Security-by-Design: Light Water Small Modular Reactor

Prepared for
U.S. Department of Energy

Alan Evans, Matt McCullough
Sandia National Laboratories

April 2025
SAND2025-11640R

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-NA0003525.

ABSTRACT

The growing demand for nuclear power is increasing pressure to find solutions to cost prohibitive requirements of both construction and security. Offsite response has been proposed as an option to reduce costs associated with training and maintaining an onsite response force. A previous report explored this option and revealed that security could be provided at the required level, but cost savings was not a result of this methodology.[1] An offsite response strategy required costly active and passive delay barriers to provide sufficient time for responders to muster and deploy to a site in time to interrupt a determined and well-equipped adversary. Also, contrary to the hypothesis, the number of responders required for this strategy exceeded that needed for an onsite response force, as the adversaries could avail themselves of advantageous positions within the facility to repel arriving responders.

This report builds upon the previous evaluation by using the same hypothetical light water small modular reactor (LWSMR) facility model, but this time an onsite response strategy was assessed. The goal of this analysis was to show that an onsite response strategy could be implemented effectively at a cost point that removes barriers within the industry at this critical time of growth and development. The assessment of the facility design and response strategy was completed through modeling using Scribe3D© and subsequent scenario analysis over the course of a two-day tabletop exercise. Subject matter experts in nuclear security, nuclear facility design, and response strategy and tactics contributed to the effort to ensure accurate representation of hypothetical scenarios.

Several adaptations were made to the layout of the LWSMR based on lessons learned during the first day of scenario analysis. The subsequent design evaluated on the second day proved to provide a robust response posture against a large and well-trained adversary force. This report details the process of the analysis and compares the cost of the final facility design with that of the LWSMR model used for evaluation of offsite response. Ultimately, the results of this effort indicate that, when implemented correctly, an onsite response strategy is the best option from a security and cost perspective.

[1] "U.S. Domestic Small Modular Reactor Security by Design." Evans, et. al. Sandia National Laboratories. SAND2021-0768.

This page left blank

Contents

Abstract 3
List of Figures 6
List of Tables 6
Executive Summary 7
Acronyms and Definitions 11
1. Introduction 13
2. Hypothetical Facility 15
   2.1. Original Hypothetical LWSMR Facility 15
      2.1.1. Original Building Descriptions 15
      2.1.2. Reactor Description 16
   2.2. Modified Hypothetical LWSMR Facility 19
      2.2.1. Modified Safety Systems 21
3. Hypothetical LWSMR Physical Protection System Design 25
   3.1. Original Hypothetical PPS Design 25
   3.2. Modified PPS Design 28
   3.3. Hypothetical Design Basis Threat 30
4. Physical Protection System Evaluation 33
   4.1. Original LWSMR Security System Evaluation 33
      4.1.1. Considerations for a PPS Design Utilizing an Offsite Response Force 40
   4.2. Modified LWSMR Security System Evaluation 42
      4.2.1. Attacks On BBRE Facility Layout 43
      4.2.2. Attacks On Gun Port Facility Layout 47
5. Hypothetical PPS Costs and Staffing Headcounts 53
   5.1. Original LWSMR Design 53
   5.2. Modified LWSMR 56
6. Recommendations 61
References 63

LIST OF FIGURES

Figure 1. Original LWSMR Facility Layout....16
Figure 2. Initial PSIT Configuration. 19
Figure 3. Modified LWSMR Facility....20
Figure 4. Modified LWSMR Above-Grade Floor....22
Figure 5. Modified LWSMR Security Floor....23
Figure 6. Modified LWSMR First Below-Grade Floor....23
Figure 7. PIDAS Cross-section....25
Figure 8. Original PPS Design 27
Figure 9. Original PPS Exterior and Interior Intrusion Detection Systems 28
Figure 10. Modified Blisters Design....29
Figure 11. Modified Gunport Design....30
Figure 12. Active Delay, Extended Detection, and Person Traps....35
Figure 13. Hardened Stairwells with Man Traps and Slippery Agents....37
Figure 14. Original LWSMR 30-Minute Offsite Response 39
Figure 15. Original LWSMR 60-Minute Offsite Response 40
Figure 16. Facility Layout with BBREs In Corners....43
Figure 17. Five-Adversary Attack on BBRE Facility Layout 44
Figure 18. Eight-Adversary Attack on BBRE Layout – Initial Assault 45
Figure 19. Eight-Adversary Attack on BBRE Layout – Facility Breach....46
Figure 20. Eight-Adversary Attack on BBRE Layout – Response Defeat....46
Figure 21. Facility Layout with Gun Ports....48
Figure 22. Five-Adversary Attack on Gun Port Facility Layout....49
Figure 23. Eight-Adversary Attack on Gun Port Layout – Initial Assault....50
Figure 24. Eight-Adversary Attack on Gun Port Layout – Facility Breach....51

LIST OF TABLES

Table 1. Total Technology Cost for Offsite Response 8
Table 2. Total Technology Cost for Onsite Response....8
Table 3. Original LWSMR Staffing Headcount 9
Table 4. Modified LWSMR Staffing Headcount....9
Table 5. Example of Delay Multiplication Factors....36
Table 6. Adversary Task Times for Various Locations....37
Table 7. Sample of Probability of Neutralization....38
Table 8. Original LWSMR Security Technology Costs....53
Table 9. Original LWSMR Staffing Headcount 56
Table 10. Hypothetical Security Technology for Modified LWSMR Design 56
Table 11. Modified LWSMR Staffing Headcount....58

EXECUTIVE SUMMARY

This report built on previous efforts by conducting an analysis of an onsite response strategy on the same light water small modular reactor (LWSMR) model that was used for evaluation of offsite response strategies.[2] The goal of this work is to evaluate the differences and cost-effectiveness of an offsite verses an onsite response force and to assist vendors in making design decisions that will produce the most cost-effective plant design. The primary tool for analysis of each facility model and response strategy was Scribe3D©. This software, developed by Sandia National Laboratories (Sandia), enables quick and inexpensive modeling of hypothetical facility designs and facilitates evaluation of hypothetical physical protection systems (PPS) and response strategies through scenario analysis by subject matter experts.

The LWSMR used low-enriched uranium (LEU) fuel like traditional light water reactors, but it incorporated many SMR design features that reduced the facility footprint, increased passive safety, and reduced potential for sabotage leading to radiological release. The initial design, which was evaluated with an offsite response in mind, incorporated a significant number of passive and active delay elements to provide at least 30 minutes of delay for an adversary and allow an offsite response force to muster, deploy, and interrupt the adversary before they were able to complete their sabotage objectives. When adapting the facility for an onsite response strategy, the reactor design features that contribute to safety and security were maintained. Changes to the design included removal of office buildings from the protected area, minimization of the below-grade footprint, addition of a "security floor" above the operational facilities, and integration of hardened fighting positions (HFPs) from which the responders could engage.

The removal of office buildings from the protected area (PA) had several benefits. First, additional buildings within the PA provided adversaries with cover and concealment, creating a path of cover as they moved from the perimeter barriers to the reactor building. Removing these structures allowed responders to have clear, overlapping fields of fire across the entirety of the PA. Additionally, locating office buildings outside of the PA provided further cost savings and the logistical advantage of reducing the number of employees who needed to be included in the human reliability program. Finally, reducing the number of those coming onsite enabled better oversight of operational activities by a smaller security contingent. Once shift change occurred, security had greater leverage for managing movement through the entry control point (ECP), reducing the likelihood that an adversary could exploit vulnerabilities created during activities such as deliveries, fuel shipments, or maintenance.

The first scenario evaluation for onsite response began with a facility model incorporating the design features and strategies described above, with the hardened fighting positions implemented as blast-and- ballistic-rated enclosures (BBREs) built into the corners of the reactor building on the upper security floor. Minimizing structures in the PA to only include the switchyard and the reactor building itself ensured responders posted in the corner BBREs could provide at least two overlapping fields of fire along the perimeter, with much of the PIDAS being covered by three responders. Assumptions for the scenario analysis included a design basis threat (DBT) of four-to-eight adversaries with military or equivalent training, small arms capabilities, and explosive resources to include a large vehicle borne improvised explosive device (VBIED) and up to 10kg of high explosives that could be distributed amongst the team.

[2] "U.S. Domestic Small Modular Reactor Security by Design." Evans, et. al. Sandia National Laboratories. SAND2021-0768.

Evaluation of this design revealed an effective response against a coordinated attack by an adversary team of five members; however, when the team was increased to eight members, sufficient suppressive fire on the eastern BBREs prevented the responders in those posts from engaging the adversaries as they approached the reactor building wall and allowed the adversaries to place sufficient explosives on the wall to breach through the side of the facility. Once the adversaries were inside, the design of the facility did not provide for an adequate response to be mounted on the facility interior. The adversary team was able to advance and defeat the remaining responders. Following the final engagement, the adversaries had enough surviving members and resources to carry out their act of sabotage.

These results led to a redesign of security features of the facility. The BBREs were removed from the corners of the reactor building and replaced with smaller, more distributed gun ports built into the facility exterior and interior walls. The gun ports on the corners were designed to project outward from the side of the building, providing both a port facing out from the facility as well as a port facing down at a 45-degree angle. In this way, the benefit of engaging along the skin of the building that had been provided by the BBREs was retained. The increased number of gun ports along the facility exterior allowed for greater flexibility for responder engagement while also reducing the effectiveness of suppressive fire by the adversaries. The significant decrease in cost achieved by replacing the BBREs enabled integration of gun ports in the interior of the facility as well. With this design change, the responders could engage from the security floor into critical areas and paths that the adversary would be required to take in order to reach sabotage targets.

The new security design was evaluated during a second scenario analysis. When tested against a team of eight adversaries, the new strategy allowed the responders to funnel the adversaries in directions and to locations advantageous to the response force. While the adversaries managed to enter the facility through the receiving area, the responders were positioned to safely and effectively engage the intruding force, defeating all eight adversaries without sustaining a single casualty. The security features of this final design were slightly more expensive than the security features incorporated in the design for an offsite response strategy; however, the increased cost of the security technology was significantly offset by reduced construction costs (many fewer passive and active delay elements were required with an onsite response force) and by a reduction in full-time equivalents (FTEs) required for the security force.

Table 1 andTable 2 highlight the costs to purchase security technologies for an offsite response force and an onsite response force that utilizes gun ports at various locations throughout the facility, respectively. As demonstrated, the overall security technology costs are similar. It is important to note that the total technology cost for the offsite response force does not include the costs for reinforced concrete delay barriers, which would increase the total technology costs to closer, if not greater than that for an onsite response force strategy.

Table 1. Total Technology Cost for Offsite Response

Total Technology Cost		**$ 5,976,172.68**

Table 2. Total Technology Cost for Onsite Response

Total Technology Cost		**$6,658,522.92**

Table 3 andTable 4 highlight a hypothetical staffing headcount that may be needed to effectively implement these physical protection system designs. As the tables indicate, the offsite response strategy requires a much larger response force to be effective at interrupting and neutralizing the

adversary force compared to the modified onsite response force strategy. The onsite response force strategy design, with its lower upfront security technology costs and smaller staffing headcount, could lead to both reduced upfront costs and long-term operations and maintenance costs for the physical protection system.

Table 3. Original LWSMR Staffing Headcount

Position	24/7 12 hr. Rotating Shift	FTE
Security Shift Supervisor	1	4
Field Supervisor and Response Team Lead (RTL)	2	8
Alarm Station Operators (central alarm station [CAS]/secondary alarm station [SAS])	2	8
Armed Responders	10	40
Armed Security Officers (ASOs)	4	16
Total	**19**	**76**

Table 4. Modified LWSMR Staffing Headcount

Position	24/7 12 hr. Rotating Shift	FTE
Security Shift Supervisor	1	4
Field Supervisor and RTL	2	8
Alarm Station Operators (CAS/SAS)	2	8
Armed Responders	4	16
ASOs	3	12
Total	**12**	**48**

Based on the results of the analysis, the primary recommendation is implementation of an onsite response strategy. However, the results also indicate that this strategy must be implemented properly to provide robust and cost-effective security. Crucial to this objective is the development of a design that allows responders to quickly and effectively shift from engagement on the facility exterior to engagement on the interior. While promising, the results of this effort are far from exhaustive. There is potential to complete much more analysis of scenarios against adversaries with expanded design basis threats (DBTs). The security design features could also be incorporated into other SMR designs to assess their effectiveness in other environments and conditions. As things stand, the evaluations completed thus far provide valuable insights for stakeholders at a critical time for the nuclear power industry.

This page left blank

ACRONYMS AND DEFINITIONS

Abbreviation	Definition
AC&D	alarm communication and display
ARSS	Advanced Reactor Safeguards and Security
ASO	armed security officer
BBRE	bullet- and blast-resistant enclosure
BMS	balanced magnetic switches
CAS	central alarm station
CCTV	closed-circuit television
CVCT	chemical volume control tank
CFR	Code of Federal Regulations
CUI	controlled unclassified information
DBA	design basis accident
DBT	design basis threat
DG	draft guide
DOE	Department of Energy
ECCS	emergency core cooling system
ECP	entry control point
FDB	field distribution box
FHS	fuel handling system
FTE	full-time equivalent
HFP	hardened fighting position
IDS	intrusion detection system
IR	infrared
KIA	killed in action
LEU	low-enriched uranium
LLEA	local law enforcement agencies
LE	law enforcement
LOCA	loss-of-coolant accident
LWSMR	light water small modular reactor
MOU	memorandum of understanding
MW	microwave
NRC	Nuclear Regulatory Commission
OCA	owner-controlled area
PA	protected area
PIDAS	perimeter intrusion detection and assessment system

Abbreviation	Definition
PIN	personal Identification Number
PIR	passive infrared
POE	power over ethernet
PPB	power production building
PPS	physical protection system
PSIT	passive safety injection tank
PTZ	pan-tilt-zoom
PWR	pressurized water reactor
RPV	reactor pressure vessel
RTL	response team lead
SAS	secondary alarm station
SBT	security bounding time
SMR	small modular reactor
Sandia	Sandia National Laboratories
SeBD	security-by-design
UAS	uncrewed aerial system
UHF	ultra high frequency
UPS	uninterruptible power supply
U.S.	United States
VA	vital area
VBIED	vehicle-borne improvised explosive device
VHF	very high frequency
VMS	video management system

1. INTRODUCTION

Many small modular reactor (SMR) vendors and utilities are focused on reducing costs of security systems to increase the economic viability and competitiveness with other sources of energy. SMRs are also a large portion of the push to ensure energy security and energy independence within the United States.[3] To assist vendors in designing security systems that are cost-effective both upfront and long-term for utilities, this project aims to develop recommendations to improve security effectiveness against a wide spectrum of threats while still maintaining cost-effectiveness to assist in deployment of these advanced reactor technologies. As the threat space against nuclear facilities grows in cyber capabilities and advanced technologies such as uncrewed aerial systems (UAS), it is important to ensure that the physical protection systems (PPS) for SMR facilities are designed against both the current space and to mitigate expanding threats.[4] By considering both the current and future threat landscapes in the design process, vendors and utilities can improve the overall effectiveness of the security system and reduce long-term costs that come with retrofits to mitigate against new and novel threats.

This report aims to capture lessons learned and PPS improvements that have been identified through the security-by-design (SeBD) process to create cost-effective security systems. One of the first SeBD projects conducted in the Advanced Reactor Safeguards and Security (ARSS) program was to evaluate SeBD for a light water small modular reactor (LWSMR) with an offsite response force to defend the facility from an adversary attack.[5] This baseline design and analysis identified many factors that could be used in SeBD integration. However, the PPS designed through this process did not create the most cost-effective security system. This report will describe the differences between the first LWSMR design iteration and a more cost-effective PPS design iteration.

This work can assist LWSMR and SMR vendors and future operators in designing cost-effective security systems and position security's role and impact in overall facility design to create a more effective security system that also reduces long-term operations and maintenance costs of a PPS.

[3] https://climate.law.columbia.edu/content/president-trump-orders-department-energy-build-nuclear-energy-generation-capacity#:~:text=Home-,President%20Trump%20Orders%20Department%20of%20Energy%20to%20Build%20Nuclear%20Energy,Energy%20to%20advance%20this%20policy.

[4] https://www.newsweek.com/ukraine-strikes-russian-nuclear-power-plant-says-moscow-2118411

[5] "U.S. Domestic Small Modular Reactor Security by Design." Evans, et. al. Sandia National Laboratories. SAND2021-0768.

This page left blank

2. HYPOTHETICAL FACILITY

The hypothetical LWSMR developed for this design and analysis encompasses features and capabilities of multiple U.S. domestic LWSMRs currently in development and in various domestic licensing stages. This provides a framework for the design and analysis to capture SeBD for domestic SMR applications.

2.1. Original Hypothetical LWSMR Facility

The first developed hypothetical LWSMR facility was designed to use only an offsite response force. This created a design that led to significant numbers and types of security delay barriers and detection technologies to delay the adversary long enough ensure offsite response forces could effectively interrupt and neutralize them.

