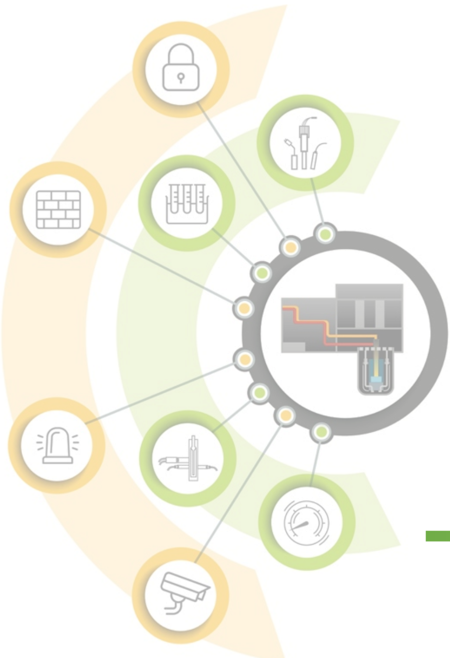


U.S. Domestic Security-by-Design: On Site Response Force Strategies

Prepared for

US Department of Energy

Alan Evans

Sandia National Laboratories

May 2023

SAND2023-XXXXR

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.

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

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-N5 A0003525.

Sandia National Laboratories

ABSTRACT

U.S. nuclear power facilities face increasing challenges in meeting dynamic security requirements caused by evolving and expanding threats while keeping cost reasonable to make nuclear energy competitive. The past approach has often included implementing security features after a facility has been designed and without attention to optimization, which can lead to cost overruns. Incorporating security in the design process can provide robust, cost- effective, and sufficient physical protection systems. The purpose of this work is both to develop a framework for the integration of security into the design phase of High Temperature Gas Reactors (HTGRs) that utilize pebble-based fuels and microreactors. Specifically, this effort focuses on integrating security into the design phase of a model HTGR and microreactor that meets current Nuclear Regulatory Commission (NRC) physical protection requirements and providing advanced solutions to improve physical protection and decrease costs. A suite of tools, including SCRIBE3D©, PATHTRACE© and Blender© were used to model a hypothetical, generic domestic HTGR facility and microreactor facility. Physical protection elements such as sensors, cameras, barriers, and onsite response forces were added to the model based on best practices for physical protection systems. Multiple outsider sabotage scenarios were examined with four-to-eight adversaries to determine security metrics. The results of this work will influence physical protection system designs and facility designs for U.S. domestic HTGRs and microreactors. This work will also demonstrate how a series of experimental and modeling capabilities across the Department of Energy (DOE) Complex can lead to efficient security systems that utilize an onsite response force. The conclusions and recommendations in this document may be applicable to all SMR designs.

ACKNOWLEDGEMENTS

The team would like to acknowledge the many subject matter experts (Greg Baum, Steven Sweet, Doug Abell, Paul Zahnle, Jason Davenport, Ian Steagall, and Indigo Brown) who contributed their expertise to the development of this hypothetical facility, the design of the security system and the analysis of the security system.

CONTENTS

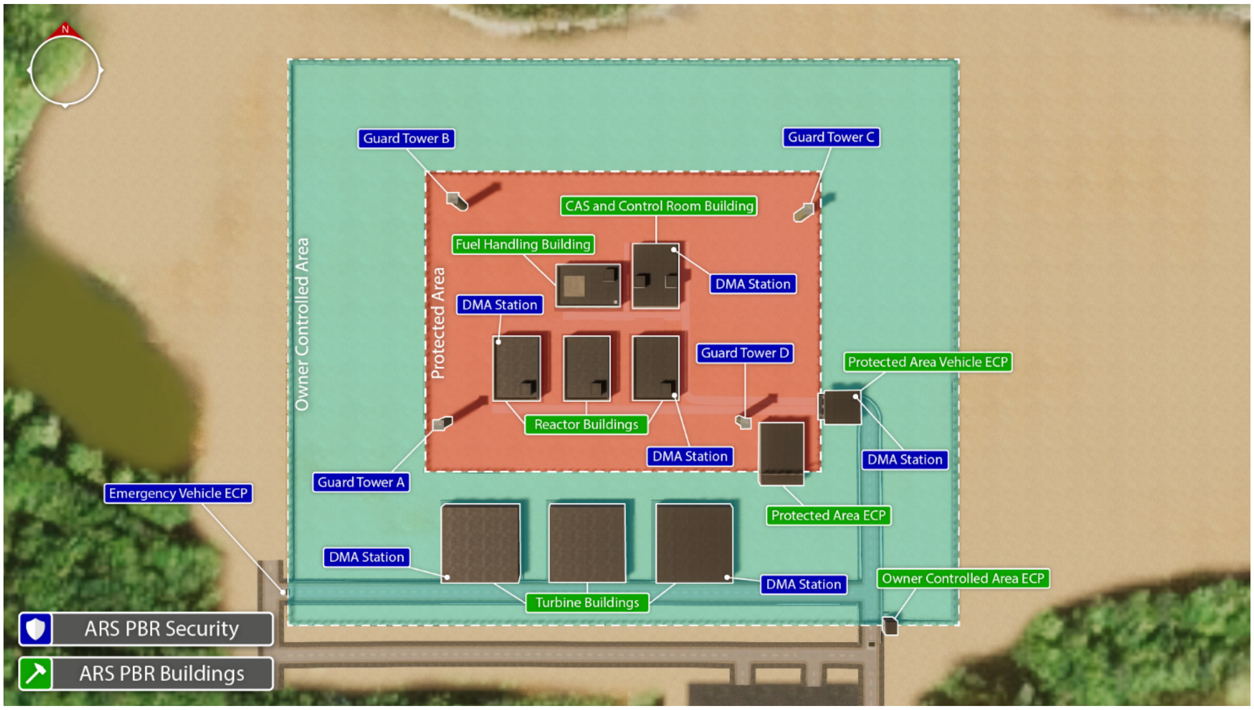
LIST OF FIGURES

LIST OF TABLES

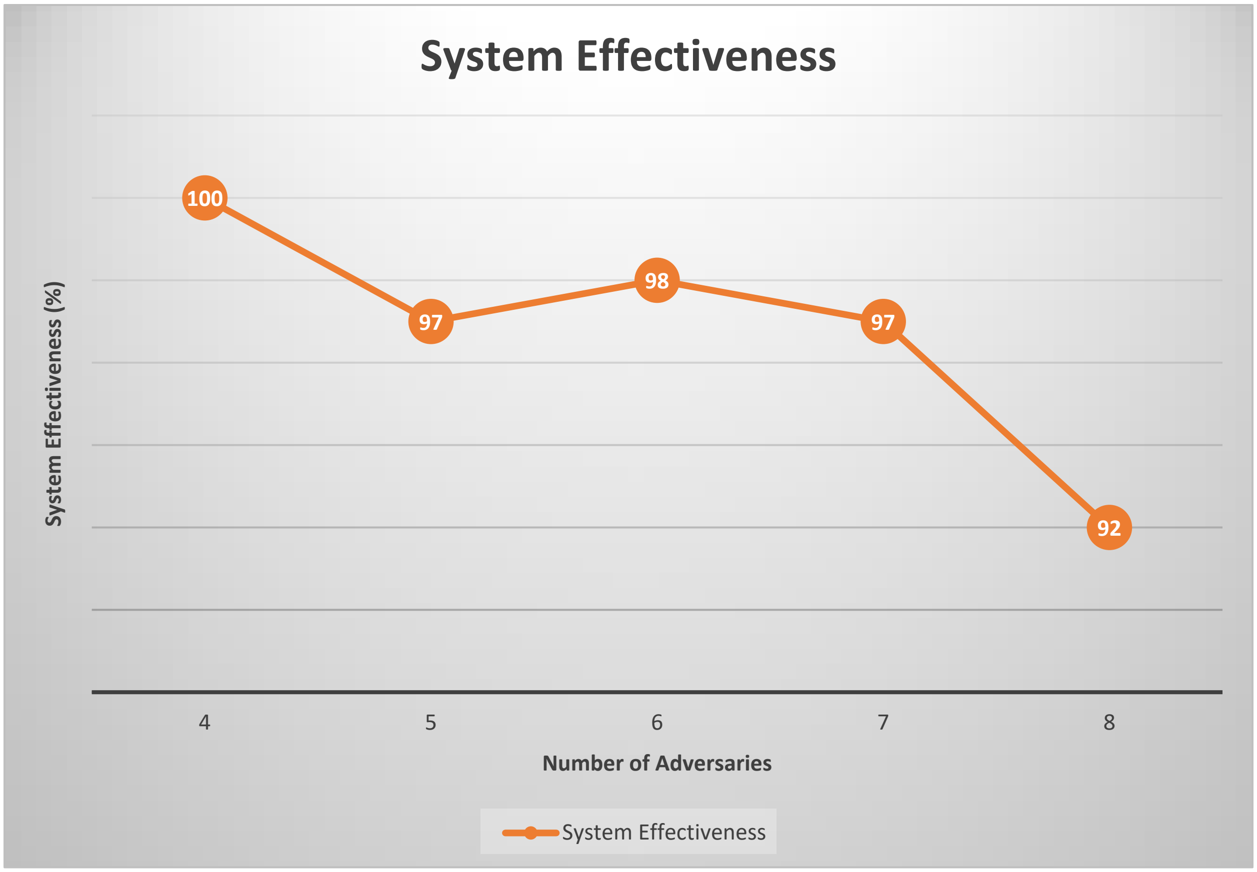
This page left blank

EXECUTIVE SUMMARY

This document highlights work to develop effective PPS strategies for a hypothetical small modular reactor and microreactor using an onsite response force. The first facility that was analyzed was a hypothetical pebble bed reactor (PBR). The PBR facility consists of three reactor buildings, a fuel handling building, a central alarm station and control building, two entry control point (ECP) buildings, and three turbine buildings. The site was designed with deliberate motion algorithm (DMA) as the primary form of external intrusion detection. The facility was designed in such a way that four external responders in bullet-resistant enclosure towers were used and one roving responder was used. To develop this strategy, three subject matter experts were used to inform the overall strategy and develop the PPS based on their experience. Tabletop exercises were conducted in SCRIBE3D© to determine advantageous adversary pathways and then to inform proper response force locations. The layout of this facility and the physical protection system (PPS) design can be seen below.



To analyze this facility, a hypothetical design basis threat (DBT) was used. This DBT can be seen in Appendix A. A range of adversaries was used to attack this hypothetical facility. Force-on-force simulations were conducted in SCRIBE3D© to determine the probability of neutralization (i.e. blue wins) and determine system effectiveness for the facility. The figure below shows the results from these force-on-force simulations.



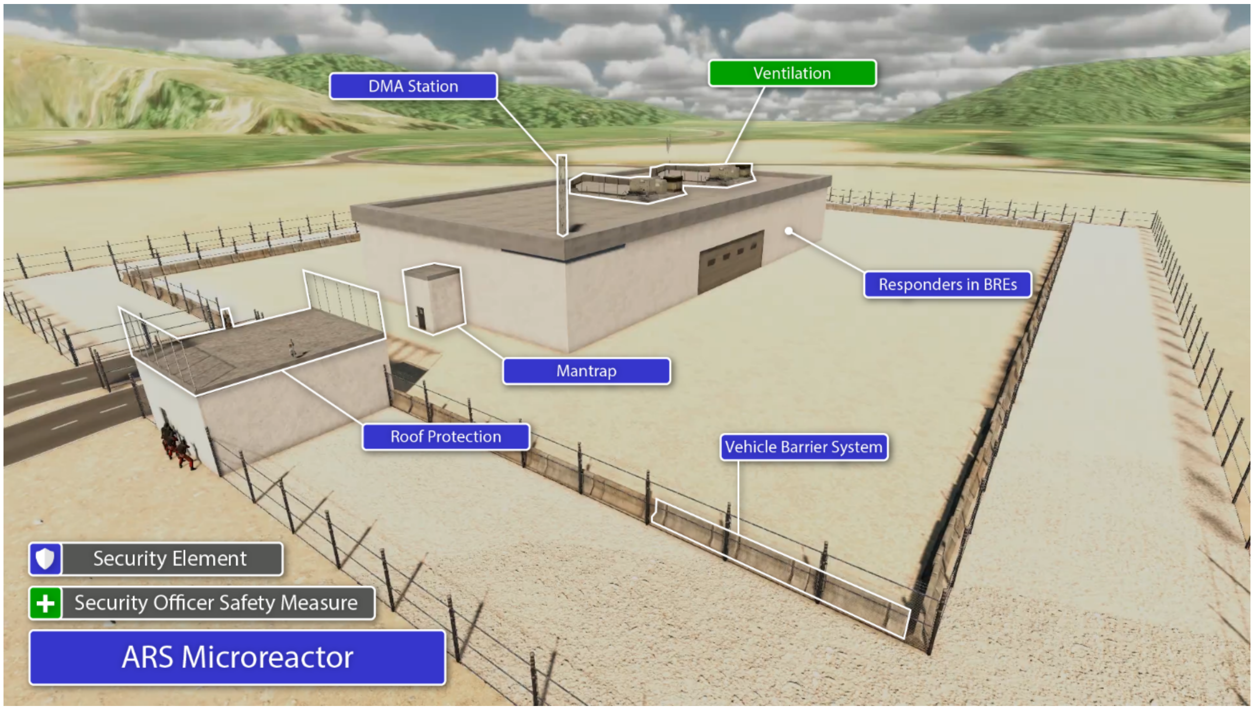
As can be seen from the figure above, the overall system effectiveness was high for this hypothetical facility across the range of adversaries that were analyzed.

A hypothetical security staffing plan was developed for the hypothetical PBR facility. This staffing plan can be seen in the table below.

