Microreactor Security-by-Design Recommendations for Domestic and International Deployments

Prepared for
U.S. Department of Energy and the National Nuclear Security Administration

Alan Evans, Matthew McCullough
Sandia National Laboratories

March 2025
SAND2025-11644R

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 & 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.

Sandia National Laboratories

EXECUTIVE SUMMARY

This report outlines methods vendors can use to incorporate security-by-design (SeBD) into their microreactor facility design to support and address security for both U.S. and international deployment. The team developed a hypothetical below-grade microreactor with a physical protection system (PPS) to protect the microreactor against acts of theft and sabotage and evaluated it against two adversary attack scenarios defined by a group of adversary subject matter experts (SMEs). The hypothetical microreactor facility consists of two distinct buildings. The first is the above-grade protected area (PA) entry control point (ECP) building, which houses security personnel responsible for conducting screenings and managing access to the PA. The second building is the reactor building, which features both an above-grade floor and a below-grade floor. Figure 2 provides a visual representation of this layout.

Figure 1. Hypothetical Microreactor Facility

The following information lists design features within the hypothetical microreactor facility and the implication of these design choices on SeBD.

- **Above-Grade Facility Functionality:**
  - Provides critical response capabilities for the microreactor.
  - Acts as a barrier against radiological release.
  - Facilitates access to the below-grade section of the microreactor.
  - **SeBD Benefit:** An empty above-grade floor creates numerous advantages for a PPS design that can lead to increased system effectiveness. These benefits include additional space for delay (which is critical in microreactor facility designs), added protection of the reactor and vital equipment from external attacks, and a barrier against radiological release.
- **Microreactor Arrival and Entry Process:**
  - New microreactors enter the facility exclusively through a roof hatch on the above-grade floor, before moving below-grade.

- The roof hatch is a moveable, reinforced concrete barrier, requiring simultaneous control by both the control room operator and the central alarm station (CAS) operator, thereby enforcing the two-person rule.
- Upon arrival, the operators lift the microreactor with a crane into the above-grade section and then securely close the roof hatch.
- **SeBD Benefit:** Placing the microreactor below-grade enables improved nuclear material accounting and control principles and ensures two-person control by requiring a multi-department approach at the facility to remove a spent reactor unit and install a fresh reactor unit. This design and process introduces more people into the control of microreactor unit movements and supports increased delay times against adversaries attempting theft of a microreactor unit.

- **Transfer to Below-Grade Facility:**
  - Once the control room and CAS operators close the roof hatch, they together open a hatch leading to the below-grade section.
  - An internal crane transfers the microreactor between the facility's floors.
  - After the microreactor is positioned below-grade, the CAS and control room operators close the hatch (the facility follows the same process in reverse for outgoing microreactor units).
    SeBD Benefit: This below-grade transfer process provides an additional layer of security for the microreactor during movement, compared to above-grade placement. The outer walls of the ground floor protect the microreactor once it enters through the roof hatch, and internal crane placements inside the facility minimize the amount of time outside personnel control the microreactor.

- **Access Control and Security:**
  - The below-grade section has a single entry point, strategically positioned behind the response force area to ensure surveillance of all personnel accessing the area.
  - Only the CAS operator and control room operator require below-grade access, as microreactors are designed to minimize onsite personnel.
  - **SeBD Benefit:** The smaller staffing levels and radiation-controlled area enable a single below-grade entry point, which results in a decrease in needed PPS technologies (i.e., CCTV cameras, intrusion detection sensors, access control devices, etc.) and forces a choke point for external adversaries attempting to enter the facility. Creating choke points for external adversaries can lead to a smaller number of onsite responders to secure the facility against a design basis threat (DBT). The decrease in technology and personnel can lead to reductions in both up-front capital costs for the security system and long-term operation and maintenance costs for the PPS.

- **Advantages of Below-Grade Placement:**
  - Provides inherent protection against large vehicle-borne explosive devices (VBEDs), reducing overpressure impact on the microreactor and its critical structures.
  - Enhances resilience against advanced threats, such as attacks by kinetic unmanned aerial systems (UAS).
  - Offers additional space for delay barriers and response positions, optimizing the effectiveness of the PPS.
  - **SeBD Benefit**: A below-grade design for a microreactor facility can help reduce the vehicle barrier system (VBS) size, which leads to a reduction in upfront security system costs and long-term operation and maintenance costs. It also creates more

space for delay barriers that can increase adversary task time or channel adversaries to reduce the overall number of responders (whether onsite or offsite). This may enable microreactor facilities to design more cost-effective security systems.

SMEs developed adversary attack scenarios, which the team analyzed in Scribe3D©, a tabletop visualization tool. The team analyzed each scenario one hundred times and individually simulated each engagement between blue team members and adversary team members one hundred times. As demonstrated in the following table (Table 1), the PPS and response strategy effectiveness increased with four armed responders posted in bullet and blast resistant enclosures (BBREs), compared to two armed responders in BBREs.

Table 1. Probability of Response Force Success based on Response Numbers

	Probability of Response Force Success	
Number of Adversaries	**Using Two Responders**	**Using Four Responders**
8	59	90
7	62	93
6	70	95
5	80	95
4	87	96

This study shows microreactor vendors should consider numerous design choices to minimize the PPS and develop response strategies to create cost-effective PPSs. These elements include, but are not limited to:

1. Considering both U.S. and international DBTs when designing the PPS to include measures that mitigate varying DBT characteristics (e.g., vehicle explosives, weapon systems, and ammunition available to different adversary teams).
2. Considering below-grade siting to reduce impacts from vehicle-borne explosives and advanced adversary capabilities such as UAS, which can help reduce the size of costly items such as VBS and protect facility personnel and radiological targets from UAS.
3. Considering designs with enough space and area for additional delay features that can be integrated with responder fields-of-view, which can improve the response force's ability to neutralize adversaries effectively, thus reducing the total number of responders necessary.
4. Considering adding delay barriers that channel adversaries into responder fields-of-fire; this, combined with adding delay that extends adversary time exposed to the responders, can support smaller response force team sizes.

These considerations can help microreactor vendors decrease security system costs both upfront and long-term for future operators and utilities.

ACKNOWLEDGEMENTS

The team would like to thank Ben Stromberg and Ian Steagall for their contributions to this work. The team would also like to thank the Department of Energy's Advanced Reactor Safeguards and Security (ARSS) program and the National Nuclear Security Administration's Office of International Nuclear Security and its International Nuclear Security for Advanced Reactors (INSTAR) program for funding this work.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS AND DEFINITIONS

Term	Definition
ARSS	Advanced Reactor Safeguards and Security
BBRE	bullet- and blast-resistant enclosure
CAS	central alarm station
CCTV	closed-circuit television
DBT	design basis threat
DMA	deliberate motion algorithms
ECP	entry control point
HGU	hand geometry unit
INS	(Office of) International Nuclear Security
NRC	Nuclear Regulatory Commission
PA	protected area
PIN	personal Identification Number
PIR	passive infrared
PPS	physical protection system
PTZ	pan-tilt-zoom
SMR	small modular reactor
UAS	uncrewed aerial system
U.S.	United States
VBED	vehicle-borne explosive device
VBS	vehicle barrier system

1. INTRODUCTION

U.S. microreactor vendors aiming to build both in the U.S. and across the world face many challenges and must evaluate how to design effective physical protection systems (PPS) for both domestic and international deployments. These challenges include understanding how the unique environment may impact the PPS design and its associated elements, regulatory environments in the U.S. versus abroad, and varying design basis threats (DBT) based on the threat landscape in potential deployment locations. Security-by-design (SeBD) can play a major role and assist vendors in designing an effective PPS for both domestic and international deployments. The following definitions apply throughout the report:

- Vendor: A microreactor designer that will sell its reactor technology to an end-user.
- Operator/utility: Companies or groups of people who will purchase a reactor technology from a vendor and run it as a power plant.

1.1. Differing Regulations

Microreactor vendors must consider the regulations and requirements as well as the overall regulatory structure for a domestic deployment versus an international one. Differing regulatory structures may impact the mechanisms through which vendors and operators engage with regulators. Vendors must engage with both the U.S. Nuclear Regulatory Commission (NRC) and the relevant international regulator early in the licensing process; in an international deployment, the microreactor vendor should work with the international license applicant to coordinate with the regulator and ensure both exchange the necessary information.

