SANDIA REPORT
SAND2021-15712
Printed November 2021

Physical Protection Recommendations for Small Modular Reactor Facilities

Alan Evans, Commie Byrum, Dennis Stanford, Emily Sandt, Tommy Goolsby

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

Issued by Sandia National Laboratories, operated for the United States Department of Energy by National Technology & Engineering Solutions of Sandia, LLC.

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@osti.gov
Online ordering:	http://www.osti.gov/scitech

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Rd
Alexandria, VA 22312

Telephone:	(800) 553-6847
Facsimile:	(703) 605-6900
E-Mail:	orders@ntis.gov
Online order:	https://classic.ntis.gov/help/order-methods/

ABSTRACT

This recommendation document will provide international partners insight on physical protection systems (PPSs) for small modular reactors (SMRs). SMRs create many unique challenges for physical protection that must be addressed in design and implementation. This document will attempt to highlight possible challenges of SMRs and identify potential physical protection recommendations to mitigate these challenges. These recommendations are based on hypothetical SMR facilities and PPSs and their effectiveness against hypothetical adversaries.

ACKNOWLEDGEMENTS

The team would like to thank the many subject matter experts who contributed to content development and technical review of this document. The team would also like to thank the Department of Energy's Office of International Nuclear Security for funding this effort.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

This recommendation document will highlight specific physical protection concerns related to small modular reactor (SMR) nuclear power facilities. The recent international interest in developing SMR technologies poses a new challenge in successfully designing and implementing physical protection systems (PPSs). This document will highlight specific considerations for national regulatory bodies, security system designers, and implementers regarding the use of SMR technology. This document will begin with a discussion on security-by-design (SBD) and how SBD can be applied to PPSs and SMR nuclear power facilities. The discussion will focus on designing adequate PPSs for SMR facilities, starting from the initial design and site selection, through the process of building the facility and the PPS, and lifecycle considerations for maintaining the PPS and adapting to emerging threats and technologies. The second section of this document will focus on specific considerations for the three key functions of a PPS: detection, delay, and response for SMR nuclear facilities. This document is intended to be consistent with applicable International Atomic Energy Agency (IAEA) guidance—specifically, IAEA Nuclear Security Series No. 13, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) and IAEA Nuclear Security Series No. 27-G, Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Revision 5). This document does not address security management, nuclear material control and accounting, or cybersecurity.

ACRONYMS AND DEFINITIONS

Abbreviation	Definition
AC&D	access control and display
AI	active infrared
AR	advanced reactor
BWR	boiling water reactors
CA	control action
CAS	central alarm station
CDP	critical detection point
DBT	design basis threat
DEPO	Design Evaluation Process Outline
DMA	deliberate motion analytics
FAR	false alarm rate
FoF	force-on-force
HCF	high consequence facilities
HRC	high radiological consequence
HTGR	high temperature gas cooled reactors
HWR	heavy water reactor
IDS	intrusion detection systems
IA	inner area
IAEA	International Atomic Energy Agency
INS	International Nuclear Security
iPWR	Integral-pressurized water reactor
LAA	limited access area
LBWC	land based water-cooled
LLEA	local law enforcement agencies
LWR	light water reactor
NMAC	nuclear material accounting and control
NPP	nuclear power plant
MBWC	marine based water-cooled
Mod/Sim	modeling and simulation
MOU	memorandum of understanding
NAR	nuisance alarm rate
PA	protected area
P_D	probability of detection
P_E	probability of effectiveness

Abbreviation	Definition
P_I	probability of interruption
P_N	probability of neutralization
PIC	personal identification card
PIN	personal identification number
PPS	physical protection system
PRA	probabilistic risk assessment
PWR	pressurized water reactor
ROWS	Remotely Operated Weapon Systems
RTS	representative threat statement
SBD	security-by-design
SLM	sabotage logic model
SMR/AR	small modular reactor and advanced reactor
SMR	Small Modular Reactor
SNL	Sandia National Laboratories
SSO	safety, safeguards, and operation
STAMP	systems theoretic accident model and process
STPA	systems theoretic process analysis
TUAS	tethered unmanned aircraft systems
UAS	unmanned aircraft systems
UCA	unsafe control actions
URC	unacceptable radiological consequence
VA	vulnerability assessment
VAI	vital area identification

This page left blank

1. SMALL MODULAR REACTORS BACKGROUND

Small modular reactors (SMRs) and advanced reactors (ARs) are currently being considered by many member states of the International Atomic Energy Agency (IAEA) as possibly viable options to contribute to mitigating the effects of climate change. These reactors also provide the potential for flexible energy production [1]. SMR technologies aim to advance water-cooled, fast neutron spectrum, and high-temperature gas-cooled reactor technologies, as well as non-electric applications [1]. There is international interest in implementing SMRs because of their unique characteristics. These characteristics include incremental deployment to match increasing energy demand; significant cost reduction through modularization and factory construction; and non-electrical applications such as industrial heat, hydrogen production, and desalination of water. Some technologies, including microreactors, are being considered to replace diesel generators for small islands, remote regions, and for deployment in emergency situations. Major milestones have been reached in SMR development, including the deployment of the Akademik Lomonosov floating power plant in the Russian Federation, which was connected to the grid and started commercial operation in May 2020. Currently, there are more than seventy SMR designs under development for various applications. Two industrial demonstration SMRs are under construction in Argentina (an integral-pressurized water reactor [iPWR], Carem) and in China (a high-temperature gas-cooled reactor, CAP1000). With the international push for SMR deployment, it is important that countries are aware of physical protection insights into SMR facilities because this approach to nuclear reactors may pose new and different challenges than those associated with "regular"/known nuclear power plants (NPP).

1.1. Small Modular Reactor Types

There are several SMR types at various stages of development and construction. This section of the document will identify and discuss some of the key features of various SMR facilities. For the purposes of this document, an SMR will be defined as a reactor facility that produces up to 300 MW, and a microreactor will be defined as a reactor that produces up to 10 MW. Figure 1-1 identifies some of the SMR technologies being developed internationally.

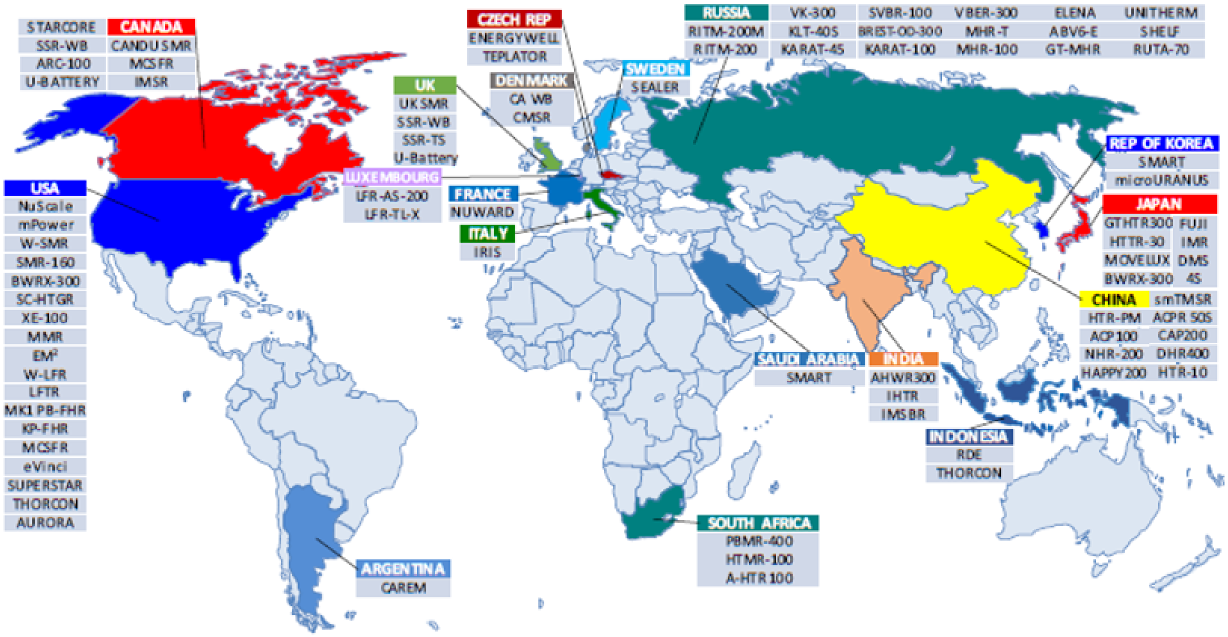

Figure 1-1. Global Map of International SMR Development [1]

Land-based water-cooled (LBWC) SMRs have various design configurations based on previous light water reactor (LWR) and heavy water reactor (HWR) technologies for on-land and on-the-grid applications. There are many international developments in LBWC SMR designs, including designs for iPWRs, loop-PWRs, boiling water reactors (BWRs), CANDU-type designs, and pool-type reactors for district heating.

Figure 1-2 shows some of the proposed SMR facilities being developed in the United States.

Figure 1-2. SMR Facilities [2], [3], [4]

As can be seen in Figure 1-2, these planned sites have significantly smaller footprints and more futuristic designs than much of the current fleet of nuclear power facilities. SMR facilities are being designed to have smaller site footprints, smaller physical protection system (PPS) infrastructure, and decreased onsite security personnel. The sites are intended to have fewer buildings and collate reactors within the same reactor building. This is meant to keep site footprints smaller and decrease construction costs, which potentially consolidates theft and sabotage targets into a smaller location and could enable more efficient protection strategies.

These reactor types provide considerable versatility by employing existing, mature reactor technology designs that can be used to provide electrical power when on-the-grid, district heating, and other purposes. The variety of operational purposes will impact the siting and location of such SMR technologies, which affects the security systems needed to secure the facilities. For example, facilities used for district heating will need to be located near a metropolitan or industrial area. Additionally, regulators may need to consider the operational purpose of an LBWC SMR when it comes to siting the SMR and selecting the PPS needed to secure it. SMRs placed in urban environments may require different security systems than SMRs in remote locations. The operating environment may also change potential threats to an SMR facility that could impact the design of a PPS.

Another SMR facility type is marine-based water-cooled (MBWC), which can be deployed in a marine environment, either through a barge-mounted floating power plant or an immersible underwater power plant. Immersible NPPs are not a novel concept; however, their use for electrical power production is novel. These SMR technologies can also be deployed as icebreaker shops. The first floating NPP was the KLT-40S for the Akademik Lomonosov floating NPP in Pevek, Russian Federation, which began operating in May of 2020.

1.2. Physical Protection Security Concerns for Small Modular Reactors

SMRs present unique challenges in security. SMR facilities will be much smaller than traditional NPPs, and SMR technologies have many applications, including electricity generation, district heating, and desalination in remote and extreme environment deployment. These operational environments must be considered when determining potential physical protection regulations and PPS designs.

The operational application for SMRs must also be considered, as this will determine potential facility siting. SMRs being developed for electricity generation may be placed near transmission stations or existing power plants, which are typically near urban areas. SMRs being used for district heating or process heating may be placed near industrial facility locations that are also near urban areas. These applications and sites require the consideration of particular types of threats and physical protection measures that may have not been considered for traditional NPPs. For example, near-urban applications may require an understanding of activist protests, environmentalist group activities, nuclear terrorism, and assessments of burglary crimes. When considering an urban environment deployment for SMRs, the regulatory body and site should consider a PPS that is effective against these types of threats, which require different protection levels and a response force that has a keen understanding of use-of-force. Addressing these threats as a part of the SMR PPS design process is necessary to ensure sites are appropriately protected.

SMRs are also being considered for remote environment deployment, including both land-based and marine-based SMR technologies. These SMRs may be deployed on remote coastal cities, remote scientific research facilities, and remote cities and towns. Remote deployments also face unique challenges, including potentially increased response times to the facility if an offsite response force is being considered. This may require the use of delay barriers to increase the adversary task time to achieve a malicious act. Remote deployment may also increase the time it takes for replacement equipment and compensatory measures to arrive to the site, so regulators and operators must consider the resiliency and lifetime of individual technologies and measures being implemented in the PPS. The site may consider having a spare part inventory for critical components or long lead items that are critical to the PPS. SMRs that are floating or transportable may also leverage technologies and lessons learned used to transport nuclear material.

SMRs placed in remote environments may also be exposed to extreme conditions. One option being considered because of ease of transport is microreactors. These could be used as an option after natural disasters to supply power to critical infrastructure, hospitals, and other facilities necessary to support recovery activities. Extreme environments may range from locations with high levels of precipitation (e.g., snow or rain) to decreased supporting infrastructure capabilities and decreased response capabilities resulting from the hazards of the environments. To assist in verifying facility operational and security personnel can effectively and safely perform their jobs at SMRs deployed in remote and extreme environments, tabletop exercises should be conducted using scenarios in which extreme environmental events may impact the security of the facility. These issues must be considered when implementing PPSs in extreme environments.