2.1.1. Original Building Descriptions

The site consists of two primary building structures and two separate entry control points (ECPs).[6]

- Office Building – The office building contains the office spaces used by site personnel.
- Switchyard – This fenced in area is where the switching substation is located. This substation enables offsite power to be connected to the site and the power produced by the LWSMR to be transmitted to the local electrical grid.
- Power Production Building – The power production building (PPB) consists of one above-grade floor and two below-grade floors. The above-grade floor is 15-feet tall, and the below-grade floors are 20-feet tall.
    - The above grade floor consists of:
        - Two turbine and battery bank rooms (59’ x 52’6”)
        - Reactor building (77’5” x 61’3”)
        - Storage building (39’ x 148’)
            - The below-grade floor of the storage building houses the response force barracks, reactor control room, and the central alarm station (CAS).
        - Nuclear receiving building (39’10” x 42’1”)
        - Non-nuclear receiving building (39’10” x 42’1”)
    - The PPB also houses the spent fuel pool, four reactor cores, and a spent fuel processing area.
    - The first below-grade floor consists of:
        - Reactor control room
        - Two battery bank and diesel generator rooms
        - Below-grade nuclear receiving building
        - Reactor building

[6] “U.S. Domestic Small Modular Reactor Security by Design.” Evans, et. al. Sandia National Laboratories. SAND2021-0768.

- The second below-grade floor consists of the reactor building.

Figure 1 displays the site layout and buildings.

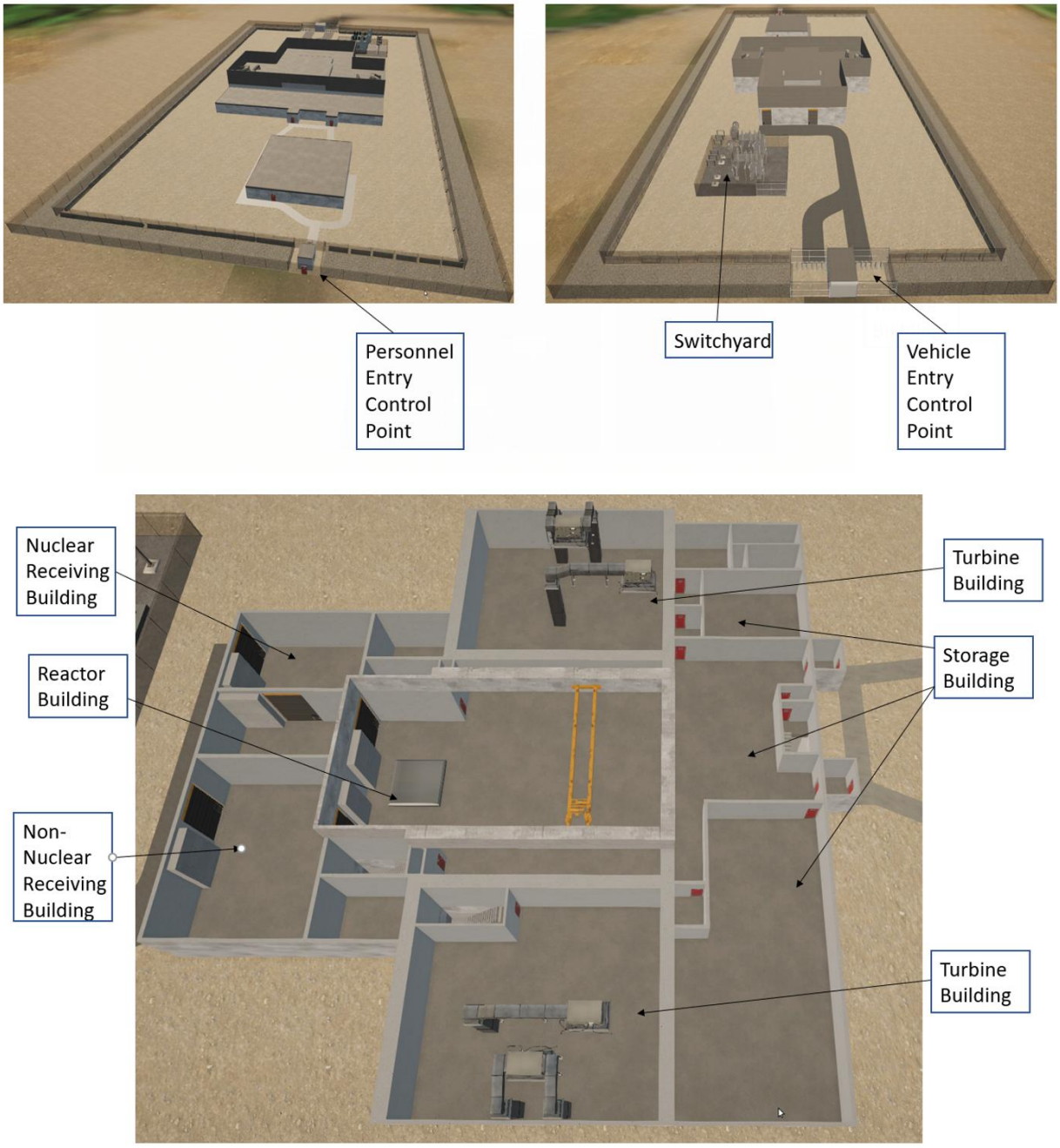

Figure 1. Original LWSMR Facility Layout

2.1.2. Reactor Description

Based on numerous U.S. domestic SMR designs, the reactors in this design and analysis are light water type small modular reactors. These reactor vessels house the reactor core, reactor core coolant pumps, pressurizer, and the steam generators inside of the reactor pressure vessel. Housing these items inside of the pressure vessel creates a smaller plant design and reduces the number of potential

sabotage targets. The LWSMR design also decreases the number of large connection pipes to the pressure vessel, which removes the risk of a primary loop large-break loss of coolant accident (LOCA). Removing primary system large-break LOCAs can reduce the risk of sabotage at an SMR facility. Each reactor is fueled by low enriched uranium (LEU) UO_2 pellets that are enriched to 4.9% U-235 for proliferation resistance. The site operates four reactor units simultaneously. Each reactor core is replaced every 24 months via an underwater refueling system, and the spent fuel core is stored onsite for 10 years in a spent fuel pool. The expected design lifetime of the plant is 60 years. Some key reactor descriptions include:

- Each reactor core produces 140 MWth
- Each reactor system can produce 49 MWe
- A total of 39 fuel assemblies are arranged in a 17x17 rod bundle (typical of a pressurized water reactor [PWR])
- The fuel is enriched to 4.9% U-235
- Primary cooling is completed with natural circulation
- The site can produce 196 MWe

The reactors are cooled and moderated by light water with boric acid for reactivity control. The reactor pressure vessel (RPV) contains all primary system components, including the reactor core, control rod drive system, integral helical coil steam generators, reactor coolant pumps, and pressurizer. The primary coolant inside of the RPV is liquid borated water maintained by the pressurizer at 15 MPa. Cooling in the primary system is performed by forced circulation with 10 internal canned motor coolant pumps. The water is forced upward through the core by the coolant pumps and flows downward through the helical coil once-through steam generators. There are two steam generators per reactor core, which combine steam before it moves to the turbine. On the secondary side, the water and steam at an average pressure of 6 MPa is heated in the steam generator in a countercurrent flow, resulting in some superheating of the steam beyond saturation. The steam then travels to a high-pressure turbine, followed by a series of low-pressure turbines. There is one high-pressure turbine per reactor core, for a total of four turbines per plant. The steam and any letdown water is collected and sent to a condenser to completely condense the steam-water mixture into liquid, then pumped back to the steam generator for heating. The condenser is cooled by the ocean for ultimate heat rejection.

Reactivity control and safe shutdown is mainly performed by the B_4C control rods. The Quad-Power RPV is 20 cm thick, 16 m high, and 3.5 m in inner diameter. The RPV is located within a 1.3-m thick concrete containment vessel located below-grade. The containment vessel inner height is 21 m, with a 5 m inner diameter. Containment is cooled with an integral water tank in direct contact outside of the concrete shell, which acts passively to transfer heat to a heat exchanger via natural circulation.

The entire reactor building, which holds the four reactors as well as the spent fuel pool, is below-grade, as is the main control room building. Both buildings are also seismic category I structures. The reactor building is only expected to be accessed during refueling operations, safeguards inspections, when maintenance is needed, or when security inspections are needed. The main control room onsite operates all four reactors and is staffed at all times by one operator and one shift supervisor.

The SMR is capable of passive cooling after a loss-of-onsite power design-basis accident (DBA) without operator action for 48 hours before any fuel melting occurs. Following a loss of on-site power, the reactors are automatically tripped, inserting its control rods and shutting down the nuclear chain reaction. In the case of a LOCA, the emergency core cooling system (ECCS) automatically initiates. The ECCS consists of passive safety injection tanks (PSITs), which inject gravity-driven water passively into the RPV following depressurization from automatic depressurization valves. Each reactor core is equipped with one PSIT, located outside the containment vessel and within the below grade-level floor of the reactor building. Each tank can maintain 48 hours of cooling. Each reactor core is equipped with its own dedicated PSIT; however, if one PSIT is lost, each reactor core can draw cooling from another PSIT in a "pair." This is performed via an operator-actioned valve that does not permit reverse flow of water. Because there are four cores, there are two "pairs" of PSITs for this redundancy. A pair of two PSITs sits on each side of the reactors, with each pair providing emergency cooling capabilities to two cores. Each PSIT is surrounded by grating, which allows leaking water to escape to the second below-grade floor. This grate allows water to flow into a holding tank where it can then be pumped into the reactor cores to provide cooling in the event the PSIT is lost. The batteries and diesel generators are elevated six feet above the ground to reduce the impact flooding would have on the safe operation of the batteries and diesel generators. Primary offsite power is transferred to battery banks and diesel generators using uninterruptable power supplies (UPS) that enable instantaneous transition from offsite power to the onsite backup power capabilities. A ventilation system exists to expel hydrogen buildup and toxic gases from the battery bank and diesel generators to reduce the risk of potential hydrogen buildup that is produced when the batteries are recharged. The ventilation system is regulated by hydrogen gas monitors in the diesel generator and battery bank room. Before the concentration of hydrogen reaches an unsafe level, the ventilation system expels hydrogen and toxic gases from the battery bank and diesel generator rooms. All safety systems are entirely passive.

Each reactor core has its own chemical volume control tank (CVCT). These tanks are used to control the boric acid within the reactor core in case the chemical volumes in the reactor core need to change. Access to all areas within this section require a two-person rule. Figure 2 highlights the PSIT configuration. The PSITs are colored in grey and green.

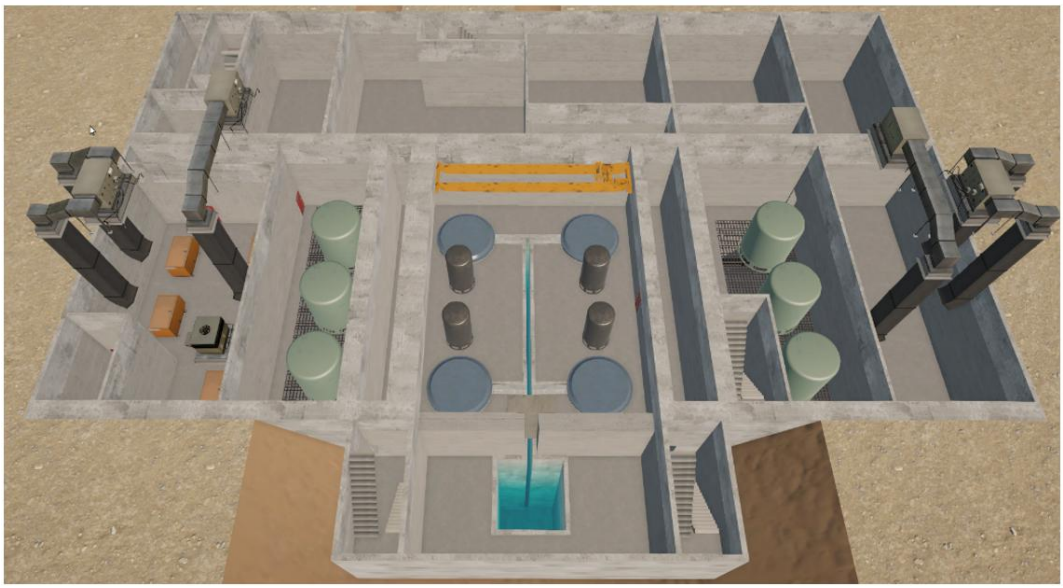

Figure 2. Initial PSIT Configuration.

2.2. Modified Hypothetical LWSMR Facility

Many modifications to the facility were made to potentially reduce the costs of securing the LWSMR facility, to include changes to the safety systems, building layouts, and the total number of buildings used onsite and within the protected area (see Figure 3).

Figure 3. Modified LWSMR Facility

2.2.1. Modified Safety Systems

One of the first changes made was to remove the redundant below-grade PSITs outside of the reactor bay and increase the size of the PSITs inside the reactor bay. This reduces the total number of targets at the facility, which will result in a reduction of security technologies and the complexity of the needed response strategy. The PSITs inside of the reactor bay are designed so that each PSIT is the primary tank for one of the four reactors and can provide 36 hours of cooling for its primary reactor. Additionally, each reactor is connected to another PSIT inside the reactor bay via a separate piping structure and system that enables each reactor to have access to 72 hours of emergency cooling.

It should be noted that in some cases, vendors may not choose this option as it introduces a location where a single point of failure could cause safety and security concerns inside the reactor bay. However, designing the PSITs such that each reactor has independent connections to two PSITs each supplying 36 hours of emergency cooling ensures adequate supplies of cooling. By minimizing the total number of locations where PSITs exist, the security system also has a reduced number of sabotage targets that it must protect and has limited the location of these targets, which can decrease the complexity of security plans and procedures and reduce the overall amount of security technology needed to protect the facility.

In the modified design, the diesel generators were moved from below-grade to above-grade. This enables the diesel generators and uninterruptable power supplies (UPS) to be placed above the PSITs and other sources of water at the facility. This may reduce the need to have sump tanks underneath the PSITs in the reactor bay design, reducing the amount of construction below-grade. Sump tanks were included in the original design to prevent flooding and damage to the diesel generators in the event the PSITs failed and leaked. The redesigned choice was made to place only necessary and radiological targets below-grade to improve the inherent security of the facility and leave support equipment above-grade to reduce costs, thereby improving the overall cost-effectiveness of the facility design. The reactor containment structures are not available for maintenance or access above-grade; however, a hatch is located on the ground of this level to support fresh fuel reloading of the reactors. Figure 4 shows where the diesel generators have been moved to within the facility and the location of the expanded PSITs.

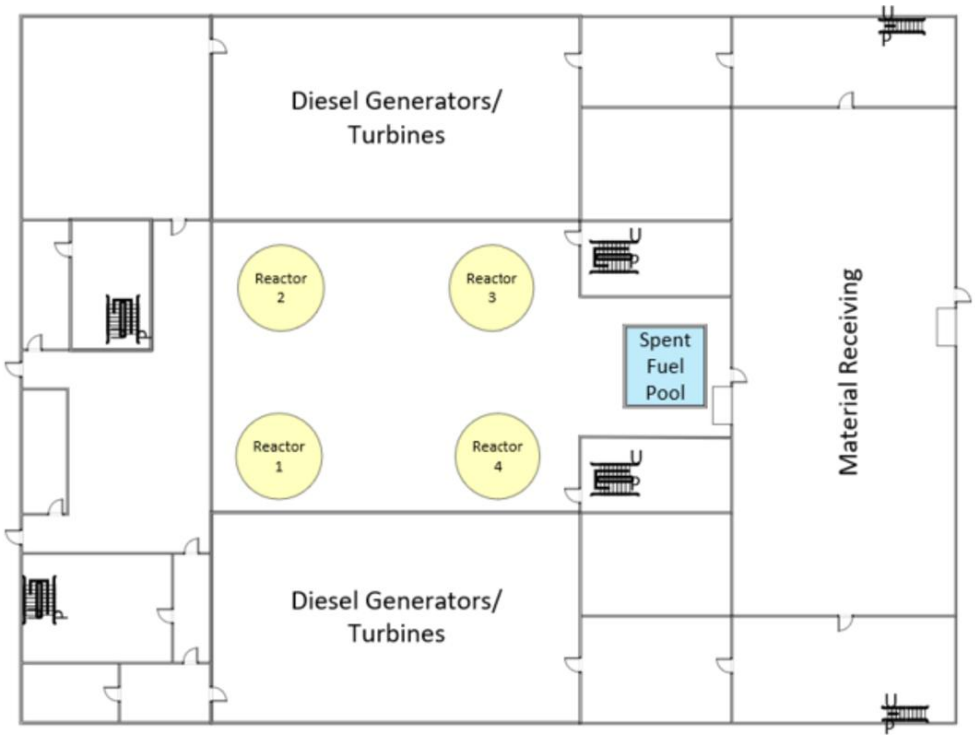

Figure 4. Modified LWSMR Above-Grade Floor

The office building inside of the protected area (PA) was removed from the PA and placed in the owner-controlled area (OCA). The office building presented an opportunity to provide the adversaries with cover and concealment along their movement up to the reactor building, and therefore, would provide greater benefit if it was moved outside of the PA. U.S. Nuclear Regulatory Commission (NRC) Draft Guide 5076 states, "Defense in depth should be provided for neutralization functions with an exterior protection layer of at least two overlapping fields of fire covering each sector of the outermost perimeter physical barrier." The PPS was designed to account for this draft guidance and the removal of the office building supported this design choice. Additionally, by reducing the overall number of personnel with PA access, the facility can reduce the number of personnel enrolled in the insider threat mitigation program or human reliability program. This also reduced throughput in the PA ECP. Both factors may reduce operations costs, and therefore, lead to improved cost-effectiveness of the PPS design.

