U.S. Domestic Microreactor Security-by-Design

Prepared for
US Department of Energy

Alan Evans, Adrienne Neef, Ben Stromberg, Collin Evans

Sandia National Laboratories

October 2021
SAND2021-13779 R

DISCLAIMER

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

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

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and 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-N5 A0003525.

Sandia National Laboratories

ABSTRACT

U.S. nuclear power facilities face increasing challenges in meeting dynamic security requirements caused by evolving and expanding threats while keeping costs reasonable to make nuclear energy competitive. The past approach has often included implementing security features after a facility has been designed and without attention to optimization, which can lead to cost overruns. Incorporating security in the design process can provide robust, cost-effective, and sufficient physical protection systems (PPSs). The purpose of this work is both to develop a framework for the integration of security into the design phase of a microreactor and to increase the use of modeling and simulation tools to optimize the design of PPSs. Specifically, this effort focuses on integrating security into the design phase of a model microreactor that meets current Nuclear Regulatory Commission (NRC) physical protection requirements and providing advanced solutions to improve physical protection and decrease costs. A suite of tools, including Scribe3D©, PathTrace©, and Blender were used to model a hypothetical, generic domestic microreactor facility. Physical protection elements such as sensors, cameras, barriers, and guard forces were added to the model based on best practices for PPSs. Multiple outsider sabotage scenarios were examined with four-to-eight adversaries to determine security metrics. The results of this work will influence PPS designs and facility designs for U.S. domestic microreactors. This work will also demonstrate how a series of experimental and modeling capabilities across the Department of Energy (DOE) complex can impact the design and implementation of Safeguards and Security by Design (SSBD) for microreactors. The conclusions and recommendations in this document may be applicable to all microreactor designs.

ACKNOWLEDGEMENTS

The team would like to acknowledge the many subject matter experts who contributed their expertise to the development of this facility, design, and analysis.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

This page left blank

EXECUTIVE SUMMARY

This report analyzes the design of a hypothetical microreactor and includes concepts of security-by-design. The design and analysis are focused on developing a microreactor facility and physical protection system (PPS) that supports an offsite response force and an effective PPS.

The initial design of this facility focused on creating the smallest footprint for the site, with the smallest and most effective PPS. This study focuses on identifying an appropriate physical security methodology for microreactor facilities, provides insights for developing a microreactor site with an effective PPS, and suggests a cost-effective design for microreactor facilities and their PPSs.

The hypothetical microreactor design is based on a heat-pipe cooled reactor, see Figure E-1-1. This design uses a fuel enrichment of 19% on a 36-month fuel-cycle. The reactor core is a solid core block that includes a matrix of fuel, heat pipes, and moderator. The core is designed to be subcritical on startup, and reflectors surrounding the core are turned inward to bring the core to its operating state. The reactor utilizes sodium-heat pipes that operate in a capillary action to transfer heat to the heat exchanger. This design allows heat to be transferred from the reactor to the heat exchanger without requiring the use of pumps. The site uses an open-air Brayton cycle to produce electrical power. An onsite control room and a remote monitoring and control system is assumed so no onsite control of the reactor is needed. Figure E-1-1 shows the hypothetical microreactor facility design and layout.

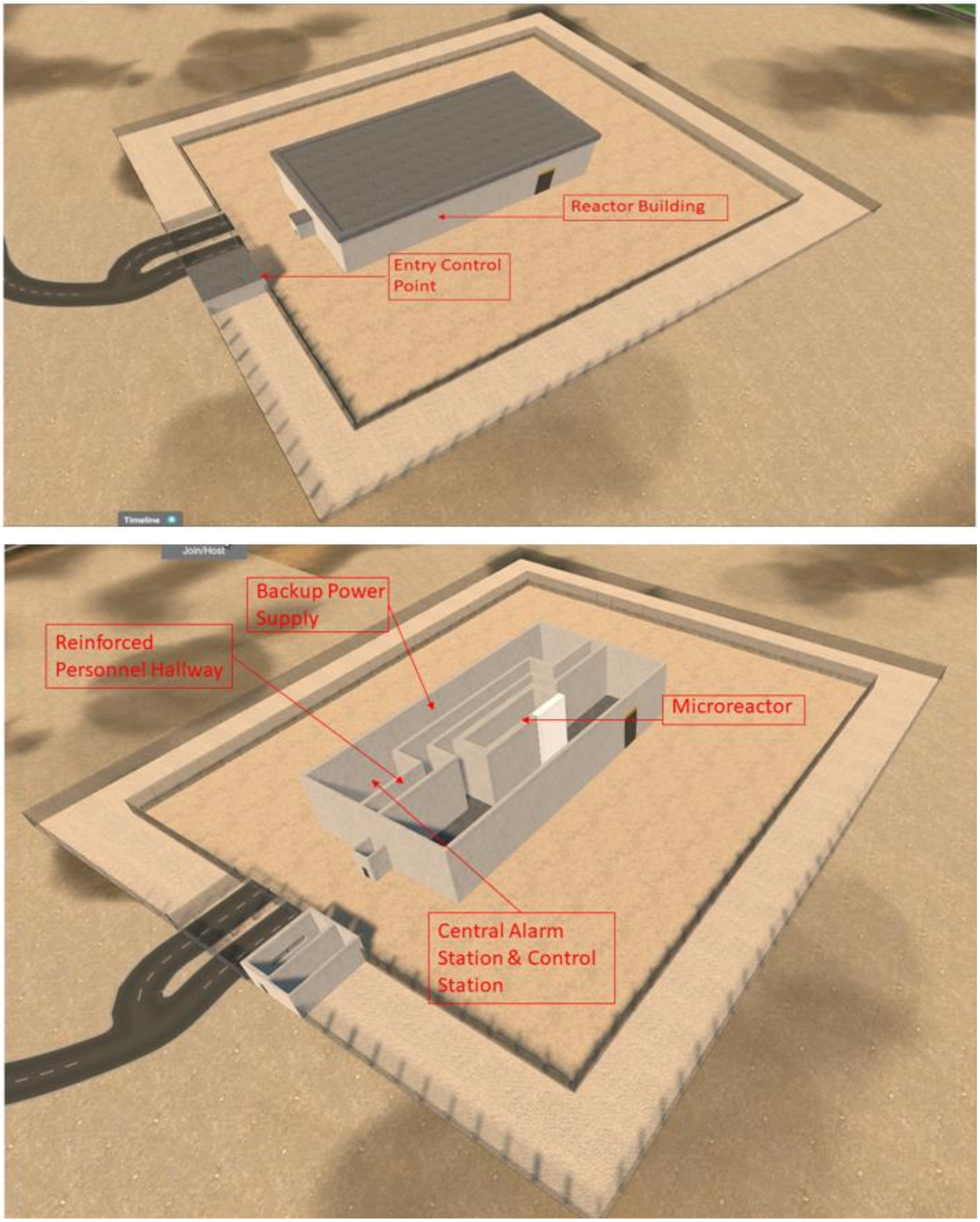


Figure E-1-1. Hypothetical Facility Layout

For this facility, a PPS was designed to provide up to thirty minutes of delay time for an offsite response force to protect against sabotage of the microreactor. To effectively achieve sabotage at the microreactor facility, the adversary must cause damage to the microreactor core (fuel elements for this facility) or cause a radiological release at the site boundary.

Many design choices were made to increase adversary task time, improve the probability of detecting the adversary force, and improve overall PPS effectiveness. These upgrades included hardening doors with steel sheeting, using active delay features such as slippery agents and obscurants in strategic locations to multiply adversary task time, and using extended detection technologies to detect adversaries before they reach the protected area boundary of the facility. Path analysis tools and force-on-force modeling simulations were used to determine the probability of interruption and the probability of neutralization (traditional methodologies for vulnerability assessments) to ascertain the overall PPS effectiveness. The design features mentioned previously were determined by a series of path analysis calculations to improve probabilities of interruption above 95% and to try to reach a system effectiveness level of 90%. The results from this analysis can be seen in Figure E-1-2**Error! Reference source not found.**. The base case PPS design was created using current Nuclear Regulatory Commission (NRC) regulations, with some exceptions made for the consideration of reduced on-site response force numbers by the small modular reactor (SMR) and microreactor community.

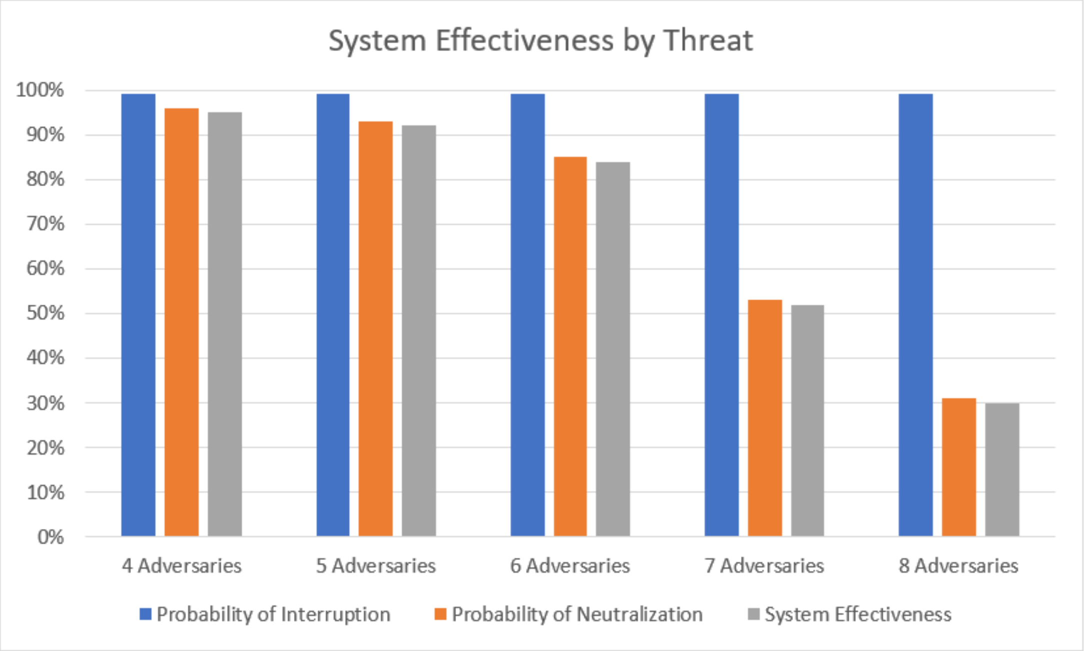


Figure E-1-2. System Effectiveness of the PPS

As can be seen by Figure E-1-2, there are two cases in which the system effectiveness is greater than 90%: specifically, the scenarios in which an offsite response force of eight trained responders attempts to recapture and neutralize an adversary force of four and five individuals. The analysis shows the system effectiveness levels for this facility typically follow the probability of neutralization. As the adversary force increases, the system effectiveness level decreases. This analysis identifies that response force tactics and planning, factors that influence the probability of neutralization, also impact PPS effectiveness.

This analysis identifies critical areas for consideration by microreactor facilities. These recommendations include:

- Ensuring the response force has adequate knowledge of the facility and target locations to implement a proper response to a malicious act
- Ensuring the response force is adequately trained to neutralize an adversary force

- Conducting exercises with the response force regularly to validate response force performance
- Considering placing microreactor facilities as close to the offsite response force as possible to decrease response force time, as this may lead to a smaller and more cost-effective PPS
- Developing secondary response force routes to reach the facility and considering methods to ensure the confidentiality of response force routes to the facility
- Leveraging facility construction materials to increase adversary delay time (i.e., reinforced doors and walls)
- Applying active delay features to multiply the task time for an adversary to defeat a fixed barrier such as a door or wall, to increase the overall adversary task time
- Implementing extended detection technologies such as deliberate motion algorithms (DMA), which may be able to detect an adversary earlier, and may be used without a traditional perimeter intrusion detection and assessment system (PIDAS), which can reduce overall PPS costs

Details for these recommendations and deployment options can be found throughout this report.

ACRONYMS AND DEFINITIONS

Abbreviation	Definition
ASD	adversary sequence diagram
BMS	balanced magnetic switches
CAS	central alarm station
CCTV	closed-circuit television
CFR	Code of Federal Regulations
DEPO	Design Evaluation Process Outline
DBT	design basis threat
DMA	deliberate motion algorithm
DOE	Department of Energy
EA	exclusion area
ECP	entry control point
KIA	killed in action
LAA	limited access area
LLEA	offsite local law enforcement agency
LWR	Light water reactor
MVP	most vulnerable path
NEIMA	Nuclear Energy Innovation and Modernization Act
NPP	nuclear power plant
NRC	Nuclear Regulatory Commission
PA	protected area
P_E	probability of effectiveness
P_I	probability of interruption
PIDAS	perimeter intrusion detection and assessment system
PIN	personal identification number
PIR	passive infrared
P_N	probability of neutralization
PPS	physical protection systems
RFT	response force time
SME	subject matter expert
SMR	small modular reactor
SNL	Sandia National Laboratories
SNM	special nuclear material
SSBD	safeguards and security by design

Abbreviation	Definition
VA	vulnerability assessment
VAs	vital areas

1. INTRODUCTION

Domestic nuclear facilities face stringent requirements for security, particularly for nuclear power generating facilities, including advanced small modular reactors (SMRs) and microreactors. This analysis focuses on the United States domestic regulatory structure from the Nuclear Regulatory Commission (NRC) perspective. Nuclear power plant (NPP) facilities must meet these stringent regulatory requirements for physical protection due to the threat posed by theft and sabotage of nuclear material. This places nuclear power at a significant disadvantage compared to other energy sources because it requires more upfront, operational, and maintenance costs in physical protection systems (PPSs) and protective force personnel.

SMRs and microreactors may be able to take credit for enhanced safety and smaller source terms to reduce onsite security presence. By only using offsite local law enforcement, operational costs may be significantly reduced. Furthermore, future nuclear facilities will need to incorporate Safeguards and Security by Design (SSBD) to optimize the performance of the PPS within reasonable cost constraints while meeting stakeholder objectives. Historically, the design of nuclear facilities has been retrofitted to accomplish the performance objectives of safeguards and security.[1] Incorporating these factors into the design phase of the facility can significantly decrease implementation and operational costs throughout the facility's lifetime. As part of this design process, it is important to assess the vulnerabilities of the facility through modeling and simulation to identify potential technological and engineering solutions to address those vulnerabilities before the facility is built.

In this report, the design process is demonstrated by identifying a hypothetical design basis threat (DBT) along with employing path and scenario analysis to identify weaknesses in a hypothetical facility's PPS.

To avoid potential sensitivities, various individual characteristics of open source planned microreactor facilities were selected and/or slightly modified for the hypothetical model.[2]

The report documents the reactor, design of the facility, operations, and PPS. The goal of the analysis is to establish an effective physical security system, including an offsite local law enforcement agency (LLEA) as the facility's response force. This report will describe the process to develop a physical security system using a security-by-design process.

This report highlights a traditional approach to designing a PPS for a microreactor facility. It also explores new technologies that may be applied with existing technologies to improve PPSs. Future efforts in this area will analyze new technologies such as final denial systems and deliberate motion algorithms (DMA) that can be used to decrease the footprint and reduce the costs of the PPS. This report will provide a baseline analysis to which the advanced technologies and systems can be compared. This will allow microreactor vendors to compare the impact of new technologies and systems and use a security-by-design informed approach to develop the most cost-effective PPS for their facility.

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

[2] "Advances in Small Modular Reactor Technology Developments. A Supplement to: IAEA Advanced Reactors Information System (ARIS)." International Atomic Energy Agency. 2020

This page left blank

2. REGULATORY CONSIDERATIONS FOR DOMESTIC SMR AND MICROREACTOR DEPLOYMENT

The U.S. Code of Federal Regulations (CFR) Title 10, "Energy" includes Chapter I Parts 1-199 applicable to the NRC. The NRC also publishes regulatory guides to aid in the implementation of these regulations. The following parts of 10 CFR are most applicable to the security and safeguards of special nuclear material (SNM):[3]

- Part 11 – Criteria and Procedures for Determining Eligibility for Access to or Control Over Special Nuclear Material
  - Establishes requirements for access to SNM[4]
- Part 25 – Access Authorization for Licensee Personnel
  - Outlines procedures for access authorization to classified information[5]
- Part 26 – Fitness for Duty
  - Describes requirements for fitness-for-duty programs of nuclear power reactor licensees[6]
- Part 73 – Physical Protection of Plants and Materials
  - Describes requirements for PPSs of plants and SNM in transit and at fixed sites[7]
- Part 74 – Material Control and Accounting of Special Nuclear Material
  - Describes requirements for control and accounting of SNM at fixed sites and in transit[8]
- Part 95 – Facility Security Clearance and Safeguards of National Security Information and Restricted Data

The NRC has many ongoing activities in the near-term, mid-term, and long-term to prepare for review and licensing of the next generation reactors. The NRC has been directed by Congress under the Nuclear Energy Innovation and Modernization Act (NEIMA) to establish a technology-inclusive regulatory framework for advanced reactor use by 2027.[9] There are two major activities that relate to physical security rulemaking: Alternative Physical Security Requirements for Advanced Reactors, NRC-2017-0227 and the Part 53 Framework, both of which will be discussed in further detail in the following sections

[3] Nuclear Regulatory Commission, "Regulations, Guidance, and Communications," accessed October 9, 2020, https://www.nrc.gov/security/domestic/reg-guide.html.

