U.S. Domestic Molten Salt Reactor: Security-by-Design

Prepared for

U.S. Department of Energy

Alan Evans, Ben Stromberg, Ian Steagall, Doug Abell, Jason Davenport
Sandia National Laboratories

June 2024

SAND2024-07607R

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-NA0003525.

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, economical, and effective physical protection systems (PPS). The purpose of this work is both to develop a framework for the integration of security into the design phase of a molten salt reactor (MSR) and show how to effectively design a PPS with a reduced staffing headcount. Specifically, this work focuses on integrating PPS design features into a developed facility layout by making minor modifications to building structures. A suite of tools, including Scribe3D©, PathTrace©, and Blender©, were used to model a hypothetical, generic domestic MSR facility. Physical protection elements such as sensors, cameras, barriers, and responders were added into the model based on defending the hypothetical MSR facility against a hypothetical design basis threat (DBT). Multiple outsider sabotage scenarios were examined, with adversary team sizes ranging from 4–8 to determine security system effectiveness. The results of this work will influence PPS designs and facility designs for U.S. domestic MSRs. 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 completion of security-by-design (SeBD) for small modular reactors (SMRs). The conclusions and recommendations in this document may be applicable to all SMR designs.

ACKNOWLEDGEMENTS

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

CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

This report analyzes the design of a hypothetical molten salt reactor (MSR) facility and its physical protection system (PPS). The MSR facility was designed to reduce the overall site footprint, upfront security capital costs, and long-term operational PPS costs. This report will discuss the methodologies and design decisions that may be impactful for MSR vendors.

The hypothetical MSR facility was designed considering various open-source descriptions of MSR technologies from U.S. vendors. By combining various features, this report highlights design strategies for an effective PPS without identifying vulnerabilities for specific MSR designs. The facility implements two MSR reactors. Each reactor produces 200 MWe from 450 MWth of heat, for an approximate efficiency of 44%.[1] High-assay, low-enriched uranium is implemented to extend time between refueling and increase burn-up relative to the existing light water reactor fleet.

The facility is made of one large reactor building that houses the reactor, safety systems, secondary systems, spent fuel storage, control room and central alarm station (CAS). The second building at the facility is the entry control point (ECP) to the facility.

The PPS was designed in such a way that a small number of onsite responders could be used to protect the facility against an adversary attack. The facility was designed with robust delay barriers at key ECPs that require the adversary to perform complex breaches while being exposed to gunfire from responders who are in protected, reinforced, and elevated positions. The facility is designed in such a way that there are large open spaces and standoff distances that the adversary must cross that allow the responders to engage the adversaries. Additionally, the response locations are bullet- and blast-resistant enclosures (BBREs) which allow the responders to engage from within and outside of the reactor building. This ability ensures that the response force has multiple opportunities and multiple angles to engage an adversary force to increase the overall likelihood that the response force can neutralize the adversary. The figure below shows the layout of the response strategy utilized in this PPS design and analysis.

---

[1] Similar to FUJI (International Thorium Molten-Salt Forum, Japan) IAEA, "Advances in Small Modular Reactor Technology Developments," 2022, pp. 273-276.

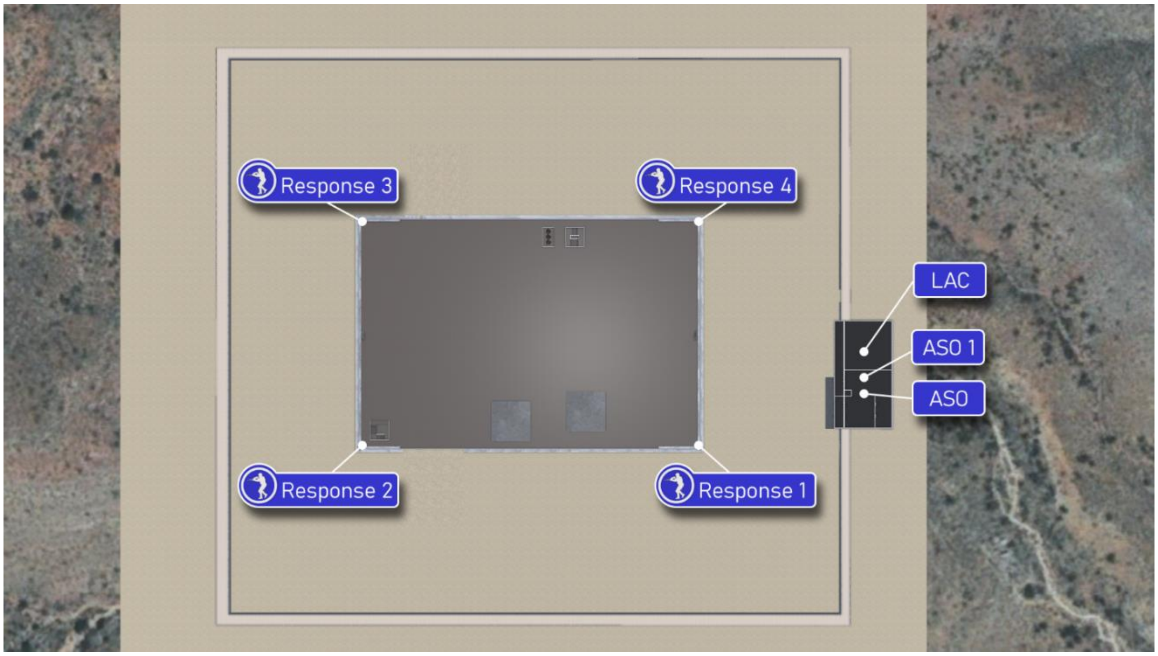

Figure E 1. Response Strategy

Three adversary attack scenarios were analyzed to determine the effectiveness of the PPS. The Scribe3D tabletop recording tool was used to conduct detailed analysis of critical engagements that would occur in the developed scenarios to determine the likelihood that the response force is able to neutralize the adversary force.

Table 1. Scenario One Results

Number of Adversaries	Engagement Number	Number of Adversaries in Engagement	Number of Responders in Engagement	Blue Wins	Red Wins	Internal Or External Engagement	Cumulative Probability of Neutralization (%)
8	1	8	2	64	936	External	92
	2	6	2	924	76	Internal	
7	1	7	2	575	425	External	99
	2	2	2	999	1	Internal	
6	1	6	2	554	446	External	99
	2	3	2	997	3	Internal	
5	1	5	2	768	214	External	99
	2	3	2	996	4	Internal	
4	1	4	2	946	54	External	94

Table 2. Scenario Two Results

Number of Adversaries	Engagement Number	Number of Adversaries in Engagement	Number of Responders in Engagement	Blue Wins	Red Wins	Internal Or External Engagement	Cumulative Probability of Neutralization (%)
8	1	4	2	936	64	External	99
	2	4	2	947	53	External	
7	1	3	2	985	15	External	99
	2	4	2	947	53	External	
6	1	3	2	985	15	External	99
	2	3	2	990	10	External	
5	1	2	2	993	7	External	99
	2	3	2	990	10	External	
4	1	2	2	993	7	External	99
	2	2	2	998	2	External	

Table 3. Scenario Three Results

Number of Adversaries	Engagement Number	Number of Adversaries in Engagement	Number of Responders in Engagement	Blue Wins	Red Wins	Internal Or External Engagement	Cumulative Probability of Neutralization (%)
8	1	1	1	923	77	External	99
	2	4	2	874	126	External	
	3	3	2	997	3	External	
7	1	1	1	923	77	External	99
	2	3	2	983	17	External	
	3	3	2	997	3	External	
6	1	3	2	993	17	External	99
	2	3	1	844	156	External	
5	1	2	2	996	4	External	99
	2	3	1	844	156	External	
4	1	2	2	996	4	External	99
	2	2	2	1000	0	External	

From the above tables it can be seen there are scenarios and engagements in which there are large number of adversary wins and large numbers of blue wins with high cumulative probabilities of neutralization. These high cumulative probabilities of neutralization result from the total scenario that was analyzed. In these scenarios, a large number of adversary wins was achieved during the scenario when the adversary team largely outnumbered the response force engaging the adversary team at the perimeter of the facility. However, due to the design of the facility and the defense-in-depth approach the response force is able to neutralize the remaining adversary forces in a high number of engagement simulations. This is due to the response force being able to shift the strategy to defend internal to the facility. In these scenarios, the response force only has to neutralize the adversary force before they make entry into doorways and has an advantage because they may be achieve fist shots in any internal engagement based on the door placements. Therefore, the large red wins in certain engagements is curtailed by larger response force wins in other engagements where the response force can neutralize the adversary force.

As can be seen from the scenario results in Section 5, the PPS design is highly effective against the range of adversaries and adversary attack scenarios.

Based on the design and analysis for this hypothetical MSR, several PPS design recommendations for both MSR and small modular reactor (SMR) vendors have been identified.

1. Using a square building design can allow for a smaller response force to provide effective security to the facility.
    a. Secondary systems and energy production systems should be located within the PA to ensure easier protection of the nuclear facility and reduce the number of buildings that may impact line-of-sight and response strategies.
        i. This ensures protection of long-lead items, plant capital equipment, and energy production equipment.
2. Consider methods that allow for force multipliers to reduce the overall security staffing headcount (including responders)
    a. Design delay barriers to channel adversaries into areas where the likelihood the response force can succeed is higher.
    b. Design delay barriers that cause adversaries to expose themselves for longer to increase the likelihood that the response force is successful.
    c. Ensure large standoff distances that force the adversaries to cross open and exposed spaces to increase the likelihood of success for the response force.
    d. Design delay features that require the adversary to use more of their explosive capabilities before reaching target locations.
3. Consider using roof plugs or hatches to allow for large equipment deliveries rather than large roll-up doors
    a. Creates additional delay time and can allow the PPS design to use door placements to channel adversaries into strategic locations
4. Consider the insider threat according to the DBT and capabilities of the insider threat.
5. Keep the PA within the facility clean and clear of obstructions.
    a. This does not require the PPS be evaluated or changed for laydown yards or other things.
6. Limit the number of vehicles in the PA.
    a. No storage of vehicles within the PA.

7. Consider legal and regulatory requirements for use-of-force and rules of engagement.
    a. The response strategy and PPS will need to be tailored to the rules of engagement requirements.
8. Designers should consider multi-modules on site early in the design process
    a. Consider intrusion detection system design for multi-modules as one unit is operational and the next unit is being built
    b. Consider response force strategies to be deployed

ACRONYMS AND DEFINITIONS

Abbreviation	Definition
ASO	armed security officer
BBRE	bullet- and blast-resistant enclosure
CAS	central alarm station
CCTV	closed-circuit television
CFR	Code of Federal Regulations
DBA	design basis accident
DBT	design basis threat
DEPO	design and evaluation process outline
DOE	Department of Energy
ECP	entry control point
FS	field supervisor
FTE	full time equivalent
LAC	last access control
LLEA	local law enforcement agency
MSR	molten salt reactor
NPP	nuclear power plant
NRC	Nuclear Regulatory Commission
OCA	owner-controlled area
PA	protected area
PH	probability of hit
PIDAS	perimeter intrusion detection and assessment system
PIN	personal Identification Number
PK	probability of kill
P_N	probability of neutralization
PPS	physical protection system
RCS	reactor cooling system
RTL	response team lead
SFR	sodium fast reactor
SME	subject matter expert
SMR	small modular reactor
Sandia	Sandia National Laboratories
SeBD	security-by-design
SSS	security shift supervisor
UPS	uninterruptible power supply

Abbreviation	Definition
U.S.	United States
VBS	vehicle barrier system

1. INTRODUCTION

Domestic nuclear facilities face stringent requirements for security, particularly for nuclear power-generating facilities, which include advanced small modular reactors (SMRs). This analysis focuses on the United States' (U.S.) 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, since it requires more upfront, operational, and maintenance costs in physical protection systems (PPS) and protective force personnel.

Future nuclear facilities will need to incorporate security-by-design (SeBD) 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.[2] In contrast, 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.

The molten salt reactor (MSR) facility described in this report is hypothetical. To avoid potential sensitivities, various individual characteristics of open-source, planned sodium fast reactor (SFR) facilities were selected and/or slightly modified for the hypothetical model.

The report documents the reactor, design of the facility, operations, and PPS. The goal of this report is to understand the feasibility and effectiveness of PPS designs that utilize an onsite, armed response force and remote operated weapon systems.

---

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

2. HYPOTHETICAL MOLTEN SALT REACTOR SITE

The hypothetical facility developed for this design and analysis draws from features in multiple SFR designs currently in development within the U.S. and internationally.[3] While all design features, specific values, or characteristics are notional, attempts were made to develop a design that provides valuable insight into principles applicable for domestic MSR development. This study establishes this design and imposes a framework for the design and analysis to capture SeBD features for domestic MSR applications.