A second above-grade floor was added that functions as a "security floor" for the armed responders, armed security officers (ASO), and the CAS and its operators. Figure 5 shows the security floor that was added to the facility. The red highlighted portions in the figure show gun ports that can be used by the armed responders to engage adversaries external of the building and internal to the building. This enables a defense-in-depth approach for the armed responders at the facility to ensure a high probability that the responders can interrupt and neutralize adversaries attempting a malicious act.

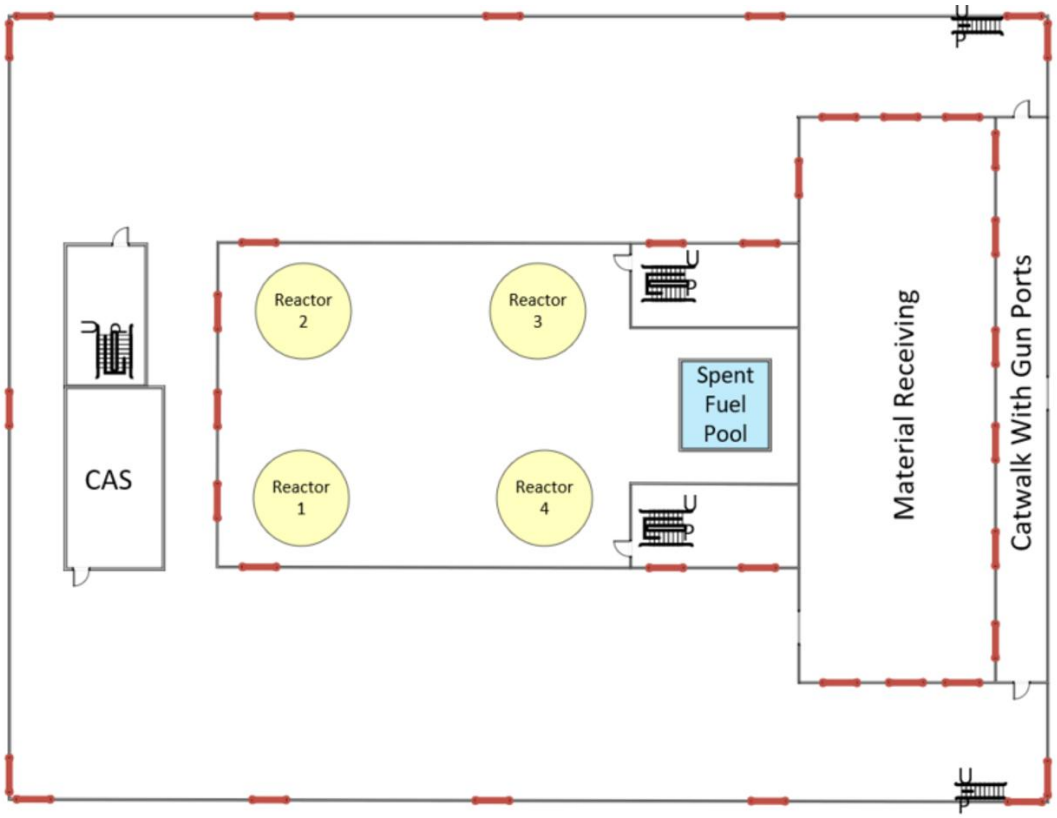

Figure 5. Modified LWSMR Security Floor

The below-grade floor of the facility contains the control room, the reactors, the PSITs, spent fuel pool, and spent fuel packaging area. This has reduced the overall floor plan for the below-grade portion of the facility and potentially reduces the overall cost to construct the facility. Figure 6 shows the location of a secondary alarm station (SAS). The below-grade location provides inherent resilience and separation from the CAS. While many SMR vendors are aiming to use remote wireless communications to the SAS, this design creates space for an onsite SAS. Alternatively, there is space inside of the PA ECP where the SAS could be located to reduce the overall amount of construction required below-grade.

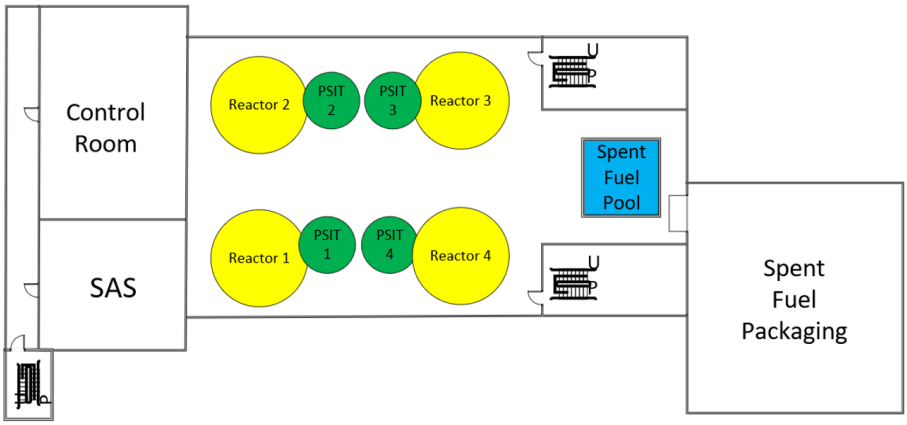

Figure 6. Modified LWSMR First Below-Grade Floor

These design choices highlight a key element of the security-by-design process to consider providing inherent security to target locations, which reduces the overall cost of the facility. Because this design places potential radiological sabotage targets below-grade and within multiple layers of security, the facility is also hardened against vehicle-borne explosive devices and emerging threats such as explosive UAS. This design also minimizes the amount of underground construction and overall size of the facility, which can lead to reduced construction costs.

3. HYPOTHETICAL LWSMR PHYSICAL PROTECTION SYSTEM DESIGN

3.1. Original Hypothetical PPS Design

The original PPS design was based solely on the use of an offsite response force, and the PPS was designed to enable that offsite response force to be effective at mitigating the adversary team as defined in the hypothetical DBT. The offsite response team consisted of six armed responders. The PPS was first designed to enable an offsite response force to arrive at the facility and provide response to an adversary attack within 30 minutes and 60 minutes. Because of this, much of the PPS design focuses on detection and delay technologies that would allow the offsite response force to arrive in time to interrupt and successfully neutralize the adversary force.

The site's PA is controlled by a perimeter intrusion detection and assessment system (PIDAS) consisting of an outer and inner fence line (eight-feet tall with outriggers) that are separated by an isolation zone with sensing, see **Error! Reference source not found.**The isolation zone sensing technology consists of bistatic microwave sensors and active infrared sensors. The 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 5 seconds before and after an alarm.

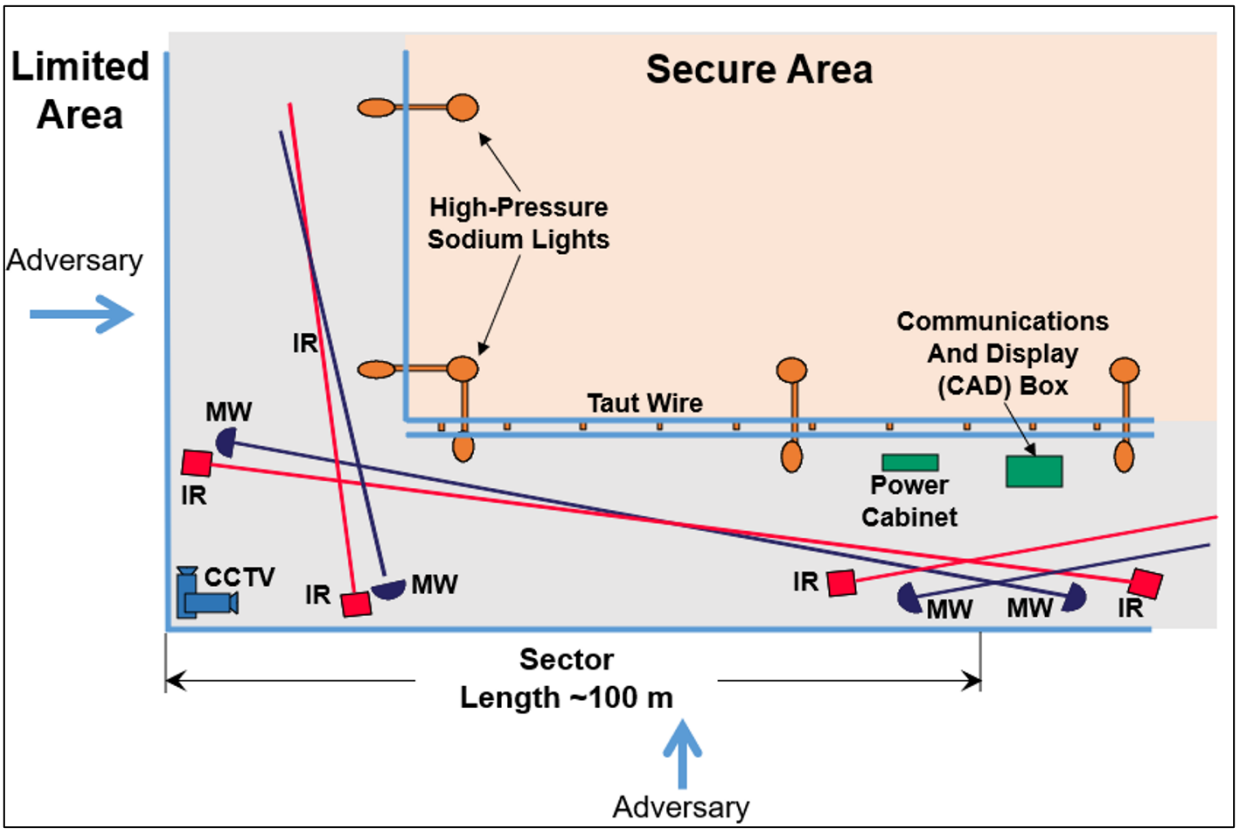

Figure 7. PIDAS Cross-section

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 receipt of new reactor fuel or equipment. Inner and outer hydraulic vehicle barriers are raised when the access point is not operational. The personnel entrance is manned 24/7 by two guards who perform detection of

prohibited items before allowing personnel entry into the PA. 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 a proximity card and the entering of a personal identification number (PIN). When receiving new reactor fuel or equipment to 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 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 and the inner gate 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.

All building entrances inside the PA are armed with balanced magnetic switches (BMSs) and all entrance doors are monitored by security cameras. Building entrances, except for vital areas (VAs), are secured by proximity card reader access controls. The site operates four vital areas: the reactor building, two battery bank and diesel generator rooms, and the nuclear receiving building. The VAs are secured with two-factor authentication using a hand geometry reader and a PIN entry to allow access. All access to the reactor building, the battery bank and diesel generators, as well as the PSIT rooms requires the implementation of the two-person rule and direct visual observation to mitigate the insider threat risk. Figure 8 and Figure 9 provide a layout of the baseline PPS design.

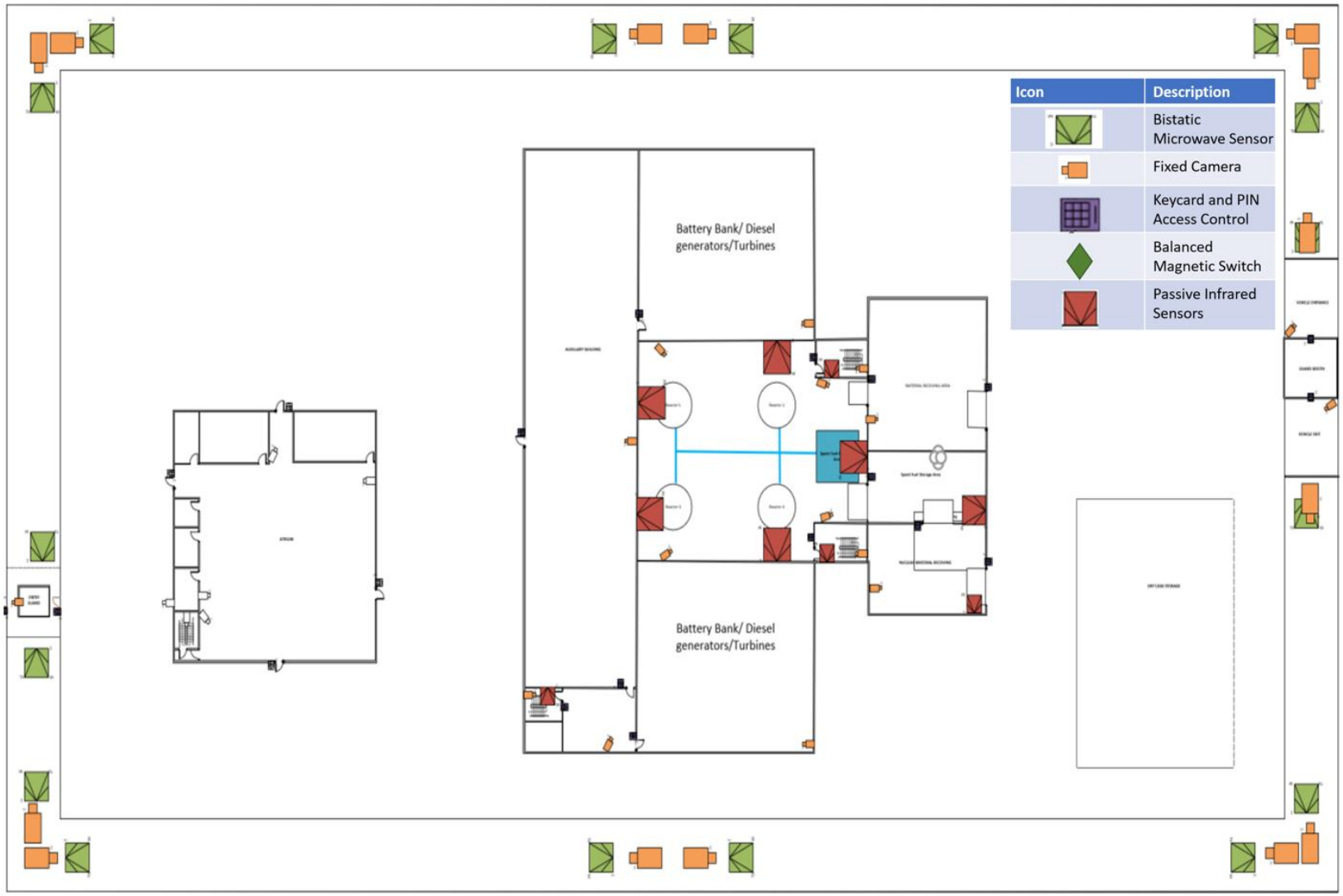

Figure 8. Original PPS Design

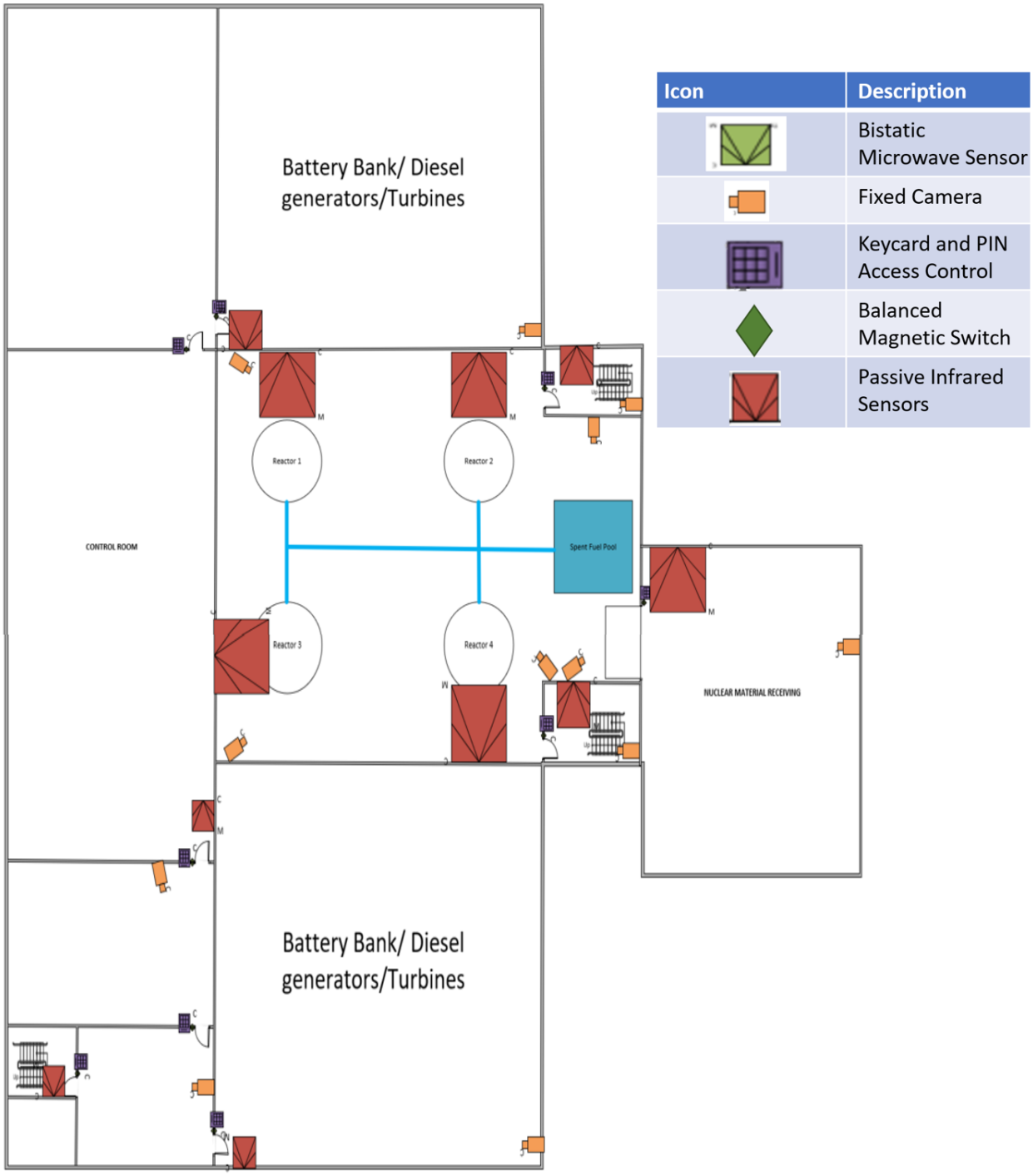

Figure 9. Original PPS Exterior and Interior Intrusion Detection Systems

3.2. Modified PPS Design

Compared with the previous report, facility design changes were made both for adaptation to an onsite response strategy and from the standpoint of lessons learned regarding the design of active and passive safety features for SMR operations. As the result of several changes, administrative and

operational spaces were consolidated into a single structure and underground space was minimized, reducing the need for costly excavation. This report further evaluated two separate layouts for onsite response. One layout was created with "blisters," ballistic- and blast-resistant enclosers (BBREs) placed in the corners of the upper level of the main structure, to provide hardened fighting positions with overlapping fields of fire in each direction out from the facility as well as along the skin of the building (Figure 10).

