

Where $p(T_j)$ is the probability for the $j^{th}$ value from the set of values for $T_{REMAININGi} = T_{ADVi} - T_{GRi}$.

$P_{TD\ POSITIVEi}$ is a value, not a distribution.

Equation 5 becomes:

$$P_E = \sum_{i=1}^{m} \left( \prod_{j=1}^{i-1} (1 - P_{D_j}) \right) P_{D_i}\, P_{ASSESS_i} P_{WIN_i} P_{TD\ POSITIVE_i} \qquad \text{(Eqn. 7)}$$

where each term is evaluated by convolution, with $P_{TD\ POSITIVEi}$ being a point value in that convolution.[27]

### 5.2.1.3 Evaluation of C and CR

An uncertainty distribution is defined for the consequence C. If more than one type of consequence is to be considered, once the separate constituents of C have been assigned a common measure, C is calculated by adding the separate consequences using convolution.

For example, if C is comprised of a set of n separate consequences, then:

$$C = \sum_n C_n \qquad \text{(Eqn. 8)}$$

where the $C_n$ are expressed using a common measure, such as willingness to pay.

Once $P_E$ and C have been evaluated, then CR is evaluated using Equation 1 by multiplication using convolution.

That is, the final equation to be evaluated is:

$$CR = (1 - \sum_{i=1}^{m} \left( \prod_{j=1}^{i-1} (1 - P_{D_j}) \right) P_{D_i}\, P_{N_i}) \; x \sum_n C_n \qquad \text{(Eqn. 9)}$$

[27] Equation 7 suffers from the repeated variable type of dependence, e.g., $P_{Dj}$. Evaluating equation 7 with sampling techniques automatically resolves the repeated variable problem.

### 5.2.2 Risk Performance Measures

There are two problems with the current approach for measuring security system performance: the likelihood of the initiating event—the threat scenario—is not addressed, and epistemic uncertainty is not considered.

Using PRA for a safety analysis, risk parameters can be used as performance measures. These risk parameters are generally shown as probability distributions that reflect epistemic uncertainties in the models and data inputs. Using the URA approach described in Section 5.4, a similar risk performance measure can be used for security that uses a belief/plausibility methodology. The URA approach addresses both of the problems with the current evaluation of security, in that the likelihood of the threat scenario is considered and epistemic uncertainty is considered.

## 5.3 Threats and Challenges

Threats to the facility are the threat scenarios of concern. The threat is ever changing, as indicated by the significant changes in the DBT since September 11, 2001. Better techniques to identify and rank order the threat scenarios of concern are needed for a new facility design to prevent costly modifications in the near term in response to an ever-changing threat. The risk approach is a technique that can evaluate the wide range of possible threat scenarios to rank order those of concern using the risk metric.

By opening up the evaluation to use risk instead of being constrained to the DBT, issues can be identified and addressed in the design phase. Of course, no prediction of the future is perfect. As discussed in Section 2.5 in the discussion of the dynamic aspect of assured security, the last-resort options can be considered in the design to provide protection for threats outside the capabilities of the traditional security system. This is exactly analogous to the weak-link concept currently in use for nuclear weapons safety in that for undefined environments, perhaps beyond the capabilities of the strong links, failure of weak links renders the weapon safe [22].

## 5.4 Integrated Risk Analysis Methods

### 5.4.1 Comparison of Risk for Safety and Security

The evaluation of risk for safety concerns is well established using PRA. Security concerns can also be evaluated using risk, but there are important differences between safety concerns and security concerns that must be considered. First, the similarities are discussed.

In general, risk can be defined as a function of three variables:

- likelihood of initiating event
- probability of failure of protection system(s) given the initiating event
- consequence(s) given failure of the protection system(s)

Note that the probability of failure of the protection systems is conditional on the occurrence of the initiating event. Consequence(s) is conditional on failure of the protection systems.

The initiating event is typically expressed as a frequency. Risk is evaluated for each of a set of initiating events, as the performance of the protection systems depends on the specific initiating event. For example, the response to an earthquake is different than the response to a flood. In

many cases, there is more than one category of consequence of concern (e.g., economic loss and injuries may be of concern as well as deaths).

Two standard measures of risk are used:

- a product, and
- a likelihood of exceedance of consequence.

The product measure expresses risk as the product of the initiating event, the probability of failure of system(s) response, and the consequence(s). Also, risk has the units of consequence per unit time (e.g., deaths/year). The product measure indicates a fundamental property of risk: a low-likelihood, high-consequence event can have similar risk as a high-likelihood, low-consequence event. However, the product measure of risk does not delineate between high-likelihood, low-consequence and low-likelihood, high-consequence events with similar risk. Another measure of risk is the likelihood of consequence, which provides more information than the product measure [10]. The likelihood of consequence is expressed as a graph of the frequency of exceedance of consequence.

Using point estimate values, the product measure of risk is a point value and the likelihood of exceedance of consequence is a single curve. With uncertainty, the product measure of risk is a probability distribution, and the likelihood of exceedance of consequence is a family of curves.

Risk for either a safety or a security concern can be evaluated using either measure for risk. This allows comparison among safety-related initiating events and security-related initiating events. For example, using the product measure of risk, risk from a safety event and a security event both have the units of consequence per unit time.

### 5.4.2 Differences in Evaluating Risk for Safety and Security

There are important differences between evaluating the risk of an event of concern for a safety analysis and an event of concern for a security analysis.

A terrorist attack is not a random event—it involves a specific scenario that is selected, planned, and implemented by the adversary. Consider the failure of a specific building in response to an earthquake, which is a “dumb” random event. The risk from the earthquake considers the likelihood of the earthquake, the fragility of the building (used to calculate the response of the building to the earthquake), and the number of people killed if the building fails. The likelihood and magnitude of the earthquake are independent of the fragility of the building. However, for an intentional terrorist attack against the building, the adversary estimates the resources required to destroy the building based on an evaluation of the fragility of the building, and decides if the potential consequences are worth the effort to bring the resources to bear necessary to destroy the building. The adversary has a choice as to which building to attack, while the earthquake does not.

Most of the uncertainty associated with estimating the frequency of an intentional event is epistemic (state of knowledge), not aleatory (stochastic or random); the probability measure of uncertainty has difficulty capturing epistemic uncertainty.

Many of the considerations for evaluating the likelihood of an intentional terrorist act involve variables that are difficult to evaluate numerically; for example, consider the adversary level of training. Any numeric scale assigned to such a variable is arbitrary and the use of arbitrary

numeric scales leads to numeric results for convoluted variables that are meaningless, as subsequently discussed.

### 5.4.3 Evaluation of Risk for Intentional Acts

We have applied new techniques to evaluate the risk of intentional acts. These techniques were selected based on the following criteria:

- reduce to traditional PRA when the uncertainty is purely aleatory (stochastic),
- capture and propagate epistemic uncertainty, and
- allow purely linguistic variables.

The first criterion is satisfied using the Belief/Plausibility measure of uncertainty; this measure was developed to deal with epistemic uncertainty and both belief and plausibility reduce to the standard probability measure of uncertainty if there is no epistemic uncertainty. The second criterion is satisfied using the standard mathematics for convoluting evidence with belief/plausibility, which is an extension of convoluting probability distributions. The third criterion is satisfied by using pure linguistic fuzzy sets for linguistic variables, and performing linguistic convolution using approximate reasoning. Therefore, we apply the following established techniques:

- Belief/Plausibility measure of uncertainty,
- fuzzy sets for segregation of variables, and
- approximate reasoning for combining linguistic variables.

This new technique is called Uncertainty Risk Analysis (URA); PRA is a subset of this technique. The custom Java software that was developed to implement URA is BeliefConvolution for numeric variables and LinguisticBelief for linguistic variables.

The references provide a detailed description of the URA technique and its application to evaluating the risk of terrorist acts. The next section is an overview of the technique.

### 5.4.4 Overview of URA Technique for Evaluation of Risk for Intentional Acts

First, a general discussion of uncertainty is presented, and then the URA process is presented.

#### 5.4.4.1 Overview of Uncertainty

Each variable contributing to risk has uncertainty. To include uncertainty in the evaluation of risk, each variable is treated as a random variable with a likelihood distribution. The likelihood distributions are convoluted under the appropriate algebraic operations used to evaluate risk.

Over the last 50 years, mathematicians and logicians have developed measures of uncertainty that are more general than probability, and that specifically address epistemic uncertainty. The references provide details.

The belief/plausibility measure of uncertainty from the Dempster/Shafer Theory of Evidence is an extension of the probability measure of uncertainty that can better capture epistemic uncertainty [12]. Belief/plausibility is a superset of probability. Under certain conditions, belief and plausibility both become probability; under other conditions, belief/plausibility become

necessity/possibility, respectively.[28] Belief/plausibility addresses a type of uncertainty called ambiguity, which is the uncertainty associated with predicting an event in the future.

A simple example illustrates the difference between aleatory and epistemic uncertainty, and the use of a belief/plausibility measure. Consider a fair coin, with heads on one side and tails on the other, with each side equally likely. The uncertainty as to the outcome of a toss—heads or tails—is aleatory. The probability of heads is ½ and the probability of tails is ½. The uncertainty is due to the randomness of the toss. Suppose, however, that a person does not know the coin is fair; the coin could be biased to come up heads, or the coin could be two-tailed. The person now has epistemic uncertainty; because his or her state of knowledge is insufficient to assign a probability to heads or tails, the only thing the person knows is that the likelihood of heads (or tails) is somewhere between 0 and 1. To consider epistemic uncertainty as well as aleatory uncertainty, belief/plausibility can be used as the measure of uncertainty. With total ignorance about the coin, the belief that the toss will be heads is 0 and the plausibility that the toss will be heads is 1; similarly, the belief that the toss will be tails is 0 and the plausibility that the toss will be tails is 1. Belief/plausibility form an interval that can be interpreted as giving the lower and upper bound of probability. If a person has enough information, both belief and plausibility reduce to a single value, probability. Figure 5 illustrates this concept. Epistemic uncertainty can be reduced with more information. If the coin is tossed a few times and a head and a tail occur, it is apparent that the coin is two-sided; with more tosses, the fairness of the coin can be evaluated. Aleatory uncertainty cannot be reduced with more information.

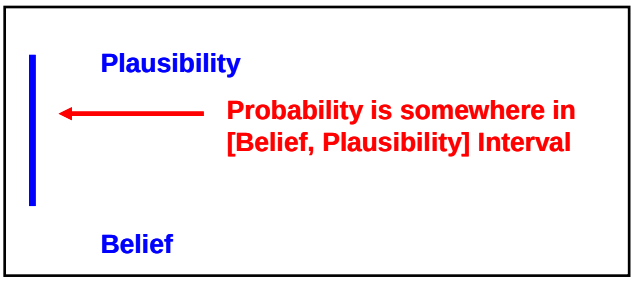



**Figure 5. Belief/Plausibility as Bounds on Probability**

For the belief/plausibility measure of uncertainty, evidence is assigned to intervals, as discussed in the references. Figure 6 is an example assignment of evidence over intervals contrasted with a discrete probability distribution—where the intervals degenerate into specific values.