2. SECURITY BY DESIGN

Security-by-design (SBD) is an approach to integrating physical protection into the design of nuclear facilities while holistically including security, safeguards, safety, and operations [5]. SBD utilizes engineering design to enable security, safeguards, safety, and operations to be designed together to improve the overall effectiveness of these functions and decrease costs required to build, implement, and maintain the nuclear facility. This section will identify factors regulators, designers, and operators should consider for SMR facilities.

SBD is important for cost-effective deployment of SMR technologies and can be implemented to ensure the facility design aids the inherent effectiveness of the security system. By considering security in the design of an SMR, construction materials can be chosen that increase adversary task time, targets (i.e., reactors, spent and fresh fuel storage, safety equipment, etc.) can be placed below-grade, and a site location can be selected that provides inherent advantages to a PPS. Making these decisions at the beginning of an SMR design can enable decreased lifecycle operations costs and decrease the need for and the number of expensive retrofits made to the facility to improve security. SBD can also allow the facility to be designed with security features that can defend against beyond-design basis threat (DBT) capabilities and provide the facility with greater flexibility as the DBT changes.

2.1. Implementation of Security-by-Design

SBD must include regular communication and coordination in the design phase among the regulatory body, facility designers, reactor designers, future operational personnel, and site safety and security experts. Including this integration and interface at the design phase will improve facility operations, security, safeguards, and safety.

2.1.1. Security Interface with Safety, Safeguards, and Operation

Designing PPSs should include integration with and consideration of the interface that PPSs can have with safety, safeguards, and facility operations (SSO). PPSs and technologies can integrate with SSO components and systems to provide additional layers of protection and enforce SSO operations.

PPSs and technologies like access control, intrusion detection, and delay can be used to control access to safety and operational components at an SMR facility. Access control devices can be used to ensure that only authorized individuals are accessing operational equipment, provide surveillance over operational activities, and ensure proper use of operational equipment and systems. Access control devices also can be installed to ensure proper authorized access into operational equipment areas. These access control devices can be implemented to allow varying levels of access to the facility depending on authorization levels and other site determinations. Specific access control considerations will be discussed in a later section. Intrusion detection technologies can be used to monitor unauthorized access into areas with operational equipment and systems. These technologies may be used to ensure authorized access is occurring and provide direct observation of personnel entrances and exits into and out of areas with operational equipment. Delay technologies and barrier systems may be integrated with SMR facility designs to increase adversary task time to reach operational equipment. Ultimately, detection, delay, and response capabilities can increase the efficiency and use of operational equipment and systems. However, access control devices must be customized and adjusted depending on the type of SMR.

PPS technologies can be applied to protect safeguards program equipment through access control, intrusion detection, and delay technologies. Access control devices and systems can be used to maintain authorized only access to safeguards equipment and systems. These access control devices can be used to ensure two-person rules, proper access procedures, and controlled personnel access to safeguards technologies and systems. Controlling access to nuclear material accounting and control (NMAC) technologies ensures the proper implementation of safeguards programs.

2.2. Defining Protection Strategies and Requirements for Small Modular Reactors

A compromised SMR could lead to unacceptable consequences. To address these potential consequences, protection strategies at facilities with a sabotage concern are generally designed using a denial protection strategy. In other words, the adversaries must be denied the ability to perform actions that could result in an unacceptable radiological release.

A protection strategy defines the strategic goal of a PPS. In effect, it sets the win/loss threshold of a given system. It is an important concept to understand when designing, implementing, evaluating, or upgrading a PPS. Each protection strategy requires different levels of detection, delay, and response resources, which can in turn have a drastic effect on total system cost. Because of the sabotage concern, there are two primary protection strategies that can be utilized:

- Denial of task
- Denial of access

A denial-of-access strategy should be implemented when the mere presence of an adversary in a defined location results in a situation so grave the risk-accepting authority cannot accept the potential for such an event to occur. In practical terms, denial-of-access strategies should be employed to protect targets of sabotage concern when adversary timelines, once in the target location, are extremely short and the consequences of sabotage are very high. Traditionally, the denial-of-access strategy has been employed in protecting vital areas in NPPs; however, the case can be made that this application of the denial-of-access strategy is, in many cases, overly conservative.

Another denial strategy focuses on preventing an adversary from completing a task within an area. This strategy, denial of task, is preferred when an adversary must complete a series of actions or tasks before successfully sabotaging a target or releasing material. This strategy is generally suited to most targets of sabotage concern because once an area has been accessed, the adversary must physically complete one or more tasks before radiological material is assumed to be released or equipment damaged. This strategy is somewhat less resource intensive than a denial-of-access strategy, as the timeline for adversary success has increased and potentially allows for a longer response time for the response force.

Either strategy can be implemented. The decision on what strategy to use can be dictated by the regulator or it may be left up to the licensee. However, before any decisions are made as to which protection strategy to pursue, detailed validation activities should occur, such as a vulnerability assessment to determine system effectiveness, accompanied by a regulatory review and approval process.

2.3. Consultation with Local Law Enforcement Agencies

Interface with law enforcement is critical, especially if they provide all or some of the response. Formal agreements (memorandum of understanding [MOU]) or informal agreements may be necessary, depending on the requirements within a given country. Formal agreements are recommended when possible to reduce ambiguities.

Whether or not law enforcement provides response at the site, it is assumed they will be involved if the incident goes beyond the site boundary, whether the result is a release due to sabotage or removal of material. Consideration should be given to communication between various responding organizations. In the event of an attack or a nuclear security event, has a system been established that will allow for communication between those organizations?

The facility/site should have developed an emergency plan, security plan, and contingency plan as part of the initial design process. If those plans require coordination with law enforcement, is law enforcement aware of what actions they are expected to perform?

Potential topics for MOU/formal agreements:

- Constabulary authority for onsite responders (if any)
- Law enforcement authority on site (e.g., arrest, use of force, etc.)
- Law enforcement authority (e.g., local and provincial/state) related to material outside of regulatory control
- Law enforcement oversight of weapons qualification for onsite responders (if any)
- Law enforcement authority over use of force (i.e., lethal or non-lethal) for onsite responders (if any)

This list should not be considered all-inclusive. Ministerial and regulatory authorities will differ from one country to another. Those differences may result in the removal of some of the above items or the need for additional items.

This page left blank

3. ENGINEERING APPROACHES FOR PHYSICAL PROTECTION SYSTEMS

PPS designers must take a systems-engineering approach to designing PPSs for SMR facilities. The Design Evaluation Process Outline (DEPO) methodology, outlined in Figure 3-1, has been used for many years in designing and analyzing PPSs and can be applied for developing effective PPSs for SMR facilities [9]. This methodology is divided into three major steps: Define PPS Requirements, Design/Characterize the PPS, and Evaluate the PPS.

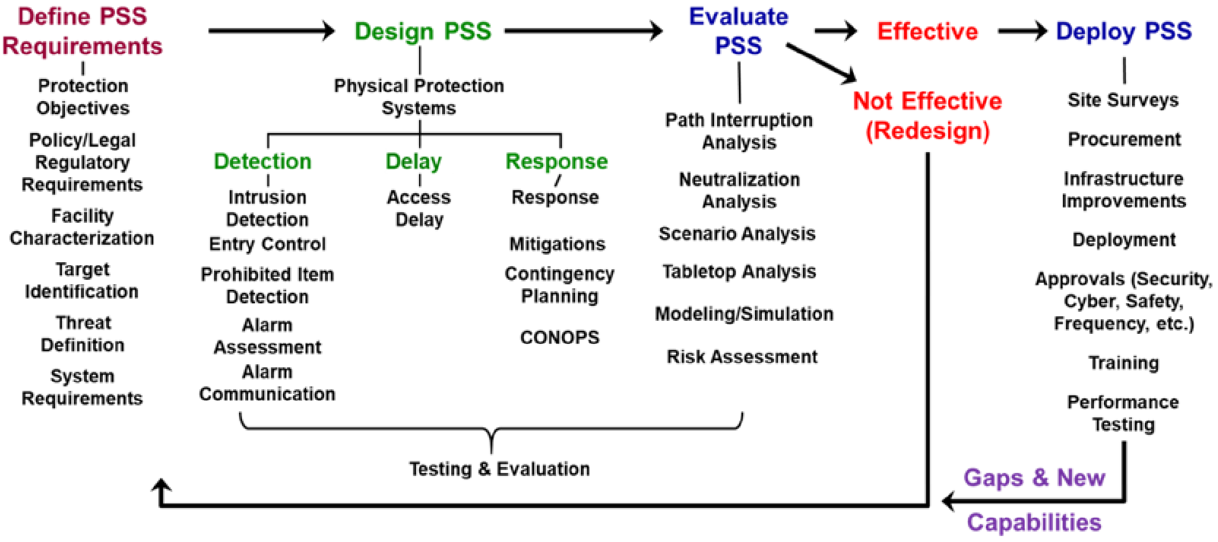

Figure 3-1. DEPO Methodology

The DEPO methodology, which has been used to design and analyze security systems for high consequence facilities (HCF) for decades, can be used within an SBD framework to design security systems into an SMR facility before deploying it. Incorporating this methodology at the beginning of an SMR facility design may improve the effectiveness of the PPS and decrease the installation cost of a security system for an SMR facility. Using the DEPO methodology in the design phase can also increase the operational efficiency of an SMR facility by integrating the PPS design at the beginning of the facility design.

3.1.1.1. Defining PPS Requirements

When designing any new system, a regulatory review should be the first step of the process to determine what current requirements are in place for the PPS. This process may determine the targets, type of protection strategy to employ, specific performance requirements of the system elements, and the threat to defend against. Furthermore, the regulations will determine if the regulatory body prescribes the physical protection requirements or if the regulatory body requires a performance-based system.

Next, the characterization of the facility is required. This step examines anything that may impact the performance of the security system, such as physical and environmental conditions, operations, policies and procedures, regulatory requirements, and safety requirements. An example of this could be any type of terrain that hampers visual observation or limits the ability of a particular technology to be effective. Another example would be any type of operational impacts that could limit the types of PPS elements that are used in the facility.

The next step is to identify the facility targets. This would include listing or defining and then categorizing the inventory of nuclear and other radioactive materials within the facility . It would also include identifying components or equipment that, if compromised, could lead to indirect sabotage.

Finally, the threat the facility must defend against would need to be defined. For NPPs, this is typically outlined in the form of a DBT or a representative threat statement (RTS). The DBT or RTS is set by the regulatory body, in cooperation with intelligence agencies and security and law enforcement agencies in-country. In addition, this threat should cover the equipment and capabilities possessed by both outsiders and insiders.

3.1.1.2. Design/Characterize the PPS

PPS designs are based on minimizing security risk as much as possible, and to an extent that satisfies requirements from a regulatory body. A PPS should protect nuclear material and nuclear facilities against theft and sabotage to minimize the risk to the environment and public.

3.1.1.2.1. Security Risk Management

Risk is defined in *Risk Management: A Tool for Improving Nuclear Power Plant Performance* (IAEA-TECDOC-1209) as, "The potential for things to change, and the magnitude of the consequences if they do change" [6]. The term risk is used in various fields—safety, accident analysis, health, finance, and many others—to mean different things. In general terms, risk refers to the possibility of future harm or loss resulting from the occurrence of some undesired event. Risk involves two factors: (1) the likelihood of an undesired event occurring and (2) the consequences that result if it occurs.

In safety, risk is defined as the likelihood of an initiating (abnormal) event and the magnitude of the consequences of the event. Initiating events are random in nature and could be the result of equipment failure, human error, natural disaster, or other random occurrences. Security risk is the possibility of future harm or loss due to malicious actions of a person or group of persons. These are planned acts, not random events.

Undesired events span a large range, including events resulting in:

- Loss or damage to property or facilities
- Injuries or death to people
- Damage to the environment

Nuclear security risk is the likelihood that a threat (a person or group of persons) is successful in attempting to cause an undesired event paired with the consequence of the undesired event. Nuclear security risk can be portrayed as the qualitative or quantitative expression of possible harm, which considers the likelihood that acts to cause an undesired event are successful and the consequences of those acts.

In the *Amended Convention on the Physical Protection of Nuclear Materials* (CPPNM) [7], two types of undesired events are of concern on an international level with regard to nuclear material and facilities:

- Unauthorized removal (theft) of nuclear material
- Sabotage of a nuclear facility or nuclear/radiological material

A model of security risk applied to nuclear security is based on the underlying assumption that nuclear security risk can be described using three important factors that contribute to risk. These factors are:

- Consequences of the undesired event if successful
- Probability the PPS will prevent the undesired event
- Likelihood of a threat attempting to cause an undesired event

Assessing these factors to the extent possible provides insights into nuclear security risk and aids in decision-making.