U.S. regulatory requirements for response force implementation may differ from those in other countries. Some countries may prohibit the use of private onsite response forces or even local law enforcement as an onsite response force at a nuclear facility. In some cases, higher government authorities define these regulatory requirements, rather than the competent authority. Using an onsite rather than an offsite response force may dramatically shift the overall PPS design. An onsite response force will have a much shorter response time than an offsite response force, meaning the PPS design can include shorter detection and delay timelines than required for an offsite response. Additionally, an offsite response force will have to deploy and arrive at the site, provide an initial containment of the scene, and control the perimeter of the facility. After they arrive at the facility, the response team will develop a tactical response plan, and then, finally, implement the plan. To delay adversaries long enough for either interruption or neutralization, planners and designers must allocate sufficient delay time based on the overall time needed for a response team to arrive and conduct these activities. In contrast, onsite response results in decreased time to interrupt an adversary.

1.2. Differing Design Basis Threats

The DBT and regulatory requirements primarily drive PPS design. The U.S. NRC DBT likely differs from other countries' DBTs, which will impact the overall design of the PPS, including all three functions of detection, delay, and response. In addition to the three functional areas, different DBTs will impact things such as vehicle barrier design; vehicle barrier construction; blast-resistant materials; and even the location of key components of the PPS, such as the central alarm station (CAS), response force locations, types and number of intrusion detection technologies, types of closed-circuit television (CCTV) cameras, access control features, and insider threat mitigation approaches. This section touches on adversary numbers, response force requirements and scaling, and vehicle barrier system (VBS) considerations in the DBT.

The DBT should identify the total number of adversaries the PPS must protect against. Changing this number will impact the overall PPS design, the response strategy used to defend the facility, and delay measures implemented at the site. As the adversary force size increases, the protection strategy may have to change to effectively interrupt and neutralize the adversary force. **Microreactor vendors should consider coordinating with the international operator to identify DBT considerations for the design of the PPS.** The earlier the microreactor vendor identifies the differences between the U.S. DBT and the relevant international DBT, the better they can assess the impacts and necessary PPS design changes for both U.S. and international deployments.

Generally, as the number of adversaries increases, the number of responders needed to interrupt and neutralize the adversary team will increase. The one-to-two principle, where for each adversary attempting a malicious act at a facility, two responders are needed to ensure effective neutralization or interruption, formalizes this generalization. Historically, facilities have implemented this principle, but it may not be applicable based on technological advancements and facility PPS design and response strategies. For example, if the microreactor vendor integrates the facility and PPS design to create paths that force adversaries into advantageous positions for the response force (channeling adversaries for increased probability of neutralization), the site can reduce the total number of responders. As an example of technological advancements, responders or CAS operators could use video motion detection (VMD) cameras to accurately determine the location of adversaries and more effectively direct a response to an adversary incursion. Additionally, different adversary numbers can change the number of weapons, the total weight of explosives, and the difference of total tools available to the adversary group committing a malicious act. When varying deployment locations indicate differences in these adversary numbers and tools, microreactor vendors must change the PPS design to ensure effective detection, delay, and response to adversary threats. For example, if the adversary team has more explosive charges due to a different DBT, vendors may need to change the delay barrier design for that deployment to account for this increased level of explosives.

Microreactor vendors should also consider the type of vehicles included in both the U.S. and relevant international DBTs and the weight of explosives that can be carried in each vehicle. If one DBT vehicle is smaller than the other DBT vehicle, a VBS designed for the larger vehicle may be able to defend against both. Microreactor vendors should evaluate the DBTs to include the size, speed, and explosive-carrying weight of the vehicles when designing their PPS. The larger the vehicle-borne explosive device (VBED) carried by the DBT vehicle, the larger the standoff distance necessary to ensure the protection of vital areas, targets, necessary security equipment, and personnel at the facility. A vendor should consider designing for the most conservative vehicle and DBT (i.e., larger vehicle and larger VBED) and make changes for smaller DBT considerations, rather than starting with the requirements for the smaller DBT and redesigning for the larger.

1.3. Differing Deployment Locations

Microreactor vendors looking at deployments both in the U.S. and internationally must also consider how their PPS design will handle varied environmental and weather conditions. The environmental conditions can impact many of the design choices made by microreactor vendors, including the selection and operation of intrusion detection sensors, use and operation of vehicle barriers, external delay barriers, external response positions, response force strategy and movements, transportation security, and the ability for an offsite response force to respond to a security event. When evaluating various deployment locations, vendors must consider the potential impact on several other factors, including staffing for the facility and security system, as well as the logistics involved in transporting the microreactor and delivering spare parts and inventory.

Weather and environmental variations between deployment locations may necessitate using different external intrusion detection sensors, influenced by factors such as waterfall, snowfall, sunlight, wind, and other conditions. For instance, pooling water may trigger high nuisance alarms for microwave sensors deployed in exterior environments, and significant snowfall accumulation may also lead to high nuisance alarms or sensor malfunctions. Vendors can include mitigation measures based on the facility location and design to ensure proper drainage from water or snow melt to minimize nuisance alarms. Additionally, the design of intrusion detection systems (IDS) at each site may differ due to various factors including sunrise and sunset times. These can cause nuisance alarms on some exterior sensors such as active infrared sensors and affect the visibility of CCTV cameras when sunlight enters the camera's field of view. Microreactor facility designers and vendors should acknowledge these impacts, recognizing that designs may need to be adapted depending on the environmental and weather conditions at each deployment location.

Other challenges unique to individual deployment locations include the transportation of new microreactor units, response times for offsite response forces (if offsite response forces are permitted), staffing for facility operations, and security system staffing. Response times for offsite forces or supplemental local law enforcement can vary significantly across different sites. For instance, a microreactor located remotely may require longer response times compared to one situated near an urban area with quicker access to offsite response forces. Additionally, staffing a remote microreactor facility, including hiring adequate personnel for security roles, might be difficult due to a limited pool of qualified individuals. This shortage can affect the ability to fully staff the security system, taking into account factors like sickness, holidays, vacation, and work-hour regulations. Vendors should integrate all these considerations into the design of the security system and facility, as well as their operations, to ensure effectiveness and resilience.

2. HYPOTHETICAL MICROREACTOR FACILITY

The hypothetical microreactor facility developed for this design and analysis integrates features and capabilities of multiple international microreactors. The team engineered it to achieve the smallest PPS footprint and require the smallest number of security personnel necessary to defend against a wide range of adversaries using an open-source DBT. This facility serves as a simplified model to demonstrate SeBD concepts for a microreactor facility. This hypothetical setup excludes many operational components to minimize the sensitivity of the analysis and ensure the protection of actual operating microreactors.

2.1. Climate and Environmental Considerations

The following points summarize the environmental conditions of the region where the hypothetical microreactor sits, highlighting key climate and environmental factors that could impact facility operations and security:

- Climate Characteristics:
  - Cooler and wet overall climate
  - Summers: Comfortable and cloudy
  - Winters: Frigid, snowy, partly cloudy
- Temperature Details:
  - Warm season: May to early September
  - Average daily high above 73°F
  - Cold season: September to March
  - Average daily high below 16°F
  - Rarely exceeds 70°F, ensuring infrared technologies remain unaffected
- Precipitation and Humidity:
  - Low humidity levels generally
  - Annual precipitation:
    - Rain: 12 inches
    - Snow: 61 inches
- Potential Impacts on Security:
  - Precipitation may induce sensor noise
  - Risk of degradation in security elements due to:
    - Mold
    - Rust
    - Mineral deposits
    - Electrical shorts

2.2. Buildings and Microreactor Operations

The hypothetical microreactor facility consists of two distinct buildings. The first is the above-grade protected area (PA) entry control point (ECP) building, which houses security personnel responsible for conducting screenings and managing access to the PA. The second building is the reactor building, which features both an above-grade floor and a below-grade floor. Figure 2 provides a visual representation of this layout.

Figure 2. Hypothetical Microreactor Facility

The following information lists design features within the hypothetical microreactor facility and the implication of these design choices on SeBD.

- Above-Grade Facility Functionality:
    - Provides critical response capabilities for the microreactor.
    - Acts as a barrier against radiological release.
    - Facilitates access to the below-grade section of the microreactor.
    - SeBD Benefit: An empty above-grade floor creates numerous advantages for a physical protection system (PPS) design that can lead to increased system effectiveness. These benefits include additional space for delay (which is critical in microreactor facility designs), added protection of the reactor and vital equipment from external attacks, and a barrier against radiological release.

- Microreactor Arrival and Entry Process:
    - New microreactors enter the facility exclusively through a roof hatch on the above-grade floor, before moving below-grade.
    - The roof hatch is a moveable, reinforced concrete barrier, requiring simultaneous control by both the control room operator and the CAS operator, thereby enforcing the two-person rule.
    - Upon arrival, the operators lift the microreactor with by a crane into the above-grade section and then securely close the roof hatch.
    - SeBD Benefit: Placing the microreactor below-grade enables improved nuclear material accounting and control principles and ensures two-person control by

requiring a multi-department approach at the facility to remove a spent reactor unit and install a fresh reactor unit. This design and process introduces more people into the control of microreactor unit movements and supports increased delay times against adversaries attempting theft of a microreactor unit.

