Cyber-Physical Tabletop Exercise for Small Modular Reactor Facilities

Prepared for

U.S. Department of Energy

Alan Evans[1], Steve Sweet[1], Andrew Hahn[1], Remy Pierce[1]

Charlie Nickerson[2]

[1]Sandia National Laboratories

[2]Idaho National Laboratory

September 2025

SAND2025-12429R

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

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

ABSTRACT

U.S. nuclear power facilities face increasing challenges in meeting dynamic security requirements caused by evolving and expanding threats while keeping costs reasonable to make nuclear energy competitive. This evolving threat landscape includes adversaries having offensive cyber capabilities to attack information technology (IT) systems and operation technology (OT) systems. These adversaries may have the ability to attack the physical protection system (PPS) networks with potential consequential impacts that could degrade the effectiveness of the PPS. These cyber attacks may also be used to attack the safety and operational systems used to operate and ensure the safety of the reactor. Additionally, adversaries may gain access to unmanned aerial systems (UAS) that may be used to provide reconnaissance and surveillance of the facility, provide information to the adversaries, and be equipped with kinetic capabilities such as explosives or weapons that can be used to directly attack the facility. The Department of Energy's Office of Nuclear Energy's Advanced Reactor Safeguards and Security (ARSS) program funded Sandia National Laboratories (SNL) and Idaho National Laboratory (INL) to develop a cyber-physical tabletop exercise (TTX). This exercise was conducted on a hypothetical small modular reactor (SMR) facility, and only considered a potential adversary cyber attack on the PPS to a physical attack on the hypothetical facility to achieve a radiological release. This cyber-physical TTX is meant to provide lessons learned to integrate the cyber security system design and the physical protection system (PPS) design to decrease design, operation, and maintenance costs as well as increase effectiveness for defending against design basis threat attacks at the facility. This TTX will also provide a framework and method for SMR and microreactor vendors to conduct their own cyber-physical TTX and gain impactful insights to improving the cyber and physical protection system design for their SMR or microreactor facility design.

ACKNOWLEDGEMENTS

The team would like to acknowledge the many subject matter experts who contributed their expertise to the development of this exercise, the design recommendations, and to conduct this cyber-physical tabletop exercise.

CONTENTS

LIST OF FIGURES

ACRONYMS AND DEFINITIONS

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

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

1. INTRODUCTION

Small modular reactor (SMR) and microreactor vendors are facing unique design choices and a unique operational environment. SMR vendors will be faced with an uncertain regulatory environment, competing economic constraints, and many new adversary capabilities that may impact the overall design of a cybersecurity system and physical protection system (PPS). SMR vendors will be faced with a design that considers defending against external threats physically attacking the facility, insider threats that may attack the facility or pass information along to external actors, actors that may use cyber attacks on the PPS or the operational and safety systems, unmanned aerial systems (UAS), or a combination of these threats to attack an SMR facility. These attacks should be considered by SMR vendors in the design phase. By considering these various attack vectors in the design phase SMR vendors may be able to realize cost savings while improving the overall effectiveness of the security system to defend against possible adversary attacks on the facility.

This cyber-physical TTX attempts to evaluate various conceptual areas. These conceptual areas and questions are identified below.

1. Cyber Attack Effectiveness
    a. How much did the cyber attack contribute to delaying detection?
    b. Did the cyber attack remove any security layers, or did it just delay engagement with the attacking force?
    c. If the cyber attack did not exist, how much sooner would the response force have detected and engaged the attackers?
    d. Was there a critical point of failure in cyber defenses that made the attack more effective (e.g. shared credentials, flat network)?
2. Physical Protection System Resilience to Attack
    a. What PPS elements (response towers, lighting, human performance) made the biggest difference in stopping the attack?
    b. How did the engineering of response positions influence the outcome?
    c. If the response force were compromised (fatigued, understaffed, disorganized), would any of these attacks have succeeded?
    d. Are delay barriers on door entrances a critical delay mechanism, or were they just a minor obstacle?
3. Identifying Insights for Cyber-Physical Security Integration
    a. Did the cyber attacks play a critical role or was the resilience of the physical protection system the deciding factor?
    b. If the attackers had purely relied on physical breach techniques, would the outcome have been different?
    c. How can a PPS be designed so that cyber compromise does not lead to a radiological release from an act of sabotage?

PPS designs have utilized tabletop exercises (TTXs) for decades to consider design choices that could be made to develop an effective PPS. TTXs may consider the use of all adversary capabilities, including cyber attacks, in a TTX to develop design choices that may improve the effectiveness of the PPS. This report will

summarize the results from a cyber-physical TTX conducted at Sandia National Laboratories (Sandia) with subject matter experts (SMEs) from SNL and Idaho National Laboratory (INL). Additionally, this report will outline a framework and method that SMR or microreactor vendors can utilize to conduct their own exercise to design an effective cybersecurity system and PPS.

2. TABLETOP EXERCISE SETUP

The cyber-physical TTX considered a three-unit SMR facility with an established PPS design. By utilizing an established PPS design the PPS operational network could be easily identified. The PPS has many electronic security measures including access control devices, sensors, magnetic locks, an onsite central alarm station (CAS), shark cages, turbine grating delay barriers, and an offsite secondary alarm station (SAS). The TTX considered multiple different attack scenarios and alternating blue teams (facility response and cybersecurity teams) and red teams (adversary attack teams). This allowed for many different attack scenarios to be analyzed against the facility and various SMEs to implement measures to defend the facility against an attack and different methods for attacking a facility to be considered. This ensures a wide-range of attack vectors are chosen and different measures and strategies to be considered to defend the facility against the different attack vectors. To conduct the TTXs three teams were created. The green, red, and blue teams consisted of one cybersecurity SME and one physical protection SME. Additionally, the tabletop used a SCRIBE3D operator. When the Cyber Security Operation Center (CSOC) was involved in an exercise, the Sandia Experiment Control System (ECS[1]) was used to simulate the cyber attacks and operator interfaces.

2.1. Scenario Development

Each TTX started with the development of an adversary attack scenario and development of the response approach to postulated adversary attack scenarios. For each scenario analyzed, the red and blue teams had approximately one-hour to design the adversary attack scenario and the response force strategy for the adversary attack scenario. The red and blue teams are each provided their own individual room to develop their adversary attack scenarios and response force planning, and the green team moves between rooms to facilitate the scenario development. During this time, the red team would consider and document the following:

- The proposed cyber attack and attack vector
- What systems and technologies the proposed cyber attack would interrupt or disable
- The movements of the ground-based adversary attack team
- The use of a vehicle-borne explosive device
- The overall sabotage target at the facility
- A full adversary pathway from outside of the facility to the target location

During this time, the blue team would consider and document the following:

- The proposed response strategy to postulated adversary attack scenarios
- Identify security technologies that would be critical to facilitate an effective response strategy

During this time, the green team is:

- Moving between the red and blue team planning rooms to gain an appreciation for the adversary attack plan and response strategy
- Determining if adversary strategies, adversary turns, and adversary capabilities to be used are acceptable

[1] Sandia National Laboratories, "Sandia Experiment Control System", 2023, https://github.com/sandialabs/ECS

- Determining if response moves are within the limitations of the response strategy

The scenario development sessions were concluded once the red and blue teams were finished with their portions of planning for the scenario and the green team was accepting of the planned scenario.

2.2. Tabletop Execution

Once the scenario was planned and developed, the overall TTX would then begin. The following outline the steps in which the TTX was conducted:

1) Red team begins first adversary attack portion of the scenario
    a) This first step would be the initial cyber attack that disables the PPS components
        i) The green team determines if this cyber attack fits within the adversary capabilities
        ii) If the CSOC is used, cyber attack simulations are deployed on the CSOC operator interface
    b) Red team and green team are the only groups in the TTX room
2) Red team begins first physical attack steps until detected by the response force or the PPS
    a) Red team and green team are the only groups in the TTX room
3) Blue team is able to respond to the initial adversary move once detected by the responders or the PPS
    a) Blue team and green team are the only groups in the TTX room
    b) If the CSOC is used, the blue team is able to respond to cyber alerts and IOCs

The above process is continued until the red team is successful in achieving sabotage at the facility, the response force is able to neutralize all adversary members, or the red team has lost enough adversaries that successful completion of the act of sabotage determined in the adversary attack scenario is not possible.

During this process, the red team and the blue teams were separated and only the team whose move was occurring was in the room. This brings realism to each scenario that prevents the red team from knowing blue team response moves, and the blue team from knowing the moves and plans of the red teams.

Once the TTX is completed, a hot wash was conducted. The TTX hot wash is an important factor in detailing and documenting the overall scenario that was developed and analyzed. A hot wash encompasses the blue, green, and red teams during the TTX discussing the overall scenario, what changes would be made by the red team to improve their adversary attack, modifications the blue team would propose to improve the likelihood that the PPS would be able to defend against the adversary attack, and then identify potential additional scenarios that could be analyzed based on the results of the previous scenario.