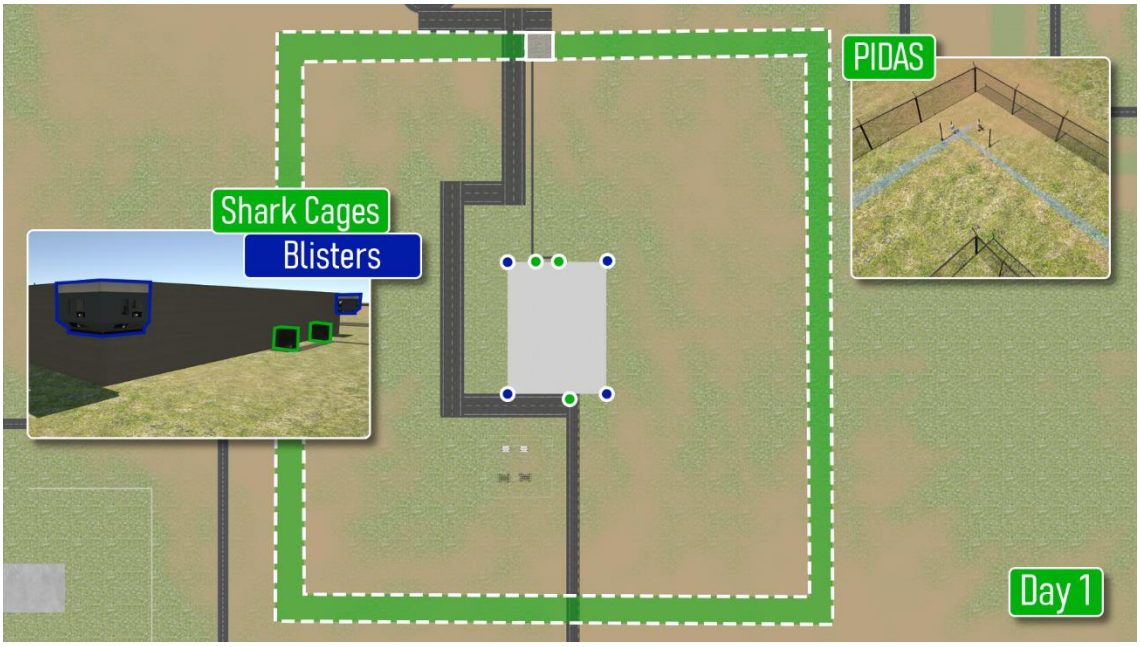

Figure 10. Modified Blisters Design

The second layout removed the blisters, opting instead for gun ports distributed around the walls of the upper level facing out in each direction, as well as gun ports looking into the receiving area, stairwells, and reactor hall from the security level of the second floor. The second layout reduces construction costs by eliminating the expensive BBREs. In addition, subsequent evaluation will show that the cheaper, more numerous gun ports distributed throughout the facility provide better defense of the vital areas at a lower cost. See Figure 11 for an example of the gunport design.

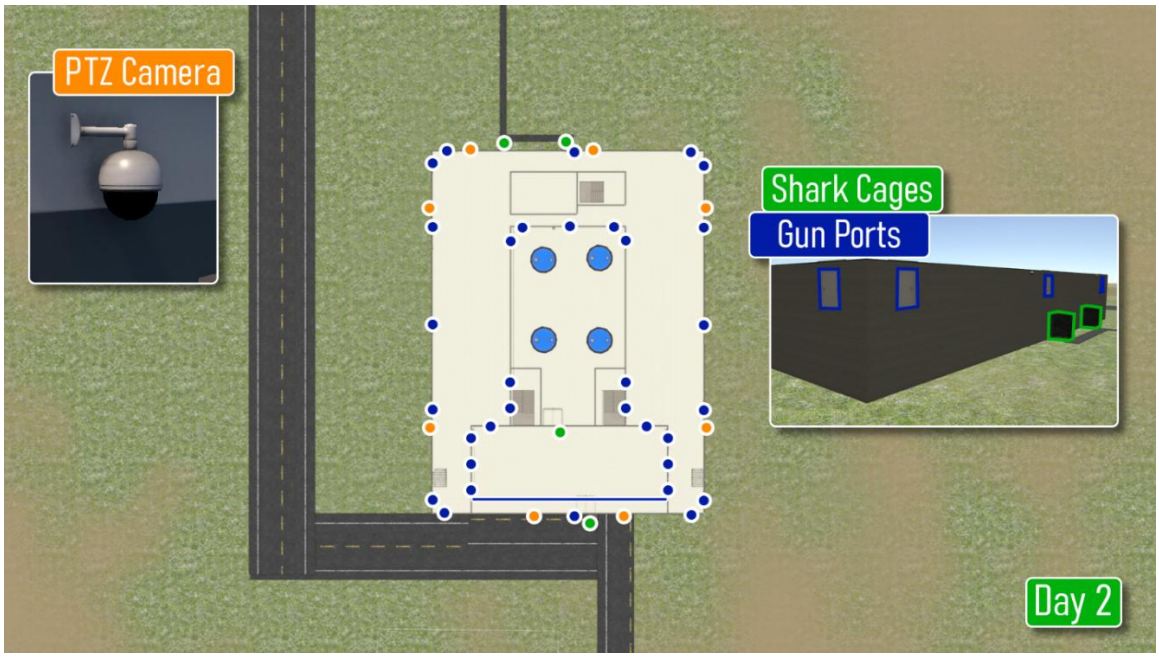

Figure 11. Modified Gunport Design

3.3. Hypothetical Design Basis Threat

To conduct the insider analysis for impact of abrupt theft, protracted theft, and sabotage, a hypothetical DBT was developed to bound the analysis and recommendations.

The DBT assumed for this analysis is based on information from the 10 Code of Federal Regulations Part 73.1 (10 CFR 73.1) and an open-source hypothetical DBT. The adversary team members were assumed to have the following characteristics:

- Group size of 4-to-8 individuals
- 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 and a 9-mm pistol; ammunition; grenades; satchel charges containing bulk high explosives, not to exceed 10 kg total; detonators; bolt cutters; and miscellaneous other tools
- Each able to carry a man-portable total load of 29.5 kg (65 lb)
- Assumed run speed of 3 m/s
- One active non-violent insider (not included in the adversary group of 4-to-8 individuals)

This page left blank

4. PHYSICAL PROTECTION SYSTEM EVALUATION

In the design and analysis of a PPS for a nuclear power facility, PPS designers must first consider the adversary pathway into the facility to reach a target location and the adversary scenario that will define how the adversary may reach target locations to conduct sabotage.

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. For the assessment of onsite response, detection and delay still play a role in supporting the response strategy; however, the necessity of costly delay elements is greatly reduced by shortening the timeline for responders to get into advantageous positions. Detection still performs a critical function by providing information to the CAS operator/response team lead to direct the movements and actions of responders across the facility during an attack. For this assessment, adversary paths were selected to increase the likelihood of the adversary force reaching the skin of the building without being targeted directly by response forces. Due to the nature of onsite response, the adversary strategy included diversionary attacks, suppressive fire, or both.

For this analysis, the adversary team is attempting to attack the facility with the objective of sabotage. Sabotage targets include the PSITs or the reactor vessels themselves to cause a radiological release from the facility. The PSITs provide passive cooling to the reactors that would ensure the fuel in the reactor is cooled and also ensure that fuel was covered in the reactor core. Because the PSITs can deliver water to the reactor passively, or through operator action, an adversary would have to sabotage the tank, the piping infrastructure, or otherwise prevent water from the tank reaching the reactor core.

To evaluate the effectiveness of the security systems for the original and modified hypothetical LWSMR, Scribe3D© was used to conduct analysis and tabletop exercises evaluating the PPS against the developed adversary attack pathways and attack scenarios.

4.1. Original LWSMR Security System Evaluation

The analysis of the PPS design for the original LWSMR was evaluated using PathTrace and a version of Scribe3D[7] that no longer exists, which enabled each scenario to be analyzed multiple times to create a representative sample of the overall likelihood the response force was able to neutralize an adversary attack scenario.

To design and evaluate the PPS for the LWSMR using an offsite response force, the delay time at the facility must first be increased to ensure that an offsite response could effectively respond to a nuclear security event in either 30 minutes or 60 minutes. To design and evaluate these approaches, PathTrace was used to introduce delay features that could support a 30-minute or 60-minute response time to the facility.

The changes to the overall facility design included the addition of extended detection technologies, active delay features such as obscurants and slippery agents, and the use of reinforced concrete person traps. Extended detection technologies include radar, lidar, and deliberate motion analytics.[8] Many of these technologies applied on their own can moderately increase adversary task times to reach target locations or can detect the adversary earlier and enable more delay barriers to be

[7] https://modsimtools.sandia.gov/scribe3d/

[8] https://www.sandia.gov/app/uploads/sites/273/2024/01/RIC-Conf-Adv-Sec-Concepts-final-02-23-2023.pdf

credited toward the overall adversary attack timeline. However, when they are incorporated together, these features can significantly increase the adversary task time.

Figure 12 shows locations where active delay and person traps were incorporated together throughout the facility. The active delay features such as slippery agents and smoke are considered delay multipliers, which, if placed in front of passive delay features (i.e., doors, windows, walls), can multiply the total time it takes the adversary to penetrate or bypass a barrier.

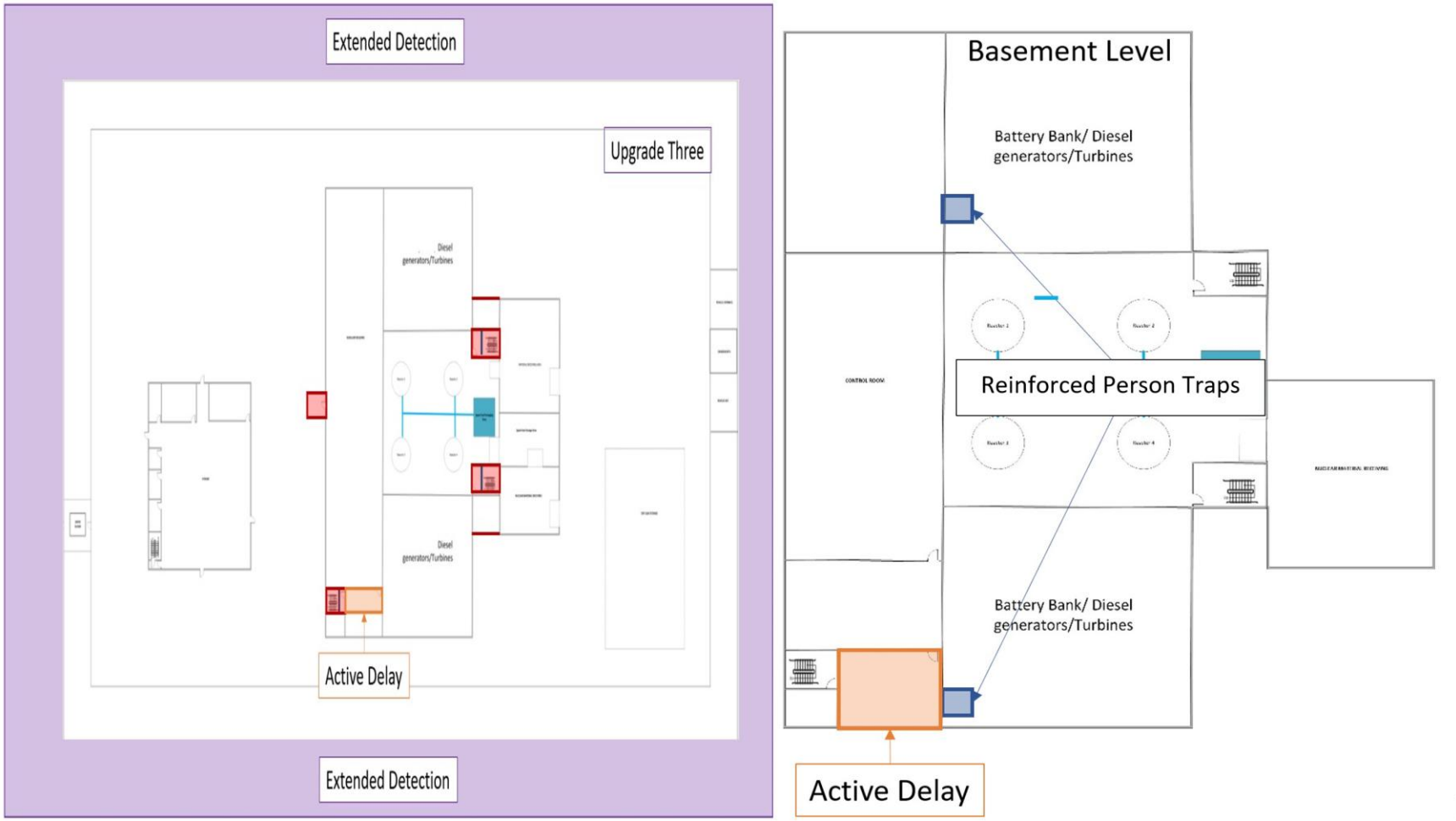

Figure 12. Active Delay, Extended Detection, and Person Traps

When these active delay features are applied in a person trap, it can substantially increase the adversary task time to breach a person trap. A person trap consists of one exterior door that is protected with an access control device that must first be passed and entered. Once inside the trap, the outer door must be closed and locked. Then, the individual must use a two-factor authentication access control device to enter through the second door in the trap. Additionally, the second door in the person trap can be locked and controlled by the CAS operator and unlocked only by the CAS when an accepted access control credential is used to gain access through the person trap. Table 5below highlights how multiplication factors are used to determine overall adversary delay times.

Table 5. Example of 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

Person traps were installed at all locations that personnel enter into the facility. These person traps were also filled with active delay features to increase the adversary task time to breach into the facility. Additionally, the stairwells in the facility were equipped with active delay features that are used to increase the adversary task time to reach target locations in the below-grade portions of the facility. These modifications can be seen in Figure 13.

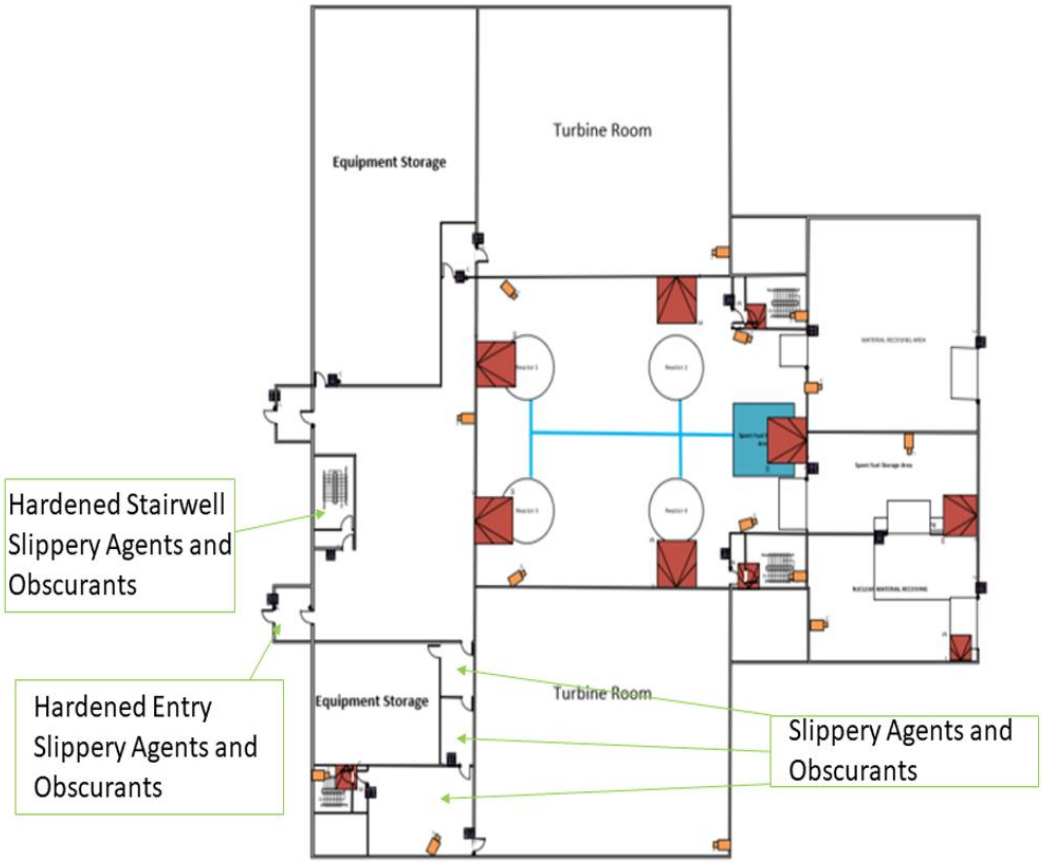

Figure 13. Hardened Stairwells with Man Traps and Slippery Agents

Table 6 summarizes the total adversary task time to reach and sabotage potential target locations in the original LWSMR facility. As shown in the table, for a 30-minute response time, the PPS design was developed to ensure a high probability of interruption for the overall security system design.