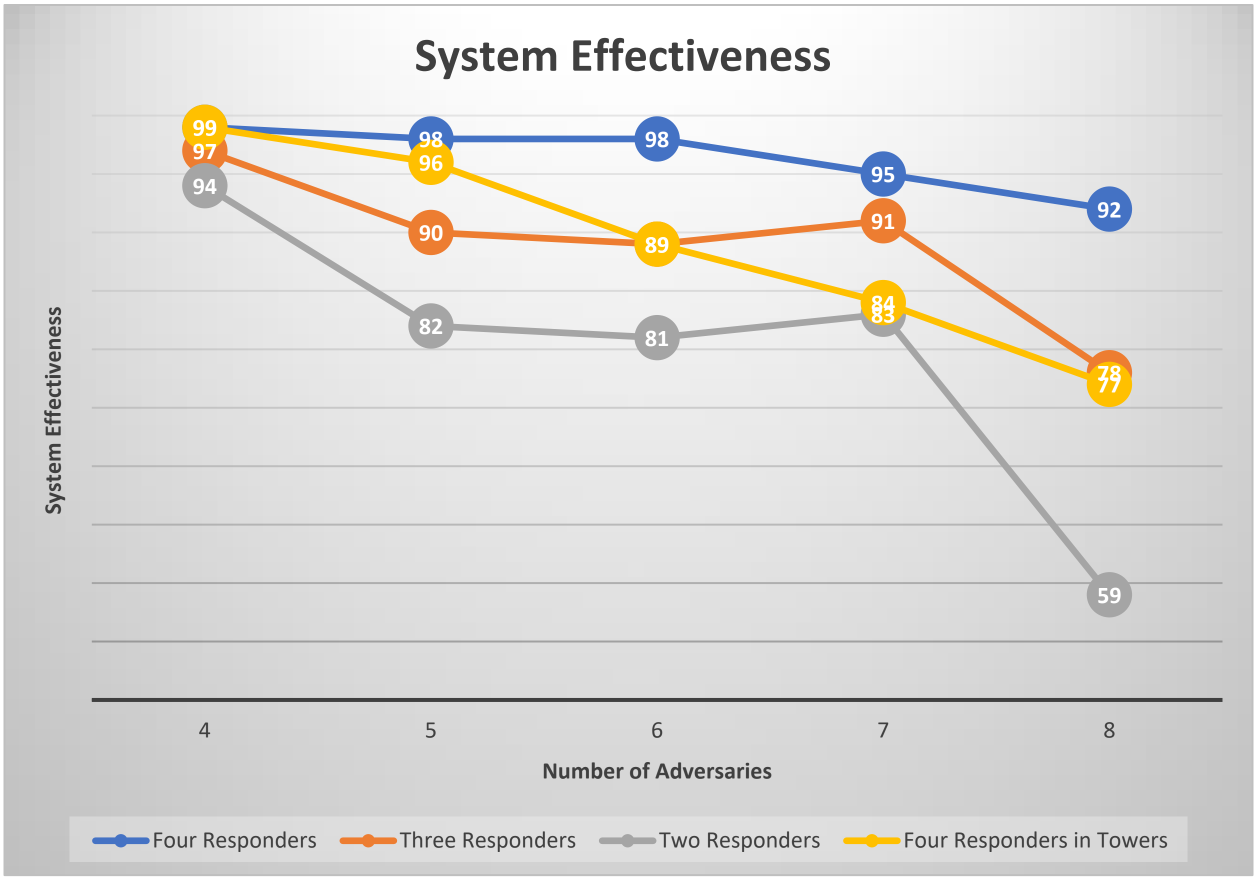
Position	24/7 12 hr. Rotating Shift	FTE
Security Shift Supervisor	1	4.7
Field Supervisors (One Response Team Leader)	2	9.4
Alarm Station Operators (CAS/SAS)	2	9.4
Armed Responders	6	28.2
Armed Security Officers (Personnel, vehicle, and material processing)	3	14.1
Total	14	**65.8**

The staffing plan shows a much smaller security staffing headcount than those for traditional nuclear power plants. One of the reasons for this is a much smaller armed responder footprint and a smaller armed security officer footprint. There may be further ways to decrease the total headcount further in some locations. For example, decreasing the armed security officer headcount by one and allowing the position of last access control to be handled by a security shift supervisor from the central alarm station.

Additionally, a hypothetical microreactor facility was also analyzed for an onsite response force strategy. The lessons learned form the PBR facility were taken into consideration when designing the PPS for this facility. For this analysis, two different response force strategies were analyzed. One strategy only considered responders in BREs on the interior of the building and a range of four to two responders was considered. The second strategy considered only responders external to the reactor building in BRE towers. DMA was again used as the primary external intrusion detection system. The layout of this PPS design can be seen in the figure below.



To analyze this facility, a hypothetical design basis threat (DBT) was used. This DBT can be seen in Appendix A. A range of adversaries was used to attack this hypothetical facility. Force-on-force simulations were conducted in SCRIBE3D© to determine the probability of neutralization (i.e. blue wins) and determine system effectiveness for the facility. The figure below shows the results from these force-on-force simulations.



As can be seen from the figure above, the most effective PPS and response strategy consisted of four responders internal to the facility in BREs. The other scenarios and PPS designs considered showed a decrease in system effectiveness as the number of adversaries increased. It is also important to note that the strategy with the responders in internal BREs had high system effectiveness until the adversary team reached eight individuals.

A hypothetical security staffing plan was developed for the hypothetical microreactor. The hypothetical staffing plan for the response force strategy with four internal responders can be seen in the table below.

Position	24/7 12 hr. Rotating Shift	FTE
Security Shift Supervisor	1	4.7
Field Supervisors (One Response Team Leader)	2	9.4
Alarm Station Operators (CAS/SAS)	2	9.4
Armed Responders	5	23.5
Armed Security Officers (Personnel, vehicle, and material processing)	3	14.1
Total	13	**61.1**

Similarly to that of the PBR, the microreactor staffing headcount is smaller than traditional nuclear power plants. However, this staffing plan may need to be reduced further for the viability of microreactor facilities.

This report details the design methodology, design specifics, and design integration for physical protection systems that use onsite response forces at a hypothetical PBR and microreactor. This report also details some logistical considerations that should be incorporated into the overall design of any small modular or microreactor facility.

ACRONYMS AND DEFINITIONS

Abbreviation	Definition
ASD	Adversary sequence diagram
BAS	Backup alarm station
BMS	Balanced magnetic switch
CAS	Central Alarm Station
CFR	Code of Federal Regulations
CCTV	Closed circuit television
CDP	Critical detection point
CVCT	Chemical volume control tank
DBA	Design basis accident
DBT	Design basis threat
DEPO	Design and evaluation process outline
DMA	Deliberate motion algorithm
ECCS	Emergency core cooling system
ECP	Entry control point
FRB	Fuel Receiving Building
HTGR	High Temperature Gas Cooled Reactors
iPWR	Integral-Pressurized Water Reactor
KIA	Killed in action
LAA	Limited access area
LEU	Low-enriched uranium
LLEA	Local law enforcement agency
LOCA	Loss of coolant accident
LWSMR	Light Water Small Modular Reactor
LWR	Light water reactor
MVP	Most vulnerable path
NRC	Nuclear Regulatory Commission
NEIMA	Nuclear Energy Innovation and Modernization Act
OCA	Owner-Controlled Area
PA	Protected area
PBSMRF	Pebble Bed Small Modular Reactor Facility
P_D	Probability of Detection
P_E	Probability of Effectiveness
P_I	Probability of Interruption

Abbreviation	Definition
PIDAS	Perimeter intrusion detection and assessment system
PIN	Personal Identification Number
P_N	Probability of Neutralization
PPB	Power production building
PPS	Physical Protection System
PSIT	Passive safety injection tank
RF	Response force
RFT	Response force time
RPV	Reactor pressure vessel
RWMT	Residual water makeup tanks
SFSC	Spent Fuel Storage Canister
SMR	Small Modular Reactor
SMRF	Small modular reactor facility
SNL	Sandia National Laboratories
SNM	Special Nuclear Materials
SSBD	Safeguards and Security by Design
TRISO	TRI-structural ISOtropic
UPS	Uninterruptible power supply
URC	Unacceptable radiological consequence
VA	Vital area

1. INTRODUCTION

Domestic nuclear power facilities face stringent requirements for the physical protection of the nuclear facility. The US Nuclear Regulatory Commission is currently proposing two new sets of rulemaking for small modular reactors (SMRs) and microreactors. These regulations might allow for changes that allow for SMRs and microreactors to be cost effective in the energy production market. The Department of Energy's Office of Nuclear Energy Advanced Reactor Safeguards (ARS) program has worked to help domestic SMR and microreactor vendors understand security-by-design options for various physical protection system (PPS) designs and response force strategies that allow for reduced costs to decreased security personnel requirements and decreased security technology infrastructure.

Security-by-design (SeBD) is the process in which security features, the PPS, and response force strategy are considered and designed as part of the overall facility design. SeBD is focused on increasing system effectiveness for a PPS, creating cost-efficient PPS designs, and meeting the intent or meeting regulations.

Previous reports created under the ARS program focus on designing physical protection systems that are conducive for an offsite response force or a response force that consists of remoted operated weapon systems. In this report, onsite response force strategies are developed and analyzed for a hypothetical microreactor and SMR. Three subject matter experts (SMEs) with varying backgrounds in law enforcement and armed response at nuclear facilities were used to develop these strategies. These backgrounds include, law enforcement, correctional facility officers, military operations, armed response at various nuclear facilities, and armed response experience at domestic nuclear power plants (NPPs).

2. ONSITE RESPONSE FORCE FOR A PEBBLE BED REACTOR

To develop a strategy for an onsite response force for the hypothetical pebble bed reactor (PBR)[1], each SME (discussed above) first developed a strategy to defend the facility based on their previous background and experience. Each of the individual physical protection systems (PPS) were unique and generally followed from the experience of each SME. However, many similarities emerged from the individual designs. The individual designs consisted of response strategies that included armed responders in fixed positions such as towers or bullet-resistant enclosures (BREs) externally or internal BREs, armed responders that were mobile and continuously moved around the facility and could enter internal BREs to protect the facility, and one design included the use of an armored vehicle (which was excluded due to the desire to increase cost-efficiencies through the facility design). Each individual design was then run through a series of tabletop exercises (TTXs) that allowed the other SMEs to attack the facility using a defined adversary design basis threat (DBT)[2]. The TTXs were very informative to the larger team developing the design of the security system and many lessons were learned based on protecting a facility with four separate target buildings and seven individual targets. The figure below shows the plant layout that was developed by the three SMEs collectively based on an onsite response force strategy and the hypothetical DBT.

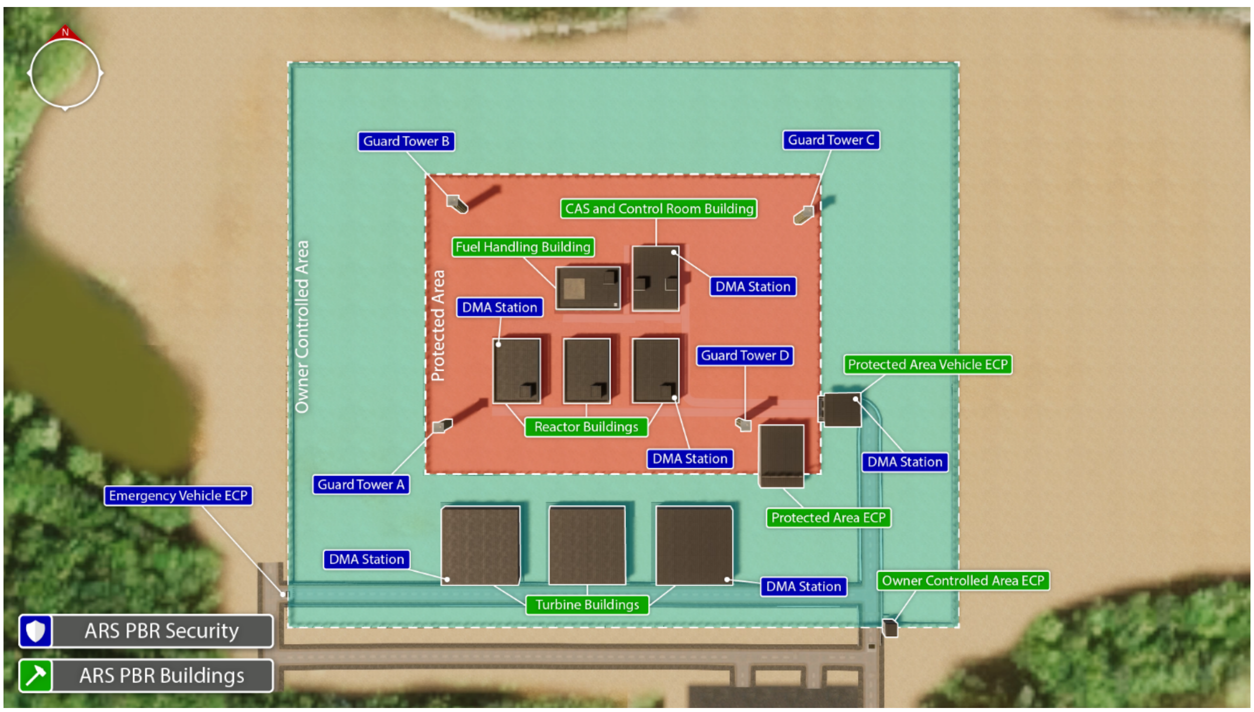


Figure 1 PBR Facility Layout

As can be seen in Figure 1, all the plant buildings are located within the owner-controlled area (OCA). The turbine buildings are located outside of the protected area (PA) to reduce the number of individuals needing access into the PA. This helps keep the number of employees in the PA down, reduces the size of the human reliability program (HRP) and adds some reduced cost to site operators. The southeast corner of the facility provides both an OCA entry control point (ECP)

---

[1] "U.S. Domestic Pebble Bed Reactor: Security-by-Design." Evans, A. et al. Sandia National Laboratories. SAND2021-13122R. October 2021.

[2] See Appendix A

where all personnel must badge into and a precursory vehicle search point to search any vehicle coming into the site for large vehicle borne explosive devices (VBEDs). The OCA ECP was located at such a distance that a large VBED could not cause damage to any of the vital areas located inside the reactor building, the central alarm station (CAS), or the control room building. The southwest corner of the facility shows the emergency vehicle ECP, which will only be used in emergencies, this gate and ECP remains locked with vehicle barriers in place when not in use. Inside the OCA fence line, a vehicle barrier system is used that can prevent DBT vehicles from proceeding further into the facility. Along the main roadways into the site vehicle barriers exist to funnel the vehicles toward the PA vehicle ECP and prevent a vehicle from driving into the turbine building.

The three reactor buildings (RBs) and fuel handling building (FHB) are the only buildings onsite with credible radiological release targets. The table below identifies the sabotage targets that were considered in this analysis.