3. HYPOTHETICAL FACILITY

The site consists of three reactor buildings, three turbine buildings, a fresh fuel storage and central alarm station (CAS) building, and an underground spent fuel storage building. The site also has a protected area (PA) ECP for both vehicles and personnel.

- Fresh Fuel Storage and Central Alarm Station – The office building has one above-grade floor and one below-grade floor. The above-ground floor contains the office spaces that can be used by site personnel. The below- grade floor houses the Central Alarm Station (CAS) and the reactor control room.
    - The building is 40' wide by 57' long
- Switchyard – This fenced in area is where the switching substation is located. This substation allows for offsite power to be connected to the site and the power produced by the reactors to be transmitted to the local electrical grid.
- Three Reactor Buildings – Each reactor is housed within its own reactor building. The reactor building consists of one above-grade floor and two-below grade floors.
    - The reactor building is 40' wide by 57' long
- Spent Fuel Storage Building – The Spent Fuel Storage Building is used to store spent pebbles in canisters at the facility. The storage location is located fifteen-feet below-grade with a large concrete cover over the top of the spent fuel storage area.
    - The Spent Fuel Storage Building is 60' wide by 50' long
- Three Power Production Buildings – The Power Production Building (PPB) consists of one above-grade floor and one below-grade floor. The above-grade floor houses the turbine and diesel generators, the below-grade floor houses battery banks.
    - The power production building is 72' long by 70' wide

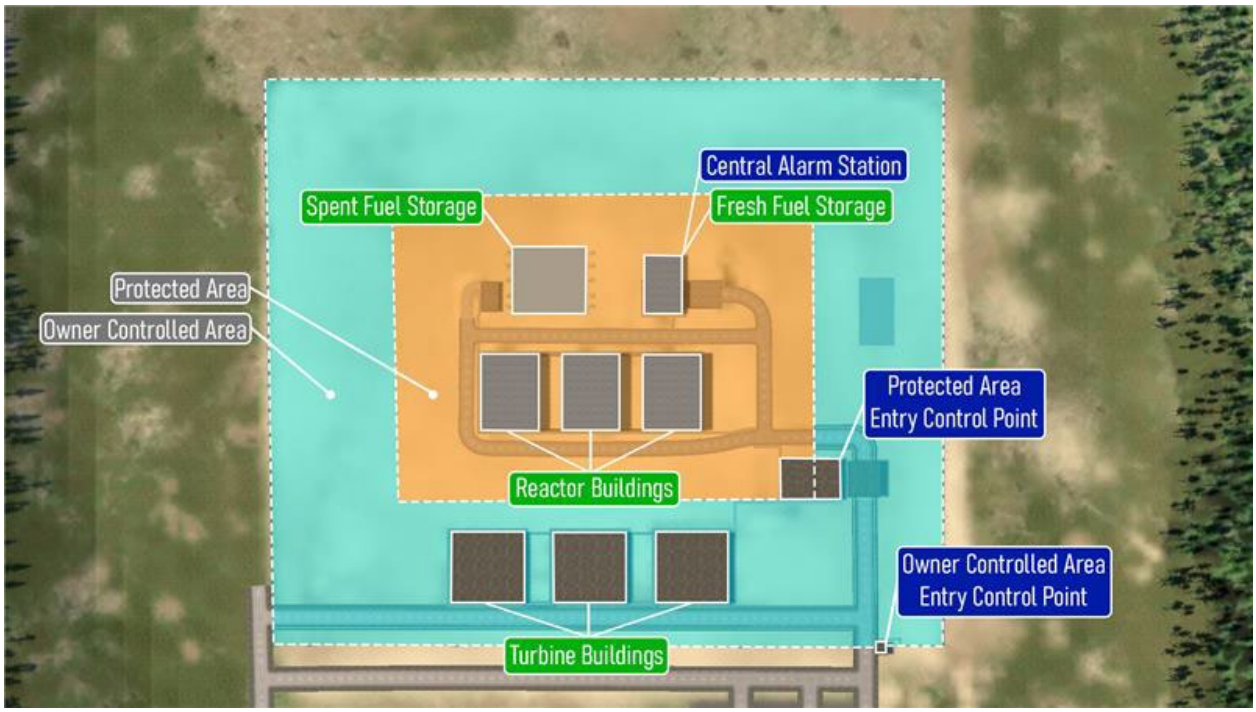


Figure 1 Hypothetical SMR Facility

3.1. Reactor Description

Based on numerous HTGRs,[2] the site operates three reactors and three turbines for electricity production. Each reactor is located in a separate building. Key reactor components such as the fuel pebbles, moderators and reflectors, control rods and other core internals are housed within a confinement structure. The confinement structure allows for possible venting in the very unlikely case of radiological effluent release from the fuel. The following are a list of key components of the HTGR reactors:

- Each reactor core produces 360 MWth with an efficiency of 42% for a power output of 150 MWe
- The core is fueled by TRI-structural ISOtropic (TRISO) particle fuel pebbles with an enrichment of 8.5% (i.e., equilibrium core)
- The TRISO fuel particle[3] includes a uranium, carbon, and oxygen fuel matrix kernel of approximately 500 micrometers in diameter[4] embedded in multiple layers of containment in order to physically protect the fuel and prevent the escape of fission products. This makes the fuel robust and resistant to high temperatures for extended periods of time while maintaining fission product retention. Outside of the fuel kernel is porous carbon for fission gas

[2] For numerous examples of high-temperature gas-cooled small modular reactors in the open source, see: "Advances in Small Modular Reactor Technology Developments," A Supplement to: IAEA Advanced Reactors Information System (ARIS), 2020 Edition, Vienna Austria, September 2020, pp. 135-194.

[3] Department of Energy Office of Nuclear Energy, "TRISO Particles: The Most Robust Nuclear Fuel on Earth," July 9, 2019, retrieved January 14, 2021, https://www.energy.gov/ne/articles/triso-particles-most-robust-nuclear-fuel-earth#:~:text=TRISO%20stands%20for%20TRi%2Dstructural,release%20of%20radioactive%20fission%20products.

[4] Similar to the PBMR®-400 from Pebble Bed Modular Reactor SOC Ltd in South Africa. See: "Advances in Small Modular Reactor Technology Developments," A Supplement to: IAEA Advanced Reactors Information System (ARIS), 2020 Edition, Vienna Austria, September 2020, p. 164.

accumulation. Following this is an inner pyrolytic carbon layer, a structural silicon carbide layer, and finally an outer layer of pyrolytic carbon.[5] Each pebble consists of approximately 15,000 coated fuel particles in a graphite matrix with a 5 mm buffer which makes up the 6 cm diameter pebble.[6]

- Each core has 420,000 pebbles[7] in circulation at any given time.
- Pebbles are offloaded once they reach the target burnup (i.e., 90 GWd per ton). Refueling occurs online with continuous addition and removal of pebbles. Pebbles pass through the reactor until they reach a tube and flow through a measurement system to measure burnup. Once the pebble reaches the target burnup, it is sent to a spent fuel container. If the burnup is not met, it is pneumatically sent back up to the top of the core for another pass.
- Primary cooling is conducted by forced circulation from a helium circulator[8]
- Core reactivity is controlled by boron carbide (i.e., B_4C) control rods and small absorber spheres[9]

The reactors are cooled through the forced circulation of helium gas and the transfer of this heat to a steam generator.[10] The core is moderated by graphite within the pebbles, a centralized graphite column, and an outer core reflector, making this a thermal reactor powered by mostly thermal neutrons.[11] The reactor pressure vessel (RPV) contains primary system components including control rods, fuel pebbles, graphite central column, and graphite reflector. The primary helium coolant pressure inside the reactor is maintained by a compressor that keeps the helium at a constant 7MPa.[12] Primary circulation is conducted by a forced helium circulator/blower and via a compressor external to the vessel. Each reactor utilizes one helical-coil steam generator in a countercurrent flow to transition heat from the helium to the water to convert into superheated steam. The superheated steam exiting from the steam generator is transferred to a high-pressure turbine, followed by two low-pressure turbines. There is one turbine series per reactor core, making a total of three turbine series on site. The steam and any letdown water are collected and sent to dry-cooling towers to condense the steam-water mixture into liquid. The liquid water is then pumped back to the steam generator for heating. The condenser is ultimately cooled by the environmental air.

---

[5] Paul Demkowicz, Ph.D., "TRISO Fuel: Design, Manufacturing, and Performance," Idaho National Laboratory, NRC HTGR Training, July 16-17, 2019.

[6] Similar to the PBMR®-400 from Pebble Bed Modular Reactor SOC Ltd in South Africa. See: "Advances in Small Modular Reactor Technology Developments," A Supplement to: IAEA Advanced Reactors Information System (ARIS), 2020 Edition, Vienna Austria, September 2020, p. 164.