- Transfer to Below-Grade Facility:
  - Once the control room and CAS operators close the roof hatch, they together open a hatch leading to the below-grade section.
  - An internal crane transfers the microreactor between the facility's floors.
  - After the microreactor is positioned below-grade, the CAS and control room operators close the hatch (the facility follows the same process in reverse for outgoing microreactor units).
    SeBD Benefit: This below-grade transfer process provides an additional layer of security for microreactors during movement, compared to above-grade placement. The outer walls of the ground floor protect the microreactor, and once it enters through the roof hatch internal crane placements inside the facility minimize the amount of time outside personnel control the microreactor.

- Access Control and Security:
  - The below-grade section has a single entry point, strategically positioned behind the response force area to ensure surveillance of all personnel accessing this area.
  - Only the CAS operator and control room operator require below-grade access, as microreactors are designed to minimize onsite personnel.
  - SeBD Benefit: The smaller staffing levels and radiation-controlled area enable a single below-grade entry point, which results in a decrease in needed PPS technologies (i.e., CCTV cameras, intrusion detection sensors, access control devices, etc.), and forces a choke point for external adversaries attempting to enter the facility. Creating choke points for external adversaries can lead to a smaller number of onsite responders to secure the facility against a DBT. The decrease in technology and personnel can lead to reductions in both up-front capital costs for the security system and long-term operation and maintenance costs for the PPS.

- Advantages of Below-Grade Placement:
  - Provides inherent protection against large vehicle-borne explosive devices (VBEDs), reducing overpressure impact on the microreactor and its critical structures.
  - Enhances resilience against advanced threats, such as attacks by kinetic UAS.
  - Offers additional space for delay barriers and response positions, optimizing the effectiveness of the PPS.
  - SeBD Benefit: A below-grade design for a microreactor facility can help reduce the VBS size, which leads to a reduction in upfront security system costs and long-term operation and maintenance costs. It also creates more space for delay barriers that can increase adversary task time or channel adversaries to reduce the overall number of responders (whether onsite or offsite). This may enable microreactor facilities to design more cost-effective security systems.

3. MICROREACTOR FACILITY PPS DESIGN

The proposed PPS design focuses on achieving significant reductions in both up-front and long-term operational costs. Microreactors used for power production encounter distinct challenges compared to other small modular reactor (SMR) designs and the existing fleet of traditional large light water reactors (LLWRs). Due to their lower power output, microreactors may face more stringent limitations related to operational expenses, to include the PPS and required number of armed responders. The PPS outlined and evaluated in this study aims to demonstrate a design that offers a high likelihood of successfully countering potential adversary threats while also minimizing initial and ongoing costs. The following key assumptions form the basis of this hypothetical design:

1. Allowance for below-grade siting
2. Sufficient standoff distance outside the perimeter for extended detection technologies (e.g., deliberate motion analytics [DMA])
3. Exemptions from various regulatory statutes

3.1. Exterior Intrusion Detection System Design

The exterior IDS in this hypothetical design includes DMA; to support this, the facility would place sensors on two opposite corners of the microreactor building to provide detection and assessment. The team implemented DMA[1] to reduce the necessary infrastructure required for deploying a PPS. DMA utilizes motion tracking algorithms, radar detection technologies, and pan-tilt-zoom (PTZ) cameras to identify alarm sources and distinguish between nuisance alarms and actual adversaries. This technology may reduce the necessary security infrastructure and improve the effectiveness of alarm station operators in identifying threats to a facility by reducing the potential sources of nuisance alarms. DMA builds on object tracking toward a secure area (i.e., protected area boundary) and slewing the PTZ camera to determine the cause of that object's movement. In testing configurations, DMA has reduced overall nuisance alarms and requires a smaller infrastructure for communications and power, compared to traditional exterior IDS. Ultimately, using this technology may reduce costs compared to current IDS designs. Figure 3 shows the locations of DMA stations at the hypothetical facility.

[1] "A Novel Architecture for Intrusion Detection Based on 'Deliberate Motion Analytics.'" John Russell, et.al. Sandia National Laboratories. SAND2022-4542C

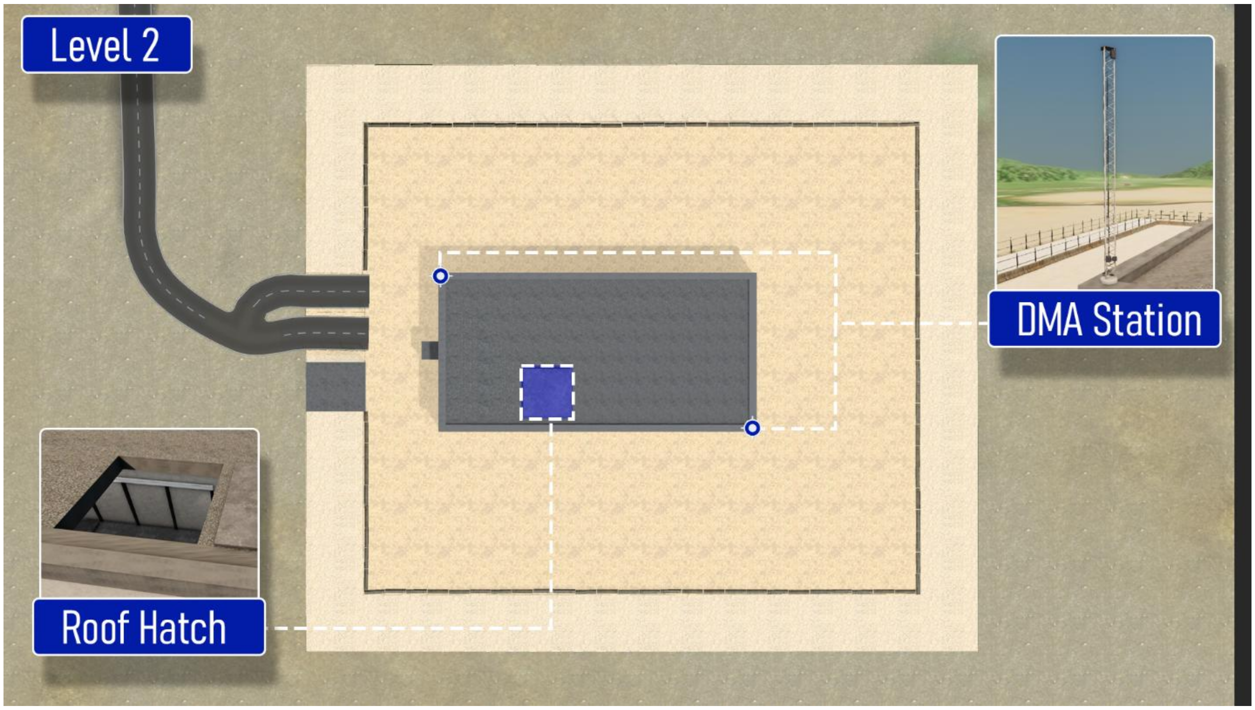

Figure 3. DMA Application

Figure 4 highlights the radar (notional) and PTZ camera (notional) for this DMA station.

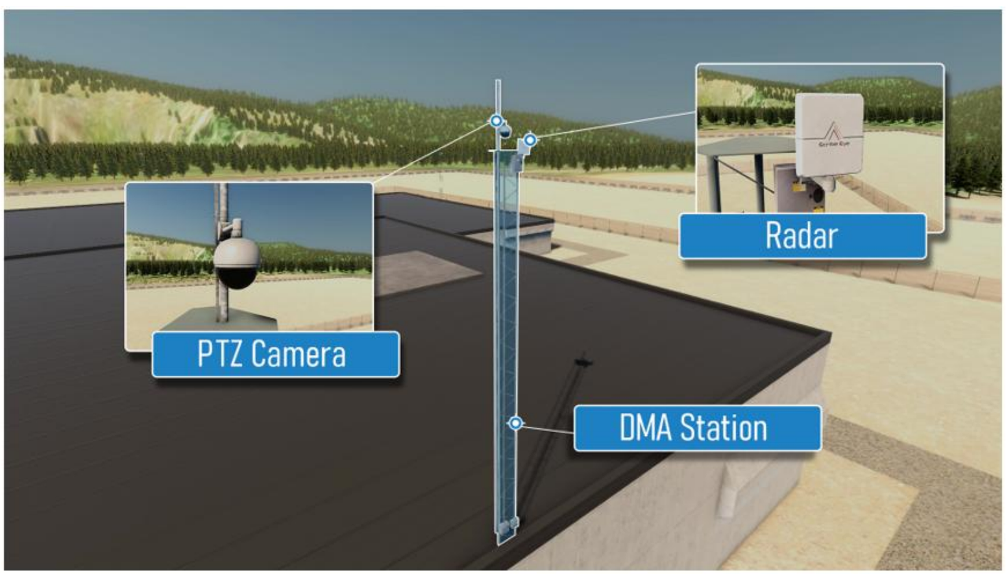

Figure 4. DMA Station Breakdown[2]

[2] "U.S. Domestic Molten Salt Reactor: Security-by-Design." Alan Evans, et. al. Sandia National Laboratories. SAND2023-09146R

3.1.1. *Intrusion Detection Systems for Microreactors*

Microreactor facilities face many difficult challenges when implementing an IDS, including the costs of the following:

- Purchasing and installing the IDS,
- Implementing compensatory measures when needed, and
- Conducting long-term maintenance.