[4] Nuclear Regulatory Commission, "Part 11 – Criteria and Procedures for Determining Eligibility for Access to or Control Over Special Nuclear Material," page last reviewed/updated September 15, 2020, accessed October 9, 2020, https://www.nrc.gov/reading-rm/doc-collections/cfr/part011/full-text.html.

[5] Nuclear Regulatory Commission, "Part 25 – Access Authorization," page last reviewed/updated September 15, 2020, accessed October 9, 2020, https://www.nrc.gov/reading-rm/doc-collections/cfr/part025/full-text.html.

[6] Nuclear Regulatory Commission, "Part 26 – Fitness for Duty Programs," page last reviewed/updated September 15, 2020, accessed October 9, 2020, https://www.nrc.gov/reading-rm/doc-collections/cfr/part026/full-text.html.

[7] Nuclear Regulatory Commission, "Part 73 – Physical Protection of Plants and Materials," page last reviewed/updated September 15, 2020, accessed October 9, 2020, https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/full-text.html.

[8] Nuclear Regulatory Commission, "Part 74 – Material Control and Accounting of Special Nuclear Material," page last reviewed/updated September 15, 2020, accessed October 9, 2020

[9] "Advanced Reactor Details", Nuclear Regulatory Commission, Accessed July 19, 2021, https://www.nrc.gov/reactors/new-reactors/advanced/details.html.

2.1. NRC-2017-0227 – Alternative Physical Security Requirements for Advanced Reactors

The 2018 document SECY-18-0076 "Options and Recommendation for Physical Security for Advanced Reactors" evaluated alternatives for physical security for advanced reactors.[10] As an outcome of SECY-18-0076, the NRC proposed a rulemaking effort to establish new alternative physical security regulations for SMRs and advanced reactors to protect against radiological sabotage.[11] This evolved into NRC-2017-0227 limited-scope rulemaking, which proposes amending physical security requirements for SMRs and other advanced reactor designs commensurate with the risk to the public health and safety. If the licensee can meet certain performance-based eligibility criteria, then the licensee would be eligible for certain voluntary alternative requirements.[12] Specific sections assessed for alternatives include 10 CFR 73.55 "Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors against Radiological Sabotage," which defines requirements to protect against the DBT of radiological sabotage. The NRC is requesting comment on a proposed rule change to current regulations to give more flexibility to SMRs and other advanced nuclear technologies by developing dedicated physical security requirements to reduce the burden on licensees to request exemptions.[13] This proposed rule aims to keep the requirements of 73.55 to protect against radiological sabotage of the DBT but set out additional guidance for advanced reactors that can establish a performance-based approach for meeting these requirements.

The NRC is proposing to amend the 73.55 security requirements based on three performance metrics. If any individual criterion is met, the revised requirements would be applicable and the licensee would be able to follow the performance-based alternative approach:[14,15]

1. "The radiological consequences from a hypothetical, unmitigated event involving the loss of engineered systems for decay heat removal and possible breaches in physical structures surrounding the reactor, spent fuel, and other inventories of radioactive materials result in offsite doses below the reference values defined in §§ 50.34(a)(1)(ii)(D) and 52.79(a)(1)(vi) of this chapter."
2. "The plant features necessary to mitigate an event and maintain offsite doses below the reference values in §§ 50.34(a)(1)(ii)(D) and 52.79(a)(1)(vi) of this chapter cannot reasonably be compromised by an adversary as defined by the design basis threat for radiological sabotage."

[10] SECY-18-0076, "Options and Recommendation for Physical Security for Advanced Reactors," dated August 1, 2018, (ADAMS Accession No. ML18170A051).

[11] SECY-18-0076, Nuclear Regulatory Commission, Margaret M. Doane, Options and Recommendation for Physical Security for Advanced Reactors," August 1, 2018, https://www.nrc.gov/docs/ML1805/ML18052B032.pdf.

[12] Planned Rulemaking Activities – Rule, "Alternative Physical Security Requirements for Advanced Reactors," NRC-2017-0227, https://www.nrc.gov/reading-rm/doc-collections/rulemaking-ruleforum/active/ruledetails.html?id=76.

[13] "Physical Security for Advanced Reactors," A Proposed Rule by the Nuclear Regulatory Commission on 07/16/2019, accessed October 13, 2020, Document Citation: 84 FR 33861, Page: 33861-33864, Agency/Docket Number: Docket No. NRC-2017-0227, RIN: 3150-AK19, Document Number: 2019-15008, https://www.federalregister.gov/documents/2019/07/16/2019-15008/physical-security-for-advanced-reactors.

[14] Please see NRC Markup of NEI-20-05 Draft B Comments on "Methodological Approach and Considerations for a Technical Analysis to Demonstrate Compliance with the Performance Criteria of 10 CFR 73.55(a)(7)", NRC-2017-0227-0027, March 8, 2021. Note that these criteria, as with the entirety of the rulemaking activities, are draft and therefore subject to change.

[15] World Institute for Nuclear Security and Nuclear Threat Initiative, "Security of Advanced Reactors," August 2020, ISBN: 978-3-903191-75-4

3. “Plant features include inherent reactor characteristics combined with engineered safety and security features that allow for facility recovery and mitigation strategy implementation if a target set is compromised, destroyed, or rendered nonfunctional, such that offsite radiological consequences are maintained below the reference values defined in §§ 50.34(a)(1)(ii)(D) and 52.79(a)(1)(vi) of this chapter.”

NOTE: These criteria, as with content involved within the entirety of the rulemaking activities, are draft and therefore subject to change.

If any of these eligibility criteria are satisfied, the licensee is eligible for the application of several voluntary performance-based alternatives specified in 73.55(s), which describes prescriptive requirements within 73.55 (b), (e), (i), and (k). Specifically, the proposed change calls out (but is not limited to):[16]

- Licensee may rely on local law enforcement to perform the interdiction and neutralization requirements
  - This relieves a licensee of 73.55(k)(5)(ii), minimum number of armed responders
  - This relieves a licensee of other requirements in 73.55(k)(3-7) and (k)(8)(ii)
- Relieved of 73.55(e)(9)(v) and 73.55(i)(4)(iii) requiring the secondary alarm station, including if offsite, be designated and protected as a vital area
  - Sites must still have two onsite alarm stations per 73.55(i)(2), but a designated secondary alarm station may be offsite; it is not r[17]equired to be a vital area, nor is its associated secondary power supply required to be

[For full descriptions of the proposed alternatives, follow the rulemaking activities at Regulations.gov under docket ID: NRC-2017-0227]

The licensee must perform and submit a site-specific analysis of how their design satisfies the security requirements and performance criteria.

2.2. Part 53 – Risk Informed, Technology-Inclusive Regulatory Framework for Advanced Reactors

This rule is intended to be used by advanced reactor applicants by December 31, 2027. It is in addition to, but also in coordination with, the limited-scope rulemaking NRC-2017-0227. Rulemaking documents and preliminary proposed rule language can be found on Regulations.gov under document ID NRC-2019-0062. As part of this, proposed language is in development for a technology-inclusive performance-based program that supports a risk-informed graded approach to physical security, cyber security, and information security, as well as fitness-for-duty programs and access authorization. The proposed 53.830 Security Program in Subpart F requires the implementation of a physical protection program that, 1) protects SNM according to Parts 73 and 37, and 2) protects against radiological sabotage per requirements within 73.55 or the proposed 73.100 unless the following is satisfied:

[16] Revised Preliminary Proposed Rule Language, Posted by the Nuclear Regulatory Commission on Sep 13, 2020, NRC-2017-0227-0023.

[17] Nuclear Regulatory Commission June 10, 2021, Public Meeting Presentation, “Part 53 Risk-Informed, Technology-Inclusive Regulatory Framework for Advanced Reactors Rulemaking – Subpart F and 10 CFR Part 73 Emergency Preparedness and Security.”

> *"The radiological consequences from a hypothetical, unmitigated event involving the loss of engineered systems for decay heat removal and possible breaches in physical structures surrounding the reactor, spent fuel, and other inventories of radioactive materials result in offsite doses below the values in §§ 53.210(b)(1) and (2)."*[18]

This proposed language relieves the applicant from protecting against the DBT of radiological sabotage if the licensee can perform an analysis demonstrating compliance with the criteria. If the criteria are not met, the licensee would have to protect against the DBT with a physical protection program and demonstrate that it meets current performance and prescriptive requirements in either 73.55 or the newly proposed 73.100. The proposed section of 73.100 outlines a novel framework to meet general objectives and performance requirements and provides optimal flexibility to protect the plant against the DBT.

[18] "Section 53.210(b)(1): 25 rem (250 mSv) total effective dose equivalent (TEDE) at any point on the boundary of the exclusion area for any 2-hour period following. Section 53.210(b)(2): 25 rem TEDE at outer boundary of the low population zone." Quoted directly from June 10, 2021 NRC Public Meeting Presentation, "Part 53 Risk-Informed, Technology-Inclusive Regulatory Framework for Advanced Reactors Rulemaking – Subpart F and 10 CFR Part 73 Emergency Preparedness and Security."

3. HYPOTHETICAL MICROREACTOR SITE

The hypothetical microreactor developed for this design and analysis encompasses features and capabilities of multiple U.S. domestic microreactors currently in development. This provides a framework for the design and analysis to capture SSBD for domestic microreactor applications. The hypothetical microreactor facility in this study is located 15 miles outside of Fairbanks, Alaska, in an area with a population of approximately 31,551 people.

3.1. Site Description

3.1.1. Climate

The region surrounding the facility has a cooler and wet climate. Its summers are comfortable and cloudy, and its winters are frigid, snowy, and partly cloudy. The warm season starts in May and lasts until early September, with an average daily high temperature above 73°F [17].[19] The cold season is between September and March and has an average daily high temperature below 16°F. As temperatures rarely exceed 70°F, the temperature should not affect any infrared technologies. The region generally has a low level of humidity but receives an average of 12 inches of rain and 61 inches of snow per year.[20] This level of precipitation may induce noise in sensors and cause the degradation of security elements (e.g., mold/rust/mineral deposits/electrical shorts).

3.2. Microreactor Site Description

3.2.1. Buildings and Microreactor Operations

The site operates two buildings. The primary building is the reactor building that houses the reactor, the central alarm station (CAS), and emergency backup power. The second building is the entry control point (ECP) building. Figure 3-1 shows this hypothetical site layout. The secondary system building houses backup battery power and diesel generators that provide secondary power systems needed to operate the security and safety systems at the site.

[19] "Average Weather in Fairbanks, Alaska, United States, Year Round - Weather Spark." n.d. Weatherspark.com. https://weatherspark.com/y/273/Average-Weather-in-Fairbanks-Alaska-United-States-Year-Round.

[20] "Fairbanks, Alaska Climate." 2016. Bestplaces.net. 2016. https://www.bestplaces.net/climate/city/alaska/fairbanks.

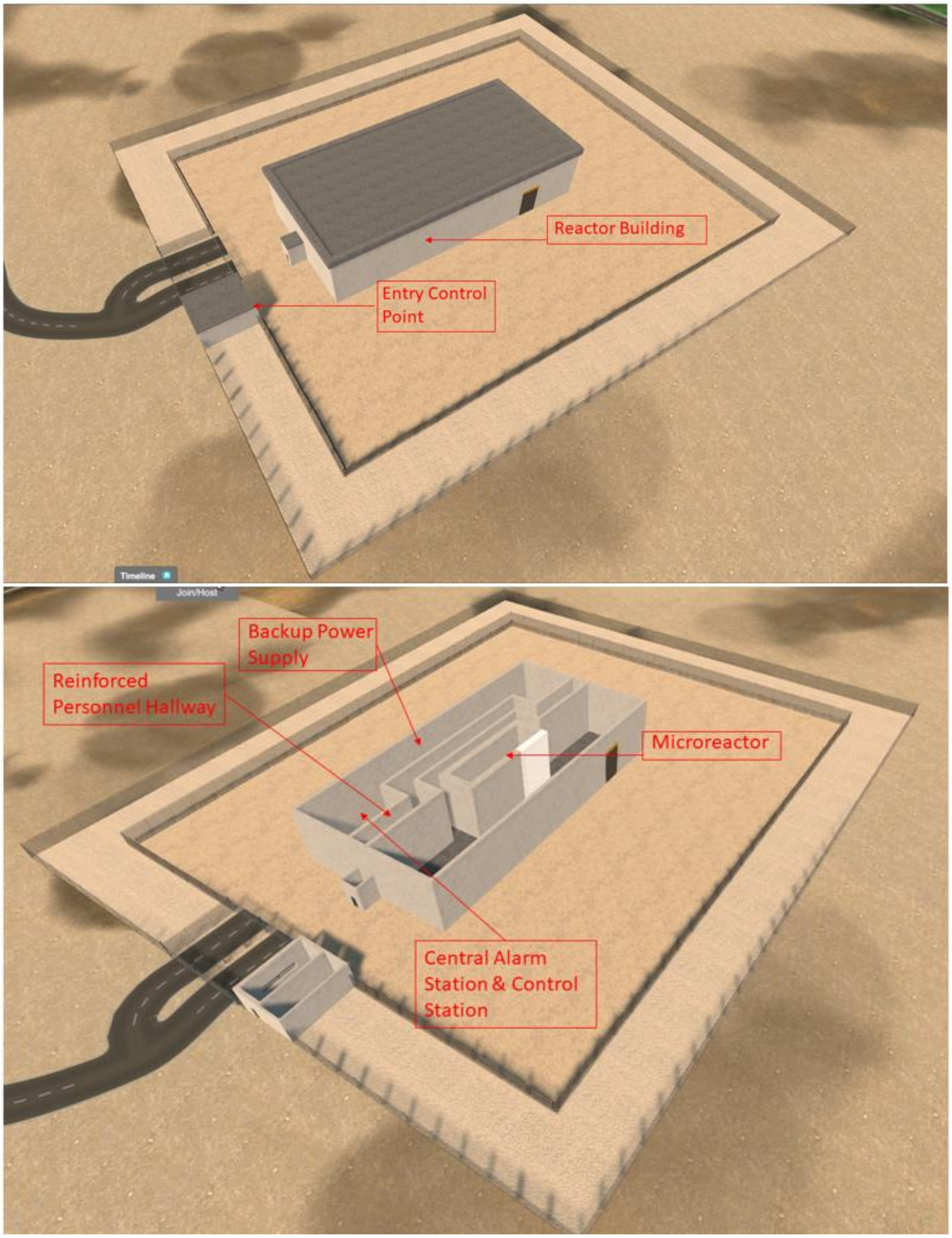


Figure 3-1. Microreactor Facility

This hypothetical microreactor design is based on a heat-pipe cooled reactor. This design uses a fuel enrichment of 19% on a 36-month fuel cycle. The reactor core is a solid core block that includes a matrix of fuel, heat pipes, and moderator. The core is designed to be subcritical on startup, and reflectors surrounding the core are turned inward to bring the core to its operating state. The reactor utilizes sodium-heat pipes that operate in a capillary action to transfer heat to the heat exchanger. This design allows heat to be transferred from the reactor to the heat exchanger without requiring the use of pumps. The site uses an open-air Brayton cycle to produce electrical power. This reactor design utilizes an onsite control room and a remote monitoring and control system so no onsite control of the reactor is needed.

During abnormal or emergency conditions the reactor can be shut down from the onsite control room or the remote monitoring and control system. When the reactor is shutdown, decay heat removal is conducted passively where the outer walls of the reactor can dissipate heat to the surrounding air. Inherently, the heat pipes will also allow for a large amount of decay heat removal, and the passive system of transferring heat to the air is effective at cooling the reactor in an abnormal event or emergency.

This hypothetical facility has been designed in such a way that the whole core will be replaced after 36 months of operations and the as few personnel as possible need to be onsite for maintenance, repair or operations, and security.

This page left blank

4. OVERVIEW OF VULNERABILITY ASSESSMENT

The evaluation of an existing or proposed PPS requires a methodical approach that measures the ability of the security system to meet defined protection objectives. Without this kind of careful assessment, valuable resources might be wasted on unnecessary protection or, worse yet, fail to provide adequate protection of material against a theft or sabotage attack by the defined threat. The vulnerability assessment (VA) methodology was developed to implement performance-based physical security concepts at nuclear sites and facilities.