[7] Similar to the HTR-PM from Tsinghua University, ChinaSee: "Advances in Small Modular Reactor Technology Developments," A Supplement to: IAEA Advanced Reactors Information System (ARIS), 2020 Edition, Vienna Austria, September 2020, pp. 137-140.

[8] C. F. McDonald and M. K. Nichols, "Helium Circulator Design Considerations for Modular High Temperature Gas- Cooled Reactor Plant," GA Technologies, Inc., San Diego, California, GA Project 6300, December 1986, https://inis.iaea.org/collection/NCLCollectionStore/_Public/19/005/19005804.pdf.

[9] Similar to Urenco's U-Batter from the United Kingdom. See: "Advances in Small Modular Reactor Technology Developments," A Supplement to: IAEA Advanced Reactors Information System (ARIS), 2020 Edition, Vienna Austria, September 2020, pp. 293-296.

[10] Similar to the HTMR100 from STL Nuclear in South Africa. See: "Advances in Small Modular Reactor Technology Developments," A Supplement to: IAEA Advanced Reactors Information System (ARIS), 2020 Edition, Vienna Austria, September 2020, pp. 171-174.

[11] Annular core with central graphite column similar to the PBMR®-400. See: "Advances in Small Modular Reactor Technology Developments," A Supplement to: IAEA Advanced Reactors Information System (ARIS), 2020 Edition, Vienna Austria, September 2020, pp. 163-166.

[12] Similar to the HTR-PM from Tsinghua University, China. See: "Advances in Small Modular Reactor Technology Developments," A Supplement to: IAEA Advanced Reactors Information System (ARIS), 2020 Edition, Vienna Austria, September 2020, pp. 137-140.

Each reactor pressure vessel is approximately 30-m (98.4-ft) tall and 6-m (19.7-ft) in diameter. The RPV sits within a confinement structure. The confinement structure is made of 1-m (3.3-ft) reinforced concrete and contains venting mechanisms[13] that allow for the potential venting of steam. Each reactor is housed in its own confinement structure. The RPV is partially located below-grade with the reactor core being below-grade. The confinement buildings are only expected to be accessed during maintenance, delivery of new fuel or removal of spent fuel, domestic safeguards inspections as needed by the, or when security inspections are needed. The site has one onsite control room for all three reactors that is always staffed by two control room operators. The site does not have a traditional spent fuel pool; however, each reactor is equipped with spent fuel storage canisters (SFSC).[14] Once a tank is filled it can be moved to an interim storage facility located onsite. All SFSCs are located below grade.

[13] IAEA, "Advances in Small Modular Reactor Technology Developments," Vienna, 2020, p. 170.
[14] Similar to the PBMR®-400 from Pebble Bed Modular Reactor SOC Ltd in South Africa. See: "Advances in Small Modular Reactor Technology Developments," A Supplement to: IAEA Advanced Reactors Information System (ARIS), 2020 Edition, Vienna Austria, September 2020, pp. 163-166.

3.2. Hypothetical Design Basis Threat

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

- Group size of 4-8 individuals
- Ability to conduct a determined, violent external assault
    - Attack by stealth or deceptive actions
    - Operate in groups through a single entry point
    - Have multiple groups attacking through multiple entries
- Military training and skills, willing to kill or be killed, enough knowledge to identify specific equipment or locations necessary for a successful attack
- Land or water vehicles, which could be used for transporting personnel and their hand-carried equipment to the proximity of vital areas
- Land vehicle bomb assault, which may be coordinated with an external assault
- Ability to conduct a cyber-attack
- Ability to perform any of the tasks needed to steal or sabotage critical assets
- Armed with a 7.62-mm rifle; a pistol; ammunition; grenades; satchel charges containing bulk high explosives, not to exceed 10 kg total; detonators; bolt cutters; and miscellaneous other tools[15]
- Each able to carry a man-portable total load of 29.5 kg (65 lb)
- Assumed run speed of 3 m/s
- **One active non-violent insider (not included in the adversary group of 4-8 individuals)**

There is no cyber DBT currently, the adversary capabilities were based on the PPS red teaming conducted at Sandia and Idaho National Laboratory. The cyber adversary is assumed to have the following capabilities:

- Cannot generate zero-day attacks
    - Attacks must be based on demonstrated real-world adversary capabilities
- Able to execute any exploits which do not require state-level threat actor capabilities
- Insider is able to install a wireless device on the network
    - This is not detectable if there is no CSOC in play
- Insider is able to temporally plug in a malicious USB into one system to deploy malware
- Able to conduct sufficient cyber reconnaissance to accurately understand the network and

[15] 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

PPS systems.

3.3. Physical Protection Systems

The PPS design for this facility included novel technologies to allow for detection and assessment of adversary intrusions to the facility. Deliberate motion analytics (DMA) ensures that the requirement that adversaries can be detected before the 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. 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. Additionally, all response towers are equipped with pan-tilt-zoom (PTZ) cameras that can be used by the response force to periodically scan the OCA perimeter for potential adversary threats. This can be seen in the figure below.

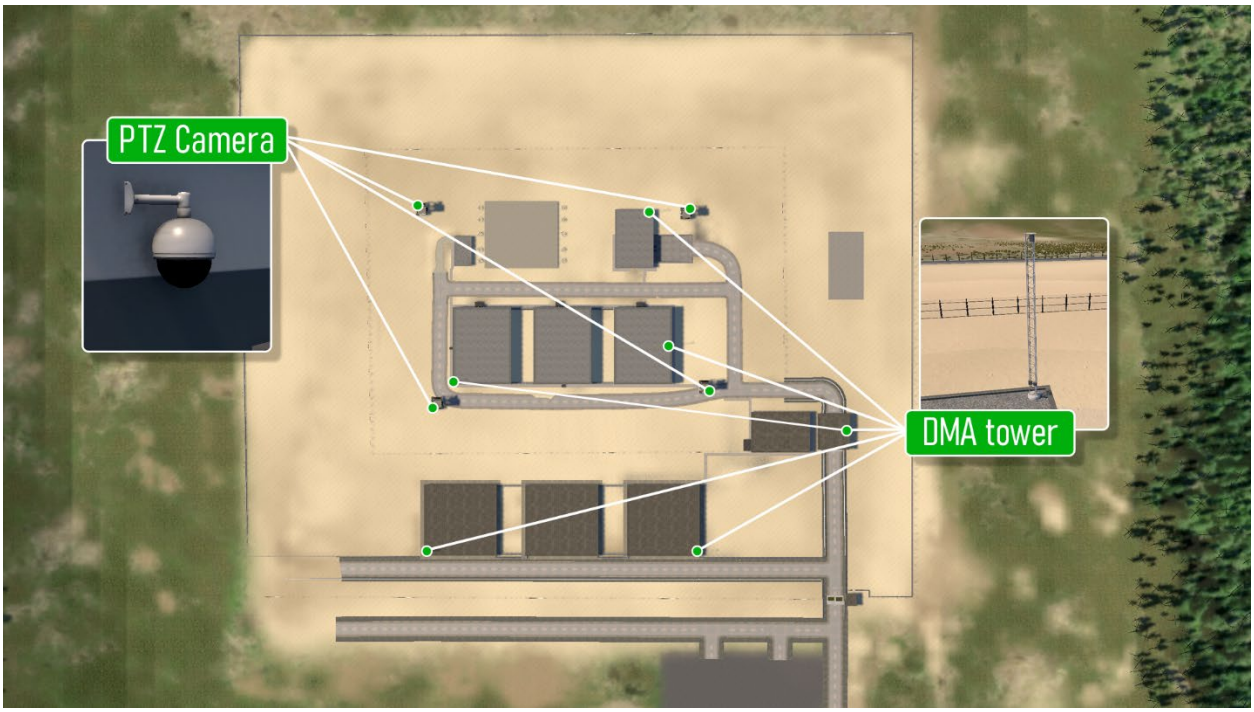


Figure 2 PTZ and DMA Locations

On the immediate interior of the OCA fence line is a modular block wall that forms the vehicle barrier system around the PBR facility. At the OCA, there is vehicle ECP and a personnel ECP. Upon arrival of any vehicle to the OCA, the vehicle must be searched by two-armed security officers (ASOs) for large vehicle bombs that could be stored in the vehicle. At the PA ECP, a further detailed search is conducted for individuals and vehicles. Any individuals with packages or bags entering the PA must be screened, passing through a metal detector and passing through an explosives detector. Vehicle drivers must exit their vehicle, proceed through the personnel ECP entrance, then return to their vehicle to enter the PA. This ensures the integrity of the vehicle search

and the personnel search for all vehicles and persons entering the PA. The PA ECP can be seen in the figure below.

