INL/EXT-19-54452
Revision 0

Light Water Reactor Sustainability Program

Current Challenges, Constraints and Recommendations for Reducing Cost of Physical Security at U.S. Commercial Nuclear Power Plants

June 2019

U.S. Department of Energy

Office of Nuclear Energy

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

INL/EXT-19-54452
Revision 0

Current Challenges, Constraints and Recommendations for Reducing Cost of Physical Security at U.S. Commercial Nuclear Power Plants

Vaibhav Yadav
Steven R. Prescott
John W. Buttles
John Weathersby
Mark R. Holbrook
Ronald Boring
Douglas Osborn
Jerud Hanson

June 2019

Prepared for the
U.S. Department of Energy
Office of Nuclear Energy

EXECUTIVE SUMMARY

Economic or financial causes have led to closure or announced early retirement of several US nuclear reactors in the last five years. The published report "Economic and Market Challenges Facing the U.S. Nuclear Commercial Fleet – Cost and Revenue Study" by Idaho National Laboratory identified 63 of the 79 studied nuclear power plants (NPPs) lost money in the year 2016. The revenue gap analysis performed in the study also concluded that additional revenue is required to return most of these nuclear power units to profitable operations. This can be achieved by reducing operation and maintenance (O&M) costs that accounts for about 70% of total operating expenditures for an NPP. The Light Water Reactor Sustainability (LWRS) Program conducts research and development, sponsored by the US Department of Energy, that provides a technical foundation for licensing and managing the long-term safe and economical operation of current nuclear power plants, utilizing the unique capabilities of the national laboratory system. Reduction in O&M costs aligns with the LWRS program's mission of providing science-based solutions to the nuclear industry to implement technologies and methodologies for safe, efficient, economical, and long-term operation.

The requirements for U.S. nuclear power generation sites to maintain a large on-site physical security force, implemented after the terrorist attacks on September 11, 2001, rank high for related plant operational costs. The cost of maintaining the current physical security posture is approximately ten percent of the overall O&M costs for the commercial NPPs. The goal of this LWRS Physical Security Initiative is to develop methods, tools, and technologies and generate the technical basis for an optimized plant security posture. The conservatisms built into the security posture can be targeted in order to reduce security costs while still ensuring adequate security and operational safety.

This report summarizes the initial efforts undertaken under the LWRS Physical Security Initiative to review current physical security postures and provide preliminary recommendations for optimization. The first section describes the current physical security posture of a typical US commercial nuclear power plant, illustrating the regulatory requirements and their impact on the technology and personnel currently employed as part of physical security of a nuclear power plant. The second section illustrates the challenges facing the physical security regime that were identified during this effort, including specific details of regulatory, technological and other challenges that, if addressed, would result in near-term and long-term relief to the nuclear industry. The final section outlines the recommendations for deployment of advanced solutions in order to address the identified challenges. The major recommendations are to develop a methodology to implement risk-informed physical security and a measure of effectiveness to provide the technical basis for an optimized plant security posture that leverages automated weapon systems and advanced sensors and instrumentations.

CONTENTS

FIGURES

ACRONYMS

AEA	Atomic Energy Act
CAF	Composite Adversary Force
CAS	Central Alarm Station
DBE	Design Basis Event
DBT	Design Basis Threat
DOE	Department of Energy
DOE-NE	Department of Energy Office of Nuclear Energy
EFOF	Expanded FOF
EMRALD	Event Modeling Risk Assessment using Linked Diagrams
FOF	Force-On-Force
GPS	Global Positioning System
HEP	Human Error Probability
HRA	Human Reliability Analysis
JCNRM	Joint Committee for Nuclear Risk Management
LWRS	Light Water Reactor Sustainability
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission
Pd	Probability of Detection
PPS	Physical Protection System
PRA	Probabilistic Risk Assessment
PSF	Performance Shaping Factor
ROWS	Remote-Operated Weapons System
SDP	Significance Determination Process
SSC	Structure, System, or Component
SNM	Special Nuclear Material
U.S.	United States
Vs	Vulnerability to Defeat

CURRENT CHALLENGES, CONSTRAINTS AND RECOMMENDATIONS FOR REDUCING COST OF PHYSICAL SECURITY AT U.S. COMMERCIAL NUCLEAR POWER PLANTS

1. INTRODUCTION

1.1 General

1.1.1 Overview

Economic or financial causes have led to closure or announced early retirement of several US nuclear reactors in the last five years. The published report "Economic and Market Challenges Facing the U.S. Nuclear Commercial Fleet – Cost and Revenue Study" by Idaho National Laboratory identified 63 of the 79 studied nuclear power plants (NPPs) lost money in the year 2016 [1]. The revenue gap analysis performed in the study also concluded that additional revenue is required to return most of these nuclear power units to profitable operations. This can be achieved by reducing operation and maintenance (O&M) costs that accounts for about 70% of total operating expenditures for an NPP [1]. The Light Water Reactor Sustainability (LWRS) Program conducts research and development, sponsored by the US Department of Energy, that provides a technical foundation for licensing and managing the long-term safe and economical operation of current nuclear power plants, utilizing the unique capabilities of the national laboratory system. Reduction in O&M costs aligns with the LWRS program's mission of providing science-based solutions to the nuclear industry to implement technologies and methodologies for safe, efficient, economical, and long-term operation.

The requirements for U.S. nuclear power generation sites to maintain a large on-site physical security force, implemented after the terrorist attacks on September 11, 2001, rank high for related plant operational costs [2]. The cost of maintaining the current physical security posture is approximately ten percent of the overall O&M costs for the commercial NPPs. The goal of this LWRS Physical Security Initiative is to develop methods, tools, and technologies and generate the technical basis for an optimized plant security posture. The conservatisms built into the security posture can be targeted in order to reduce security costs while still ensuring adequate security and operational safety.

This report documents the technical review, insights, feedback, and recommendations for evaluating the current challenges and constraints associated with the physical security regime in the domestic light water reactor nuclear industry. As part of this initial assessment, investigations into areas of improvements for an effective security program are conducted. Additionally, an initial evaluation of existing validated methods that can be used to implement an updated and optimized physical security regime at domestic nuclear power plants (NPPs) is discussed. Section 1 provides an overview of the current physical security posture of U.S. commercial NPPs. Section 2 describes the identified challenges faced by the physical security. Section 3 discusses future work that can be performed to address the identified challenges.

1.1.2 LWRS Program Physical Security Initiative

This Department of Energy (DOE) Office of Nuclear Energy (DOE-NE) Light Water Reactor Sustainability (LWRS) Program effort seeks to create tools, methods, and technologies that will:

- Apply aspects of risk-informed techniques for physical security decisions and activities to account for a dynamic adversary
- Apply advanced modeling and simulation tools to better inform physical security posture

- Assess benefits from proposed enhancements, novel mitigation strategies, and potential changes to regulations

The primary deliverables for the DOE-NE LWRS Program Physical Security Initiative are to:

- Validate methods that can be used to implement an updated physical security regime and optimize the physical security at domestic NPPs
- Develop tools that create a robust risk-informed technical basis for physical security decisions
- Create potential security architectures that incorporate technology to optimize human in-the-loop activities
- Implement results of this initiative into national consensus standards.

The intent of the LWRS Physical Security Initiative is to develop methods, tools, and technologies and generate recommendations that provide the technical basis for an optimized plant security posture. This could consider reducing conservatisms in that posture, in order to reduce security costs for the nuclear industry while ensuring adequate physical security. The LWRS Physical Security Initiative will analyze the existing physical security regime (regulations, personnel, technologies, etc.) and current best fleet practices, and compare/contrast insights derived from this activity with alternatives and methods that leverage advanced modeling and simulation, modern technologies, and other advanced techniques to enhance approaches for domestic NPP physical security.

1.2 Regulatory Requirement

10 CFR 73, "Physical Protection of Plants and Materials," [3] prescribes requirements for the establishment and maintenance of a physical protection system (PPS) that will have capabilities for the protection of special nuclear material (SNM) at fixed sites and in transit and of NPPs in which SNM is used. 10 CFR 73.55, "Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors Against Radiological Sabotage," [4] requires each nuclear power reactor licensee to implement the requirements of 10 CFR 73.55 through its U.S. Nuclear Regulatory Commission (NRC)-approved physical security plan, training and qualification plan, safeguards contingency plan, and cyber security plan referred to collectively hereafter as "security plans." The requirements of 10 CFR 73.55 are intended to establish and maintain a physical protection program that provides reasonable assurance that activities involving SNM are not contrary to the common defense and security and do not constitute an unreasonable risk to public health and safety. This includes the ability to protect against the design basis threat of radiological sabotage (i.e., significant core damage and spent fuel sabotage). The security plans describe how the 10 CFR 73.55 requirements will be implemented through the establishment and maintenance of a security organization, use of security equipment and technology, training and qualification of security personnel, implementation of predetermined response plans and strategies, and protection of digital computer and communication systems and networks. The regulatory analysis in this report will focus on physical security requirements that would benefit from optimization of current physical security posture that would potentially reduce security costs for the nuclear industry.