4.1. Modeling Tools

4.1.1. PathTrace©

PathTrace© is a path analysis tool that is used to analyze all facility paths adversaries may take to achieve their goal. This tool was used in this analysis to determine the probability of interruption (P_I) using a hypothetical PPS.

To determine the potential adversary paths, the software identifies multiple pathways adversaries may take. Specifically, the tool develops three paths:

- The quickest adversary path, where decreasing the task time is prioritized over decreasing the probability of detection
- The stealthiest path, where decreasing the probability of detection is prioritized over decreasing the task time
- The most vulnerable path (MVP), where the path is optimized considering the probabilities of detection, adversary task time, and response timelines

4.1.2. Blender

Blender[21] is a free and open-source 3D creation suite that is widely used throughout the 3D modeling community. It supports the entirety of the 3D pipeline and is designed to create efficient, highly detailed 3D models that can be ingested by any engine. The Blender toolset enables the creation of detailed, to-scale models of facilities, vehicles, and equipment that can be used for visualization, analysis, and training. The team used Blender to create the facility 3D model for this project.

4.1.3. Scribe3D© – Tabletop Recorder and Automated Tabletop Data Tool

Scribe3D© is a 3D tabletop recording and scenario visualization software created by Sandia National Laboratories (SNL). It was developed for use by other national laboratories, government organizations, and international partners using the Unity[22] game engine (which has been used for several other training and analysis tools within the DOE complex). Unity is a commercial game engine built for developers and non-developers to create a wide variety of games and applications. It features a fully customizable framework and set of development tools.

Scribe3D© is used to create, record, and play back scenarios developed during tabletop exercises or as a planning tool for performance testing, force-on-force, and other security analysis-related applications. The capabilities offered by Scribe3D© can help open discussions and capture the

[21] Blender Foundation, available at www.blender.org/about/ (2019).

[22] Unity Technologies, available at unity3d.com/unity (2019).

results, visualize consequences, collect data, and record events, as well as help make decisions while users develop scenarios. Data can be viewed in 2D or 3D and be played back in real-time or at various speeds. Transcript reports are automatically generated from the recorded data. The automated functions of Scribe3D© enable recorded scenarios to be run in a Monte Carlo fashion to collect large quantities of data for analysis purposes after initial scenarios are defined in the traditional tabletop exercise.

4.2. System Effectiveness Analysis Assumptions

The vulnerability assessment process is based on the following assumptions:

- Pathways are determined using tabletop analysis and subject matter expert (SME) judgement
- Target areas and operational states are accurately identified
- Adversary acts are planned and executed at a time that provides maximum opportunity for success for the adversary
- Facility security features function as-designed, and the response force responds as-defined
- Appropriate threat attributes and capabilities are identified
- When data are limited or missing and the analyst must rely on subjective expert opinion, the analysis is conducted conservatively with the advantage weighted toward the adversary
- Adversaries and response force are assumed to be equal in training and combat ability
- Adversaries are willing to die to achieve their mission
- Only sabotage scenarios are analyzed
- Response force strategy is denial only

5. HYPOTHETICAL MICROREACTOR PHYSICAL PROTECTION SYSTEM DESIGN

The PPS design for the microreactor applies both traditional PPS designs and the implementation of new features and approaches. The Design Evaluation Process Outline (DEPO) methodology, see Figure 5-1, was one of the guiding principles for the design of the PPS.[23]

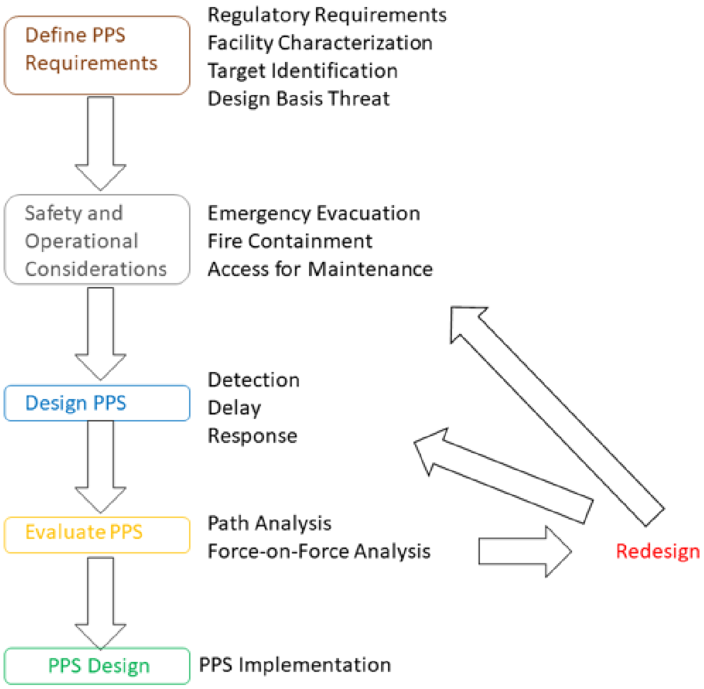


Figure 5-1. Security-by-Design DEPO[24]

The DEPO methodology, tailored to security-by-design, starts with defining the physical protection requirements, characterizing the facility operations, identifying theft and sabotage targets onsite, and determining the DBT the PPS must defend against. For this design and analysis, the current framework and proposed rule changes from the NRC were used as the regulatory basis of the PPS. Once the PPS requirements were defined, the team considered how the PPS would impact safety and operational environments. Some of these considerations include emergency evacuation from the site, fire containment, and access for facility maintenance. These factors are important for both ensuring the site meets all necessary safety requirements and reducing the burden on the operations of a facility that result from security system design and implementation. Integrating safety and operational considerations is important for increasing operational efficiency and decreasing operational costs at the facility. Once the safety and operational aspects have been considered, the PPS design begins. This design is based on detecting external and insider adversary forces by detecting and delaying them until an adequate response force can arrive to interrupt and neutralize them. Modeling and simulation tools such as PathTrace© were used to design the PPS with an effective probability of interruption. Once an effective probability of interruption is reached, a force-

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

[24] A. Evans, J. Parks, S. Horowitz, L. Gilbert, R. Whalen. "U.S. Domestic Small Modular Reactor Security by Design." SAND2021-0768.

on-force analysis is conducted to determine the probability of neutralization. If the PPS is deemed not effective, the system is redesigned based on the above-mentioned information.

5.1. Current Physical Protection Practices for SMRs and Microreactors

The base case for the design and analysis of the PPS includes an exclusion area (EA) that functions as a limited access area (LAA), a protected area (PA), and vital areas according to current NRC regulations found in the 10 Code of Federal Regulations Part 73 (e.g., 10 CFR 73). This project will evaluate the effectiveness of a PPS based on the information and regulations found in 10 CFR 73 as well as proposed rule-making changes for non-light water reactors (LWRs). This effort focuses on analyzing the PPS design as well as minimal-to-no onsite response force, which is a large effort for the SMR and microreactor community.

5.2. Perimeter Physical Protection System Design

The site includes an EA, which functions as the site's LAA. The EA encompasses an eight-foot-high fence that operates as demarcation, is not manned by guards, and does not contain any detection or assessment technologies. The entry point for the fence is usually unlocked during standard work hours. Since the EA does not include any sensing or entry control technology, it is excluded from this analysis.

For this facility design a traditional perimeter intrusion detection and assessment system (PIDAS) is applied to detect and delay a malicious act at the facility. This choice was made because the technologies and subsystem of a PIDAS have been tested and validated in many scenarios. However, further development technologies such as DMA and fused sensors could be used to detect adversary intrusion to a facility. These technologies may remove the need and requirement for a traditional PIDAS. Work in the future will examine the feasibility of these technologies as a replacement for the PIDAS versus the cost associated with PIDAS installation, operation, and maintenance.

The site's PA is controlled by a PIDAS consisting of an outer and inner fence line (e.g., eight-feet tall with outriggers) that are separated by an isolation zone equipped with sensing technology, see Figure 5-2. The isolation zone sensing technology consists of bistatic microwave sensing, and the inner fence includes a vibration sensor. The entire isolation zone is covered by closed-circuit television (CCTV) cameras for assessment from the CAS. All on-site CCTV cameras are on a loop recording and automatically save 10 seconds before and after an alarm.

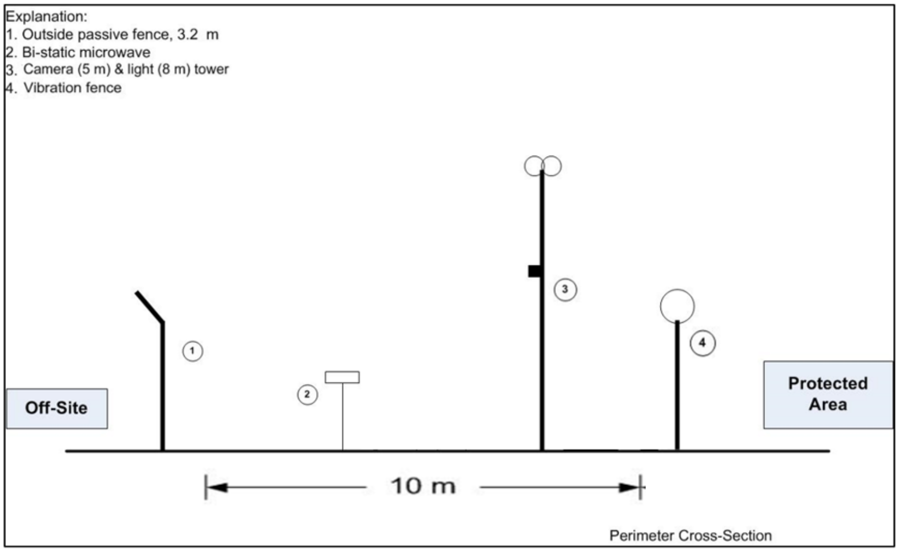


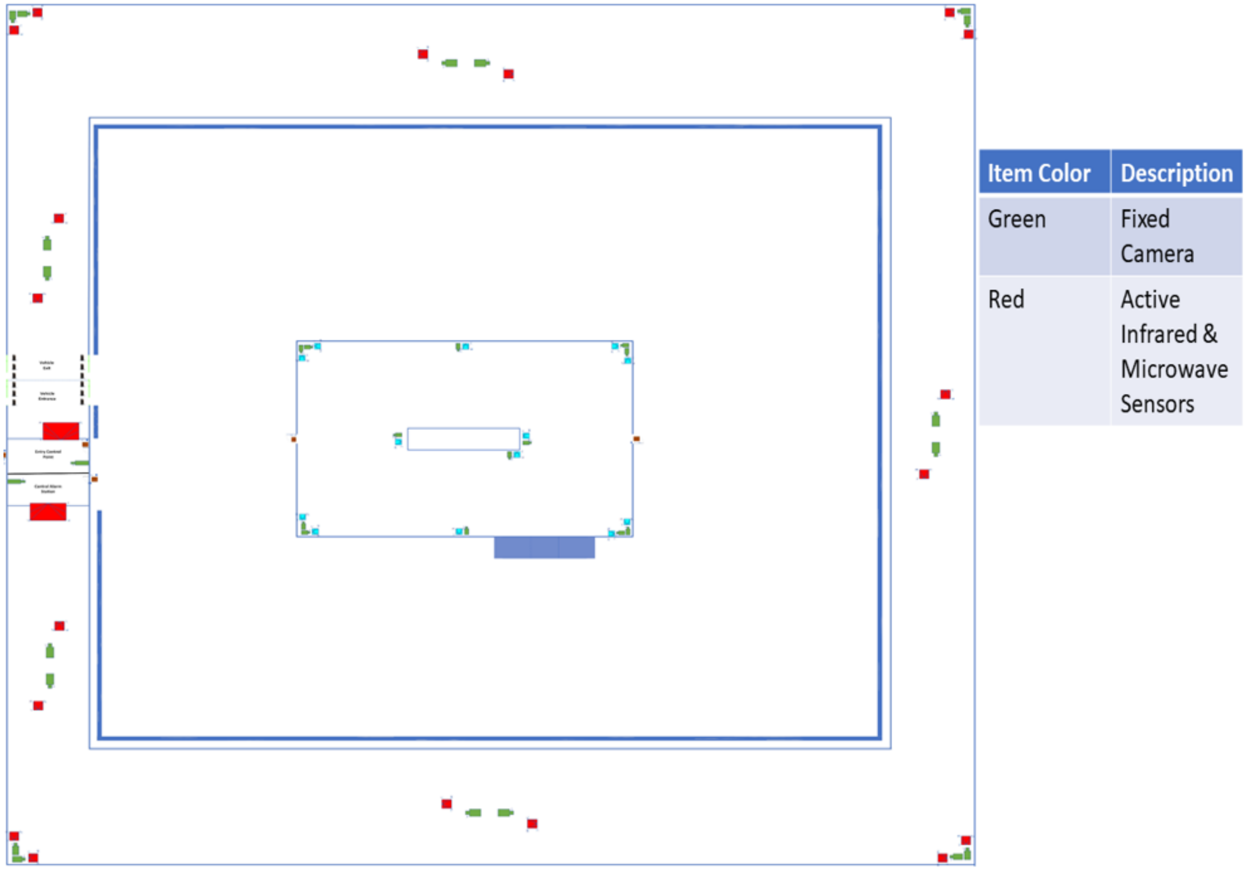
Figure 5-2. PIDAS Cross-section

The PA has two points of entry, one for personnel and one for vehicles, which are also both assessed with CCTV. The vehicle entrance is only operational during the receipt of a new reactor core or equipment. Inner and outer hydraulic vehicle barriers are raised when the access point is not operational. The personnel entrance is manned by two guards who perform detection of prohibited items before allowing personnel entry into the PA, when personnel or equipment need to gain access to the site. Pedestrians must pass through a metal detector, an explosives detection portal, and have their on-person items sent through an x-ray machine. Once through contraband detection, pedestrians are granted access with the use of a proximity card and the entering of a personal identification number (PIN). When receiving new reactor fuel or equipment at the site, the facility is notified ahead of time and the vehicle entry point is manned by two guards. The vehicle access control point consists of an inner and outer gate, with vehicle barriers on the outer side of each. The hydraulic vehicle barriers are maintained in a raised position when operational and only lowered one at a time as an authorized vehicle passes through as follows:

1. The driver and all other vehicle passengers must stop at the access point at the outer gate
2. One of the guards at the access point steps out of the guardhouse and verifies the driver's and any passengers' credentials, as well as the shipment authorization forms
3. If authorized, the outer gate is opened, and the inner vehicle barrier is lowered by the second guard
4. The driver is then instructed to drive inside the gate and stop before the second vehicle barrier
5. The outer vehicle barrier is raised, and the outer gate is closed
6. The passengers and driver then exit the vehicle and process through the personnel entrance in the same manner as described above
7. During this time, one of the guards at the vehicle access point visually inspects the vehicle for contraband and explosives
8. Once validated and granted access, the driver and any passengers return to the vehicle
9. The inner hydraulic barrier is lowered by the second guard, the inner gate is opened by the first guard, and the vehicle passes through

10. The inner gate is closed, the inner vehicle barrier is raised, and the process repeats

Figure 5-3 shows the design of the external PPS.