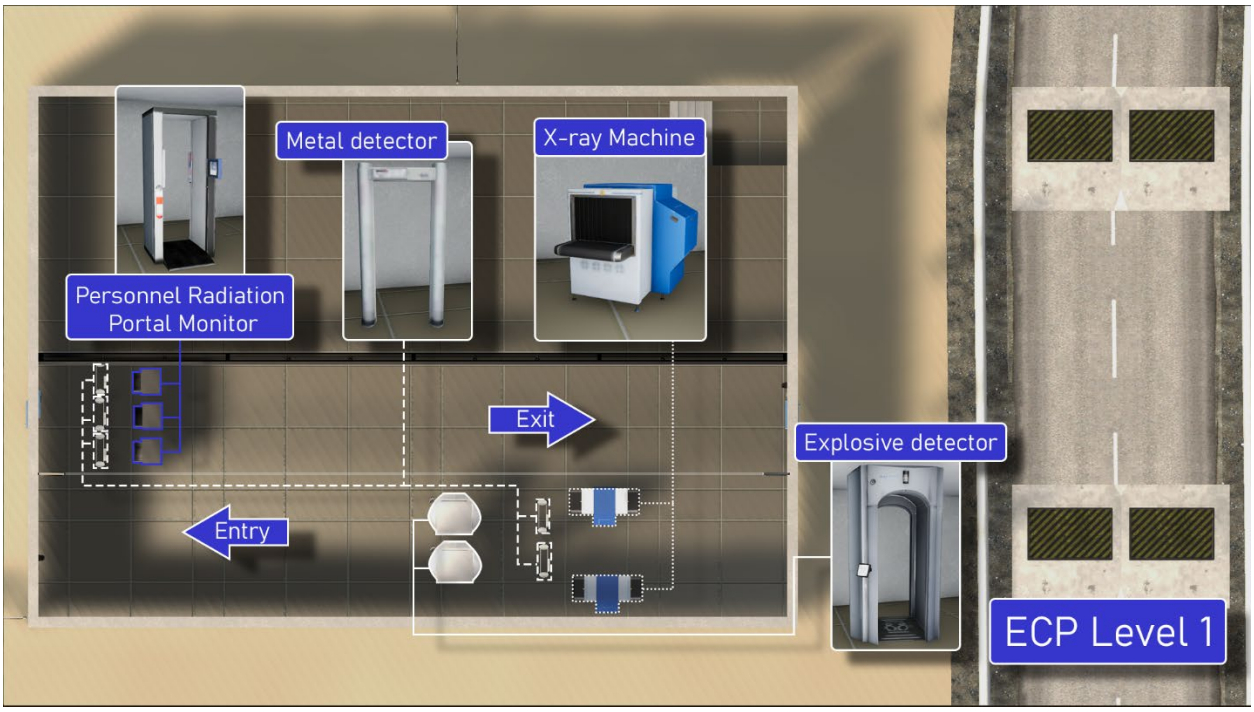


Figure 3 Protected Area Entry Control Point

At the exterior of buildings in the PA, all entrances are secured by "shark cages." The shark cages are containers made of turbine grating. The shark cages are anchored into the ground using concrete anchors and are additionally anchored into the walls of the buildings. The shark cages on the exterior of the building are access-controlled with a badge and PIN reader. The shark cages create additional delay time exposed to responders who can engage an adversary team. Additionally, the shark cages provide another barrier that the adversary team must use tools or explosives to breach and therefore decreases the amount of explosives available to them.

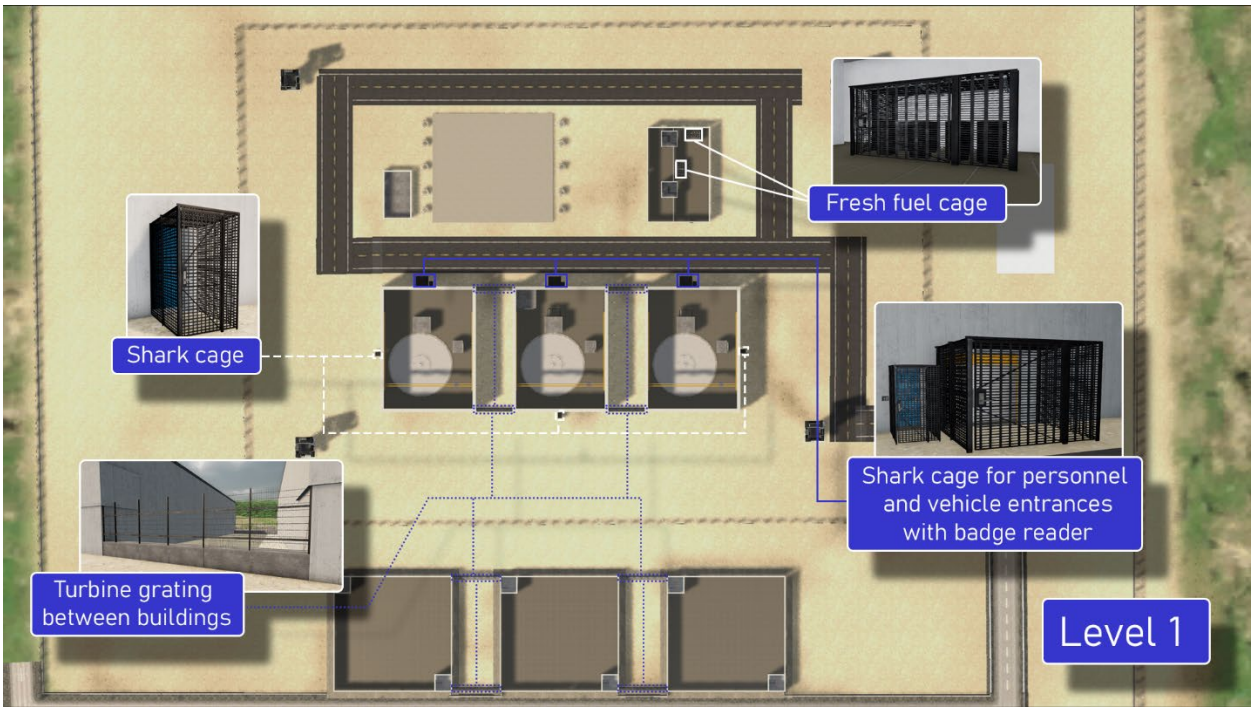


Figure 4 Exterior Physical Protection Features

Each reactor building has two personnel doors and a high-bay door that can be used to move equipment in and out of the reactor buildings. Every door into the reactor building is secured with a shark cage that is access-controlled using a badge and PIN reader to enter into the building. These shark cages add an additional delay barrier to the adversary force. One benefit of the shark cages is their robustness to adversary attacks using explosives. Because the shark cages are not a solid structure, due to the spacing between the turbine grating, the pressure from explosives passes through these gaps and does not impact the turbine grating as it would a solid concrete structure. The shark cages in front of the high-bay doors also require a badge and PIN reader to open and allow a forklift to pass through the shark cage and the high-bay door. In addition to this step, the CAS operator will not allow the high-bay door to be unlocked and opened until the forklift enters the shark cage and the shark cage is closed. Once the shark cage is closed, the CAS operator will unlock the high-bay door and open the high-bay door. This additional step ensures that the forklift or equipment moving into the reactor building is the correct equipment and material and provides an additional layer of security for fresh fuel while moving from fresh fuel storage to the correct reactor building.

Once inside the reactor building, there is a room where fresh fuel intake begins for each PBR, and a separate room houses an elevator and a stairwell for equipment and personnel. At the fresh fuel intake, the entrance is protected by another shark cage with a badge and PIN reader and intercom. To access the fresh fuel intake, two individuals must be present from operations and security. The individuals must call the CAS and verbally state their name. Once the CAS operator receives this call, they check the identities of the individuals using the CCTV cameras at the fuel intake structure entry point, verifying the individuals are the ones moving the material and inserting fresh fuel into the reactor. After calling the CAS operator, the two individuals will both present their badges and enter their PINs at the badge and PIN reader. Once this process has been completed, the shark cage is unlocked and opened by the CAS operator. Similar to the outdoor shark cage, the high-bay door for the fresh fuel intake cannot be opened until the shark cage is closed, with both members from

operations and security inside the shark cage with the fresh fuel. This again provides another delay barrier for external adversaries and helps to reduce the insider risk with multiple verification steps to the process of inserting fresh fuel into the reactor.

Inside the reactor building, there is also an entry point that allows access to the reactor structure below-grade. This entry point is meant to be accessed by individuals performing maintenance and operational work on the reactor units. This structure provides access for both individuals to move to below-grade portions of the reactor (using the stairs), and to move equipment to the below-grade floors (using the elevator). The elevator has been designed in such a way that equipment and individuals can't fit into the elevator at the same time. This process adds additional task time for operations and maintenance personnel but increases adversary task time to get to target locations to cause sabotage or theft of material. At the entrance to this access point, a one-foot-thick reinforced concrete rolling door is placed in front of the stairwell and elevator door. To access the stairs or equipment elevator, authorized individuals must first contact the CAS operator using the intercom outside of the door. After the CAS operator is called, the individual will use their badge and PIN at the badge and PIN reader. If access is granted, the CAS operator will unlock the magnetic lock on the moveable concrete door and begin to open the concrete door.