1.2.1 Physical Security Requirements

The nuclear power reactor licensee is responsible for maintaining the onsite physical protection program in accordance with NRC regulations through the implementation of security plans and written security implementing procedures. The design of the physical protection program is focused on a series of target sets that require protection. A critical element of the security plan is the need to demonstrate the ability to meet requirements including the ability of armed and unarmed personnel to perform assigned duties and responsibilities required by the security plans and procedures. That, in turn, leads to development and implementation of a training and qualification program (in accordance with 10 CFR 73.55, Appendix B, Section VI) along with a performance evaluation program (10 CFR 73.55, Appendix B) to ensure the effectiveness of the licensee's armed and unarmed personnel.

1.2.2 Other Related Security Requirements

In addition to the physical security requirements, the licensee's security plans include details describing the following related security topics:

- The requirements for the access authorization program as stipulated in 10 CFR 73.56, "Personnel Access Authorization Requirements for Nuclear Power Plants" [5].
- A Safeguards Contingency Plan that describes how the criteria set forth in Appendix C, Section II, "Licensee Safeguards Contingency Plans," of part 73 will be implemented [6].
- A Cyber Security Plan that describes how the criteria set forth in 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks," will be implemented [7].

1.3 Current Physical Security Posture

While the U.S. commercial nuclear power industry is among the most robust and well protected critical infrastructures in the world, increased costs of regulation in nuclear security since the terrorist attacks of September 11, 2001 threaten the long-term operation and future of the existing fleets. Maintaining security of commercial NPPs to protect against deliberate acts of terrorism has always been a concern but was significantly elevated to a national security issue following the 9/11 attacks [2]. NRC and industry approach to maintaining effective security (see Figure 1) at a plant includes various security programs, each with its own individual objectives that when combined provide a holistic approach to maintaining effective security of the plant. There has been a continued buildup within these various security programs for commercial nuclear power producing what is widely considered to be the most robustly fortified and protected commercial critical infrastructure in the world. Although it's been seventeen years since the 9/11 attacks, security at NPPs remains an important concern for NRC, the commercial nuclear power industry, and the nation. Addressing this concern has come at a very high cost for the nuclear power industry that is extremely difficult to sustain in the current energy situation impacting our electricity generation, particularly in consideration of the recent and announced plant shutdowns the nation has continued to see over the past several years. If commercial nuclear power generation is to be sustained within the United States, an optimized plant physical security posture is needed that will reduce conservatisms in that posture and potentially reduce security costs for the nuclear industry while meeting the requirements of 10 CFR 73 [3].

1.3.1 Perimeter Intrusion Detection and Assessment System

The perimeter intrusion detection and assessment system (PIDAS) is the system at a nuclear power plant that is used for ensuring protection and safety of the several areas within the plant [8]. NRC defines four key areas within a nuclear power plant as follows:

Exclusion Area: The exclusion area is the area in which the licensee has the authority to determine all activities including exclusion or removal of personnel and property of the area. The licensee may or may not have fences, guard posts or PIDAS for the exclusion area.

Protected Area: The protected area is an area within the exclusion area encompassed by physical barriers, such as one or more chain-link fences. The protected area is primarily protected by the PIDAS and access to protected area would required authorization.

Vital Area: Vital areas are located within protected areas and have additional barriers and alarms to protect vital equipment. Additional authorization is required for access to vital areas.

Material Access Area: Material access area is similar to vital areas but control access to forms of special nuclear material for which protection against theft and diversion is required. The physical protection of this area is more stringent than that of vital area.

The PIDAS is a sophisticated and complex system along the fence line of protected area of a nuclear power plant that consists of intrusion sensors, alarm system, alarm communication system, video cameras, alarm and video display, communication system and personnel. The goal of PIDAS is fast and accurate detection of an intrusion attempt, both intentional-by an adversary, or unintentional-by a stray animal etc. The process of detection is complete only after an accurate assessment of the type and magnitude of the intrusion. Appendix A provides a review of the features and characteristics of different PIDAS technologies [8].

1.3.2 Security Officers, Roving Patrol, and Other Personnel

10 CFR 73.55(d)(1) states, "The licensee shall establish and maintain a security organization that is designed, staffed, trained, qualified, and equipped to implement the physical protection program in accordance with the requirements of this section" [5]. NRC security requirements for commercial operating nuclear sites increased exponentially following the 9/11 terrorist attacks, resulting in a significant increase of onsite response force personnel across the nuclear industry. The requirements for U.S. nuclear power generation sites to maintain a large onsite physical security force continues to rank high for related NPP operational costs. In referring to a plant's response force, this includes the minimum number of armed responders as required in 10 CFR 73 and security officers tasked with assigned duties, such as stationary observation/surveillance posts, foot-patrol, roving vehicle patrols, compensatory posts, and other duties as required [4]. The nuclear industry is need to pursue an optimized plant security posture that considers efficiencies and innovative technologies to reduce costs while meeting security requirements.

1.4 Force-on-force Inspection

10 CFR 73.55(k)(1), "The licensee shall establish and maintain at all times, properly trained, qualified and equipped personnel required to interdict and neutralize threats up to and including the design basis threat of radiological sabotage as defined in § 73.1, to prevent significant core damage and spent fuel sabotage" [5].

NRC, as part of its comprehensive security program, has regularly carried out FoF exercises at operating NPPs since 1991. FoF security exercises were suspended after the September 11, 2001, attacks because the conduct of such exercises would have been a significant distraction to site security forces which were at NRC's highest level of alert. In July 2002, NRC reinstated the table-top component of FoF exercises to evaluate the site's protective strategy against the enhanced adversary force capabilities.

In February 2003, NRC established an Expanded FoF (EFOF) exercise pilot program. The full exercise, which included tabletop and FoF exercises, was conducted over a period of several days. First, NRC security, emergency preparedness and operations specialists conducted table-top exercises in which they evaluated the effectiveness of site security plans against a series of attack scenarios. The role of Federal, State, and local law enforcement and emergency planning officials was also discussed in this phase of the exercise. Exercise coordinators learned the number of defenders, their protective positions and their protective strategies. In the second phase, armed with information from the table-tops, and with information gathered prior to the table-tops, detailed plans were made for a number of commando-style attacks seeking to probe for potential deficiencies in the protective strategy. A CAF carried out these attacks. The aim of the site's protective strategy was to protect target sets that would prevent radiological sabotage and protect the health and safety of the public.

From March 2004, through October 2004 the transitional FoF program was implemented with the following objectives:

- To evaluate the process and scope of FoF exercises, potential adjustments to the Interim Compensatory Measures (ICM), and other significant physical security improvements prior to resuming full scale FoF exercises

- To evaluate sites' capabilities to protect against the revised DBT
- To identify generic power reactor site vulnerabilities

NRC reinstated the FoF process in November 2004. The objectives for this process as stated in NRC Inspection Procedure 71130.03 are:

1. To verify and assess the ability of sites' physical protective systems and security organizations to provide high assurance that activities involving SNM are not inimical to the common defense and security of the facilities, and do not constitute an unreasonable risk to public health and safety.
2. To verify and assess the effectiveness of the sites' implementation of their protective strategies in accordance with NRC-approved plans and related implementation procedures, regulatory requirements, and any other applicable NRC requirements such as orders or confirmatory action letters.
3. To assess each site's protective strategy to ensure that it has been appropriately developed, is being effectively implemented, and provides high assurance of protecting target set equipment and critical personnel from the DBT.
4. To assess the site's capabilities relative to conducting a FoF exercise.
5. To assess the site's conduct of the Emergency Preparedness (EP) portion of the FoF exercise, including the adequacy of actions to integrate security, plant operations and emergency response, and the site's critique process to identify and correct EP weaknesses.