2.1. Site Description

2.1.1. Climate

The hypothetical MSR facility in this study is located 15 miles outside of Portland, Oregon. The region surrounding the facility has a moderate, wet climate. Summers are warm and dry, and winters are cool and wet. The warm season starts in June and lasts until September, with an average daily high temperature above 76°F.[4] The cold season is between November and February and has an average daily high temperature below 52°F.[1] As temperatures rarely exceed 95°F, the temperature should not affect any passive infrared (PIR) technologies. The region generally has a low level of humidity but receives an average of 43 inches of rain and three inches of snow per year.[5] This level of precipitation may induce noise in sensors and cause the degradation of security elements (mold/rust/mineral deposits/electrical shorts). Portland is cloudy about 60% of the time and foggy about 34% of the time.[6] This may impact assessment via electronic means or visual inspection by patrols or response forces.

2.1.2. Local Wildlife

Oregon has a large variety of wildlife that may affect day-to-day operations at a nuclear facility. These include multiple species of deer, elk, antelope, and moose.[7] These animals are not intimidated by fences and can jump up to seven or eight feet high.[8] While these animals are not a danger to nuclear materials, they may impact staff movement, disrupt operations, and set off nuisance alarms. The Pacific Northwest is also home to black bears and multiple species of foxes. Foxes[9] can climb fences or tunnel underneath them, which may cause nuisance alarms and impact operations. Oregon

---

[3] For numerous descriptions of sodium fast reactors, see: International Atomic Energy Agency, "Advances in Small Modular Reactor Technology Developments," A Supplement to: IAEA Advanced Reactors Information System (ARIS), 2022 Edition, Vienna Austria, September 2022, pp. 223-230, and International Atomic Energy Agency, Advanced Reactors Information System (ARIS), https://aris.iaea.org/sites/SFR.html.

[4] Weather Spark, "Climate and Average Weather Year Round in Portland," https://weatherspark.com/y/757/Average-Weather-in-Portland-Oregon-United-States-Year-Round

[5] Best Places, "Climate in Portland, Oregon," https://www.bestplaces.net/climate/city/oregon/portland

[6] Current Results, "Total Cloudy and Foggy Days at US Cities a Year," https://www.currentresults.com/Weather/US/cloud-fog-city-annual.php

[7] Oregon Department of Fish & Wildlife, "Hoofed Mammals," https://myodfw.com/wildlife-viewing/species/hoofed-mammals

[8] https://sciencetrek.org/sciencetrek/topics/elk/facts.cfm#:~:text=Elk%20can%20run%20up%20to,up%20to%208%20vertical%20feet, https://www.ncwildlife.org/Learning/Species/Mammals/Whitetail-Deer/Fencing-to-Exclude-Deer#:~:text=An%20adult%20deer%20can%20easily,vertical%20or%20horizontal%20slatted%20fences., and https://northamericannature.com/moose/#:~:text=The%20moose%20are%20also%20used,as%20high%20as%207%20feet.

[9] https://www.wildlifeonline.me.uk/articles/view/red-fox-deterrence

is also home to many species of large birds, including the Trumpeter Swan,[10] which may exceed 30 lbs. Birds may induce nuisance alarms as they move throughout the property, including motion detectors and fence vibration sensors.

2.2. MSR Buildings

The MSR site consists of one building called the reactor building surrounded by the protected area (PA). On the boundary of the PA is an entry control point (ECP) building. The ECP includes an access point for personnel and vehicles. Figure 2-1 depicts the overall site layout used for the MSR facility. The facility is comprised of one reactor building, with an above-grade and below-grade floor, and an entry control point building.

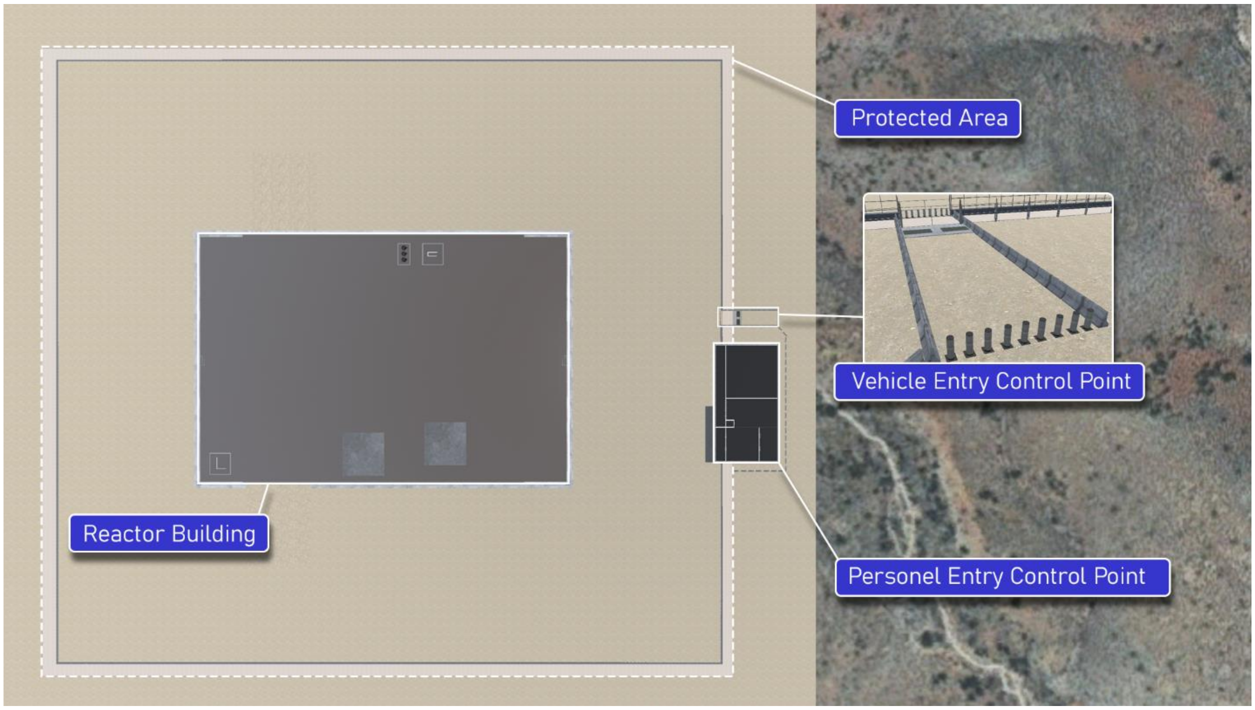

Figure 2-1. MSR Facility Layout

---

[10] https://myodfw.com/wildlife-viewing/species/trumpeter-swan

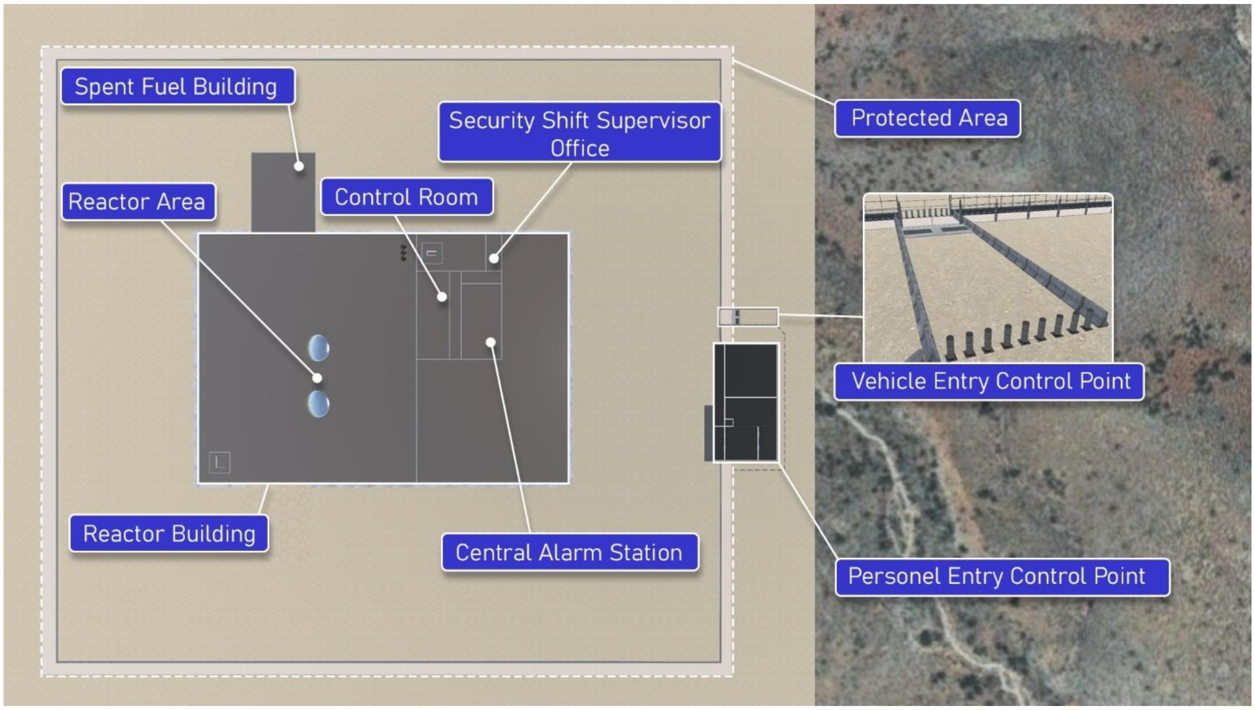

Figure 2-2. MSR Below-Grade Floor Plan

2.3. Reactor Description

Based on numerous MSRs, the site operates two reactors inside a single reactor building. Each reactor unit consists of the primary system components inside of a containment vessel. A reactor pressure vessel is not needed, due to the low pressure (near atmospheric) inside of the reactor. The confinement structure is 25-m deep with a 15-m diameter. The confinement is surrounded by a reinforced-concrete wall that can withstand airborne missiles caused by environmental events. Most materials in contact with the salt are made of a nickel alloy material (Hastelloy-N) due to its resistivity to corrosion[11]. Only one reactor is refueled at a time to ensure there is constant power coming from the plant. The reactor core is not refueled; instead, the entire unit is replaced at end of life. Passive reactivity control is achieved through the negative temperature reactivity coefficient, while active reactivity control is performed with control rods and fuel salt draining. A freeze valve, which is placed below the reactor, melts in cases where temperatures exceed safety ranges and withdraws the coolant into the drain tanks[10]. (These tanks are designed such that criticality conditions are not met by the fluid.) A fuel salt off-gas system is used to remove volatile fission products, while all other fission products are considered contained in the primary salt system[12].

---

[11] IAEA, "Advances in Small Modular Reactor Technology Developments," 2022, pp. 253-288.

[12] Similar to IMSR400 (Terrestrial Energy Inc. Canada) IAEA, "Advances in Small Modular Reactor Technology Developments," 2022, pp. 253-256

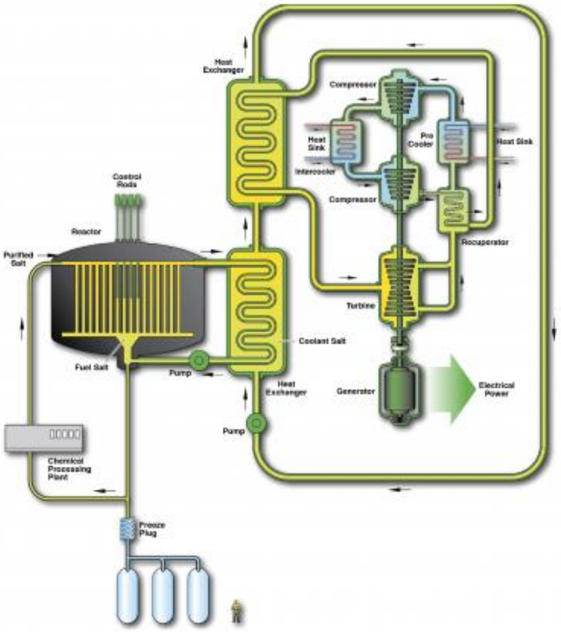

Figure 2-3. Molten Salt Reactor Example[13]

Each reactor has a primary system that consists of a forced molten salt (coolant, which is circulated with a single centrifugal pump that contains liquid fuel, which is pumped through a graphite moderator by a single centrifugal pump). The primary salt then enters a heat exchanger where it will pass off heat to a secondary salt coolant. The secondary salt is forced with one centrifugal pump to a steam generator. The secondary system does not contain any fission products under normal operating conditions. The secondary pump and most of the secondary loop sends heat from the primary system inside of the reactor to the steam generator located outside of containment. The steam generator has superheated steam up to 18 MPa and 560°C[14]. Once sent to the turbine, the steam is condensed through the ultimate heat sink and then is pumped back to the steam generator for reheating.

Each reactor produces 200 MWe from 450 MWth of heat for an approximate efficiency of 44%.[15] High-assay, low-enriched uranium is implemented to extend time between refueling and increase burn-up relative to the existing light water reactor fleet.