The spent fuel storage area can be accessed through the below-grade portions of any of the reactor units themselves. Additionally, there is an access point to the spent fuel storage area through the middle reactor unit building. This access point is identical to all the others in the reactor buildings that have a personnel ladder and equipment elevator. This access point is protected with a one-foot-thick reinforced moveable concrete door that operates in the same way as the other below-grade entry points.

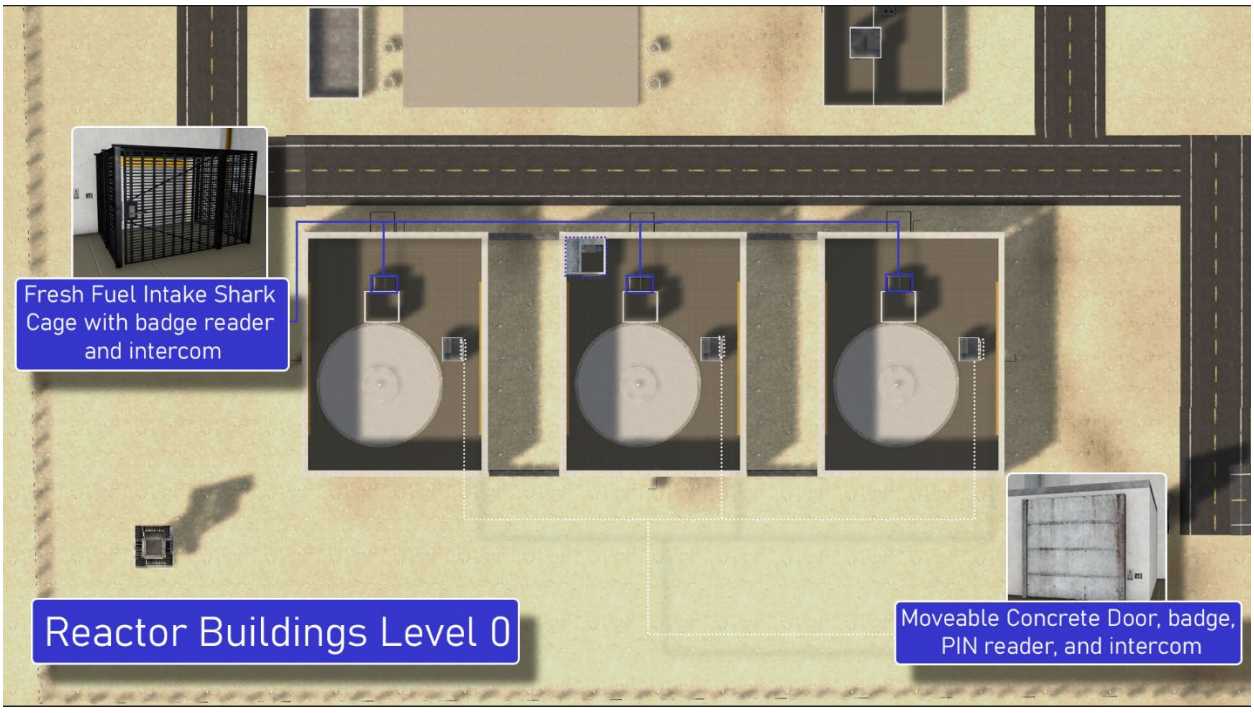


Figure 5 Interior Reactor Building PPS Measures

The response force posture for this hypothetical PBR facility consists of four responders located in four BBRE towers. The four BBRE towers are located in a somewhat square shape around the reactor buildings, spent fuel storage building, and the fresh fuel storage building. The location of

these BBRE towers also allows for compensatory measures to be taken in the event that the perimeter intrusion detection system is not functional for any reason. The BBRE towers are equipped with pan-tilt-zoom (PTZ) cameras that allow the responders to have constant observation of the PA boundary and perimeter of the facility.
The design of delay barriers inside the PA was integrated with the response force strategy to channel adversaries to advantageous locations for the response force to engage and neutralize an external adversary force. Between buildings, there are turbine grating fences that force an adversary team to breach the turbine grating, climb the turbine grating, or defeat the turbine grating in some fashion. This the adversaries to spend time outside of the building without cover or concealment to try to successfully breach the turbine grating. The figure below shows the locations of these BBRE towers.

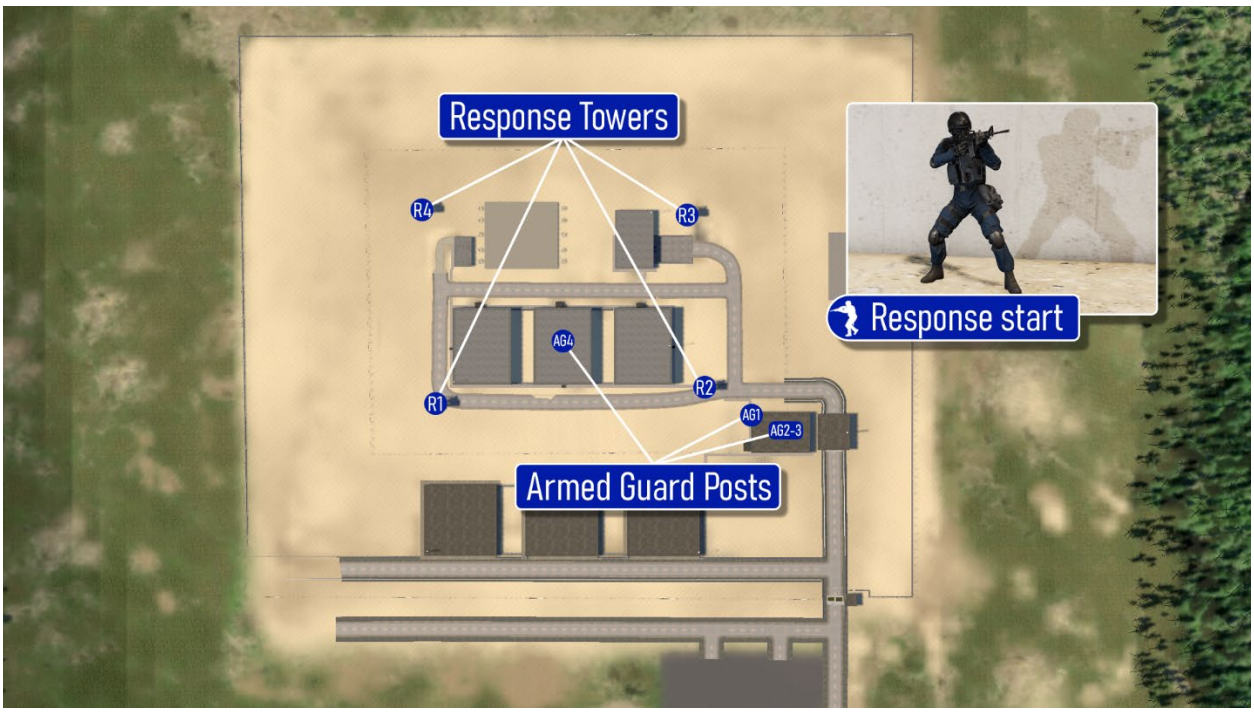


Figure 6 Response BBRE Tower Locations

3.4. Physical Security System Network and Cybersecurity

The physical security system network for the facility is based on research and training PPS networks at the Sandia Nuclear Security Technology Complex (NSTC) and the Sensor Test and Evaluation Center (STEC). These networks are constructed in the same way most security system networks are: flat, centralized, and air-gapped. Figure 7 depicts a generalized network architecture for a flat PPS network. Local components of the PPS such as cameras, biometric readers, door sensors, locks, and motion detectors are wired to a Field Distribution Box (FBD). These FDBs contain the PPS functional resources for that local area such as power supplies, network switches and PPS controllers. The PPS controller manages local I/O such as door sensors and locks and communicates back to a central PPS management server. Cameras connect to the FBD and over the network to the video management server. The biometric system connects to the PPS controller as a dry contact or serial device to actuate the door, but it requires network access as well to communicate to its management server.