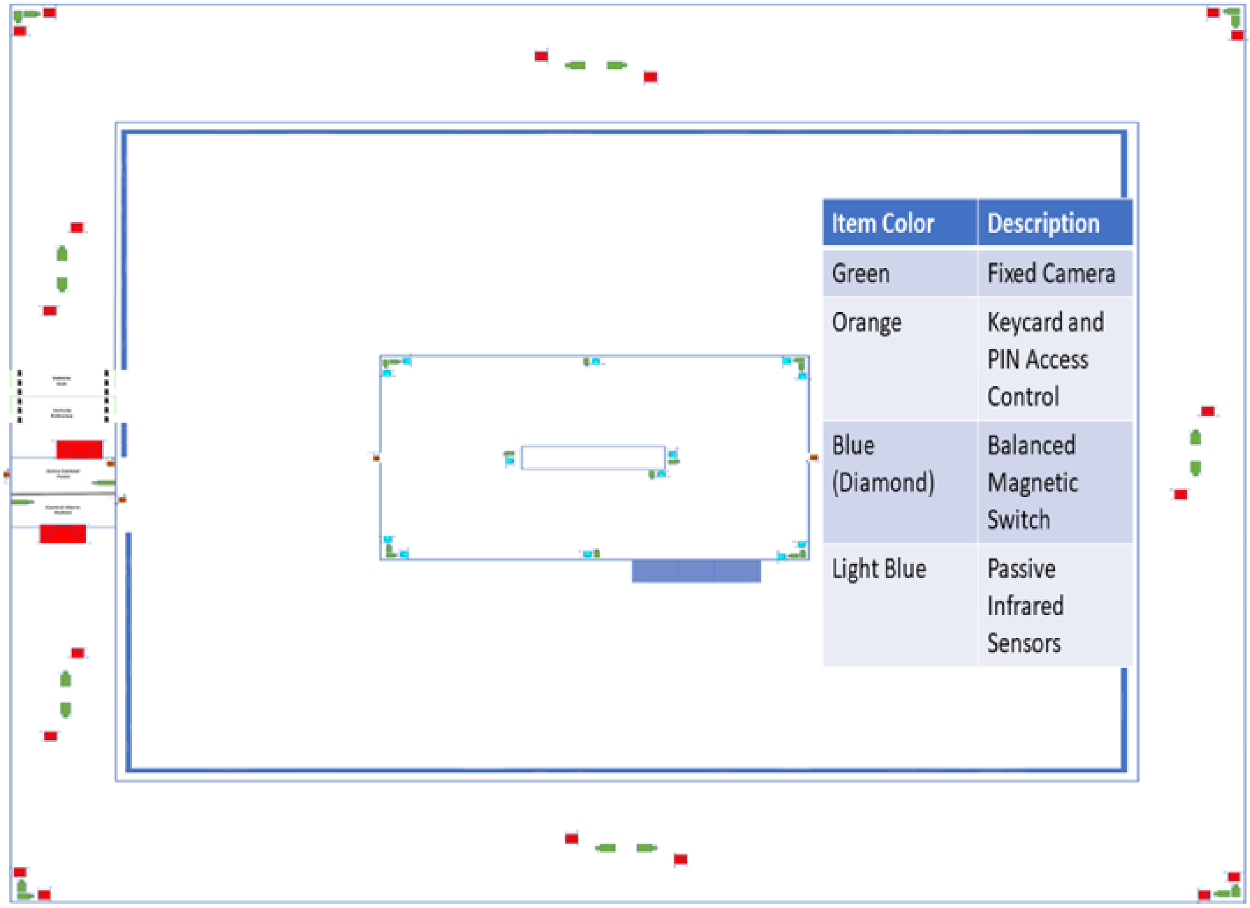
Item Color	Description
Green	Fixed Camera
Red	Active Infrared & Microwave Sensors

Figure 5-3. External Physical Protection System

A PIDAS may not always be necessary for a microreactor facility deployment. A PIDAS was used in this document as it is the currently available technology that has been tested for deployment for perimeter intrusion detection and assessment. Later sections of this report will discuss how technological advancements may enable detection beyond the fence line of the facility and decrease the need for a PIDAS to be deployed.

5.3. Interior Physical Protection System Design

The interior PPS design focuses on detecting access and intrusion into the building and delaying the adversary as much as possible. The PPS contains access control devices such as badge and PIN readers and balanced magnetic switches (BMS) on each doorway into the facility. The building interior has closed-circuit television (CCTV) cameras and passive infrared (PIR) sensors. **Error! Reference source not found.** shows the internal PPS.



Item Color	Description
Green	Fixed Camera
Orange	Keycard and PIN Access Control
Blue (Diamond)	Balanced Magnetic Switch
Light Blue	Passive Infrared Sensors

Figure 5-4. Internal Physical Protection System

This page left blank

6. TARGET IDENTIFICATION

The analysis centered on adversary attacks of three target locations, with a focus on direct sabotage of nuclear material. Due to inherent safety features and the complexity of these safety features, only direct sabotage scenarios were considered in this analysis.

The microreactor facility was designed to operate 19.55% enriched U-235 reactor fuel. The reactor operates within the main building onsite. The goal of this design and analysis is preventing theft and sabotage of the microreactor and, specifically, denying access to the microreactor. Denying access to the reactor for longer periods of time can increase the PPS effectiveness. For this analysis, sabotage was defined as when the adversary could properly place any breaching mechanism and successfully breach the microreactor to cause a possible release of radioactive material. This definition of sabotage is aligned with the proposed rule-making changes by the NRC, as discussed in Section 2. It will be important for microreactor facilities to not allow an adversary force to access the facility. Previous studies have shown that the longer the adversary is in the facility, the greater ability the adversary force has to harden themselves against the response force.[25]

In addition to the microreactor, other targets that are a concern for protection include the CAS and backup power supplies. If an alarm station is located onsite, it is necessary to maintain its security so CAS operators are able to continuously report alarms and adversary capabilities to the response force. This will ensure an effective response can be provided to the site. Backup power supplies are also important to operate the PPS if offsite power is lost. This will ensure that a loss of offsite power will not degrade the effectiveness of the PPS.

[25] A. Evans, J. Parks, S. Horowitz, L. Gilbert, R. Whalen. "U.S. Domestic Small Modular Reactor Security by Design." SAND2021-0768.

This page left blank

7. RESPONSE FORCE

The site will have one onsite guard to conduct personnel and package searches for those who need access into the facility. The site will also have one guard in the CAS, with one shift commander present to relieve CAS operator. These guard decisions were based on the premise of reducing onsite guard members to decrease operational cost. Guards are equipped with the following:

- Batons
- Pepper spray
- Handcuffs with keys
- Handheld radios

The offsite response force members are required to complete certification and training on selected weaponry and equipment that may be necessary in the event of an adversary attack. Weaponry and equipment for the response force members includes:

- Handguns with approximately 45 rounds of 9-mm ammunition
- Shoulder-fired weapons (e.g., 9-mm H&K MP-5s and 5.56-mm type rifles)
- Batons
- Pepper spray
- Handcuffs with keys
- Handheld radios

7.1. Response Force Assumptions

Due to the uncertainty in future SMR security designs and regulations, the analysis will focus on a PPS that does not use onsite armed response force personnel. Based on this assumption, no armed responders are on site, and response force times of 30 and 60 minutes were assessed.

This page left blank

8. THREAT ASSUMPTIONS AND CHARACTERISTICS

The concept of the DBT is used to establish the threat against which the PPS of a facility is designed. For this study (i.e., a notional facility with a notional threat) a DBT will not be used. Rather, this section will characterize the threat spectrum used for the security study. In this vulnerability assessment, the number of adversaries were varied from four to eight. It is assumed that a passive, nonviolent insider is providing facility knowledge for the outsider threat group.

8.1. The Vulnerability Assessment Process

The evaluation of an existing or proposed PPS requires a methodical approach that measures the ability of the security system to meet defined protection objectives. Without this kind of careful assessment, valuable resources might be wasted on unnecessary protection or, worse yet, fail to provide adequate protection of material against a theft attack by the defined threat. The vulnerability assessment (VA) methodology was developed to implement performance-based physical security concepts at nuclear sites and facilities.

The measure of overall security effectiveness is described as system effectiveness and expressed as a probability of effectiveness (P_E). P_E is determined using two terms: the probability of interruption (P_I) and the probability of neutralization (P_N). Analysis techniques are based on the use of adversary paths, which assume that a sequence of adversary actions is required to complete an attack on an asset. It is important to note that P_E will vary with the threat. As the threat capability increases, performance of individual security elements or the system will decrease.

Interruption is defined as the probability of arrival by the security force at a deployed location to halt adversary progress. Interruption may lead to the initiation of a combat event; however, it does not mean the task has been literally interrupted, simply that security forces have arrived before completion of the adversary task.

Neutralization is defined as the defeat of the adversaries by the security forces in a combat engagement or by other means. P_N is a measure of the likelihood that the security force will be successful in overpowering or defeating the adversary, given interruption. This defeat could take many forms; it could mean the adversaries are rendered task-incapable because a vital vehicle is disabled, or key personnel are neutralized. It could mean that all adversaries are neutralized. Neutralization is simply the ability of the security force to prevent the adversary from completing its mission.

These probabilities are treated as independent variables when the defined threat:

1. Selects a path that exploits vulnerabilities in the system, and
2. Is willing to use violence against the security forces.

In this case, the effectiveness of the system (P_E) against violent adversaries, expressed as the probability of interrupting and neutralizing the adversaries, is calculated by the following formula:

$$P_E = P_I x P_N$$

It is important to stress the conditional probability. Interruption (P_I) is meaningless without neutralization (P_N). If a system has a very high probability of interruption but lacks the firepower to respond to the given threat, the system fails. Conversely, if the system lacks the timely detection to get responders to the fight, it does not matter how well staffed and armed the response is.

8.2. Threat Assumptions and Characterization

The DBT assumed for this analysis is based on information from the 10 Code of Federal Regulations Part 73.1 (i.e., 10 CFR 73.1), see Table 8-1. The adversary team members were assumed to have the following characteristics:

- Intend to conduct a determined, violent external assault
  - Conduct the attack by stealth or deceptive actions
  - Operate in groups through a single-entry point
  - Have multiple groups attacking through multiple entries
- Have military training and skills, be willing to kill or be killed, and have enough knowledge to identify specific equipment or locations necessary for a successful attack
- Receive aid from an active or passive insider
- Have land or water vehicles, which could be used for transporting personnel and their hand-carried equipment to near the VAs
- Be able to conduct a land vehicle bomb assault, which may be coordinated with an external assault
- Be able to conduct a cyberattack
- Be able to perform any of the tasks needed to steal or sabotage critical assets
- Be armed with a 7.62 mm rifle or 7.62 mm belt-fed machine-guns (2), a pistol, ammunition, grenades, satchel charges containing bulk high explosives (not to exceed 10 kg total), detonators, bolt cutters, and miscellaneous other tools[26]
- Be able to each carry a man-portable total load (i.e., 29.5 kg [65 lb.])
- Be able to run at a speed of 3 m/s

For all scenarios, it was assumed each attack would start when the adversaries verified that no response force element (e.g., roving patrol) was within visual range of the initial breach. They would also avoid hardened and manned response positions if possible.

[26] 10 Code of Federal Regulations "Physical Protection of Plants and Materials."

Table 8-1. Outsider High-Level Threat Assessment Used for Analysis

High Level Terrorist Threat		
Motivation		Ideological; cause public terror (regionally and internally)
Goals		Theft and/or sabotage of nuclear materials/items
Capabilities and Attributes	Numbers	4/5/6/7/8; may divide into two or more teams
	Weapons	7.62 mm (assault rifles), 762 mm MGs (machine guns, RPG (rocket propelled grenade), sniper rifles, hand grenades
	Explosives	Improvised explosive device (IED), shape charges, vehicle bomb, suicide vest/backpack, commercial and military explosives (assume adversary carries sufficient amounts to complete objective)
	Tools	Night vision devices, hand tools, power tools, bridging/breaching equipment, chains, ladders, ropes, cutting torches, radios, fake/stolen identification, stolen/purchased uniforms and insignias
	Weight Limit	20 kg (45 lb) per person
	Transportation	Foot, bicycle, motorcycle, automobile (truck, car, off-road), all-terrain vehicles, boat (rubber zodiac, small boat, fishing craft)
	Knowledge • Facility • Security System • Operations	Assume full knowledge of facility layout and target locations, security system (people, equipment/technology, and procedures), and mission-critical operations, functions, and processes
	Technical Skills	Military training, demolition, information technology, general and site-specific engineering
	Funding	High – regional and international support
	Insider Collusion	Planning, local cell structure, safe-havens, sympathetic population, logistics, money
	Support Structure	One passive insider (providing information only)

This page left blank

9. PATH ANALYSIS AND FACILITY UPGRADES

The analysis focused on developing a PPS that creates an effective probability of interruption for the entire site with an offsite response force. PathTrace© was used to identify potential outsider adversary pathways that could be used to commit a sabotage act at the facility. The first portion of the analysis centered on designing a security system with a P_I of 95% or greater for a response time of 30 minutes. The second portion of the analysis centered on developing a PPS with a P_I of 95% or greater for a microreactor facility that was placed below-grade.

9.1. Above-Grade Physical Protection System Design

An above-grade facility design was considered first for the layout and PPS design, with a goal probability of interruption of 95% or greater.

9.1.1. Base Case

The base case was designed according to appropriate NRC regulations and effective emergency management procedures and policies. The basis for this design is referenced in Figure 5-3 and **Error! Reference source not found.**. A path analysis was conducted in PathTrace© to determine the probability of interruption, the results of which can be seen in Table 9-1. In this case, both theft and sabotage of the microreactor were considered. However, the primary concern for this design was microreactor sabotage.

Table 9-1. Base Case Path Analysis Results

Target	Attack Type	Task Time (s)	Cumulative Probability of Detection (%)	Probability of Interruption (%)	Response Time (s)
Reactor	Sabotage	534	99	0	1800
Reactor	Theft	556	99	0	1800

Figure 9-1 shows the adversary path determined to be the MVP for this facility design. The adversaries breached the perimeter fence lines of the PIDAS and then infiltrated the facility through the entrance. Because of this low probability of interruption, the PPS was changed to improve the probability of interruption.

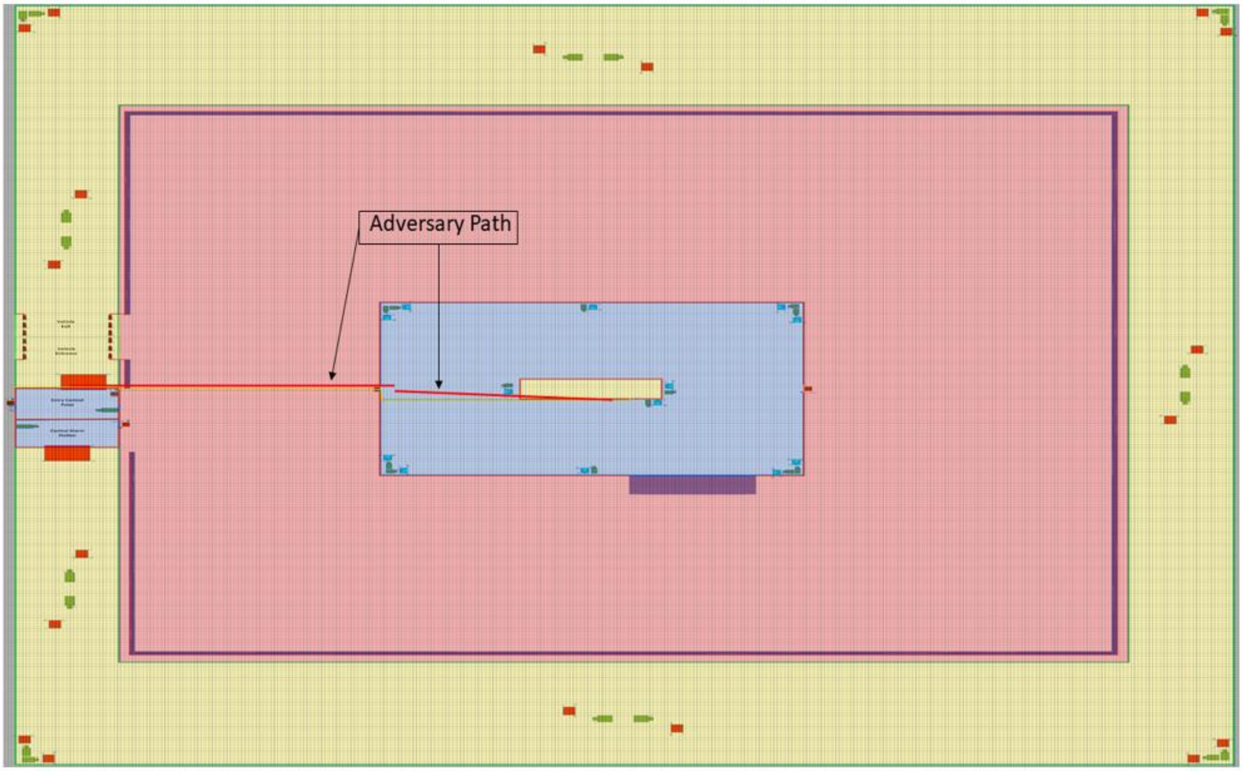


Figure 9-1. Base Case MVP

9.1.2. Upgrade One – Active Delay and Mantraps

The first upgrade implemented active delay features in the main reactor building and doorway mantraps. Active delay features are used to multiply adversary task times to complete tasks like moving through the facility, breaching doorways, or conducting sabotage. Mantraps are the result of an outer doorway and an inner doorway that enable secure entry into a facility, with access control devices that grant authorization for access. This can make entering a facility much more difficult for an adversary force. In this analysis, active delay such as slippery agents and obscurants were used. The delay multiplication factor can be seen in Table 9-2.

Table 9-2 Delay Multiplication Factors

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

These upgrades can be seen in Figure 9-2.