Impacts to the cost of an exterior IDS include trenching power and communication to the sensors outside of the protected area boundary, implementing multiple lines of detection, and maintaining and testing these technologies. Microreactor vendors are considering unique and novel technologies such as DMA, radar, and lidar to potentially reduce costs for an exterior IDS. However, when relying on these technologies, operators may face difficulties implementing compensatory measures when they fail. Compensatory measures may require the use of facility personnel to detect and assess potential incursions into the facility. Using personnel as compensatory measures may lead to cost overruns, thereby increasing the overall cost of the PPS. Additionally, implementing a traditional exterior IDS that utilizes multiples lines of sensors and assessment capabilities can incur costs. The more technologies a vendor implements in the IDS design, the more performance tests and maintenance activities required of the facility to ensure the effectiveness of the IDS. Vendors must consider all of these factors when choosing their final intrusion detection system design.

3.2. Delay Barriers

The first delay barriers adversaries encounter are at the microreactor building exterior. Adversaries must breach the external walls or the external doors that allow entry into the microreactor building. The exterior building walls incorporate a 2-foot-thick, reinforced concrete wall with a complex rebar lattice structure. These reinforced concrete walls require an external adversary team to breach through using some of their explosive breaching and other tool resources. Metal security doors comprise the external doors of the facility. These doors lock from the inside using magnetic locks (and physical locks for power loss) and require breaching or power tools to access. In the event of a a loss of power, the doors physically lock from the inside. Emergency crash bars exist on the inside of the door to enable egress from the facility in a safety or emergency event. To access any exterior door, individuals must present a proximity badge and correct personal identification number (PIN) to a badge and PIN reader at the door and then use the hand geometry unit (HGU) to enter into the facility. Figure 5 shows these PPS measures at exterior doors.

Figure 5. Exterior Door Physical Protection Measures

The team included “shark cages” on the interior sides of doors entering the facility. Shark cages are enclosed structures made of turbine grating and anchored into the wall. This design places the shark cages on the interior of doors, since the response force sits interior to the microreactor building. These shark cages present a unique challenge to an adversary force in that they require precise breaching to correctly defeat the barrier, and once defeated, “channel” the adversaries, which aids the response force inside the microreactor building. This creates delay for the adversary team, and the complexity of the breach provides an opportunity for the response force to engage the adversaries while they have no cover or concealment.

Facility personnel process through the shark cages by placing their proximity badge and PIN into a badge and PIN reader at the shark cage door. The shark cage doors include crash bars on the protected side that facilitate quick egress from the facility. The shark cage doors lock with both magnetic locks and a cypher lock. The magnetic locks will unlock when personnel use a correct badge and PIN at the badge and PIN reader. In the event of loss of power, the shark cage locks using a cypher lock and only facility personnel with a need to access inside the reactor building know the code. The arrows in Figure 6 show the shark cage placement at both entrances into the above-grade floor of the microreactor building.

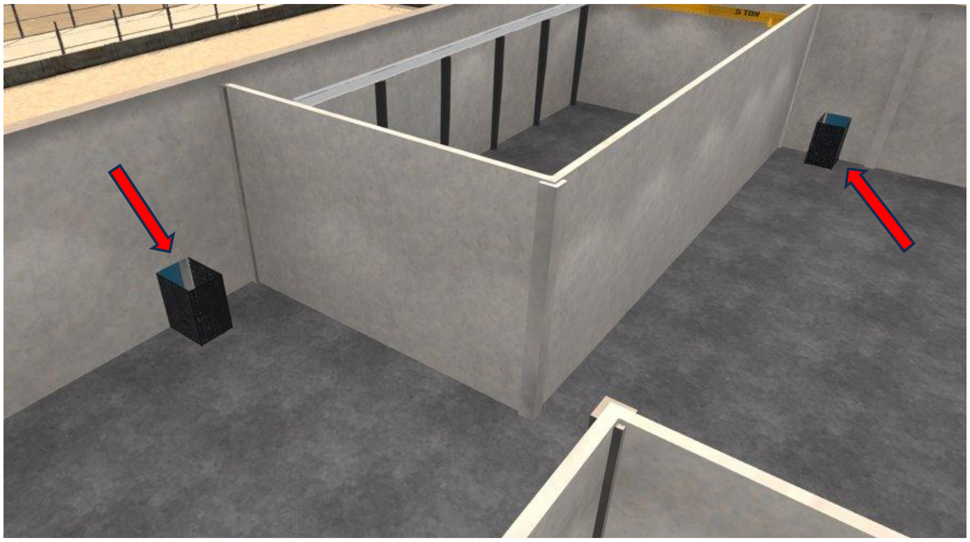

Figure 6. Shark Cage Applications

To access the below-grade portion of the microreactor building, individuals must pass through a vault-type door secured with a badge and PIN reader and an HGU. The CAS operator applies an initial screening measure at this location using a facial recognition camera placed above the vault-type door, which allows them to confirm the identity of the individual based on the facial recognition and the badge presented to the badge and PIN reader. A magnetic lock also secures the vault-type door, and only the CAS operator can unlock it. The facility may need to implement compensatory measures if power fails for an extended period. Additionally, a power loss will force the magnetic lock to fail, enabling safe egress from the facility. Figure 7 shows this application.

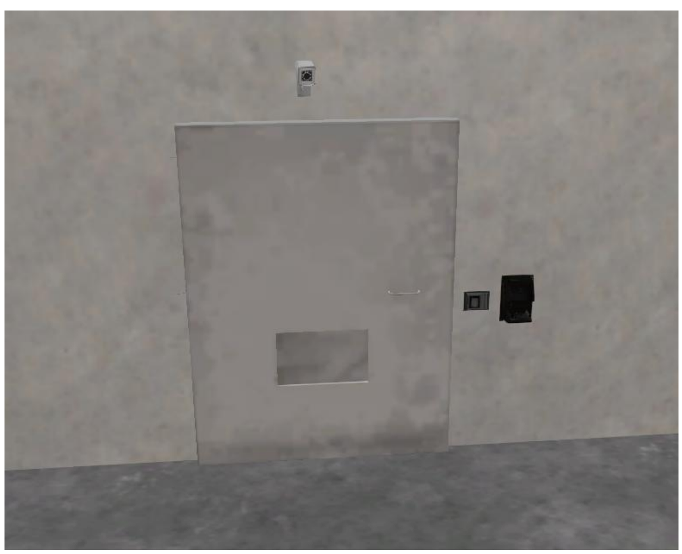

Figure 7. Below-Grade Entrance Location

Once an individual enters through this door, they must proceed below-grade using a stairwell. This stairwell includes a passive infrared (PIR) sensor that detects movement from above-grade to below-grade. Figure 8 represents the sensor coverage provided by the PIR in the stairwell.

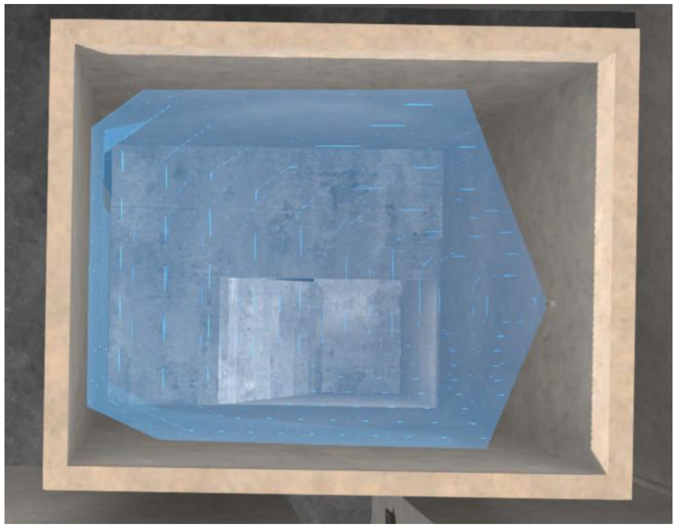

Figure 8. Stairwell PIR

A shark cage also protects the below-grade stairwell. This shark cage includes a magnetic lock, which requires a badge and PIN reader for access. If power fails for an extended period, the facility can physically lock the shark cage. Similar to all other shark cages, a crash bar exists to facilitate quick egress in an emergency situation. Figure 9 shows this below-grade shark cage.