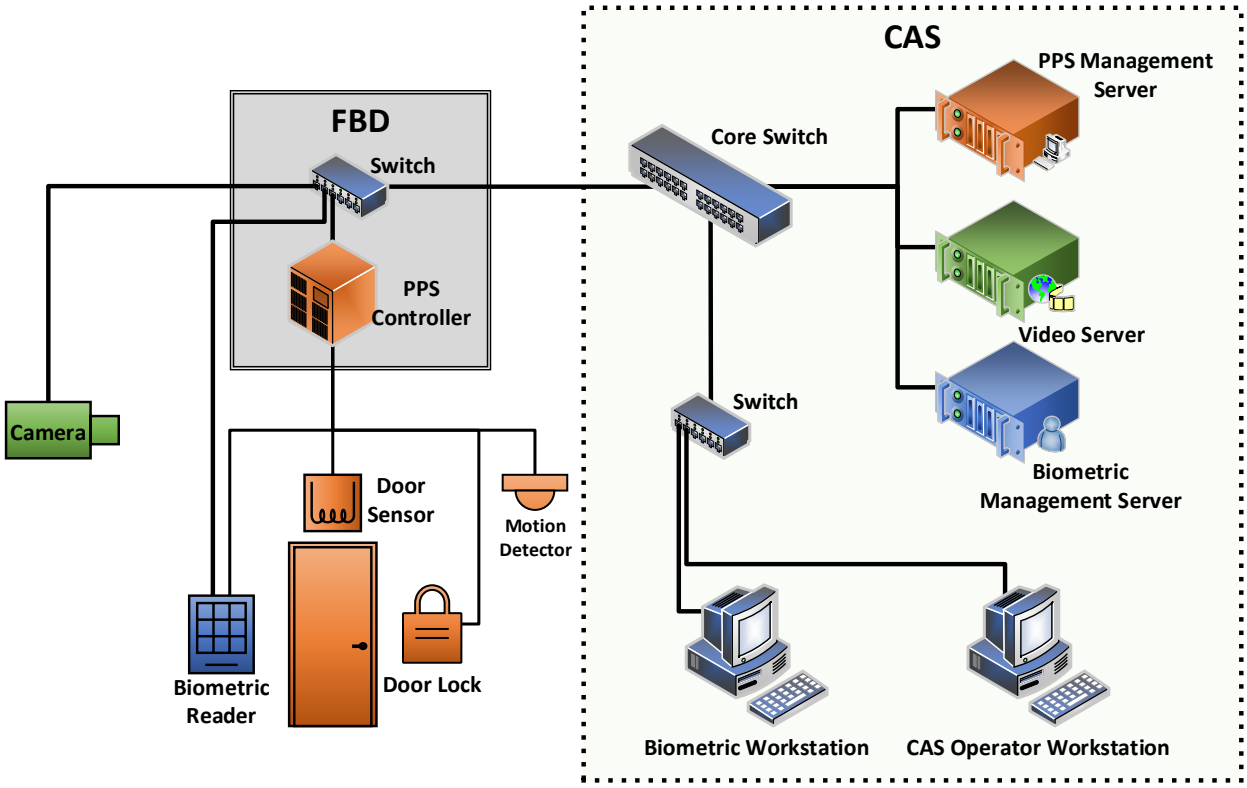


Figure 7: Example PPS network architecture.

Across the facility there are 6 FDBs assembled in a simple hub and spoke topology which is centrally connected to and managed by the CAS. With this facility, there is also a connection to a SAS which is established over a secure wireless network which connects to the core switch. As is typical with PPS networks, the servers and workstations are Windows based and the controllers and cameras are Linux based systems. The only segmentation on the network is VLAN separation of the camera systems from the rest of the PPS components, otherwise the network is entirely flat.

Currently, cybersecurity monitoring of the PPS network through a CSOC is rare, very few if any plants are actively monitoring the PPS network via a CSOC. Thus, exercises considered situations with and without a Cyber Security Operations Center (CSOC) at the facility. The CSOC collects cybersecurity information from the network and PPS devices to rapidly identify Indicators of Compromise (IOCs), which would alert the defenders to a cyber threat and which systems are affected. The CSOC design in this facility consists of an isolated Security Information and Event Management (SIEM) server which sits behind data diodes, collects network traffic from the core switch and system logs from each device capable of generating logs. The SIEM analyzes the stream of data coming from the network and searches for matches to IOC patterns or network rules violations. CSOC operators are alerted to any suspect traffic, or IOCs detected by the SIEM and are able to inform the CAS of degradations of PPS performance due to cyber-attack.

4. ADVERSARY ATTACK SCENARIOS EVALUATED

Within this project three adversary attack scenarios were developed that were within the boundaries of the overall DBT discussed previously. A fourth scenario was analyzed that considered adversary capabilities that were above the DBT initially considered. These capabilities included the use of a kinetic uncrewed aerial system (UAS) that is equipped with a one-kilogram explosive charge that could be used to attack the facility or a member of the response force in their BBRE towers.

> **Note:** All engagements between responders and adversaries were simulated with the engagement tools that are available within SCRIBE 3D. All engagements between responders and adversaries were individually analyzed one hundred times. If the engagement resulted in a sixty-percent or higher that an individual was neutralized, the TTX considered that individual as neutralized moving forward.

4.1. Attack Scenario One

The first adversary attack scenario started with a group of five adversaries parking one vehicle on the main entry road leading to the SMR facility and exiting that vehicle and entering a second vehicle. The first vehicle was parked on the side of the road with hazard lights on as to not draw attention to itself. As the adversary team proceeds to the facility staff parking lot outside of the PA. As the adversary team parks their vehicle, the vehicle on the roadway is detonated with the maximum vehicle explosive weight and the cyber attacker also begins to execute an attack to disable the DMA towers and PTZ cameras responsible for detection and assessment along the southern portion of the facility. The start of the adversary attack scenario can be seen in the figure below.

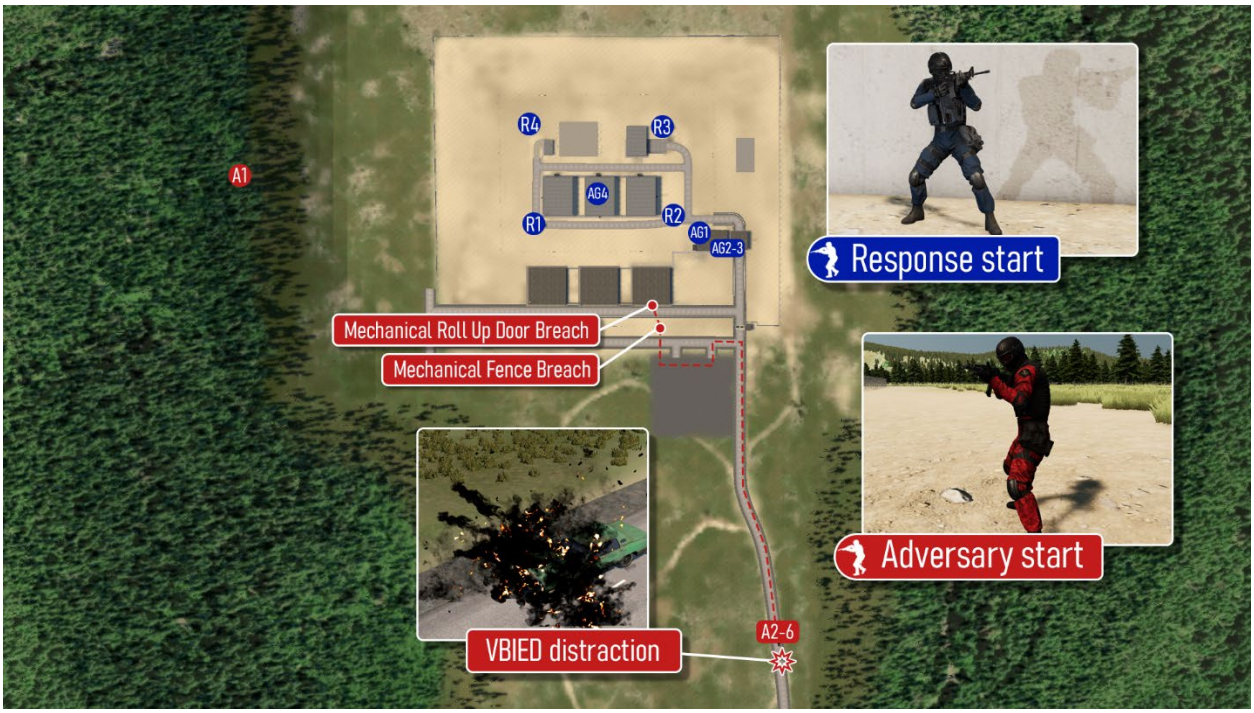
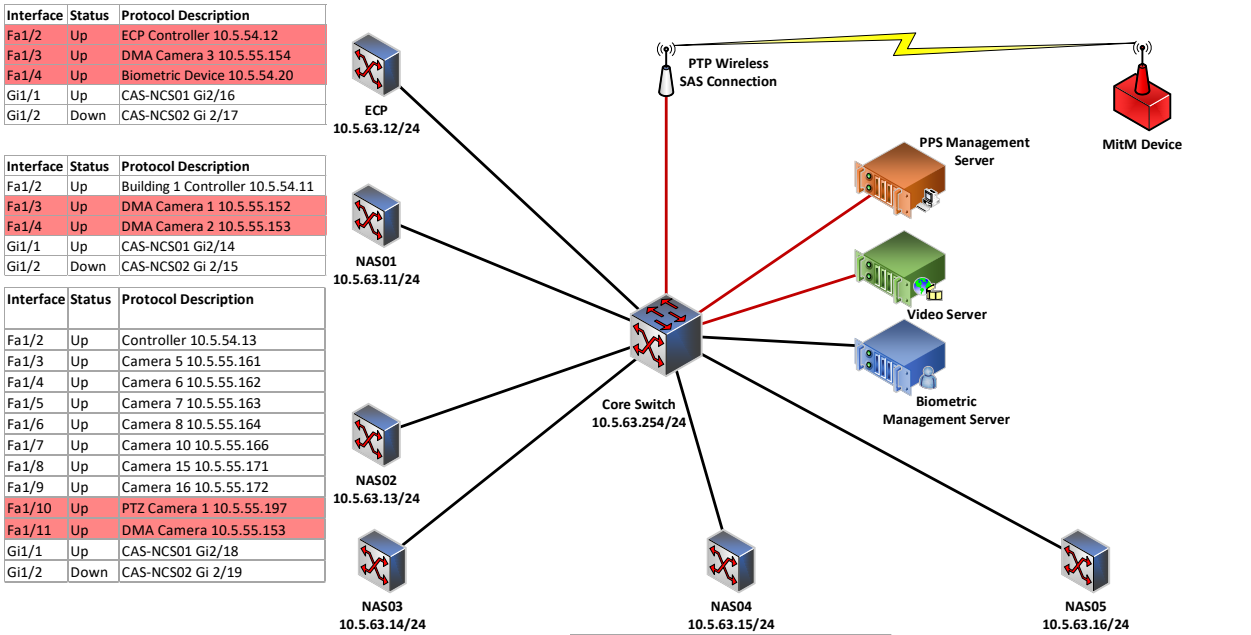