Table 6. Adversary Task Times for Various Locations

Target	Task Time (s)	Probability of Detection (%)	Probability of Interruption (%)	Response Time (s)
Reactor	5513	99	99	1800
Spent Fuel Pool	5032	99	99	1800
Battery Bank	2567	99	100	1800
Control Room	3043	99	99	1800
Reactor PSIT	4307	99	99	1800
CAS	3037	99	99	1800

Once the PPS was designed to provide an adequate delay time to allow for an offsite response force to effectively interrupt the adversary team, tabletop exercises and simulated adversary attack scenarios were conducted in Scribe3D. Various adversary attack scenarios were considered with various response force strategies to respond to these adversary attack scenarios.

In the first adversary attack scenario, the adversary team would proceed to sabotage the diesel generators that could be used to pump water from the sump into the reactor core if the PSITs were damaged, and then they would sabotage the PSITs for a given reactor. The second scenario considered the adversaries splitting into teams to attack the PSITs and the diesel generators separately. Once these scenarios were analyzed, hardened fighting positions (HFP) were added into the facility at key locations where the adversary must breach through to reach target locations. This design iteration considered two onsite responders that would respond to these HFPs and then be supported by the offsite response force that was arriving onsite to interrupt and neutralize the adversary force. The response force was made up of 10 individuals. If the response force was offsite, all 10 responders arrived at the perimeter; in the scenarios where HFPs were used, two armed responders manned the HFPs and eight responders made up the offsite response force team.

Each adversary attack scenario was simulated one hundred times using the Scribe3D software to determine probability of neutralization for the scenario investigated;[9] probability of neutralization was identified by dividing the total number of blue winds by the total number of simulations. Table 7 shows the detailed results from one of these simulations.

Table 7. Sample of Probability of Neutralization

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	100	100	96	90	85
Red Wins	0	0	4	10	15
Average Engagements	18	23	26	32	37
Average Killed in Action (KIA) Engagements	5	7	8	10	11
Blue Force Count	8	8	8	8	8
Average Blue Force KIA	1	2	2	4	4
Average Blue KIA in Win	1	2	2	3	3
Red Force Count	4	5	6	7	8
Average Red KIA	4	5	6	7	7

[9] The analysis version of Scribe3D is no longer a supported function in the Scribe3D software.

Name	Results: 4 Adversaries	Results: 5 Adversaries	Results: 6 Adversaries	Results: 7 Adversaries	Results: 8 Adversaries
Average Red KIA in Win	N/A	N/A	3	5	5

Once the simulations were conducted and the probability of neutralization determined for each scenario, the overall system effectiveness could be determined for each attack scenario and response force configuration. System effectiveness is determined by multiplying the probability of interruption and the probability of neutralization. For all the scenarios, the overall system effectiveness can be seen in Figure 14.

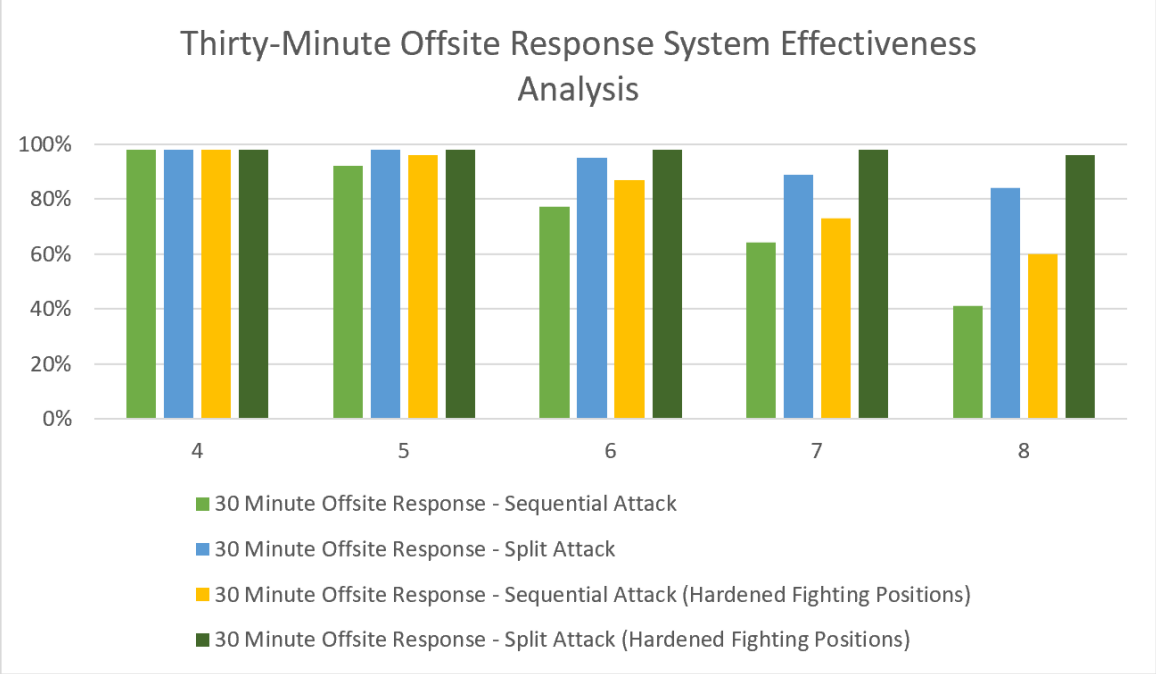

Figure 14. Original LWSMR 30-Minute Offsite Response

Additional analysis was conducted using the same adversary attack scenarios but considering an offsite response force time of sixty minutes. This analysis also considered the use of HFPs in tandem with an offsite response force (Figure 15).

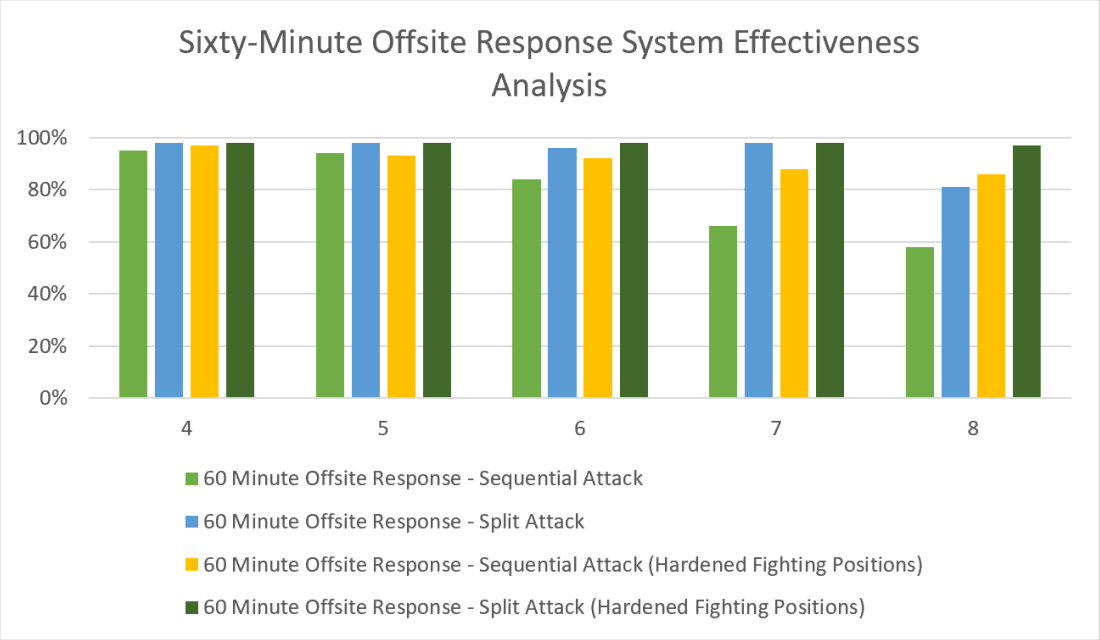

Figure 15. Original LWSMR 60-Minute Offsite Response

4.1.1. Considerations for a PPS Design Utilizing an Offsite Response Force

This study was one of the first PPS design and analysis studies conducted under the ARSS program to provide recommendations for SMR facility designers. The results from this study show that a PPS designed with an offsite response force strategy may be effective against various adversary attack scenarios. However, many lessons have been learned that show this strategy may not be as cost effective as other design methods and will require numerous delay barriers to be implemented at the facility to ensure the response force can effectively interrupt the adversary force. While a sensitivity study was not conducted to determine the total number of armed responders necessary, the number of responders seems to be higher than other potential design options. In many of the attack scenarios described above, the number of responders that are killed increases as the number of adversaries increases. This increase in number of responders killed during the scenario shows that more than four responders may be necessary to protect the facility when an offsite response force strategy is utilized.

One of the other considerations that must be made for using an offsite response force is the cost of the offsite responders, especially when considering an offsite response force comprised of local law enforcement agencies (LLEAs). NRC DG-5076 "Guidance for Technology-Inclusive Requirements for Physical Protection of Licensed Activities at Commercial Nuclear Plants" states,

> *…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 a DBT adversary force; conducting exercises regularly with the response force for training and to validate the effectiveness of the physical protection system; ensuring the response force arriving from offsite have adequate knowledge to respond to an adversary force that has already taken control of the site; and developing secondary contingency routes for the response force to reach the facility and considering methods to ensure the confidentiality of response force routes to the facility.*

DG-5076 also references DG-5072 "Guidance for Alternative Physical Security Requirements for Small Modular Reactors and Non-Light Water Reactors," for further guidance for implementing an offsite response force. To implement a PPS utilizing an offsite response force consisting of LLEA,

> *Where 10 CFR 73.55(s)(1)(ii) is satisfied for applying the alternative requirement in 10 CFR 73.55(s)(2)(ii), licensees or applicants should incorporate security delay systems in the design of a physical protection system to provide sufficient time for LE or other offsite armed responders to interdict and neutralize threats up to and including the DBT of radiological sabotage. To provide adequate delay, licensees or applicants should design their security systems to be able to delay the DBT for a time equal to or greater than a site's SBT, based on the process described in Appendix C, "Security Bounding Time and Adversary Interference Precluded Time," of this guidance.*

In this definition LE means law enforcement (i.e., local law enforcement agency). Based on this guidance, a facility must include adequate delay to meet the requirements of 10 CFR 73.55 and must also provide delay equal or greater to the security bounding time (SBT), which will require the facility to determine its SBT. This may require facility designs to have more delay than is necessary for the offsite response to effectively interrupt and neutralize the adversaries and could lead to both large upfront and long-term operations and maintenance costs. Additionally, DG-5072 states,

> *The licensee should identify any mutual aid agreements for sharing resources between LEs that may be applied in such contingencies in the MOU. The licensee should establish additional MOU with any mutual aid LE agencies that may be relied on to respond to a DBT attack. To maximize the likelihood that the required LE assistance will be available and reliable at all times, a licensee should consider establishing MOUs with at least two LE agencies that have not entered into a mutual aid agreement with each other and that are independently capable of interdicting and neutralizing the DBT.*

This will require the facility to evaluate multiple LLEAs and their ability to support responding to a nuclear security event at an SMR facility.

DG-5072 states,

> *When a licensee relies on offsite proprietary or contract armed responders to interdict and neutralize the DBT adversary, the licensee should house the full number of responders who are needed to adequately defend against the DBT in at least two separate offsite locations. This arrangement will provide defense in depth and ensure the continuous availability and reliability of the offsite response.*

Additionally, with regard to this housing, DG-5072 states, "Considerations should include protection against unauthorized access by personnel or vehicles, disruption of communications, and delay or blockage of the facilities' egress routes." DG-5072 also states,

> *When the licensee relies on LE to perform the interdiction and neutralization function, the licensee should ensure that the activities, tactical response drills and force-on-force exercises are planned and conducted in a manner to make them available to the LE agency. The licensee should conduct a sufficient number of security drills and exercises to enable LE armed responders who may implement contingency response and licensee protective strategy to participate in the licensee-conducted drills and exercises. When the licensee relies on other (i.e., licensee proprietary or contract) offsite armed responders to perform the interdiction and neutralization function, the licensee should ensure that all armed responders who may implement contingency response and licensee protective strategy participate in licensee-conducted security drills and exercises. Licensee conducted security drills and exercises are performed at the following minimum frequencies:*

- *Tactical response drills – quarterly*
- *Force-on-Force exercise – annually.*

While this is not an exhaustive list from these guidance documents, it highlights the amount of information, planning, and testing that will be needed to implement an offsite response force. Based on these draft guidance documents, there is differing guidance for LLEAs and contracted offsite response forces, which may also drive design decisions for a vendor and how an operator may implement their PPS. Based on these guidance documents and the analysis conducted for the original LWSMR facility, there are many factors that may influence whether a reactor vendor or operator utilizes an offsite response force. These factors include but are not limited to:

- *The expense for hiring and fulfilling potential pay rates of LLEAs or offsite response contractors:* LLEAs may require an operator to pay an hourly rate for officers dedicated to respond to a nuclear security event at an SMR facility. This is based on LLEA need around the country to ensure public safety and security and then an additional need to respond to a high security facility such as an SMR site. LLEAs may ask for an hourly pay rate to guarantee that officers can respond to an event 24/7 rather than be rerouted from ongoing work or be dispatched away from current functions.
- *Time spent training LLEAs or offsite response contractors:* The operator should consider the costs it will take for internal security members to conduct trainings, review qualifications, and conduct site familiarization efforts with LLEAs or offsite response contractors. The operators may need to provide an individual who is in charge and coordinates all response force trainings and tests as well as helps to implement the tactical response drills and force-on-force exercises with either LLEAs or the offsite response contractors.
- *Facilities to house offsite response contractors:* If the operator chooses to use an offsite response contracting company, they may have to consider the location to house those responders, provide security for the building in which the responders are housed, and potentially, have two housing areas for the offsite response force.

SMR vendors and operators should consider the potential impacts of selecting an offsite response force as part of the PPS design and strategy. There are many areas that may impact both upfront costs and long-term operation and maintenance costs, depending on the design of the facility and the offsite response force configuration chosen.

4.2. Modified LWSMR Security System Evaluation

In order to perform an evaluation of the modified LWSMR, Scribe3D was once again employed to assess PPS and responder performance under various conditions and scenarios. The newest version of Scribe3D does not have the analysis feature that was used in the previous evaluation, as funding objectives led to different areas of focus in the development and application of the tool. As such, evaluation was conducted through scenario analysis in a traditional tabletop exercise, incorporating input from subject matter experts in nuclear security, nuclear facility design, and response strategy and tactics. Over the course of two days, multiple scenarios were developed and evaluated using Scribe3D. While entire scenarios were no longer evaluated in large volumes, each engagement within the scenarios was analyzed 100 times to maintain both qualitative and quantitative assessment of the design. The following sections provide a description of each of the scenarios evaluated during the tabletop exercise and their corresponding outcomes.

4.2.1. Attacks On BBRE Facility Layout

The following sections describe the results of two adversary attack scenarios against the facility model developed for response from BBRE "blisters" in the corners of the building. In both cases, the attack originated on the east side of the facility and incorporated a diversionary attack on the ECP followed by suppressive fire at the BBREs on the east side of the facility. The attacks varied in the number of adversaries involved.

4.2.1.1. Response Posture

For the BBRE facility layout, one responder is posted in each corner of the second floor of the facility. These responders are each able to look out in two cardinal directions, as well as see directly down and along the skin of the building in two directions. The corner blisters provide overlapping fields of fire, resulting in at least two responders being able to target any point on the perimeter fence and, at many points along the perimeter, three responders can provide simultaneous coverage (Figure 16). Additionally, two armed responders are posted in the ECP. As a last line of defense, the CAS operators and response team leader are armed and may engage in the event of the adversary defeating the initial responders.