3.1.1.2.2. PPS Design Principles

PPSs are based on key elements such as defense-in-depth, balanced protection, and a graded approach to protection. These three elements are used to design PPSs that are effective for securing nuclear facilities and can be effective for designing SMR facilities.

Defense-in-depth is the concept of providing multiple layers of physical protection technologies, policies, and procedures to protect nuclear facilities. Defense-in-depth uses the concept of multiple security areas that increase the likelihood that an adversary can be detected and increase the likelihood that the adversary is delayed, allowing for an effective response to a nuclear security event. Security areas or layers are used to create defense-in-depth. This can be seen in Figure 3-2 .

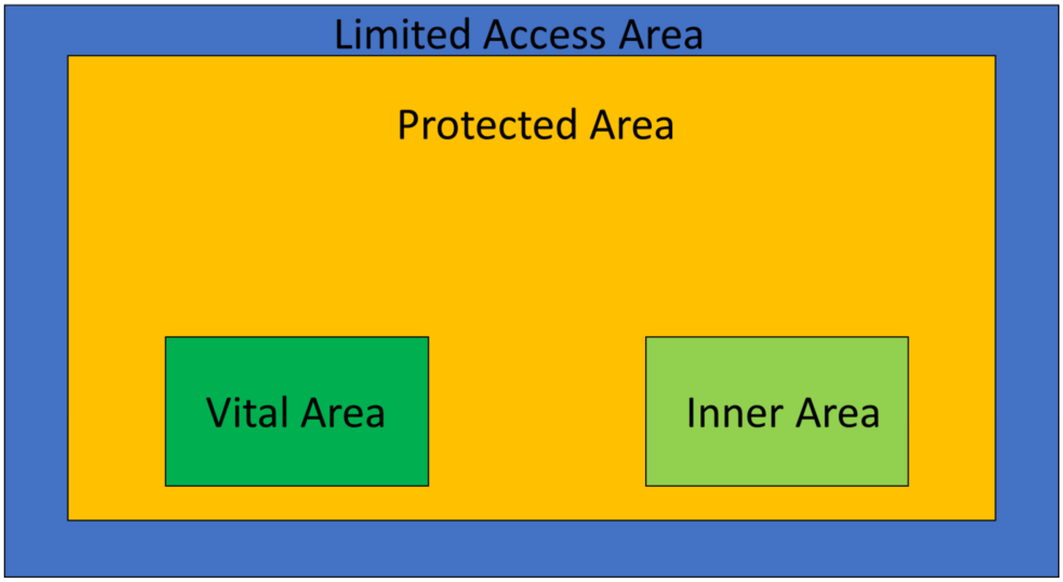

Figure 3-2. PPS Security Areas

These security areas provide layered protection of nuclear material and targets that, if sabotaged, could provide a radiological release. These security layers are based on another PPS concept, using a graded approach.

A graded approach is used to protect high consequence materials. Using the security layers note in Figure 3-2, Category-III nuclear material should be stored within a limited access area (LAA), Category-II nuclear material should be stored within a protected area (PA), and Category-I nuclear material should be stored within an inner area (IA). This requires higher consequence material to be stored in more secure locations. Vital areas are used to locate material, safety systems, structures, and components that, if sabotaged, could result in an unacceptable radiological consequence (URC) or high radiological consequence (HRC). For SMR facilities an LAA, PA, and vital areas may be required to protect the facility from theft and sabotage.

The final key element in PPS design is balanced protection. Balanced protection is used to ensure there is not one adversary path to a target location that is more vulnerable than another path to a target location. Balanced protection uses detection technologies and delay barriers along all potential adversary pathways to a target location to ensure a response force can interrupt and neutralize an adversary force.

When designing a PPS system, detection is one of the first elements to evaluate. Detection is the first key function used to prevent an adversary from accomplishing a malicious act. The earlier an adversary is detected, the greater the chances the response force will be successful in preventing the malicious act. The detection elements are most effective when each element is supplemented by operational and procedural controls that are correctly installed, maintained, and tested. Lapses in detection element implementation can lead to a single point failure in a security system. Security systems with single point failures are particularly vulnerable to insider exploitation because an insider may know more about the facility, and its detection capabilities than most security managers. With this in mind, facilities should pay close attention to things like sensor selection, which should be based on the facility characterization. Each detection element has different characteristics; therefore, it is often beneficial to use multiple and complementary sensor types.

The next step is to design the delay elements of a PPS system. These elements are designed to impede the adversary once they are detected. The use of effective delay elements provides the response force with adequate time to respond and interrupt or neutralize the adversary in a timely manner. Delay can be accomplished using passive and active delay elements. Facilities should evaluate the use of multiple types of delay elements, which forces the adversary to change tools or tactics during the attack.

The last element of an effective PPS system characterization or design is the response. For a response to be effective, both interruption and neutralization of the threat are required before the adversary can complete their task. In addition, response must be of adequate size, arrive in a timely manner, and have the proper response protocols in place. These response plans and procedures need be well documented and validated prior to any implementation. One of the considerations that needs to be closely reviewed is the placement of response forces. Adversary task times for sabotage events on these types of facilities can be extremely short. Ensuring the response forces can interrupt the adversary is critical in achieving an effective design. When designing a system, the decision to use offsite or onsite response forces should be based on a thorough analysis. In addition, ensuring that an effective response strategy is coupled with the appropriate detection and delay elements is vital in the design phase so that costly upgrades do not have to be implemented later.

3.1.1.3. Evaluate the PPS

The final step in the DEPO process is to analyze the system effectiveness of the PPS.

Analyzing the likelihood that the response force will be able to interrupt the adversaries prior to the completion of the adversary task time is the first step. This is known as the probability of interruption. To accurately assess this, information is needed on the number of adversaries, their capabilities, and their tools according to the DBT/RTS. Additionally, the adversary pathways of concern to the sabotage and theft targets should be known. Once this data is gathered, it is used to analyze a series of scenarios.

In addition to probability of interruption, the probability of neutralization should also be analyzed. Essentially, this analysis involves comparing the number of adversaries and weapons (according to the DBT/RTS) to the response force in a defined scenario.

Finally, the overall system effectiveness should be evaluated. For a system to be effective against both theft and sabotage scenarios, the response force must both interrupt and neutralize the adversary prior to the adversary completing their task. To determine this, a site would analyze all targets onsite against the defined threat to determine how the total system performs. This would be accomplished using several tools such as adversary sequence diagrams or other path analysis tools, expert opinions, tabletop exercises, performance tests, force-on-force (FoF), or other modeling tools that postulate an adversary attack.

3.1.1.4. Deploy the PPS

All the above items should be considered before installation and testing of the PPS. Of particular importance is reviewing the intended design with the regulator. Following international guidance, the security plan is the document the operator uses to describe the security system to the regulatory body. It must be remembered that the security system includes people, procedures, and equipment. Once the design is finalized, the licensee may want to prepare a draft of the security plan for discussion with the competent authority to determine if there are any problem areas before initiating design.

Installation of the physical protection components should be coordinated with facility operations personnel to ensure the work does not inhibit site operations more than necessary.

Once the system is installed, correlative procedures will need to be developed, and system testing (acceptance or functional testing) should be performed. It is recommended that the licensee provide the competent authority an opportunity to observe the testing. It is also recommended that the licensee take photographs or video of testing activities. Upon acceptable completion of testing, the next step would be training personnel on operation of the new components. After completion of these activities, the security plan should be finalized by the licensee and submitted to the competent authority for review/approval. The competent authority may perform a site inspection to validate the security plan. Once the security plan is approved, the security system may begin operation.

This page left blank

4. SMALL MODULAR REACTORS AND PHYSICAL PROTECTION

PPSs are traditionally defined by three functions: detection, delay, and response, as shown in Figure 4-1.

Figure 4-1. PPS representation

The detection function is meant to detect threats and capabilities that are of concern to the facility, allow authorized access into the site, and enable a central alarm station (CAS) operator to quickly assess alarms. Access delay is meant to delay the adversary along their path line to a target location. If implemented as repeating layers of delay placed immediately after detection, the delay will also increase the probability of detecting an adversary. Once the intrusion is detected, assessed, and the response force is notified, the remaining time it takes for the adversary to complete each task and the total time after the response force notification that it takes for the adversary to achieve a malicious act will both be credited as delay time and not just task time. The response function requires adequately trained and equipped personnel who are capable of interrupting and neutralizing an adversary force attempting a malicious act. The response force is meant to interrupt (i.e., impede adversary movement to a target location) and neutralize (i.e., stop the adversary from moving forward through a malicious act) the adversary force. The concept of the PPS stool (Figure 4-1) emphasizes that to have an effective PPS, the legs of the stool need to be balanced. However, if one leg is limited in capability, the other two legs can be significantly increased in capability to make up for the weak leg and still result in an effective PPS.

Figure 4-2 shows the timeline comparison that PPSs are designed to meet. There are two competing timelines in PPSs: the adversary task time and the PPS timeline.

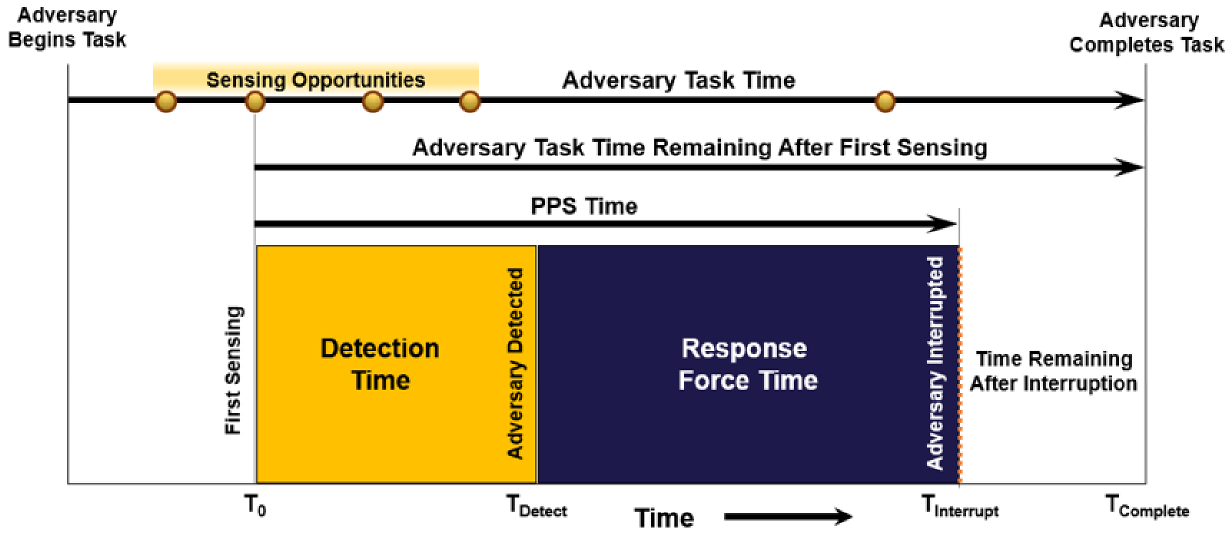

Figure 4-2. Security system timeline comparison

The PPS time must be less than the adversary task time after the adversary has been detected and the assessment and response portions can be initiated. Long response force times are being considered for SMRs. These long response force times are driven by the desire for less onsite staffing, meaning decreasing the number of onsite responders or potentially removing all onsite responders. This removal of onsite responders may require the use of local law enforcement agencies (LLEAs) to provide response to a nuclear security event. This must be taken into consideration, as a long PPS time will require improvements in detection and delay and careful design to be effective for the security of an SMR.

The following discussion will be based on the understanding that remote deployment will create a better understanding by regulators and operators of the PPS that is needed for an SMR site.

4.1. Target Characterization

An important step for developing an effective PPS is the identification of targets that must be protected from adversary attack. These target sets may change for SMRs due to the decreased complexity of safety systems, and especially safety systems that are external to the reactor.

SMRs may also have unique theft threats when compared to traditional NPPs. Spent nuclear fuel from NPPs is considered self-protecting and its protection levels can be lowered when considering theft of spent fuel. However, due to the high burnup being designed for some SMRs, there is potential to produce Category-I quantities of nuclear material in spent SMR fuel. This fuel could be considered a theft target and, therefore, sites may choose a higher-level of protection. These factors should be reviewed and understood by the regulatory body before the design of a PPS for an SMR.