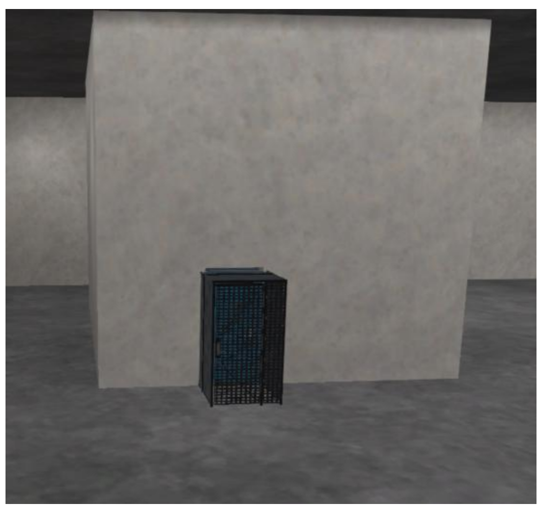

Figure 9. Below-Grade Stairwell Exit Shark Cage

3.2.1. Delay Barriers for Microreactors

Microreactor vendors should consider many forms of delay barriers for their design, including both active and passive options. Vendors may find passive delay barriers more cost-effective compared to active delay barriers. Once installed, passive delay barriers remain in place at all times and should fail secure. Passive barriers represent a one-time cost for the facility and may not require performance testing to validate the associated delay time. Active barriers (such as smoke, obscurants, slippery agents, etc.) may act as delay multiplication factors and multiply the task time for an adversary to penetrate a passive delay barrier. Applied in small spaces, these active delay features increase the overall adversary task time to penetrate a barrier. When used with fixed barriers and in conjunction with a well-designed response force, these active barriers can improve the response force's ability to interrupt and neutralize an adversary force. However, active barriers may increase operational and maintenance costs to ensure their functionality. For example, the security plan for the facility may require frequent operational testing of an active barrier that dispenses cold smoke to ensure it functions properly.

3.3. Response Strategy

The response force strategy considers two internal blast- and bullet-resistant enclosures (BBREs). The design for internal BBREs positions must protect the responders inside the BBREs and ensure they can neutralize an adversary force. The team designed each position to be blast resistant from potential explosives used by adversaries internally, an external large VBED, and explosives applied to exterior walls. The BBRE encloses the responders on all four sides and includes two fighting ports on each side and in the door. This design supports the flexibility to add more responders into the BBRE if necessary to improve the likelihood of effective neutralization of an adversary force. Figure 10 shows the location of these BBREs.

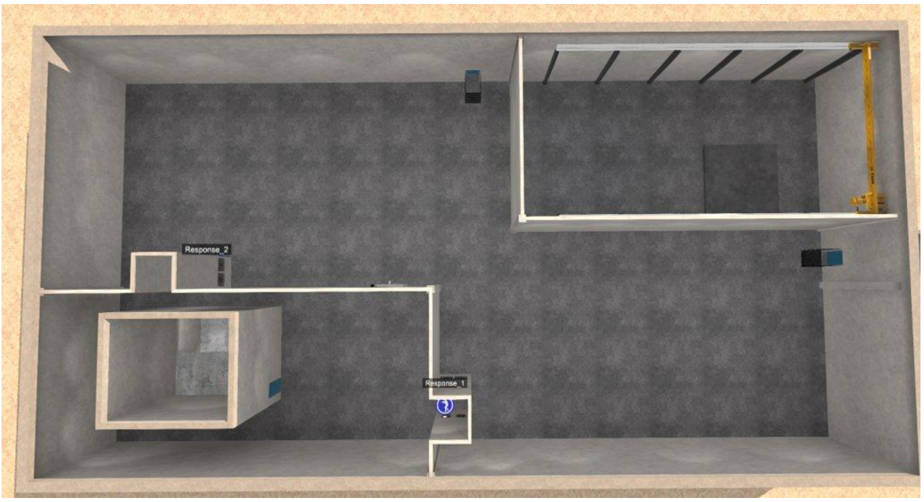

Figure 10. Above-Grade Response Force Strategy

Figure 11 shows multiple fighting ports on one face of the BBRE.

Figure 11. Fighting Ports on BBRE Face

Figure 12 shows a representative example view of a BBRE fighting port that enables the response force to visualize and engage an adversary who enters the building and remains in the shark cage.

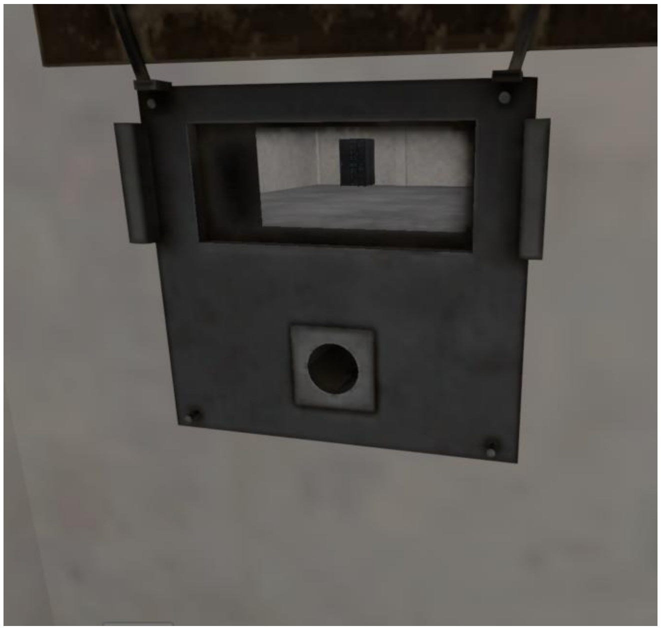

Figure 12. Representative View from BBRE Fighting Ports

Figure 13 shows the location of the CAS operator and response team leader (RTL). These locations also include fighting ports they can use to engage an adversary that enters the below-grade portion of the facility.

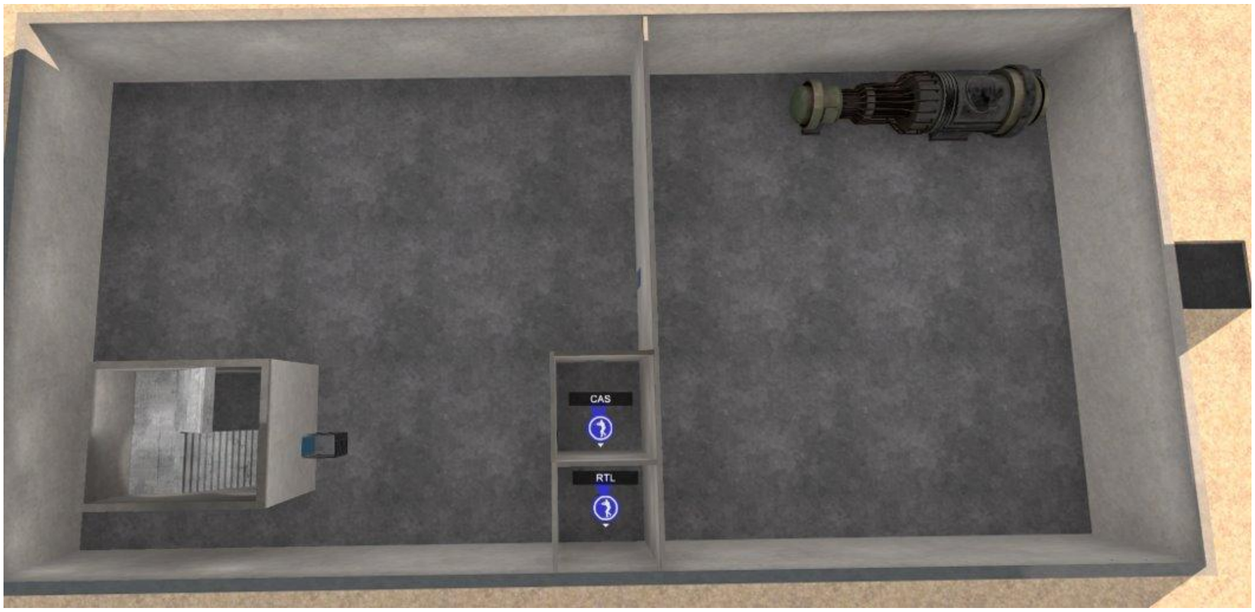

Figure 13. Potential Response Defense-in-Depth

3.3.1. Response Strategies for Microreactors

Microreactor facility vendors should consider multiple options for response strategies, including an onsite or offsite response force and a denial of task or a denial of access strategy. This report considers an onsite response force implementing a denial of access strategy, which means the response force and PPS are designed to prevent adversaries from accessing the target location and microreactor facility below-grade. When facilities use an offsite response force, they most commonly implement a denial of task strategy. A PPS design that considers an offsite response force aiming to implement a denial of access strategy will require significant delay. Implementing the necessary delay and associated robust IDS to support this strategy will likely increase overall costs. A denial of task strategy implemented with an offsite response force may not need as many delay barriers or as much delay time as a denial of access strategy with the same offsite response force.