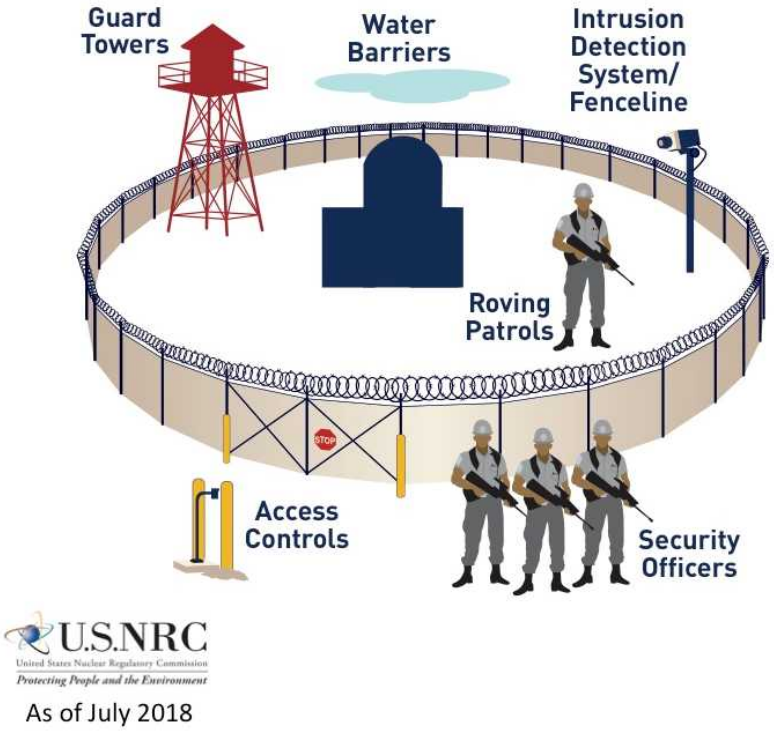

Figure 1. Components of security at a typical U.S. commercial NPP.

2. CHALLENGES

2.1 Regulatory Challenges

Maintaining regulatory certainty and predictability is key for the nuclear industry to move toward an optimized and more efficient security posture. From the industry perspective, maintaining certainty and predictability within regulation is fundamental so that clear guidance is in place to facilitate the industry's efforts to innovate and implement transformational changes that are needed for commercial nuclear power generation to be sustained.

The NRC staff has recognized the need for transformational changes to NRC's regulatory framework, culture, and infrastructure to further enhance effectiveness, efficiency, and agility. In SECY-18-0060, "Achieving Modern Risk-Informed Regulation," [9] the staff noted:

> *"Either we embrace change in the industry or we will, through the use of dated, inflexible, and inefficient regulatory approaches, be an unnecessary barrier to technology advances.*
>
> *The staff's recommendations are a recognition that as the NRC's regulatory programs evolve, the agency must accept a greater degree of risk and uncertainty in areas of low safety or risk significance as the staff appropriately balances the regulatory principles of reliability, clarity, and efficiency."*

Concerning physical security, there are several challenges that need to be overcome for transformational change to occur. An NRC-approved and standardized methodology for risk-informing specific aspects of physical security should be established to assist licensees in providing NRC with the technical basis needed to implement optimized, innovative changes needed by the existing fleet to sustain commercial nuclear power generation. Risk-informing criteria and processes should reflect realism: performance-based approaches and data are preferred; approaches will likely use qualitative and semi-quantitative analyses as quantitative data may not be available or feasible to produce. Such a standardized methodology will enable commercial nuclear power plants to gain efficiencies through flexible post staffing and rotation requirements; gain efficiencies by basing security equipment surveillance/testing activities on performance and reliability.

2.2 Current Labor-intensive Posture

Domestic nuclear power generation faces increasing economic pressures, in part, by post-Fukushima regulatory requirements, an increase in subsidized renewable energy sources, and current low-cost natural gas, but mainly as result of additional NRC physical security requirements for U.S. NPPs following the 9/11 terrorist attacks. The cumulative impacts of additional NRC security requirements have forced NPPs to maintain a large onsite physical security force, which ranks among the highest related NPP operational costs industry wide. U.S. NPPs are seeking novel physical security methods and technologies to reduce cost in order to sustain nuclear power generation in the United States.

DOE national laboratories have extensively studied various physical security configurations that couple detect, delay, and response attributes to regulatory-required physical security postures. The LWRS Program physical security initiative initially seeks to assess benefits (e.g., reduced costs, margins in regulation compliance) from proposed enhancements, novel mitigation strategies, and potential changes to regulations, while re-evaluating adequate physical security. The long-term efforts are intended to provide the technical basis to enable regulatory change of 10 CFR 73.55 minimum security staffing requirements [4]. These long-term efforts are intended to meet the overall vision of enabling a reduction in 10 CFR 73.55 minimum security staffing requirements for at-power operations [4]. Other modes of operation could require higher or lower staffing limits and will be fully evaluated.

2.3 Technological Challenges

2.3.1 Sensor Performance and Probability of Detection

Sensor performance is made up of two elements: probability of detection and the sensor's vulnerability to defeat. Probability of detection (Pd) is the likelihood of detecting an adversary within the area covered by a particular sensor. Sensors vulnerability to defeat (Vs) is the possibility that an adversary could successfully defeat the sensor. They are related by the equation Pd $\approx 1/Vs$ [8]. All sensors can be defeated given the proper expertise, time and tools. With this in mind sensor selection is critical based on the area to be protected and the type of threat that would enter the area. Appendix A shows a comparison of different types of sensors features, advantages/disadvantages and maintenance skill level requirements. With proper sensor selection Vs is low. This coupled with proper physical installation, correct signal interfacing to an alarm assessment system and a maintenance plan the initial Pd level is high, usually above 95%. Other factors affecting sensor performance are testing and nuisance or false alarms.

2.3.2 Testing and Maintenance Requirements

Testing of an intrusion detection system device or subsystem consists of an acceptance test, performance test, and ongoing operability testing. Acceptance testing ensures that the installation matches the original design, which includes an inspection of physical installation (mounting attachments, spacing, protection of wiring in conduit and other manufacturer's requirements), correct signal and power connections, and initial performance test to measure and establish the level of performance. This is the most important step for any intrusion detection system as it will directly determine the cost of future testing and maintenance.

Performance testing is performed usually on a yearly basis, in conjunction with scheduled maintenance or after a system upgrade, to measure the level of performance to ensure the intrusion detection system device or subsystem has the same level of performance determiner by the acceptance test.

Ongoing operability testing provides a level of reasonable assurance that the intrusion detection system device or subsystem detects the threat it was designed for. Various methods have been devised for testing based on manufacturer's recommendations and the combined fleet experience in conducting tests. The frequency of testing is based on identifying system degradation due to manufacturer's mean time between failure predictions that the system will fail to detect the threat it was designed for. These tests are done using a combination of maintenance and security personal. The combination of testing methods and frequency of testing has resulted in an increase of the amount of time devoted to operability testing with the results being almost always the same, the system detects the threat it was designed for. The challenge is in determining the right amount of operability testing and which testing methods should be used that will reduce the cost of operability testing and still achieve a level of reasonable assurance.

2.3.3 Nuisance Alarms and False Alarms

Nuisance alarms are any alarms that are not caused by an unauthorized entry, zone detection, or penetration. False alarms are alarms without an apparent cause. These erroneous alarms by an intrusion detection system device or subsystem results in the unnecessary response by the plant security force to verify the validity of the alarm. This not only wastes a valuable resource, but repeated nuisance or false alarms leads to a complacency posture which decreases the response time for real alarms. Also, with today's stressed maintenance force, the system creating the nuisance or false alarms may be temporarily disabled until repairs are made. This leads to initiating compensatory measures, usually in the form of posting security personnel, as a substitute for the failed device, which increases cost.

The current fleet works hard to reduce nuisance or false alarms but as intrusion detection systems age or increase in numbers due to added security requirements, the challenge will be to reduce or eliminate the number of nuisance or false alarms to decrease the cost of maintenance and extra security forces.

2.4 Measure of Effectiveness

One major roadblock to an effective risk-informed approach to physical security is the difficulty in measuring the effectiveness using the current evaluation process. Evaluation of current force on force exercises is done on a pass-fail basis. Additionally, historical data such as determined plausible scenarios and mitigation strategies are either not kept or only recorded by individual sites. Having graded measurements and historical data makes it possible to implement statistical evaluation for risk-informed decisions.