4.1.1. Vital Area Identification

A vital area is an area containing equipment, systems or devices, or nuclear material, the sabotage of which could directly or indirectly lead to HRC. Traditionally, the vital area identification (VAI) process has been used to identify the areas and items within a facility that must be protected against an adversary threat to prevent HRC. It is recommended that States each determine thresholds between a URC and an HRC. The VAI method uses a fault tree basis to identify vital areas and leverages a probabilistic risk assessment (PRA) conducted to satisfy safety requirements as a large information input within the VAI process. The VAI approach considers various conditions such as at full power, on standby, refueling, and others to identify a full set of targets that must be protected. The VAI model utilizes the following steps [11]:

1. Identify radioactive material inventories (include this list in the sabotage logic model [SLM])
2. Determine if direct dispersal of these inventories is possible (include as an event in the SLM)
3. Identify initiating events (solely or in combination with a malicious act) that can indirectly lead to sabotage of each inventory
    a. This phase can leverage a PRA for the site
    b. It is important to identify mitigating systems for these events
4. Develop parts of the SLM to represent combinations of events that may lead to indirect sabotage
5. Eliminate events from the SLM that are beyond the DBT
6. Identify areas corresponding to events in SLM and replace events with their associated areas
    a. These events could include direct dispersals, initiating events, and mitigation system disablement events
7. Identify target sets, areas in which an adversary must gain access to cause a radiological sabotage event
8. Identify vital area sets, combinations of areas that must be protected to prevent sabotage
9. Select the vital area to be protected

The above-mentioned process should be considered as a method for identification of vital areas and target sets that must be protected in an SMR facility. Regulators could consider the implementation of the VAI process due to its robust use and implementation for identifying vital areas for the current fleet of NPPs. This robust use will provide SMR facilities and regulators with a foundation and examples on how the VAI process could be applied to SMR facilities.

4.1.2. Leveraging a Novel Approach

A novel approach in the nuclear security space may also be applicable for target set and vital area identification for SMRs. Systems Theoretic Process Analysis (STPA) is a top-down hazard analysis technique built on the Systems Theoretic Accident Model and Process (STAMP) causality model [12]. Briefly, STAMP combines pieces of systems theory (in the form of emergence and hierarchical concepts) with pieces of control theory (in the form of communication and constraint ideas) to identify hazards in a complex/large system [13]. The system consists of interrelated components that communicate via information/feedback loops and focus on a system's ability to maintain a state that eliminates losses resulting from being in an increased risk state that experiences an external event.

STPA extends this causality model to be used for the identification of undesired system states in complex systems. Such undesired states can result from physical and cyber system elements, component interactions, complex human decision-making actions, and other factors (e.g., social, organizational, managerial, etc.) related to the system. STPA does not prioritize or rank the hazards identified. Instead, it provides additional information and insight for decision-makers/designers to use when making decisions about implementing technologies and creating protocols. While STPA was originally designed for use in systems safety applications, it is discipline agnostic and has been used in a variety of applications. For example, STPA has been shown to be highly suitable for nuclear security, as it can be used to provide a structured problem-framing process to secure real systems and refocus efforts to improve concentric security layers toward manageable security control actions that allow security to be embedded in everyday work practices [14], [15], [16].

STPA consists of four prescriptive steps:

1. List the scope of analysis, losses of concern, and hazards that could lead to such losses
2. Construct the hierarchical control structure of the system
3. Identify unsafe (or insecure) control actions (UCAs)
4. Identify loss scenarios

The first three steps result in the identification of potential inadequate control actions that may lead to hazardous state(s). The last step provides a realistic causal scenario description in which such states could occur. For use in VAI or target set identification space, Step 4 is considered superfluous to the objective of the analysis. However, this step can be a convincing tool to justify how a scenario can occur for decision-makers.

In Step 1, the analysts bound the scope of the work and list the items/qualities that are important and cannot be lost[1]. This can include loss of radioactive material, loss of profit, loss of life, loss of reputation, etc. From the listed losses, a list of hazards[2] is generated. Example hazards can include not having heat removal capabilities, lacking reactivity control, reactor trip, etc. Losses and hazards are indexed (L1, L2, L3… for losses; H1, H2, H3… for hazards) for use in Step 3.

Step 2 requires the bulk of the background work for an analysis. For this step, system experts are needed to provide input and details on how the system is structured, what components can act as controllers (both digital and human), what components are controlled, as well as what actions controllers can take and what feedbacks they can receive. External controllers can also be considered, such as the electrical grid (to load follow). It is likely that this step will result in a large diagram of the control structure. Each of the actions identified should be numbered and labeled with what the action is. For example, one control action could be "digital controller inserts control rods" and another could be "digital controller withdraws control rods." Because these are two distinct actions, they should be separate control actions (versus a more generic control action of "digital controller moves control rods").

From the hierarchical control structure created in Step 2, the analysts construct a table of UCAs (although the nomenclature may be considered "unsafe" in a security application). The UCA table provides a set of conditions within which each control action (CA) is evaluated. These conditions are:

- Action was needed, but not provided (i.e., where procedures state an action should have been taken, but the controller/operator did not take the action)
- Action was provided, but not needed (i.e., where procedures do not state an action should have been taken, but the controller/operator acted)

[1] In STPA, "loss" is defined as involving something of value to stakeholders.

[2] In STPA, "hazard" is defined as a system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to a loss.

- Action was provided too early/too late/in the wrong order (i.e., where an action was taken before it should have been, after it should have been, or in an incorrect order from the procedures)
- Action was stopped too soon or applied too long (i.e., where an action was stopped before it should have been or continued beyond the point where it should have been stopped)

Each control action in the diagram from Step 2 is given a row in the table and evaluated in these four situational parameters (columns of the table). Each cell follows a general formula of:

<Source Controller> + <Situational Parameter> + <Control Action> + <Context>; <Hazard>

where the first four components form the "unsafe control action" statement, and the final component relates that UCA back to its associated hazard(s).

If a situational parameter does not apply (such as the time duration of a binary control action), the cell is left empty. If a situational parameter cannot be attributed to some sort of unsafe state by the system experts in the group, the cell is left blank. Any cell with an entry is considered a UCA and is insight for target set identification. An example UCA is below for the CA of *rotating control drum inward* under the situational parameter of action not being provided, but is needed:

CA 1a: Operator ***does not rotate*** control drum in when a lower power level is desired [H1, H4]

The bracketed information in the example refers to the numbered hazards identified in Step 1, allowing the analysts to directly trace each UCA back to the hazards within the problem scope. A single cell can have multiple entries if multiple contexts are identified.

Having system experts in the room for this effort is very important as those experts are likely to be able to devise how an action applied at the wrong time could affect the system and push it toward a hazardous state. Recall that cell entries are not "what will happen if *X* occurs" but are "if *X* happened and the worst-case environment incident occurred, there would be a loss" entries.

After completing the UCA table, many UCAs will have been identified. Since STPA does not prioritize or rank the UCAs, it is left to the subject matter experts to review the UCAs and determine which are of the most importance.

STPA requires minimal formal training and can be completed in a relatively quick timeframe depending on system size (order of weeks to months) if system experts are involved. Any STPA needs a group of people working collaboratively to combine their expert knowledge on the system (particularly for construction of the hierarchical control structure) and at least one person with STPA experience to act as a facilitator. The advantages of STPA as discussed can be beneficial for deployment of SMR facilities; it may decrease the analytical capabilities needed to conduct VAI and may allow for vital areas to be identified after modifications to the site have been made.

4.1.2.1. Advancements on STPA for use in VAI Space

VAI, using any method, requires the consideration of adversary capabilities and potential motivations. In the traditional VAI method from Section **Error! Reference source not found.**, the logic model is trimmed to remove those events that are beyond the DBT. In STPA, an analyst can add an adversary factor into Step 1—where losses/hazards are defined, and the problem is scoped [17].

For instance, an adversary could be a generic protester hoping to gain attention by causing a plant trip or total shutdown. Another adversary could be a violent extremist looking to cause core melt and a large release of radioactivity from the facility. Both adversary types (and others) can be analyzed using a single STPA, despite their wildly different objectives. The protester might be labeled “A1” and the extremist “A2.” Similarly to how hazards are tracked throughout the process, the adversary labels can be carried forward to the resulting UCA list. From there, when the analysts are selecting UCAs to focus on those of concern, the adversary may be readily considered in that decision-making process. This allows a single STPA of a design to be used in areas worldwide where threats may vary greatly and could be an advantage for wide deployment of a particular SMR design.

4.2. Threat Characterization

As with any design, the ability to characterize the threat the system must be designed to defend against is critical. Often, defining the threat is one of the most difficult things to do. In contrast to the past, there is no absolute, unequivocal, or explicit primary threat. Instead, nuclear facilities face complex threats generated by a diverse host of actors. The complexity of the adversary and threats are ever changing. This is particularly true for facilities that process or possess highly enriched uranium or plutonium. SMRs have a different threat environment than traditional NPPs may have. SMRs are being considered for deployment in urban environments, which may change the types of adversaries that may be considered in the DBT or RTS. These threats may range from terrorist groups, to environmentalist activists, to petty criminals. SMRs may also be placed in rural environments, which can result in a change to DBTs. These remote areas, coupled with a change in the DBT, could have impacts on the PPS designed to defend the facility.

The threat characterization is typically defined by the State. A State can perform this function in many ways, resulting in establishing a DBT or RTS that is shared with the licensees. This threat may be for radiological sabotage, or the theft of nuclear material, or both. Whatever the approach, the licensee should be required to design the PPS to defend against the threat. However, there are three approaches to the design of a protection system that a State can pursue:

- The competent authority will provide the DBT or threat to the licensee, along with guidance on effectiveness of the PPS to protect against it
- The regulator will establish performance requirements based on the DBT or threat statement and then provide the performance requirements to the licensee
- The regulator will define prescriptive requirements based on the DBT or threat statement and provide these to the licensee

Additionally, it should be noted that threat characterization is a continuous process. As new information becomes available or new capabilities are realized, it will be important to reevaluate the threat so there is a sound basis for the requirements, design, and evaluation of a PPS. Another important consideration for facilities is to properly characterize the knowledge that an adversary force may have about a particular SMR design. Due to the publicity of SMR designs, and inherent safety characteristics, regulatory bodies may consider the knowledge adversaries may have as part of the DBT or RTS.

4.3. Intrusion Detection Systems

Intrusion detection systems (IDSs) aggregate various components that sense adversary activity and transmit a signal to the monitoring station, where the operator performs assessment and initiates response if necessary. These devices include magnetic door switches, motion sensors, capacitance sensors, vibration sensors, etc. There are many types of sensors, each of which generally has a specific application. IDSs may be passive (e.g., device 'listens' or searches for energy coming from the adversary—an infrared sensor, for example) or active (e.g., device emits energy to detect the adversary—a break beam sensor, for example). These devices may be covert (i.e., hidden from view) or overt (i.e., visible), and can be volumetric (e.g., cover height, width, and length), or line detection (i.e., provide coverage of a narrow, two-dimensional area).

Sensor performance is described by three fundamental characteristics:

- Probability of detection (P_D)
- Nuisance alarm rate (NAR) and false alarm rate (FAR)
- Vulnerability to defeat

P_D is a statistical function that represents the lower confidence level of a binomial equation. If a sensor is tested 30 times and passes each time, the P_D is 0.9 at a 95% confidence level. This primarily means there is not enough testing to prove the P_D is any better than this.

A high NAR can degrade P_D because of the cry wolf syndrome. There are two kinds of alarms: valid alarms (e.g., an adversary entering the detection zone) and all other alarms, whatever the cause (i.e., these other alarms are all nuisances). A subset of nuisance alarms are false alarms[3]. It is important to know the FAR for a sensor. If the alarm is caused by a bird or rabbit that can be seen on the assessment camera, then the alarm is not a valid alarm (i.e., it was not an intruder), and the alarm was not a false alarm (i.e., the sensor was alarming correctly on an object), but it was a nuisance.

It is important to remember that detection cannot and does not occur without assessment. If the adversary opens an alarmed door, and no one assesses the alarm, there is no detection. If the P_D for a given device is credited at 0.95 but the alarm is not assessed, the actual P_D is 0.

SMRs should consider technologies that enable extended and earlier detection of an adversary force. Examples of these technologies could include LIDAR and RADAR. Extended detection can allow the site to detect adversary intrusion beyond the perimeter of the facility. This can be beneficial for sites to be deployed in rural environments. Detecting an adversary earlier can enable the response force to deploy earlier. This allows for improved probability of interruption and probability of detection.

4.3.1. Exterior Intrusion Detection

Most security requirements related to reactors require some sort of exterior detection system. The extent of that system is dependent on the regulatory requirements for a given country, but the PPS timeline (Figure 4-2) highlights the importance of detecting adversarial action as early outside the facility as possible. Exterior IDSs may be complicated by the desire for a smaller site footprint and to reduce the infrastructure and size of the PPS. However, the use of extended detection technologies may support an effective external IDS. This enables detection of the adversary at the facility perimeter and increases the amount of time available for the response to get into position. Detection of the adversary at the area boundary rather than at the target entrance will increase the effectiveness of the security system.