A microreactor facility will face many tradeoffs when considering the type of response force for the facility. An offsite response force may come with costs associated with contracting an offsite law enforcement agency (unless the response force is provided by the national government), but an onsite response force will also encounter contracting costs. **When considering the response force strategy, vendors and utilities must consider offsite versus onsite costs. Offsite response includes both the costs associated with the increased delay requirements and the costs of the response force itself. In contrast, onsite response costs include training and implementation.**

To ensure the PPS effectively mitigates the DBT, microreactor vendors and utilities must also consider the *integration* of IDS, delay barriers, and response strategy. Integrating detection, delay, and response can lead to the most cost-effective PPS designs. One aspect of this includes defining how an integrated detection, delay, and response can effectively act as a compensatory measure for a failed function at the facility. For example, when a delay barrier fails or a portion of the IDS fails, members from the response force or security personnel may function as a compensatory measure. Microreactor vendors can develop a cost-effective, robust PPS design when considering these elements and measures holistically.

4. MICROREACTOR PPS ANALYSIS

This analysis considered two separate adversary attack scenarios developed by SMEs who have experience with force-on-force and tabletop exercises for operational nuclear facilities. The analysis conducted and described in this section only considers engagements between armed responders and armed adversaries, as the security plan for this facility does not include the RTL and CAS operator as official armed responders.

4.1. Attack Scenario One

The first attack scenario considered a group of 4-to-8 adversaries attacking through one entry door into the microreactor facility above-grade. The adversaries make entry into the building and try to proceed below-grade using the stairwell. Figure 14 highlights the start of this attack scenario.

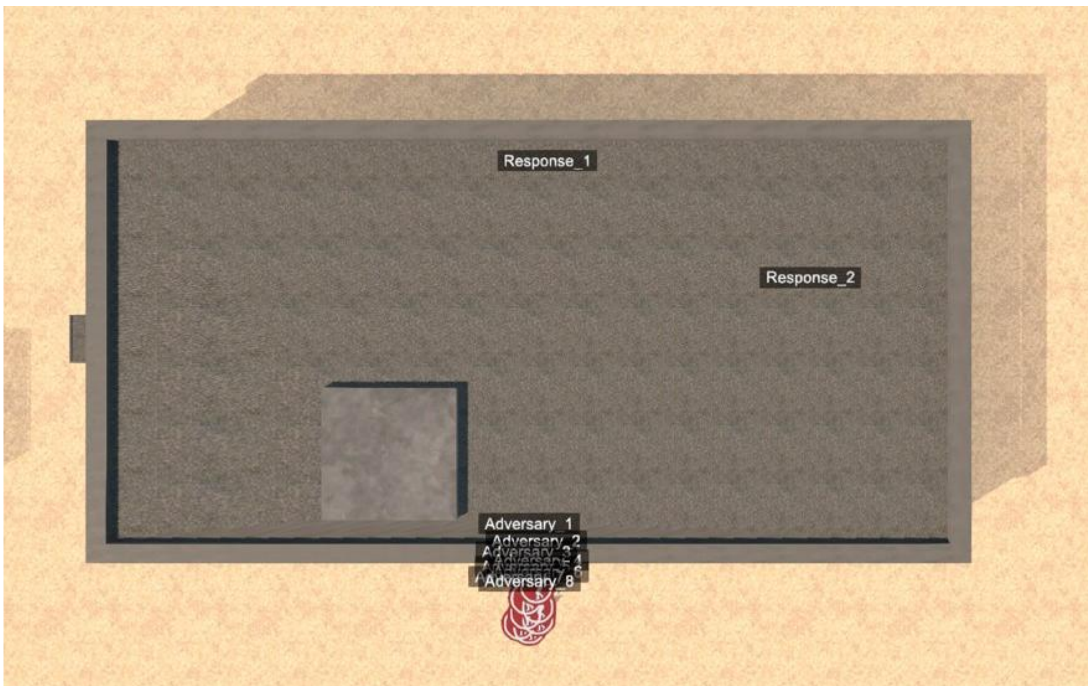

Figure 14. Adversary Attack Scenario One

In this adversary attack scenario, the CAS identifies the adversary team approximately 15-seconds before they reach the vehicle barrier outside of the protected area. DMA provides this initial detection point, which identifies a vehicle approaching the facility. After this initial detection, the RTL notifies the armed responders above-grade. Once the adversary team reaches the protected area boundary, the CAS operator and RTL see the adversary team moving to the southern doorway entrance. Using the PTZ cameras around the perimeter and on the DMA towers, the responders now know that all adversaries have positioned themselves along this doorway to enter into the facility. This allows both responders in the above-grade positions to focus their fields-of-fire on the southern entrance into the building. The adversary team must first breach into the building door; once inside the door, the adversary team will have to breach the interior shark cage to continue their attack on the facility. The shark cage forces the adversary team to use an explosive breach to reduce their time exposed to the response force and decrease their task time in this attack scenario. After breaching the shark cage, the adversaries must proceed to the below-grade entrance point location. The adversary team uses explosives to reduce their overall task time to breach this entry door. Once the below-grade entrance door has been breached the adversary team must enter the room and breach the stairwell doors to proceed below-grade. As the adversary team proceeds below-grade, they will encounter a doorway that does not require an explosive breach; however, immediately exiting the stairwell they face another shark cage they must explosively breach. After the adversary finishes the breach on the shark cage, they can move toward the doorway that separates the office space from the operating microreactor space. The adversary team must explosively breach this doorway to gain access to the microreactor. Many of these breaches require the adversary team to spend time exposed to the above-grade responders or exposed to the CAS operator and RTL below-grade. Additionally, all breaches that require explosives will force the adversaries either to retreat outside of the facility (if the breach occurs above-grade) or retreat above-grade (if the breach occurs below-grade). **Placing barriers that require adversaries to conduct explosive breaches internal to the facility increases the adversary task time and forces them to spend time and energy retreating to a safe location within or outside of the facility.**

4.1.1. Attack Scenario One Results

The facility analysis of attack scenario one used two armed responders in the above-grade BBRE positions and the CAS operator and RTL in the below-grade portion of the facility. Table 2 show the results based on the number of blue (site response force) wins and red (adversary force) wins for each scenario. If the response neutralized or rendered combat ineffective all adversaries, blue won. If the adversary neutralized all responders above grade, red won.[3]

Table 2 Scenario One: Two Responders (Above-Grade Only Engagements)

Number of Adversaries	Probability of Response Success (%)
8	31
7	54
6	60
5	65
4	85

In the case of two armed responders, the adversaries remain quite successful until the adversary team size drops to four.

Upon initial entry into the building and when the adversary encounters the internal shark cage, the response force successfully neutralizes three adversaries at the beginning of the scenario and gains an advantage. The adversary team regroups outside of the building and can make entry with suppressing fire on the gunports of the BBREs, while one adversary attempts to breach the shark cage. Once the adversaries breach the shark cage, they proceed forward and continue to suppress the gunports to engage the responders and try to make entry below-grade. The adversaries neutralize the above-grade responders either in engagements in the gunports or once they breach the doorway

[3] The team analyzed each scenario one hundred times and individually simulated each engagement between blue team members and adversary team members one hundred times.

to access the below-grade portion of the microreactor building. In this scenario, the low number of blue wins precipitated an upgrade to place four armed responders into the above-grade BBRE positions (see Table 3 for results).

Table 3. Scenario One: Four Responders (Above-Grade Only Engagements)

Number of Adversaries	Probability of Response Success (%)
8	90
7	92
6	95
5	99
4	100

As shown in **Error! Reference source not found.** andTable 3, the effectiveness of the PPS increased with four armed responders posted above-grade, compared to when the response team only consisted of two dedicated armed responders.