In addition to ambiguity, we have another type of uncertainty called vagueness. Vagueness occurs when linguistics (words) are used to classify events. For example, yesterday was "sunny," public confidence in the stock market is "high," etc. Vagueness is uncertainty as to how to classify a *known* event. For example, assume that a person knows how tall John is, but instead of saying John is 6 feet 2 inches tall, John is instead categorized as "tall" without a

[28] To be precise, if the focal elements are singletons, belief/plausibility both become probability. If the focal elements are nested, belief/plausibility become necessity/possibility, respectively.

precise definition of "tall." The linguistic "tall" is vague. Vagueness can be addressed using the mathematics of fuzzy sets.

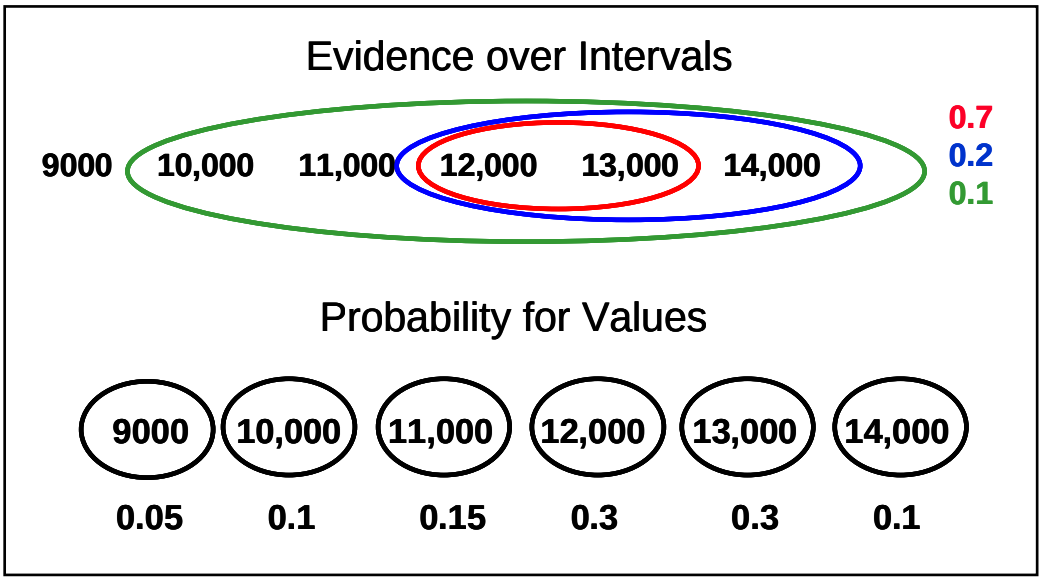



**Figure 6. Evidence for Intervals and Probabilities for Values for Variable "Dow Jones Industrials Close on Dec. 31, 2007"**

A simple example of fuzzy sets is as follows. Consider a random variable for consequence as "the number of deaths from a terrorist attack" for which the range is [0, $10^6$]. For estimating the consequence from a particular scenario, it is better to reason at a higher level than a specific number of deaths for two reasons: there is too much uncertainty to distinguish between, for example, 1000 and 2000 deaths; and when comparing scenarios with widely different consequences, such as blowing up a building versus detonating a nuclear device, there are orders of magnitude of difference in the consequence.

Suppose the range is partitioned with crisp sets commensurate with the "accuracy" to which consequence is to be measured; for example, [0, 10), [10, 100), [100, 1000), [1000, $10^4$), and [$10^4$, $10^6$]. There are defined sets, subsets of the range, at the "fidelity" to which we wish to reason. Names can be assigned to these sets, such as "minor" for [0, 10), "moderate" for [10, 100), "high" for [100, 1000), "major" for [1000, $10^4$), and "catastrophic" for [$10^4$, $10^6$]. A name has also been assigned to the crisp sets of interest, but a problem has occurred with these sets. The consequence is "high" if 999 people die, but if 1000 people die, the consequence is "major." While the crisp sets solve the problem of reasoning at too fine a level, they suffer from the problem of sharp boundaries. Ideally, 999 deaths should be considered both high *and* major to some degree, which can be done by making the sets fuzzy. Specifically, "minor" is defined as "up to *about* 10," "moderate" as " between *about* 10 and *about* 100," "high" for "between *about* 100 and *about* 1000," "major" for "between *about* 1000 and *about* $10^4$," and "catastrophic" for "greater than *about* $10^4$." Degrees of membership mathematically define these fuzzy sets as indicated in Figure 7.

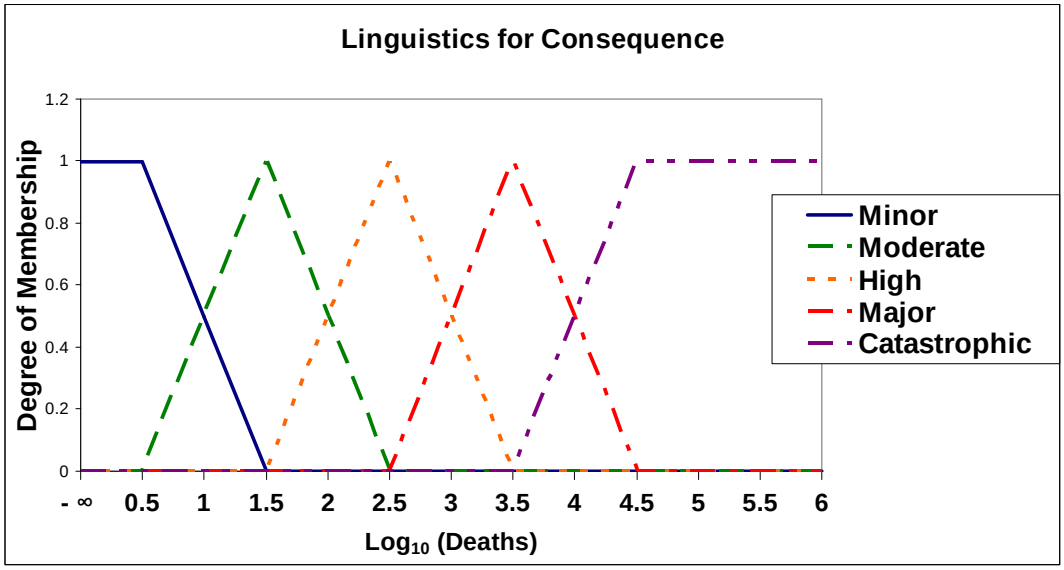



**Figure 7. Fuzzy Sets for Consequence (Deaths)**

Uncertainty involving both ambiguity and vagueness can be addressed by extending belief/plausibility to fuzzy sets. [11] Thus, the belief/plausibility measure of uncertainty can be applied to fuzzy sets as well as to crisp sets.

For example, given degrees of evidence assigned to crisp intervals in the range for deaths, such as 0.7 for [10, 1000] and 0.3 for [1, 50,000], the belief/ plausibility can be calculated for the fuzzy sets defined for deaths in Figure 7.[29] For "minor," belief/plausibility is 0/ 0.65. For "moderate," belief/plausibility is 0/ 1. For "high," belief/plausibility is 0/ 1. For "major," belief/plausibility is 0/ 0.65. For "catastrophic," belief/plausibility is 0/ 0.3.

The application of belief/plausibility to purely linguistic variables is discussed in the next section.

### 5.4.4.2 The URA Process for Evaluating Risk of Intentional Acts

The URA process has the following attributes:

- **Scenarios are evaluated by risk, where Risk is a combination of threat, vulnerability, and consequence.** Threat is the frequency of the scenario, vulnerability is the probability that the scenario is successful, and consequence is the undesirable result of a successful scenario.
- **Risk is evaluated from both the adversary and the defender perspectives.** Specifically, threat is evaluated from the perspective of the adversary; Vulnerability and consequence are evaluated from the perspective of the defender. The adversary *is* the threat, but has uncertainty for both vulnerability and the consequence. The defender knows the vulnerability and consequence better than the adversary, *given* the threat, but has considerable uncertainty regarding the threat.

[29] Yager addresses the more general situation where the evidence is also on fuzzy sets. [11]

- **The evaluation is linguistic.** Since the adversary has a choice, all variables of concern to the adversary must be "acceptable" for a specific scenario; otherwise the adversary will select a more "attractive" scenario. Some variables of importance to the adversary, such as "Adversary Technical Expertise" are not amenable to numeric evaluation. The linguistic evaluation is accomplished by using fuzzy sets for each variable and by combining the fuzzy sets with approximate reasoning.
- **The evaluation captures and propagates uncertainty.** Much of the uncertainty is epistemic (state of knowledge) rather than aleatory (stochastic). For example, the threat is not random, it is known with no uncertainty by the adversary; however, the defender has considerable epistemic uncertainty for threat. The evaluation uses the belief/plausibility measure of uncertainty from the Dempster/Shafer Theory of Evidence to handle the epistemic uncertainty.
- **The evaluation provides a simple summary of results for decision making.** Scenarios are rank ordered by the highest non-zero likelihood of exceeding the worst risk value. Likelihood is a belief/plausibility interval and risk value is modeled linguistically using fuzzy sets. The complementary cumulative belief/plausibility distribution is used for the rank ordering.
- **The evaluation uses proven mathematical techniques**. Specifically, fuzzy sets, approximate reasoning, and belief/plausibility are used. All of these techniques are axiomatically defined, as discussed in the references. The implementation of these techniques for evaluating the risk of terrorist acts is described at length in some of the references [15] [18].

**Evaluation of Scenarios.** Risk is evaluated by scenario—a scenario consists of a particular adversary group, adversary resources, a target, and an attack plan. Different adversary groups have different objectives and resources. Adversary resources consist of attributes and knowledge. Attributes include the number of adversaries, their equipment, weapons, technical expertise, etc. Knowledge includes information from numerous sources, such as open literature/web, reconnaissance, and insider assistance.

There is no attempt to mathematically combine "all" scenarios, since the number of scenarios can be infinite. Instead, scenarios, or classes of scenarios, of concern are evaluated individually and rank ordered. Scenarios can be defined and evaluated at any level of detail necessary for the evaluation, since uncertainty is considered. For example, a scenario at a high level may be associated with any of 1000 similar targets, while a scenario at a specific level may be for one specific target.

**Adversary/Defender.** The adversary and the defender each have different states of knowledge and different goals. There is no uncertainty in threat for the adversary because the adversary *is* the threat. The adversary has uncertainty in the vulnerability of the target, which he attempts to reduce by gathering information. Based on an estimate of the vulnerability, the adversary will decide if he has the resources necessary to exploit the vulnerability, and if the potential consequence is worth using those resources for the candidate scenario. The adversary has a specific consequence in mind, and selects those targets that have the potential for causing that consequence. The adversary has uncertainty in the magnitude of the consequence that he attempts to reduce by gathering information and customizing the scenario to maximize consequence. In practice, consequence is a combination of numerous specific types of consequences.