The containment structures are located below-grade, with the reactor building partially below-grade for protection against various safety and security events.

2.4. Safety During Abnormal and Emergency Conditions

During a loss of offsite power event, the reactor shuts down via insertion of the safety control rod. In case of a control rod malfunction, defense-in-depth is achieved via passive negative temperature

---

[13] https://www.energy.gov/ne/articles/3-advanced-reactor-systems-watch-2030

[14] Similar to Compact Molten Salt Reactor (Seaborg Technologies, Denmark) IAEA, "Advances in Small Modular Reactor Technology Developments," 2022, pp. 265-268

[15] Similar to FUJI (International Thorium Molten-Salt Forum, Japan) IAEA, "Advances in Small Modular Reactor Technology Developments," 2022, pp. 273-276.

reactivity and coolant/void density feedback to maintain the reactor in a safe condition.[16] No electricity or active operation of components is necessary to cool the reactor sufficiently. In cases of severe temperatures, the freeze plug melts and drains the fuel salt, which halts all fission reactions. These safety features ensure that passive features are sufficient to maintain the plant in a safe shutdown state indefinitely following multiple design basis accident (DBA) conditions. Additionally, the core can be cooled by natural air reactor cooling system (RCS) that will circulate air around the reactor core.

One emergency diesel generator is provided for each reactor core in the plant and there is one emergency backup diesel generator, for a total of three diesel generators onsite. The diesel generators are in the turbine building within the owner-controlled area (OCA). While not necessary for safe cooling of the reactors during loss of power, the diesel generators can provide emergency power for physical security-related equipment, safety-related instrumentation and control (including reactor sensors such as humidity or gas sensors for chemical control), and communications equipment. As long as one diesel generator is functioning for each reactor, the generators can provide power to security and sensing equipment for 168 hours (seven continuous days).

---

[16] Based broadly on principles derived from "IAEA Advances in Small Modular Reactor Technology Developments," 2022, pp. 253-288

3. HYPOTHETICAL MSR PHYSICAL PROTECTION SYSTEM DESIGN PROCESS

3.1. PPS Design Process

The PPS design process used for this facility focused primarily on subject matter expert (SME) interviews and tabletop exercises (TTXs). Publicly available information was used to design the reactor facility, the safety systems, and overall plant layout. Figure 3-1 shows the design process that has been used in previous designs and analyses.

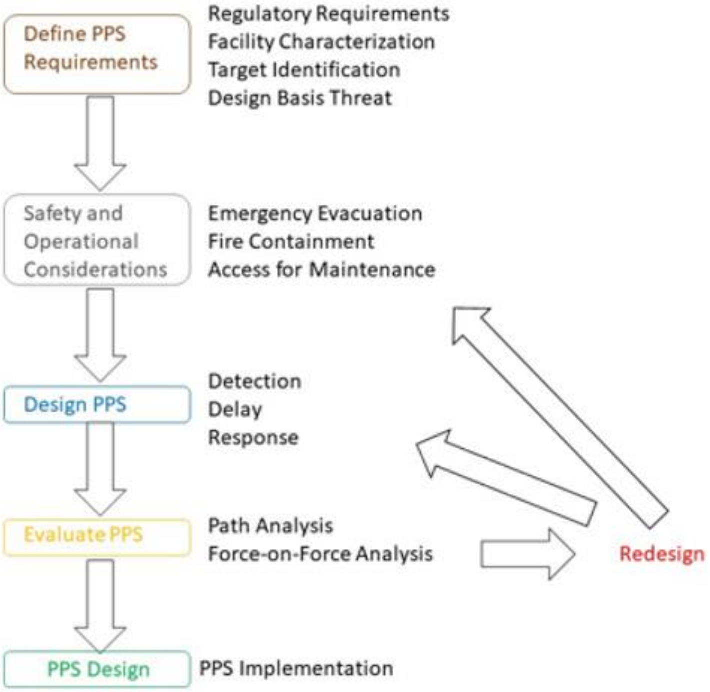

Figure 3-1. Security-by-Design Design and Evaluation Process Outline (DEPO) Approach

The design process utilized for this hypothetical facility and the associated PPS was conducted in the following steps.

1. Design of the reactors and associated safety systems
2. Design building and site layout
3. Develop initial PPS
4. Analyze initial PPS
5. Redesign and reconfiguration of the PPS

The initial steps in the design process were to design the reactor, the reactor safety systems, and the operational and control systems necessary for the reactor. Because this facility is hypothetical, there is less detailed information on this section of the design process. However, SMR designers should consider how the design of the reactor, safety systems, and operational systems may impact the design of the PPS. For example, in this design, the reactor core was designed to be below-grade with access points to maintenance areas further below-grade. By having the reactor and maintenance areas below-grade, the PPS can be designed with a defense-in-depth approach to require the adversaries to bypass multiple lines of detection and delay, and creates opportunities for the response force to engage the adversaries. Additionally, the spent fuel storage area was designed to be below-grade in the facility as well. By placing the spent fuel below-grade, the site can minimize the amount of equipment and line-of-sight obstructions for the response force on site. This design choice should consider the amount of spent fuel being generated by the facility, the required space needed to store fuel long-term, and if there is potential to expand the storage area. This approach allowed the active fuel, safety systems, reactor control room, and spent fuel to be secured and protected by all the detection, delay and response layers at the site.

The second step in the design process was an initial design of the building layout around the safety systems and operational systems. Previous hypothetical facility designs had separate buildings and a single building with various shape sizes. The figure below shows a previous hypothetical design that considered one external building structure.

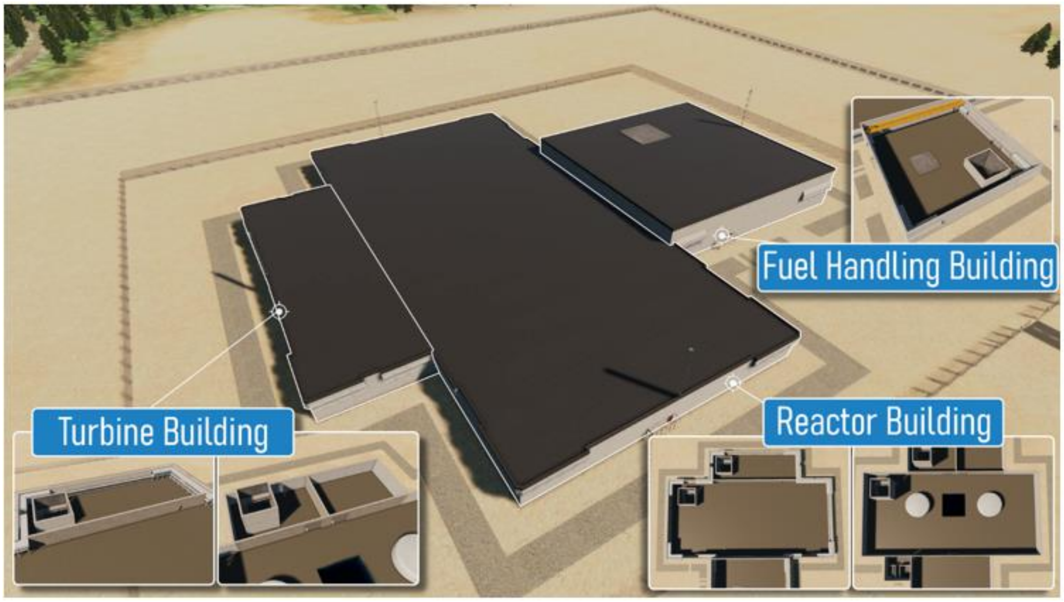

Figure 3-2. Hypothetical Sodium Fast Reactor (Single Building)[17]

For the hypothetical Sodium Fast Reactor (SFR), the PPS was designed to minimize access to the reactors, the safety systems, and the spent fuel storage located below-grade. When the PPS was analyzed against a hypothetical adversary force, the shape of the building created some issues for the response force to engage the adversary force; the responders were unable to see the entire protected area from their positions. Because the reactor building in the center of the site is wider than the other buildings, the PPS had to be redesigned and reevaluated to consider a different response force strategy. As can be seen from Figure 2-2, this hypothetical facility was designed to have a continuous square footprint to aid the response force visualization and potentially allow for a higher effectiveness with a smaller response force and overall PPS staffing headcount. During the site layout and building design phase, it is important to consider the regulatory requirements that may drive the decisions for building design and site layout. During this phase, the target identification process and vital areas identification process were conducted to identify the targets and vital areas that need to be protected to meet regulatory requirements. Additionally, during the building design and site layout phase, emergency evacuation requirements should also be considered. Emergency

---

[17] “U.S. Domestic Sodium Fast Reactor: Security-by-Design.” Evans, et.al. Sandia National Laboratories. SAND2023-09146R.

exit requirements can have an impact on potential access points for an adversary team and must be secured by the PPS. It is important for the facility designers to identify where these locations may best be placed to aid in evacuations and to not hamper the effectiveness of the PPS. Finally, during the design phase of the site layout and site building, the DBT capabilities should also be considered. If construction materials and multiple access points can be designed into the buildings or site to increase the delay time or increase the amount of explosives the adversary must use before getting to the target, this will deteriorate their capability to complete an act of sabotage at the facility.

It should be noted that the initial PPS design was integrated into the building design and site layout. To develop the initial building and site layout and the initial PPS design, a 3D model of the facility was developed in Scribe3D. A group of SMEs used the 3D model to make changes to the facility design and design the initial PPS. During this phase, the PPS design is developed through a form of TTXs. To conduct these TTXs, the hypothetical DBT is used and the group of SMEs acts as an adversary team, or red team, to identify the potential adversary attack scenarios that a credible adversary would consider. As these adversary attack plans are being created and modeled, the SMEs developed PPS features and response strategies to counter the adversary attack scenarios being developed. While going through this process, it is important that the SMEs and the team developing the PPS design also consider the cost of each PPS measure being deployed. The team of SMEs working on this hypothetical facility evaluated the cost measures based on the following factors:

1. Initial feature cost
2. Sustainability and maintenance cost
3. Feature ability to reduce total PPS staffing headcount

By evaluating the above three factors, the team of SMEs identified features and procedures that could mitigate many of the adversary attack scenarios that had low initial feature cost, low sustainability and maintenance costs, and could lead to a reduced total PPS staffing headcount. This process was used to develop the initial PPS design that was then evaluated in multiple TTXs.

NOTE: During these TTXs, it is important for the SMEs to consider credible attack scenarios, utilize the DBT, and that the SMEs have experience in TTXs, force-on-force exercises, or adversary attack planning.

Once the initial site layout and PPS design were developed, the PPS was analyzed using the tabletop feature of Scribe3D. Each adversary scenario developed by the SME team was analyzed using the range of hypothetical adversary capabilities. During the PPS analysis process, it is important that all assumptions used are documented and the results of key interactions between the adversary and the PPS and the adversary and the response force are noted and detailed. Detailed notes and interactions are important to identify the results of scenarios and where or why certain changes may be needed for the PPS or response force strategy.

Once the analysis has been completed, the PPS may be redesigned or reconfigured to improve the PPS against the defined adversary attack scenarios that have been developed by the SMEs. The redesign should use a similar approach to the process identified above, considering both cost and impact to improving the PPS. Figure 3-3 below outlines the updated design methodology that was used for this hypothetical facility.

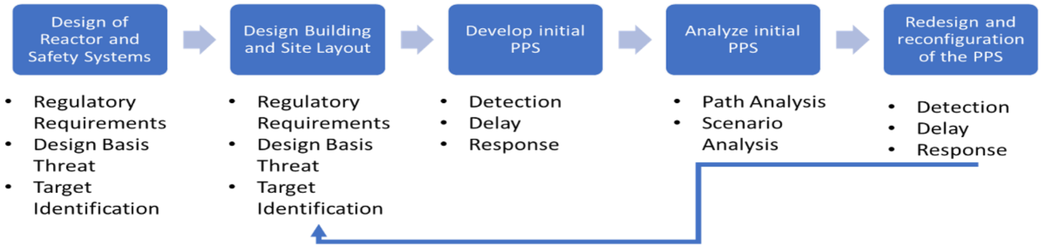

Figure 3-3. Hypothetical SMR and PPS Design Process

3.1.1. Hypothetical Facility Target Identification

The target identification process used for this hypothetical facility was not a holistic target identification process. Many resources exist for conducting target identification and vital area identification[18]. The targets chosen to protect for this facility were those that could cause a potential release of radiological material to the environment and targets that are commonly considered as vital areas, such as the control room and central alarm station (CAS).

The targets that will be protected are highlighted in Table 3-1.