NRC security requirements defined in 10 CFR 73 are focused on protecting against acts of radiological sabotage and preventing theft or diversion of SNM. 10 CFR 73 provides a mixture of performance-based and prescriptive security requirements that require nuclear facilities to establish and maintain an onsite physical protection program that protects against the DBT and focuses on preventing significant core damage and spent fuel sabotage as the means of providing reasonable assurance that the public is not exposed to unacceptable health and safety risk.

NRC establishes the DBT based upon adversary characteristics, which are independent of the design features or technology of the facility. NRC requires nuclear facilities to have physical barriers, to identify targets, and to have a security organization with the capabilities to detect, assess, interdict and neutralize the DBT. It also requires nuclear facilities to have a physical security plan, a training and qualification plan, security contingency plans, access authorization program, insider mitigation program, and a cyber security plan. NPPs are required to demonstrate the effectiveness of the security organization through FoF activities, coordinate with other onsite plans and procedures, and provide defense-in-depth through the integration of systems, technologies, programs, equipment, supporting processes, and implementing procedures.

Nuclear facilities are permitted to propose alternative methods or approaches to meet these physical security requirements, long as they offer equivalent protection and meet the same intent. Exemptions may also be requested to address specific unique characteristics of plant design and operation. However, these processes are not efficient or preferred to address generic policy or technical issues.

A risk-informed approach of security requirements commensurate with the off-site radiological risk, including an increased reliance on the engineered features and a decreased reliance on the security organization's response, is not new and offers an approach to measuring system effectiveness consistent with other approaches currently within NRC regulation and inspection. 10 CFR 73.25, "Performance capabilities for physical protection of strategic SNM in transit," 10 CFR 73.45, "Performance capabilities for fixed site physical protections systems," and 10 CFR 73.51, "Requirements for the physical protection of stored spent nuclear fuel and high-level radioactive waste" credit the engineered features of the designs and require the security response organization to detect, assess and communicate/interdict, commensurate with the risks these activities pose to public health and safety [10-12].

U.S. nuclear facilities have implemented and maintain very robust physical security programs; however, operational experience has called into question the contribution of recent security enhancements to overall security effectiveness. Applying a risk-informed approach to physical security programs addresses these questions by enabling a meaningful technical basis for measurement of the security effectiveness, thus allowing for the identification and prioritization of physical security measures that add value. This process places a much greater emphasis on protective measures that significantly contribute to a facility's overall risk profile.

2.5 Force-on-Force Inspection

In order to test the effectiveness of the response force and site protective posture, NRC conducts a force-on-force (FoF) Inspection once every three years for each licensee. This inspection is designed to test the effectiveness of the site's security posture, to include security programs, procedures, protective

strategy, and competency of the security force in protecting the NPP against a terrorist attack intent on causing radiological sabotage. The mock adversary force used by NRC and the nuclear industry to conduct these simulated assaults is referred to as the composite adversary force (CAF), which consists of security responders from the industry that have been selected to perform as a CAF team member for a designated period, generally not to exceed three years. The CAF conducts an assault on the plant in accordance with the design basis threat (DBT) criteria established for the nuclear power industry by NRC in consideration of terrorist activities that have occurred throughout the world or are deemed to be feasible. The DBT establishes the weapons, equipment, knowledge, capabilities, and level of training and tactical expertise the CAF may use in developing scenarios used to conduct a simulated attack on the plant. The DBT is also used by NRC and the nuclear industry to determine the overall level of security required to effectively protect a plant. NRC utilizes an FoF inspection team and a significance determination process (SDP) to evaluate the licensee's security posture and performance during the FoF exercise. If issues in performance are identified, the NRC inspection team may issue findings based on the SDP and the licensee would conduct an evaluation on the cause of an issue identified during an exercise and implement corrective actions through internal site programs. Much of the scenarios used to conduct FoF exercises are based on artificialities that often serve to increase the complexity of the inspection, while simultaneously reducing the realism of the scenario. This process often results in an increase of security requirements throughout the industry without a sound technical basis for the increase in security posture. Examples of the types of artificialities imposed on a FoF exercise that can give the adversary forces an unrealistic advantage include, but are not limited to such things as:

The adversary force describing how they would breach a barrier, but not actually having to perform the task. Since it would be total unrealistic to have the adversary force actually destroy a barrier during the exercise, often, they are required to go through the steps that would be involved, then a "hold time " is imposed on the exercise, and the adversary force is taken to the other side of the barrier before the exercise can continue. Although this is the best way in which the exercise can be conducted, it does create some unrealistic situations.

Although these restrictions do insert a degree of un-realism, FoF exercises are still an extremely useful tool in the physical protection strategy. Restrictions that are not often noticed in modeling and simulations, can often be detected in FoF exercises such as; Restricted visibility due to equipment, material storage or vegetation; Blind spots caused by too much or too little lighting; Difficult traverses due to uneven surfaces or soft soil conditions. Additionally, paths and time lines can be updated in the computer models, based on actual times observed in the FoF exercises. Bringing adversary forces form off site, brings a fresh perspective that can often identify vulnerabilities that the protective force had not considered, and finally, FoF exercises are one of the best training tools for the protective force.

In general, FoF models are quite conservative in their modelling approach. FoF models do not take credit or consider the various security activities and barriers that exist outside the boundary of the physical plant. These are numerous and substantial including protections provided by the federal, state, and local governments in the form of border security, active vigilance, and extensive protocols to coordinate responses to a diverse set of threats. It is difficult to analyze and incorporate these additional layers of protection. However, analyzing and taking credit for these additional elements could prove beneficial for accurately depicting the threat basis plants must be prepared to defend against. Within the physical boundary of the plants, the FoF models are also conservative in their modeling.

The FoF models tend to model only the chance of preventing access to the facility. The modeling stops at the point of successful intrusion into the facility in the attack scenarios and assumes success of the adversary. This represents a form of conservatism in modeling, because there exists many additional barriers beyond the first line of defenders that help protect the plant. Additional physical barriers significantly slow access to the most vulnerable parts of the facility. Gaining access through multiple defense-in-depth physical barriers buys time for additional responders to defend the facility and recover the plant prior to actual harm. Thus, as the intrusion progresses, the delays posed along the way serve to

significantly decrease the chance of adversarial success. Moreover, the facility features numerous functional protection systems that render the facility less vulnerable in certain states. The transition from full power to safe shutdown at the plant—such as triggered when tripping the reactor—significantly reduces the opportunity for physical damage to the facility. The complexity of the plant and systems pose a further barrier to adversaries, as the requisite operational and technical knowledge to render damage relies on specialized training and expertise that is unlikely to be available to external parties.

3. RECOMMENDATIONS FOR FUTURE WORK

3.1 Regulatory

3.1.1 Risk-informed Physical Security

The implementation of security systems and programs at commercial nuclear facilities are designed to protect one or more target sets that if damaged or lost, could result in radiological sabotage as described in 10 CFR 73.1 [3]. The target set and result due to a loss of a target set needs to be clearly identified, as does the threat defined within the DBT. The protection of nuclear materials as well as the associated facility and activities require security systems and programs that are designed and operated based on the requirements described in 10 CFR 73 [3]. These criteria should be based on an assessment of the risks and are an important element in the regulatory framework established in the rule. Proven compliance with the rule and associated guidance is an essential component of confidence in the security system and program's appropriateness and effectiveness. However, it is equally important that security performance be assessed directly and dynamically. If a security system or program is determined to be insufficient, it is vital that it be corrected. This might require anything from a strengthening of site processes and procedures to a change in a regulatory guide or NRC-endorsed security guidance. In order to do this effectively and more efficiently with the objective of optimizing security posture and increasing efficiency, a systematic, structured, comprehensive and appropriately transparent framework is needed to risk-inform physical security. This framework should be implemented with the intent of using both quantitative and qualitative results, be consistent with requirements and guidance provided in current regulation and be acceptable for use by the nuclear industry through the approval or endorsement of the NRC.

Risk-informed physical security is intended to provide realistic models of security that capture potential performance shortfalls (i.e., vulnerabilities) in the security posture at a facility thereby providing a formal mechanism of addressing potential shortfalls through plant changes and the incorporation of security-related technologies. Typical risk-informed approaches use a scenario-based approach (either quantitative or qualitative) to describe types of events that could occur in a facility such as a NPP. Quantitative risk analysis then includes a quantification of the onset of the off-normal condition (called "initiating events") and the plant response (including components, software, and people). Risk-informed physical security builds upon these ideas to incorporate security aspects such as physical systems or structures and the plant security personnel into scenarios that are thought to be plausible. In a modern risk analysis approach, the model would include understanding the reliability of plant response of physical security; plant operations via operators and plant staff; and systems, structures, and components. The model would also include integration with physical phenomena such as the primary system thermal-hydraulics and plant operation.