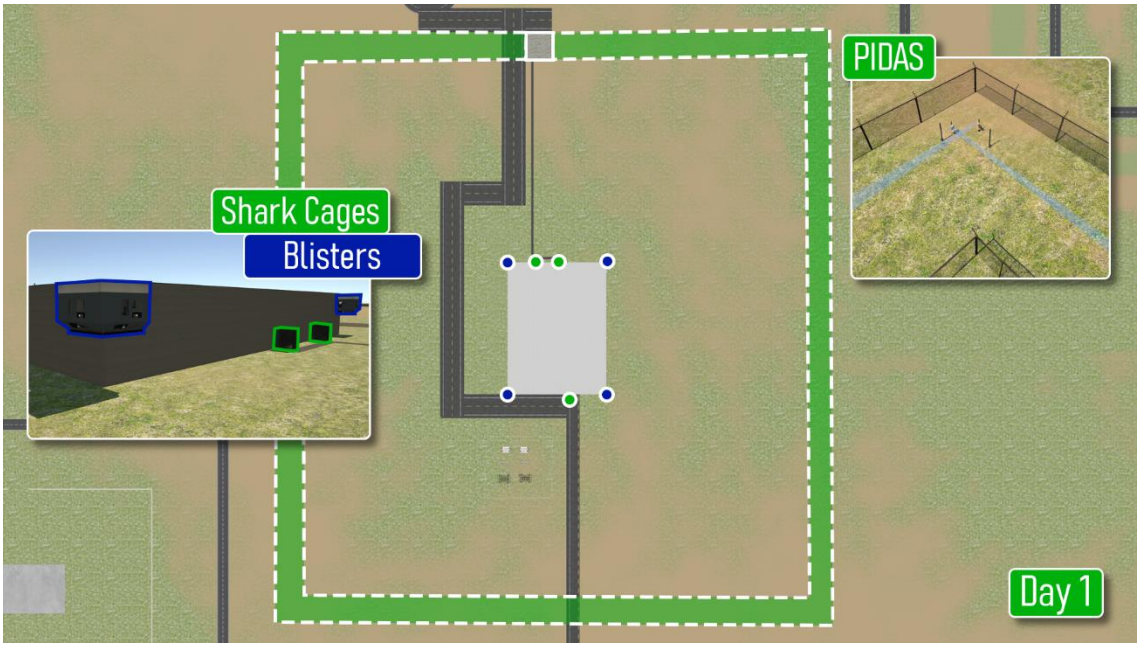

Figure 16. Facility Layout with BBREs In Corners

4.2.1.2. Response Force Win Criteria

At the end of each simulation, a response force win is awarded in the event that the adversary is unable to successfully sabotage all three targets due to attrition of adversary personnel and/or lack of required equipment to complete the necessary breaches or sabotage acts.

4.2.1.3. Five-Adversary Attack

The adversary timeline begins with an adversary exiting a vehicle at the front of the ECP, throwing Molotov cocktails at the face of the ECP and onto the roof, and, finally, getting back in their vehicle and detonating a large vehicle borne improvised explosive device (VBIED). These actions cause the two responders in the ECP to lock down the entrance and retreat toward the interior facility. The

Molotov cocktails are also the catalyst for the primary adversary attack from the east side of the facility. As the two responders retreat toward the main building, one adversary positioned on the east side of the PIDAS engages and kills the responders as they cross the protected area. At the same time, two adversaries begin suppressive fire on the two BBREs on the east side of the facility. This suppressive fire provides sufficient cover for an additional adversary to begin breaching the exterior fence of the PIDAS. After completing the breach of the outer fence, the same adversary crosses the isolation zone and completes a breach of the inner fence.

The breaching adversary moves through the breach and begins to cross the protected area, approaching the southeast corner of the building. As they make their approach, they cross into the field of view of a port on the northeast BBRE that cannot be suppressed by the adversaries from the east. From a stable and protected fighting position, the responder in the northeast BBRE is able to engage and neutralize the approaching adversary. Two additional adversaries cease their suppressive fire and begin to follow the first adversary through the breach and toward the southeast corner of the facility. The break in suppressive fire provides sufficient time for the responder in the southeast BBRE to engage and neutralize the two additional adversaries. The final adversary is subsequently engaged and killed by the responder in the southeast BBRE. This facility design proved to be highly effective against an adversary force of this size, preventing the adversaries from even reaching the skin of the building despite a coordinated diversionary attack and the killing of two responders posted in the ECP (Figure 17).

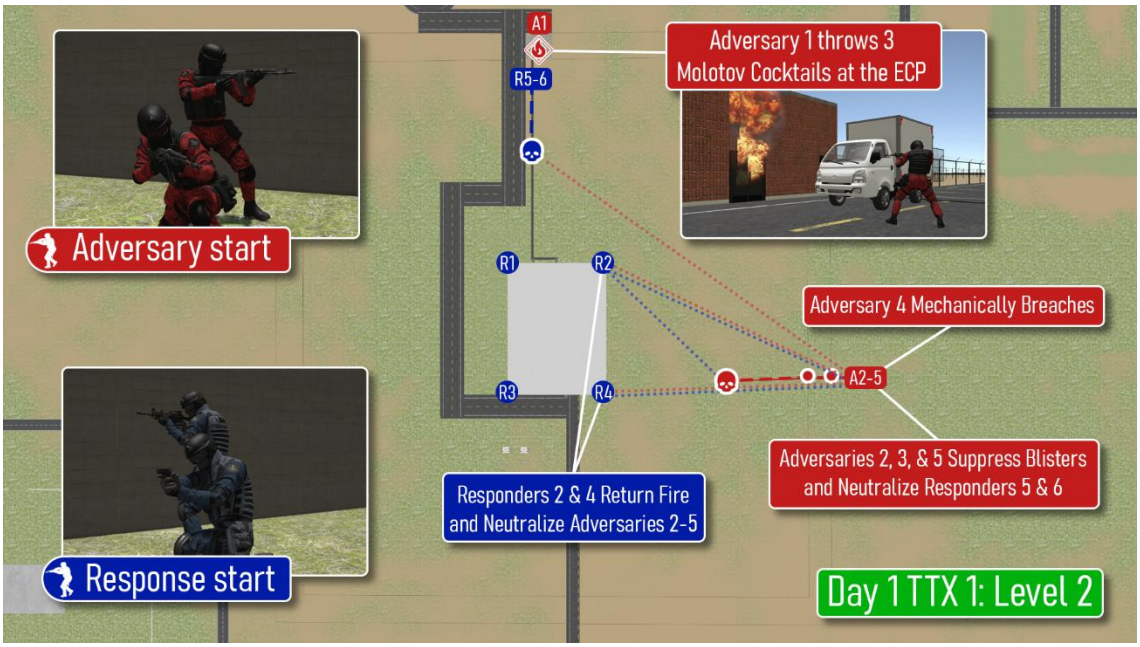

Figure 17. Five-Adversary Attack on BBRE Facility Layout

4.2.1.4. Eight-Adversary Attack

After the overwhelming success of the response against a five-adversary team, the decision was made to attempt the same style of attack with eight adversaries. The attack proceeded in the same manner as the first, not deviating in approach or results until the breach of the inner fence of the PIDAS. At this point, four additional members of the adversary team passed through the breach at the same time as the first adversary. The five adversaries then moved in a coordinated formation and used suppressive fire on both the northeast and southeast BBREs during their approach. This

allowed them to reach the skin of the building and send one adversary to detonate an explosive underneath the northeast BBRE, killing the responder inside and self-sacrificing in the process.

The two adversaries remaining at the facility perimeter were able to shift the focus of their suppressive fire to the southeast BBRE. This allowed the four adversaries that remained against the east wall of the facility to place a breaching charge on the exterior wall, retreat around the south side of the building during the detonation, and return to a successful breach into the east diesel generator and turbine room of the building. Knowing that the adversaries were breaching the east wall, the responder in the southwest BBRE moved to the reactor hall and took up a fighting position near the east stairwell. The responder in the northwest BBRE moved to the west end of the receiving area. Figure 18 shows the initial assault on the facility.

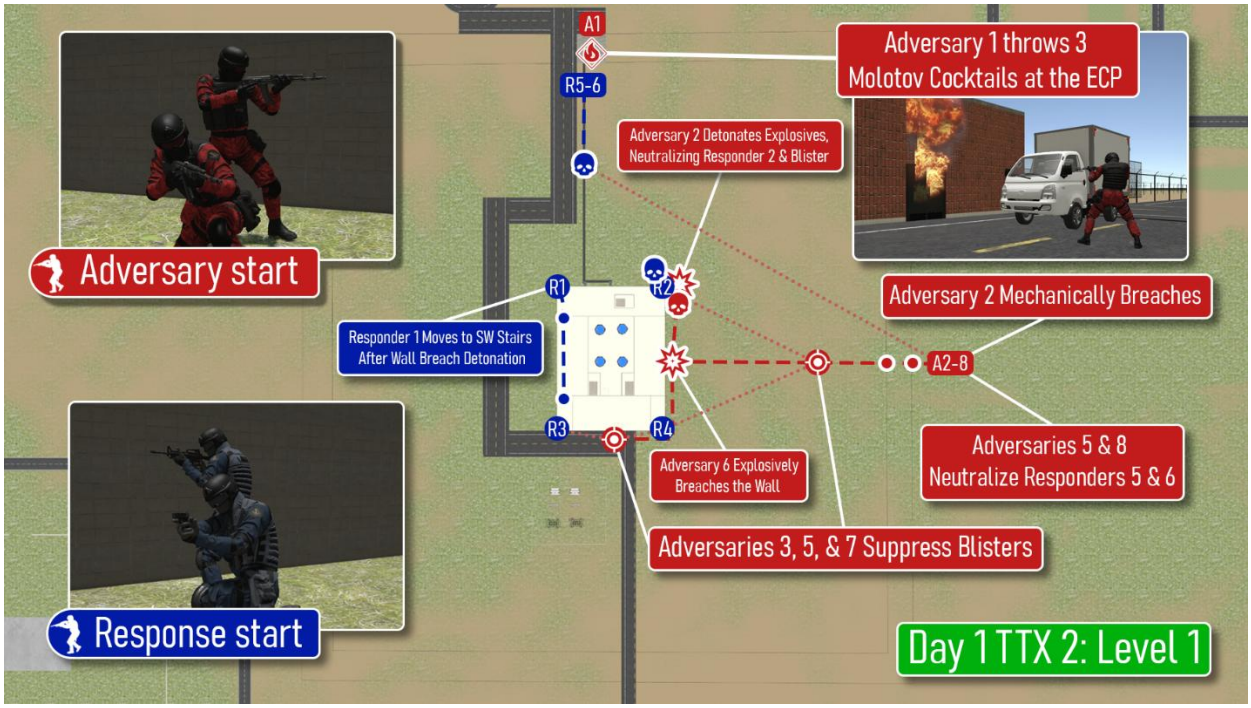

Figure 18. Eight-Adversary Attack on BBRE Layout – Initial Assault

Once inside the building, one of the adversaries began a breach of the first door enroute to the reactor hall, while another adversary placed two explosive charges on the diesel generators in the east room. The four adversaries performed two additional door breaches to advance into the receiving area, the only part of the facility with an entrance into the reactor hall. As the adversaries began their breach into the reactor hall, the CAS operator was able to provide critical information about their positions based on CCTV footage. This allowed the responder now positioned in the reactor hall to engage the adversaries through the roll-up door. During this engagement the responder from the southeast BBRE was able to advance on the east door of the receiving area and engage, killing two adversaries, but also being killed. Two adversaries remained in the receiving area and waited for the final adversary to enter the building from outside the PIDAS (Figure 18).

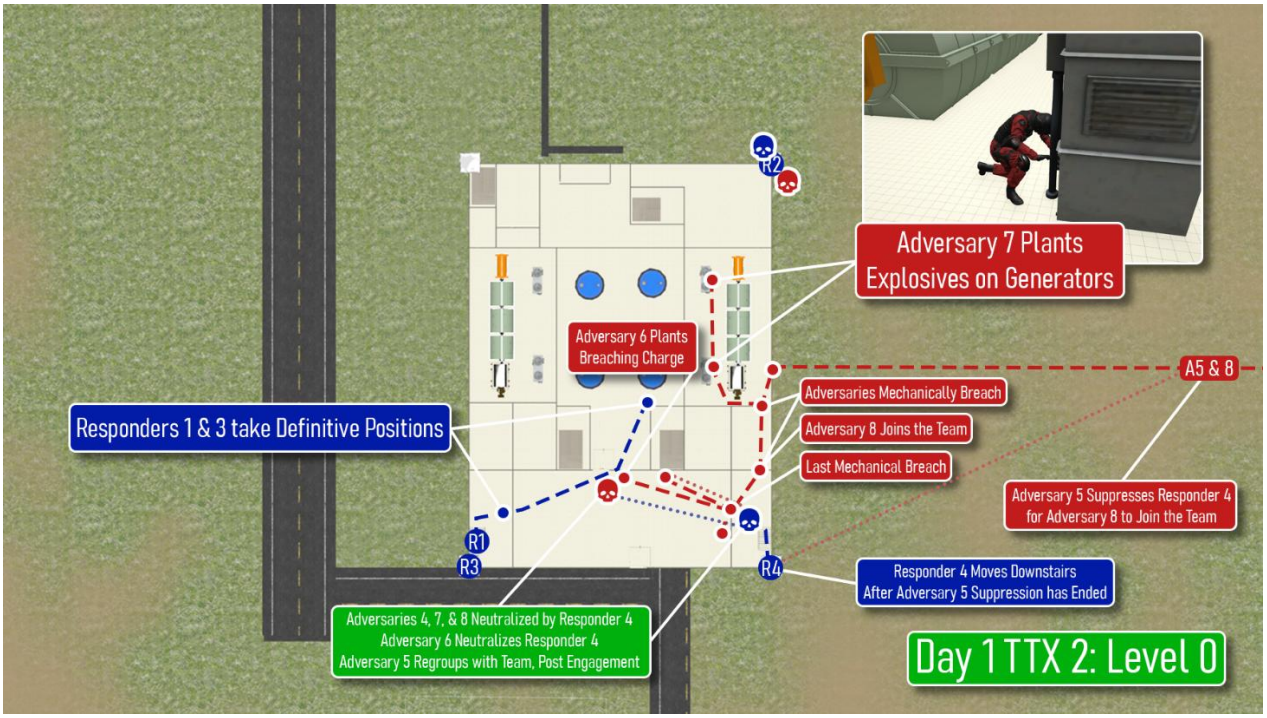

Figure 19. Eight-Adversary Attack on BBRE Layout – Facility Breach

Once the final three adversaries were gathered in the receiving area, they breached the personnel entrance into the reactor hall, threw an explosive charge into the room, killing the responder inside, and made entry. The one remaining responder moved to the reactor hall and attempted to engage but was killed by the remaining three adversaries. At this point, the three adversaries were able to complete their sabotage activities without further interruptions from response (Figure 20).

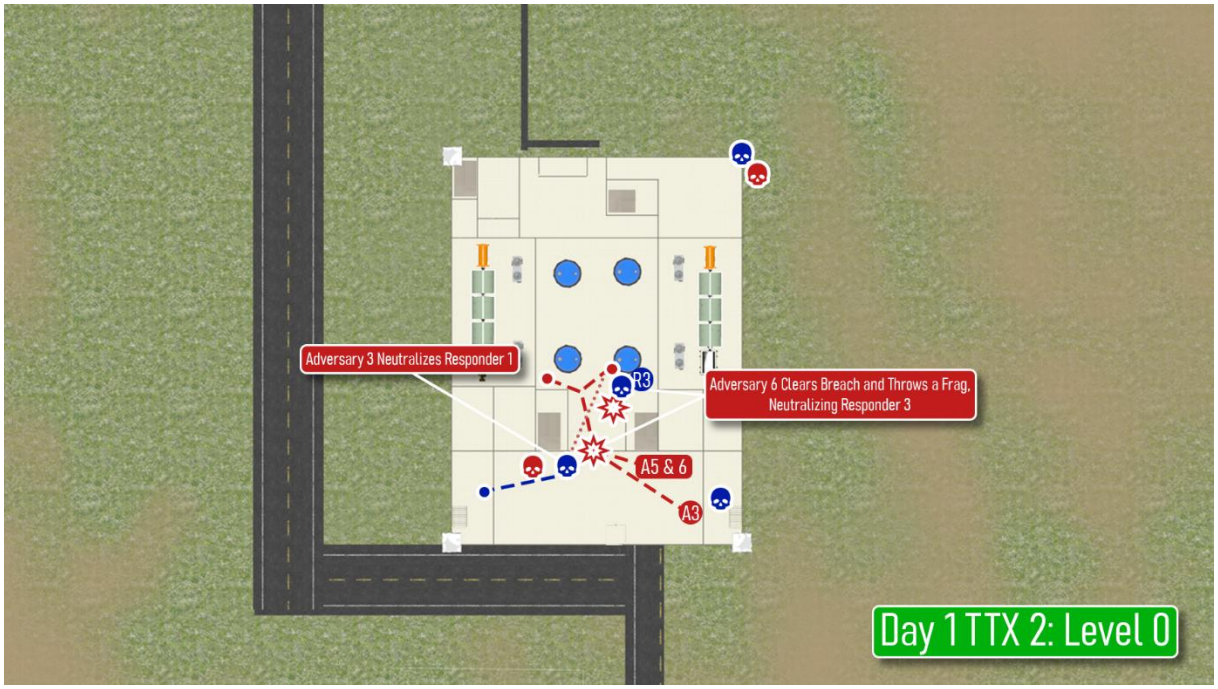

Figure 20. Eight-Adversary Attack on BBRE Layout – Response Defeat

After action review of this scenario revealed two critical weaknesses in the response posture. First, the response in the BBREs could be rendered ineffective with a coordinated barrage of suppressive fire by multiple adversaries. Second, the responders had no effective positions from which they could engage if an adversary managed to get inside the facility. Based on the findings, a new model design was developed and a scenario with eight adversaries was run against the upgraded response posture.