With four responders, the response force effectively neutralizes the adversaries across all ranges by engaging them from multiple gun ports in the BBREs, combined with the small amount of space the adversaries have to make entry into the above-grade area with the shark cage. As the adversaries enter the building, the response force neutralizes two-to-three adversaries. In a similar fashion to the scenario with two responders, the adversary team regroups outside the building. However, because of its advantageous positions and greater numbers, the response force neutralizes a majority of the adversaries before they breach the doorway that would allow them access to the below-grade portion of the facility.

4.2. Attack Scenario Two

The second adversary attack scenario analyzes the adversary team attacking the facility through both doors that enter into the above-grade portion of the reactor building. This scenario assumes the adversaries split into two equal teams to breach into the facility (see Figure 15). This adversary attack scenario follows a similar sequence of events as the first scenario.

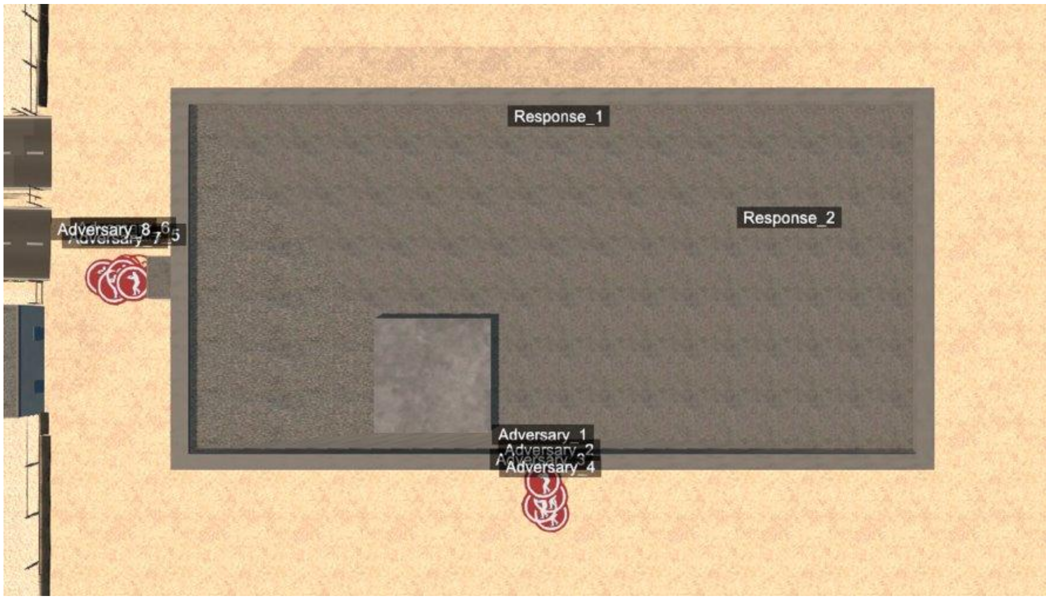

Figure 15. Adversary Attack Scenario Two

4.2.1. Attack Scenario Two Results

Similar to the first scenario, this analysis included two armed responders in the above-grade BBRE positions and the CAS operator and RTL in the below-grade portion of the facility. The adversary team attacks the facility and the entrance doors in a similar fashion, and the response force neutralizes an adversary as they enter the building, before they can achieve a breach on the shark cage. As a result, the adversary team must begin suppression of all the gun ports in the BBREs as they set up a breach of the shark cage. The two armed responders have fewer targets to engage and do so more effectively compared to all eight adversaries entering through one door (as in the previous scenario). They can neutralize up to three adversaries before the adversaries successfully breach the entrance door to the below-grade portion of the reactor building. However, once this breach occurs, the adversary force can neutralize the responders and proceed below-grade (with no additional dedicated armed responders; see Table 4). As in scenario one, this precipitates an upgrade to four responders above-grade (Table 5).

Table 4. Scenario Two: Two Responders (Above-Grade Only Engagements)

Number of Adversaries	Probability of Response Success (%)
8	59
7	62
6	70
5	80
4	87

Table 5. Scenario Two: Four Responders (Above-Grade Only Engagements)

Number of Adversaries	Probability of Response Success (%)
8	90
7	93
6	95
5	95
4	96

As shown in Table 4 and Table 5, PPS effectiveness increased when the response team increased from two to four armed responders. The above-grade responders neutralize four adversaries on the initial breach into the shark cage enclosures in almost all scenarios. This means the responders have a much higher probability of neutralizing all adversary ranges. Advantages in this scenario include the hardened positions, the knowledge of adversary locations, and multiple weapons used on adversaries conducting the breaches. With four armed responders, the response force has fewer targets to engage and can effectively neutralize more adversaries, compared to the first attack scenario. This results from a more effective PPS design and response force strategy against the hypothetical DBT to neutralize the adversary.

Microreactor vendors and utilities should consider the design of BBRE fighting ports during the facility design process. Traditional fighting ports have viewing glass and a sliding port that enables larger angles of engagement but can lead to greater exposure of the responders in the BBREs (i.e., the ports can be opened). **To reduce the probability that an adversary can engage and neutralize a responder through larger fighting ports, designers can modify them to allow just the muzzle of the rifle through, while still enabling the responder to visualize engagements through the viewing glass.** The smaller port configuration would also potentially increase opportunities for responders to engage the adversary force.

4.3. Additional Adversary Attack Scenario Considerations

Microreactor vendors and utilities looking to deploy microreactors should consider other potential adversary attack scenarios in their designs. Examples of these considerations include adversary tunneling, adversary breaching time of exterior walls, and the adversary using cyberattacks to disable PPS elements to aid in an attack (thereby decreasing PPS effectiveness).

An adversary using access and knowledge to exploit cyber vulnerabilities by conducting a cyberattack on the PPS network could create an advantage for an adversary team attempting a physical assault on the facility. For example, using the PPS design in this hypothetical facility, an adversary could disable the camera feed outside of the microreactor building entrances or the DMA stations used as the exterior IDS. This would disable the exterior IDS, which impacts response force notification of an adversary incursion at the facility and disables situational awareness for the armed responders in the BBREs protecting the facility, as they would not know through which entry point the adversaries attempt to enter the facility. In addition, the magnetic locks on the shark cage door could be exploited with a cyberattack, which degrades the effectiveness of these barriers, particularly if the cypher lock is also unlocked. Analysis shows shark cages provide a significant advantage to the response force and, if compromised, could lead to degradation in the overall effectiveness of the PPS.

In this hypothetical PPS design, the response force sits internal to the facility, with no fighting positions on the exterior of the building. This enables the adversaries to spend large amounts of time outside of the building, attempting to penetrate exterior walls. This could pose potential risks to the facility and require a mobile response force. Ensuring the exterior walls of the above-grade portion of the reactor building can withstand a direct adversary breach can decrease the likelihood of success for this attack type. This may include measures such as increasing the concrete thickness of exterior reactor building walls, increasing the complexity of the rebar lattice structure of exterior walls, or adding an air-gapped wall outside of the existing exterior above-grade walls. These measures may increase the amount of explosives required to breach the exterior walls and increase the adversary delay time such that an additional offsite response force (i.e., local law enforcement agency) may successfully respond on the exterior of the facility. Designs should also consider the roof of the reactor building, which poses additional vulnerabilities to the facility based on a lack of exterior response capabilities.

Microreactor vendors should also consider adversaries who have the ability to tunnel long distances underneath the facility and can attempt a direct breach through the below-grade walls to gain access to the microreactor. Mitigations for this scenario include installing exterior underground sensors around the boundary of the facility that may detect adversaries attempting to tunnel below-grade. In addition, the facility could consider vibration sensors or other sensors around the below-grade walls of the microreactor facility that could detect adversary penetration attempts.

5. STAFFING PLANS AND COST ANALYSIS

The total costs for a PPS are subject to change and depend on things such as the price of the technology at the time of purchase, installation costs, engineering costs, and the current pay rates for security professionals. This section captures costs associated with technology purchases and the annual costs for the security personnel and response force. **This cost estimate does not account for installation, trenching, communication lines, power connections, and maintenance and testing of PPS components.** The team developed the staffing plans in this section based on the previously described PPS design and the number of personnel needed to operate the PPS. These numbers can change. **The cost analysis and staffing plan uses a four (4) full-time equivalent multiplier for each 24-hour 7 day-a-week position. The staffing plan does not account for testing and maintenance personnel.**

5.1. Staffing Plans

The number of positions needed to implement day-to-day operations at the microreactor facility determines the staffing plans for the site, and includes armed responders, guards or armed security officers, CAS operator, and the RTL. The security plan defines armed responders as a dedicated position that only responds to security events. The guard and armed security officer conduct searches for prohibited items of personnel and vehicles that enter the facility. If a vehicle arrives at the facility, the CAS operator will also assist the guard or armed security officer in the vehicle search. When this happens, the RTL will take over operational control of the CAS. The RTL dictates how the response force will respond to a security event. In this scenario, the RTL also acts as the security shift supervisor, who organizes and assigns site-level activities for security such as testing, maintenance, and other day-to-day activities of the security system. Table 6 shows the staffing plan for the security system that utilizes four armed responders.