Following are some of the objectives identified for a risk-informed physical security methodology in order to provide facilities responsible for protecting nuclear material with:

1. Risk methods to improve the alignment of the security mission to that of the safety mission of nuclear facilities.
2. Risk methods and approaches to establish risk-significance criteria and associated technical basis as applied to nuclear facility security programs.
3. Quantitative and qualitative methods that can be used to assess the effectiveness of security programs, as well as, the significance of security-related events originating internally or externally to the facility.
4. A means to assess, monitor, and observe ongoing performance trends of security functions through risk-informed facility-specific performance indicators.

3.1.2 Addressing Ambiguity with Clear Guidance

The Atomic Energy Act (AEA) of 1954, as amended, which authorizes and governs NRC, does not specify the precise level of safety NRC must assure or define the factors NRC may or should consider in defining the appropriate level of safety. Instead, the AEA gives NRC broad discretion to weigh and balance factors, such as the state of the art of nuclear safety, the risk of accidents, the record of past performance, and the need for further improvement in nuclear safety, along with other matters, in reaching decisions. Similarly, the AEA does not define "reasonable" or "adequate." It does, however, contain language such as "adequate protection," "unreasonable risk," "minimize danger," and "inimical." "Adequate protection" focuses rather narrowly on radiological risk, and not on something broader. Looking at these terms to try to determine what "reasonable assurance" means, NRC has historically inferred from these words that some risks may be tolerated, and that something less than absolute protection is required. The legal standard for licensing decisions at NRC is to have reasonable assurance of adequate protection, but not the elimination of all risk. NRC implements the requirements of the AEA through its regulations where absolute safety or zero-risk is not a requirement. As nuclear technologies continue to advance and utilities seek ways to further innovate and enhance efficiencies at licensed nuclear facilities, to include innovations in nuclear security, NRC should recognize this and NRC should clearly define what constitutes "reasonable assurance of adequate protection" while also clearly defining that it is NOT an absolute assurance or guarantee. NRC taking this approach in providing clear expectations on what constitutes reasonable assurance of adequate protection will further provide clarification to both licensees and inspectors in determining at what point security requirements have been met in accordance with regulation. Further, it will facilitate increased regulatory certainty and predictability throughout inspections for licensees, as opposed to licensees' susceptibility to regulation by inspector interpretation of requirements.

3.2 Automation

3.2.1 Remote-Operated Weapons

Remote-operated weapons systems (ROWSs) are used by many of the worlds militaries. Most of the deployed systems are designed for armored vehicles and maritime use. Systems such as the U.S. Army Common Remotely Operated Weapons Station are capable of handling a variety of weapons such as the MK-19 grenade launcher, M2 0.50 Caliber Machine Gun, M240B Machine Gun and M249 Squad Automatic Weapon. The system allows the operator to engage targets while remaining in the relative protection of the armor vehicle. The system is composed of two parts: the mount that is attached to the exterior of the vehicle, and the control group. The mount allows for 360-degree horizontal rotation and 80-degree vertical rotation. Gyro-rotation provides stability and easy target tracking even while the system is in motion. The sight package includes a daylight video camera, a thermal camera, and a laser rangefinder. These capabilities allow the operator to identify and engage targets that would be difficult for the unaided human eye to identify.

Although designed for military use, ROWSs have applications that could be beneficial to the commercial nuclear power industry. Multiple fixed ROWSs can be controlled by a single operator, therefore acting as a force multiplier. The operator would have almost instant response time to multiple points of concern. Due to their design features, ROWSs are usually much more accurate than human-operated weapons, and the multiple sight options can allow the operator to engage targets in environments that would be difficult for the protective force to operate in. Finally, ROWSs allow the protective force to engage targets while remaining in the relative safety of the operators' bunker thereby removing the operator from the "fog of battle."

While the technology is similar, ROWSs designed for situations other than military applications, require special considerations. Improved robustness to a different and varied failure modes, more stringent safe requirements, and concerns for collateral damage are just a few of the issues that have to be

addressed. Sandia National Laboratory's High Consequence, Automation and Robotics Department has developed an advanced command and control system for ROWSs that is addressing these concerns. This technology has the potential to increase the security of high consequence targets, while also reducing the cost of protecting those targets.

3.2.2 Unmanned Aerial Vehicles

Unmanned aerial vehicles (UAVs) or drones is developing rapidly, along with drone software is creating new opportunities for security and also threat in NPPs. High-frequency radar can detect drones far enough away such that countermeasures can be initiated before the drones can complete their mission. These radar units can be coordinated to form an electronic three-dimensional detection dome over an area. Defense drones are now equipped with net shooters that capture the attacking drone. The captured drone can be examined to identify its origin and possible attacker or, if equipped with an explosive device, delivered to a safe place for disposal.

Along with net shooters, small caliber guns can be outfitted on a drone and directed by a combination of ground radar and onboard cameras to neutralize an attacker drone. This solution works best when several drones (swarms) are attacking at once. Using a net shooter only captures one drone letting the rest of the swarm continue their mission.

Tethered drones use a cable that secures the drone above a fixed point on the ground or building roof. This cable provides power and communication at all times to the drone. All controlling and video signals are transferred through this cable. The drone is able to hover indefinitely up to 200 feet above the anchor point and is very well suited as a substitute for a moveable camera mounted on a mast. The drone can be scheduled to automatically take off according to a predefined time schedule or manually. When the drone is not in the air and is active, it can be hidden from its surroundings and from any attacker surveillance.

Bullet detection and stopping drones can listen for a gun shot and place themselves between security personal and an incoming bullet. They have harden cases with special software for gunshot recognition.

With a spectrum analyzer the control frequencies used by the drone operator to fly the drone can be identified. Once identified these can be jammed or spoofed to take control of the drone or force it to land because of a loss of control signal. GPS jammers and spoofing can disrupt a drone by sending false location signals to either cause the drone to lose its location and fall from the sky or redirect it in a different direction away from the protected area. These signals only affect a small area, so legitimate users of GPS signals are not affected.

As drones become more sophisticated and less expensive, they will become more incorporated into PPS security systems. Currently one of the most common uses for drones at the moment is in perimeter security. It's significantly more cost effective, and safer for personnel, for an always-on-duty drone to patrol along the outskirts of a property, rather than having a security officer patrol the entire area, or outfitting a large perimeter with a complex deployment of cameras and sensors. Plus, there's the bonus of using that flight for inspection or sensor testing purposes. Based on the technology, optics or sensors can be fitted on the drone to collect a host of valuable information, all at high resolution. If there does happen to be a security breach, a drone can usually navigate to a location significantly faster than a person could to assess the risk level and it can also act as a visible deterrent to intruders once it arrives at the scene. The use of drones can create both great security and business value while reducing cost. Drones should always be considered as an integral part of the overall total PPS security management, and not used as a stand-alone security solution.

3.3 Technological

3.3.1 Advanced Sensors and Testing

The current PIDAS of a commercial nuclear power plant can gain significant efficiency and increase in performance by adopting advanced and digital solutions. Digital sensors are known to have higher

effectiveness of detection, increased sensitivity, faster response and increased life compared with the traditional analog devices. The digitization will result in the PIDAS of the future that also consists of a modernized Central Alarm Station (CAS) that houses the screens displaying video feeds from the cameras installed along the fence and within the plant, alarm display and communication, and access controls, all manned by the CAS operator. The advanced and digital PIDAS system will enhance the detection and assessment capabilities of not only the technology but also the CAS operators enabling the operators and responders to take swift and accurate actions. An example of such modernization is the computer vision technology that uses machine learning algorithms on the feeds from video cameras and makes decision on the size, type and magnitude of the intruding element. Such computer vision technology aides the CAS operator in differentiating between nuisance or false alarms from legitimate alarms, correctly identifying the intruder as human or not, armed or unarmed etc. Naturally, such technological enhancements will result in improved performance and lower cost of operation and maintenance. The advanced digital sensors that are equipped with self-diagnosing capabilities and algorithms would also address the current regulatory requirement of periodic performance testing.