4.2.2. Attacks On Gun Port Facility Layout

The following sections describe the results of two adversary attack scenarios against the upgraded facility model, following evaluation of the response positioned in BBREs on the facility corners. In the new model, the BBRE "blisters" were removed from the corners and replaced with gun ports built into the exterior wall of the building. The gun ports were placed on the faces of the building as well as the corners. The gun ports on the corners of the facility were designed to project outward enough from the face of the structure to allow for ports at a 45-degree angle down to the ground. This design enabled responders to observe and engage along the skin of the building. Gun ports were placed on interior walls as well, providing fighting positions from the top security floor into the receiving area, the reactor hall, and into the stairwells to the lower levels.

4.2.2.1. Response Posture

For the gun port facility layout (Figure 21), one responder is posted in each corner of the second floor of the facility. From this position, the responder can see out of gun ports in two directions. If a port is receiving suppressive fire or becomes compromised, the responder is able to move to different gun ports along the face of the building. Their positions also provide quick access to gun ports that face into the receiving area, the reactor hall, and the stairwells leading down to the reactor containment vessels and spent fuel pool. This layout provides greater flexibility for the responders to engage both on the exterior and interior of the building without exposing themselves to ballistic attacks from adversaries. As with the previous layout, two armed responders are posted in the ECP. Finally, the armed CAS operators and the response team leader are able to leave the CAS as a last line of defense.

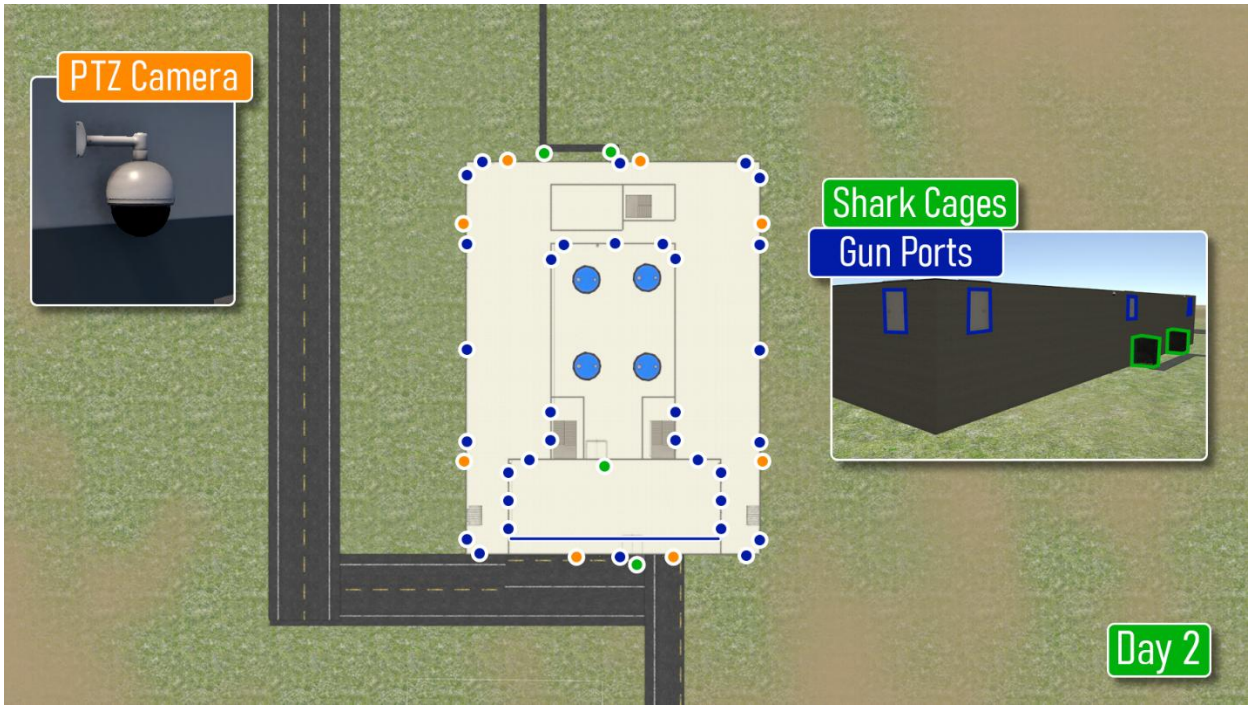

Figure 21. Facility Layout with Gun Ports

4.2.2.2. Response Force Win Criteria

At the end of each simulation, a response force win is awarded in the event that the adversary is unable to successfully sabotage all three targets due to attrition of adversary personnel and/or lack of required equipment to complete the necessary breaches or sabotage acts.

4.2.2.3. Five-Adversary Attack

The attack by five adversaries was conducted in the same manner as with the previous facility layout to ensure that new vulnerabilities had not been created in the new design. The attack unfolded in the same manner, and the adversaries were defeated as they attempted to cross the protected area between the PIDAS and the building's east face. No new vulnerabilities were discovered, and it was noted that the gun ports allowed the responders on the east side of the facility to engage earlier in the scenario, as the adversaries were not able to suppress all of the available gun ports provided in this design (Figure 22).

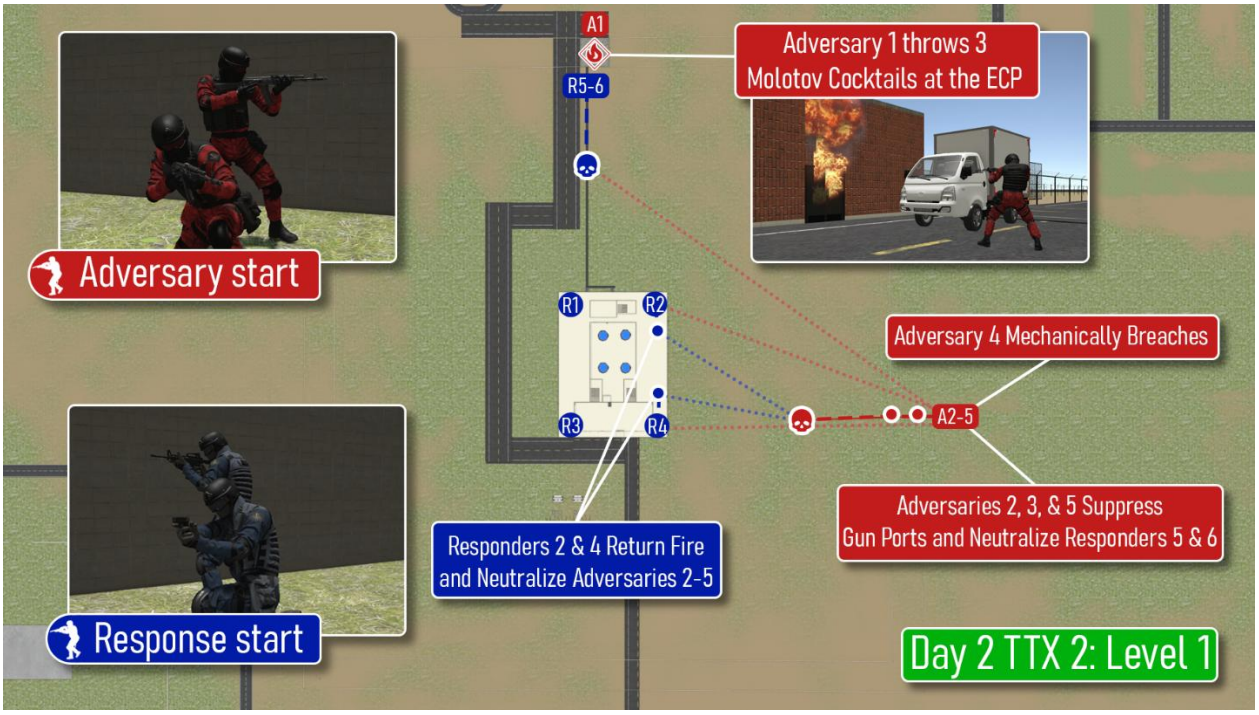

Figure 22. Five-Adversary Attack on Gun Port Facility Layout

4.2.2.4. Eight-Adversary Attack

Given the overwhelming advantage of the response over a force of five adversaries, the new facility design was subsequently tested against a force of eight adversaries. In this case, the eight adversaries attacked from the south side of the facility, attempting to use the switchyard to their advantage as concealment upon their approach to the south face of the building. The attack was initiated by four adversaries using suppressive fire against the gun ports on the southwest and southeast corners of the facility. The remaining four adversaries breached the PIDAS, approached the switchyard, and skirted around the southeast corner of the switchyard to approach the center of the south face of the building. Once at the skin of the building, the adversaries breached the roll-up door and threw an explosive charge into the receiving area in an attempt to kill or disorient any responders in the immediate vicinity.

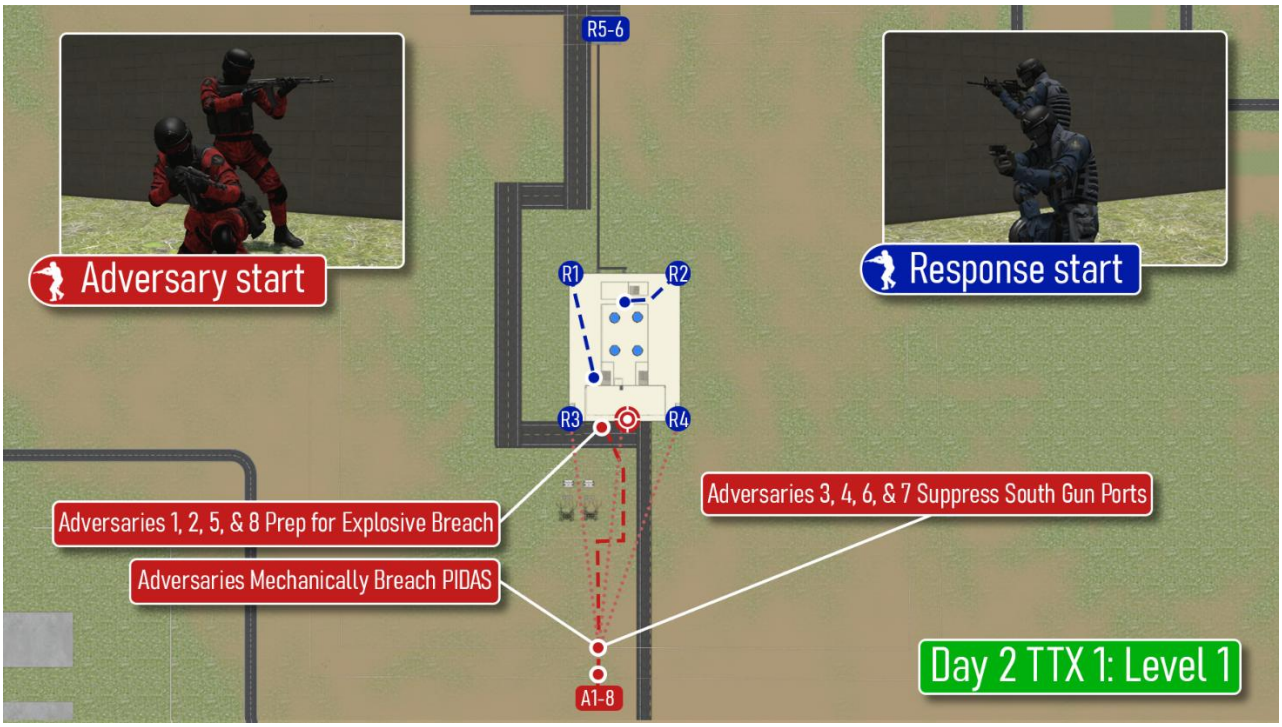

Figure 23. Eight-Adversary Attack on Gun Port Layout – Initial Assault

As the assault began on the corner gun ports of the south face of the facility, the responders in those gun ports moved to internal gun ports facing into the material receiving area, knowing that the adversaries must enter through that area in order to reach the reactor hall. They yielded the south side of the facility grounds, knowing they would have an overwhelming advantage over the adversaries as they entered the receiving area. The responders in the gun ports on the north end of the facility likewise shifted to interior posts, one running to a gun port facing the material receiving area and one to a gun port at the north end of the reactor hall (Figure 23).

When the breaching adversaries threw an explosive charge into the material receiving area, two of the responders at gun ports on the second floor were within a range such that they became disoriented for about 10 seconds. The adversaries entered the material receiving area and took positions against the wall underneath the catwalk. Faced by eight gun ports on three sides, three of the four adversaries began to suppress the gun ports to the best of their ability. As they were unable to suppress all the gun ports, one of the responders was able to engage from a gun port not being suppressed and kill three of the four adversaries. The last of the four retreated to a corner of the room but was quickly killed by the two responders who were initially disoriented by the explosive charge.

The final four adversaries approached the south end of the facility from the PIDAS. Their progress was unimpeded, as the responders remained positioned at interior posts. The four adversaries gathered at the south face of the building and tactically entered through the breached roll-up door. The responders, having been briefed by the CAS operator about the approaching adversaries, were prepared for the second wave of the assault. As soon as the adversaries entered the material receiving area, the responders on the second floor engaged from three gun ports with overlapping fields of fire and neutralized the remaining adversaries (Figure 24).

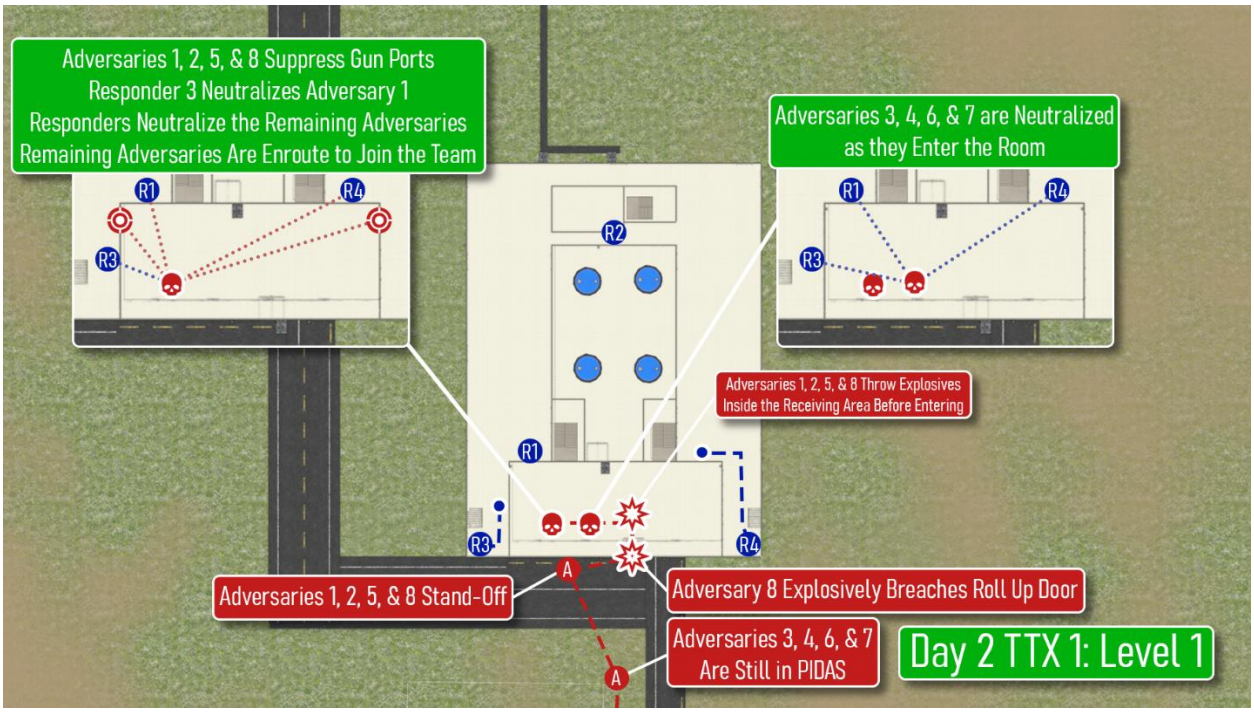

Figure 24. Eight-Adversary Attack on Gun Port Layout – Facility Breach

This design proved highly effective against a large, well-trained adversarial force. The layout funneled adversaries to a point of significant advantage for the responders. The final scenario showed that a smaller response force was able to effectively engage and defeat a larger, determined adversary armed with small-arms weapons and explosives. Further evaluation would be needed to assess the effectiveness of this physical protection system and response force against an adversary with UAS capabilities and/or rocket-propelled explosive weapons.

This page left blank

5. HYPOTHETICAL PPS COSTS AND STAFFING HEADCOUNTS

This section of the report outlines the cost to purchase the necessary security technologies for the facility designs considered in this report. It should be noted that these costs are hypothetical; may not represent today's purchase prices of technologies; and these prices do not account for installation, operation, maintenance, and testing.

5.1. Original LWSMR Design

The original LWSMR facility design with an offsite response force has similar costs for technologies as the modified LWSMR facility design. The largest cost drivers are the modular block wall, radio systems, hydraulic wedge barriers, and other elements of the security system. Additionally, the original LWSMR design integrated active delay features such as glycol foggers and slippery agent dispersal machines. This design also includes many locations with reinforced concrete for delay and the addition of person traps constructed of reinforced concrete that are not accounted for in the costs in Table 8. This table highlights the estimated security technology costs for the original design.