The defender has less uncertainty than the adversary for vulnerability and consequence, given the threat. However, the defender has considerable uncertainty in the threat scenarios that the adversary will select.

The defender is concerned with using available resources to minimize risk. The adversary is concerned with using available resources to maximize consequence.

The adversary and defender may have different consequence measures. The adversary-desired consequences are part of the threat, in that targets with desired consequences are more likely to be chosen. The defender consequences are part of the consequence term in the risk equation in that these are the consequences of concern for risk for the defender. For example, the adversary may consider "Religious Significance" as well as "Deaths" and "Economic Loss" for consequence, while the defender may focus on "Deaths," "Economic Loss," and "Regional Impact" for consequence, as indicated conceptually in Figure 8.

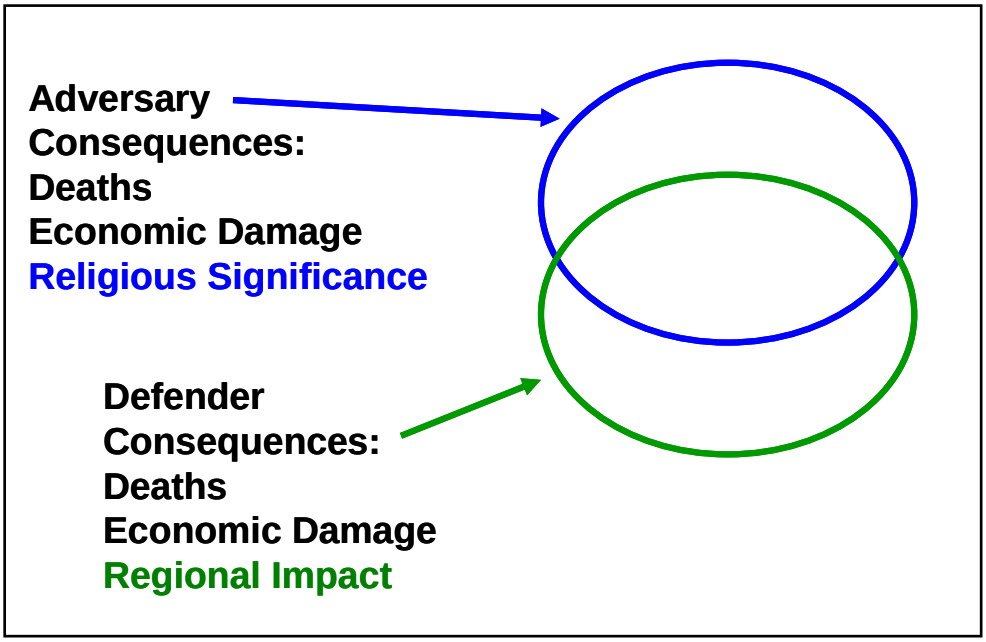



**Figure 8. Adversary and Defender: Different Consequences of Concern**

Figure 9 is an overall picture of the adversary-defender model for risk. Figure 10 is an illustration of implementation of the model in the LinguisticBelief software, discussed later.

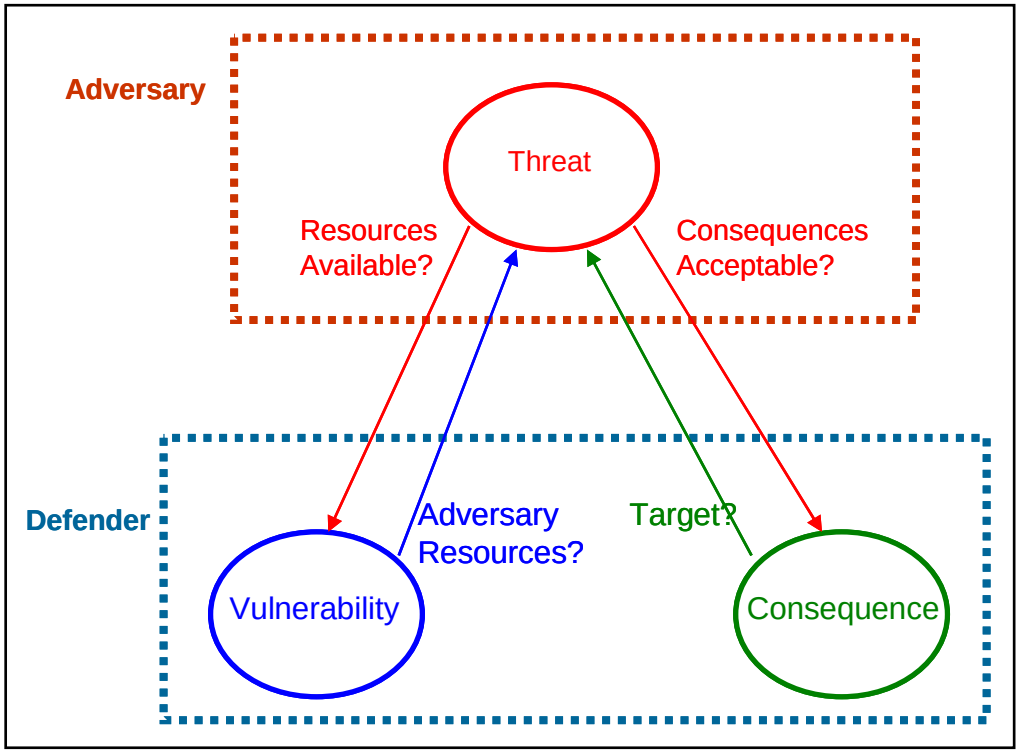



**Figure 9. Overall Adversary-Defender Model for Risk**

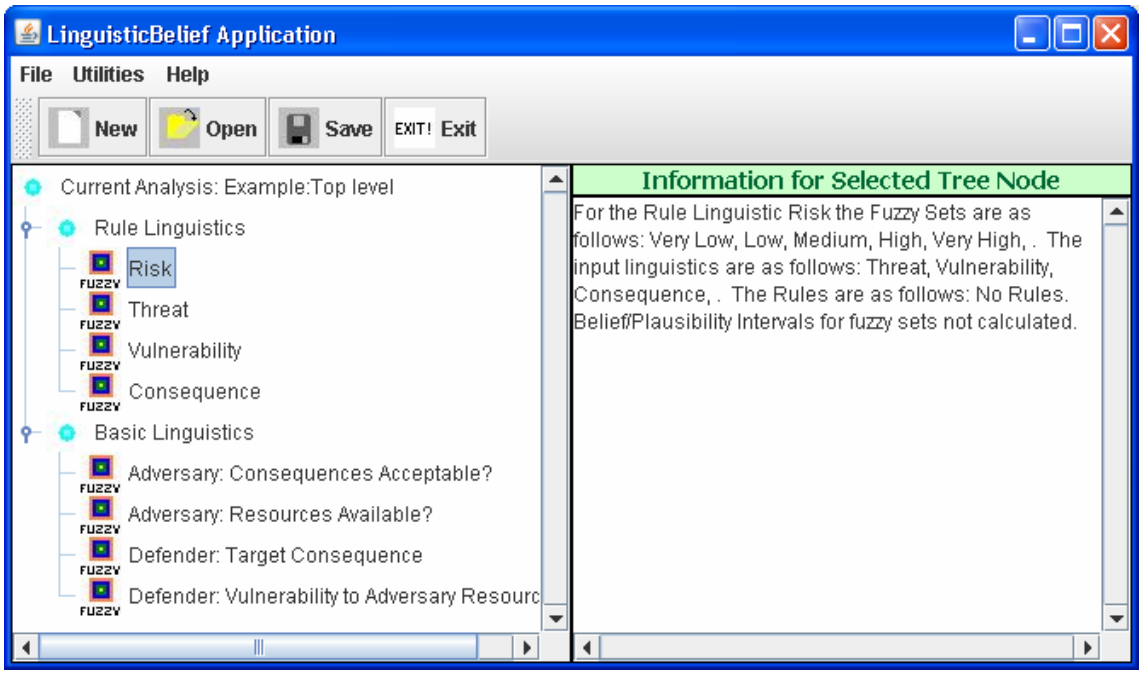



**Figure 10. Overall Adversary-Defender Model for Risk in LinguisticBelief Software**

Figure 11 is a conceptual picture of the Adversary Model. For a given scenario, the defender "thinks like the adversary" to evaluate the Expected Consequence, defined as the consequence if the scenario is successful weighted by the probability that the scenario will be successful.

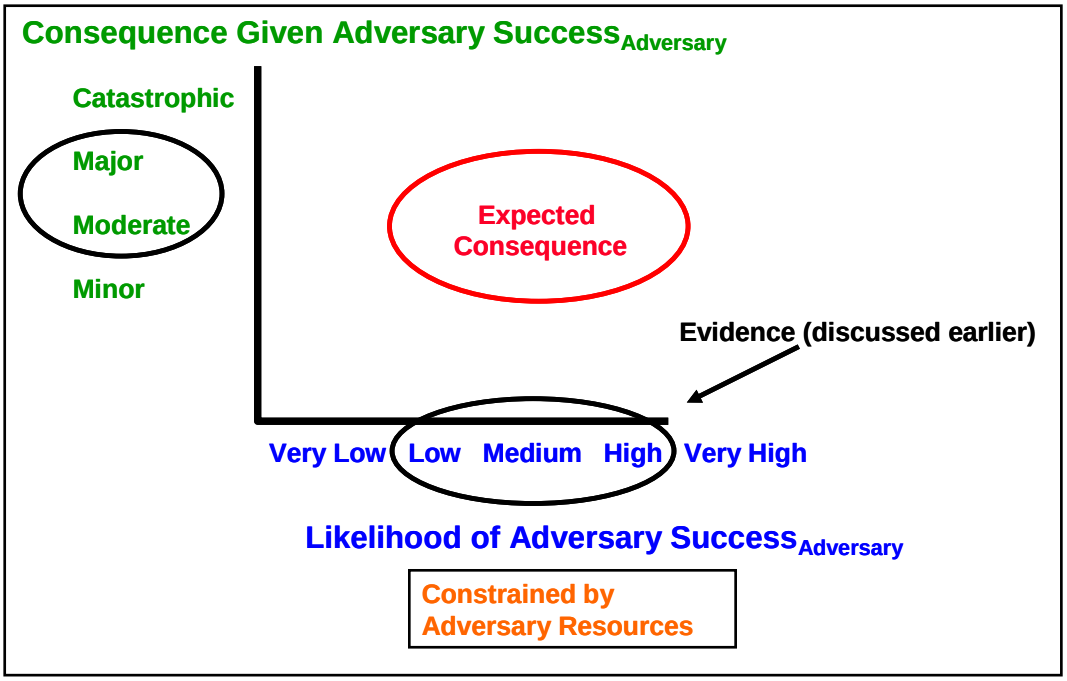



**Figure 11. Adversary Model**

Figure 12 is a conceptual picture of the Defender Model. The defender evaluates the risk of the scenario, using the information from the adversary model for the threat.