3.4 Measure of Effectiveness

3.4.1 Quantitative Measure Instead of Success/Failure

One difficult aspect of current defensive measures is determining how effective they are in a quantitative manner. In order to form a robust risk-informed methodology, evaluation must be more than just a pass/fail and additional statistical data needs to be collected and available for site evaluation. Current site inspections and FoF evaluation methods result in limited data to be used by the involved facility let alone use by other facilities.

Current industry probabilistic risk assessment (PRA) modelers have access to data with failure rates for general and specific components depending on the amount of data available. This data allows for accurate and detailed models for the safety of a plant given an initiating event and random failures. A system for similar data to be gathered from FoF exercises, guard training, operation events of physical protection equipment, and manufacturer and third-party testing needs to be implemented. This storage and data access system will provide the information needed for some direct risk-informed decision and provide the data needed for new technologies to perform advanced simulation and analysis for guidance in other risk-informed decision-making.

Advanced FoF exercise simulation methods are currently being used by facilities to compare and evaluate protection strategies. Facilities using these simulation tools currently use the conservative requirements imposed on the physical FoF exercises for building these models and results match those exercises very well. This is a good cross validation of both FoF exercises and the simulation tools. The next step is to enable the use of these tools to sample more realistic data collected from the system described above. This will provide probabilistic results for scenarios and an overall quantitative analysis of the security plan. While these tools should not be used to replace all physical FoF exercises, they should provide an avenue for both an optional reduction in FoF exercises and verification of equivalent protection with changes to protection design, equipment, and/or strategy.

An additional benefit of the data storage system is that it will allow for more efficient and effective site evaluations. By using the system to retain both, identified issues and accepted solutions, sites can know of previously identified issues, identify if those same issues exist at their facility, and stay informed of possible solution or add new solutions that could be more secure or cost effective.

3.4.2 Integrated Modeling and Simulation of Security Events

There are more characters and systems involved in a security event than just the adversaries and the security detail (detection and protection), equipment. and targets. These other personnel and systems are critical to the outcome of a facility if initial defense measures fail weather due to beyond DBT, unrealized

scenario, or failure of personnel or equipment. Currently, these other items are either ignored or very limited in the credit they provide. This is due to either the cost and complexity to model, lack of tools, or regulation restrictions.

New advanced modeling and simulation tools are being used by industry to simulate FoF exercises involving various attack scenarios. These tools have an immediate benefit to evaluation of security effectiveness, but once modeled, provide an opportunity for a more comprehensive and realistic picture of what would happen during a security event. By combining both the FoF attack simulation with operator actions and the plant model, a complete picture with quantitative results can be generated. Additionally, this type of modeling can show how a vulnerability that may be cost prohibitive to protect against through manpower, could be more effective and cost beneficial through secondary equipment or an operation procedure change.

We propose the use of the event modeling risk assessment using linked diagrams (EMRALD), a dynamic risk assessment tool, that can couple with other simulation or physics tools to develop a modeling methodology for coupling FoF simulation with (operator and/or personnel) actions, plant models, and secondary equipment such as FLEX portable equipment [13].

EMRALD is a state diagram modeling tool based on three-phase discrete event simulation, where the next events in time are sampled [14]. This allows for fast runtimes with either close, long, or bunched spacing of events in time. A user interface allows for quick and easy-to-understand modeling of scenarios and system, component, and operator actions.

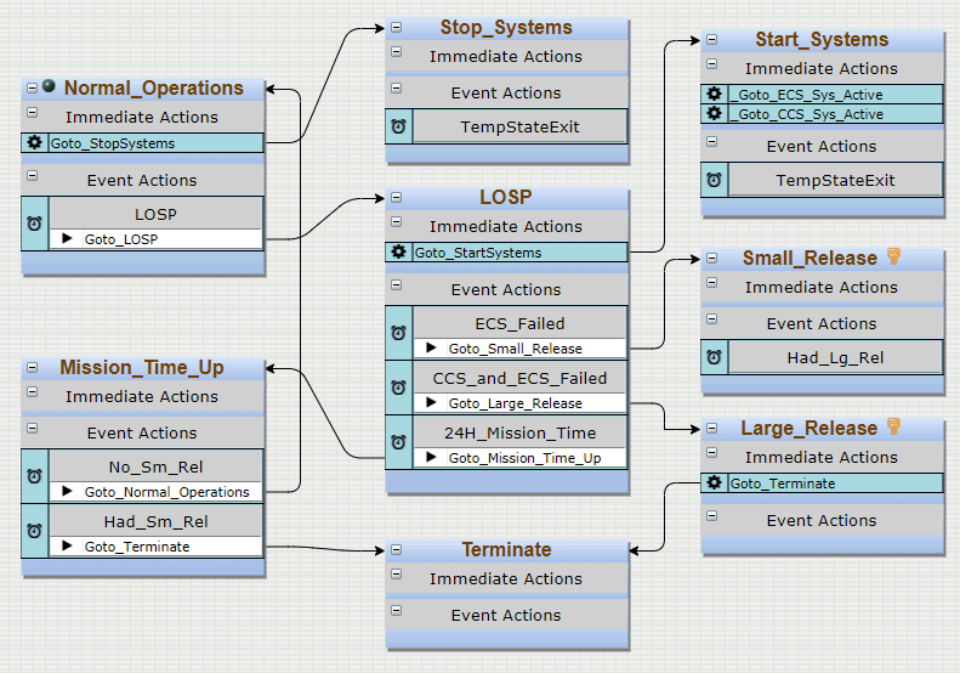

Figure 2. Example of an EMRALD diagram with states, events, and actions.

Coupling with an EMRALD model can be done through both one-way and two-way coupling. One-way coupling allows EMRALD to set up an external code or model given current states and values in EMRALD model, run it, and then process the results for transitioning between switch states and continuing the simulation. This is the most common method as it covers the needs of most scenarios and requires no external code modifications or programming interface to be written. When feedback loops, where the second application requires evaluation of its data from the initial application before continuing,

then two-way coupling is required and an open message protocol system is available. It is anticipated that initial coupling and method development will be simple and will only require one-way coupling.