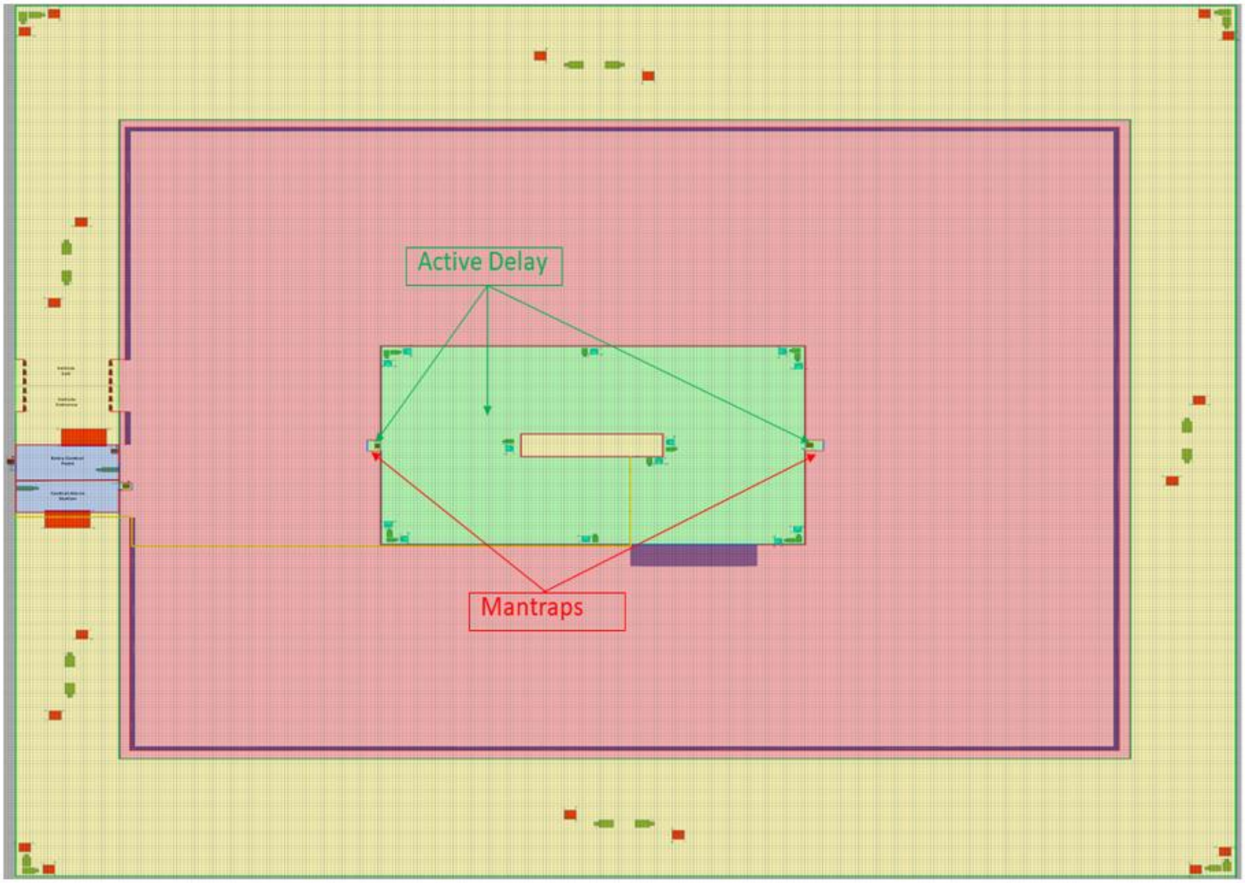


Figure 9-2. Upgrade One

The results from this upgrade can be seen in Table 9-3.

Table 9-3. Upgrade One Path Analysis Results

Target	Attack Type	Task Time (s)	Cumulative Probability of Detection (%)	Probability of Interruption (%)	Response Time (s)
Reactor	Sabotage	546	99	0	1800
Reactor	Theft	701	99	0	1800

The MVP for reactor sabotage from this upgrade can be seen in Figure 9-3.

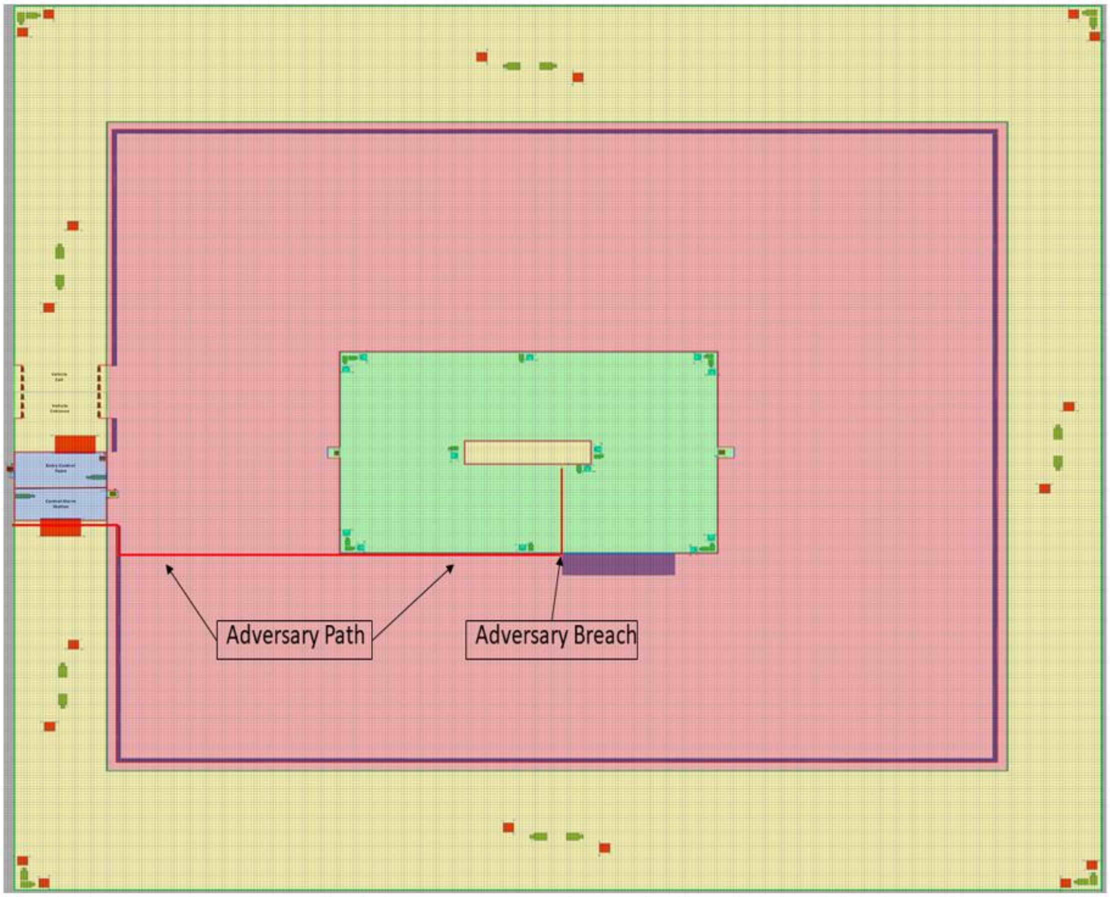


Figure 9-3. Upgrade One MVP

The adversary force in this case enters the facility by breaching the fences of the PIDAS, traverses the open space of the protected area, and then breaches the roll-up door to the facility. This allows the adversary to gain access to the facility in less time than it takes for the response force to arrive. Based on the adversary path, reinforcement was applied to all facility doors, including the roll-up doors, to increase the adversary task time of reaching the microreactor.

9.1.3. *Upgrade Two – Hardened Doorways, Security Area Around the Microreactor*

The second upgrade entailed placing the microreactor inside of another security area (i.e., placing the microreactor inside a reinforced concrete structure with access controls) and reinforcing facility doors and roll-up doors. These doors are reinforced by placing moveable reinforced concrete barriers behind them to increase the overall adversary task time to reach the reactor. Figure 9-4 depicts this upgrade.

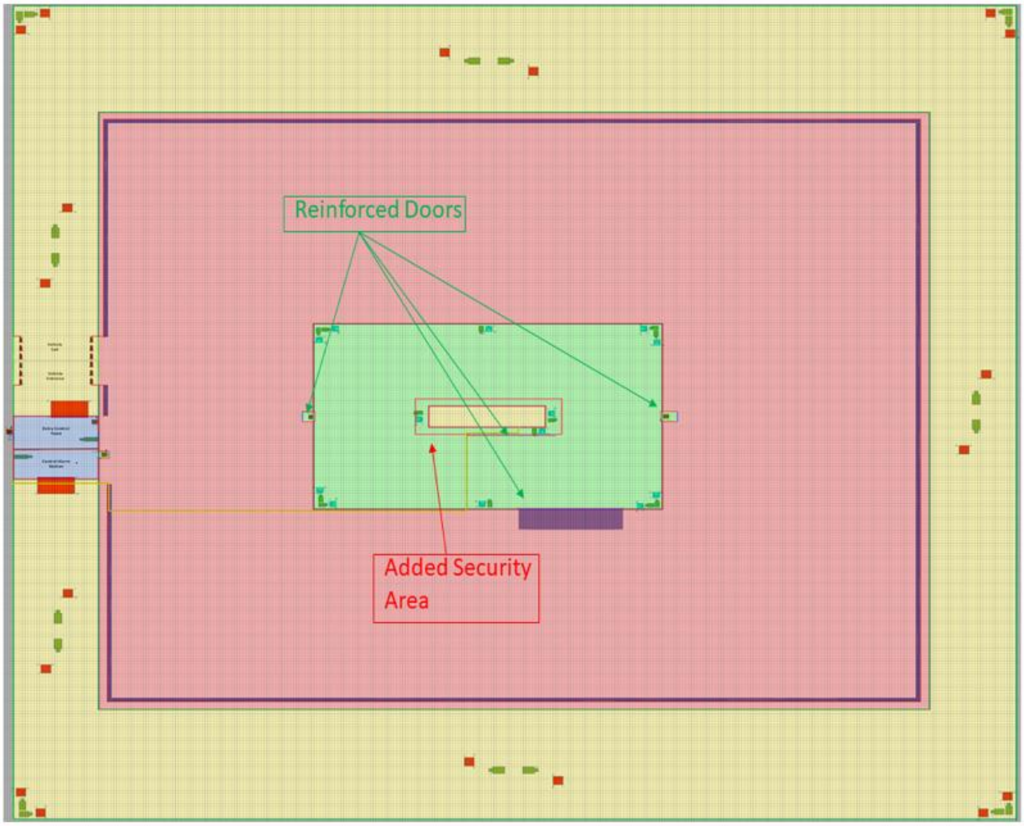


Figure 9-4. Upgrade Two

The results from this upgrade can be seen in Table 9-4.

Table 9-4. Upgrade Two Path Analysis Results

Target	Attack Type	Task Time (s)	Cumulative Probability of Detection (%)	Probability of Interruption (%)	Response Time (s)
Reactor	Sabotage	1498	99	0	1800
Reactor	Theft	1658	99	0	1800
CAS / Control Room	Sabotage	304	99	0	1800

The MVP for reactor sabotage from this upgrade can be seen in Figure 9-5.

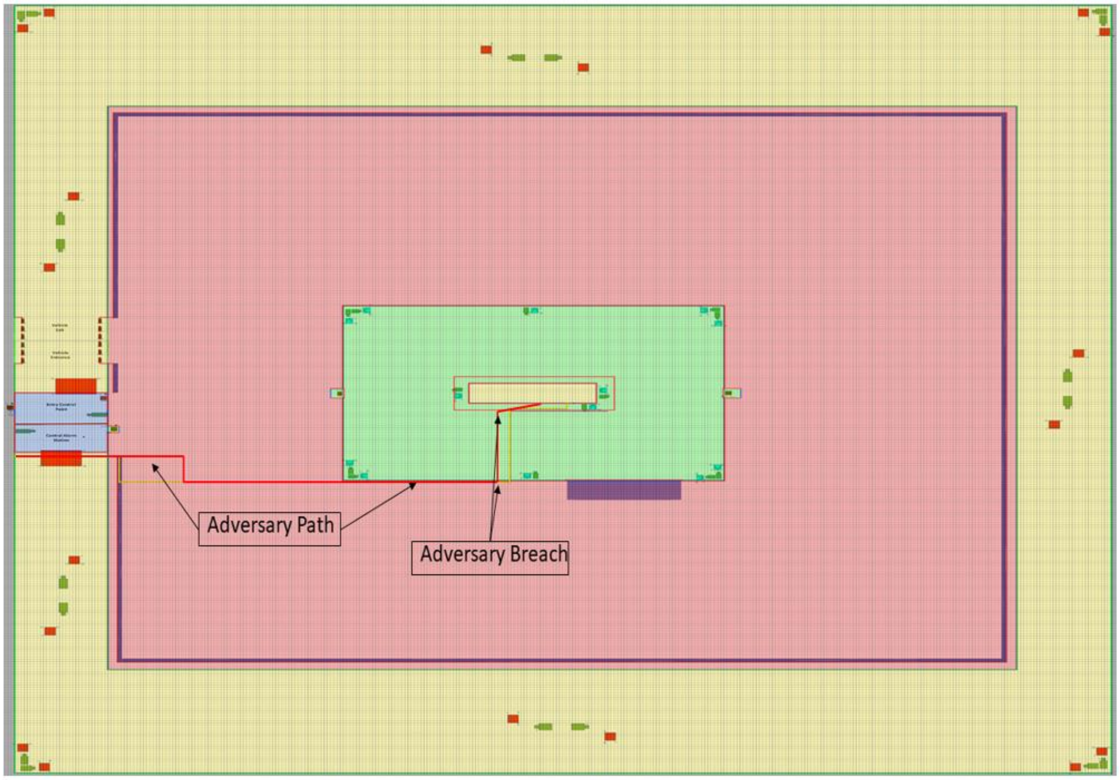


Figure 9-5. Upgrade Two MVP

The adversary enters the facility by breaching the two fence lines of the PIDAS, traversing the protected area, breaching through the facility outer wall, breaching the added security area around the microreactor, and gaining access to the microreactor. To achieve greater delay time for increasing the adversary task time, the wall thicknesses around the facility were increased.

9.1.4. Upgrade Three – Increased Wall Thickness and Internal Facility Hallway and Extended Detection

Due to the reinforced doorways, the adversary seemed to breach through walls instead. PPSs are designed around a concept called "no-weak links." The reinforced doorways included inside of walls with shorter delay times created a vulnerability to the site. To address this vulnerability, the wall thickness was increased from 0.6 m thick reinforced concrete to 1.2 m thick reinforced concrete. When the walls were updated with these increased thicknesses, the reinforced doorways were also increased in thickness. In addition, an internal hallway was created for the facility. This internal hallway separates the reactor from where the backup power supplies, used for security and safety purposes, could be located. Extended detection was also implemented in this design. Using a combination of radar and video motion detection that reaches far beyond the facility perimeter, the deliberate motion algorithm (DMA) can decipher motion moving toward the facility, while minimizing nuisance alarms from weather or traffic in the area. It is assumed that detection begins between 200 and 300 meters from the perimeter fence line of the facility. This in effect allows the RF to muster and arrive onsite earlier than if adversary detection began in the PIDAS. These upgrades can be seen in Figure 9-6.

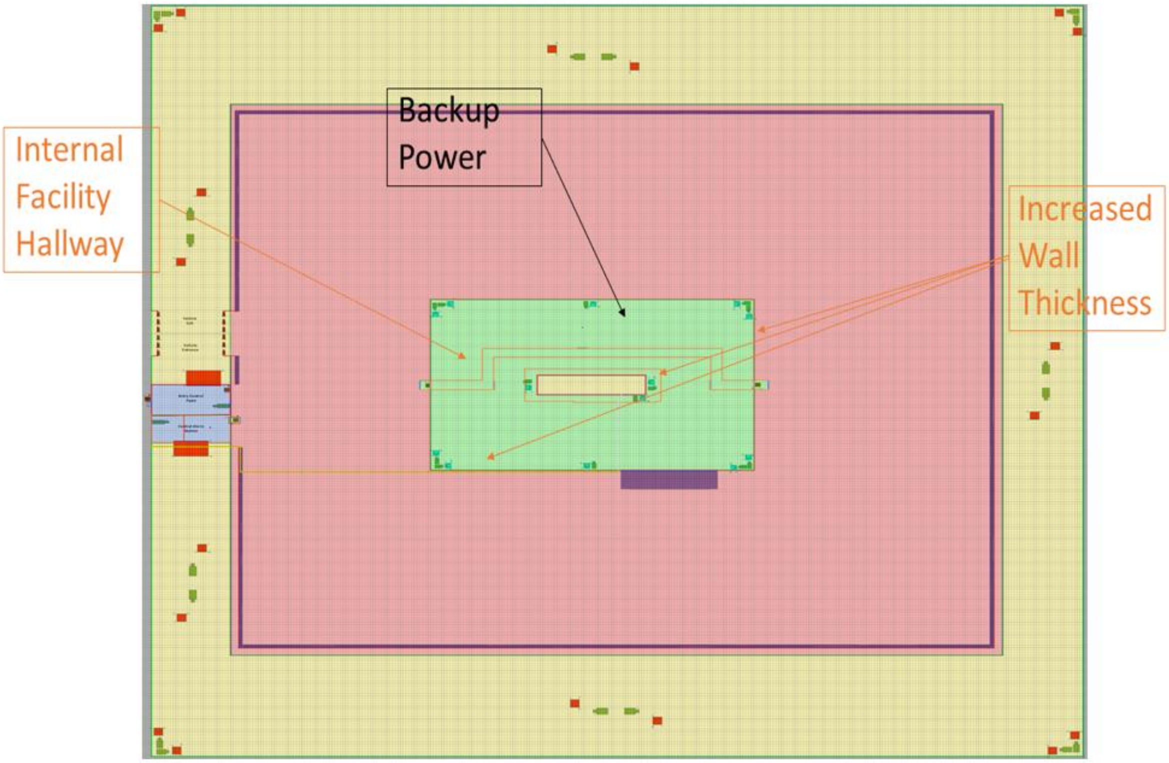


Figure 9-6. Upgrade Three

The results of this upgrade can be seen in Table 9-5.