Figure 8 Scenario Initiation

The cyber-attack is initiated by a Man-in-the-Middle (MitM) attack on the wireless connection between the CAS and SAS. Once the MitM is established, the adversary watches the network and communications between the CAS and SAS to passively build a network map and either capture a

password or crack a password on the core switch and the PPS management and video servers. The physical attack will wait until the cyber adversary has enough control over the system that they believe they will be effective. Roughly 30 seconds after the physical adversaries leave their vehicle the cyber attackers disable the DMA on the east side of the complex and the ECP access controls and cameras. When the adversaries are breaching the fence, the DMA and PTZ cameras are subjected to a Denial of Service (DoS) attack. Additionally, the reactor building network switch is disabled, taking out the alarms for the doors on the reactor building. This loss of view for the CAS triggers a response to put the facility on high alert.



Interface	Status	Protocol Description
Fa1/2	Up	ECP Controller 10.5.54.12
Fa1/3	Up	DMA Camera 3 10.5.55.154
Fa1/4	Up	Biometric Device 10.5.54.20
Gi1/1	Up	CAS-NCS01 Gi2/16
Gi1/2	Down	CAS-NCS02 Gi 2/17

Interface	Status	Protocol Description
Fa1/2	Up	Building 1 Controller 10.5.54.11
Fa1/3	Up	DMA Camera 1 10.5.55.152
Fa1/4	Up	DMA Camera 2 10.5.55.153
Gi1/1	Up	CAS-NCS01 Gi2/14
Gi1/2	Down	CAS-NCS02 Gi 2/15

Interface	Status	Protocol Description
Fa1/2	Up	Controller 10.5.54.13
Fa1/3	Up	Camera 5 10.5.55.161
Fa1/4	Up	Camera 6 10.5.55.162
Fa1/5	Up	Camera 7 10.5.55.163
Fa1/6	Up	Camera 8 10.5.55.164
Fa1/7	Up	Camera 10 10.5.55.166
Fa1/8	Up	Camera 15 10.5.55.171
Fa1/9	Up	Camera 16 10.5.55.172
Fa1/10	Up	PTZ Camera 1 10.5.55.197
Fa1/11	Up	DMA Camera 10.5.55.153
Gi1/1	Up	CAS-NCS01 Gi2/18
Gi1/2	Down	CAS-NCS02 Gi 2/19

Interface	Status	Protocol Description
Fa1/2	Up	Controller 10.5.54.14
Fa1/3	Up	Camera 11 10.5.55.167
Fa1/4	Up	Camera 12 10.5.55.168
Fa1/5	Up	Camera 13 10.5.55.169
Fa1/6	Up	Camera 14 10.5.55.170
Fa1/7	Up	Camera 17 10.5.55.173
Fa1/8	Up	Camera 18 10.5.55.174
Fa1/9	Up	Camera 19 10.5.55.175
Fa1/10	Up	Camera 20 10.5.55.176
Fa1/11	Up	Camera 21 10.5.55.177
Fa1/12	Up	Camera 22 10.5.55.178
Fa1/13	Up	Camera 29 10.5.55.179
Gi1/1	Up	CAS-NCS01 Gi2/20
Gi1/2	Down	CAS-NCS02 Gi 2/21

Interface	Status	Protocol Description
Fa1/2	Up	Controller 10.5.54.15
Fa1/3	Up	Camera 23 10.5.55.179
Fa1/4	Up	Camera 24 10.5.55.180
Fa1/5	Up	Camera 25 10.5.55.181
Fa1/6	Up	Camera 26 10.5.55.182
Fa1/7	Up	Camera 28 10.5.55.184
Fa1/8	Up	Camera 30 10.5.55.186
Fa1/9	Up	PTZ Camera 3 10.5.55.199
Fa1/10	Up	PTZ Camera 4 10.5.55.200
Fa1/11	Up	DMA Camera 4 10.5.55.155
Fa1/12	Up	Camera 22 10.5.55.178
Fa1/13	Up	Camera 29 10.5.55.185
Gi1/1	Up	CAS-NCS01 Gi2/22
Gi1/2	Down	CAS-NCS02 Gi 2/23

Interface	Status	Protocol Description
Fa1/2	Up	CAS Workstation 10.5.54.8
Fa1/3	Up	Camera 33 10.5.55.189
Fa1/4	Up	Camera 35 10.5.55.191
Fa1/5	Up	Camera 36 10.5.55.192
Fa1/6	Up	Camera 37 10.5.55.193
Fa1/7	Up	Camera 40 10.5.55.196
Fa1/8	Up	PTZ Camera 2 10.5.55.198
Fa1/9	Up	DMA Camera 5 10.5.55.156
Gi1/1	Up	CAS-NCS01 Gi2/24
Gi1/2	Down	CAS-NCS02 Gi 2/25

Figure 9: Scenario one cyber-attack targets on PPS network.

After the initiating event occurs the adversary team of five begins to breach the OCA fence at the perimeter. Immediately after the fence is breached by the adversary team one adversary in using a sniper rifle is posited in the woods and starts to suppress responder one and four in their BBRE towers. As the adversary sniper begins to suppress the response towers the remaining adversaries move and breach into the turbine building. Once inside the turbine building, the adversaries proceed up to the turbine grating between two turbine buildings. Once the adversaries reach this point, adversary two begins to breach the turbine grating and adversaries three, four, five and six begin suppressing responders one and two, as well as the ASO located in the PA ECP fighting port. This can be seen in the figure below.