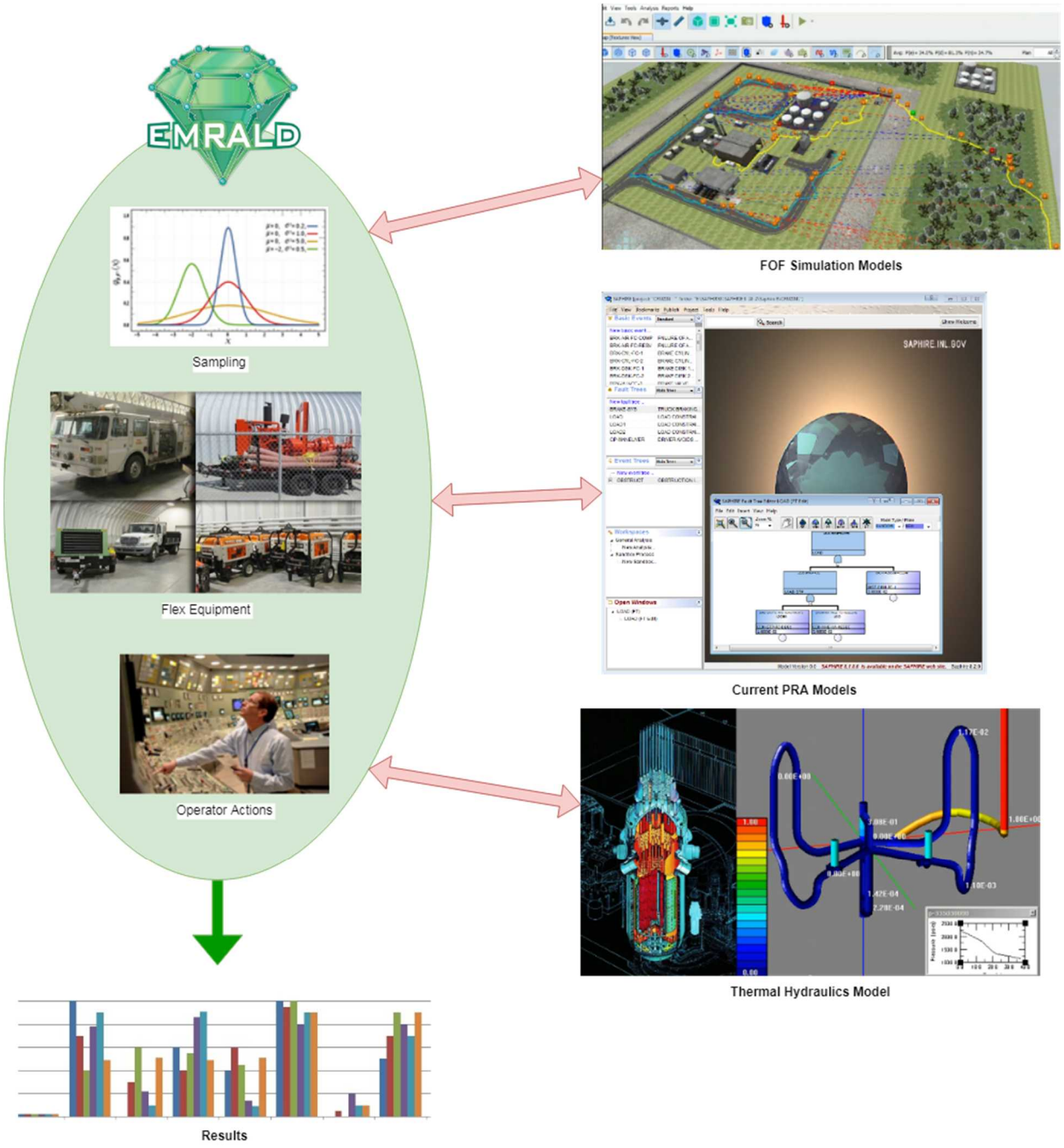

Figure 3. Coupling of tools using EMRALD.

3.4.3 Human Reliability Analysis in Security Modeling

Human reliability analysis (HRA) involves the study of human actions or inactions that contribute to the decrease in the safety or security of systems and functions. Humans are typically less reliable than hardware. Therefore, HRA is often treated as a punitive aspect of risk. It models the probability of human

error, with the typical outcome that the human actions increase overall system risk due to the high error propensity of humans. However, HRA may also model cases where human actions are likely to be successful and decrease the overall system risk. Crediting positive human actions is an important but often neglected facet of risk models, even though most modern HRA estimating methods support positive as well as negative effects of performance.

Most HRA methods consider performance shaping factors (PSFs) that act to change a nominal human error probability (HEP). This HEP is in turn considered in the fault and event tree logic alongside hardware reliability. PSFs include internal aspects of the human such as psychological stress, personal fitness, or skills. They also include external aspects that impinge upon the human such as environmental factors or the nature of the task. A PSF like personal fitness can be seen to have a positive effect, whereby it reduces the resultant HEP compared to a normal case. A well trained athlete, for example, would have greater agility and endurance to complete a strenuous physical task such as an assault on a guarded facility. The expected error rate would therefore be lower than an average, non-athlete human. Conversely, a human who is physically unfit will have decreased agility and endurance. In this case, it would be expected that the physically unfit human would be less likely than an average human to successfully complete the task. Their HEP would be increased to account for the negative effect of the fitness PSF.

In the case of physical security, the humans involved are both adversaries and defenders. There is a tradeoff or inverse relationship between adversaries and defenders—the success of an adversary comes at the cost of the failure of the defender. Conservative current modeling practices tend to give more credit to the success of the adversaries and less credit to the effectiveness of the response force. This may introduce unrealistic conservatism to the effectiveness of the defenders, effectively giving them high HEPs while crediting adversaries with corresponding low HEPs.

HRA for physical security relies on three pieces of modeling that are not currently being performed at plants:

- Accurately crediting the effectiveness of the defender (i.e., plant personnel) across multiple intrusion scenarios
- Accurately accounting for performance decrements in the adversary seeking access to the facility
- Modeling consequences if access to the facility is gained.

The latter modeling consideration builds on the existing PRA and HRA models at the plant. Accurately modeling the defenders and adversaries requires observation and consideration of the PSFs associated with specific scenarios. Facility-specific observations provide a basis for this modeling.

HRA in practice is considered static, in that it only models a set of predefined scenarios, typically those determined to be most risk significant. Unfortunately, modeling a finite set of scenarios is only possible by focusing on errors of omission—failures to perform expected actions. Errors of omission are the basis for typical risk accident sequences at the plant, because it is considered unlikely that operators would deviate significantly from mandated procedures in the control room. Errors of commission—those things actively done at the plant that disrupt its function—either maliciously or unintentionally—encompass a wider range of possible activities and outcomes than errors of omission. Modeling errors of commission with static HRA is a very labor-intensive task that often fails to anticipate every failure path that is possible. Dynamic HRA model considers multiple and emerging scenarios, thereby creating a distribution of outcomes that inform the overall risk. Building on dynamic HRA work being conducted for FLEX scenarios, a dynamic HRA model of defenders and adversaries will be created in EMRALD. This effort leverages recent efforts at Idaho National Laboratory to create realistic human performance models for balance-of-plant activities. Most HRA methods primarily address control room actions by licensed operators. In the EMRALD HRA models, activities outside the control room are modeled in the context of virtual human defenders and adversaries within a virtual environment. The permutations of

different scenarios will be modeled, considering especially the impacts of relevant PSFs on overall scenario outcomes. Modeling assumptions will be validated with plant personnel.

The product of this physical security HRA will be a more realistic assessment of the effectiveness of defensive personnel and insights on possible ways to decrease the success rate of adversaries. By tracing through possible effects beyond entry to the plant, the HRA modeling will allow identification of those areas of greatest risk to physical security breaches. These inputs will serve as ways to increase security margins and new opportunities to take credit for protection of the plant.

3.5 Force-on-Force Inspection

NRC has established a set of regulatory requirements for nuclear facilities to ensure that these facilities do not impose undue risk to the health and safety of the public, thereby providing reasonable assurance of adequate protection of public health and safety. The current body of NRC regulations and their implementation are largely based upon deterministic or prescriptive methods. These deterministic methods have been used to establish design and operational requirements necessary for obtaining regulatory approvals for construction and operation of nuclear facilities. Similarly, the deterministic or prescriptive approach has been used by NRC to establish the set of requirements and expectations for nuclear facility physical security.

The deterministic approach used for design and operational considerations establishes conservative requirements for engineering margin and quality assurance in design, manufacture, and construction. In addition, it requires assumptions relative to adverse conditions that can exist (e.g., equipment failures and human errors) and establishes a specific set of design basis events (DBEs). The deterministic approach then requires that the facility include safety systems capable of preventing or mitigating the consequences of those DBEs to protect public health and safety. Those structures, systems, and components (SSCs) necessary to defend against the DBEs are defined as "safety-related," and these SSCs are the subject of additional regulatory requirements intended to ensure that they are of high quality and reliability, and capable of performing their intended function during postulated design basis conditions.

A risk-informed approach would modify this traditional deterministic approach by considering a broader set of potential challenges to plant safety (e.g., beyond DBE), providing a logical means for prioritizing these challenges based on risk significance, and considering a broader set of capabilities to respond to these challenges. In contrast to the deterministic approach, a risk-informed approach would address the impact of credible initiating events by assessing event frequency, mitigating system reliability and event consequences, and enabling treatment of SSCs in accordance with their relative risk-significance over the lifetime of the facility. More specifically, a risk-informed approach consists of a categorization process to determine the risk significance of SSCs, determination of appropriate SSC requirements to maintain SSC functionality and reliability, and periodic assessments to make categorization and/or requirement adjustments based on operating experience and feedback, as needed. The overall result intended to be emphasis on risk-significant SSCs (i.e., those components most important to nuclear safety) that ensure safety while improving efficiency. Underlying risk assessment techniques utilized by a risk-informed approach would range from very simple and qualitative to more complex and quantitative.

Using a risk-informed approach such as this to inform physical protection of nuclear facilities would not only prioritize challenges for the licensee based on risk significance, but would also result in an NRC inspection program focused on these priorities to assist licensees in mitigating these challenges, and a physical security inspection program consistent with other inspections within nuclear reactor regulation.