Table 9-5. Upgrade Three Path Analysis Results

Target	Attack Type	Task Time (s)	Cumulative Probability of Detection (%)	Probability of Interruption (%)	Response Time (s)
Reactor	Sabotage	2454	99	99	1800
Reactor	Theft	2610	99	99	1800
CAS / Control Room	Sabotage	784	99	0	1800
Backup Power Supplies	Sabotage	1244	99	0	1800

The MVP for reactor sabotage for this upgrade can be seen in Figure 9-7. Upgrade Three MVPFigure 9-7.

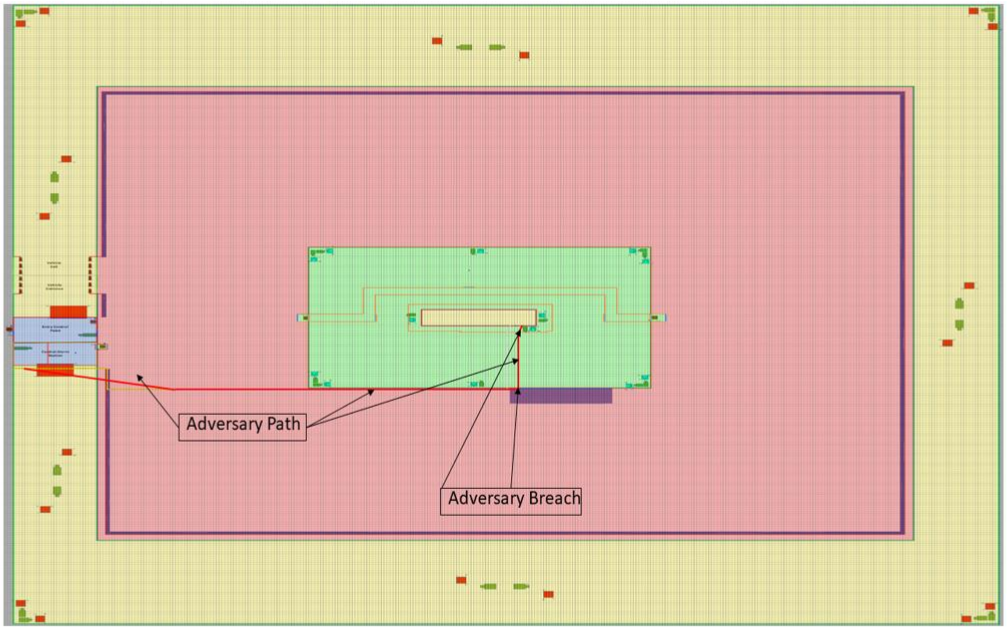


Figure 9-7. Upgrade Three MVP

This upgrade shows that a personnel hallway and increased wall thickness increases the adversary task time to longer than the 30-minute offsite response force time. This is a great improvement for delaying the adversary from entering the facility and reaching near the microreactor.

9.1.5. Upgrade Four – Moved Central Alarm Station and Control Room

To increase the adversary task time for reaching the CAS and control room area in this upgrade, both were moved into the reactor building separated by the hallway. This upgrade can be seen in Figure 9-8.

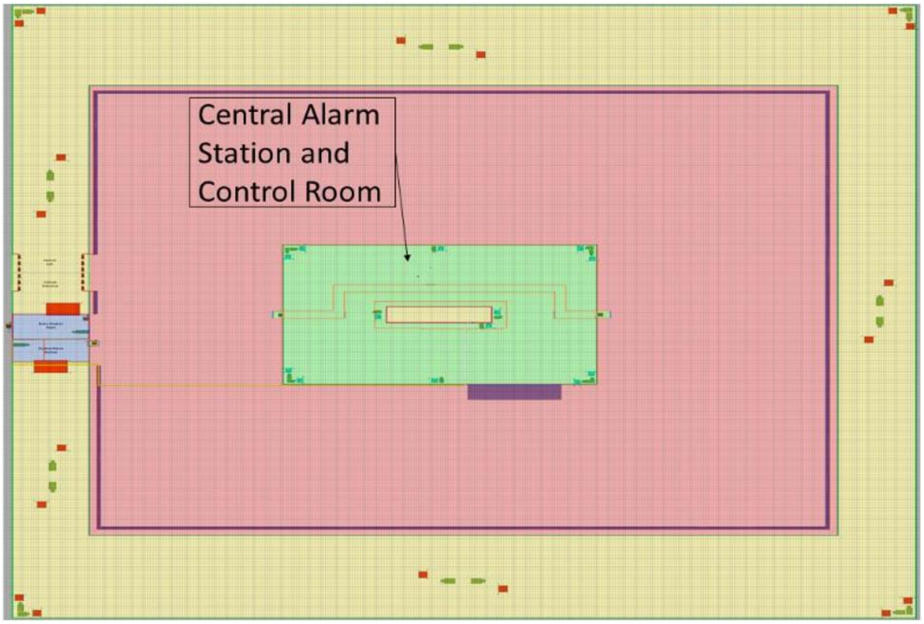


Figure 9-8. Upgrade Four

The results from this upgrade can be seen in Table 9-6.

Table 9-6. Upgrade Four Path Analysis Results

Target	Attack Type	Task Time (s)	Cumulative Probability of Detection (%)	Probability of Interruption (%)	Response Time (s)
Reactor	Sabotage	2454	99	99	1800
Reactor	Theft	2610	99	99	1800
CAS / Control Room	Sabotage	1245	99	0	1800
Backup Power Supplies	Sabotage	1244	99	0	1800

This upgrade increased the adversary task time to sabotage the CAS and the control room area of the site. Based on the primary purpose of reaching a high probability of interruption, these upgrades show an adversary may be able to be delayed long enough to allow for an offsite response force.

However, underground siting of a microreactor facility with similar upgrades may extend adversary task times even longer and account for complex adversary attack scenarios. The following section defines an underground microreactor facility and upgrades that could be made to increase adversary task times.

9.1.6. Above-Grade Path Analysis Results Comparison

Some of the PPS upgrades do not have a drastic impact on the total adversary task time. For example, upgrade one does not significantly increase the task time for theft and sabotage. However, it is important to understand that these upgrades were chosen based on increasing the effectiveness of the PPS by defending against the most vulnerable path. If a suggested upgrade is to harden a door, it may be worth considering hardening all the doors into the facility. This decreases the chance for a vulnerability at all doorways into the facility. It is important that the PPS be designed to provide balance along all paths for an adversary.

Table 9-7. Above-Grade Path Analysis Comparison

Target	Attack Type	Task Time (s)	Probability of Interruption (%)	Upgrade Scenario
Reactor	Sabotage	534	0	Base Case
Reactor	Theft	556	0	Base Case
Reactor	Sabotage	546	0	1
Reactor	Theft	701	0	1
Reactor	Sabotage	1498	0	2
Reactor	Theft	1658	0	2
Reactor	Sabotage	2454	99	3

Target	Attack Type	Task Time (s)	Probability of Interruption (%)	Upgrade Scenario
Reactor	Theft	2610	99	3
Reactor	Sabotage	2454	99	4
Reactor	Theft	2610	99	4

As Table 9-7 demonstrates, only the first three upgrades may need to be considered for this microreactor facility. The fourth analysis set was conducted to increase the adversary task time to attack the alarm station and backup power. As the second upgrade is applied, the cumulative upgrades result in an increase to more than double the total adversary task time. The effects of upgrades can cumulatively increase the overall adversary task time at the microreactor facility.

9.2. Below-Grade Microreactor Facility

Siting nuclear facilities below-grade has been done for many years for high value assets including nuclear materials. Placing theft and sabotage targets below-grade may inherently provide additional layers of security and radiation containment for nuclear facilities. The following information is based on the previously described design, but the microreactor will be placed below-grade. The above-grade portion of this facility will be primarily used for access to the below-grade portion of the facility. Figure 9-9 shows how this facility may be implemented below-grade.

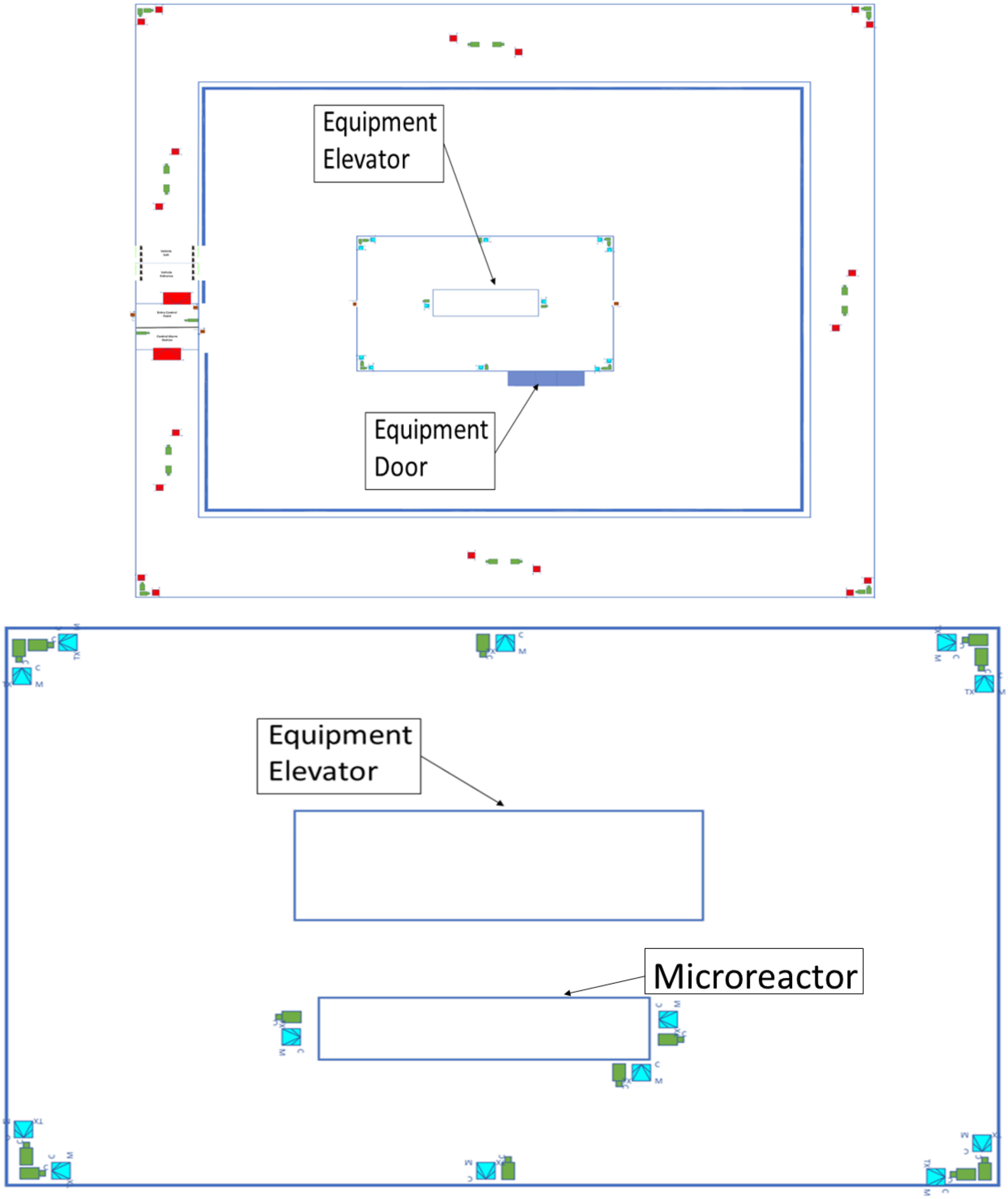


Figure 9-9. Below-Grade Microreactor Facility

In this design the microreactor is placed below-grade. An equipment elevator may have to be implemented for deployment of a whole-core replacement. In this model, the reactor would be brought in through the equipment door, moved to the equipment elevator, and moved below-grade and put in place.

Table 9-8 shows the path analysis for the above-mentioned facility design.

Table 9-8. Below-Grade Base Case Path Analysis Results

Target	Attack Type	Task Time (s)	Cumulative Probability of Detection (%)	Probability of Interruption (%)	Response Time (s)
Reactor	Sabotage	573	99	0	1800
Reactor	Theft	611	99	0	1800
CAS / Control Room	Sabotage	338	99	0	1800

In this analysis, the adversary team breached the two PIDAS fence lines, entered the facility through the entry door, entered the below-grade area via the stairwell, and then conducted sabotage on the reactor. These results show low probabilities of interruption, and therefore, further upgrades were made.

9.2.1. Upgrade One – Active Delay, Mantraps and Reinforced Doorways

For this upgrade mantraps were added at the external facility doors, reinforced moveable concrete barriers were placed at all doorways including rollup doors and the equipment elevator, and active delay was placed within the facility. These upgrades follow some of the upgrades prescribed in earlier sections of this report and can be seen in Figure 9-10.

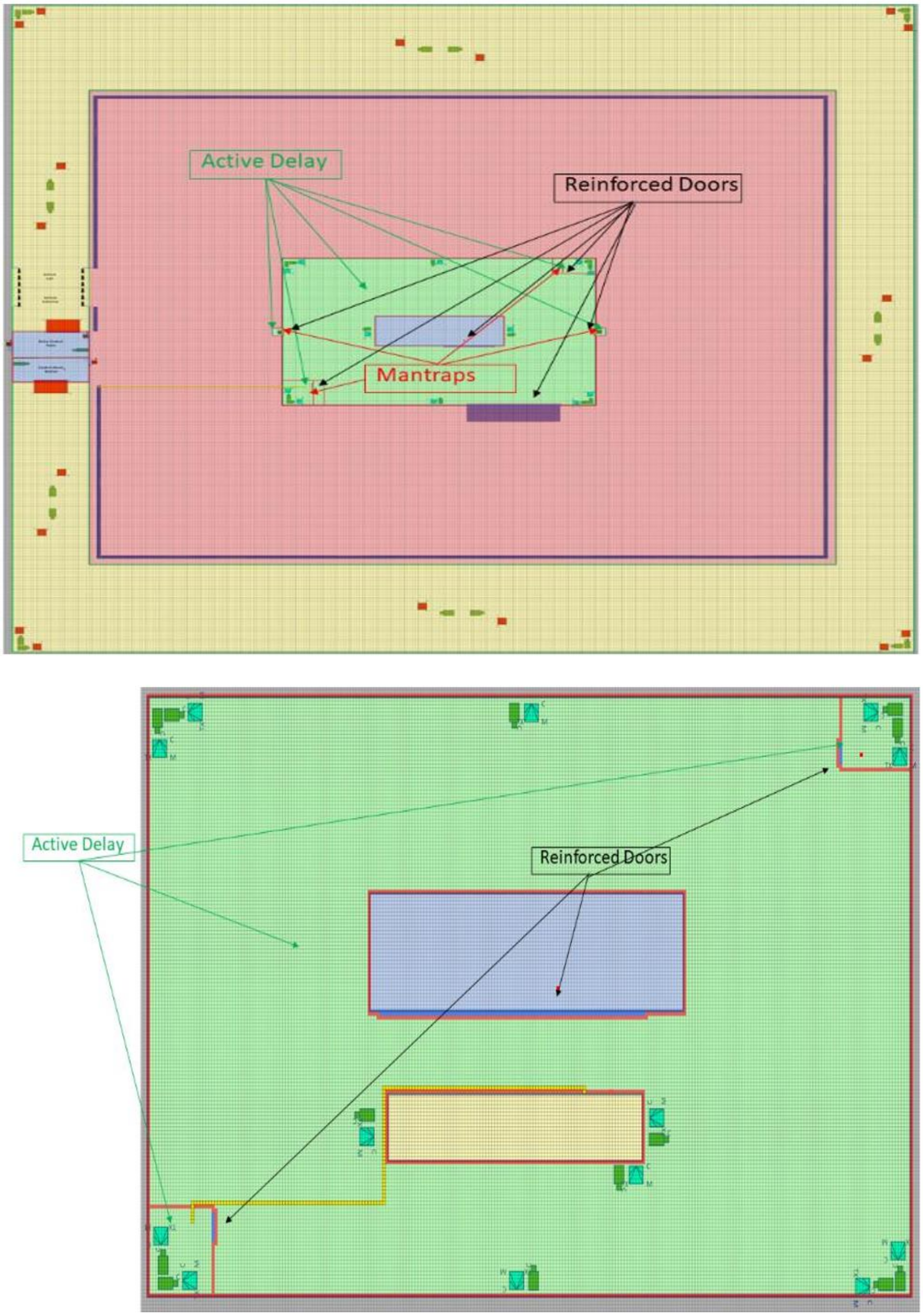


Figure 9-10. Below-Grade Upgrade One

The effects of these upgrades can be seen in Table 9-9.