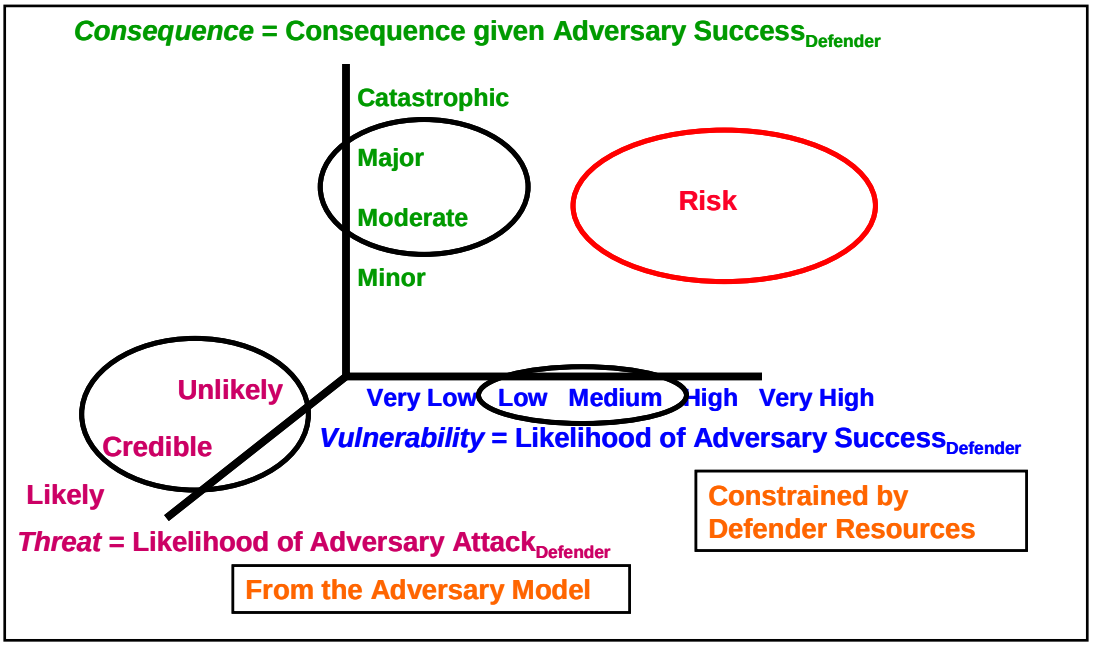



**Figure 12. Defender Model**

**Variables for Evaluation.** At the top level, risk is evaluated from threat, vulnerability, and consequence. Although the evaluation can be done at this level, typically each of these three variables is built-up as a combination of lower level variables. For example, in the Adversary Model, the "Likelihood of $\text{Success}_{\text{Adversary}}$" may be evaluated as a combination of "Adversary Ability to Gather Information," "Adversary Level of Technical Training," "Adversary Estimate of Likelihood of Not being Detected while Gathering Resources," and "Adversary Estimate of Likelihood of Defeating Security System." Consequence is typically a combination of numerous specific consequences as discussed previously.

Each variable is segregated into fuzzy sets. Some variables are numeric and some are not as indicated in Figure 13.

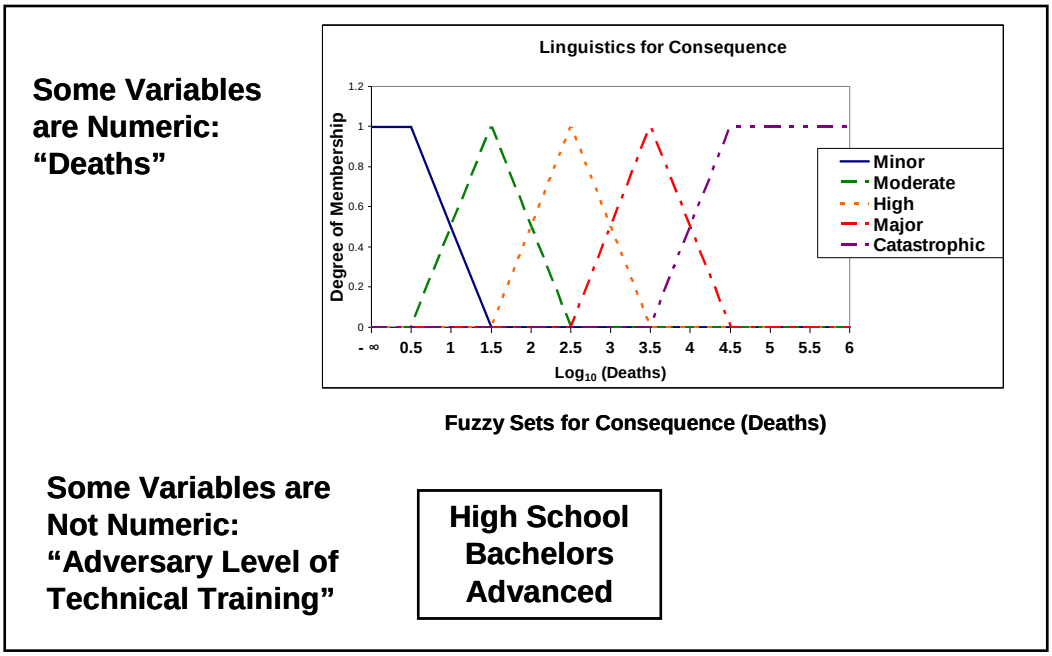
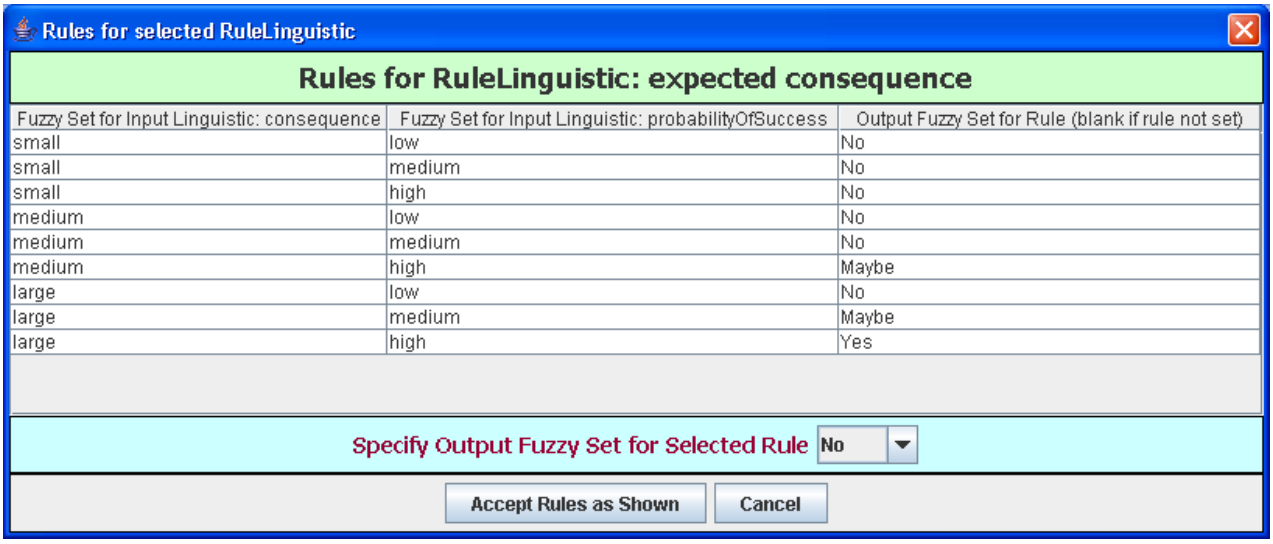



**Figure 13. Fuzzy Sets for Numeric and Non-Numeric Variables**

Non-numeric variables should not be modeled as numeric variables. For example, the scale for assigning numbers to the fuzzy sets for "Adversary Level of Technical Training" is not known; is it 1, 2, 3 or 1, 10, 100 for "High School," "Bachelors," and "Advanced," respectively? The problem of arbitrary scale is magnified when variables are combined.

In the evaluation, all variables are treated linguistically and are combined using approximate reasoning, which is a rule base for combining fuzzy sets of different variables. Figure 14 is a rule base for "Expected Consequence" as a combination of "Consequence" and "Probability of Success."



Rules for selected RuleLinguistic

**Rules for RuleLinguistic: expected consequence**

| Fuzzy Set for Input Linguistic: consequence | Fuzzy Set for Input Linguistic: probabilityOfSuccess | Output Fuzzy Set for Rule (blank if rule not set) |
|---|---|---|
| small | low | No |
| small | medium | No |
| small | high | No |
| medium | low | No |
| medium | medium | No |
| medium | high | Maybe |
| large | low | No |
| large | medium | Maybe |
| large | high | Yes |

Specify Output Fuzzy Set for Selected Rule: No

Accept Rules as Shown | Cancel

**Figure 14. An Approximate Reasoning Rule Base for Expected Consequence**

**Uncertainty.** The belief/plausibility measure of uncertainty is used to evaluate of the risk of a scenario. Belief and plausibility are lower and upper bounds on probability, respectively. Belief and plausibility are calculated from evidence as discussed in the references. If the evidence is specific, both belief and plausibility are the same: probability. Figure 15 is an example for a numeric variable, and Figure 16 is an example for a non-numeric variable.