Table 1 PBR Sabotage Targets

Location	Building Area	Form of Material	Amount of Material On-site (% Enrichment)	Total Isotope Amounts	Level of Radiation
Reactor Building 1	Reactor	TRISO pebbles	3,780 kg U (8.5% U-235)	321 kg U-235	High
Reactor Building 1	Spent Fuel Canister	TRISO pebbles	1,890 kg U (8.5% U-235)	161 kg U-235	High
Reactor Building 2	Reactor	TRISO pebbles	3,780 kg U (8.5% U-235)	321 kg U-235	High
Reactor Building 2	Spent Fuel Canister	TRISO pebbles	1,890 kg U (8.5% U-235)	161 kg U-235	High
Reactor Building 3	Reactor	TRISO pebbles	3,780 kg U (8.5% U-235)	321 kg U-235	High
Reactor Building 3	Spent Fuel Canister	TRISO pebbles	1,890 kg U (8.5% U-235)	161 kg U-235	High
Spent Fuel Storage Building	Below-Grade Storage	TRISO Pebbles	5,760 kg U (8.5% U-235)	482 kg U-235	High

The PBR facility has seven different targets spread out amongst four buildings. The large number of targets spread across the facility required a well-thought physical protection system (PPS) and response force strategy.

The OCA ECP is protected by hydraulic wedge barriers that form a vehicle trap. If a vehicle is scheduled to arrive on site, two-armed security officers (ASOs) will exit the PA ECP and move toward the OCA ECP. The ASOs will then allow the vehicle into the trap before the OCA fence and conduct a precursory search of the vehicle and the driver for large explosives either in the vehicle or on the driver. While the two ASOs are conducting the vehicle search, another ASO from the PA ECP is performing the last access control duties for entry into the PA. During this time the last access control ASO will lockdown the PA ECP so that no entry is allowed until the vehicle has fully processed through the OCA ECP and the PA ECP. The figure below shows the OCA ECP.

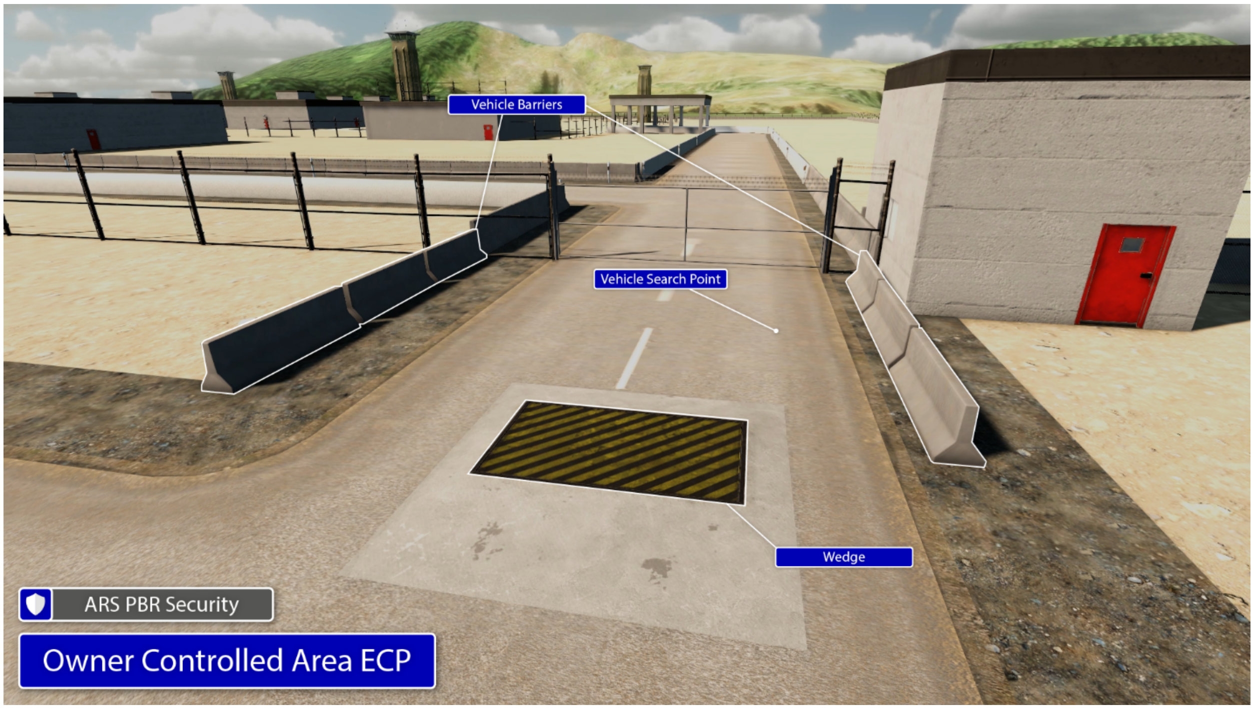


Figure 2 OCA ECP

Figure 3 Vehicle Barriers Around OCA

The PA ECP allows for all vehicles to go through a full search for all contraband material. Once the vehicle is clear at the OCA ECP, the CAS operator lowers the hydraulic wedges and allows the vehicle to proceed to the PA ECP. The road to the PA ECP is lined with vehicle barriers and a sharp turn to decrease the speed of the vehicle. Decreasing the speed of the vehicle allows for smaller and more cost-effective vehicle barriers to be used, and reduces the likelihood that the vehicle can penetrate the PA. The PA ECP for vehicles uses hydraulic wedge barriers to form a vehicle trap while the ASOs conduct a search of the vehicle. Once the vehicle has entered the vehicle trap, the driver exits the vehicle and proceeds to the PA ECP for an individual search. Once the driver has processed through the search they can return to the vehicle and are allowed to proceed with the vehicle into the PA. The figure below shows the vehicle ECP at the PA boundary.

Figure 4 PA Vehicle Search Point

It should be noted that for SMR facilities, smaller numbers of vehicles are expected during normal operation. Therefore, when a vehicle approaches the OCA ECP that is not scheduled to be onsite, the security system and security officers should be put into a higher state of alert due to the anomalous behavior occurring.

Previous designs of this hypothetical facility had considered large high-bay doors to allow vehicles to offload material into the facility. These large vehicle doors created inherent vulnerabilities and required measures such as moveable reinforced concrete walls to create equal amounts of delay, and compensatory measures for when these doors and the moveable reinforced concrete walls were open. During the SME development time for this facility, it was decided to install a roof plug on the roof of the FHB and on the ground floor. As equipment or material arrives onsite, the roof plug on top of the FHB is first opened by the security shift supervisor (SSS) and the operations manager for the shift. This ensures that the roof plug must be opened by two individuals from separate organizations (i.e. reduces insider threats). Additionally, when the roof plug on top of the FHB is opened, the roof plug between the above-grade floor and the below-grade floor cannot be opened. The two roof plugs are also offset so that if an item is dropped it cannot penetrate the second roof plug and increases the inherent security of this system. Once the material enters the FHB, the roof plug is closed on the roof of the FHB. Once inside an internal crane again operated by the SSS and the operations manager move the material through the roof plug between the two floors and below-grade. This process and system decrease the number of compensatory measures that are needed and additional security features that are needed. It should also be noted that all surface areas of the buildings in the PA are made of 2-foot-thick reinforced concrete, including the roof plugs to ensure adequate and equal delay across all potential adversary pathways. The figure below shows these roof plugs for the PBR facility.

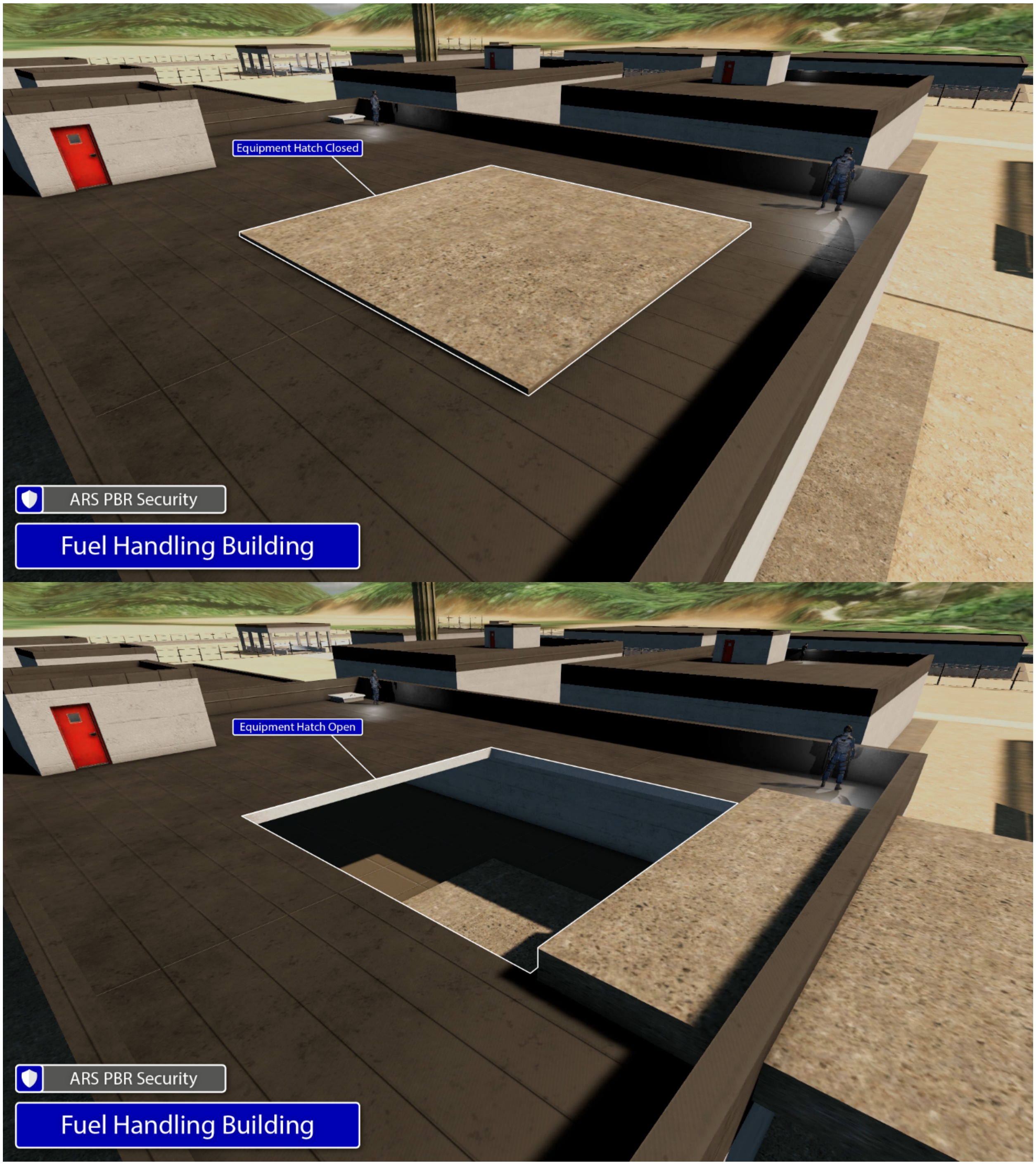


Figure 5 Roof Plugs for FHB

The figure below shows the emergency vehicle ECP. This vehicle ECP will only be used in the case of an emergency or in a compensatory measure state when the primary OCA ECP is not operational. The emergency vehicle ECP is protected with two different vehicle barriers that are controlled in the CAS. In the figure below, the vehicle gate is open to visually display the vehicle barriers more easily.