Table 3-1. Targets at the SFR Facility

Target	Location
Reactor 1	Below-Grade Reactor Building
Reactor 2	Below-Grade Reactor Building
Spent Fuel Pool	Below-Grade Reactor Building
Reactor Primary Coolant System	Below-Grade Reactor Building
Central Alarm Station	Below-Grade Reactor Building
Control Room	Below-Grade Reactor Building

3.1.2. Hypothetical Facility Design Basis Threat

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), and an open-source hypothetical DBT. The adversary team members were assumed to have the following characteristics:

- Adversary group size of 4-8 individuals

---

[18] "Vital Area Identification for U.S. Nuclear Regulatory Commission Nuclear Power Reactor Licensees and New Reactor Applicants." G. Bruce Varnado. Donnie W. Whitehead. Sandia National Laboratories. SAND2008-5644.

- Ability to conduct a determined violent external assault
    - Attack by stealth or deceptive actions
    - Operate in groups through a single-entry point
    - Have multiple groups attacking through multiple entries
- Military training and skills, willing to kill or be killed, enough knowledge to identify specific equipment or locations necessary for a successful attack
- Information/access from an active or passive insider
- Land or water vehicles, which could be used for transporting personnel and their hand-carried equipment to the proximity of vital areas
- Land vehicle bomb assault, which may be coordinated with an external assault
- Ability to conduct a cyber-attack
- Ability to perform any of the tasks needed to steal or sabotage critical assets
- Armed with a 7.62-mm rifle or 7.62-mm; a pistol; ammunition; grenades; satchel charges containing bulk high explosives, not to exceed 10 kg total; detonators; bolt cutters; and miscellaneous other tools[19]
- Each able to carry a man-portable total load of 29.5 kg [65 lb.]
- Assumed run speed of 3 m/s

---

[19] 10 Code of Federal Regulations Part 73 "Physical Protection of Plants and Materials," https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/full-text.html

4. HYPOTHETICAL FACILITY PHYSICAL PROTECTION SYSTEM DESIGN

4.1. Protected Area

The PA boundary around the hypothetical facility is designed similarly to a traditional perimeter intrusion detection and assessment system (PIDAS). The perimeter consists of one primary vehicle ECP and one personnel ECP.

4.1.1. Protected Area Boundary

In the original case, the facility perimeter is designed to use a PIDAS that is comprised of:

- Two fence lines
    - Outer nuisance fence
    - Inner fence
- An isolation zone
    - 20-ft wide isolation zone
    - Microwave sensors
    - Closed-circuit television cameras (CCTVs) equipped for both light and dark environments

Figure 4-1 shows the design of the PIDAS. The isolation zone is equipped with microwave sensors around the entire perimeter of the facility. On the ground, bistatic microwave sensors are deployed and the roof is protected by a monostatic microwave sensor. Additionally, the perimeter of the facility is equipped with CCTV cameras. The figures below highlight the microwave sensors and CCTV cameras.

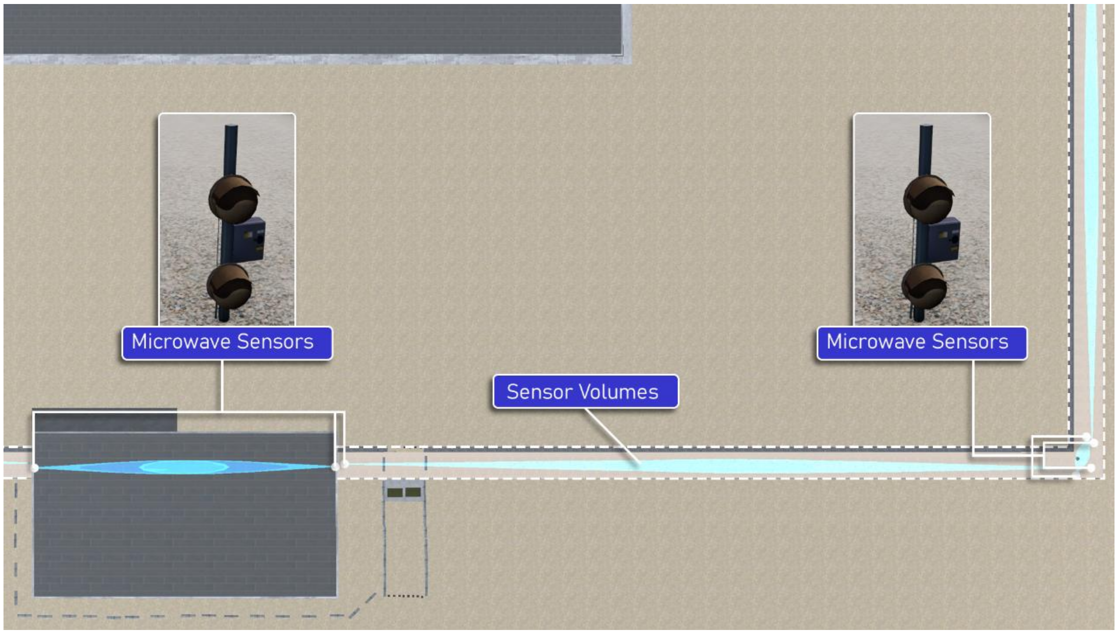

Figure 4-1. Perimeter Microwave Sensors

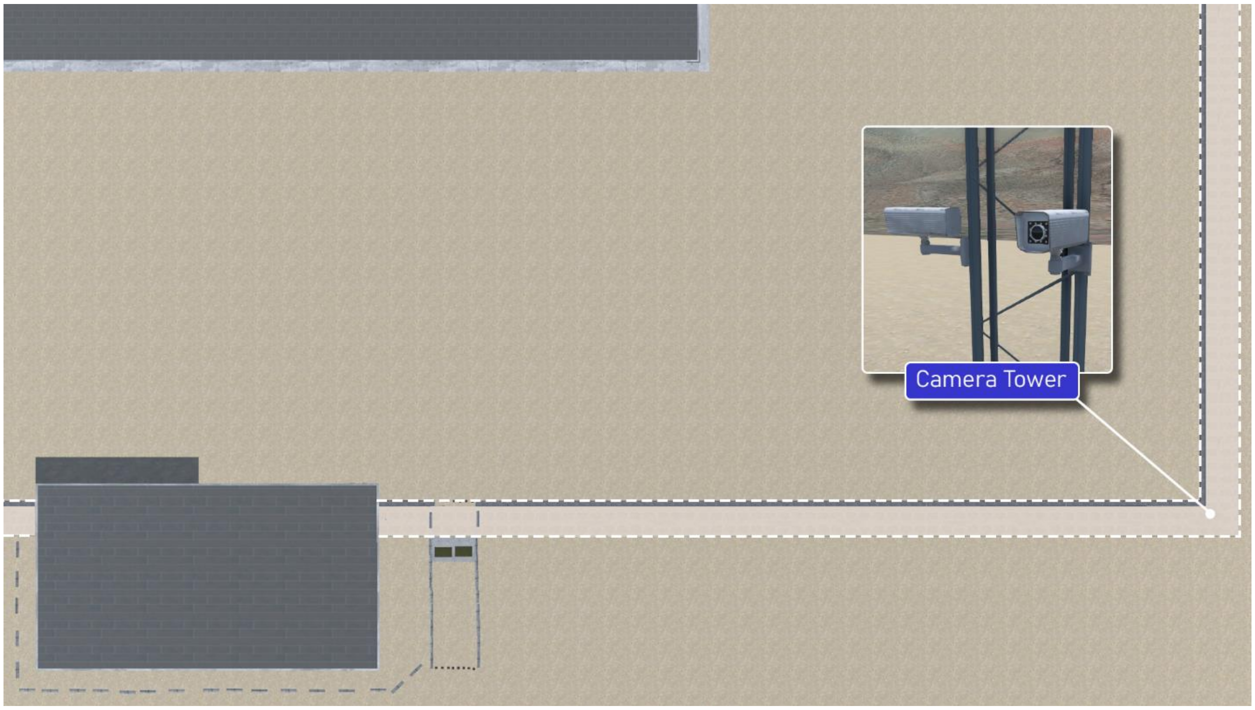

Figure 4-2. Perimeter CCTV Cameras

The inner fence of the PIDAS is designed as a combination of vehicle barrier and turbine grating, which functions as the PA boundary. The base of the PA boundary is a modular block wall; the top is turbine grating. The turbine grating provides some inherent resilience to explosive breaches and can increase the adversary task time of penetrating the inner fence with hand tools or power tools. The modular block wall that forms the base of the inner fence is designed to be 4 feet tall and the turbine grating extends another 8 feet above the top of the modular block wall. This allows the inner fence to be a total of 12 feet tall around the entire perimeter of the facility. Figure 4-3 shows the design of the inner fence line and vehicle barrier system (VBS).

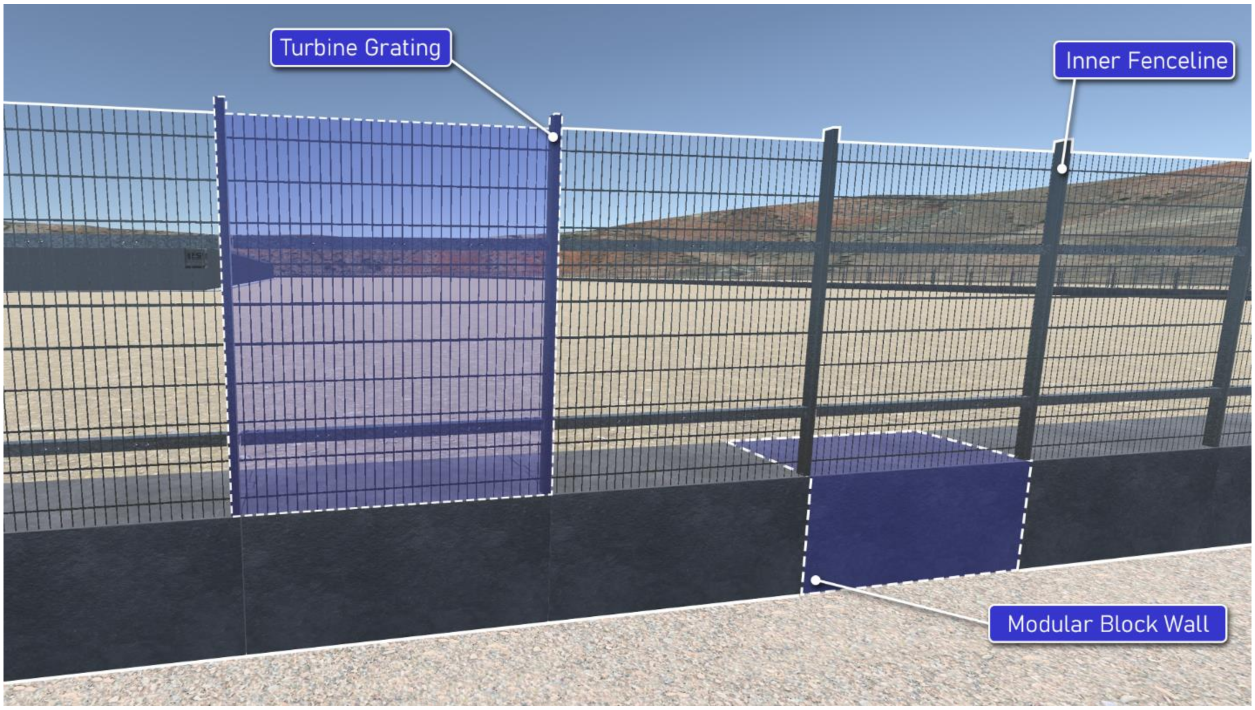

Figure 4-3. Inner Fence and Vehicle Barrier System

4.1.2. Protected Area Entry Control Point

There is one primary ECP for both vehicles and personnel into the PA. The site also has an emergency vehicle ECP, in the event the primary vehicle ECP is compromised. The site only operates one personnel ECP.

4.1.2.1. Personnel Entry Control Point

The personnel ECP is equipped with contraband detection as well as intrusion detection technologies. The personnel ECP has three search lanes. Two of the search lanes will be used at all times and monitored by two armed guards. The third lane is a redundant lane to handle an influx of personnel or when the other two search lanes are not operational to ensure all personnel can enter the site. The personnel ECP is also staffed by the last access control officer who is armed. The last access control officer is responsible for locking down the PA ECPs (to include the personnel and vehicle ECPs) in the case of an emergency or security event. The last access control officer is positioned in a BBRE to ensure this goal can be accomplished. The ECP is equipped with metal detectors for personnel searches and X-ray machines to search bags and packages coming into the PA. The current fleet of NPPs in the U.S. also deploys explosive vapor detection machines that are meant to detect explosive residue on individuals entering the PA. For this design, explosive vapor detectors were not considered as part of the contraband detection process for entrance into the PA.

The personnel ECP is equipped with PIR sensors and CCTV cameras. During shift changes, the PIRs in the ECP are placed into access mode to decrease the number of alarms entering the CAS. The CCTV cameras in the personnel ECP are meant to record all access into the PA and allow the shift supervisor to provide additional surveillance of the ECP search process.