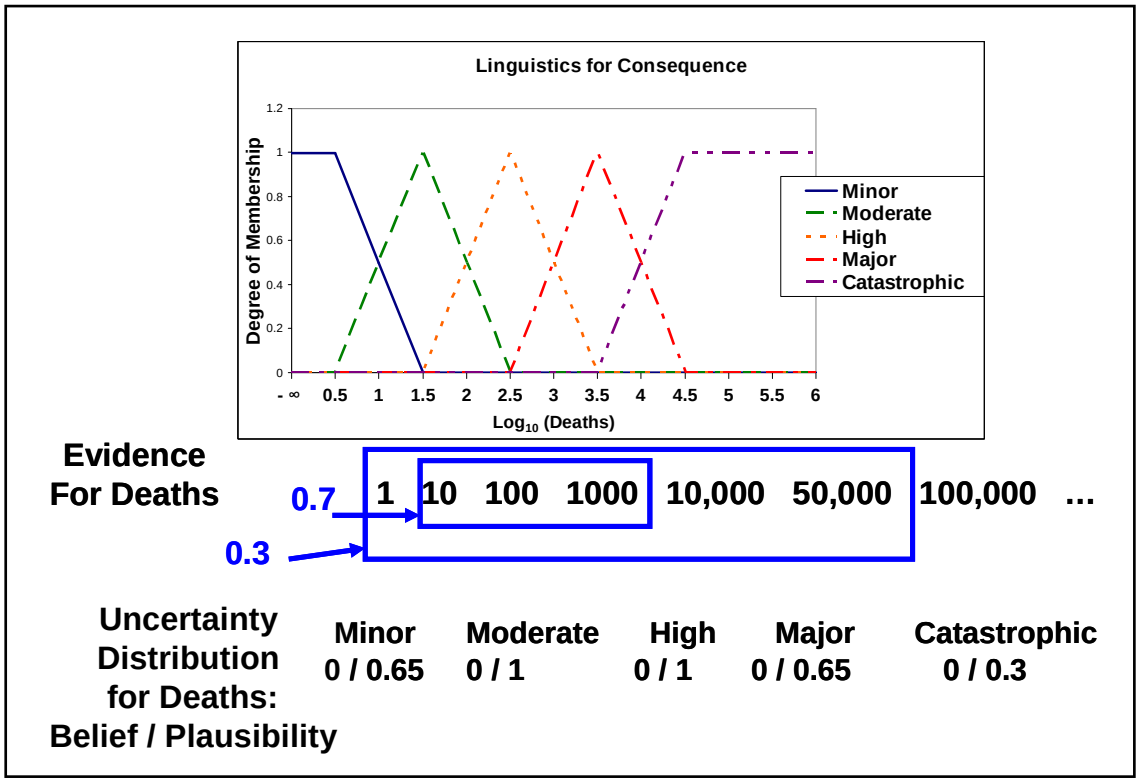



**Figure 15. Belief/Plausibility for Evidence on Numeric Variable**

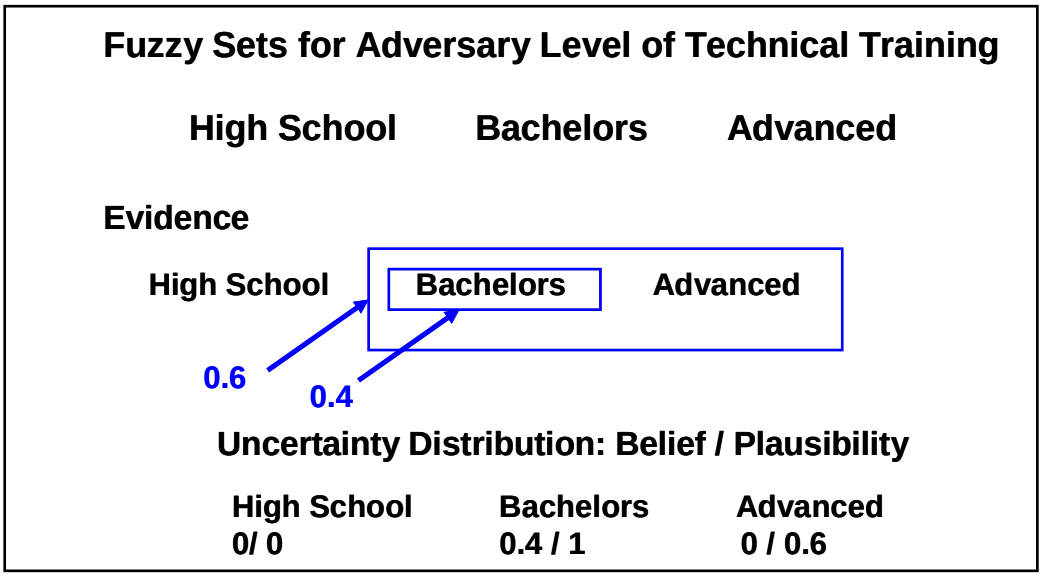



**Figure 16. Belief/Plausibility for Evidence on Linguistic Variable**

**LinguisticBelief Code.** LinguisticBelief is a java code written at SNL to perform the evaluation of scenarios using the techniques previously described [17]. Figure 17 is an example evaluation created and evaluated in LinguisticBelief.

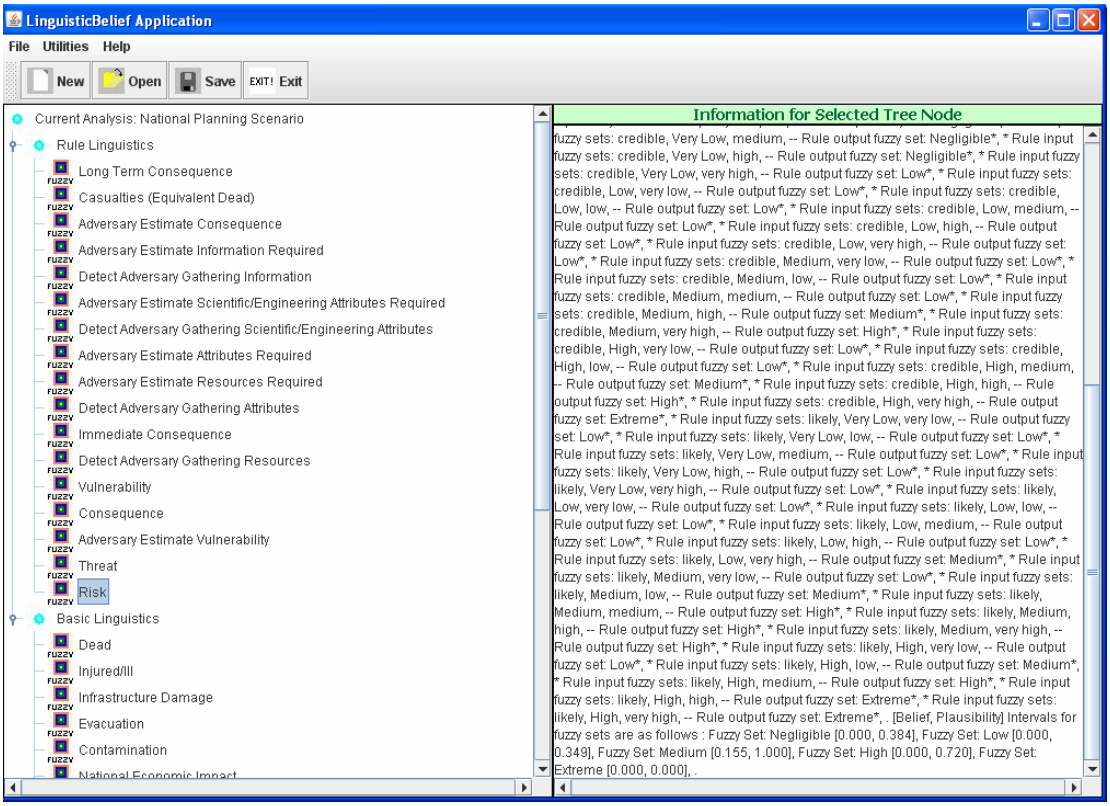



**Figure 17. Evaluation in LinguisticBelief**

**Ranking of Scenarios.** Scenarios are ranked by the highest non-zero plausibility of exceeding the worst fuzzy set for risk. Scenarios with equal plausibility are sub-ranked by belief. Figures 18 through 22 graphically illustrate the ranking of five scenarios (taken from another study) [18].

The graphs indicate that three scenarios have a plausibility of 1.0 of *exceeding* "Risk Level" "High:" CBRNE_2B, CBRNE_3B, and CBRNE_4B. Of these three, CBRNE_2B has the highest belief, 0.94, of *exceeding* "Risk Level" "High." Therefore, Scenario CBRNE_2B is of most concern, followed by scenario CBRNE_3B and scenario CBRNE_4B. Of the two remaining scenarios, CBRNE_1B and CBRNE_5B, CBRNE_1B is of more concern since it has a plausibility of 0.5 of *exceeding* "Risk Level" "High," while scenario CBRNE_5B has zero plausibility of *exceeding* "Risk Level" "High."

The ranking process has been automated in a Java utility program, RankScenarios. Using this program, the ranking of the scenarios is given in Listing 1.