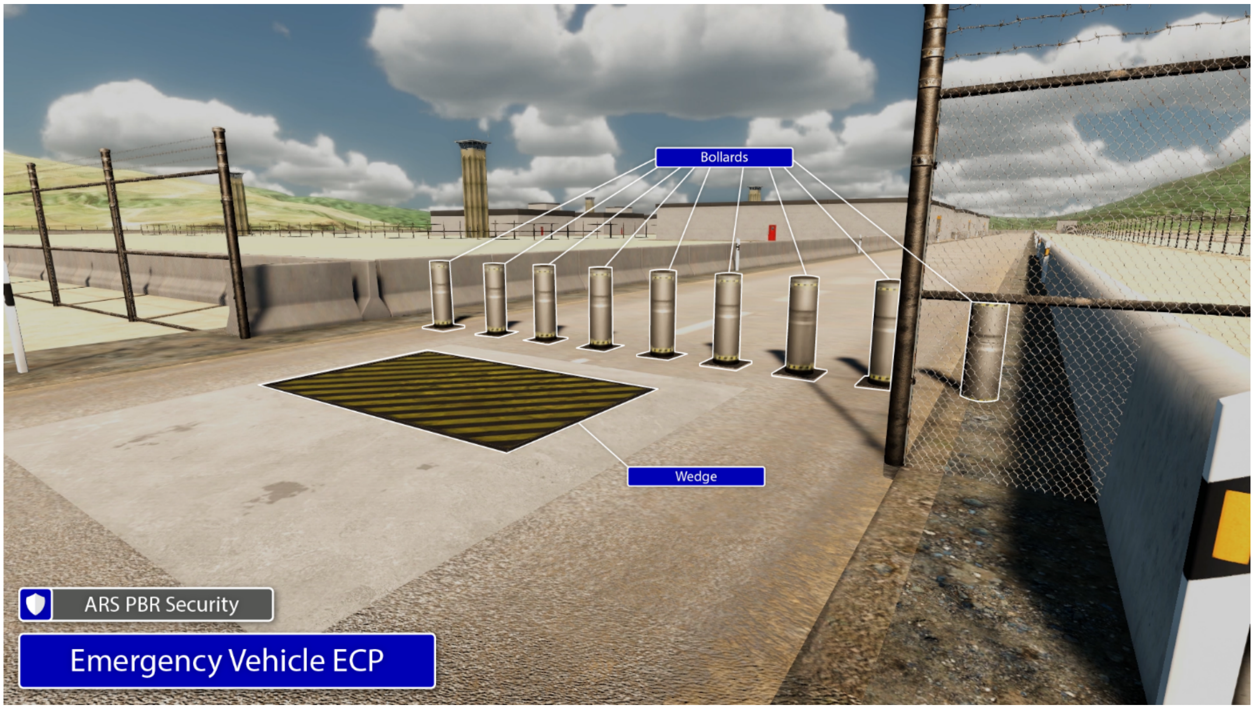
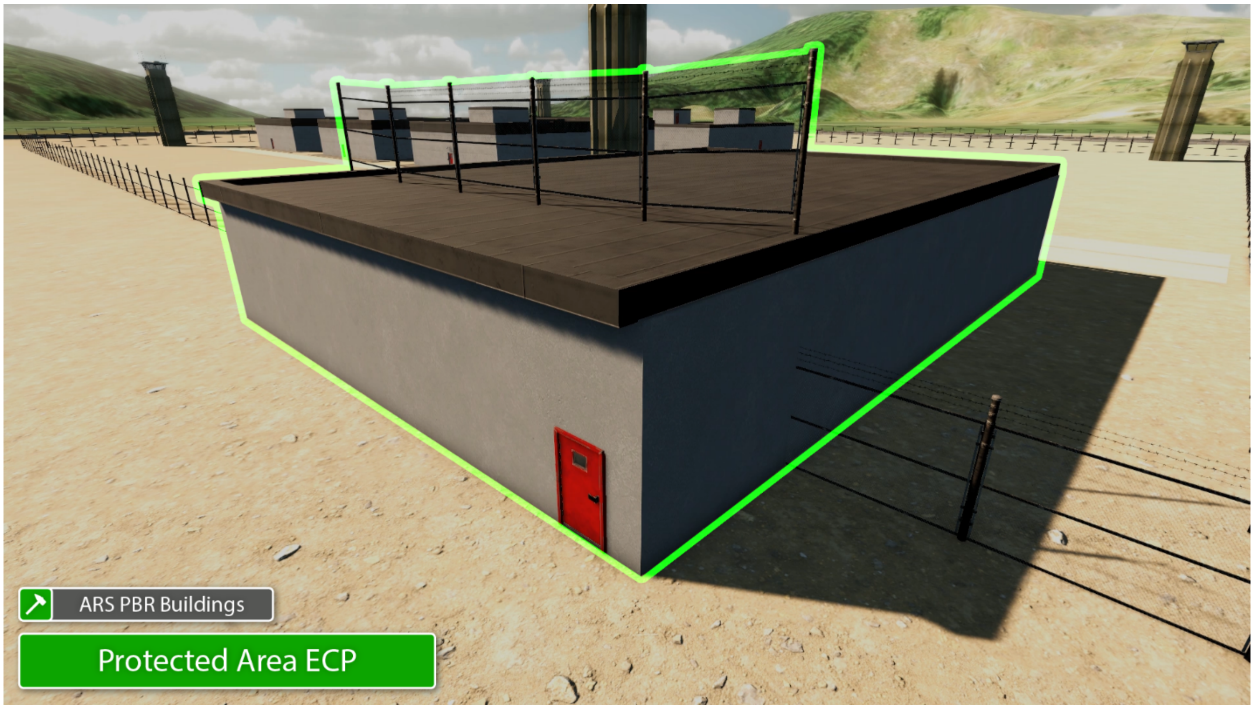
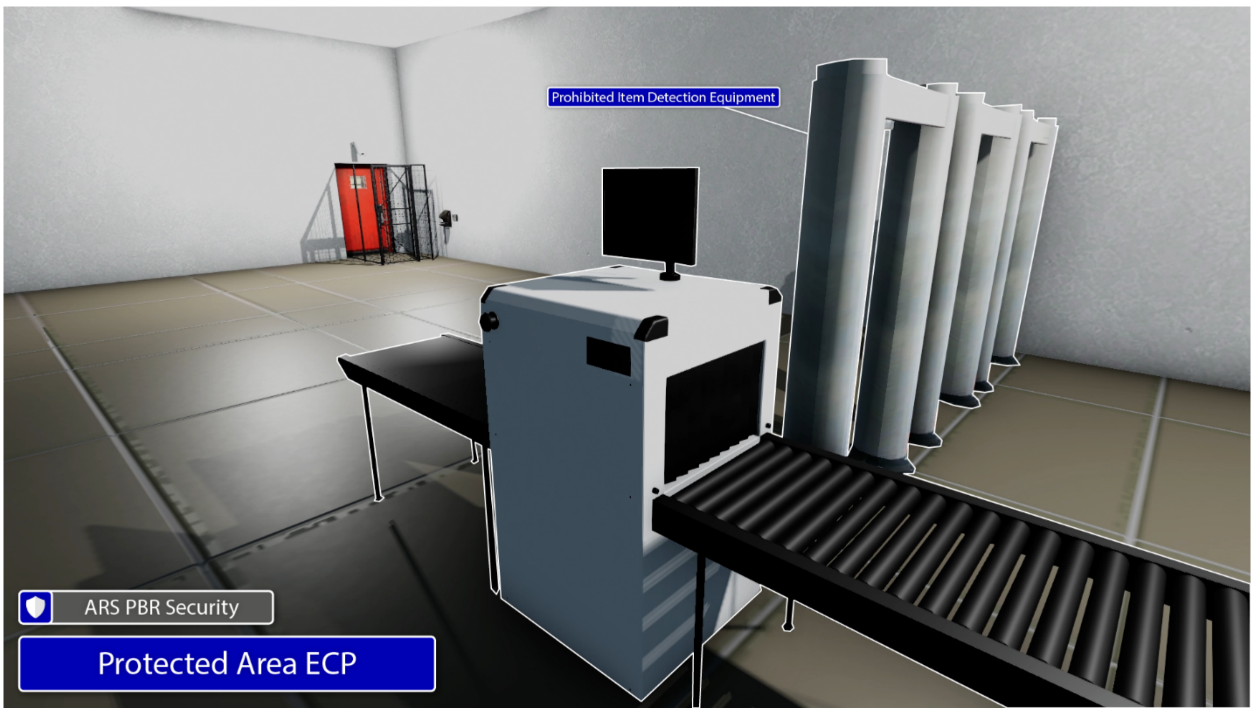


Figure 6 Emergency Vehicle ECP

Figure 5 below shows the PA personnel ECP. As can be seen from the first graphic, the roof is protected using a fence line to create a continuous PA barrier around the facility. Once inside the PA ECP, metal detectors, X-ray machines and explosive detectors are used to detect contraband items such as explosives, firearms, etc. The final graphic shows the view from the last access control point overwatch position. The ASO stationed in this position ensures that the search lanes can be monitored, and during a security event that the PA can be locked down. Additionally, the last access control point is equipped with firing ports to engage any potential adversaries that attempt to breach the facility using the PA personnel ECP.


ARS PBR Buildings
Protected Area ECP


Prohibited Item Detection Equipment
ARS PBR Security
Protected Area ECP

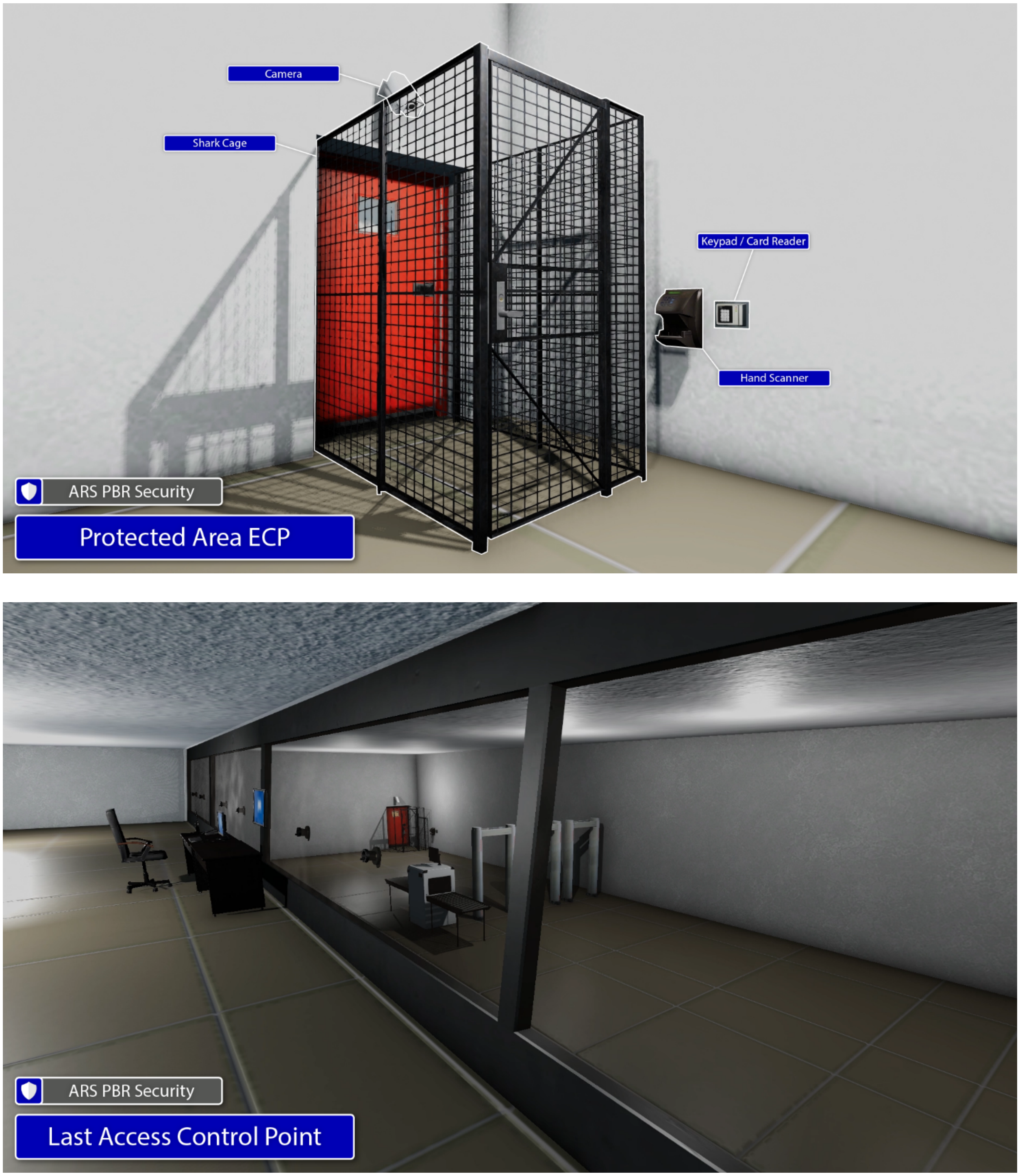
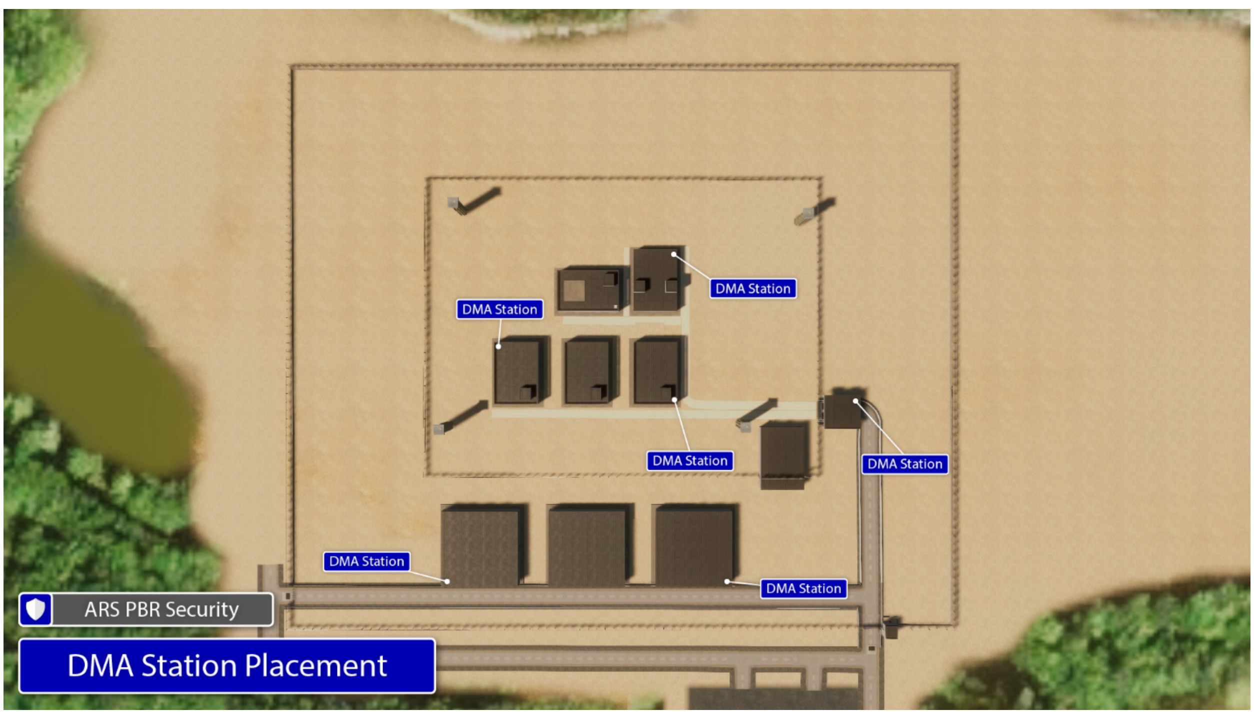


Figure 7 PA ECP and Last Access Control

Designing the PPS and the response force strategy for this hypothetical facility was complicated by the number of targets and unique locations. It was therefore decided that an external response strategy would best protect the facility. The facility was designed considering five armed responders, four of the responders would be positioned in elevated bullet-resistant enclosure (BRE) towers and one responder would be a floating responder in the facility. The floating responder could move between any of the RBs or the FHB and access rooftops on any of the RBs or FHB. The response strategy was based on the four static tower positions and the fifth responder making his way to a rooftop. During the design process it became very important to ensure that the responders had direct line-of-sight around the entire facility, including the space between turbine buildings if the adversary team attempted to breach from that side of the facility.

DMA is used for external intrusion detection at the facility. DMA allows for adversaries to be detected once they cross the outer fence of the PIDAS-like structure. DMA ensures that the requirement that adversaries can be detected before the protected area (PA) is breached. DMA is based on RADAR technology, video motion detection (VMD) and machine learning to screen out nuisance alarms and generate alarms based on objects that are continually moving toward target locations. The DMA stations ensure that detection of an adversary can be achieved after the OCA is breached. The combination of line-of-sight for the responders to the OCA becomes very valuable for engaging the adversary force and increases the open space that adversaries must traverse before they enter any of the buildings inside. This facility requires the use of five DMA stations to properly ensure adequate detection to the OCA boundary. The primary reason for multiple DMA stations is that the buildings within the facility block some of the RADAR which requires additional stations to ensure adequate detection around the facility. The figure below shows the placement of DMA stations around the facility.