Table 8. Original LWSMR Security Technology Costs

Security Technology	Quantity	Unit Cost	Estimated Cost ($USD, sorted high to low)
modular block wall	385	$ 5,000.00	$ 1,925,000.00
radio system software	1	$ 970,285.13	$ 970,285.13
hydraulic wedge barriers	4	$ 150,000.00	$ 600,000.00
tri-axle camera tower	8	$ 55,000.00	$ 440,000.00
vehicle radiation detector	1	$ 372,151.00	$ 372,151.00
gravel	167	$ 1,500.00	$ 250,500.00
radio base station console	1	$ 180,000.00	$ 180,000.00
personnel radiation monitor	2	$ 86,386.00	$ 172,772.00
fencing material & gates	1.078	$ 146,886.00	$ 158,343.11
hand-held radio ultra high frequency (UHF)/very high frequency (VHF)	17	$ 5,244.33	$ 89,153.61
double stack microwave sensor	8	$ 10,017.00	$ 80,136.00
hand-held explosive detector	2	$ 30,000.00	$ 60,000.00
power-over-ethernet (POE) network switch	10	$ 5,500.00	$ 55,000.00
UPS 20 KVA	10	$ 3,420.00	$ 34,200.00
access control in/out	2	$ 16,814.00	$ 33,628.00
vehicle explosive detector	1	$ 30,000.00	$ 30,000.00
X-ray machine	1	$ 28,000.00	$ 28,000.00
NVR - 40TB storage	2	$ 14,000.00	$ 28,000.00
pole mount day/night weatherproof infrared cameras	16	$ 1,650.00	$ 26,400.00
core switch	4	$ 5,500.00	$ 22,000.00
large server rack	8	$ 2,730.00	$ 21,840.00

Security Technology	Quantity	Unit Cost	Estimated Cost ($USD, sorted high to low)
distribution switch	4	$ 5,100.00	$ 20,400.00
active infrared (IR) sensor	11	$ 1,394.00	$ 15,334.00
FDB (field distribution box)	10	$ 1,500.00	$ 15,000.00
alarm communication and display (AC&D) workstation	3	$ 4,500.00	$ 13,500.00
KVM switch	10	$ 1,175.00	$ 11,750.00
intercom server	2	$ 5,700.00	$ 11,400.00
hand geometry reader	5	$ 2,246.00	$ 11,230.00
mag lock	23	$ 435.00	$ 10,005.00
badge printer/maker	1	$ 8,646.99	$ 8,646.99
printer	1	$ 7,995.00	$ 7,995.00
fiber patch panel	10	$ 750.00	$ 7,500.00
proximity readers	24	$ 305.00	$ 7,320.00
metal detector	2	$ 3,618.00	$ 7,236.00
ACS server	2	$ 3,500.00	$ 7,000.00
controller	2	$ 3,000.00	$ 6,000.00
media convertor	4	$ 1,365.00	$ 5,460.00
intrusion detection system (IDS) server	1	$ 5,000.00	$ 5,000.00
radar	2	$ 35,000.00	$ 70,000.00
video management system (VMS) server	1	$ 5,000.00	$ 5,000.00
cooling fan	10	$ 500.00	$ 5,000.00
power supply	10	$ 450.00	$ 4,500.00
expansion module	2	$ 2,200.00	$ 4,400.00
SFP modules	20	$ 190.00	$ 3,800.00
BMS – high security BMS contact	23	$ 150.00	$ 3,450.00
gate intercom	2	$ 1,695.00	$ 3,390.00
cell phone locker	1	$ 3,017.00	$ 3,017.00
access control input/output module	2	$ 295.00	$ 295.00
raised floor for server rooms	1	$ 2,500.00	$ 2,500.00
access control rackmount enclosure w/power supplies	2	$ 1,235.00	$ 2,470.00
router	4	$ 600.00	$ 2,400.00
passive infrared (PIR) 360	22	$ 75.72	$ 1,665.84
emergency exit push button	4	$ 285.00	$ 1,140.00
hand-held radiation detector	2	$ 379.00	$ 758.00
(12) fuse outputs	10	$ 50.00	$ 500.00

Security Technology	Quantity	Unit Cost	Estimated Cost ($USD, sorted high to low)
AC&D licensing	1	$ 495.00	$ 495.00
hand-held metal detectors	2	$ 225.00	$ 450.00
bispectral pant-tilt-zoom (PTZ) camera	2	$ 28,700.00	$ 57,400.00
fiber optic patch cords	20	$ 15.00	$ 300.00
guard workstation	1	$ 285.00	$ 285.00
battery	10	$ 20.00	$ 200.00
cat-6 patch cords	40	$ 5.00	$ 200.00
glycol fogger	6	$ 4,500.00	$ 27,000.00
slippery agent dispenser	6	$ 4,500.00	$ 27,000.00
tamper switch	10	$ 15.00	$ 150.00
patch panels – 48s	4	$ 35.00	$ 140.00
duress button	3	$ 27.00	$ 81.00
Total Technology Cost			**$ 5,976,172.68**

As can be seen from Table 8 (and noted at the beginning of this section), the largest drivers of costs in this design are the vehicle barrier system and some portions of the exterior intrusion detection system. These costs are similar to the costs of the modified LWSMR facility design and onsite response strategy and may be even more similar when the costs of the additional delay barriers are included in the overall cost of the PPS.

A hypothetical staffing headcount was developed for this facility based on the PPS design. The following security positions were used for this analysis.

- Security Shift Supervisor: handles day-to-day operations of all PPS assets (testing, maintenance, evaluation, etc.), schedules force-on-force exercises, etc.
- Field Supervisor: Conducts all field operations for the PPS including, but not limited to, testing activities, training activities, maintenance activities, and installation of equipment.
- Response Team Lead: Leads the response team in all actions for responding to security events, including the implementation of compensatory measures.
- Armed Responders: Responsible for responding to security events, interrupting and neutralizing adversaries, and implementing contingency plans.
- Armed Security Officers (ASOs): Facilitate vehicle and personnel searches, escort material, conduct vital area checks, etc.

Table 9 highlights the staffing headcount to implement the PPS for the original LWSMR design. For each 24/7 position, a full time equivalent (FTE) number was identified by using a multiplier of four. These FTE multipliers are used to determine the total number of people required to implement the PPS when accounting for holidays, sick time, vacation, medical emergencies, and other factors. In this facility design, ten armed responders are used to respond to the DBT adversary attack scenarios at the facility. In addition, four ASOs were utilized. Two of the ASOs were used to oversee entry of

individuals into the protected area. The other two ASOs are utilized to perform vital area lock checks, act as rovers for the armed responders, and to conduct vehicle searches for any vehicles entering the PA.

Table 9. Original LWSMR Staffing Headcount

Position	24/7 12 hr. Rotating Shift	FTE
Security Shift Supervisor	1	4
Field Supervisor and RTL	2	8
Alarm Station Operators (CAS/SAS)	2	8
Armed Responders	10	40
ASOs	4	16
Total	**29**	**76**

5.2. Modified LWSMR

Table 10 is a summation of the costs for all security technology items associated with the physical protection system as defined for the modified LWSMR. The table is sorted by highest total cost per item. The total cost of all security technology for this design is $6,658,522.92, with the greatest cost being associated with the vehicle barrier system. The first day of scenario evaluation revolved around a model with BBREs built into the corners of the reactor building. On the second day of evaluation, the facility design was modified from one employing the use of BBREs to one incorporating smaller but better distributed gun ports that were integrated in the walls of the facility. The change from BBREs to gun ports resulted in a considerable savings of more than $8,000,000, while leading to significant improvement in the ability of responders to engage threats exteriorly and interiorly, should an adversary manage to breach into the facility. The final overall cost for the security technology in the modified LWSMR exceeded that of the original LWSMR design; however, the increased cost in technology was offset by savings in both upfront construction costs and in ongoing costs of operation, as the number of FTEs required for security was significantly reduced.

Table 10. Hypothetical Security Technology for Modified LWSMR Design

Security Technology	Quantity	Unit Cost	Estimated Cost ($USD, sorted high to low)
modular block wall	384	$ 5,000.00	$ 1,920,000.00
radio system software	1	$ 970,285.13	$ 970,285.13
hydraulic wedge barriers	4	$ 150,000.00	$ 600,000.00
bispectral PTZ camera	14	$ 28,700.00	$ 401,800.00
tri-axle camera tower	7	$ 55,000.00	$ 385,000.00
vehicle radiation detector	1	$ 372,151.00	$ 372,151.00
ball gun ports	30	$ 12,075.00	$ 362,250.00
personnel radiation monitor	2	$ 86,386.00	$ 172,772.00
gravel	167	$ 1,500.00	$ 250,500.00
corner ball gun ports	8	$ 28,500.00	$ 228,000.00
radio base station console	1	$ 180,000.00	$ 180,000.00

Security Technology	Quantity	Unit Cost	Estimated Cost ($USD, sorted high to low)
fencing material & gates	1.078	$ 146,886.00	$ 158,343.11
double stack microwave sensor	8	$ 10,017.00	$ 80,136.00
hand-held explosive detector	2	$ 30,000.00	$ 60,000.00
hand-held radio UHF/VHF	9	$ 5,244.33	$ 47,198.97
POE network switch	7	$ 5,500.00	$ 38,500.00
access control in/out	2	$ 16,814.00	$ 33,628.00
vehicle explosive detector	1	$ 30,000.00	$ 30,000.00
X-ray machine	1	$ 28,000.00	$ 28,000.00
NVR – 40TB storage	2	$ 14,000.00	$ 28,000.00
UPS 20 KVA	7	$ 3,420.00	$ 23,940.00
core switch	4	$ 5,500.00	$ 22,000.00
large server rack	8	$ 2,730.00	$ 21,840.00
distribution switch	4	$ 5,100.00	$ 20,400.00
mag lock	36	$ 435.00	$ 15,660.00
active IR sensor	11	$ 1,394.00	$ 15,334.00
monostatic microwave sensor	3	$ 4,655.00	$ 13,965.00
AC&D workstation	3	$ 4,500.00	$ 13,500.00
intercom server	2	$ 5,700.00	$ 11,400.00
proximity readers	36	$ 305.00	$ 10,980.00
FDB (field distribution box)	7	$ 1,500.00	$ 10,500.00
IDS server	2	$ 5,000.00	$ 10,000.00
VMS server	2	$ 5,000.00	$ 10,000.00
media convertor	7	$ 1,365.00	$ 9,555.00
badge printer/maker	1	$ 8,646.99	$ 8,646.99
KVM switch	7	$ 1,175.00	$ 8,225.00
printer	1	$ 7,995.00	$ 7,995.00
metal detector	2	$ 3,618.00	$ 7,236.00
ACS server	2	$ 3,500.00	$ 7,000.00
controller	2	$ 3,000.00	$ 6,000.00
BMS – high security BMS contact	36	$ 150.00	$ 5,400.00
fiber patch panel	7	$ 750.00	$ 5,250.00
shark cage	4	$ 1,306.00	$ 5,224.00
raised floor for server rooms	2	$ 2,500.00	$ 5,000.00
hand geometry reader	2	$ 2,246.00	$ 4,492.00
expansion module	2	$ 2,200.00	$ 4,400.00
cooling fan	7	$ 500.00	$ 3,500.00
gate intercom	2	$ 1,695.00	$ 3,390.00

Security Technology	Quantity	Unit Cost	Estimated Cost ($USD, sorted high to low)
power supply	7	$ 450.00	$ 3,150.00
cell phone locker	1	$ 3,017.00	$ 3,017.00
SFP modules	14	$ 190.00	$ 2,660.00
access control rackmount enclosure w/power supplies	2	$ 1,235.00	$ 2,470.00
router	4	$ 600.00	$ 2,400.00
PIR 360	26	$ 75.72	$ 1,968.72
emergency exit push button	4	$ 285.00	$ 1,140.00
AC&D licensing	2	$ 495.00	$ 990.00
hand-held radiation detector	2	$ 379.00	$ 758.00
access control input/output module	2	$ 295.00	$ 590.00
hand-held metal detectors	2	$ 225.00	$ 450.00
(12) fuse outputs	7	$ 50.00	$ 350.00
guard workstation	1	$ 285.00	$ 285.00
fiber optic patch cords	14	$ 15.00	$ 210.00
duress button	6	$ 27.00	$ 162.00
patch panels – 48s	4	$ 35.00	$ 140.00
battery	7	$ 20.00	$ 140.00
cat-6 patch cords	28	$ 5.00	$ 140.00
tamper switch	7	$ 15.00	$ 105.00
Total Technology Cost			**$ 6,658,522.92**

Table 11 highlights the staffing headcount for the modified LWSMR design. The overall staffing headcount would be identical for the gunport design or the blisters design. As the table shows, the number of security personnel is decreased by a total of six positions, which results in twenty-four fewer personnel needed to operate the PPS.

Table 11. Modified LWSMR Staffing Headcount

Position	24/7 12 hr. Rotating Shift	FTE
Security Shift Supervisor	1	4
Field Supervisor and RTL	2	8
Alarm Station Operators (CAS/SAS)	2	8
Armed Responders	4	16
ASOs	3	12
Total	**12**	**48**

Based on the overall technology costs and the staffing headcounts, the modified LWSMR facility is a more cost-effective design when considering security technologies, personnel, and reduction in

construction of the facility. This design would enable improved cost-efficiencies to be made and potentially increase the economic viability of these designs.

This page left blank

6. RECOMMENDATIONS

The latest effort to evaluate the LWSMR model focused on two different onsite strategies. The first relied on expensive BBREs built into the corners of the reactor facility. While this strategy proved effective against a small adversarial force, it did little to reduce large up-front costs. The second design eliminated the costly BBREs and replaced them with smaller, more distributed gun ports both on the exterior and interior of the facility. The gun ports, which are much less expensive, resulted in a significant reduction of $8,000,000. In addition, the gun ports greatly improved the ability of the onsite responders to engage adversaries both exteriorly and interiorly, resulting in a much more robust response, even against a larger adversary force.

The results of this evaluation led to several recommendations and conclusions:

- An onsite response force may be more cost-effective for LWSMR facilities, rather than an offsite response force.
    - An offsite response force may require more security personnel to respond to nuclear security events, therefore increasing long term costs for the facility.
    - Security technology prices are very similar for an offsite response strategy and an onsite response strategy. The costs for an offsite response force strategy may be higher when structural delay barriers are incorporated as well.
    - Additionally, NRC draft guidance may also increase the costs for using an offsite response force, especially when considering a contracted offsite response force.
- Utilizing security-by-design principles, low-cost gun ports were integrated into the facility structure and provided flexibility for response to a wide variety of threats.
    - Gun ports at exterior and interior locations can improve response capabilities and safety.
    - This provides a defense-in-depth approach to interrupt and neutralize adversaries externally and internally to the facility.
- Construct a security level at the top of a facility to provide secure, quick access for responders between different response locations and along critical pathways for the adversary to reach target locations
    - An open layout for the security floor provides clear, quick access for responders between gun ports, both interior and exterior to the facility.
    - An open concept for a security floor also reduces construction costs and provides protection for the CAS onsite.
- Minimize the below-grade footprint of the facility.
    - While there are some security benefits to locating critical infrastructure below-grade, comparable levels of security can be attained with above-grade strategies for a lower financial and logistical burden.
    - Consider the placement of only structures, systems, and components that are needed to prevent a radiological release (i.e., targets and target sets) below-grade and house all other systems above-grade. This can help reduce overall construction costs while improving security system effectiveness.

- Minimize structures within the protected area.
    - Structures surrounding the reactor building provide cover and concealment for approaching adversaries. Additionally, this may reduce the ability of the facility to ensure overlapping fields-of-fire at the perimeter of the facility.
    - By locating office buildings outside the PA, there is a reduction in the time and money spent on the insider threat mitigation or human reliability program. Additionally, this reduces the overall number of people who need to access the PA, and therefore, can reduce operational burdens and costs for the facility.

REFERENCES

[1] "U.S. Domestic Small Modular Reactor Security-by-Design." SAND2021-0768. Alan Evans, Jordan Parks, Steven Horowitz, Luke Gilbert, Ryan Whalen. https://www.sandia.gov/app/uploads/sites/273/2022/07/US_DomesticSmallModularReactorPhysicalProtectionSystemAnalysisSAND2021-0768_REV-4.pdf

[2] *President Trump Orders Department of Energy to Build Nuclear Energy Generation Capacity | Sabin Center for Climate Change Law*. climate.law.columbia.edu/content/president-trump-orders-department-energy-build-nuclear-energy-generation-capacity#:~:text=Home-,President%20Trump%20Orders%20Department%20of%20Energy%20to%20Build%20Nuclear%20Energy,Energy%20to%20advance%20this%20policy.

[3] Cook, Ellie. "Ukraine Strikes Russian Nuclear Power Plant, Moscow Says." *Newsweek*, 24 Aug. 2025, www.newsweek.com/ukraine-strikes-russian-nuclear-power-plant-says-moscow-2118411.

[4] "Scribe3D." *Modeling and Simulation Tools*, modsimtools.sandia.gov/scribe3d.

[5] Russell, John and Management Sciences Inc. (MSI). "Deliberate Motion Analytics (DMA)." *RIC Conference*, 16 Feb. 2023, www.sandia.gov/app/uploads/sites/273/2024/01/RIC-Conf-Adv-Sec-Concepts-final-02-23-2023.pdf.

[6] NRC DG-5076 "Guidance for Technology-Inclusive Requirements for Physical Protection of Licensed Activities at Commercial Nuclear Plants;" https://www.nrc.gov/docs/ML2328/ML23286A282.pdf

[7] DG-5072 "Guidance for Alternative Physical Security Requirements for Small Modular Reactors and Non-Light Water Reactors;" https://www.nrc.gov/docs/ML2326/ML23263A997.pdf