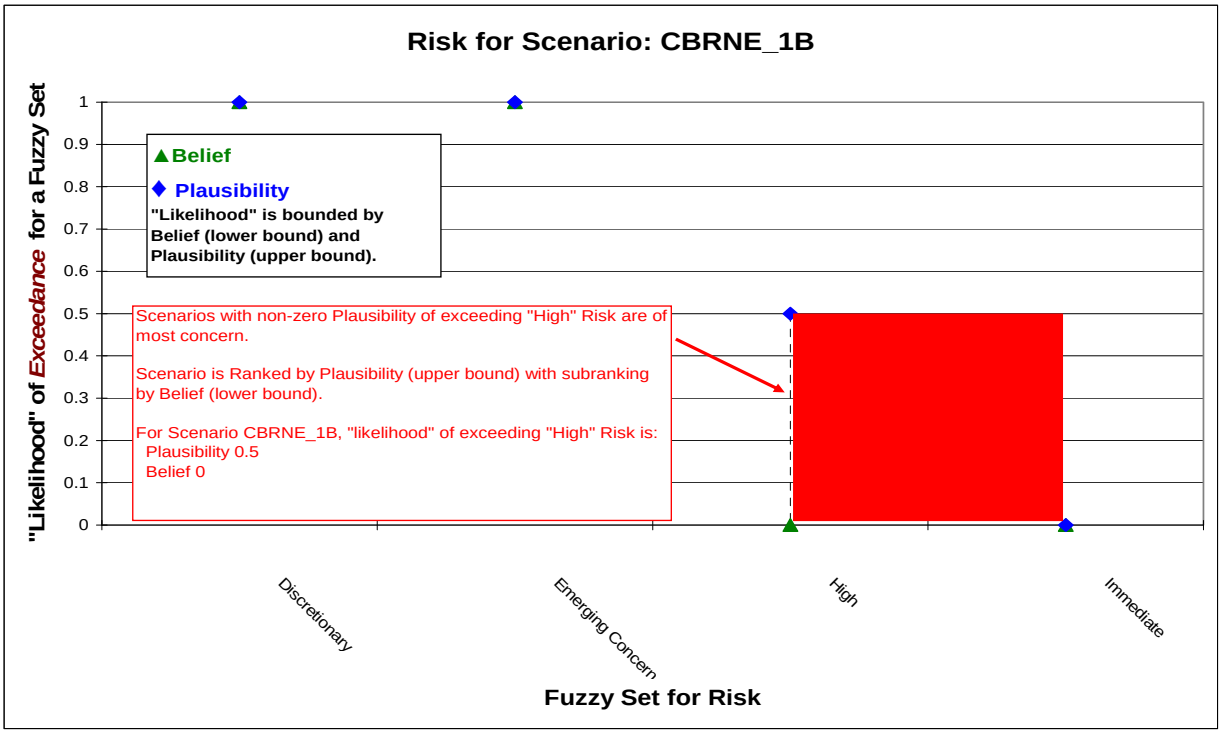



**Figure 18. Ranking of Scenario CBRNE_1B**

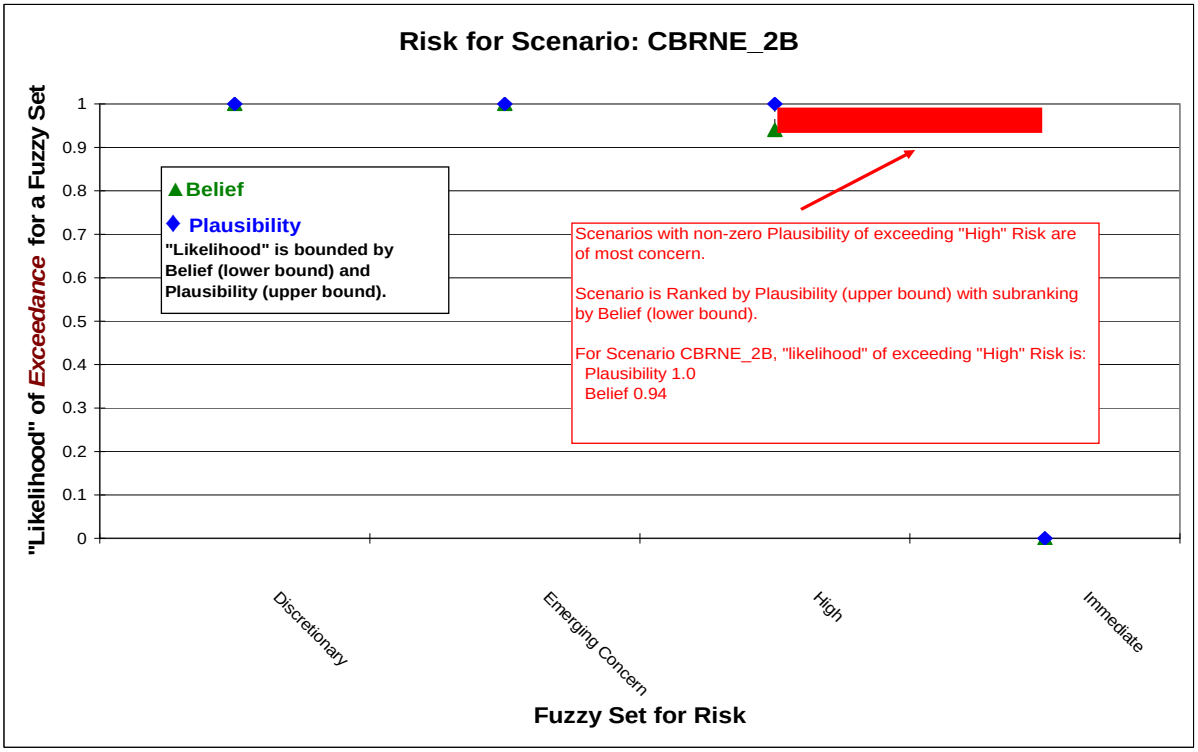



**Figure 19. Ranking of Scenario CBRNE_2B**

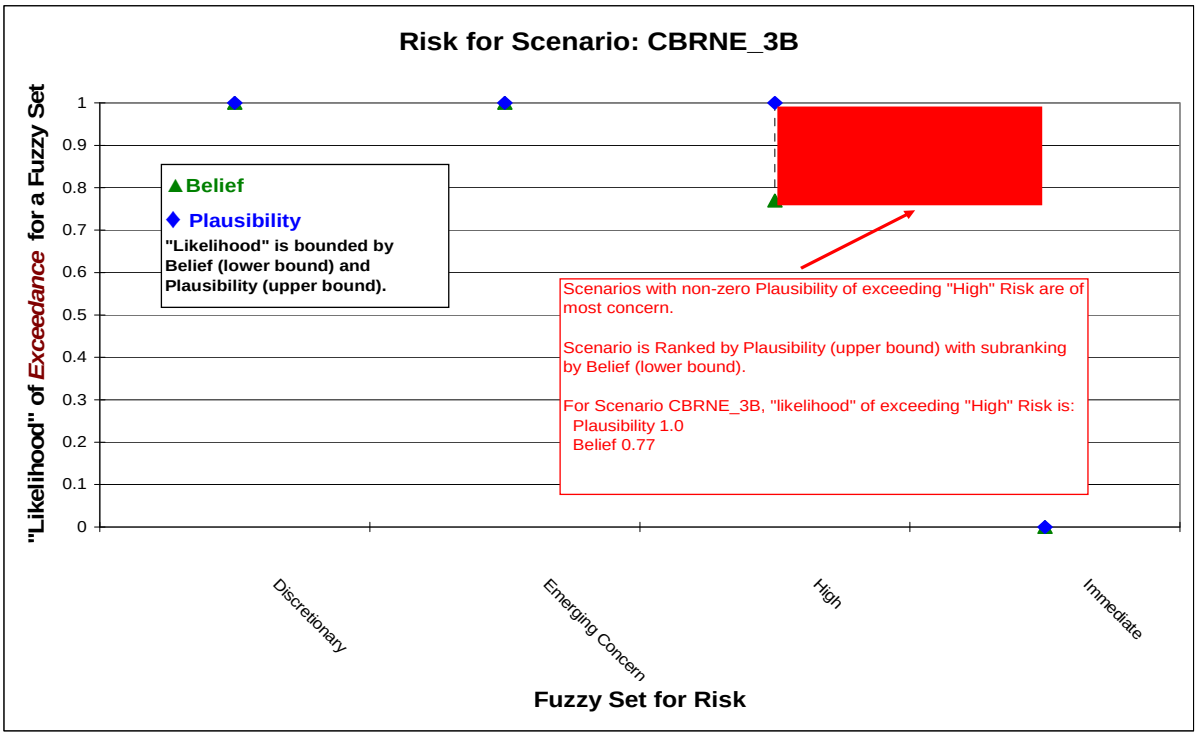



**Figure 20. Ranking of Scenario CBRNE_3B**

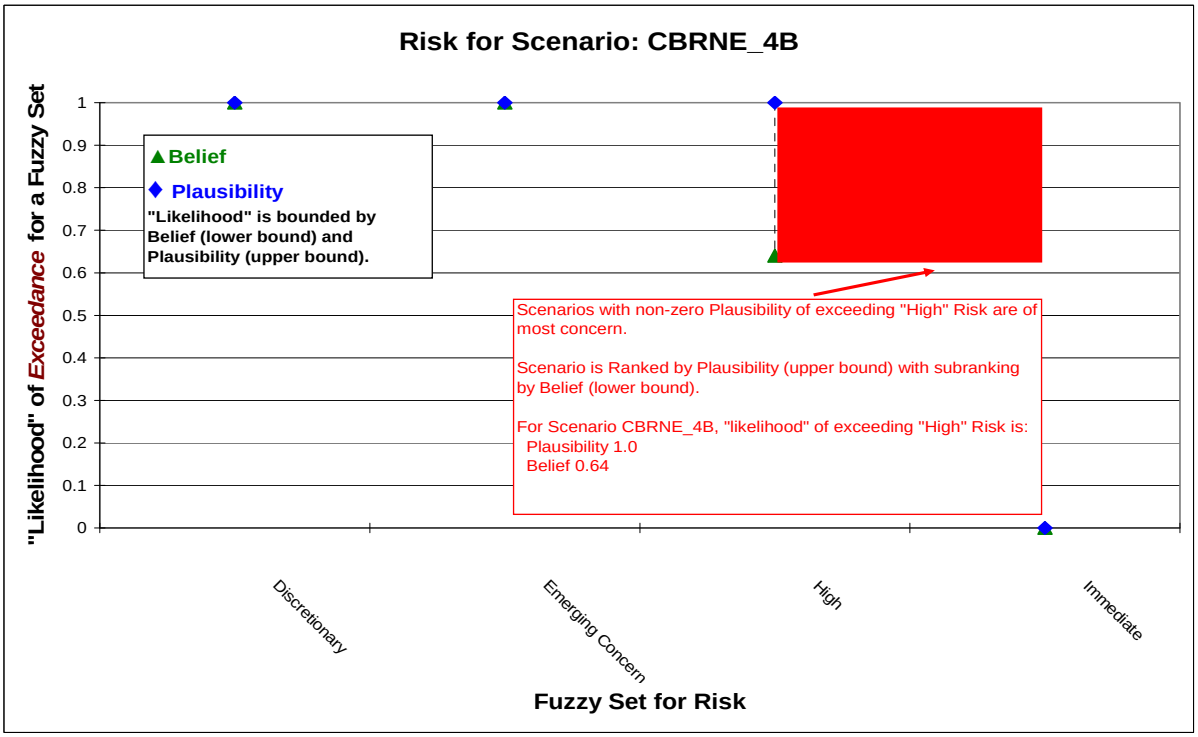



**Figure 21. Ranking of Scenario CBRNE_4B**

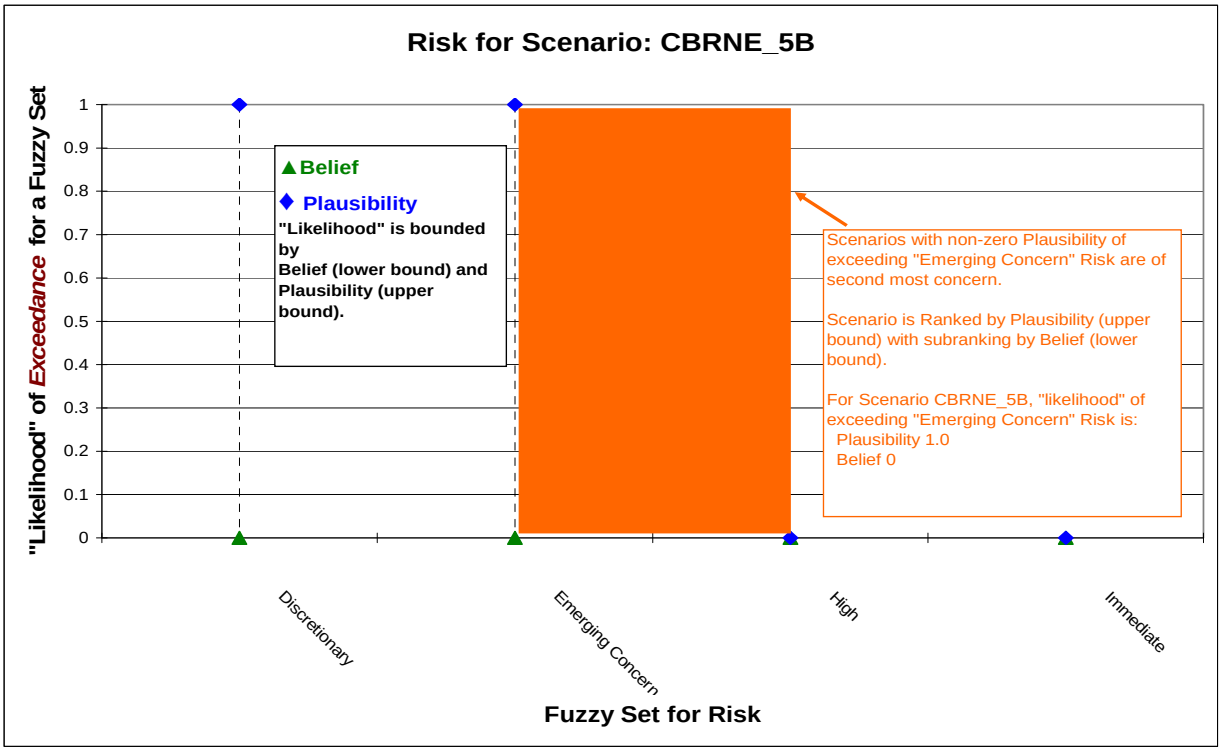



**Figure 22. Ranking of Scenario CBRNE_5B**

**Listing 1. Ranking of Scenarios by "Risk Level" Considering Uncertainty**

**RANKING FOR SCENARIOS CBRNE_1B through CBRNE_5B**

**For *Exceeding* Fuzzy Set "High" the Scenarios rank ordered (decreasing) are:**

**CBRNE_2B has plausibility of exceedance of 1.0 and belief of exceedance of 0.94**

**CBRNE_3B has plausibility of exceedance of 1.0 and belief of exceedance of 0.77**

**CBRNE_4B has plausibility of exceedance of 1.0 and belief of exceedance of 0.64**

**CBRNE_1B has plausibility of exceedance of 0.5 and belief of exceedance of 0.0**

**For *Exceeding* Fuzzy Set "Emerging Concern" the Scenarios rank ordered (decreasing) (not already ranked for a worse fuzzy set) are:**