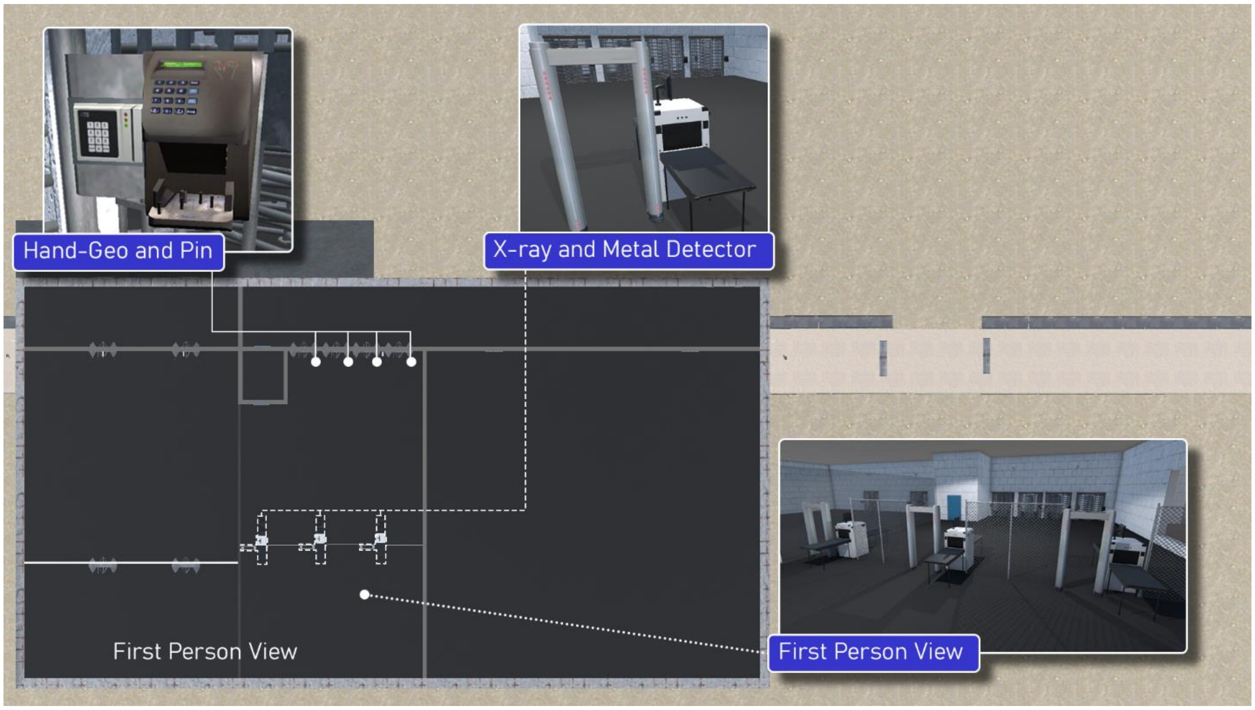

Figure 4-4. Personnel Entry Control Point

4.1.2.2. Vehicle Entry Control Point

The vehicle ECP is designed to form a vehicle trap for any authorized vehicles coming to the site. The outer layer of the trap contains hydraulic pop-up bollards and the inner layer is formed by hydraulic wedge barriers. Modular blocks are used to guide the vehicle into the vehicle trap and are positioned around the personnel ECP to protect the buildings from adversaries that may drive a vehicle directly into the ECP.

When a vehicle arrives at the site, the outer pop-up bollards will be lowered to allow the vehicle into the trap. The pop-up bollards and the hydraulic wedge barriers are designed with controls that do not allow both barriers to be opened at the same time. Once the vehicle enters the vehicle trap the driver and any passengers must process through the contraband detection search in the personnel ECP. Once the drivers and passengers of the vehicle are searched, they will proceed back to the vehicle with two armed guards to conduct a search of the vehicle. Once the vehicle, driver, and passengers have been searched, the vehicle will be allowed to enter the PA. Upon entering the PA, the vehicle will be escorted by two armed guards and the vehicle path will additionally be monitored by responders in elevated positions. Figure 4-5 shows the vehicle ECP for the hypothetical facility.

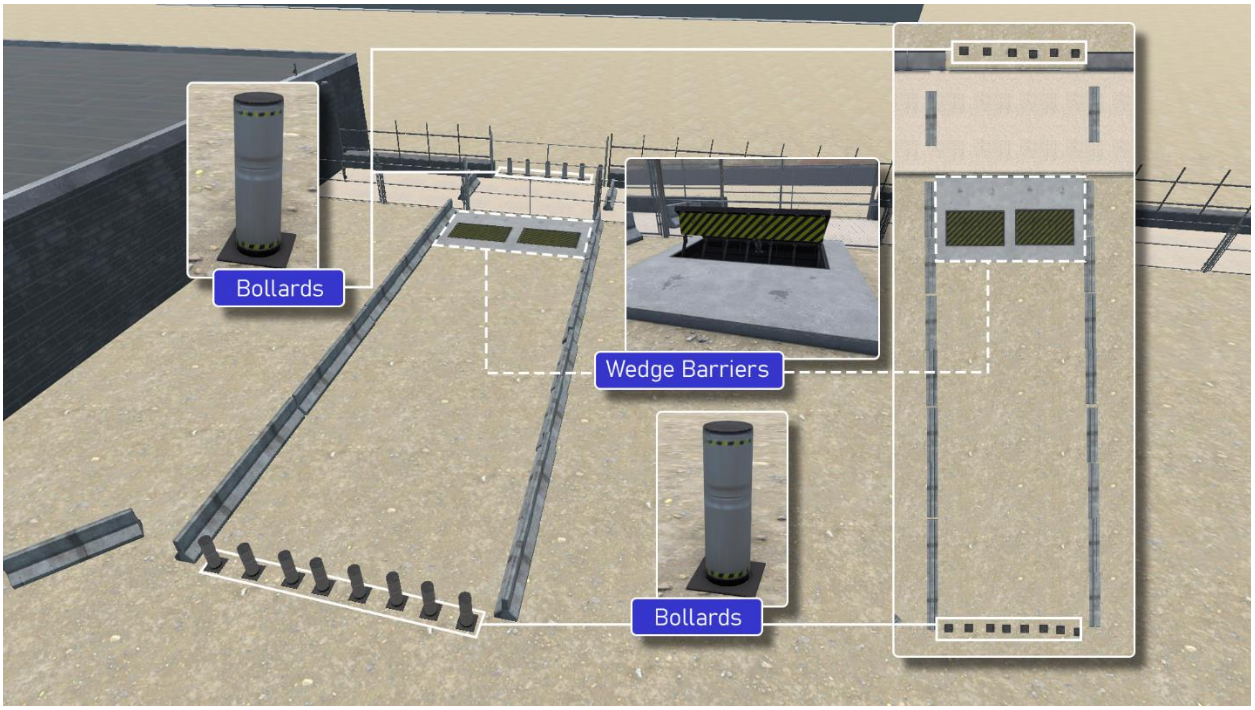

Figure 4-5. Vehicle Entry Control Point

4.2. Reactor Building Personnel Entry Points

There are two entry/exit points from the reactor building. Each of the reactor building entrances are protected by shark cages. The shark cages are made of turbine grating and because of the open-air nature of the shark cages, a large explosive charge is required to forcefully breach into the shark cage. This additional delay barrier forces the adversary to spend more time on the exterior portion of the building, exposing them to response force fire without cover. The exterior portion of the shark cage is protected by a cypher lock and to open the door to the reactor building, a proximity badge and a correct personal identification number (PIN) must be used to enter the building. The shark cages are protected by vehicle barriers to prevent vehicles from destroying the shark cages. The vehicle barriers around the shark cages were designed because of the TTXs and discussion related to insider threats, vehicle access and vehicle parking in the PA. If a vehicle is left in the PA with the keys still in the vehicle, the adversaries could gain access to the vehicle and destroy the shark cage and provide a form of cover for the adversaries to breach into the facility.

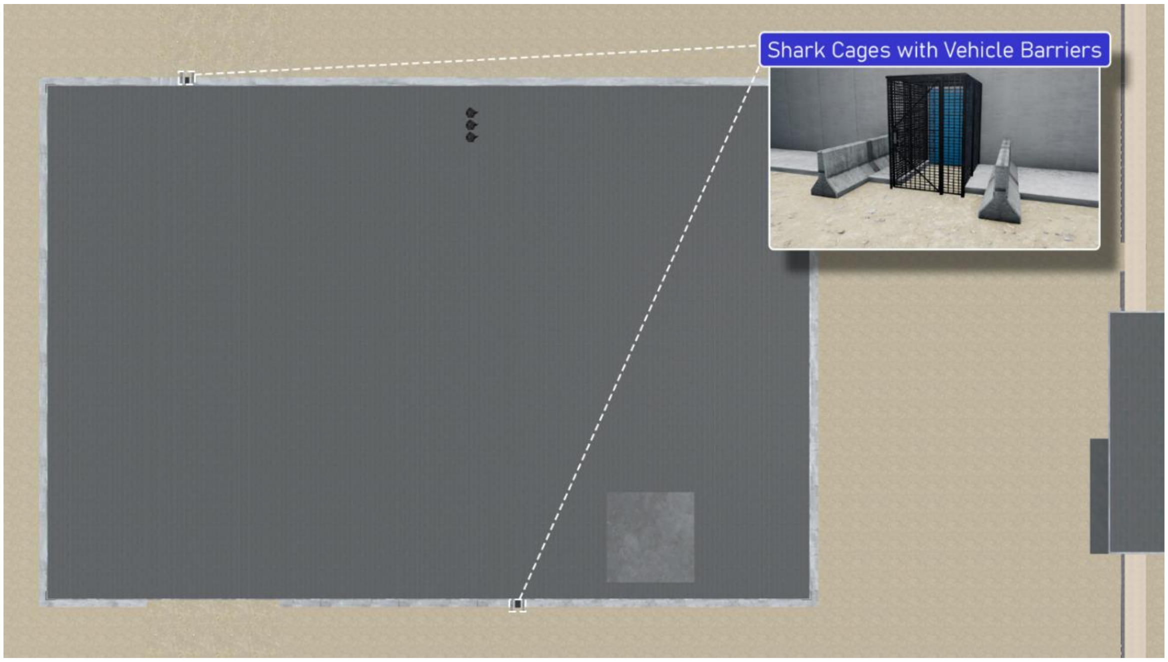

Figure 4-6. Reactor Building Entry Points

4.3. Vital Areas

Four targets were analyzed in the design of the PPS: the CAS, control room, reactors, and spent fuel storage. During the design phase, the team configured the building in such a layout that only two vital area access points were developed and require protection to meet the requirements related to access control, detection, and assessment. Each individual area is equipped with access control devices but to reduce the burden on random searches and checks of vital area barriers, only two vital areas were considered in the design process.

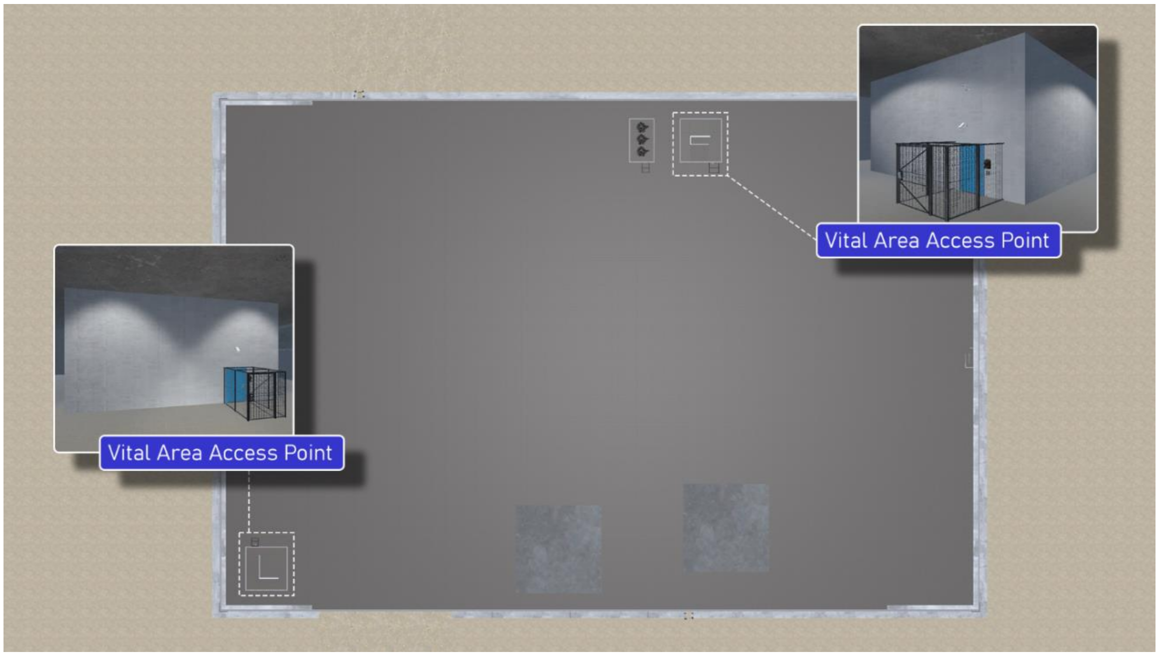

Figure 4-7. Vital Area Access Points

Figure 4-7 shows the two personnel vital area access points. The other vital area access points are the equipment hatches that are used to move fresh fuel into the reactor portion of the facility and move equipment into the secondary and energy conversion portion of the facility. These equipment hatches are always locked and can only be opened from the reactor control room. To move the equipment hatches, the reactor control room operator must contact the CAS and the CAS can unlock the equipment hatch for the reactor control room to open the equipment hatches.