Table 6. Four Armed Responders Staffing Plan

Position	24/7 Positions	Total Head Count
Armed Responder	4	16
Guards/Armed Security Officers	1	4
CAS Operator	1	4
RTL	1	4
Total	7	28

Table 7 shows a similar staffing plan but considers two armed responders instead of four.

Table 7. Two Armed Responders Staffing Plan

Position	24/7 Positions	Total Head Count
Armed Responder	2	8
Guards	1	4
CAS Operator	1	4
RTL	1	4
Total	5	20

5.2. Cost Analysis

The team conducted a hypothetical cost analysis based on the previously described design of the facility. The largest drivers of PPS technology cost include the VBS and the BBREs for internal response positions. The team assumed a K12 modular block wall vehicle barrier for the site. The necessary standoff distance to ensure the survival of responders inside of the facility drives the vehicle barrier distance in this design.[4] Additional cost estimates focused on the armed responders, CAS operators, RTL, and the guards or armed security officers. Because of the flexible nature required by the smaller staffing numbers at this facility, all personnel must train and qualify as both responders and CAS operators. The costs in Table 8 and Table 9 include estimates for the total full-time-equivalent number of personnel needed to operate the facility. The total summarized in the tables includes the up-front security technology costs and the annual costs to operate the response force and other security personnel on site. Table 8shows the cost estimate for the facility design utilizing four onsite armed responders.

Table 8. Costs for PPS Design Using Four Armed Responders

Position	Costs
PPS Technology Costs	$6,300,000
Response Force Annual Costs	$4,650,000
Other Security Staff Annual Costs	$3,400,000
Total (Annual Costs and PPS Technologies)	**$14,350,000**

Table 9 shows the cost estimate for the facility design utilizing two onsite armed responders.

Table 9. Costs for PPS Design Using Two Armed Responders

Position	Costs
PPS Technology Costs	$6,300,000
Response Force Annual Costs	$2,230,000
Other Security Staff Annual Costs	$3,400,000
Total (Annual Costs and PPS Technologies)	**$11,930,000**

[4] Vendors should also consider additional requirements for VBSs including U.S. NRC requirements such as 10 CFR 73.55(e)(10)(I)(A).

6. RECOMMENDATIONS AND CONCLUSIONS

This report highlights a design strategy based on lessons learned working with microreactor vendors and those who express interest in operating a microreactor. Although this report focuses on one PPS design for a microreactor, it is based on the methods of sound PPS design and overall reductions for upfront capital costs and long-term operations and maintenance costs.

6.1. Recommendations

Microreactor vendors interested in domestic and international deployments can consider the following recommendations. However, implementation of each recommendation may vary, based on the vendor design and deployment location.

1. Evaluate various potential adversary attack scenarios and adversary group sizes to increase design flexibility for various deployment locations.
    a. Microreactor vendors should consider various attack scenarios and use open-source information to identify potential credible threats to microreactor facilities (e.g., large numbers of responders, explosive/kinetic UAS systems, rocket-propelled-grenades, etc.) to create defense-in-depth for various potential deployment locations, develop robust PPS designs, and ultimately improve overall PPS effectiveness.
2. Place the microreactor and associated targets below-grade to improve resilience to adversary attack scenarios and enable reductions in overall costs for the PPS.
    a. By placing the microreactor and associated targets below-grade, a vendor may increase facility resilience to various adversary capabilities and threats such as explosive/kinetic UAS, VBEDs, and explosives applied to the exterior of the buildings. Additionally, placing the microreactor below-grade enables a decrease in the size of the VBS (due to the inherent standoff applied to targets below-grade), which may offset the costs for construction of a below-grade facility.
3. Create channels / funnels that force adversaries to protected response positions to increase the effectiveness of the response force.
    a. Designs that channel adversaries to response force positions create a funneling effect where the response force can neutralize more adversaries effectively. Channeling the adversaries into these locations can also force a single point of failure for an adversary. In this hypothetical design, the adversary team must complete a complex breach while under fire from responders. This increases the overall difficulty of the attack, and therefore, increases the effectiveness of the security system.
4. Consider adequate BBRE designs that minimize the potential for adversaries to suppress responders in BBRE positions.
    a. Minimizing the adversary's ability to engage and suppress responders increases the overall system effectiveness. Designing the fighting ports to reduce the adversary's ability to visualize responder positions can give the response force the advantage of first-to-engage, thereby increasing their chances of neutralizing the adversary force. This improves both response force survivability and capability to neutralize the adversary force.
5. Consider all deployment locations and regulatory constraints during the design phase.

   a. Microreactor vendors must consider how deployment locations and regulatory constraints may impact the overall PPS design. For example, a deployment location in one environment may not support below-grade placement of the microreactor, while a second deployment location may, resulting in drastically different overall facility and PPS designs. Multiple cost-effective facility and PPS designs may exist for various deployment locations. Factors to consider include adding internal security measures to create defense-in-depth and increase the effectiveness of the PPS against higher-threat environments. Additionally, vendors should account for how differing local laws may impact PPS design and implementation, different costs such as labor or the availability of labor, and differences in response force capabilities.

6. Develop a robust training program for all security personnel at the facility.
   a. Utilities planning to operate a microreactor facility should develop a robust and rigorous training program for responders and security personnel. Microreactor economic viability suggests the necessity of lower numbers of overall security staff compared to other SMRs and the current fleet of nuclear power plants. To enable a smaller security staff, the microreactor facility will need a robust training program that ensures that security personnel can perform multiple job functions on site. This includes training personnel to perform as a CAS operator, a responder, and conduct personnel and vehicle searches.

7. Utilize roof hatches to move the microreactor and other equipment below-grade.
   a. Roof hatches require automated features and cranes to move the microreactor into proper position, which can increase costs. However, the roof hatches present less vulnerabilities than high-bay doors. High-bay doors are generally made of material that is not difficult to penetrate; to mitigate this, sites can install delay barriers, but installation and maintenance of these barriers can significantly increase costs. Roof hatches reduce these vulnerabilities at a potentially lower cost.

8. Install active delay barriers in microreactor facilities to improve PPS effectiveness.
   a. Active delay barriers such as smoke, fog, and slippery agents may improve effectiveness of delay barriers. For example, applying smoke, fog, or slippery agents inside of shark cages increases the overall difficulty of breaching the shark cage. This increases adversary task time, which increases the opportunity for a responder who is in a position to engage to do so effectively, thereby improving overall system effectiveness.

6.2. Conclusions

This report analyzed a hypothetical microreactor facility design and a hypothetical PPS based on lessons learned from providing support to microreactor vendors. The following lists of conclusions resulting from this design and analysis.

1. Reductions in response force size may require a shift to an internal response strategy that focuses on denying access.
   a. In this analysis, the team chose an “internal only” response strategy to reduce the response force size. To facilitate an external response strategy, the facility design requires larger fields-of-view to enable the response force to neutralize adversaries before they make entry into the microreactor building, which can increase costs. An

internal strategy that includes effective use of channeling adversaries can improve the response force ability to neutralize adversaries, while maintaining lower numbers of responders.

2. Using novel security technologies for exterior IDS can increase the need for compensatory measures. An internal response force without visual observation may not be able to act as a compensatory measure for a loss of exterior IDS.
    a. Novel technologies such as DMA may reduce the costs of a PPS but may not account for compensatory measures. Sites must implement compensatory measures if these technologies fail. A response force positioned to visualize the perimeter of the facility could act as a continuous compensatory measure without increasing the security budget (one benefit of an external response force strategy). Vendors must consider compensatory measures in the design phase of the overall PPS and facility, as they act as a cost compounding factor. A design to reduce up-front capital costs in security technologies may result in a tradeoff with increased operational costs to implement compensatory measures at a microreactor facility.
3. One PPS design may not fit all deployment locations and regulatory requirements.
    a. Lessons learned from supporting microreactor vendors show that one PPS design may not fit all potential deployments and regulatory requirements associated with those deployment locations. For example, a deployment location in one environment may not support below-grade siting, while a second deployment location may. As a result, the vendor may forego one deployment environment in order to design a PPS for an optimal deployment environment. In addition, different deployment locations may have drastically different regulatory requirements, which may also result in differing PPS designs.

Sandia National Laboratories

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