Table 9-9. Below-Grade Upgrade One Path Analysis Results

Target	Attack Type	Task Time (s)	Cumulative Probability of Detection (%)	Probability of Interruption (%)	Response Time (s)
Reactor	Sabotage	1490	99	0	1800
Reactor	Theft	1543	99	0	1800
CAS / Control Room	Sabotage	315	99	0	1800

This analysis increased the overall adversary task time. However, further upgrades are still needed to increase the overall adversary task time to reach the necessary probability of interruption.

9.2.2. Upgrade Two – Security Area Around the Microreactor

To increase the adversary task time to achieve sabotage of the microreactor, an additional wall and security area were created around the microreactor. These upgrades were initiated in a similar fashion as the above-grade facility upgrades. This upgrade can be seen in Figure 9-11.

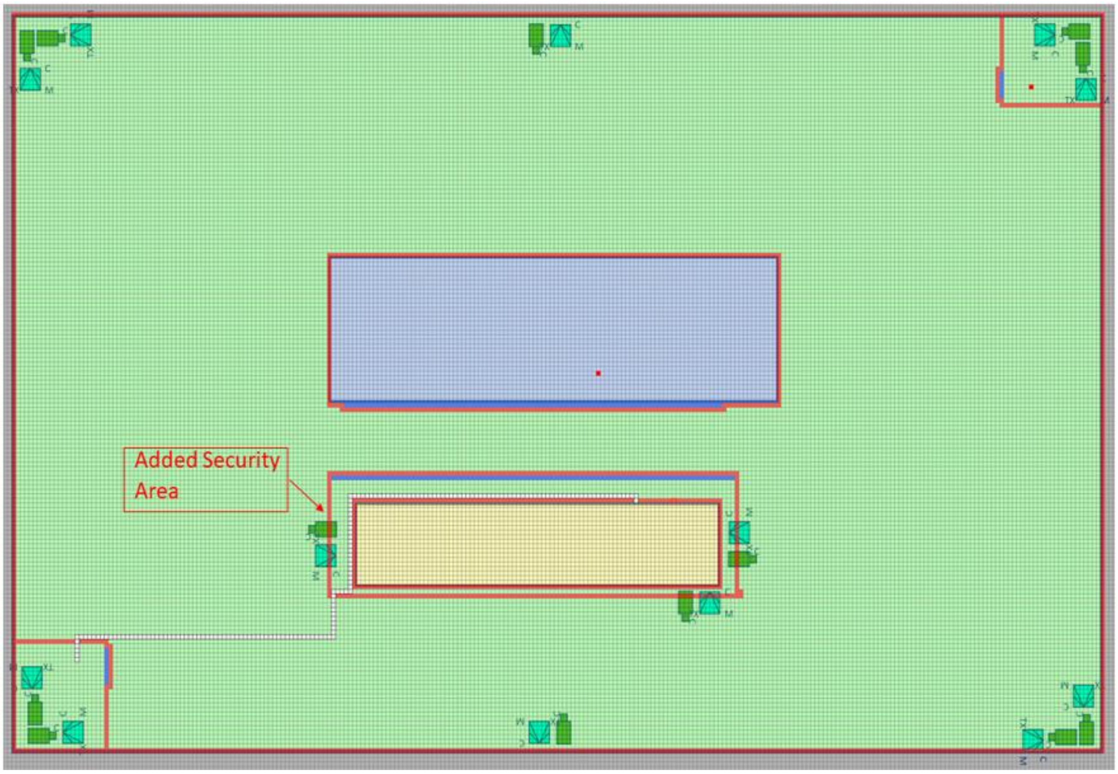


Figure 9-11. Below-Grade Upgrade Two

The effects of these upgrades can be seen in Table 9-10.

Table 9-10. Below-Grade Upgrade Two Path Analysis Results

Target	Attack Type	Task Time (s)	Cumulative Probability of Detection (%)	Probability of Interruption (%)	Response Time (s)
Reactor	Sabotage	1969	99	76	1800
Reactor	Theft	2022	99	76	1800
CAS / Control Room	Sabotage	315	99	0	1800

These upgrades increased the overall adversary task time. However, this did not achieve the probability of interruption desired. In this scenario, the adversary force penetrated directly into the stairwell to reach the below-grade floor and then breached the additional security area to sabotage the microreactor. Therefore, further upgrades were needed.

9.2.3. Upgrade Three – Increased Wall Thickness Around Reactor Security Area, Movement of Control Center and Extended Detection

In this upgrade the wall thickness around the microreactor was increased to match upgrade three of the above-grade facility design. Extended detection technologies were also applied. In addition, the CAS and control room were moved inside of the reactor building. These upgrades can be seen in Figure 9-12.

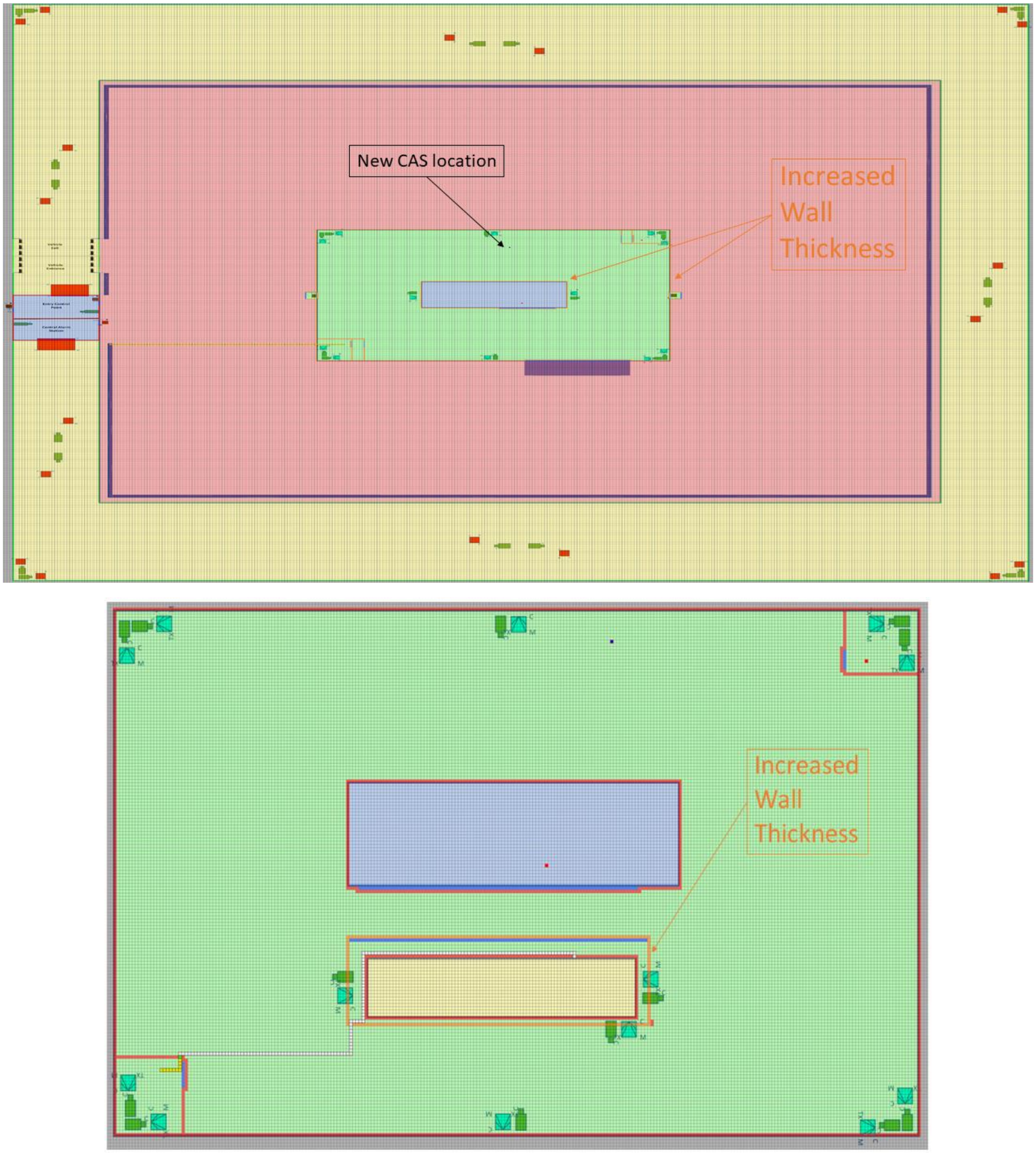


Figure 9-12 Below-Grade Upgrade Three

The results from this upgrade can be seen in Table 9-11.

Table 9-11. Below-Grade Upgrade Three Path Analysis Results

Target	Attack Type	Task Time (s)	Cumulative Probability of Detection (%)	Probability of Interruption (%)	Response Time (s)
Reactor	Sabotage	2450	99	99	1800
Reactor	Theft	2502	99	99	1800
CAS / Control Room	Sabotage	793	99	0	1800
Backup Power Supplies	Sabotage	1236	99	0	1800

As shown in Figure 9-12 and Table 9-11, below-grade siting can have very similar impacts as above-grade siting. However, this upgrade was completed without increasing wall thicknesses at all locations at the facility, unlike what was done in the above-grade design. The following upgrade will show how increasing wall thicknesses impacts the total adversary task time to achieve reactor theft and sabotage.

9.2.4. Upgrade Four – Increased all Wall Thicknesses

This purpose of this upgrade was to compare the difference between an above-grade and below-grade site configuration where all the walls and reinforced doors are of the same thickness. These upgrades can be seen in the Figure 9-13.

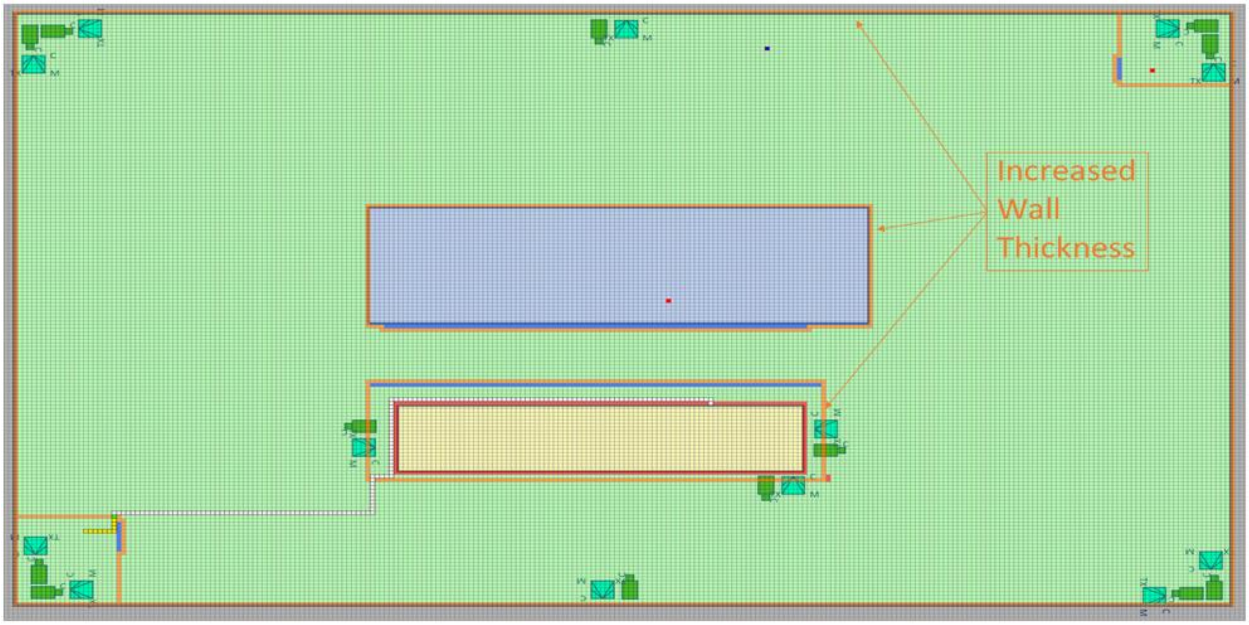


Figure 9-13. Below-Grade Upgrade Four

The results of this analysis can be seen in Table 9-12.

Table 9-12. Below-Grade Upgrade Four Path Analysis Results

Target	Attack Type	Task Time (s)	Cumulative Probability of Detection (%)	Probability of Interruption (%)	Response Time (s)
Reactor	Sabotage	3409	99	99	1800
Reactor	Theft	3462	99	99	1800
CAS / Control Room	Sabotage	1273	99	0	1800
Backup Power Supplies	Sabotage	2196	99	76	1800

As shown in Table 9-12, by moving the microreactor below-grade and applying similar upgrades, the adversary task time verges on 60 minutes. This allows for more flexibility for an offsite response force and can aid in the overall effectiveness of a PPS applied to a microreactor facility.

9.2.5. *Below-Grade Path Analysis Result Comparisons*

Placing the microreactor below-grade with similar upgrades as the above-grade design shows how the adversary task time can increase by placing the microreactor below-grade. However, in the below-grade case the first upgrade has a significant impact on the total adversary task time. It also shows that at the second below-grade upgrade, a thirty-minute response force time may be achieved.

Table 9-13. Below-Grade Path Analysis Comparison

Target	Attack Type	Task Time (s)	Probability of Interruption (%)	Upgrade Scenario
Reactor	Sabotage	573	0	Base Case
Reactor	Theft	611	0	Base Case
Reactor	Sabotage	1490	0	1
Reactor	Theft	1543	0	1

Target	Attack Type	Task Time (s)	Probability of Interruption (%)	Upgrade Scenario
Reactor	Sabotage	1969	76	2
Reactor	Theft	2022	76	2
Reactor	Sabotage	2450	99	3
Reactor	Theft	2502	99	3
Reactor	Sabotage	3409	99	4
Reactor	Theft	3462	99	4

The cumulative upgrades applied to the below-grade design drastically increase the adversary task time. Placing the facility below-grade has a tremendous impact on the PPS.

10. VULNERABILITY ANALYSIS OF FACILITY DESIGN

VA results are based on analysis of the physical paths that the adversary follows to achieve its objective or a set of objectives. The protection functions of detection and delay along the paths are key factors in determining the adversary attack scenario that is most likely to succeed. There are many possible combinations of potential paths to get to a target location and sabotage specific targets; therefore, all possible adversary paths must be considered. The following steps were taken in this analysis to determine system effectiveness (and ultimately system vulnerability) and facility risk:

1. An adversary timeline was constructed and all physical protection elements in the system were identified
2. Detection and delay values for each protection layer and path elements in the adversary sequence diagram (ASD) were incorporated
3. The MVPs were identified by analyzing the effectiveness of detection and delay along each possible path
4. Scenarios of concern were developed, response timelines and effectiveness were evaluated, and system effectiveness was determined

After completing the system effectiveness analysis, the VA team examined the paths and scenarios that had lower-than-desired system effectiveness (i.e., high vulnerability) and scenarios of interest that posed a risk to the facility. The goal was to identify the system's greatest vulnerabilities to theft so they could be mitigated.

10.1. Definition of Adversary Path

An adversary path is an ordered series of actions against a facility that, if completed, will result in a successful radiological sabotage event. Protection elements along the path potentially detect and delay the adversary so the dedicated response force can interrupt the series of events. The performance capabilities of detection, assessment, delay, and response are used in path analysis to determine the probability of interruption (P_I). Key performance measures included in estimating P_I are the probability of detection (P_D), delay time, and response force time (RFT).

10.2. Adversary Attack Scenarios

This hypothetical microreactor was designed to minimize the targets. For this analysis the primary target is reactor sabotage. See Table 10-1.