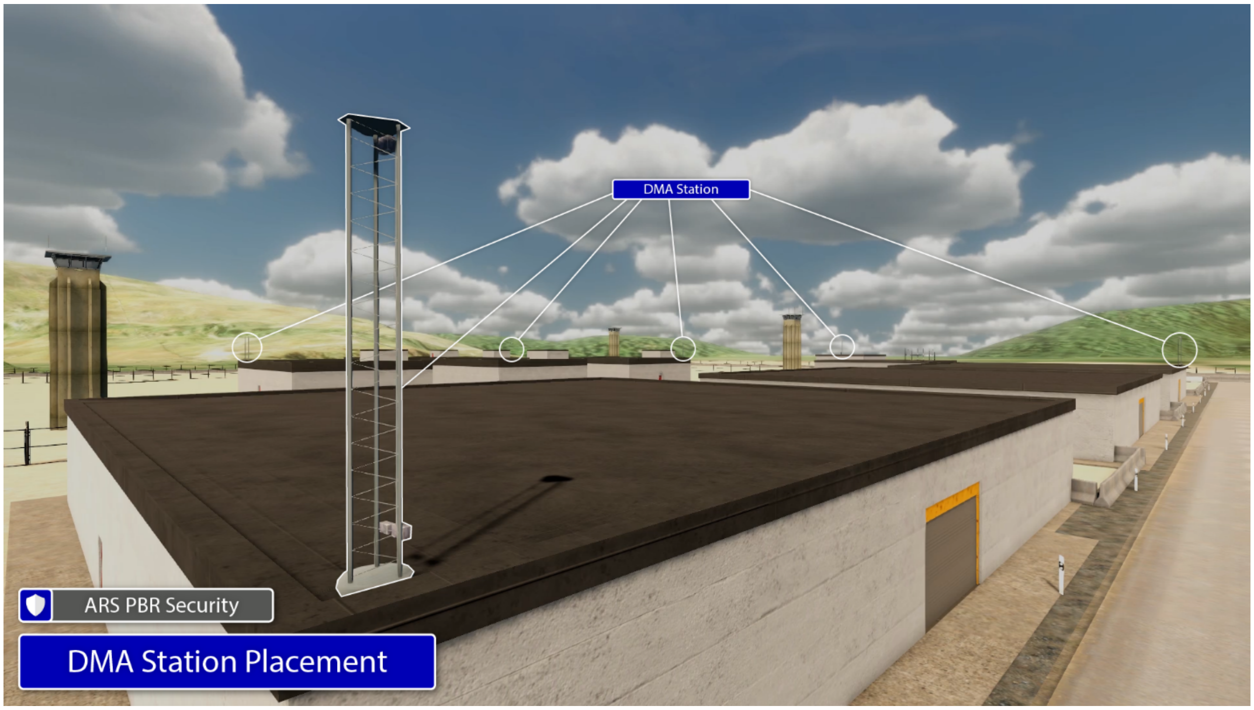


Figure 8 DMA Placement

The figure below shows the location of the response towers and subsequent figures show the responder points of view (POV) from these towers. Additionally, the rooftops on the RBs and the FHBV are designed with a hardened parapet. The parapet is made of BRE material to provide cover to the floating responder as they move to different elevated fighting positions. It should also be noted both in the figure below and Figure 1 that the FHB is the only building that has a different rotation than the others. This was because the FHB rooftop provides a clear line-of-sight between reactor buildings and turbine buildings, using a different orientation, to increase the engagement opportunity for the floating armed responder.

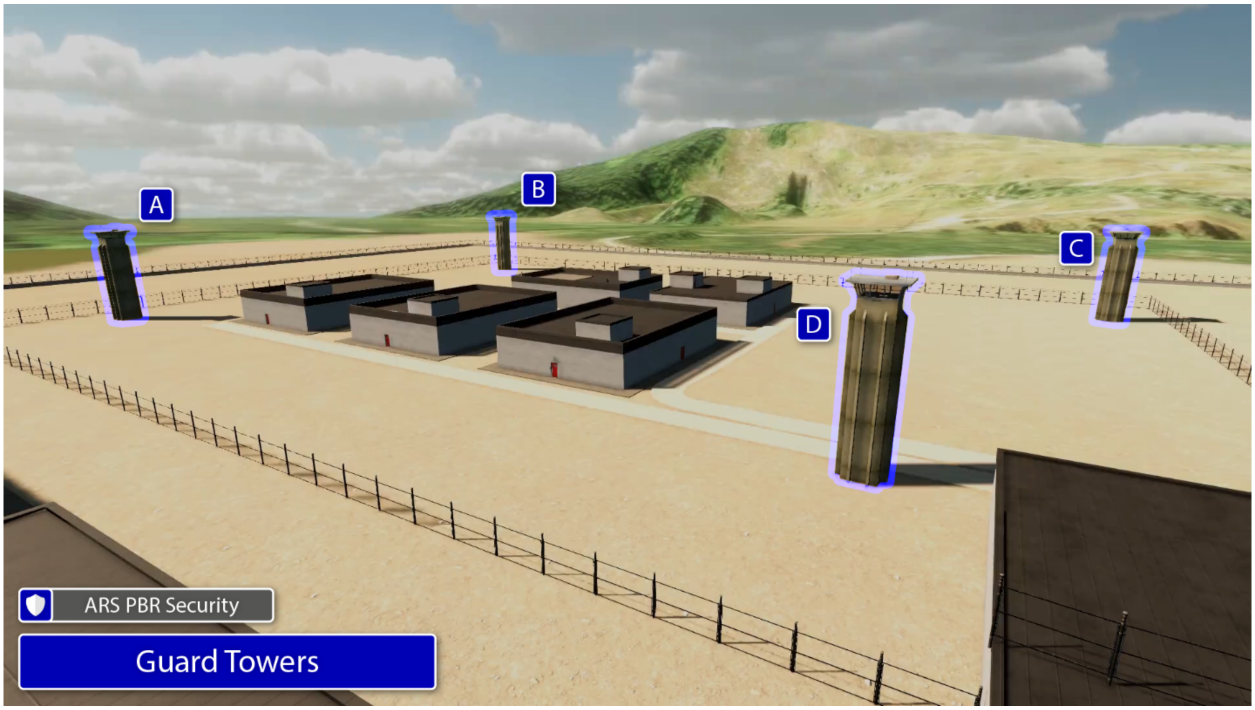


Figure 9 Guard Tower Locations

Figure 10 Response POV from Tower A

Figure 11 Response POV from Tower B

Figure 12 Response POV from Tower C

Figure 13 Response POV from Tower D

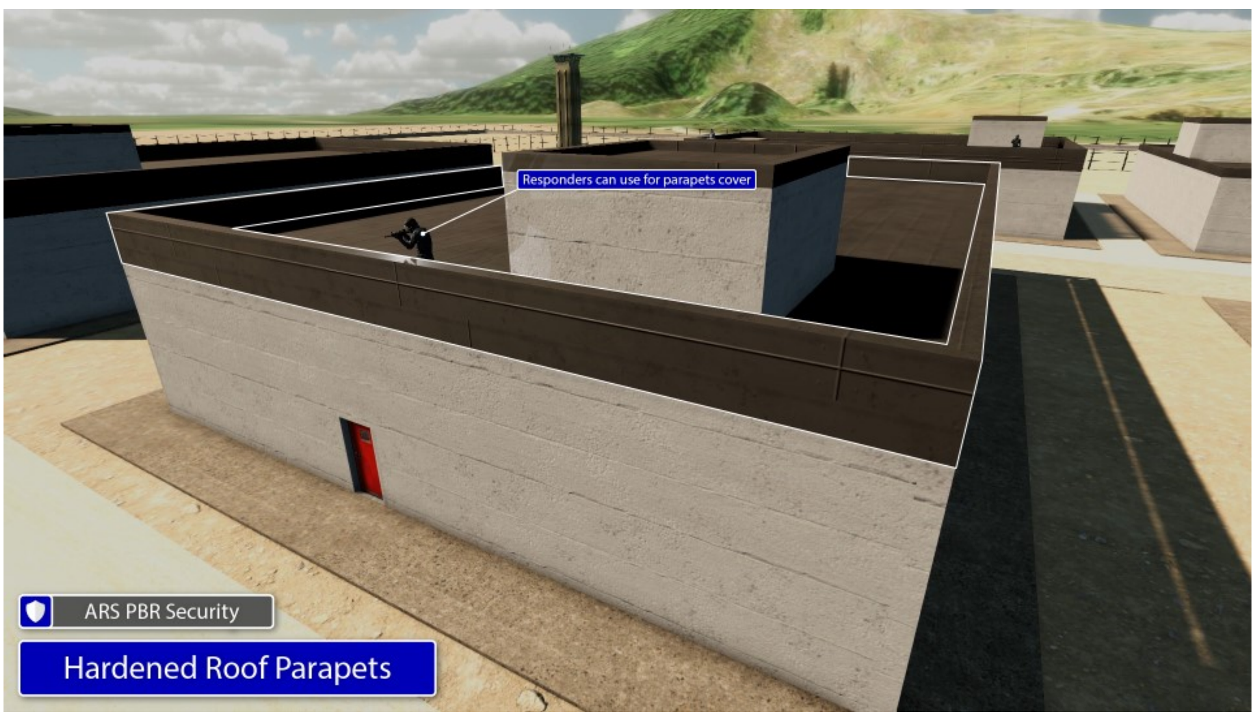


Figure 14 Roof Parapets

The entryway into each of the RBs and FHB is protected by a badge and PIN (personal identification number) reader on the outside of the door. The badge and PIN reader force the adversaries to explosively breach the exterior door of the buildings, which causes the adversary to stay on the exterior of the buildings and exposes them to the responders in towers or on any of the rooftops. Once the external door has been breached, inside of the door is a turbine grating "shark cage" that is equipped with a cypher lock. The cypher lock combination is only known by site personnel. This increases the delay time for adversaries and forces another breach that would cause the adversaries to stay exposed on the outside of the facility for longer periods of time. The shark cages are designed in such a way that successfully breaching them would require the adversaries to move out of the entryway and retreat to a standoff distance to ensure survivability of the blast. Additionally, by placing the shark cages inside, the longevity of the shark cages can be ensured because they are not exposed to the weather of the outdoor environment. During normal operations the shark cage door will be left open, during a security event the shark cages are closed when the ASO in last access control locks down the site. Each entry door for these buildings is protected in this fashion. The figure below shows these shark cages.

Figure 15 RB and FHB Shark Cages

Because all the sabotage targets at this facility are located below-grade the vital areas are also below-grade. This requires the stairwell access points to be considered as the vital area barrier. Each stairwell is protected with a badge and PIN reader, a hand geometry reader and CCTV cameras. Additionally, the concrete surrounding the stairwell is protected using a vibration sensor. This meets the requirements for alarming and controlling access to vital areas. The figure below shows these protection elements for the vital area access points.

Figure 16 Vital Area Access Points

As can be seen through the above figures, the PPS and response strategy are designed around engaging the adversaries on the exterior of the RBs and FHB to increase the likelihood that the adversary team can be effectively neutralized.

2.1. System Effectiveness Evaluation

The table below highlights the results from force-on-fore (FOF) simulations that were ran in SCRIBE3D©. The adversary attack scenario that was created involved the adversary force attacking from the south end of the facility. This attack plan was established during the TTXs that were conducted to develop the security system for this hypothetical facility. The adversaries would separate into teams to draw fire and cause confusion for the responders in the towers. The adversary team once it breached the OCA would proceed up to the PA boundary by staying close to the turbine buildings to increase the cover that was provided to them. One adversary team member would proceed up to the PA boundary to breach the fence line while the other adversary team members would provide covering fire onto the responders positioned in the towers. Once the breach was completed, the adversary force would attempt to move up to the middle reactor building (which offered the most cover) and attempt to breach into the reactor building. Once inside the adversary team would continue to move through the reactor building and proceed below-grade to sabotage the reactor or spent fuel storage locations.

The response strategy consisted of the DMA systems being able to provide the CAS operators and therefore responders in the towers known location of adversary team members. This allowed the responders in the towers to better focus their field-of-fire toward known adversary locations. The floating responder would be dispatched to the roof of the FHB as soon as possible to allow for that responder to have a line-of-sight on the adversary force. A denial of access strategy was implemented to ensure that adversaries did not enter the reactor buildings.

Table 2 PBR Neutralization Analysis

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	97	98	97	92
Red Wins	0	3	2	3	8
Average Engagements	45	67	67	77	93.7
Average killed in action (KIA) Engagements	5	6	8	9.3	11
Blue Force Count	10	10	10	10	10
Average Blue Force KIA	1.2	1.3	2	2.4	3.2
Average Blue KIA in Win	1.2	1.3	1.9	2.2	2.8
Red Force Count	4	5	6	7	8
Average Red KIA	4	5	6	6.9	7.8

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	4.5	4.3	5.6

As can be seen from the table above the PPS and response strategy are effective at neutralizing the adversary force. In the scenarios where the adversary team won (i.e. completed sabotage), shown as red team wins, the system failed because the floating armed responder could not make it to a rooftop quickly enough to add more support to the other responders in engaging the adversary.