While each site will be unique, it is recommended that some sort of exterior intrusion detection and assessment is incorporated into the PPS. The most reliable and effective systems will include complementary sensors—two different types of sensors with the same coverage area. This increases

[3] A false alarm is any alarm that is from an unknown source.

the likelihood of detection and can complicate the adversary's attack plan because different defeat methods may be required for each type of sensor. The farther these sensors are placed from the facility, the greater the adversary task time, which means responders have more time to implement their protection strategy. Obviously, the perimeter increases in size as it moves away from the facility, which will increase the cost and complexity of the system. As stated above, the perimeter boundary may be placed based on nuclear safety/standoff analyses. If so, this is generally a good location to place exterior sensors within an isolation zone—two fences or barriers separated by some distance with the sensors placed in-between the fences.

The isolation zone is often configured in zones, and the IDS and assessment can be configured similarly, so the alarm indicates "zone 3" and provides assessors and responders with the location of the alarm. This may reduce both assessment and response time.

Exterior intrusion detection includes many different types of components suited to different purposes. A primary consideration for exterior sensors is environmental conditions. Different types of devices may operate differently under varying environmental conditions. Specific concerns are rain/storms, lightning frequency, annual temperature range, and humidity. Consideration should also be given to the size of the perimeter. A 2 km perimeter may not be difficult to cover with sensors and cameras. A 20 km perimeter would be much more complex and much more expensive.

4.3.1.1. Design Considerations for exterior sensors

Continuous line of detection – This requires the sensors form a continuous line of detection around the perimeter. In practice, this means configuring the sensor hardware so the detection zone from one perimeter sector overlaps the detection zones for the two adjacent sectors. Continuous line of detection is often violated at entry control points.

Balanced detection – No matter how an adversary attempts to accomplish their goal, effective elements of the PPS will be encountered.

Defense-in-depth – This means the use of multiple lines of detection. Protection-in-depth involves using different layers of detection, which could inclcude early warning, perimeter, and interior sensors. Thus, at least two continuous lines of detection are used in high-security systems.

Complementary sensors – The perimeter sensor system can achieve significantly better performance when different and complementary types of sensors are selected for the multiple lines of detection. (i.e., microwave and active infrared). Different sensor technologies with different P_D, NAR, and vulnerabilities are combined to increase the effectiveness of the exterior perimeter IDS. Complimentary sensors have overlapping detection, so they must be defeated at the same time. They also are affected differently by different weather conditions.

Priority schemes – A recommended method currently in use, this practice requires the system operator to assess all alarms with the aid of a computer that establishes the time order of assessment for multiple simultaneous alarms. The computer sets a priority for each alarm based on the probability that an alarm event corresponds to a real intrusion.

Another consideration for specific areas is the use of video motion detection. Video motion detection generally involves monitoring an image or set of pixels for changes, which will transmit an alarm signal. A benefit of video motion detection is that one device can provide both detection and assessment. A detriment is that video motion is based on the image and if the image is corrupted or obscured, the action may not be detected. For example, exterior video motion detection may be degraded in rain or fog conditions.

These considerations may apply to fixed-site and on-land SMRs. Technologies that have been applied to transportation security of maritime vessels, such as SONAR, RADAR, and LIDAR may also be applicable to SMRs that are placed on ships.

4.3.2. Access Controls

Access control methods should be selected and installed in accordance with regulatory requirements. Assuming a graded approach is used, this would mean access control at the site boundary or perimeter would be less restrictive than access control nearer to the target area. Exactly how this would be implemented will likely differ from one site to another, but it is recommended that some sort of electronic access control be established at the PA boundary, and that additional restrictions be implemented for IAs, vital areas, or other areas as recommended or required. Certainly, for IAs and vital areas, three factor authorization is recommended, as well as two-person authorization for specified target areas.

Using a graded approach, some areas or locations may have more stringent requirements than others. For example, the turnstile to enter the fenced area may have a proximity card reader that requires a personal identification card (PIC) and entering a personal identification number (PIN). A nuclear material storage area may require biometric access or even two-person authorization.

Access control tends to be discriminated by three factors:

- Something you have
- Something you know
- Something you are

Using the example above, the turnstile access (PIC and PIN) would be two-factor—something you have (PIC) and something you know (PIN). Vault access would be considered three-factor—something you have (PIC), something you know (PIN), and something you are (i.e., a fingerprint). The higher the number of factors, the more difficult it will be for an adversary to defeat. Clearly, the adversary's task increases greatly if all three factors are combined into a single system. Capturing a single factor (e.g., especially a PIC/credential or PIN) is not difficult. Capturing two is more difficult. Defeating a system that has combined all three is very difficult (e.g., PIN, plus coded badge, plus hand geometry).

Biometric access types include:

- Eye features like retina or iris
- Hand and finger features like palm print, fingerprint, or subcutaneous infra-red mapping
- Facial recognition
- Voice

Biometrics are based on measurable physical or behavioral features.

4.3.2.1. Design Considerations

To successfully implement biometrics in a security system, the devices must be easy to use and acceptable to the population that has to use them. Some people will likely resent using a biometric device for privacy or health concerns and, in some situations, people have refused to use biometric devices for religious concerns.

Throughput is another high-impact aspect, and will be a determining factor in how many devices will be required to get people into a facility in a timely fashion. Many devices allow for parallel processing of individuals into a facility.

The device's security is also a concern. Whether by imposter attack or simple physical attack, easily defeated devices are not suitable for high-security applications.

The reliability of devices will impact operating costs. Frequent repairs lead to higher operating costs. Also, when devices are not operational, personnel might have to go to other portals to enter the facility, causing delays and frustration. It will be important for SMR facilities to consider designing access controls into all onsite buildings and locations that may need them. This includes planned buildings to house reactors, as the site may modularize. Building in the access control systems at the beginning will decrease the cost to install these devices after the facility is built or retrofit the existing access control system.

SMRs are being designed to be operated by minimal personnel and minimal security staff. This may require a less complex access control system because there are fewer staff members onsite. If the onsite number of personnel decreases, there may not be a need to consider the operational throughput at entry control points like there is at the current fleet of NPPs. With the decreased number of personnel onsite, the access control system may only need to be applied at PA access points and vital area access points.

4.3.3. Interior Intrusion Detection

Interior and exterior intrusion detection equipment should contribute to a PPS that provides layered detection—multiple detection points along any given path. This enhances the likelihood of early detection of the adversary and complicates the adversary's progress along a given path, especially if the adversary encounters different types of detectors with different defeat methods along that path.

For a facility/structure, the assumption is that intrusion detection components would, at the least, be encountered from the entry point to the target. Alarmed turnstiles or doors at the entry point will provide detection when those items are not in use. As always, alarm assessment must be incorporated. Generally, doors that provide access to a target or vital area should be locked and alarmed. Emergency exit doors that cannot be locked should have 24/7 alarm indication.

SMR facilities will have to consider the smaller site footprint and the potential for a decreased number of target sets when designing interior IDSs. The decreased number of targets and smaller footprint will decrease the number of possible points where the adversary could be detected. Therefore, it is important to consider the design of the interior IDS. This ensures the adversary can be detected once inside the facility, and also that the CAS operators can assess and determine the location and movement of an adversary force.

Vaults, IAs, vital locations, and target areas should have some sort of volumetric or boundary IDS coverage. Volumetric sensors cover an area including length, width, and height. Boundary coverage includes walls, ceilings, floors, etc. Different types of sensors can be used to achieve the goals of the security system. In addition to a high probability of detection, environmental factors should be considered, including:

- Noise/vibration
- Temperature/humidity
- Heat sources

Vibrations and noise can interfere with some types of sensors, particularly those that use some sort of microphone or are designed to detect vibration. In addition, affixing any device to a surface with high vibration can cause operability issues.

Temperature and humidity are obvious considerations with any piece of equipment. It is important to ensure design specifications are consistent with temperature/humidity conditions found in the operating environment.

High heat sources can interfere with certain thermal or infrared sensors. If there is a high heat electrical cabinet in the coverage area, the adversary may be able to stand next to the cabinet without being detected. Infrared sensors generally emit infrared light into the area and measure the reflection. High heat equipment can also interfere with this.

4.3.3.1. Typical Interior Intrusion Detection Devices

Balanced magnetic switches – these are magnetic contacts placed on a door or other surface (e.g., cabinets, lockers, etc.) that will alarm after the door opens a specified distance.

Motion sensors – these sensors include passive infrared, monostatic microwave, sound, and dual technology (i.e., combination of two different types of sensors).

Video motion – Another consideration for specific areas is the use of video motion detection. Video motion detection generally involves monitoring an image or set of pixels for changes, which will transmit an alarm signal. A benefit of video motion detection is that one device can provide both detection and assessment. A detriment is that video motion is based on the image and if the image is corrupted or obscured, the action may not be detected. For example, exterior video motion detection may be degraded if the room is dark or if there is a high light source interfering with the camera. Some of this can be eliminated by using thermal camera video motion detection. However, thermal cameras cost much more than normal cameras, so using multiple units may be prohibitively expensive.

4.4. Access Delay

With any type of an attack, it becomes a race between the response force and the adversary unless the adversary is not detected, or not assessed, or the response force is not notified of the intrusion. To give the response force the possibility of interrupting and neutralizing the DBT adversary after attack notification, balanced delay should be implemented for all viable attack paths and the delay should be sufficient to expend all the DBT attack tools (e.g., hand, power, thermal, and explosives) prior to breach of the final denial barrier and prior to completion of the sabotage event. An effective delay system should consist of multiple types of delay (e.g., passive, active, and dispensable) designed to hamper the adversary team and aid the response forces. The delay elements are most effective when used in conjunction with detection elements against attacks by outsiders and less knowledgeable insiders. Insiders with the necessary access authorization and knowledge of the overall security system may be able to defeat some or all delays before the response force can arrive unless there are delays specifically designed to force the use of the two-person rule and those delays are beyond the capabilities described in the DBT for the insider. Detection must precede delay for the delay to truly be effective. Delay mechanisms should be numerous, different, requiring different adversary tools and skills, and increase in capability/sophistication as the adversary moves closer to the target, with each additional barrier requiring additional tools and/or access authorizations. Consideration should be given to implementing delay barriers beyond the capability of the DBT. Additionally, the importance of repeating layers of detection immediately followed by delay for all viable paths to the target is critical to the success of both detection and delay, which are both critical to the success of the response force.

Delay needs to be examined as part of an overall system that integrates the response force along with the different delay elements to ensure the interruption and neutralization of the adversary. The smaller footprint of SMR sites and their potential for remote deployment may result in a need for delay times that are much greater than that for the existing fleet of NPPs. Delay time needs to be designed to increase the adversary task time to reach the target locations. However, the use of delay systems can also impact the ability of the response force to properly respond and interrupt the adversary force.

To build in additional delay time, facilities should use multiple and different types of delay. Essentially, the role of the delay elements is to increase task times, hamper the adversary along their path or alter their path, increase the likelihood that the adversary does not have sufficiently capable tools, and increase the likelihood that lack of tool spares or tool failure will eliminate their ability to breach a barrier and channel them into a zone for response force interruption and neutralization. When implementing delay elements into a PPS, delay elements can be separated into two categories: passive delay and active delay.

For SMRs, system designers should consider identifying and analyzing site-specific conditions to determine the specific use, type, function, and placement of physical protection barriers needed to ensure the overall effectiveness of the PPS. The physical barriers at the site should be designed, constructed, installed, and maintained as necessary to control access into the facility, which should be controlled or denied to satisfy PPS requirements. The SMR's security plan should describe the physical barriers, barrier systems, and their functions within the PPS. Access delay technologies and physical barriers should be designed and constructed to protect against the DBT of radiological sabotage, and account for site-specific conditions. Physical barriers should provide delay and support detection, assessment, access controls, and mitigate the insider threat. Physical barriers should be implemented in a fashion that meets their intended purpose within the physical protection plan. Barriers with openings should be secured and continuously monitored to ensure these openings are not exploited. Whenever possible, moveable delay barriers should be implemented that fail secure in the event that they fail to operate. For example, two moveable delay barriers could be installed in series, such that one is always secured and only one can be accessed at a time (like the operation of a sally port). The site-specific conditions that affect land-based SMRs may not be applicable to marine-based SMRs. SMRs that are floating or on vessels may have to consider advanced concepts or methodologies to achieve effective delay.