Table 10-1. Sabotage Targets

Target	Location	Safety Related Purpose
Reactor	Main Building	Provides the operation of nuclear material in the reactor

For this analysis two scenarios with varying adversary team numbers and varying response force timelines were explored. These scenarios include the adversary team attempting acts of sabotage on the target mentioned in Table 10-1. The force-on-force analysis and probability of neutralization analysis is based on upgrade four of the above-grade microreactor facility design.

10.2.1. Thirty-Minute Response Time

This scenario analyzes an adversary team breaching the facility and attempting to sabotage Reactor 1. The response force arrives at the exterior protected area boundary at the 30-minute mark and begins to recapture the site and neutralize the adversary force. In this analysis, the response force is awarded a win if the adversary is unable to sabotage the target due to attrition of adversary personnel and/or lack of required equipment to complete the necessary breaches or sabotage acts.

Table 10-2. Thirty-Minute Force-on-Force Analysis Results

Name	Results: 4 Adversaries	Results: 5 Adversaries	Results: 6 Adversaries	Results: 7 Adversaries	Results: 8 Adversaries
Number of Runs	100	100	100	100	100
Blue Wins	96	93	85	53	31
Red Wins	4	7	15	47	69
Average Engagements	14	18	22	26	27
Average killed in action (KIA) Engagements	5	7	9	10	11
Blue Force Count	8	8	8	8	7
Average Blue Force KIA	2	3	4	6	4
Average Blue KIA in Win	2	2	3	4	4
Red Force Count	4	5	6	7	8
Average Red KIA	4	5	6	5	5
Average Red KIA in Win	2	2	3	3	3

As can be seen in the Table 10-2, the number of blue force wins (i.e., probability of neutralization) steadily decreases as the number of adversaries increases and then sharply decreases when the adversary force size grows to seven. As the adversary force increases, both the response force numbers and positioning of the adversary force become an advantage for the adversaries rather than the for response force. In this scenario the adversary force would enter the facility and breach the external roll-up door. The response force entered the facility through this breached roll-up door to gain access directly to where the adversary force was located. However, the adversary team had the advantage of hardening their fighting positions in the facility, being in stationary locations, and being in better, more defensible positions to engage the response force.

As can also be seen from Table 10-2, as the adversary force size increased, the average number of blue forces killed in action (KIA) increases. This is again due to the advantage the adversary force has. PPS designs should consider the survivability of the response force, which is a major consideration in the overall effectiveness of the PPS.

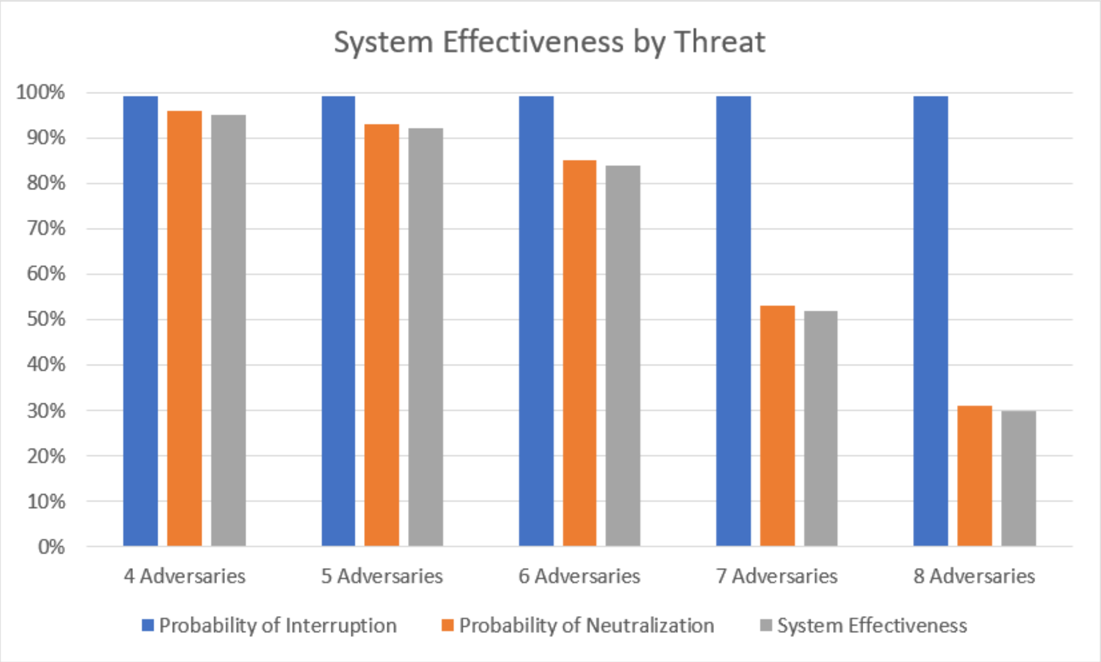


Figure 10-1. Thirty-Minute Response Time by System Effectiveness

As shown in Figure 10-1, the system effectiveness decreases as the adversary force size increases and steeply decreases when the adversary force size increases to seven. The system effectiveness of the PPS follows the probability of neutralization of the overall system. This finding is important in understanding the effectiveness of a PPS. This PPS design allowed for proper detection and delay to support an offsite response force with a 30-minute response force time. However, this design does not allow for a proper response as the adversary numbers begin to increase. Therefore, response force strategies and response force tactics would need to be evaluated and changed to improve the PPS effectiveness.

This page left blank

11. CONSIDERATIONS

The results from this analysis are useful for analyzing and designing a microreactor facility for domestic applications. Specifically, this analysis proved valuable in determining facility designs and PPSs that can be applied to improve the probability of interruption and may lead to a higher PPS effectiveness. Several aspects of facility and PPS design have been identified that should be considered when designing and siting a domestic microreactor facility.

11.1. Facility Design Considerations

Microreactor facilities must consider the facility layout when designing a PPS. In this analysis an internal hallway was added to provide additional delay to the microreactor and enable the placement of backup and emergency power supplies, the CAS, and control center in a more protected location. These design choices may incur additional upfront building costs but may result in improved PPS effectiveness. Microreactor facilities must also consider access points to the facility, both for normal operations and emergency egress from the facility. All entrances and exits into the facility present a potential pathway into the facility for an adversary force. Microreactor facility designers must analyze and understand how these ingress and egress points impact the PPS and the system effectiveness. Designers must also consider the construction materials that are used in building the microreactor facility. The construction materials and how they are used, such as wall thickness and reinforced walls, have a direct impact on the delay time inherent to the PPS. Using reinforced doors with metal sheeting can also increase delay time. These upgrades and reinforced construction materials may come at an increased upfront cost but can improve the performance of a PPS.

Federal, state, and local building codes may also impact the design of both the facility and the PPS. It is important to understand necessary building requirements for ventilation system, fire protection systems, electrical systems, and emergency exits. These features may require additional physical protection requirements to adequately protect the targets at a microreactor facility.

As was shown in the analysis, siting a microreactor facility below-grade (particularly the microreactor) can improve the delay time and total adversary task time. This increased adversary task time may increase the effectiveness of the PPS. This design choice may come at an upfront cost but allow for an effective PPS. Siting the facility below-grade may also minimize potential radiological consequences.

If an offsite response force will be the primary response force, microreactor facilities may choose to site the facility as close to the response force as possible. This placement can decrease the response force time to the facility and may improve the effectiveness of the PPS. It will also be important for the facility to determine the routes the response force can take to the facility and specifically identify the primary and secondary routes to ensure the effectiveness of the response force team and be prepared if a primary route is closed or delayed for any reason.

11.2. Physical Protection System Considerations

Microreactor facilities must include PPS components in the design of the facility. Microreactor facility designers should consider structural materials for their delay characteristics, identify access points to all security areas for the placement of access control devices and intrusion detection technologies, and placement of active delay features.

PPS designs for microreactor facilities should include the use of extended detection to detect adversaries as early as possible. Extended detection technologies like DMA, LIDAR, or RADAR can be used to detect adversaries before they reach the perimeter of the facility. Earlier detection may enable a more effective response force and, therefore, a more effective PPS. Facility siting also plays a key role in both facility design and PPS design. Extended detection such as DMA requires a facility where the landscape supports good observation and few obscurants (e.g., plant life). The use of LIDAR and RADAR technologies may also be applied for early and extended detection. DMA, LIDAR, and RADAR tend to function best in areas where visual observation is unobscured. Facility siting can also play a role in the effectiveness of the response force in neutralizing an adversary force. For example, facilities sited in higher ground can increase adversary task time in traversing hills. The use of berms can also improve the effectiveness of PPSs and decrease the consequence and likelihood of standoff attacks by an adversary force.

Site designers may also consider the use of active delay features such as slippery agents and obscurants. Active delay features can multiply the time it takes for the adversary to complete tasks and, therefore, increase the overall adversary task time for accomplishing an act of sabotage at the microreactor facility. The use of active delay features in combination with breaching walls or doors with magnetic locks will increase the task time to breach barriers and layers within the PPS. This increase in adversary task time will increase the probability of interruption and may increase the probability of neutralization, leading to improved PPS system effectiveness. Active delay features may pose a risk to site operations and personnel safety if inadvertent activation occurs. The deployment of these features may cause operational expenses for maintenance, support, activation, and the supporting infrastructure. Once these systems are deployed, they may also pose risks and increase the complexity for the response force to recapture and neutralize an adversary force. Additionally, after the features are deployed, the response force will have to gain access to the facility through these features to interrupt and neutralize the adversary force.

Microreactor facility designers may also consider the use of choke points. These choke points are locations through which the adversary must pass to gain access to facility target locations. Choke points can create targeted locations where the response force may effectively neutralize the adversary force and increase the effectiveness of the PPS.

Microreactor facilities may be designed to give CAS operators the ability to lock building doors even with the use of approved access credentials. These capabilities can increase the adversary task time to breach areas into the facility and can help mitigate insider threats at a microreactor facility. These capabilities should be applied to internal doorways before target locations to increase breach times and improve the effectiveness of the PPS.

It is also important that site security personnel and response force members are intimately familiar with the site and the target locations. This will increase the ability of response force members to respond to adversary actions and interrupt the adversary in a timely manner. The site should conduct regular exercises with onsite response force members and/or offsite response force members and correct deficiencies as soon as possible to increase the effectiveness of the response force. The roadways and paths necessary for the offsite response force to reach the site should also be considered, as weather on these roadways may increase the time it takes them to reach the site. Additionally, road blocks from traffic jams or the adversary acting as a blocking force are potential delays for the response force. Either of these scenarios increases the time it may take for the responders to reach the site. This increase in response force time can negatively impact the system effectiveness and the ability of the site to properly defend itself against an adversary threat.

12. CONCLUSION AND FUTURE WORK

The analysis shows key findings that can improve the PPS effectiveness of a microreactor facility. It is important that microreactor facility designers incorporate the PPS into the design phase, according to NRC regulations.

Offsite response forces require a facility and PPS design that implements enough delay time against the adversary for the offsite response to interrupt and neutralize the adversary. The analysis results indicate that active access delay measures with multiplication effects on adversary task time can be impactful in improving the PPS probability of interruption by allowing offsite response sufficient time to travel to the site and interrupt the adversary's progress. However, as discussed previously, active access delay features may pose a risk to operations due to their need for consistent testing and maintenance. These systems may also impact the response force's ability to respond. The site designers should consider alternative entrance points that the response force may use to interrupt the adversary before the adversary reaches the target location.

From this analysis it can also be seen that the use of extended detection can lead to improved probabilities of detection. Extended detection can improve the ability to detect an adversary force and notify the response force before the adversaries reach the protected area boundary. Extended detection will enable responders to arrive at the facility before the adversary can advance further into the facility. Based on the force-on-force analysis, this may improve the probability of neutralization and, therefore, the effectiveness of the PPS.

This analysis also showed that designing a microreactor facility and PPS to defend against sabotage may lead to effectively defending against acts of theft as well. Designing a PPS to defend against both theft and sabotage is vital for microreactor facilities.

Future efforts in this area include analyzing the placement of hardened fighting positions with a smaller onsite response force and an offsite response force. These efforts will enable an understanding of how hardened fighting positions may improve the effectiveness of the PPS. An economic analysis to determine the costs of upgrade scenarios will be conducted to determine cost-benefit tradeoffs by comparing system effectiveness with the cost of the facility and PPS design. Additional work will also consider a force-on-force analysis utilizing the below-grade facility design, as well as analyzing the impact of final denial systems on the effectiveness of the PPS.

REFERENCES

1. Garcia, M.L. 2008. Design and Evaluation of Physical Protection Systems, 2nd edition, Sandia National Laboratories.
2. "Advances in Small Modular Reactor Technology Developments. A Supplement to: IAEA Advanced Reactors Information System (ARIS)." International Atomic Energy Agency. 2020
3. Nuclear Regulatory Commission, "Regulations, Guidance, and Communications," accessed October 9, 2020, https://www.nrc.gov/security/domestic/reg-guide.html.
4. Nuclear Regulatory Commission, "Part 11 – Criteria and Procedures for Determining Eligibility for Access to or Control Over Special Nuclear Material," page last reviewed/updated September 15, 2020, accessed October 9, 2020, https://www.nrc.gov/reading-rm/doc-collections/cfr/part011/full-text.html.
5. Nuclear Regulatory Commission, "Part 25 – Access Authorization," page last reviewed/updated September 15, 2020, accessed October 9, 2020, https://www.nrc.gov/reading-rm/doc-collections/cfr/part025/full-text.html.
6. Nuclear Regulatory Commission, "Part 26 – Fitness for Duty Programs," page last reviewed/updated September 15, 2020, accessed October 9, 2020, https://www.nrc.gov/reading-rm/doc-collections/cfr/part026/full-text.html.
7. Nuclear Regulatory Commission, "Part 73 – Physical Protection of Plants and Materials," page last reviewed/updated September 15, 2020, accessed October 9, 2020, https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/full-text.html.
8. Nuclear Regulatory Commission, "Part 74 – Material Control and Accounting of Special Nuclear Material," page last reviewed/updated September 15, 2020, accessed October 9, 2020,
9. "Advanced Reactor Details", Nuclear Regulatory Commission, Accessed July 19, 2021, https://www.nrc.gov/reactors/new-reactors/advanced/details.html.
10. SECY-18-0076, "Options and Recommendation for Physical Security for Advanced Reactors," dated August 1, 2018, (ADAMS Accession No. ML18170A051).
11. SECY-18-0076, Nuclear Regulatory Commission, Margaret M. Doane, Options and Recommendation for Physical Security for Advanced Reactors," August 1, 2018, https://www.nrc.gov/docs/ML1805/ML18052B032.pdf.
12. Planned Rulemaking Activities – Rule, "Alternative Physical Security Requirements for Advanced Reactors," NRC-2017-0227, https://www.nrc.gov/reading-rm/doc-collections/rulemaking-ruleforum/active/ruledetails.html?id=76.
13. "Physical Security for Advanced Reactors," A Proposed Rule by the Nuclear Regulatory Commission on 07/16/2019, accessed October 13, 2020, Document Citation: 84 FR 33861, Page: 33861-33864, Agency/Docket Number: Docket No. NRC-2017-0227, RIN: 3150-AK19, Document Number: 2019-15008, https://www.federalregister.gov/documents/2019/07/16/2019-15008/physical-security-for-advanced-reactors.
14. World Institute for Nuclear Security and Nuclear Threat Initiative, "Security of Advanced Reactors," August 2020, ISBN: 978-3-903191-75-4
15. Revised Preliminary Proposed Rule Language, Posted by the Nuclear Regulatory Commission on Sep 13, 2020, NRC-2017-0227-0023.
16. Nuclear Regulatory Commission June 10, 2021, Public Meeting Presentation, "Part 53 Risk-Informed, Technology-Inclusive Regulatory Framework for Advanced Reactors Rulemaking – Subpart F and 10 CFR Part 73 Emergency Preparedness and Security."

17. "Average Weather in Fairbanks, Alaska, United States, Year Round - Weather Spark." n.d. Weatherspark.com. https://weatherspark.com/y/273/Average-Weather-in-Fairbanks-Alaska-United-States-Year-Round.

18. "Fairbanks, Alaska Climate." 2016. Bestplaces.net. 2016. https://www.bestplaces.net/climate/city/alaska/fairbanks.

19. A. Evans, J. Parks, S. Horowitz, L. Gilbert, R. Whalen. "U.S. Domestic Small Modular Reactor Security by Design." SAND2021-0768.

20. 10 Code of Federal Regulations "Physical Protection of Plants and Materials."

DISTRIBUTION

Email—Internal

Name	Org.	Sandia Email Address
Technical Library	01977	sanddocs@sandia.gov

Email—External (encrypt for OUO)

Name	Company Email Address	Company Name

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.