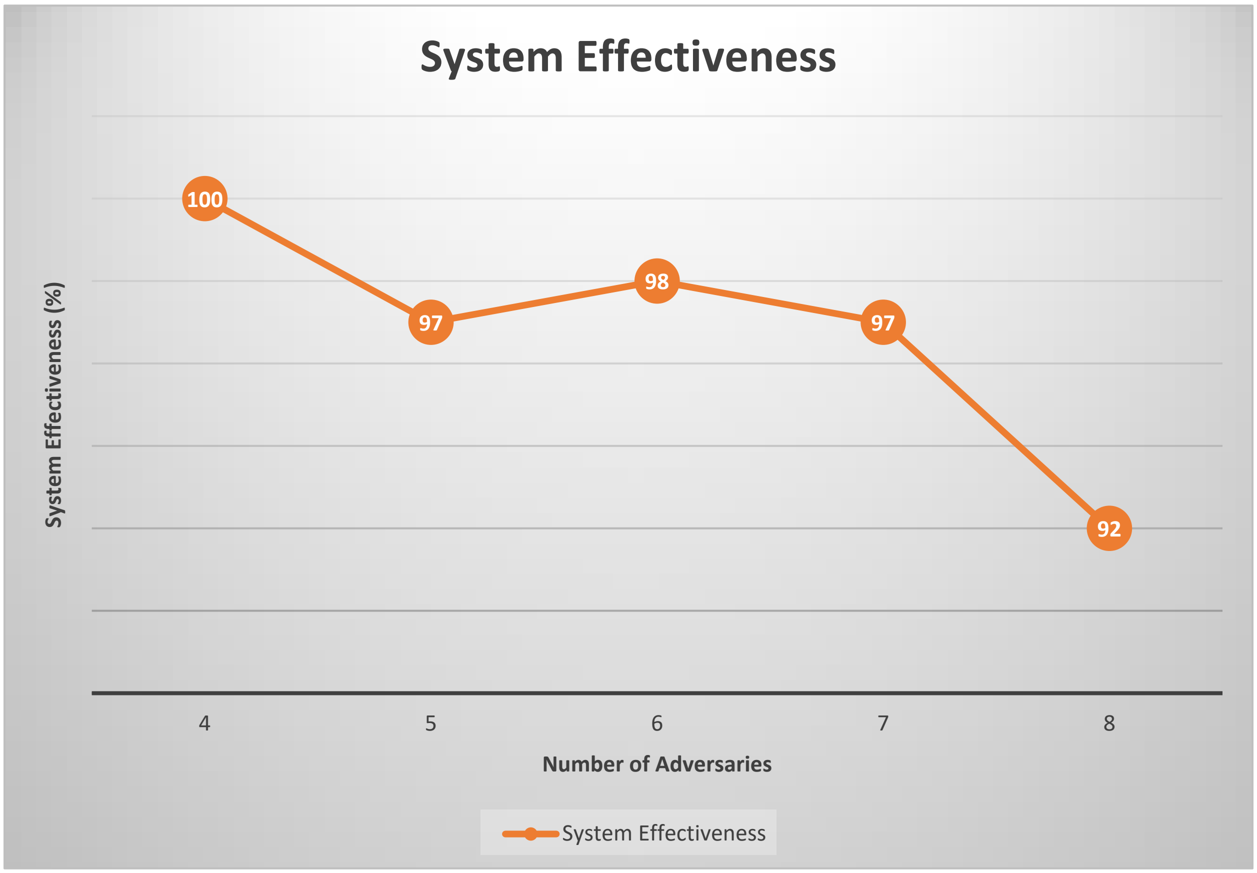


Figure 17 System Effectiveness for PBR Facility

The PBR facility was designed in such a way to maintain as small of a site footprint as possible, minimize the number of security staff as much as possible, and to decrease the security infrastructure needed to implement the strategy as much as possible. The TTXs were conducted in a way to reduce the total number of full-time positions and to reduce the complexity of the PPS for the PBR facility. A hypothetical security staffing plan for the PBR facility is shown in the table below. The table below is based on a 4.7 full-time equivalent (FTE) multiplier. This assumes 4.7 individual are required per one 24/7 position to be fully staffed.

Table 3 Hypothetical PBR Security Staff Headcount

Position	24/7 12 hr. Rotating Shift	FTE
Security Shift Supervisor	1	4.7
Field Supervisors (One Response Team Leader)	2	9.4
Alarm Station Operators (CAS/SAS)	2	9.4
Armed Responders	6	28.2
Armed Security Officers (Personnel, vehicle, and material processing)	3	14.1
Total	14	**65.8**

As can be seen from the table above, the security staffing count in total is much smaller than for a traditional nuclear power plant. The analysis that was ran only considered five armed responders, and the staffing plan consists of 6 responders. The sixth armed responder is added in as a roving responder that can relieve individual responders if needed. This should be considered in any response strategy to ensure that appropriate staffing requirements are always met. There may be ways to optimize security staffing further. Three ASOs are assumed for this facility to facilitate both personnel and vehicle access. If it can be justified that one of the positions (last access control) can be achieved by a SSS (not the response team lead) then this may allow for the reduction of one position and reduce the total full-time equivalent (FTE) number to 61.1. Additionally, the staffing plan did not consider an OCA rover since the OCA is clearly observable by all responders as well as DMA extending up to the OCA boundary. It is important that each SMR facility determine the cost-benefit tradeoff space and the regulatory risk they are willing to take on when determining staffing analysis. A description of these positions is described below.

- Alarm Station Operator (ASO): a person responsible for, but not limited to, monitoring security systems, assessing alarms, initiating response to a security threat, and making notifications to both onsite and offsite support agencies in accordance with site procedures.
- Response Team Leader (RTL): the individual responsible for directing designated members of the security force in effecting the protective strategy at the facility. The response team leader is designated by the protective strategy and identified in facility procedures.
- Security Shift Supervisor (SSS): an individual responsible for ensuring that security force personnel assigned to their shift perform their duties and responsibilities as intended and consistent with NRC requirements, site plans, and site procedures; ensuring there are an adequate number of qualified armed response team members and other security personnel available to effectively support both the normal operations and implementation of the site protective strategy; and monitoring on-duty security force members for fitness-for-duty requirements under 10 CFR 26.[3]

[3]NUREG-2203 “Glossary of Security Terms for Nuclear Power Reactors.” Amy Roundtree and Wayne Chalk. February 2017.

3. ONSITE RESPONSE FORCE FOR A MICROREACTOR

3.1. Internal Response Strategy

The lessons learned from the individual onsite response force strategies and integrating these strategies into one design were leveraged to develop a strategy for an onsite response force for the hypothetical microreactor facility[4]. The security system strategy relies on DMA as the external intrusion detection technology. Additionally, all building doors are equipped with a badge and PIN reader and a closed-circuit television (CCTV) camera to verify access to the facility. In this PPS strategy, four onsite responders were used to defend the microreactor from sabotage. Two of the responders were located on the ground floor behind bullet resistant enclosures (BREs) where the responders could view adversaries entering the building and view the adversaries before they proceeded below-grade. Two armed responders are located below-grade behind BREs that allow them to view the doorways exiting the stairwell toward the microreactor. These response positions were chosen based on responders being able to interrupt adversaries along their path and effectively engage the adversary force along their path to the target location.

The figure below shows the security measures and safety measures that have been designed into the facility. As can be seen, DMA stations are implemented as the primary external intrusion detection system. The facility uses a vehicle barrier system at an appropriate distance to prevent damage to vital areas and systems based on explosive analysis. The roof at the entry control point building is afforded roof protection using bistatic microwave sensors and a continuation of the fence line. The facility deploys mantraps at both personnel entries to increase adversary task time and ensure authorized access into the reactor building. Responders within the facility are located inside of BREs, there are two responders on the above-grade floor and two responders on the below-grade floor. Additionally, the facility has a dedicated heating, ventilation, and air conditioning (HVAC) system used to vent potential gases or incapacitating agents that could be used by the adversary force against the responders.

[4] " U.S. Domestic Microreactor Security-by-Design." Evans, A. et al. Sandia National Laboratories. SAND2021-13779R. October, 2021

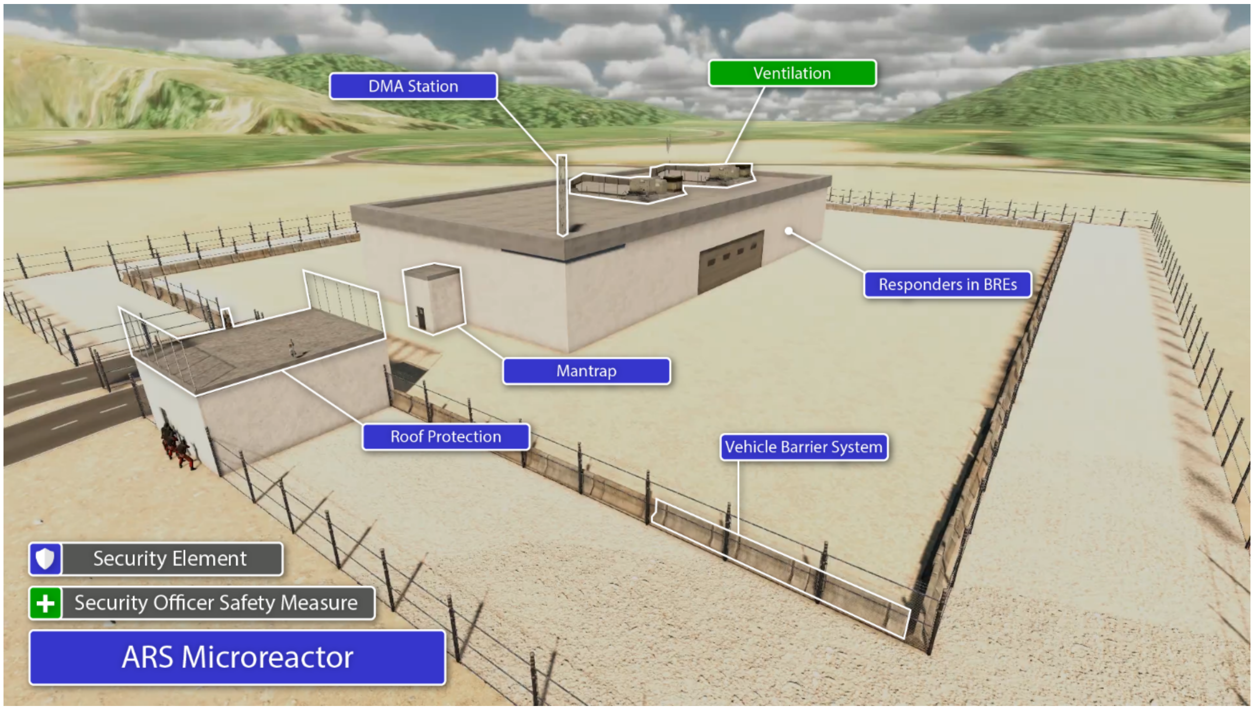


Figure 18 Internal Responders Microreactor Facility Layout

DMA is used for external intrusion detection at the facility. DMA allows for adversaries to be detected once they cross the outer fence of the PIDAS-like structure. DMA ensures that the requirement that adversaries can be detected before the PA is breached. In this facility design, one DMA station is used to provide intrusion detection around the facility. The figure below shows how the DMA station is implemented at the facility.

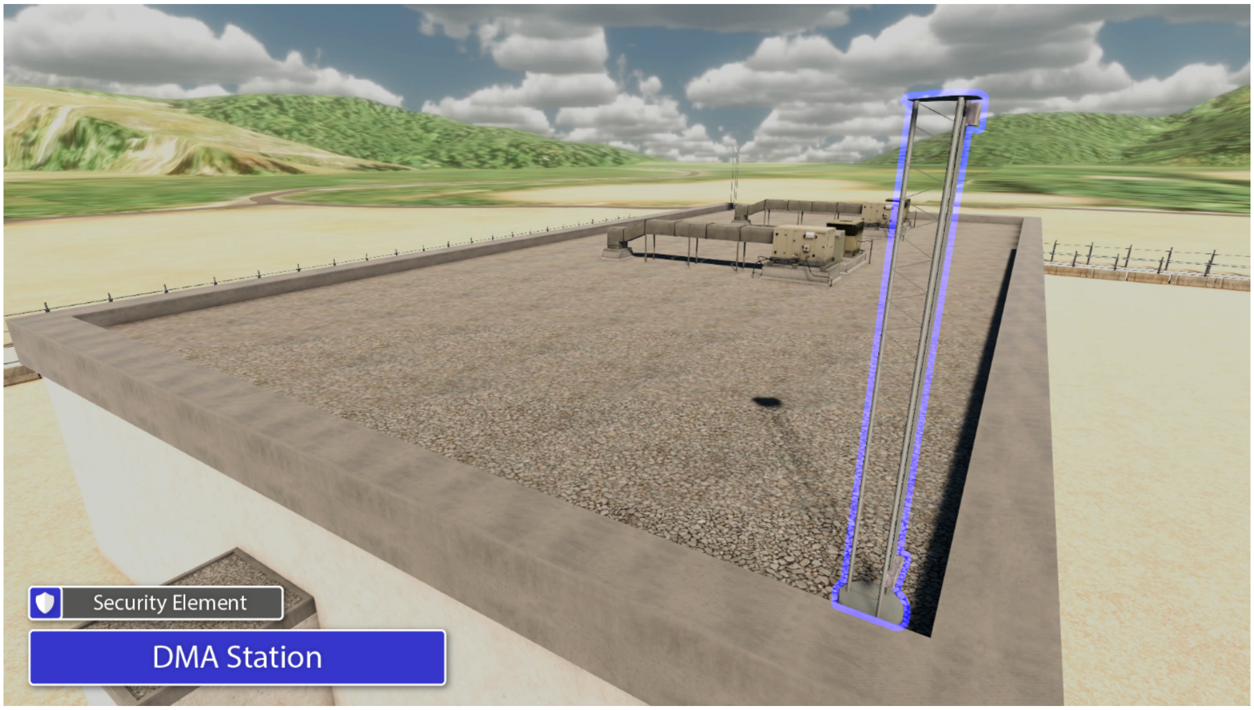


Figure 19 DMA Station

The figure below shows the protection to the roof of the entry control point (ECP) building. Because DMA is based on RADAR technology and VMD to conduct attention, the ECP building blocks the view of the RADAR. Because of this, the roof of the ECP is protected by a continued fence line and bistatic microwave sensors to ensure that detection can occur before the PA is breached. By using DMA as the primary external intrusion detection system complemented by microwave sensors on the ECP roof, the facility can ensure that a continuous line of detection is provided around the entire facility before an adversary can breach the protected area boundary.