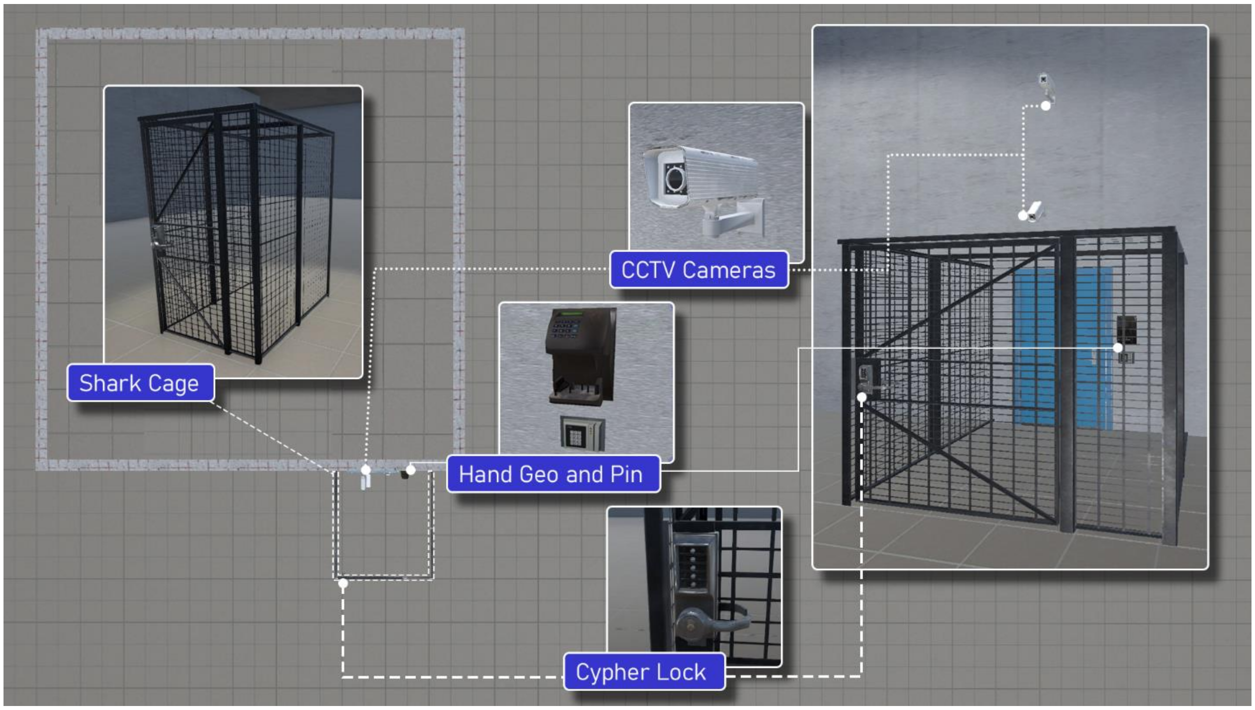

Figure 4-8. Vital Area PPS Equipment

Figure 4-8 shows the PPS equipment that is applied to protect the vital area entry points for personnel. To access the vital areas, a shark cage surrounds the door entrances. The shark cages are made of turbine grating, and because of the open-air nature of the shark cages, a large explosive charge is required to forcefully breach into the shark cage. The shark cage must be entered using a cypher lock that only the responders and PPS security personnel know. Once passing through the shark cage, the individual is seen on the CCTV camera. To enter the stairwell, any individual can only pass through once they use the hand geometry reader, use their badge on the proximity reader, and enter their PIN.

4.3.1. Central Alarm Station

The CAS and control room are both located in the below-grade portion of the building. Additionally, inside of the CAS area is the server room that also has an uninterruptable power supply (UPS) that is meant to handle the transition to diesel generator power in the case of the loss of offsite power.

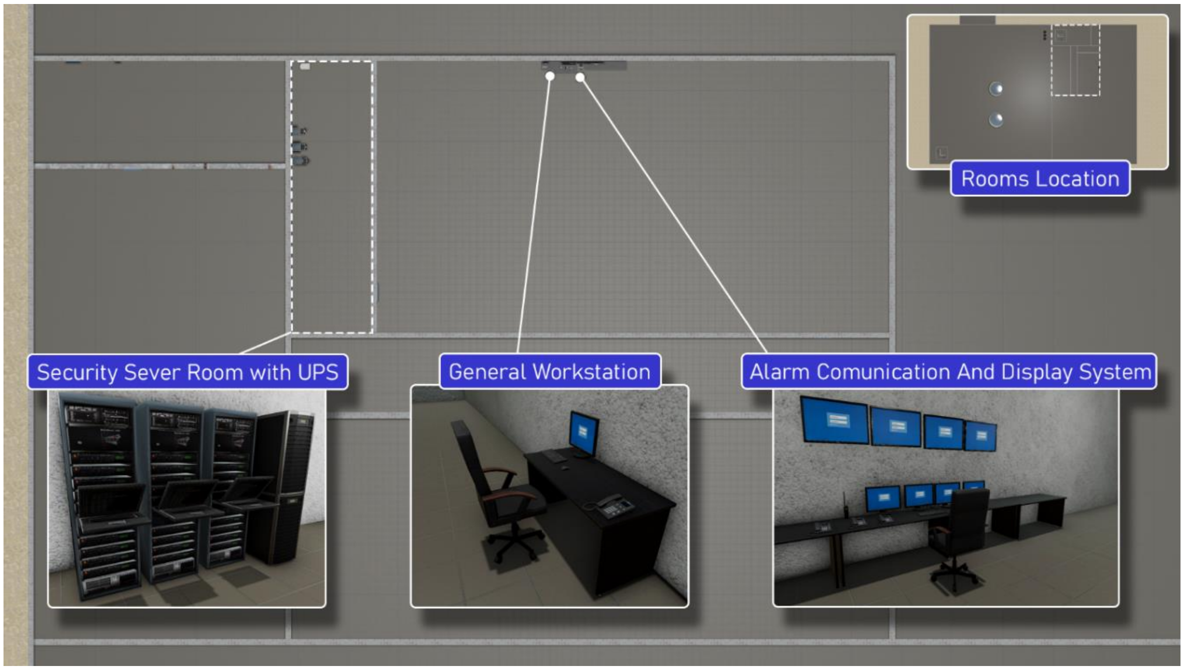

Figure 4-9. General CAS and Server Room Layout

The CAS alarm communication and display (AC&D) system is equipped with four monitors (see Figure 4-10). The four monitors on top are used for CCTV assessment in frequent areas of access, such as the personnel ECP, the vehicle ECP, and the vital area access points. The bottom four monitors are used to visualize the overall site map, a drilldown map for individual areas and buildings, an access control log, and any other areas of interest for the CAS operator. Additionally, there is a general workstation that can be used to submit timecards, answer emails, etc. The general workstation is on the general corporate network (not the security network) to access company sites and emails.

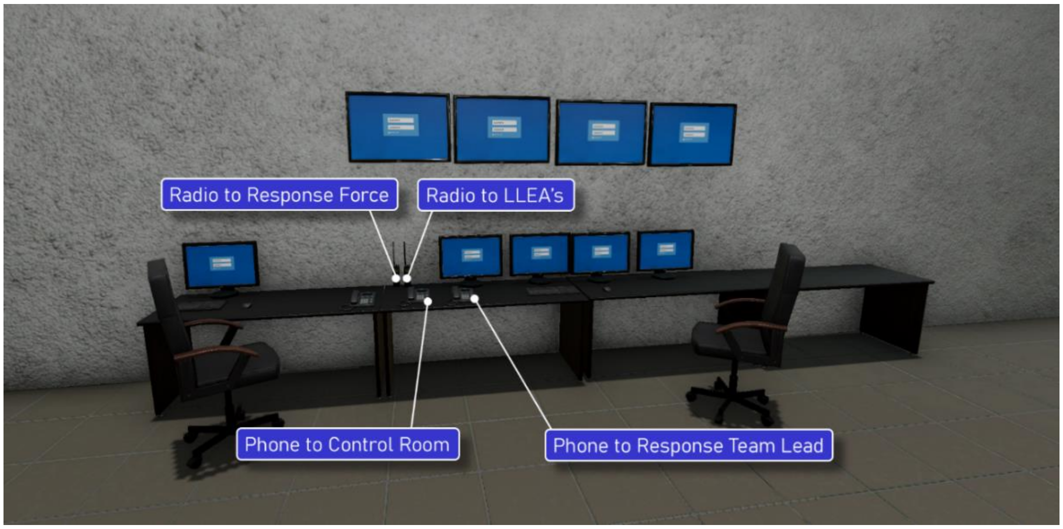

Figure 4-10 CAS AC&D System and Communication Devices

The CAS is equipped with three direct phones to communicate to the response team lead (RTL), the control room, and to offsite local law enforcement agencies (LLEAs). The CAS is also equipped with a radio to communicate to onsite responders and LLEAs, if necessary. All forms of communication are two-way and encrypted.

4.3.2. Reactors and Spent Fuel Storage

4.4. PPS Positions

The figures below show the security staffing positions that are designed into this PPS. Above-grade, there are four responders located in BBREs. From their positions, the responders can provide surveillance of the PA boundary around the site. Additionally, the responders can provide compensatory measures by maintaining surveillance around the PA if power is lost to the PA or if the microwave sensors and cameras in the PA fail to perform their function. Responder 2 and responder 3 can move across a shared facility wall to provide more support with both responders being in the same BBRE, and responders 4 and 1 have the same ability on their side of the facility. At the facility ECP, there are two armed security officers (ASOs) in the personnel ECP to oversee and conduct contraband searches of personnel and to provide vehicle searches into the PA. Additionally, the last access control (LAC) officer is in a BBRE into the PA. This officer is also armed, like the ASOs.

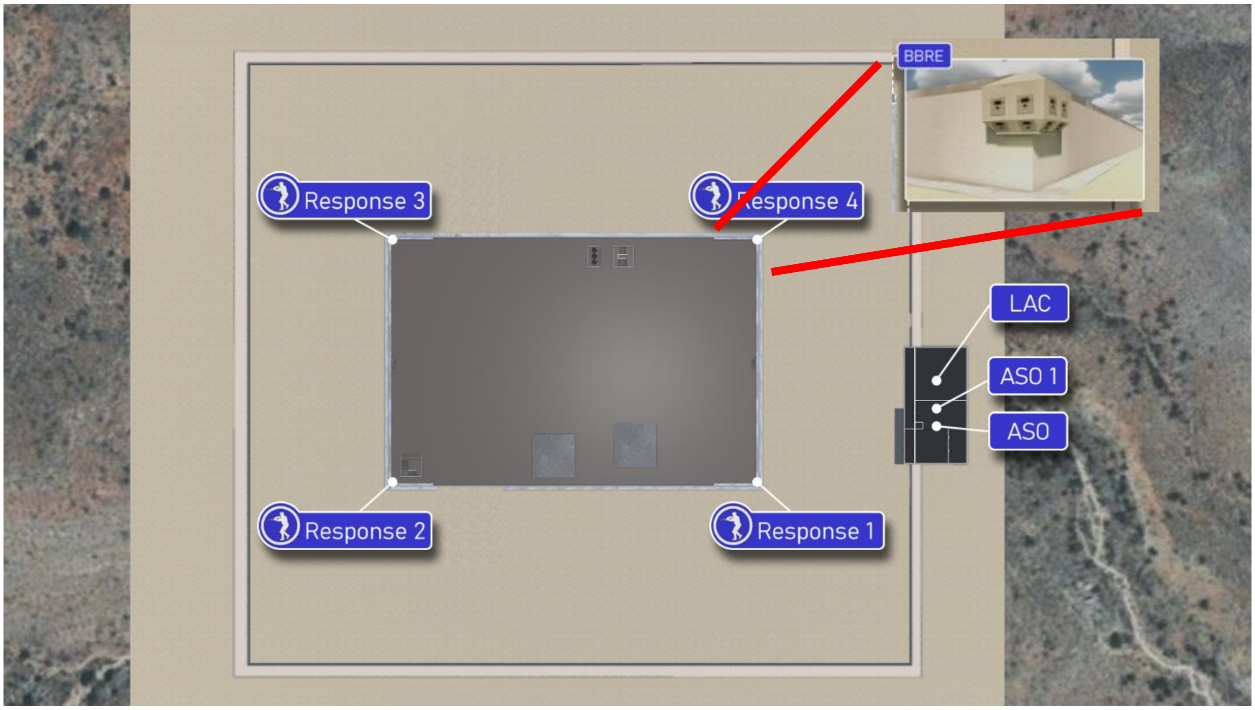

Figure 4-11. Above-Grade Security Positions

Figure 4-12 shows the below-grade PPS security positions. The CAS operator and RTL are located inside the CAS. The security shift supervisor (SSS) and field supervisor (FS) are located outside the CAS.