**CBRNE_5B has plausibility of exceedance of 1.0 and belief of exceedance of 0.0**

**Pooling Evidence from Different Experts.** More than one expert may provide degrees of evidence for basic variables. For example, Figure 13 may reflect the evidence from one expert, while another expert may assign other evidence. The Java code PoolEvidence was written to pool evidence from different experts for all the basic variables of concern. The evidence is weighted equally from each expert.

For example, assume four experts assign evidence to the variable "Adversary Level of Technical Training" as indicated in Figure 23. Figure 24 shows this evidence entered into PoolEvidence. Figure 25 shows the pooled evidence as calculated by PoolEvidence.

## 5.5 Integrated IT

The development and certification of advanced technologies are needed that will enable efficient and secure collection of data from the widest possible set of sensors and other information sources, now and in the future. Because this information must be used by multiple users for multiple purposes, robust need-to-know filters must be in place throughout. Creating an integrated information system for an entire generation of facilities will be a major element in enabling multi-level secure data access. This access includes open architecture, interface standards, and protocols based upon advanced communications and network technologies to support the needs of all users while providing them with assured security to execute their operations. The modularity of a unified data architecture will allow its application to a number of different types of facilities; it will also provide an adaptive capability that permits the flexibility to deal with requirements and technologies as they change through time.

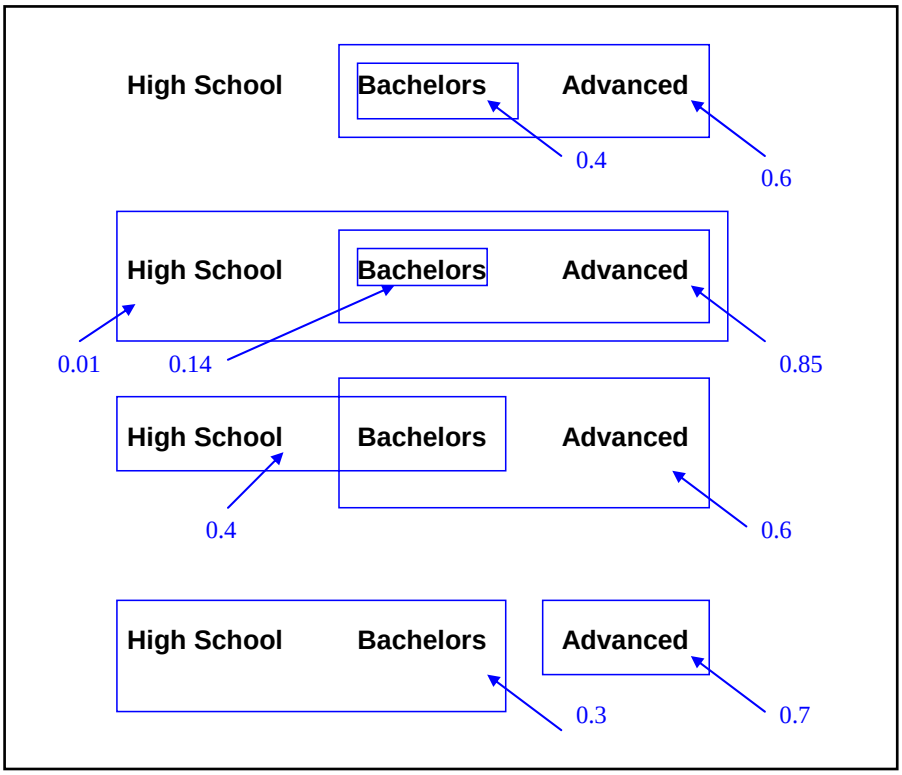



**Figure 23. Evidence from Four Experts for Adversary Level of Technical Training**

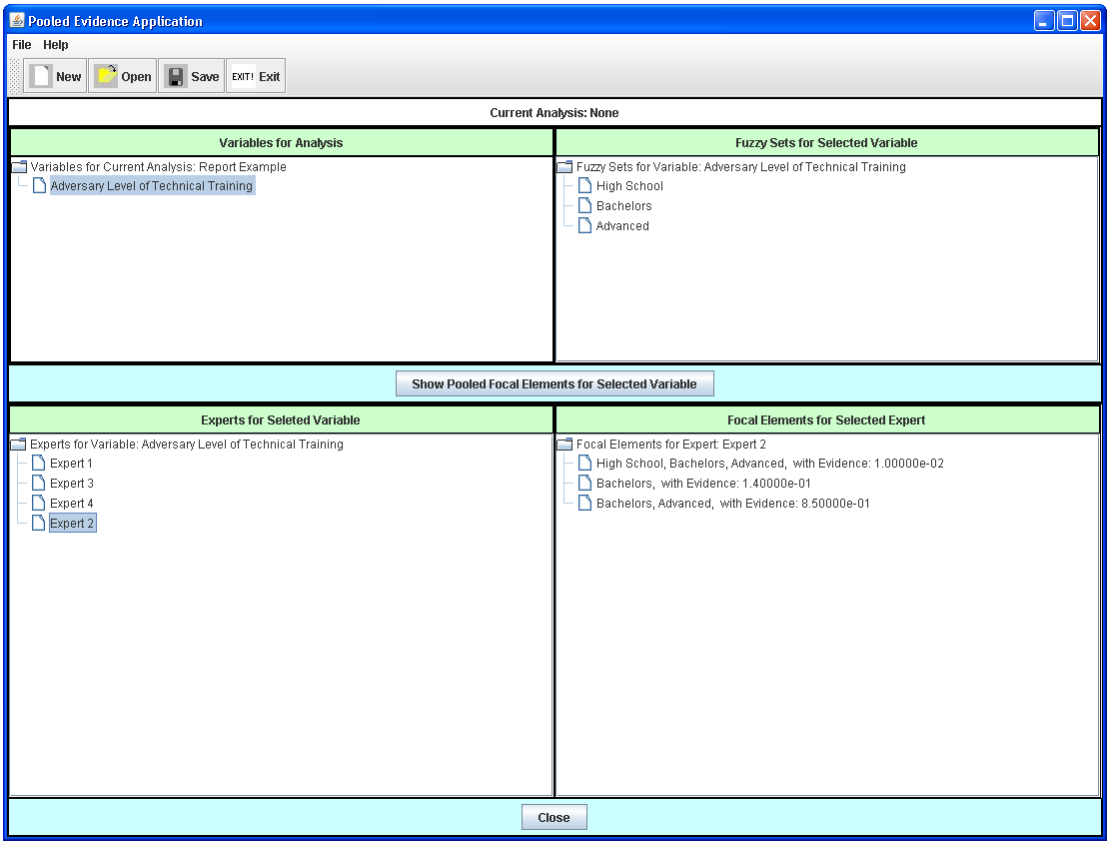



**Figure 24. Evidence Entered into PoolEvidence**

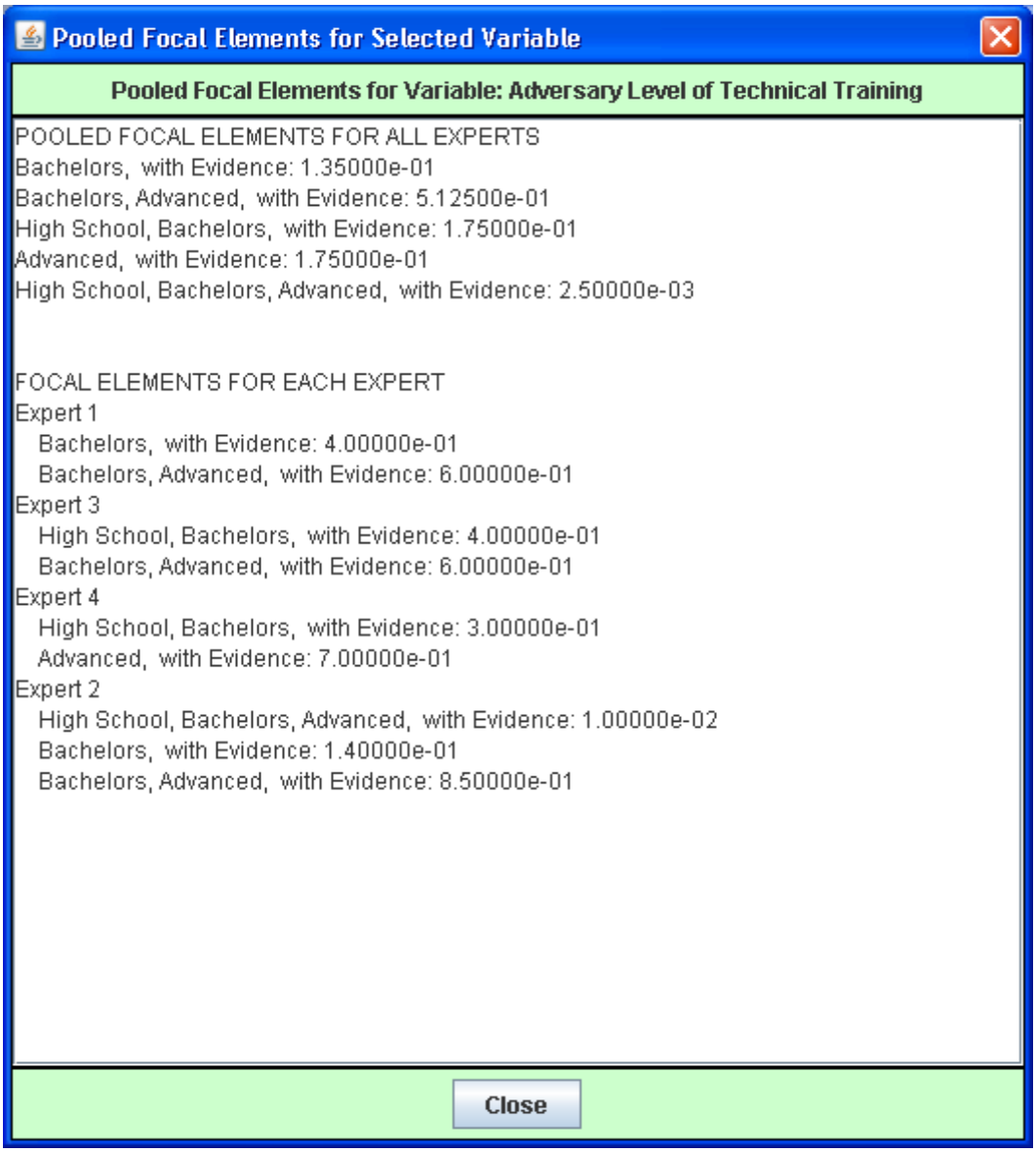



**Figure 25. Pooled Evidence for Example**

To this end, a number of technologies, capabilities, and systems need to be created or re-worked to operate in an ISOSS environment. Some of these systems, such as the Trusted Processor, come from the realm of nuclear dismantlement and involve the correct processing of highly classified information. Others, such as VPN, are easily available commercial-off-the-shelf products that need some minor adaptation to operate correctly. An incomplete list of technologies, capabilities and systems that are needed follows:

- Cradle-to-grave information encryption and authentication systems
    - Customized VPN implementations
    - Embedded cryptographic processes within sensors, monitoring systems, computers, and network hardware

- Integrated Requirements Modeling Tools
    - Up-front capability to incorporate ISOSS design requirements into designs
- Need-to-know systems and multi-level security systems
    - Exportable version (possibly commercial) of Need To Know (NTK)/Data Access Control System[30]
    - Taxonomy of metadata (controlled descriptors and limitation keywords)
    - Exportable version (possibly commercial) of the Trusted Processor
- Open IT architecture, interface standards, and protocols
    - Generic data warehouse design
    - Networking standards
    - Standard protocols for system interfaces with new devices
- All-channels communication system
    - Alerts, alarms, and emergency information to facility loud speakers, e-mail and computers, staff cell phones and PDAs
    - Interfaces with state, local, and federal emergency communications
- Verifiably secure, tamper-indicating joint-use IT resources
    - Joint-use computers
    - Shared-but-separate networks
    - Design simulations for integration design, testing, and operations
    - Verification and validation of simulation tools
    - Application beyond operations and safeguards to safety and security

## 5.6 Cost-Benefits of ISOSS

In looking at fully integrated SOSS from a financial point of view, one may take into account the entire facility as a system. This facility "bubble" forms an economic entity that may be optimized by examining the implementation costs among the numerous safety, operations, security, and safeguards systems. The key concept here is that integration for integration's sake *per se* may not necessarily lower costs, especially if new technologies must be developed in order to accomplish the integration.

However, life-cycle costs within the "bubble" must be taken into account, since the majority of the cost of a system is maintenance. For example, some authorities estimate that 80% of the life-time costs of a software system is devoted to maintenance and upgrades.[31] Thus, integration that pro-rates maintenance costs across all four SOSS domains could dramatically affect the cost-benefit ratio.

---

[30] http://www-irn.sandia.gov/iis-projects/NTK/ describes Sandia National Laboratories' Need-to-Know Project

[31] McConnell, 1996. *Rapid Development*.

Additionally, SOSS integration research and development might reasonably be apportioned among all potential facilities under design. When international safeguards are taken into consideration, this could have world-wide implications. Cost benefits of regulatory policies should be considered when responsible agencies are considering new or revised directives, regulations, and guidelines.

# 6.0 Summary

The design of nuclear facilities is primarily driven by the operational needs of the facility. For nuclear power plants, the operational requirement is to generate electrical power, while fuel cycle facilities typically manufacture and reprocess fuel. Operational and safety issues have historically been given higher priority than security and safeguard features. While safety is typically incorporated into the design and operation of a nuclear facility, security and safeguard features are generally considered add-ons, and are often done after the facility has been constructed. As a result, the design features and procedures identified to meet the requirements for SOSS can be contradictory if the individual groups have not worked together to provide a single solution meeting all SOSS requirements (e.g., requiring the same door to be locked for security and unlocked for safety). In addition, new SOSS concerns and resulting requirements are often identified after a facility is built, which sometimes requires costly back-fits. Although the back-fits may improve one SOSS element, they can adversely affect other elements. For example, increases in security to confront changing "insider" threat requirements can impose significant restrictions on the movement of personnel throughout the facility, negatively impacting normal operations.

SNL developed a preliminary framework for integrating SOSS, beginning at the facility design level and extending into the facility operation. The integration framework uses a systems engineering approach to combine the results of the individual—quantitative and qualitative—SOSS analyses to identify the SSCs (including facility operations monitoring systems, such as process control information); limits on operation; and procedures required for each of the three disciplines. The framework stresses the need to integrate SOSS very early in the design process in order to provide an optimal design with respect to all four SOSS elements.

The integrated framework addresses the following:

- the high-level SSS requirements and interactions among disciplines,
- effective management and utilization of the process information collected for each discipline,
- areas of subtle inter-disciplinary interactions,
- integration of the response procedures for safety and security personnel, and
- harmonization of the results of the various discipline analyses to achieve cost-effective facility design and operation (innovative methods may be required to meet all concerns).

The benefits of incorporating an integrated approach into the design and operation of nuclear facilities using this framework are as follows:

- providing increased security at reduced cost,
- using complementary aspects of safety systems for security systems,
- decreasing impact on operations,
- addressing both "design events" and events outside the design space,
- extending safety-based PRA to security-based URA to evaluate events outside the design space using a risk measure,
- reducing personnel costs associated with security,
- ensuring the security system is robust to changes in the threat,

- incorporating intelligence gathering to improve security, and
- incorporating safety measures for mitigating consequences into security measures for mitigating consequences.

Several enabling tools and techniques for integrating SOSS elements include the following:

- integrating SOSS information technology systems,
- integrating risk analysis tools,
- cross-training personnel in the different SOSS elements, and
- formalizing the design review process.

Several areas requiring further development for effective SOSS integration include the following:

- integrated risk-informed SOSS regulations for new nuclear facilities,
- performance measures to compare against,
- integrated risk analysis method to evaluate conflicting requirements, and
- integrated information technology systems.

# References


[1] G. B. Varnado and N. R. Ortiz, Fault Tree Analysis for Vital Area Identification, NUREG/CR-0809, SAND79-0946, Albuquerque, NM, U. S. Nuclear Regulatory Commission, Washington, DC, June 1979.

[2] R. W. Youngblood and R. B. Worrell, Top Event Prevention in Complex Systems, ASME PVP-Vol. 296, Risk and Safety Assessments: Where is the Balance?, 1995.

[3] Analytic System and Software for Evaluating Safeguards and Security (ASSESS), Sandia National Laboratories

[4] Joint Conflict and Tactical Simulation (JCATS) system, Lawrence Livermore National Laboratory

[5] SAND2007-3011P, The Concept of Assured Security by Design

[6] DOE O 470.3 A, Design Basis Threat Policy (U), Department of Energy

[7] DOE M 470.4-2 Change 1, Physical Protection, Department of Energy

[8] Saphire Risk Assessment software, Idaho National Engineering Laboratory

[9] Crystal Ball software, Version 7.0, Decisioneering Inc.

[10] Kaplan, S, and Garrick, B.J., "On the Quantitative Definition of Risk", Risk Analysis, Vol. 1 No. 1, 1981 11-27.

[11] Yager, R., "Arithmetic and other operations on Dempster Shafer structures." International Journal of Man-Machine Studies, 25: 357-366, 1986.

[12] Shafer, S., 1976, A Mathematical Theory of Evidence, Princeton University Press.

[13] Helton, J.C., Johnson, J.D., and Oberkampf, W. L., 2004, "An Exploration of alternative approaches to the representation of uncertainty in model predictions," Reliability Engineering and System Safety 85, pp. 39-71.

[14] Klir. G. J., and Yuan, B., Fuzzy Sets and Fuzzy Logic, Theory and Applications, Prentice Hall PTR, 1995

[15] Darby, J., 2007 "Evaluation of Risk from Acts of Terrorism: The Adversary/Defender Model Using Belief and Fuzzy Sets," SAND2006-5777, Sandia National Laboratories, Albuquerque.

[16] Darby, J., 2007, "Evaluation of Risk for Acts of Terrorism using Belief and Fuzzy Sets," Journal of Nuclear Materials Management, Vol XXXV, Number 2, Winter, 2007.

[17] Darby, J., 2007, "LinguisticBelief: A Java Application for Linguistic Evaluation Using Belief, Fuzzy Sets and Approximate Reasoning", SAND2007-1299, Sandia National Laboratories, Albuquerque, NM.

[18] Darby, J., 2007, "Linguistic Evaluation of Terrorist Scenarios: Example Application", SAND2007-1301, Sandia National Laboratories, Albuquerque, NM.

[19] Depoy, J.M., *et. al.*, "Critical Infrastructure Systems of Systems Assessment Methodology," SAND2006-6399, Sandia National Laboratories, Albuquerque, NM, October 2006.

[20] Darby, J., J. Phelan, P. Sholander, G.B. Varnado and G. Wyss, "A Cyber-Physical Security Assessment Methodology (CPSAM)," Proceedings of the American Nuclear Society Winter Meetings, November 2006, pp. 82-83.

[21] Wyss, G., P. Sholander, J. Darby, and J. Phelan, "Identifying and Defeating Blended Cyber-Physical Security Threats," The Gardian, Spring 2007 edition, an online publication of the InfraGard National Members Alliance (a program of the U.S. Federal Bureau of Investigation), http://www.infragardmembers.org/modules/content/index.php?id=38.

[22] Wyss, G.D."Application of the Nuclear Weapons 'Stronglink – Weaklink' Philosophy to Physical Security," white paper (Unclassified Controlled Nuclear Information), Sandia National Laboratories, Albuquerque, NM, October 11, 2004.

## Distribution

| | | |
|---|---|---|
| 1 | MS 0899 | Technical Library, 9536 (electronic copy) |
| 1 | MS 0188 | D. Chavez, LDRD Office, 1011 (electronic copy) |
| 1 | MS 1375 | Henry Abeyta, 6900 (electronic copy) |
| 1 | MS 0757 | John Darby, 6462 (electronic copy) |
| 1 | MS 1371 | Karl Horak, 6722 (electronic copy) |
| 1 | MS 0748 | Jeffrey LaChance. 6761 (electronic copy) |
| 1 | MS 6722 | Keith Tolk, 6722 (electronic copy) |
| 1 | MS 0759 | Donnie Whitehead, 6461 (electronic copy) |