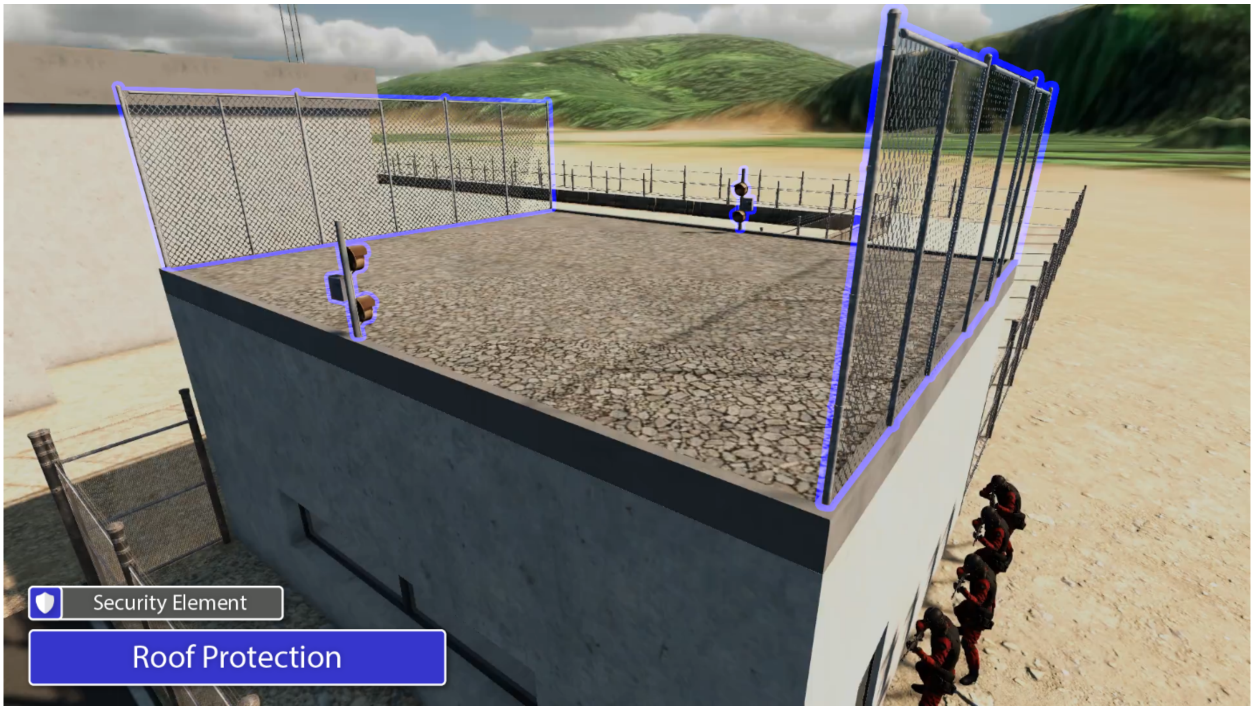


Figure 20 Roof Protection

The figure below shows how mantraps are implemented at both personnel entry points into the reactor building. On the outside of the reactor building, badge and PIN readers are implemented. Once an individual presents a proper badge and correct PIN, the individual can enter the interior of the mantrap. Once inside the CCTV camera will automatically populate live video of the inside of the mantrap. This allows the CAS operator to verify the identity of the individual entering matches the photo on the badge at the exterior badge reader. Inside of the mantrap, a hand geometry reader and another badge and PIN reader provides access into the reactor building. All doors within the PA are alarmed by magnetic locks and a badge and PIN reader. The combination of mag locks and badge and PIN readers ensures that only authorized access credentials can unlock doors into the facility. Additionally, all doors within the PA are security doors that increase adversary task time compared to traditional construction doors.

Figure 21 Mantrap

The figure below shows the vehicle barrier system (VBS) deployed on the inside of the PA. The VBS for this facility was designed and placed at a location that ensures that a DBT VBED does not cause damage to a vital area or vital equipment and ensures the survivability of the responders of the facility. It is important to note that a properly placed VBS meets two security functions. The first function is to prevent VBEDs from damaging the facility or causing radiological release from the facility and to ensure the survivability of responders protecting the facility. Secondly, the VBS can force adversaries to attack the facility on foot and this causes the adversary task time to increase and potentially increase the effectiveness of the PPS.

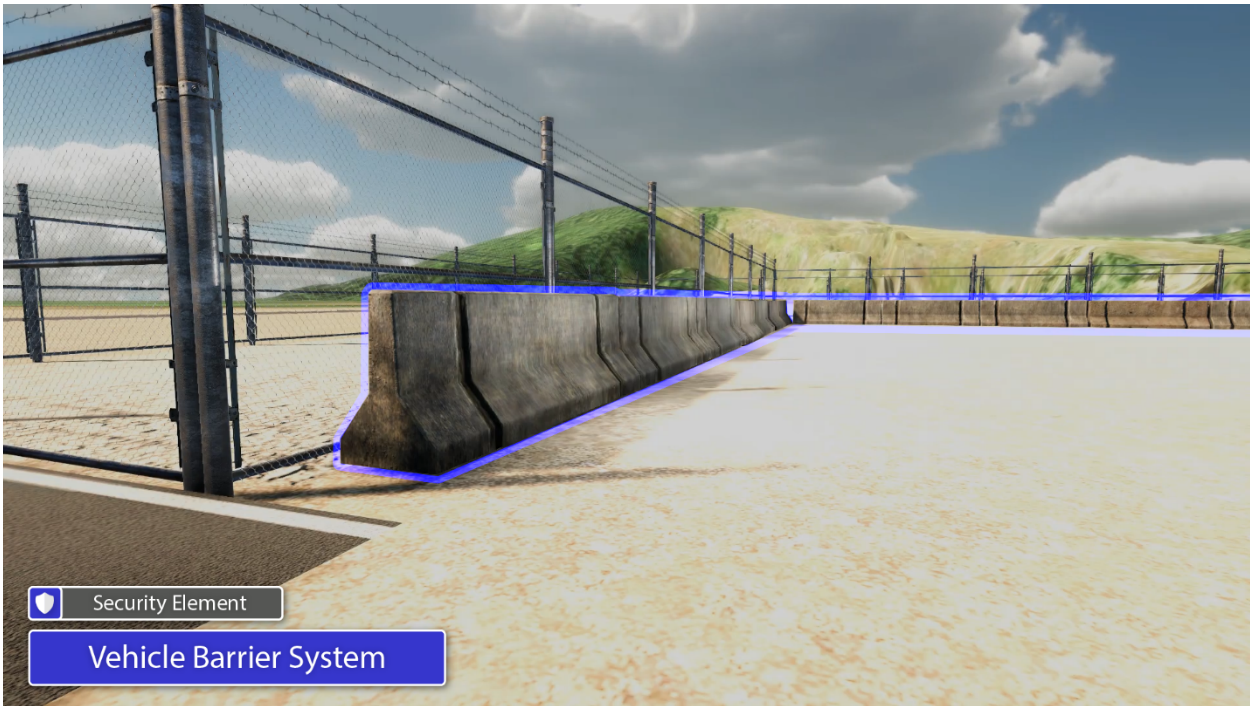


Figure 22 Vehicle Barrier System

The figure below highlights responders in internal BREs. Responders inside are positioned in such a way that they can view the entry doors into the reactor building. On the above-grade floor, the responders are in positions to view adversaries upon entry into the personnel doors and the high-bay door. On the below-grade floor, responders are able to view the adversaries after exiting the stairwell into the below-grade portion of the facility. BREs that are designed for responders must be designed to be resistant to DBT weapon capabilities and resistant to DBT explosives capabilities.

Figure 23 Responders in BREs

The figure below shows the ventilation system that is meant to exhaust air and fumes from the below-grade floor of the facility and recirculate fresh air from the outside. This feature arose from TTXs that had been conducted. Adversaries may have the ability to use incapacitating agents, chemicals, or gases, and in a confined space those can incapacitate or kill armed responders. For this reason, a ventilation system was designed to ensure the safety of the armed responders. This ventilation system is also designed with delay barriers on the rooftop portions to prevent adversaries from penetrating the building from the HVAC system and intrusion detection technologies to detect adversaries attempting to penetrate the facility through the HVAC system.

Figure 24 Ventilation System for Internal Responders

3.1.1. Microreactor Vital Area Protection

To ensure protection of vital areas it is first important to identify the vital areas at a facility. This facility contains one vital area, the below-grade floor of the facility. This floor is where the microreactor, safety systems and radioactive material are located. Because of this, the vital area barrier will be the doors leading from the stairwells into the below-grade floor, the equipment hatch cover that allows for equipment to be lowered into the below-grade floor, and the ceiling between the below-grade floor and the above-grade floor. The vital area barriers are designed in such a way that hand tools alone cannot penetrate the vital area barriers. The equipment hatch can only be opened from the CAS and must be opened by the SSS and the operations manager. In addition, the cover for the equipment hatch is a 2-foot thick reinforced concrete cover that provides the same level of protection as the 2-foot thick reinforced concrete floor. The doorways leading from the stairwell into the below-grade floor are security doors and are protected by access control devices and CCTV cameras to ensure proper access authorization is followed for entry into the below-grade floor.

3.1.2. Internal Response Strategy System Effectiveness Evaluation

different attack scenarios were analyzed. The first attack scenario considered the adversary team attacking the facility as one large group through the ECP and then into the reactor building. After entry into the reactor building the adversary team entered the below-grade portion of the facility to sabotage the micro reactor. The second scenario assumed the adversary team split into two groups. The first group attacked through the ECP and then into the reactor building, while the second group attacked from the opposite side of the facility. The goal for the adversary team was to enter the building from two different locations simultaneously to cause greater difficulties for the response force inside. The results from this scenario across an adversary range of 4-8 members can be seen below (the results assume the lowest number of blue force wins based on the two scenarios considered). The blue force is considered to win when the adversary team is rendered incapable of completing sabotage of the micro reactor. Red force wins are recorded when the adversary team successfully completes sabotage of the micro reactor.

Table 4 Four Responders PPS Strategy

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	99	99	96	93
Red Wins	0	1	1	4	7
Average Engagements	17	28	29	33	38
Average killed in action (KIA) Engagements	4	6	7	8	9
Blue Force Count	4	4	4	4	4
Average Blue Force KIA	0	1	1	1	1
Average Blue KIA in Win	0	1	1	1	1
Red Force Count	4	5	6	7	8
Average Red KIA	4	5	6	7	8

Name	Results: 4 Adversaries	Results: 5 Adversaries	Results: 6 Adversaries	Results: 7 Adversaries	Results: 8 Adversaries
Average Red KIA in Win	N/A	0	5	5	5

An additional sensitivity analysis was carried out to determine the system effectiveness as the number of responders was decreased from 4 to 3, and again from 3 to 2. This allows for a systematic study to determine the ideal number of responders needed to achieve high system effectiveness.

Table 5 Three Responders PPS Strategy

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	98	91	90	92	79
Red Wins	2	9	10	8	21
Average Engagements	21	29	27	32	36
Average killed in action (KIA) Engagements	4	5	7	8	9
Blue Force Count	3	3	3	3	3
Average Blue Force KIA	0	1	1	1	1
Average Blue KIA in Win	0	0	1	1	1
Red Force Count	4	5	6	7	8
Average Red KIA	4	5	6	7	7
Average Red KIA in Win	3	2	3	5	5

Table 6 Two Responders PPS Strategy

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	95	83	82	84	60
Red Wins	5	17	18	16	40

Name	Results: 4 Adversaries	Results: 5 Adversaries	Results: 6 Adversaries	Results: 7 Adversaries	Results: 8 Adversaries
Average Engagements	21	27	25	30	31
Average killed in action (KIA) Engagements	4	5	6	7	7
Blue Force Count	2	2	2	2	2
Average Blue Force KIA	1	1	1	1	1
Average Blue KIA in Win	0	0	0	0	0
Red Force Count	4	5	6	7	8
Average Red KIA	4	5	5	6	6
Average Red KIA in Win	1	2	2	2	2

3.2. External Responder Strategy

Additionally, another scenario that was analyzed was four responders placed in bullet resistant towers. These responders were in strategic locations that allow the response force to view all entry points into the reactor building and into the protected area. The responders are placed in such a way that the entire protected area can be viewed from all four towers. The basis of the PPS is the same as the strategy with internal responders, the only variation is four responders located in external BRE towers. The figure below shows this site layout.

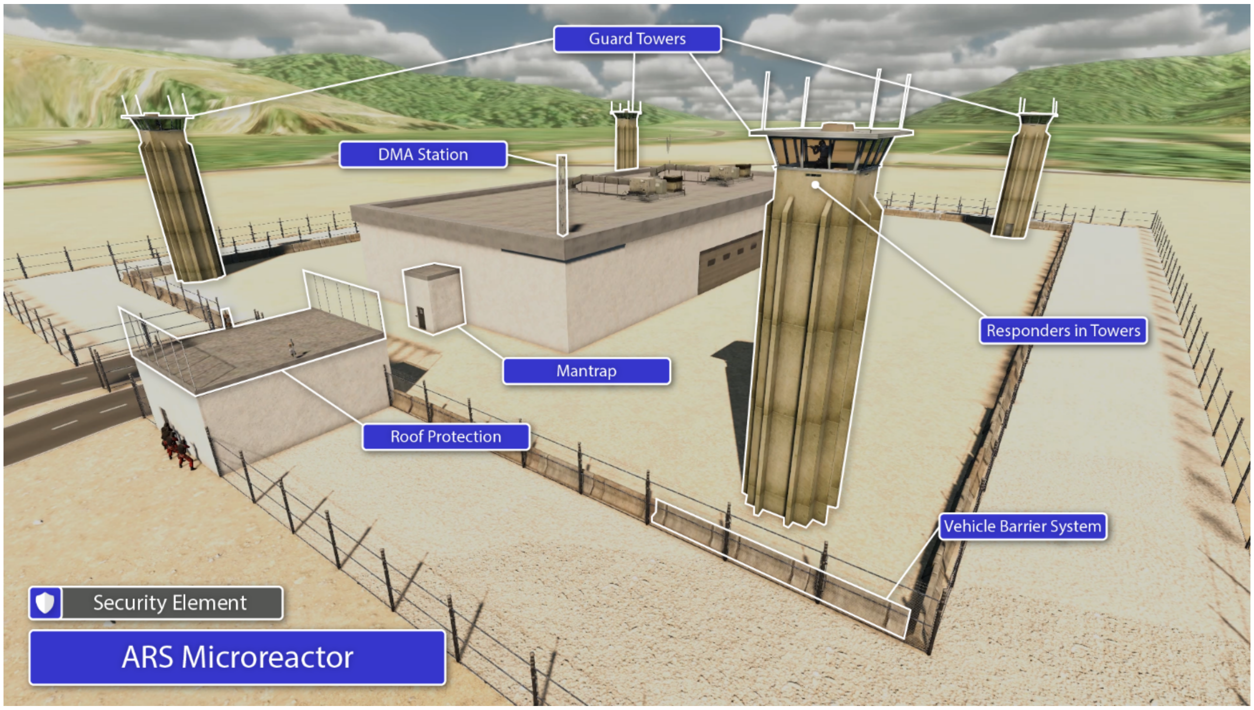


Figure 25 Responders in Towers Microreactor Facility Layout

The figure below shows the field-of-view that the responders can see from a tower and how the four towers are in line-of-sight of one another.