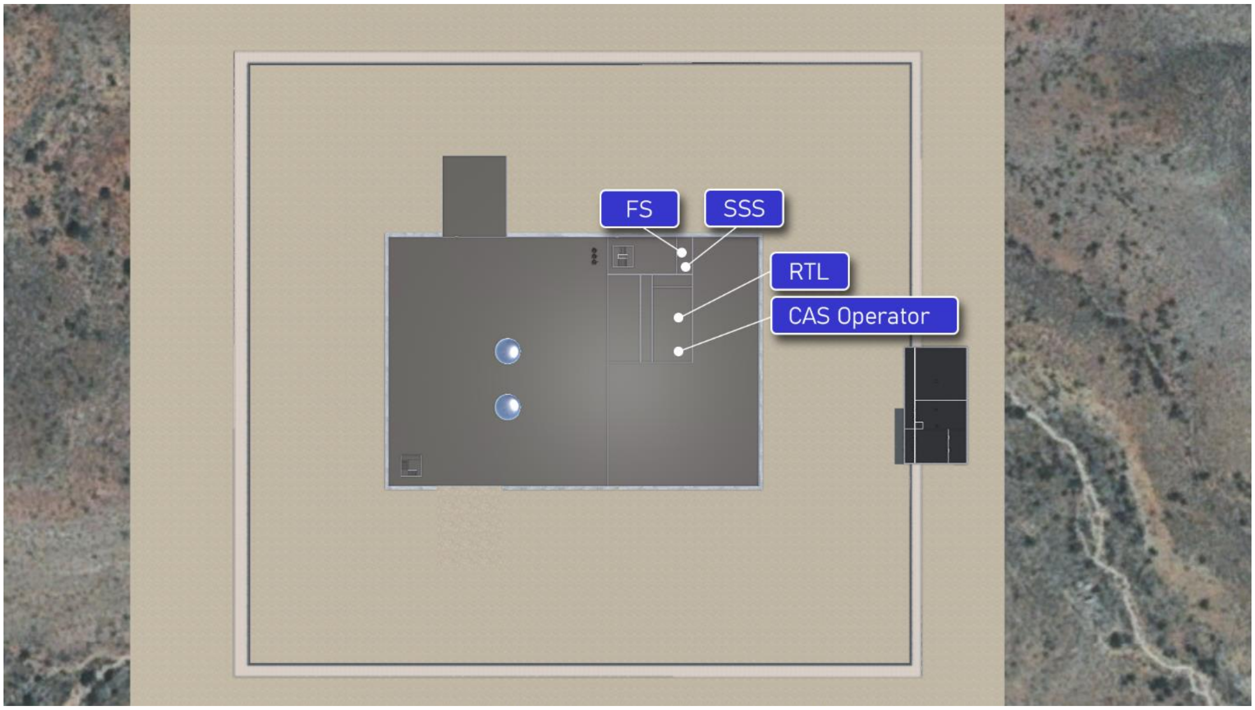

Figure 4-12. Below-Grade Physical Security Positions

Table 4-1. Initial Staffing Headcount

Position	1 Shift	24/7 FTE
Response Team Lead	1	4
Security Shift Superviros	1	4
Field Supervisor	1	4
Last Access Control	1	4
Central Alarm Station Operator	1	4
Armed Security Officer	2	8
Responders	4	16
Total	**11**	**44**

5. PPS ANALYSIS

The analysis process consisted of using three TTX scenarios developed by the SME team and conducting more detailed TTXs using the probability of hit and probability of kill (PH/PK) data within Scribe3D. Each scenario was analyzed using an adversary force ranging from four to eight individuals. Many assumptions were used in developing the adversary attack scenarios and in analyzing the engagements between the response force and the adversary for all three scenarios. These assumptions include:

1. Adversaries and responders are equipped with body armor and helmets
2. The response force could not begin engagement until the adversary team breached the inner fence (i.e., the PA boundary)
3. In each engagement scenario, the following information was used as part of the engagement analysis:
    a. The time between shots was considered to be 0.33 seconds (considering semi-automatic weapons for the responders and adversaries)
    b. The target switch delay was considered to be 1 second (this is the time it takes for an individual to stop engaging one individual and begin engaging another individual)
    c. Each individual is limited to a maximum of shooting 30 rounds at any target they are engaging (simulating magazine capacity limits)
    d. Each critical engagement was simulated 1,000 times to achieve a statistically significant number of simulations
4. The final probability of neutralization reported is the cumulative probability of response force success based on the number of engagements analyzed in the simulations. The equation below shows how this number was calculated:

$$P_N = 1 - \left(\left(1 - \frac{N_{Bwins1}}{1000}\right) * \left(1 - \frac{N_{Bwins2}}{1000}\right)\right) * \left(1 - \frac{N_{Bwinsn}}{1000}\right))$$

In the equation above, P_N is the probability of neutralization, N_{Bwins1} is the number of blue wins in the first engagement, N_{Bwins2} is the number of blue wins in the second engagement, and N_{Bwinsn} is the number of blue wins in the final engagement of the scenario.

Note: Scribe3D is not a neutralization analysis tool. The probability of neutralization here is meant to be a summary of how well the response faired against pre-defined adversary attacks using a tabletop methodology.

5.1. Scenario One: Adversaries Attacking in One Group from the East

In attack scenario one, the adversary team attacks the facility from the south side as one group. The adversary team attempts to breach the facility by penetrating the outer fence line, proceeding to breach the inner fence line, and then penetrating the reactor building above-grade. To enter the above-grade portion of the reactor building, the adversary force must first accomplish a breach of the shark cages that surround the exterior doors into the reactor building. Once entering the reactor building, the adversary team will try to breach the doorway to the below-grade portion of the reactor building through the vital area ECP. Again, this will require them to breach through a shark cage, the doorway and then enter into the area where the reactors are located. Figure 5-1 shows the above-grade portion of the adversary attack on the facility.

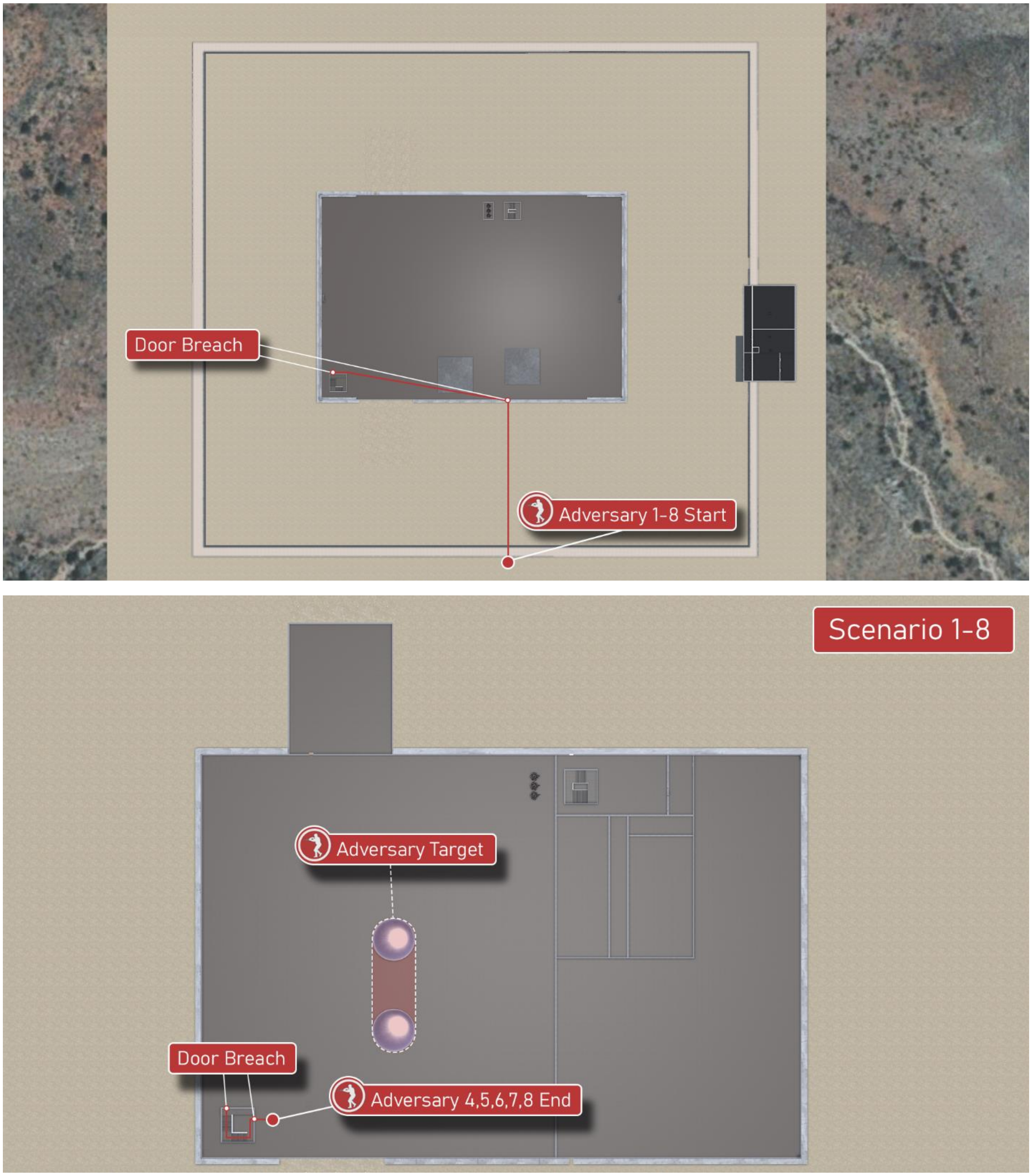

Figure 5-1. Adversary Attack Scenario One

In attack scenario one with a team of eight adversaries, there are three key engagements that involve the response force and adversary force. The first engagement occurs between eight members of the adversary force and responders 1 and 2 on the east side of the facility. In the first engagement, the adversary force is given the advantage by allowing them to engage with the two responders first.

This advantage is given to the adversary using the assumption that the response force cannot engage the adversary until they breach the PA boundary. In the engagement, the response force is in protected BBREs; to afford them credit in these scenarios, the adversary force could only see the responder's heads and engage their heads.

Table 5-1. Scenario One Results

Number of Adversaries	Engagement Number	Number of Adversaries in Engagement	Number of Responders in Engagement	Blue Wins	Red Wins	Internal Or External Engagement	Cumulative Probability of Neutralization (%)
8	1	8	2	64	936	External	92
	2	6	2	924	76	Internal	
7	1	7	2	575	425	External	99
	2	2	2	999	1	Internal	
6	1	6	2	554	446	External	99
	2	3	2	997	3	Internal	
5	1	5	2	768	214	External	99
	2	3	2	996	4	Internal	
4	1	4	2	946	54	External	94

In the analysis above, the first engagement occurs between responders 1 and 2 external to the facility. In engagement two, responders 3 and 4 engage adversaries on the above-grade floor of the reactor building. Because the first engagement with responders 1 and 2 did not have numbers of blue wins (>900 wins), the second engagement was analyzed in most scenarios to ensure that a holistic analysis of the representative adversary attack scenario that was developed. In most scenarios, the largest number of blue forces killed in action was two responders. In these scenarios, responders 1 and 2 were neutralized. Before responders 1 and 2 were neutralized, they were able to neutralize at least two adversaries in every scenario. In order for the adversary or red team to be successful, they must survive both engagements and make their way below-grade. Because of this even though in some scenarios the red team wins are high in the first engagement they are very low in the second engagement leading to a low likelihood of adversary success. As can be seen above, the response strategy overall is adequate at defending against the DBT and the defined adversary attack scenario.