To prevent vehicle penetration of the PA barrier, vehicle control measures should be implemented outside the PA barrier. This will also provide protection from vehicle bombs for plant personnel, equipment, and systems necessary to prevent acts of radiological sabotage at the SMR. Where possible, natural terrain features can be used as part of the vehicle control measures. If there is sufficient space within the PA, manmade earthen berms can be used for additional blast protection. However, this may not be applicable at all SMR locations with smaller footprints. Preventing the adversary vehicle(s) from reaching sabotage target areas forces the adversary to continue the attack on foot and significantly reduces the attack toolkit to only what can be carried.

Barriers external to the PA can provide early warning, early detection, elimination of line-of-sight adversary opportunities, and deter potential adversaries. Additional barriers such as fence and razor wire can be installed in strategic locations and, combined with other visible security features, can act as a deterrent and discourage adversaries by making the target less desirable. The adversary may opt to breach these barriers, which will expose the ill intent of the adversary and potentially provide early identification and response. This can be especially helpful to plants with a small footprint or vital areas on or near the PA barrier. After determining intent, these additional fences and razor wire may also be electrified on command to provide further deterrence and delay.

The PA perimeter at an SMR should be protected by physical barriers, with an isolation zone in outdoor areas adjacent to the perimeter barrier. This isolation zone should allow for surveillance on both sides of the PA barriers. The PA perimeter should be monitored with intrusion detection equipment and be capable of detecting both attempted and actual penetration of the PA perimeter barrier before penetration is completed. The isolation zone should be monitored with assessment equipment and provide real-time and play-back/recorded video images of the detected activities before and after each alarm annunciation.

The PA perimeter should limit personnel, vehicles, and materials access to those with authorization. These barriers should also be used for controlling the flow of personnel, vehicles, and materials into designated access control points.

PA perimeters and barriers should be separate from barriers that separate vital areas. Penetrations through the PA barrier should be secured and monitored in a manner that prevents or delays and detects the exploitation of any penetration. PA emergency exits should be alarmed and secured by locking devices that allow prompt egress during an emergency and yet satisfy the recommendations of this section for access control into the PA.

Another point for consideration at SMRs is adding delay features inside the PA. Delay barriers can be placed between the PA fence and vital areas or other structures to increase adversary task times. Delay barriers can provide additional time for immediate responders to engage, for supplemental responders to get into defensive positions, for off-site responders to deploy to the site, for the use of activated delays to increase barrier penetration times, and for the potential use of Remotely Operated Weapon Systems (ROWS). Some examples of delay barriers deployed in SMRs are fences, gates, mantraps, hardened doors, etc. Where possible, delay barriers should be able to be remotely activated such that upon declaration of a security event, the barriers can be secured immediately. Remotely activated delay barriers should not prevent or slow responders using designated response routes.

Vital equipment should be located only within vital areas, which should be located within a PA. This increases the adversary task time to reach vital equipment and build a security system using a layered (i.e., defense-in-depth) security approach. SMRs should be design to protect all vital area access portals and vital area emergency exits with intrusion detection equipment, locking devices that allow rapid egress during an emergency, hardened turnstiles, and hardened entry doors and that satisfy the vital area entry control recommendations of this section. Unoccupied vital areas should be alarmed and secured at all times. More than one vital area may be located within a PA. Active delay systems such as dispensables in vital areas may be activated by the CAS operator, automatically when multiple intrusion sensors alarm when the vital area is unoccupied, manually by guard force/response force patrols following a cyber-attack that has disabled the CAS access control and display (AC&D), etc.

4.4.1. Passive Delay

When delay elements are discussed, often the first thought is of the traditional fences, walls, gates, doors, etc. These are known as passive delay elements. The use of multiple barrier types needs to be carefully planned when designing a system. The need to use multiple types of barriers that consist of different materials or require different breaching techniques should be considered when selecting the types and placement of barriers. Often, traditional barrier elements are the easiest to implement and are designed to deter or defeat a less capable adversary. If looking to defeat an adversary with a higher level of capability, the selection and placement of these barriers becomes more difficult. The goal is to force the adversary to change tools and tactics at each layer of the system and to damage critical adversary attack tools with hidden delay features, etc. This change of tactics or tools on the adversary's part plus the tool breakage by hidden features adds time to their total task time, adds complexity to the attack, and aides the response.

4.4.2. Active Delay

Another option for access delay is the use of active delay elements. Often, these barriers are dispensable materials. These elements are frequently in the form of smoke, foam, irritants, stun technologies, deployable concertina wire, razor wire strips, etc. Active delay features are used to multiply the time it takes the adversary to breech fixed barriers. Active delay features are used to increase the difficulty of breaching fixed barriers, and, therefore, can be used to increase the overall adversary task time. This may allow for response forces to be fewer in number or further away than a traditional configuration. In addition, active delay elements force the adversary to be capable of more than just defeating the response force. They must also have the means to defeat a barrier that can require additional tools or techniques outside of what is necessary for passive delay elements. The placement of active delay elements can significantly increase the overall system effectiveness of a PPS. To be cost effective, barrier capability should increase on the path to the sabotage target, with the best passive, active, and dispensable delays directly at the target location.

Ultimately, the use of active delay elements offers the ability to significantly extend the adversary timeline. The active and passive delay elements can be designed into a system that complicates the adversary task and gives the response force a significant advantage. The traditional breaching methods that an adversary would use against passive barriers may be ineffective and force the adversary to either abandon their task or find an alternate route, which increases task time.

An additional option is to design delay and/or final denial barriers that are beyond the capability of the adversary DBT attack tool kit.

4.5. Guard & Response Force

Deployment of SMRs may reduce costs for power production. One way these costs may be reduced is by minimizing the guard and response forces present onsite or to remove all onsite response force members. It is important for SMR facility designers, operators, and security managers to determine and understand how guard and response force members will be implemented as part of the security system [19].

4.5.1. Guards

According to the IAEA, a guard is, "A person who is entrusted with responsibility for patrolling, monitoring, assessing, escorting individuals or transport, controlling access and/or providing initial response" [8]. Guards at a site typically have the functions of:

- Controlling access to a security area or into a facility
- Operating a CAS or backup alarm station

- Conducting searches of personnel and vehicles
- Performing random patrols on foot or in vehicles to detect unauthorized activities
- Responding to alarms (i.e., assessment and containment until response arrives)
- Escorting nuclear material movements

SMR facility designers and operators must ensure the site has proper guard presence to conduct the above functions. Decreasing the guard size may reduce operational costs, but it is important that facilities have the proper guard size to include for contingencies and compensatory measures. Guards may be stationed onsite in smaller numbers during normal operations of an SMR facility, and additional guards may be brought onsite during off-normal operation times at the facility. These off-normal operations may include fresh fuel shipments to the site, reactor maintenance, site inspections, or FoF exercises (as required). Additional guard force sizing considerations include:

- Implementing the two-person rule
- Providing access control functions
- Conducting searches for prohibited items
- Conducting alarm assessment
- Conducting alarm station monitoring
- Providing escorts as necessary

It is important to note that guard members generally are not accounted for as part of the effectiveness of the response force. The guard force is primarily used for access control, detection of prohibited items, initial alarm assessment and containment, and escorting nuclear material.

4.5.2. Response Forces

According to the IAEA, "Persons, on-site or off-site, who are armed and appropriately equipped and trained to counter an attempted unauthorized removal or an act of sabotage" [8]. An SMR facility may have an onsite response force to protect the site against theft of nuclear material or sabotage of nuclear material and the facility.

The success of the response to a malicious act is determined by the ability of the response force to interrupt and neutralize the adversary force. This is dependent on the response force having the proper training and capabilities to neutralize the adversary. Response force members should be:

- Familiar with the site layout
- Know the locations of targets and target sets
- Trained on contingency plans and compensatory measures
- Trained on site emergency plans
- Trained on facility access control procedures
- Trained on the site security plan
- Equipped with the necessary equipment (e.g., firearms, handcuffs, flashlights, etc.)

The response force must be familiar with the site layout to respond to malicious acts in a timely manner. Knowledge of the site and facility layout will allow the response force to be effective as part of the PPS. The response force should know the location of targets and target sets to provide effective protection for targets within the facility against a malicious act and provide a strategic response to the malicious acts. The response force knowledge of target sets also allows the security plan and posture to be implemented properly and effectively. Effective training on the contingency plans and compensatory measures by responders leads to effective deployment of these contingency plans and compensatory measures to ensure security of the SMR facility. The response force should be trained on the emergency plans to allow for security to be properly implemented during emergency events. Proper training on access control procedures enables the response force to understand the access control procedures, be familiar with implementing access control procedures, and have greater detail on the cause of alarms at the site. Response force members should be trained in and understand the site security plan for implementing the PPS, so the system ensures the protection of the facility. Providing the response force with the appropriate level of equipment necessary to neutralize the DBT is important to ensuring an effective PPS.

SMR sites and security designers must consider how the response force will be implemented as part of the PPS strategy. An onsite response force may provide a quicker response, which increases the probability that the response force can successfully interrupt a malicious act. An offsite response force may provide the flexibility to use local law enforcement agencies to provide response and potentially reduce the security system operating cost.

Response forces should also be aware of the regulations regarding use of force and ability to perform an arrest.

5. EVALUATING PHYSICAL PROTECTION SYSTEM EFFECTIVENESS

Before a PPS can be deployed, the effectiveness of the system must be determined and analyzed. Evaluating a PPS requires a methodical approach that measures the ability of the system to meet the design requirements.

5.1. System Effectiveness

To evaluate system effectiveness a vulnerability assessment (VA) process can be used. The measure of the overall PPS effectiveness is described as a probability (P_E). P_E is determined by two other probabilities, the probability of interruption (P_I) and the probability of neutralization (P_N). P_I is defined as the probability that the response force can arrive at a deployed location in a timely manner to halt adversary progress along a defined timeline of adversary tasks. Interruption does not mean the adversary task has literally been interrupted, simply that the security forces have arrived before the adversary can complete its task. Neutralization is defined as the defeat of the adversary force by combat engagements or other means that lead the adversary to not accomplishing an act of theft or sabotage. P_N is the measure of likelihood that the response force will be successful in defeating the adversary, given that interruption has already occurred.

P_I and P_N are treated as independent variables when a defined threat selects a pathway that exploits vulnerabilities within the PPS and is willing to use violence to achieve goals. With this threat the system effectiveness can be determined using the following equation:

$$P_E = P_I x P_N$$

When considering system effectiveness, it is important to remember it is a conditional probability. If the security system lacks the ability to detect and delay an adversary to achieve an interruption, then neutralization cannot occur. Conversely, if the system has a high probability of interruption but lacks the response force to neutralize the threat, the security system fails [18].

5.1.1. Probability of Interruption

Path analysis focuses on determining the P_I for a PPS. P_I estimates the likelihood that an appropriate response force can arrive and interrupt the adversary before the adversary task can be completed. In a sabotage scenario, this means the response force can arrive and interrupt the adversary before a successful sabotage attack can be completed [20].

Path analysis focuses on understanding the following concepts:

- Adversary task times for individual tasks
- The total adversary task time for completing a malicious act
- Probability of detection for individual components
- Probability of detection for the entire PPS
- Response force times to locations that allow for the response force to interrupt the adversary [21]

These components directly feed into conducting path analysis. Path analysis compares the timelines for both the adversary and the response force. Figure 5-1 shows an example of these timeline comparisons. When designing PPSs, it is important that the PPS response time be less than the adversary task time. Here, the PPS response time includes the time it takes for detection and assessment of an alarm to occur and the time it takes to deploy the response force to the proper location and interrupt the adversary. In the diagram, the adversary task time is the total time it takes the adversary to complete an act of theft or sabotage at an SMR facility.