4. REFERENCES

1. Idaho National Laboratory. (2017). “Economic and Market Challenges Facing the U.S. Nuclear Commercial Fleet – Cost and Revenue Study” (INL/EXT-17-42944). Idaho Falls: Idaho National Laboratory.
2. United States Nuclear Regulatory Commission. “Emergency Preparedness in Response to Terrorism”. https://www.nrc.gov/about-nrc/emerg-preparedness/about-emerg-preparedness/response-terrorism.html#one
3. United States Nuclear Regulatory Commission. Title 10, Code of Federal Regulations, Part 73. “Physical Protection of Plants and Materials”. https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/
4. United States Nuclear Regulatory Commission. Title 10, Code of Federal Regulations, Part 73 Section 55. “Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors Against Radiological Sabotage”. https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0055.html
5. United States Nuclear Regulatory Commission. Title 10, Code of Federal Regulations, Part 73 Section 56. “Personnel Access Authorization Requirements for Nuclear Power Plants”. https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0056.html
6. United States Nuclear Regulatory Commission. Title 10, Code of Federal Regulations, Part 73 Appendix C Section II. “Licensee Safeguards Contingency Plans”. https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-appc.html
7. United States Nuclear Regulatory Commission. Title 10, Code of Federal Regulations, Part 73 Section 54. “Protection of Digital Computer and Communication Systems and Networks”. https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0054.html
8. Garcia, Mary Lynn. “Vulnerability assessment of physical protection systems”. Elsevier, 2005.
9. United States Nuclear Regulatory Commission. “Achieving Modern Risk-Informed Regulation”. https://www.nrc.gov/docs/ML1811/ML18110A187.pdf
10. United States Nuclear Regulatory Commission. Title 10, Code of Federal Regulations, Part 73 Section 25. “Performance capabilities for physical protection of strategic special nuclear material in transit”. https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/full-text.html#part073-0025
11. United States Nuclear Regulatory Commission. Title 10, Code of Federal Regulations, Part 73 Section 45. “Performance capabilities for fixed site physical protection systems”. https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/full-text.html#part073-0045
12. United States Nuclear Regulatory Commission. Title 10, Code of Federal Regulations, Part 73 Section 45. “Requirements for the physical protection of stored spent nuclear fuel and high-level radioactive waste”. https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/full-text.html#part073-0051
13. Nuclear Energy Institute, “Guidance for Optimizing the Use of Portable Equipment”, NEI 16-08, Washington D.C., 2017.
14. Idaho National Laboratory. “Event Modeling Risk Assessment using Linked Diagrams (EMRALD)”. https://emrald.inl.gov/SitePages/Overview.aspx

Appendix A
Comparison of PIDAS Sensors

Sensor	Active/ Passive	Covert/ Visible	LOS/ Terrain	Volume /In Line	Fence Mounted/ Free Standing/Installed	Install Cost	Advantages	Disadvantages	Maintenance	Tech Level	Testing Time	Health Monitoring	Mean Time Between Failure
Microwave													
Bistatic MW	Active	Visible	LOS	Volume	Free Standing	High	Large detection area, Hard to bypass,	Medium NAR, Weather, Small animals, plant growth in detection path	High	Skilled techs	High	Available	High
Monostatic MW	Active	Visible	LOS	Volume	Free Standing	High	Large detection area for hard to cover areas, Easier installation	Medium NAR, Weather, Small animals, plant growth in detection path	High	Skilled techs	High		High
Interior MW	Active	Visible	LOS	Volume	Free Standing	High	Large detection area for hard to cover areas, Easier installation	Sees movement thru walls, Does not work well with other MW	Medium	Reg techs	Medium		High
Interior dual MW and PIR	Active	Visible	LOS	Volume	Free Standing	Low	Low NAR, Large interior detection area	Defeat one sensor then sensor is defeated	Low	Reg techs	Low	Available	High
Radar	Active	Visible	LOS	Volume	Free Standing	Very High	Early warning, Low NAR	Operator overload	Medium	Skilled techs	High	Available	High
3D (Lidar)	Active	Visible	LOS	Volume	Free Standing	High	Reduce operator load, Detect wide range of movement, detect movement that operator can not detect	Weather	Medium	Skilled techs	Medium	Available	High

Sensor	Active/ Passive	Covert/ Visible	LOS/ Terrain	Volume /In Line	Fence Mounted/ Free Standing/Installed	Install Cost	Advantages	Disadvantages	Maintenance	Tech Level	Testing Time	Health Monitoring	Mean Time Between Failure
Fence													
Electro-mech	Passive	Visible	Terrain	Line	Fence Mounted	Low	Easy installation, Fence is existing	High NAR, Requires robust fence	Medium	Reg techs	Medium		Medium
Strain	Passive	Visible	Terrain	Line	Fence Mounted	Low	Easy installation, Fence is existing	High NAR, Requires robust fence	Medium	Reg techs	Medium	Available	Medium
Geophones	Passive	Visible	Terrain	Line	Installed	High	Early warning, Low NAR	Buried cable breaks	Medium	Reg techs	Medium	Available	High
Coaxial	Passive	Visible	Terrain	Line	Fence Mounted	Low	Easy installation, Fence is existing	High NAR, Requires robust fence	Medium	Reg techs	Low		Medium
Fiber	Passive	Visible	Terrain	Line	Fence Mounted	Medium	Easy installation, Fence is existing	High NAR, Requires robust fence	Medium	Reg techs	Medium	Available	High
E-Field	Active	Visible	Terrain	Volume	Fence Mounted/Free Standing	High	Large detection area, Hard to bypass,	High NAR, Weather, Small animals, plant growth in detection path	Medium	Reg techs	High		Medium
Taut Wire	Passive	Visible	Terrain	Line	Fence Mounted/Free Standing	High	Low NAR, Large detection area, Hard to bypass	Weather, Small animals	Medium	Reg techs	Low		Medium
Ported Coax	Active	Covert	Terrain	Volume	Installed	High	Large detection area, Hard to bypass	High NAR, must be away from metal	Medium	Reg techs	High		High
Wireless fence detection	Active	Visible	NA	Volume	Fence Mounted/Free Standing	High	Large detection area, Hard to bypass	Low NAR, Weather, Small animals	Medium	Reg techs	Low	Available	High

Sensor	Active/ Passive	Covert/ Visible	LOS/ Terrain	Volume /In Line	Fence Mounted/ Free Standing/Installed	Install Cost	Advantages	Disadvantages	Maintenance	Tech Level	Testing Time	Health Monitoring	Mean Time Between Failure
Infrared													
Active	Active	Visible	LOS	Line	Installed	High	Low NAR, Hard to bypass	Weather, Small animals	Medium	Reg techs	Low		High
Passive	Passive	Visible	LOS	Volume	Installed	Low	Low NAR, Hard to bypass	Weather, Small animals, High Temp	Low	Reg techs	Low		High
Doors and Enclosures													
Tamper SW	Passive	Covert			Installed	Very Low	Early warning. Low NAR, Hard to bypass		Low	Reg techs	Low		High
Balanced Mag SW	Passive	Covert/Visible			Installed	Very Low	Early warning. Low NAR, Hard to bypass		Low	Reg techs	Low		High
Video													
Cameras	Passive	Covert/Visible	LOS	Volume	Installed	Varies low to high	Digital provides better images for many users, more imaging options	Analog at EOL, less options	Medium	Reg techs	Low	Available	Medium
DVR/NVR	Passive	Visible				Varies low to high	Allows review of past events, Used for training, face recognition	Operator overload, date storage	Medium	Reg techs	Low		Medium
Video Motion Detection	Passive	Visible				Varies low to high	Reduce operator load, Detect wide range of movement, detect movement that operator can not detect	Weather, camera shaking, requires good image contrast, no compression	Medium	Reg techs	Low		Medium

Sensor	Active/ Passive	Covert/ Visible	LOS/ Terrain	Volume /In Line	Fence Mounted/ Free Standing/Installed	Install Cost	Advantages	Disadvantages	Maintenance	Tech Level	Testing Time	Health Monitoring	Mean Time Between Failure
Unmanned Aerial Vehicle													
Surveillance Drones Tethered	Active	Visible	LOS/Terrain	Volume	Installed	Varies low to high	Reduce operator load, Detect wide range of movement, detect movement that operator can not detect, Can stay on station almost indefensibly, Can be deployed on intrusion event	Requires good camera for image contrast, used in conjunction with bullet detection	Medium	No skilled pilot	Medium	Available	Medium
Surveillance Drones	Active	Visible	LOS/Terrain	Volume	Free Standing	Varies low to high	Reduce operator load, Detect wide range of movement, detect movement that operator can not detect	Weather, requires good camera for image contrast, limited flight time	Medium	skilled pilot	Medium	Available	Medium
Defense Drones	Active	Visible	LOS/Terrain	Volume	Free Standing	High	Prevent aerial attacks, Capture drone for analysis	FAA regulations, Legal consequences	High	skilled pilot	Medium	Available	Medium
PPS Testing Drones	Active	Visible			Free Standing	Varies low to high	Reduce testing time and manpower	FAA regulations, Legal consequences	Medium	skilled pilot		Available	Medium