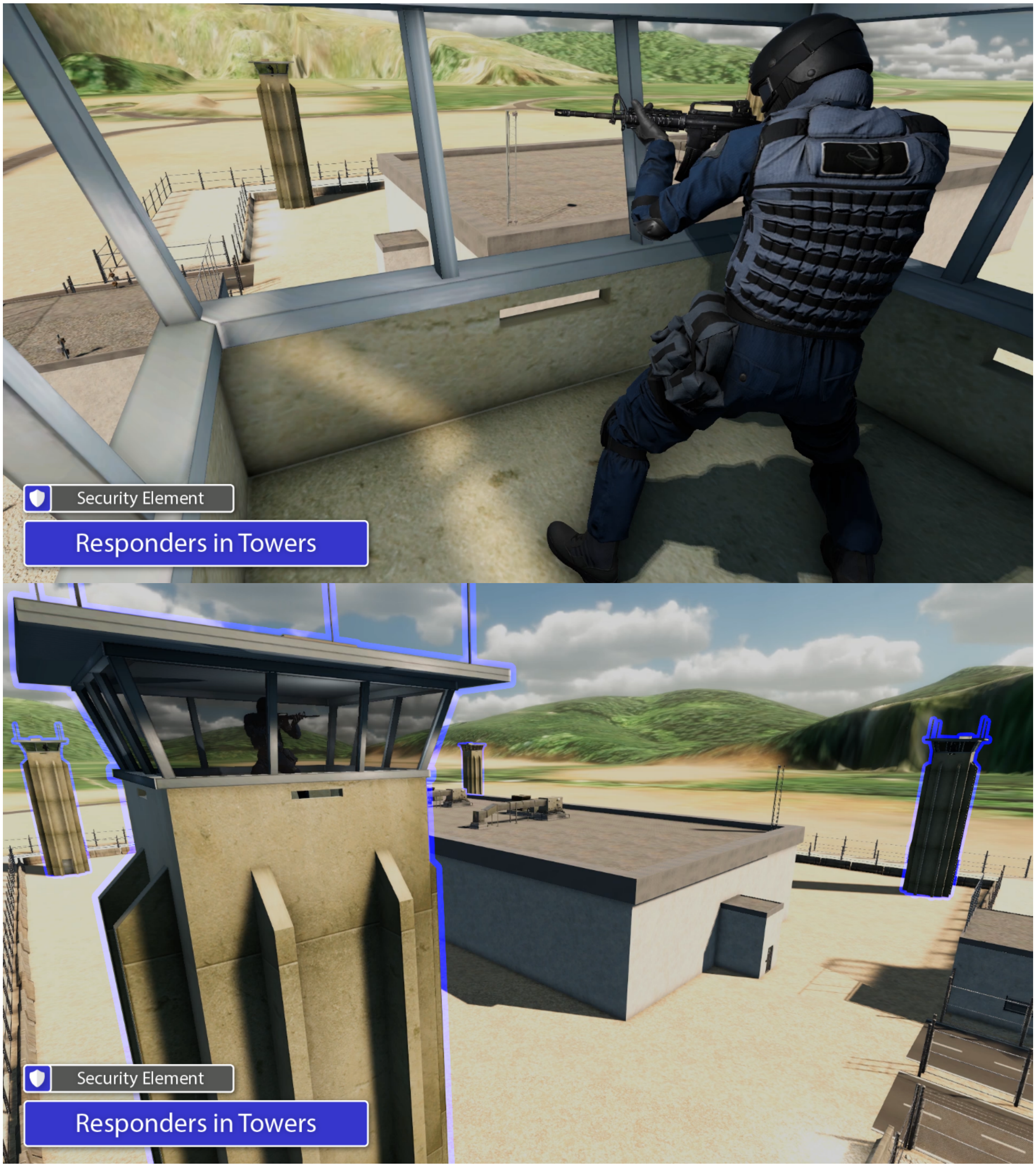


Figure 26 Responders in Towers

3.2.1. External Response Strategy System Effectiveness Evaluation

Like the range of adversaries and the two attack scenarios that were ran for the internal response force strategy, the same range of adversaries and the same adversary capabilities are evaluated using four external BRE towers. The table below shows these results.

Table 7 Four Responders in Towers

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	97	90	85	78
Red Wins	0	3	10	15	22
Average Engagements	11	15	30	35	43
Average killed in action (KIA) Engagements	4	5	7	8	9
Blue Force Count	4	4	4	4	4
Average Blue Force KIA	0	0	1	1	2
Average Blue KIA in Win	0	0	1	1	1
Red Force Count	4	5	6	7	8
Average Red KIA	4	5	6	6	7
Average Red KIA in Win	N/A	1	4	3	4

3.3. System Effectiveness Comparison

From the figure below, the highest system effectiveness was achieved by the PPS that utilized four responders in BREs inside of the reactor building. However, the PPS that used four responders in towers had a high system effectiveness until the adversary team size reached six individuals. Once the adversary team reached six, the PPS that used three responders in BREs inside of the building increased in system effectiveness. This analysis also shows that decreasing the onsite response force numbers decreases system effectiveness across all adversary team sizes. The most effective PPS for all adversary team sizes is the PPS that uses four responders internal to the facility in BREs.

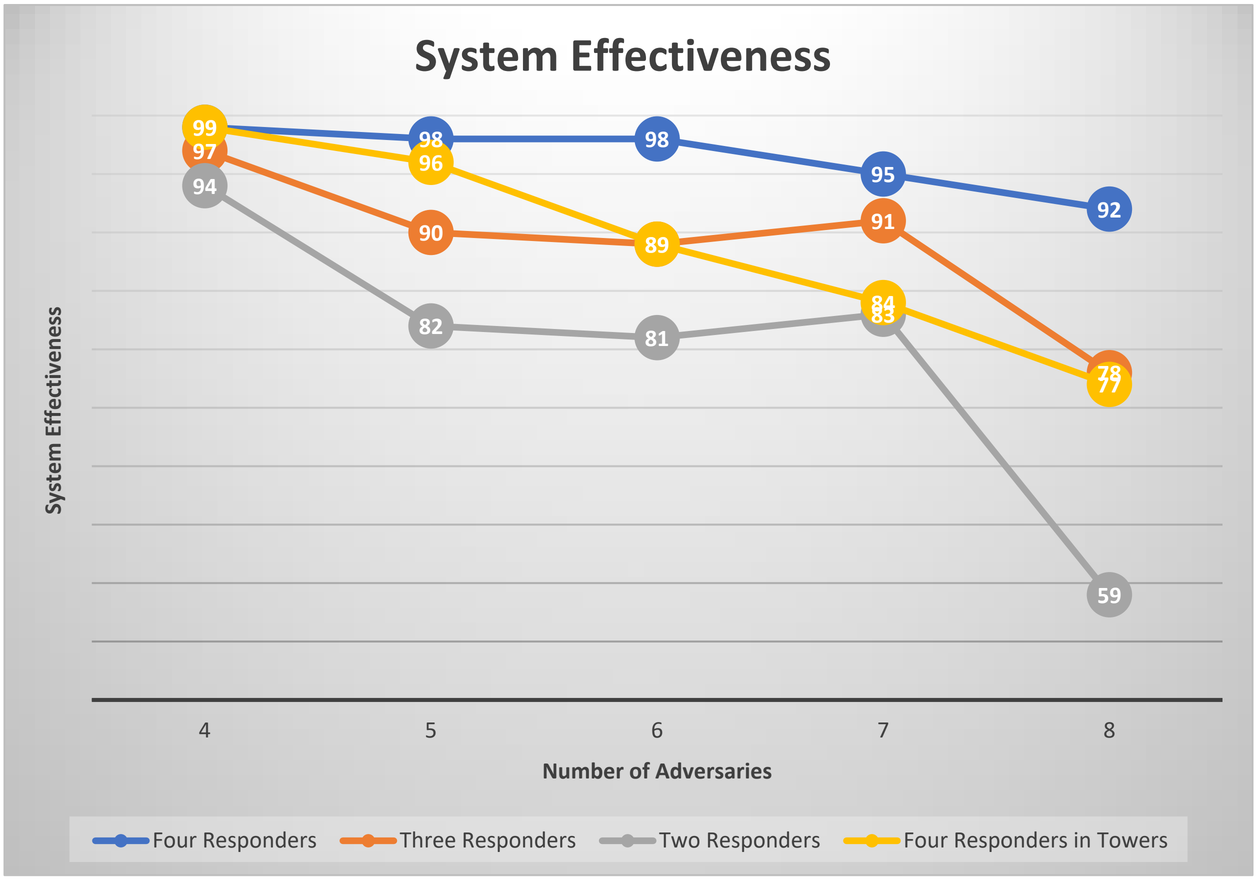


Figure 27 System Effectiveness vs Response Force Numbers

Below are staffing plans for the hypothetical microreactor for all response force configurations.

Table 8 Hypothetical SMR Staffing Plan - 4 Internal Responders or 4 Towers

Position	24/7 12 hr. Rotating Shift	FTE
Security Shift Supervisor	1	4.7
Field Supervisors (One Response Team Leader)	2	9.4
Alarm Station Operators (CAS/SAS)	2	9.4
Armed Responders	5	23.5
Armed Security Officers (Personnel, vehicle, and material processing)	3	14.1
Total	13	**61.1**

Table 9 Hypothetical Microreactor Staffing Plan - 3 Internal Responders

Position	24/7 12 hr. Rotating Shift	FTE
Security Shift Supervisor	1	4.7

Field Supervisors (One Response Team Leader)	2	9.4
Alarm Station Operators (CAS/SAS)	2	9.4
Armed Responders	4	18.8
Armed Security Officers (Personnel, vehicle, and material processing)	3	14.1
Total	12	**56.4**

Table 10 Hypothetical Microreactor Staffing Plan - 2 Internal Responders

Position	24/7 12 hr. Rotating Shift	FTE
Security Shift Supervisor	1	4.7
Field Supervisors (One Response Team Leader)	2	9.4
Alarm Station Operators (CAS/SAS)	2	9.4
Armed Responders	3	14.1
Armed Security Officers (Personnel, vehicle, and material processing)	3	14.1
Total	11	**47**

There may be ways to further reduce the staffing counts. For example, the analysis that was ran only considered four, three and two armed responders, and the staffing plan consists of five, four, and three responders. The extra armed responder is added in as a roving responder that can relieve individual responders if needed. This should be considered in any response strategy to ensure that appropriate staffing requirements are always met. Additionally, three ASOs are assumed for this facility to facilitate both personnel and vehicle access. If it can be justified that one of the positions (last access control) can be achieved by a field supervisor (not the response team lead) then this may allow for the reduction of one position and reduce the total FTE Additionally, the staffing plan did not consider an OCA rover since the OCA is clearly observable by all responders as well as DMA extending up to the OCA boundary. It is important that each SMR facility determine the cost-benefit tradeoff space and the regulatory risk they are willing to take on when determining staffing analysis.

4. CONCLUSIONS AND LESSONS LEARNED FROM ONSITE RESPONSE DESIGN

The design meetings that were held with the individual SMEs allowed for lessons learned and recommendations to be made when considering designing a physical security system for an SMR that relies on an onsite response force. The first lesson learned was to ensure the integrity of contraband searches for both personnel and vehicles. When searches are conducted at the outer security layer, persons and vehicles can move around the outer security area unmonitored. One of the ways to ensure this that was discussed is to ensure that the DMA intrusion detection technology maintains surveillance of individuals after the enter the security area, or to ensure that ASOs conducting searches at an outer security layer escort the vehicle to the next search area. DMA might be used to identify if personnel are staying around the edge of the security layer for a contraband item to get passed to them. In the site design the DMA detection envelope was designed to extend beyond the outer security fence line. By extending the detection envelope beyond the fence line any adversaries or individuals attempting to move into the security layer can be detected and the onsite response force can be used to investigate those individuals. However, by extending DMA detection beyond a controlled security layer, additional operational considerations must be made. For example, a parking lot for site employees may need to be pushed further away from the site to not interfere with the DMA detection envelope. For vehicles entering the site, the vehicles must be searched before entering the protected area. Once a vehicle has entered the site escorts should be used to escort the vehicle to its destination on site. The vehicle escort allows for search integrity to be maintained while the vehicle is on site. Additionally, at all search points two security personnel should be always present and at least one of the security personnel should be armed. If the vehicle ECP and the personnel ECP is located at the same point, it was suggested that three individuals should be present. This ensures that there are enough security personnel to conduct personnel searches and vehicle searches at the same time. When conducting a vehicle search, it is recommended that two security personnel conduct the search and that one of the security personnel be armed. Across all the different designs and security system postures, all SMEs suggested having an extra armed security officer at the entry control point locations that could be used to provide key service, access control, contraband searches, relive the CAS operator, or relieve a responder from a position. By having an armed security officer that is cross trained to provide all these services can provide an advantage for the site.

It is also important to consider the logistical impacts of having personnel onsite at a nuclear facility. Current nuclear power plants have cafeterias and vending machines that serve food and other items to onsite personnel. Many of the current nuclear power plants have cafeterias that are located inside of the PA. These cafeterias require vehicles and personnel to staff. These vehicles and personnel increase the operational burden on a facility and can potentially lead to increase costs. The facility designs that have been developed for ARS have not included a cafeteria or other such service buildings. These are some of the operational concerns and logistical concerns that should be considered by SMR facility designers and operators.

The next steps under this work are to develop a hypothetical sodium-fast reactor and determine appropriate PPS strategies that are effective. Additionally, another report will be generated to highlight the PPS effectiveness and cost analysis across the hypothetical PBR, microreactor, sodium-fast reactor, and across different response strategies. The work ongoing is meant to inform SMR vendors and microreactor vendors on effective PPS strategies for these facilities.

APPENDIX A. THREAT ASSUMPTUINS AND CHARACTERIZATION

The DBT assumed for this analysis is based on information from the 10 Code of Federal Regulations Part 73.1 (i.e., 10 CFR 73.1) see Table 2. The adversary team members were assumed to have the following characteristics:

- A determined violent external assault
    - Attack by stealth or deceptive actions
    - Operate in groups through a single-entry point
    - 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
- Active or passive insider
- Land or water vehicles, which could be used for transporting personnel and their hand-carried equipment to the proximity of Vas
- Land vehicle bomb assault, which may be coordinated with an external assault
- Cyber attack
- Able to perform any of the tasks needed to steal or sabotage critical assets
- Armed with a 7.62 mm rifle or 7.62 mm belt-fed machine-guns (2), a pistol, ammunition, grenades, satchel charges containing bulk high explosives, not to exceed 10 kg total, detonators, bolt cutters, and miscellaneous other tools[5]
- Each able to carry a man-portable total load,29.5 kg [65 lb.]
- Adversary run speeds are assumed to be 3 m/s

For all scenarios, it was assumed each attack would start when the adversaries verified that no response force element (e.g., roving patrol) was within visual range of the initial breach. They would also avoid hardened and manned response positions if possible. See Table 6.

[5] 10 Code of Federal Regulations Part 73 "Physical Protection of Plants and Materials." https://www.nrc.gov/reading- rm/doc-collections/cfr/part073/full-text.html

Table 11 Outsider High-Level Threat Assessment Used for Analysis

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

DISTRIBUTION

Email—Internal

Name	Org.	Sandia Email Address
Alan Evans	06812	aevans@sandia.gov
Technical Library	01977	sanddocs@sandia.gov

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.