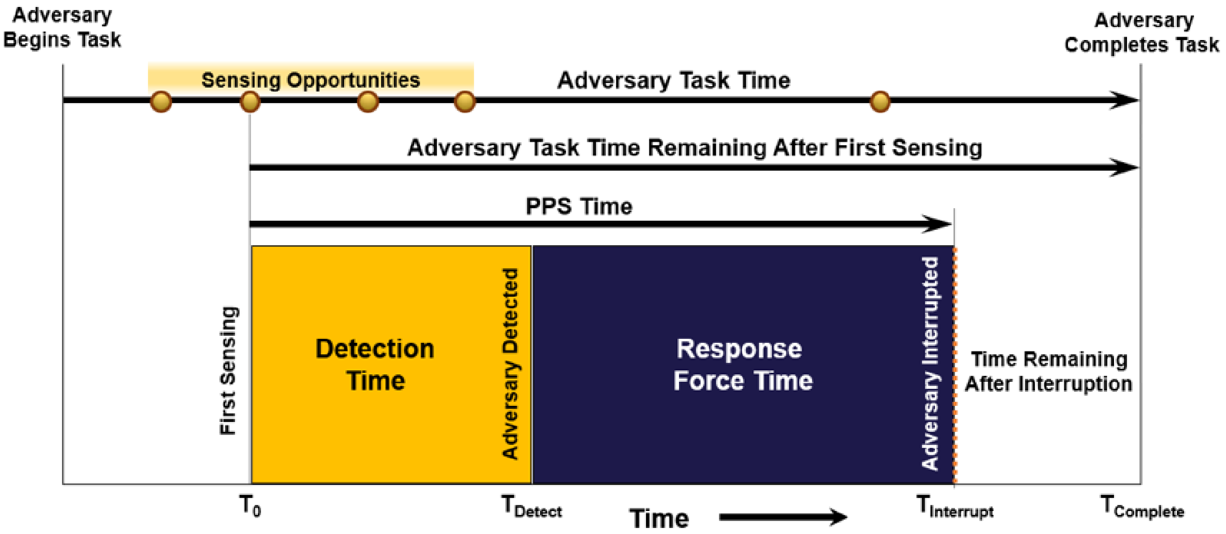

Figure 5-1. Physical Protection Timeline Comparison

Figure 5-2 shows how P_I is determined. It is important to note that in both Figure 5-1 and Figure 5-2, the green dots are sensing opportunities within the PPS. These sensing opportunities are locations along the adversary task timeline where either detection technologies or visual detection by onsite personnel could aid in the detection of malevolent adversary actions. When determining the P_I in path analysis it is important to identify the critical detection point (CDP). The CDP is the point at which the PPS response time is equivalent to the adversary task time at that point. Path analysis software allows users to identify whether a CDP exists. If a CDP exists this means the response force has enough time to respond and interrupt the adversary along their path before the adversary completes its tasks. This idea is summarized in Figure 5-2.

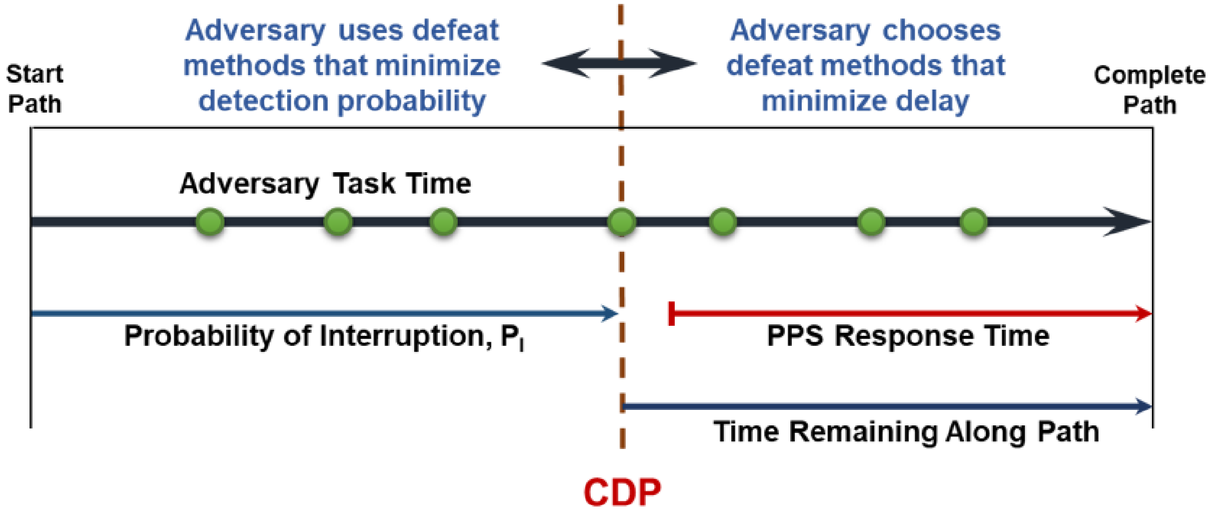
Start Path
Adversary uses defeat methods that minimize detection probability
Adversary chooses defeat methods that minimize delay
Complete Path
Adversary Task Time
Probability of Interruption, P$_I$
PPS Response Time
Time Remaining Along Path
CDP

Figure 5-2. CDP for Physical Protection Systems

The P_I can be calculated using the following equation:

$$P_I = 1 - [(1\text{-}P_{D1})*(1\text{-}P_{D2})*...(1\text{-}P_D,CDP)]$$

The P_I is the cumulative probability of detection (P_D) along a path up to and including the CDP. Here, the individual probabilities of detection are the probabilities associated to technologies or personnel onsite who have a probability of detecting an adversary along the adversary path.

SMR facility designs will impact how the P_I is achieved in a PPS design. For example, an SMR with a small facility footprint may have a decreased adversary task time and this decreased adversary task time will require the design of delay barriers that can increase the adversary task time to ensure that a high P_I can be achieved. SMRs that have a small number of targets or target sets may consider designing an effective external IDS to ensure adequate detection and assessment further from the target and use active delay barriers before a target to increase the overall adversary task time. Since the P_I is also based on the time it takes for the response force to arrive, SMR sites located closer to offsite response force, or that have an onsite response force, may be able to achieve higher P_I compared to sites in remote locations or without an onsite response force.

5.1.2. Probability of Neutralization

The P_N is the probability that once a threat is neutralized, the response force can prevent a threat from completing unauthorized removal of nuclear material or sabotage of a nuclear facility. If conducting P_N analysis, the probability can be determined by using the following equation:

$$P_N = \quad N_{wins}/N_{engagements}$$

The assumptions with this probability are:

- The number of simulations or engagements, $N_{engagements}$, is statistically significant
- All engagements start with the same initial conditions
- Only two possible outcomes exist per engagement: response force wins or response force loses

Determining the P_N requires information about adversary numbers capabilities and knowledge from a DBT, response force size and capabilities, knowledge of response force deployment routes, the facility terrain, building information, and characteristics of the PPS.

There are many methods by which the P_N can be determined. These methods include expert judgement, mathematical models, simulations, and live FoF exercises. Each of these methods has a tradeoff space between accuracy and cost. Methods that involve large amounts of personnel (e.g., expert judgment and FoF exercises) are costly but may be more accurate, while mathematical models and simulations may be less costly and less accurate.

It is also important when conducting P_N analysis to understand the factors that can and cannot be determined easily and how these factors impact determining the P_N. Easily determined factors include the time it takes for response force along pathways to interrupt the adversary, the tactics that are used by the response force, the attack scenario being conducted, and the command-and-control structure used to respond to an adversary attack. The factors that cannot be easily determined are the training levels and understanding of the adversary, response force morale, accurate intelligence about the threat, the security culture that directly impacts those operating within the PPS, and environmental factors that may inhibit the response force. When conducting this analysis, it is important to understand all these factors and how they may affect the results [21].

6. ADVANCED PHYSICAL PROTECTION TECHNOLOGIES FOR SMALL MODULAR REACTORS

Advanced physical protection technologies may be needed to provide an effective PPS with reduced staffing. These technologies may enhance detection, assessment, and delay capabilities that improve PPS effectiveness and reduce the overall cost of the PPS.

6.1. Advanced Detection and Assessment for Small Modular Reactors

Advanced detection and assessment technologies may be applied to SMR facilities to enhance the ability to detect and assess a malicious act earlier and with a higher P_D. One of these technologies might be the use of deliberate motion analytics (DMA). DMA is a mathematically fused sensor system that can provide reliable detection beyond the traditional fence line boundaries for a PPS. The ability to detect an adversary earlier can allow for increased probabilities of interruption and improve the effectiveness of the PPS.

DMA is a sensor algorithm that can fuse multiple sensor data outputs to create a multi-physics sensor. DMA uses deliberate motion to determine differences between intruder alarm sources, nuisance alarms, alarms caused by weather events, or other moving objects that may cause a sensor to alarm. This technology may have an effective use for PPSs in allowing for detection outside of the security area of an SMR facility and decreasing the operational load on alarm station operators by decreasing the number of nuisance alarms an operator may see.

This application can be used for detection outside of the security area, improving the probability of interruption by notifying the response force before an adversary can reach the site boundary. Implementing DMA, RADAR, and video analytics may also support the detection of unmanned aircraft systems [22].

6.2. Unmanned Aerial Systems for Physical Protection

There is significant potential for small unmanned aircraft systems (UAS) to play key roles in SMR site security. There is a spectrum of UAS capabilities that can be applied toward this mission space, from fully manual flights with a pilot for each UAS to an autonomous swarm of UAS that are capable of launching; flying preprogrammed or dynamic flight patterns, while simultaneously avoiding each other and other aircraft; and landing to self-recharge/refuel. Use cases can span a full spectrum of security operations:

- Security response while conducting official duties
  - Surveillance of an adversary force or trespassers
  - Surveillance of citizen protests for situational awareness
  - Surveillance of activities that require additional security measures
- Accidents / recording the scene
- Fires
- Vehicle Escorts
- Inspection of malfunctioning equipment
- Inspection of suspicious packages

- Remote assessment of perimeter alarms (e.g., autonomously deployed or manually flown)
- Autonomous perimeter sweeps

6.2.1. Tethered UAS

There are also advantages to tethered UAS (TUAS), such as:

- Significantly longer flight times, as most systems supply power to the UAS over the tether
    - Sandia National Laboratories (SNL) recently tested a power-TUAS that can run unattended all day and claims to run this way for up to 30 days
- The ability for a TUAS to follow its base station / tether reel system when mounted to a vehicle, which has the potential to:
    - Give a patrol vehicle the advantage of 360° situational awareness of the vehicle surroundings
    - Provide enhanced real-time situational awareness during nuclear material transportation activities
- The ability to rapidly deploy the TUAS in a new area of the site for inspection, situational awareness, and/or situational monitoring
- The ability to remotely deploy the TUAS as a compensatory measure if other observation/detection components of the PPS become compromised

6.2.2. Autonomous Perimeter Alarm Response and Remote Assessment

One of the most promising areas for the application of UAS autonomy to nuclear site security is in alarm response and remote assessment. If an alarm is triggered, the geospatial coordinates of that event can also be triggered to send an autonomous path plan to the closest autonomous UAS, instructing it to fly to the alarm location as it scans for intruders along the way. The vast majority of alarms that are triggered along fence lines tend to be false alarms induced by animals, weather events, or other nuisance alarm sources. This type of autonomous remote assessment has the potential to increase efficiency and cost savings for the site security force.

6.2.3. Autonomous Perimeter Sweeps

Security/response personnel can program UAS to remotely and autonomously patrol the perimeter of a property with an infrared camera, as opposed to having officers walk or drive the perimeter. Thermal imaging cameras can assist in rapidly identifying people amid a cluttered background; and artificial intelligence (AI) features that rapidly analyze imagery acquired from UAS to identify people, animals, and vehicles are commonplace (see Figure 6-1).

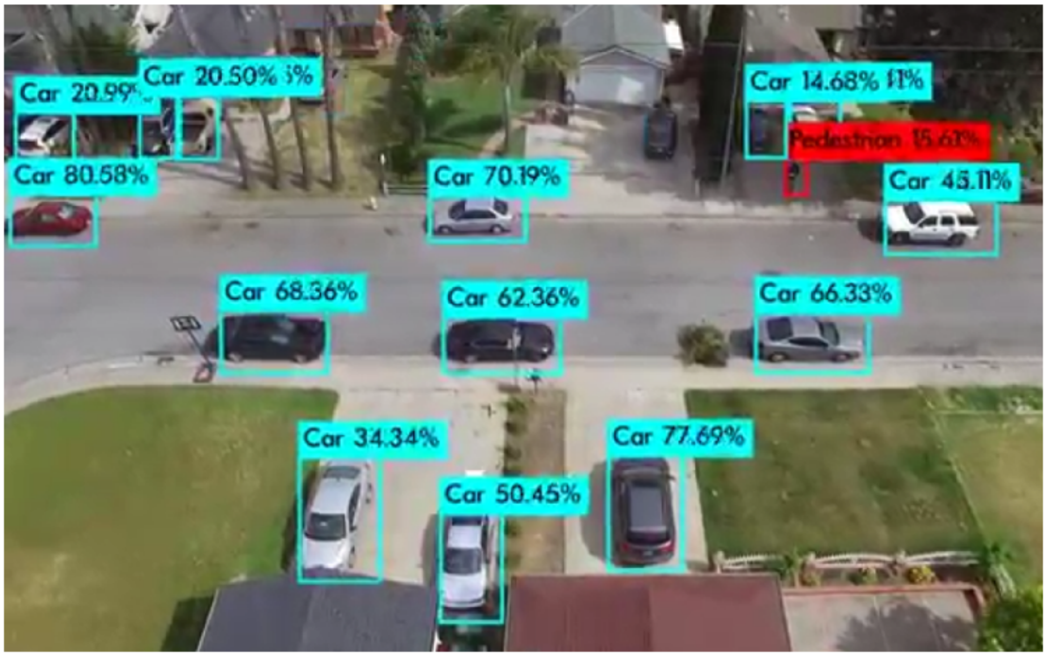

Figure 6-1. Machine learning and object recognition applied to aerial footage from small UAS

6.3. Active Delay for Small Modular Reactors

Multiple and different active delay features should be considered for SMRs. One example would be the alarm station operator activating a door closure/locking feature in the event of an adversary attack. An open door has no delay; so, closing and securing the door will provide delay consistent with the door design. And following the principle of balanced delay for all paths, the door delay should be equivalent to the delay provided by the wall containing the door. For active delay features, consideration must be given to personnel safety. For example, a security system operator may not be able to close a door if it is used as an emergency exit. However, if nuclear safety, life safety, and security personnel work together during the design phase, a solution can generally be determined that meets the requirements of all three.