5.2. Scenario Two: Adversaries Attacking in Two Groups from the North and South

The second adversary attack scenario considered the adversary group operating as two units. The adversary would split into two equal teams and attack the facility simultaneously from the north and the south. Each group starts by breaching the PA perimeter and proceeds to breach the shark cage protecting the building entrance, breach into the reactor building, and then proceed to the below-grade portion of the building to sabotage the reactors or spent-fuel storage locations.

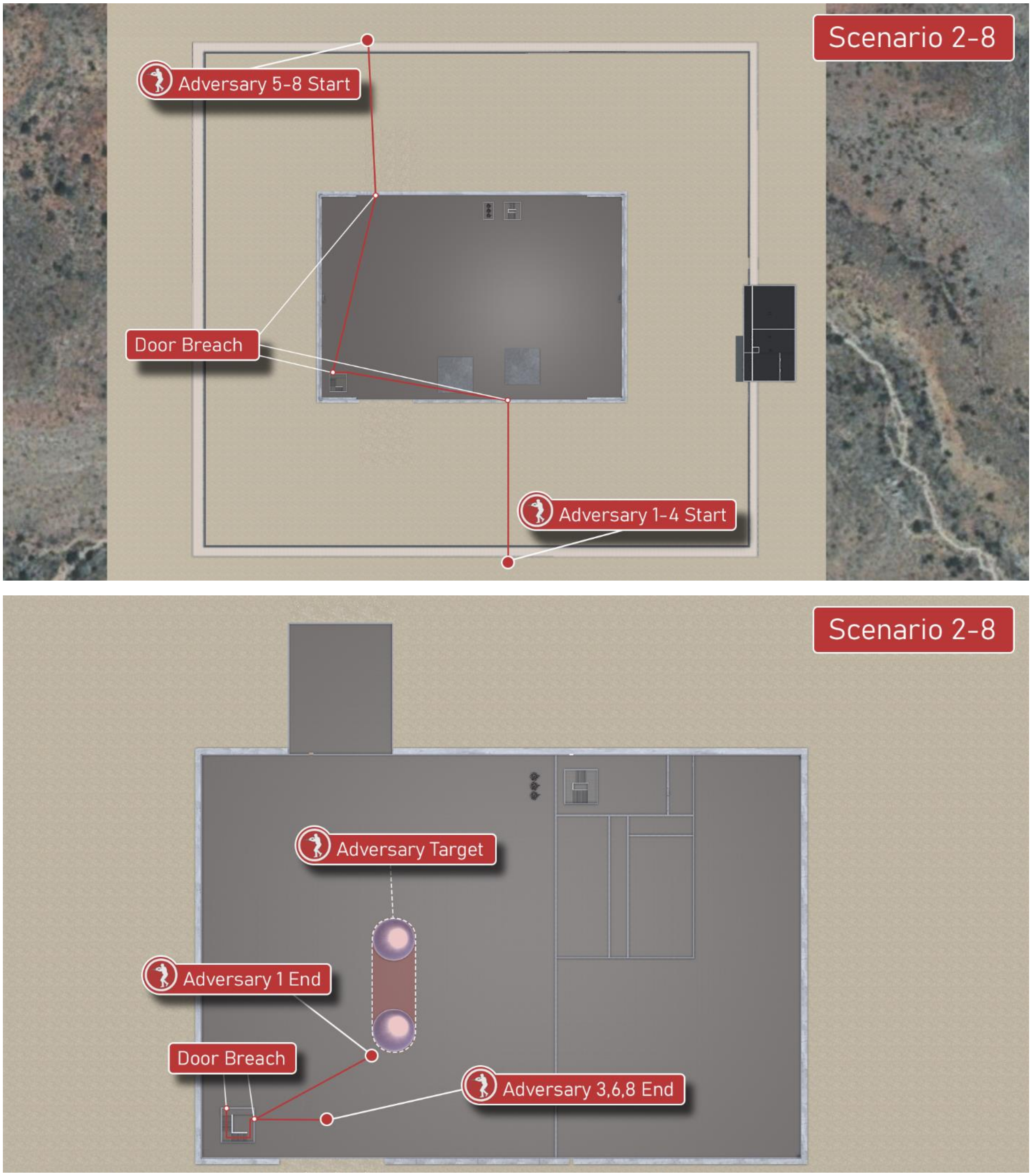

Figure 5-2. Adversary Attack Scenario Two

In the analysis of this adversary attack scenario, the adversaries are given the advantage of being able to engage the response force first. This advantage is given based on potential rules of engagement that limit the response force to engagement only when the PA has been breached. Each engagement in the analysis was analyzed one thousand times.

Table 5-2. Scenario Two Results

Number of Adversaries	Engagement Number	Number of Adversaries in Engagement	Number of Responders in Engagement	Blue Wins	Red Wins	Internal Or External Engagement	Cumulative Probability of Neutralization (%)
8	1	4	2	936	64	External	99
	2	4	2	947	53	External	
7	1	3	2	985	15	External	99
	2	4	2	947	53	External	
6	1	3	2	985	15	External	99
	2	3	2	990	10	External	
5	1	2	2	993	7	External	99
	2	3	2	990	10	External	
4	1	2	2	993	7	External	99
	2	2	2	998	2	External	

From Table 5-2, the PPS design is effective at neutralizing the adversary force in scenario two. The response force strategy and posture are very effective at neutralizing the adversary force due to the protected nature of the BBREs that the responders are positioned in and the long distance that the adversary must cross while being exposed. In this analysis, all external engagements had high success rates for the responders (>900), which resulted in the adversary being neutralized before they could enter the reactor building.

5.3. Scenario Three: Adversaries Attacking in Two Groups from the East and North

In the third scenario, the adversary groups operate in two teams. One team attacks the facility from the north side and one team attacks the facility from the east side. Once inside the perimeter, both teams advance to the personnel door on the north side of the facility to breach into the reactor building. The adversary tactic in this scenario was to occupy more responders and only allow one of the responders to engage the adversary force attacking the facility from the north.

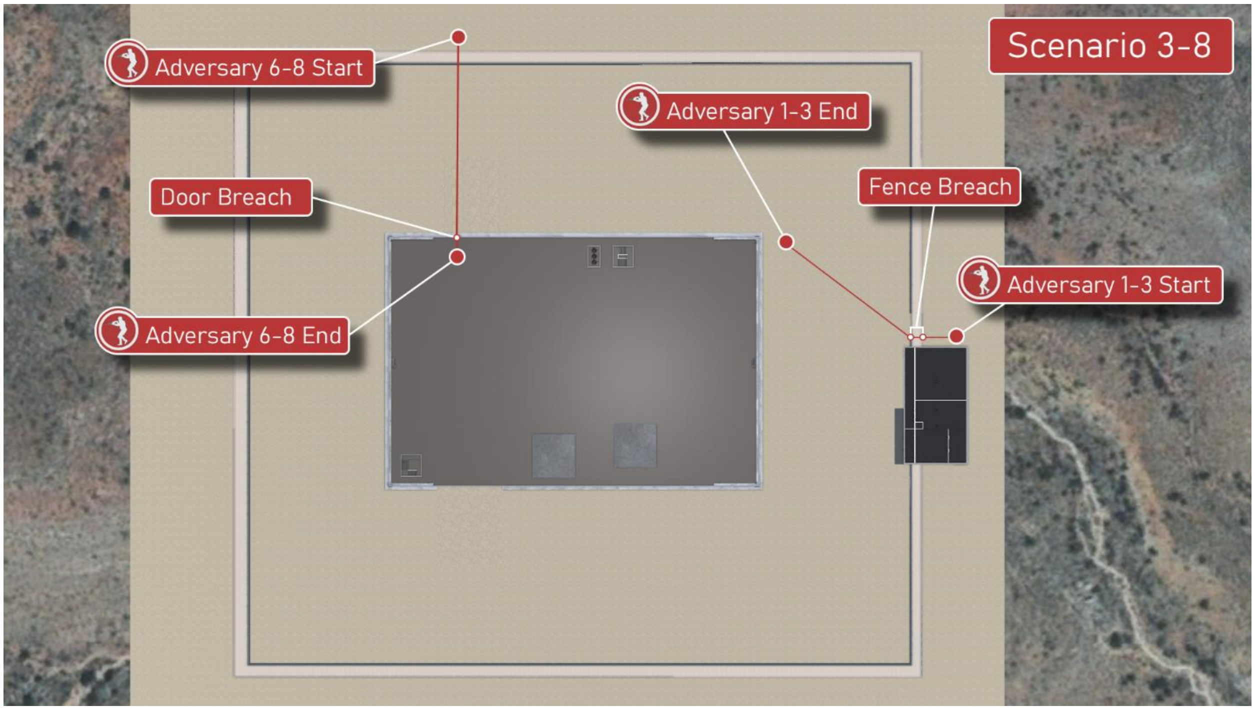

Figure 5-3. Adversary Attack Scenario Three

In this adversary attack scenario with adversary force groups of eight and seven adversaries, there is an engagement between one responder and one adversary. These scenarios consider an adversary that is trying to engage the responder in the southeast corner BBRE to occupy them from engaging with adversaries approaching from the east side of the facility.

Table 5-3. Scenario Three Results

Number of Adversaries	Engagement Number	Number of Adversaries in Engagement	Number of Responders in Engagement	Blue Wins	Red Wins	Internal Or External Engagement	Cumulative Probability of Neutralization (%)
8	1	1	1	923	77	External	99
	2	4	2	874	126	External	
	3	3	2	997	3	External	
7	1	1	1	923	77	External	99
	2	3	2	983	17	External	
	3	3	2	997	3	External	
6	1	3	2	993	17	External	99
	2	3	1	844	156	External	
5	1	2	2	996	4	External	99
	2	3	1	844	156	External	
4	1	2	2	996	4	External	99
	2	2	2	1000	0	External	

As can be seen from Table 5-3, the PPS is very effective at neutralizing the adversary force attacking the facility. The scenarios evaluating eight and seven adversaries do not gain a large advantage with the additional adversary trying to occupy the responder in the southeast corner BBRE. Overall, the PPS design was able to neutralize adversaries before they made entry into the reactor building and provided high confidence in the PPS.

6. CONCLUSIONS AND RECOMMENDATIONS

The design of this PPS has shown to be very effective against various adversary attack scenarios conducted by adversary groups of varying sizes. Additionally, the PPS design shows a reduced total staffing headcount. By utilizing a PPS with a response strategy that allows the response force to engage both internally and externally to the facility, an added layer of defense-in-depth is achieved to respond to nuclear security events. Using multiple delay barriers that force complex adversary breaches while exposed also allows for an increase in response force effectiveness to neutralize the adversary force.

Integrating the PPS design into the original building design and facility operation parameters enabled the facility to be designed in a way that is conducive to security, safety, and facility operations. Finally, integrating the detection, delay, and response subsystems into one cohesive larger system allows for each area to be optimized for cost and leads to a highly effective PPS.

6.1. Further Reducing PPS Staffing Headcounts

One possibility to further reduce PPS staffing headcounts could be to allow the CAS operator to provide the function of last access control. Capabilities for locking the PA ECP for any circumstance can be completed by the CAS operator or by any other officers in the CAS. This capability can be achieved through technical measures applied to the access control system, intrusion detection system, and video management system. This would allow for the reduction of one more person from the overall PPS staffing headcount.

6.2. Design Recommendations

The list below is meant to provide recommendations for PPS designers at MSR and SMR facilities:

9. Using a square building design can allow for a smaller response force to provide effective security to the facility.
    a. Secondary systems and energy production systems should be located within the PA to ensure easier protection of the nuclear facility and reduce the number of buildings that may impact line-of-sight and response strategies.
        i. This ensures protection of long-lead items, plant capital equipment, and energy production equipment.
10. Consider methods that allow for force multipliers to reduce the overall security staffing headcount (including responders)
    a. Design delay barriers to channel adversaries into areas where the likelihood the response force can succeed is higher.
    b. Design delay barriers that cause adversaries to expose themselves for longer to increase the likelihood that the response force is successful.
    c. Ensure large standoff distances that force the adversaries to cross open and exposed spaces to increase the likelihood of success for the response force.
    d. Design delay features that require the adversary to use more of their explosive capabilities before reaching target locations.
11. Consider using roof plugs or hatches to allow for large equipment deliveries rather than large roll-up doors

    a. Creates additional delay time and can allow the PPS design to use door placements to channel adversaries into strategic locations

12. Consider the insider threat according to the DBT and capabilities of the insider threat.
13. Keep the PA within the facility clean and clear of obstructions.
    a. This does not require the PPS be evaluated or changed for laydown yards or other things.
14. Limit the number of vehicles in the PA.
    a. No storage of vehicles within the PA.
15. Consider legal and regulatory requirements for use-of-force and rules of engagement.
    a. The response strategy and PPS will need to be tailored to the rules of engagement requirements.
16. Designers should consider multi-modules on site early in the design process
    a. Consider intrusion detection system design for multi-modules as one unit is operational and the next unit is being built
    b. Consider response force strategies to be deployed