Many active delay barriers can be considered such as movable barriers or dispensable barriers (e.g., foams, obscurants, slippery agents, irritants, stun technologies, etc.). Dispensables may be used with a fixed barrier to provide a delay multiplication factor. For example, when a dispensable is placed in front, within, after, and/or over a fixed barrier, the delay time for breaching the fixed barrier is multiplied due to the increased level of difficulty the dispensable presents to penetrating through the fixed barrier. Table 6-1 shows an example of how active dispensable barriers may increase overall delay times in a very simple PPS [18]. Note that if multiple dispensable barriers are used at the same time and that if each provides a different affect (e.g., obscuration, irritant, slippery agent, electrical stun, etc.), their individual delay multiplication factors are multiplied together to determine their combined use delay multiplication factor. Using this concept, combined delay multiplication factors greater than 10 have been achieved.

Table 6-1. Example of Delay Multiplication [10]

Active Delay Type	Delay Multiplication Factor	Example Delay time (s)
Baseline	1	30
Obscurant	1.66	49.8
Slippery Agent	1.55	46.5
Combined Obscurant and Slippery Agent	2.54	76.2

Before the response force arrives to interdict the adversary, active delays may be combined with detection and response capabilities that allow for immediate engagement of the adversary with less-than-lethal technologies (electrical stun, irritants, kinetic energy stun projectiles like bean bags or rubber bullets, etc.) up to lethal technologies, if allowed by the competent authority.

Dispensable barriers may pose safety risks to site personnel if the dispensable barriers become activated prematurely or inadvertently or leak. It is for this reason that an SMR site should consider dispensable barrier deployment be controlled by an operator in a CAS, where one operator can control the deployment of dispensable barriers. Dispensable barriers may need a command and control activation capability to be housed in the CAS, which increases the control and interaction for CAS operators in the overall PPS. If a cyberattack is allowed by the DBT and the cyberattack could render the CAS, AC&D, and dispensable command and control capability inoperable, manual activation of the dispensable(s) by the guard/response force should be included in the design.

When thinking about the development of a balanced PPS (Figure 4-1, PPS Stool), an onsite response force has often been considered a mandatory part of the balanced PPS stool. But due to the long-term significant cost of an onsite response force, the onsite response force may be replaced by a non-dedicated offsite response force like the local police, but only if the remaining PPS stool legs are made very robust. The detection leg of the stool needs to detect the attack as early as possible, with a high probability of assessed detection and with multiple layers of detection immediately followed by delay. Multiple and different delay barriers should be selected that provide increasing delay as the adversary approaches the targets. Since the onsite response force has typically provided the rapid lethal force capability if needed, lethal active delay capabilities should be considered for sites having only offsite police as their response.

Note that, for some features, inclusion in the manufacturer's design may be impracticable, and the delay features may need to be installed after the reactor is sited. Also note that, in some cases, the competent authority or licensee may want specific sensitive security features to be designed/installed outside of the purview of the manufacturer, especially if construction/installation is performed by foreign personnel or personnel who should not have access to security information.

6.4. Modeling & Simulation for Small Modular Reactor Facilities

Modeling and simulation (Mod/Sim) tools can be used by SMR designers and operators to design security systems and evaluate the effectiveness of security system designs. Mod/Sim tools may also be used to develop performance testing exercises for training response forces or local law enforcement agencies. This section will discuss how Mod/Sim tools have been developed to design and evaluate security system designs.

6.4.1. Path Analysis

Mod/Sim tools facilitate conducting path analysis work on facility PPSs. Path analysis software allows designers and operators to determine how effective the detection and delay components of the PPS are.

The Office of International Nuclear Security (INS) has developed path analysis software that allows users to develop PPS schematics for detection and delay to enable path analysis to be conducted for both theft and sabotage events. This software is called PathTrace©[4]. It was developed so users could determine the probability of interruption related to PPS designs. This software is user-friendly and allows analysis to be run on local machines.

6.4.2. Tabletop Exercises

Once a PPS has been designed, it is important for the designers and operators to consider conducting tabletop exercises. These tabletop exercises should be conducted with the response force, whether they are onsite or offsite. Tabletop exercises allow the response force and the security personnel to better understand how the PPS and the security plan are to be implemented. These tabletop exercises also allow the facility to understand if the system needs to be changed, upgraded, or adapted for the successful integration of the response force into the PPS.

INS has also developed a 3D tabletop exercise tool called SCRIBE3D©[5]. SCRIBE3D© allows users to conduct 3D tabletop exercises on facilities. This tool provides users with many advantages, such as:

- 3D tabletop exercises
- Contingency planning exercises
- Compensatory panning exercises
- Emergency response planning
- Line-of-sight visualizations

These capabilities are helpful for designers and security planners to determine if changes need to be made to the facility layout, security system, and plans that are being implemented for the security of the SMR. SCRIBE3D© allows users to conduct tabletop exercises and plan FoF exercises that can

[4] For PathTrace© licensing inquires, see https://insetools.sandia.gov/software-request.

[5] For SCRIBE3D© licensing inquires, see https://insetools.sandia.gov/software-request.

be used to determine the probability of neutralization. This is important for understanding the PPS effectiveness.

7. CONCLUSION

SMRs may have a vital role in energy production, desalination, and heating around the world. While these reactors are in the design phase, it is important to consider how these facilities should be secured, and what may impact the design of a PPS. Future SMR operators should be versed in the DEPO methodology before acquiring and deploying a reactor. This ensures the PPS design meets regulatory requirements and the necessary targets can be secured with it. Target identification can be conducted through traditional means like a VAI or novel approaches such as STPA. These novel approaches may reduce the time needed to identify vital areas and targets. A VAI or STPA process should be considered in the design phase of any SMR. This ensures all targets can be identified and the PPS can be designed to protect these potential targets. When designing the PPS, it will also be important to consider the operational environment and needs of the SMR facility to ensure the PPS does not inhibit operations.

Future SMR operators and regulators must consider if the threat environment will change or be different than the DBT that exists for the current nuclear facilities in country. Identifying the DBT that the PPS must defend against before the system is designed ensures the most cost-effective PPS can be built to defend against the DBT. When designing PPSs for SMRs, advanced technologies such as extended detection through DMA or the use of UAS may allow for detection to occur earlier and reduce the infrastructure and system cost for an external intrusion detection system. SMRs may require advanced delay technologies such as active delay systems that can be used to multiply adversary task times and increase the total adversary task time, leading to a higher probability of interruption and higher system effectiveness. It is also important to consider the protection strategy that is to be used for an SMR. The protection strategy will impact the technologies and systems chosen to defend the site against the DBT. It will also impact the overall PPS and should be considered in the design process of the SMR.

Evaluating the PPS may be conducted before the facility is built with the use of modeling and simulation tools. These tools can allow a facility footprint and layout to be used to design a PPS and assess its effectiveness. The use of path analysis software can assess whether the intrusion detection, delay capabilities, and response force posture produce an effective probability of interruption. Using this software can also enable informed design decisions to be made before the facility is built and ensure system effectiveness. Tabletop tools allow tabletop exercises to be conducted and recorded to ensure the response force procedures and tactics enable the response force to neutralize the DBT. The combination of these tools can be used to assess the capabilities of the PPS design. Once the PPS design is implemented and installed, it is important to performance test it to ensure the it operates at the as-designed performance level.

8. REFERENCES

[1] *Advanced in Small Modular Reactor Technology Developments.* International Atomic Energy Agency. Austria. September 2020

[2] World Nuclear News, *Hermes Low-Power Demonstration Reactor.* 2021. Artistic Rendering. Kairos Power, World Nuclear News, https://www.world-nuclear-news.org/Articles/Kairos-Power-plans-Hermes-demonstration-reactor-at

[3] BusinessWire. *NuScale Power's Small Modular Reactor Plant.* Artistic Rendering. 2020. BusinessWire, NuScale, https://www.businesswire.com/news/home/20200828005299/en/NuScale-Power-Makes-History-as-the-First-Ever-Small-Modular-Reactor-to-Receive-U.S.-Nuclear-Regulatory-Commission-Design-Approval

[4] Wikimedia Commons. *Rendering of Oklo Distributed Nuclear Micro-Reactor Site.* 2020. Artistic Rendering. PV Magazine, https://pv-magazine-usa.com/2020/09/28/can-20-people-with-25-million-get-oklos-fast-fission-micro-reactor-to-market/

[5] "Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Revision 5)." NSS No. 27-G. International Atomic Energy Agency. Vienna, Austria. 2018.

[6] "Risk Management: A Tool for Improving Nuclear Power Plant Performance." IAEA-TECDOC-1209. International Atomic Energy Agency. Vienna, Austria. 2021

[7] Amendment to the Convention on the Physical Protection of Nuclear Material." IAEA. October 15, 2017. Accessed October 12, 2021. https://www.iaea.org/publications/7598/amendment-to-the-convention-on-the-physical-protection-of-nuclear-material.

[8] "Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities." INFCIRC/225/Revision 5 (NSS-13). International Atomic Energy Agency. 2011

[9] *Design and Evaluation of Physical Protection Systems, 2nd edition.* Sandia National Laboratories. Garcia, M.L. 2008.

[10] *U.S. Domestic Small Modular Reactor Security by Design (SAND2021-0768).* Sandia National Laboratories. Evans, Alan S., Parks, Jordan M., Horowitz, Steven., Gilbert, Luke., Whalen, Ryan. 2021.

[11] *How STPA can be used for target set and vital area identification (SAND2021-5772PE).* Sandia National Laboratories. Sandt, Emily. 2021.

[12] N. Leveson and J. Thomas, *STPA Handbook*, (2018).

[13] A. D. Williams, D. M. Osborn, K. A. Jones, E. A. Kalinina, B. Cohn, A. H. Mohagheghi, M. DeMenno, M. Thomas, M. J. Parks, E. Parks and B. Jeantete, *System Theoretic Frameworks for Mitigating Risk Complexity in the Nuclear Fuel Cycle (SAND2017-10243)*, Sandia National Laboratories, Albuquerque, USA (2017).

[14] A. D. Williams, "System Security: Rethinking Security for Facilities with Nuclear Materials," *Transactions of the American Nuclear Society,* **vol. 109, no. 1**, pp. 1946-1947, (2013).

[15] W. Young, *A System-Theoretic Security Analysis Methodology for Assuring Complex Operations Against Cyber Disruptions*, Massachusetts Institute of Technology, Dissertation, Cambridge, MA, USA (2015).

[16] A. D. Williams, "System Security: Rethinking Security for Facilities with Nuclear Materials," *Transactions of the American Nuclear Society,* **vol. 109, no. 1**, pp. 1946-1947, (2013).

[17] Sandia National Laboratories. Sandt, Emily, Cohn, Brian, Osborn, Douglas, Williams, Adam, Clark, Andrew, Mousseau, Vincent, & Wagner, K.C. *Identifying Target Sets for Advanced Reactor Designs using Systems Theoretic Process Analysis Methodology (SAND2020-13878).* 2020.

[18] Evans, Alan Scott, and Parks, Mancel Jordan. *U.S. Domestic Small Modular Reactor Security by Design..* United States: N. p., 2020. (SAND2020-9982R)

[19] Evans, Alan, and Williams, Adam. *Advanced Nuclear Security System Design and Analysis: Guard and Response Force Sizing.* (SAND2021-2395 TR)

[20] Evans, Alan, and Williams, Adam. *Advanced Nuclear Security System Design and Analysis: Vulnerability Assessment & System Effectiveness Calculations.* (SAND2021-0682 TR)

[21] Evans, Alan, and Williams, Adam. *Advanced Nuclear Security System Design and Analysis: Path Analysis & Force-on-Force Analysis.* (SAND2021-0591 TR)

[22] Russell, John. *Performance of DMA Fused Radar and Video.* (SAND2021-3973 PE)

DISTRIBUTION

Email—Internal

Name	Org.	Sandia Email Address
Technical Library	01911	sanddocs@sandia.gov

This page left blank.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.