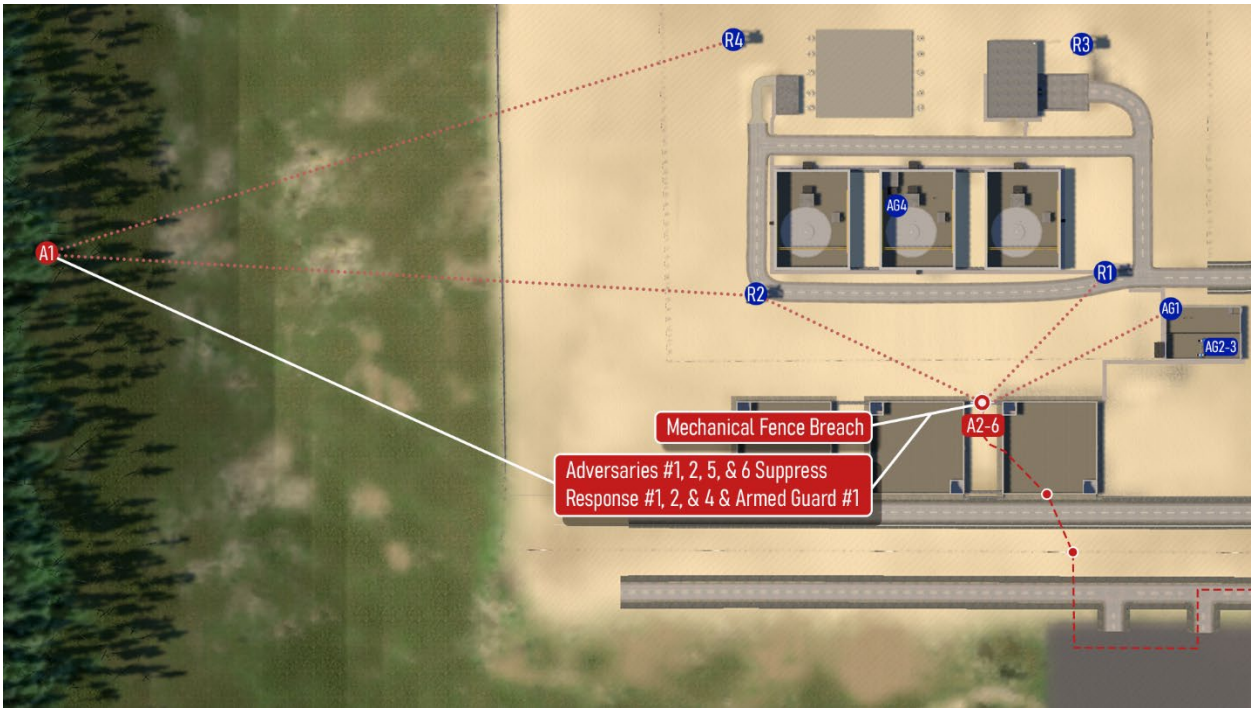


Figure 10 Adversaries Begin Suppressing Fire

Once the turbine grating has been breached by the adversaries, adversaries two, three and four deploy smoke grenades and aim to reach the shark cage that enters into reactor building two. As the adversaries cross the open space, responder one and two neutralize the three adversaries. At this point in the scenario, the adversary team does not have enough adversaries to suppress the remaining responders in the BBRE towers and the ASO who is armed and can engage from the PA ECP. Due to these factors the adversary team conceded in the TTX and allowed the blue team to win this attack scenario. The end of this first adversary attack scenario can be seen in the figure below.

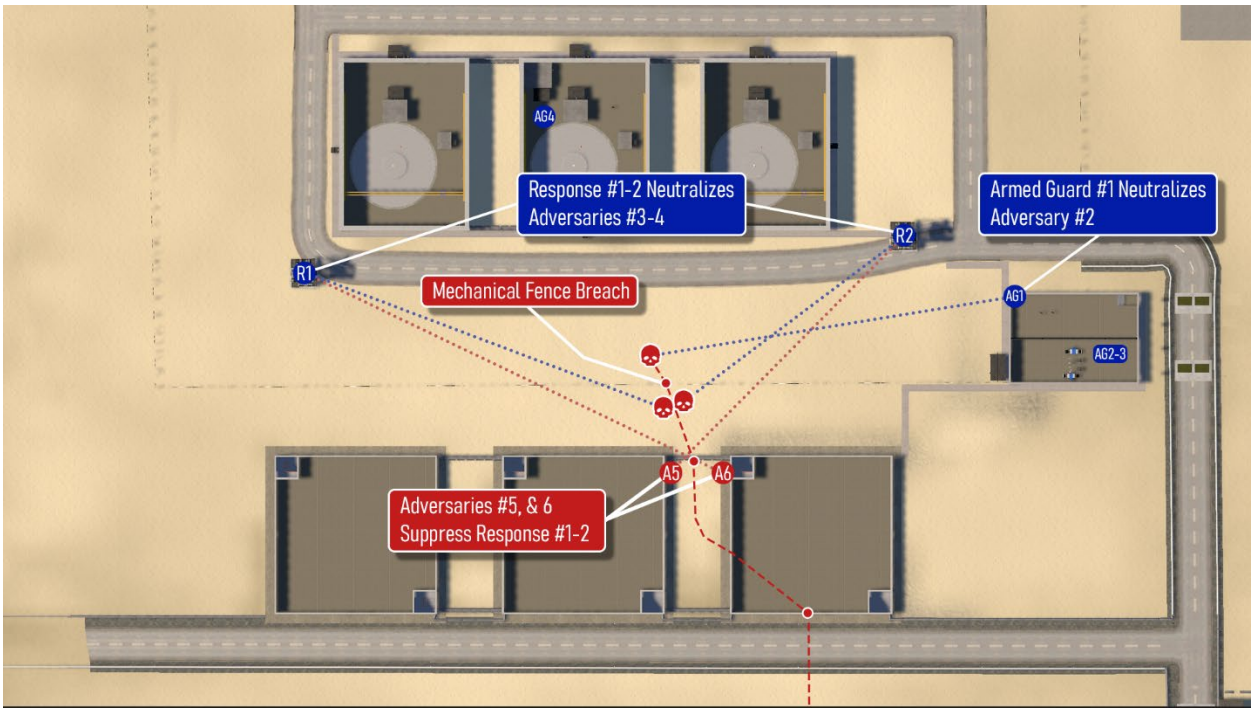


Figure 11 Attack Scenario One - End of Scenario

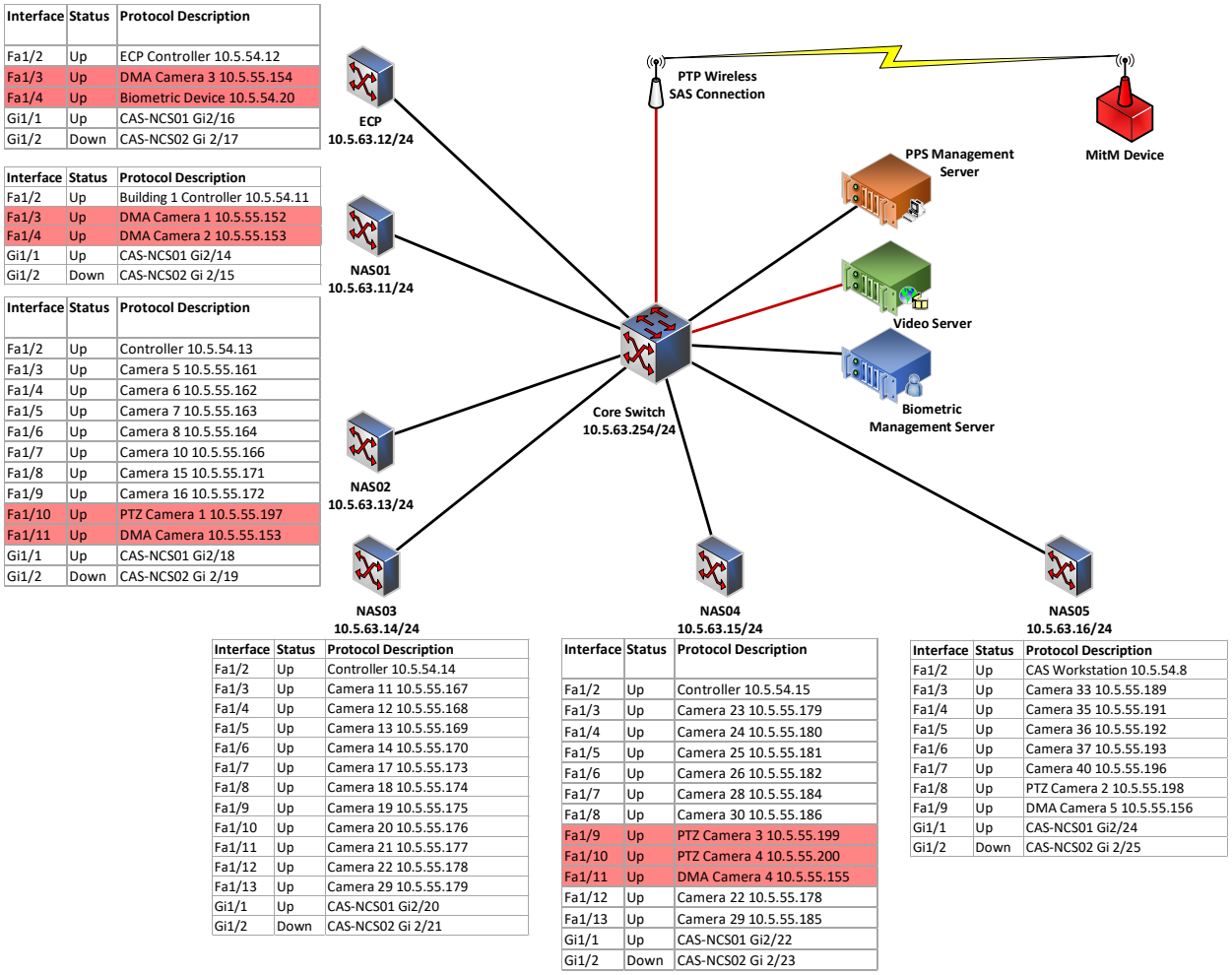
The first adversary attack scenario shows that the PPS design and the response strategy was successful at mitigating this adversary attack scenario. The attack scenario disabled the southern perimeter intrusion detection technologies and the PTZ for responders one and two. These disablements facilitated easier access into the facility and allowed the adversary team to get closer to the reactor buildings before they were detected. The adversary team is first detected when they begin to suppress the responders in the BBRE towers. As the adversary begins to suppress the response towers the responders to include the ASO in the PA ECP are able to effectively engage and neutralize the adversaries.

4.2. Attack Scenario Two

In attack scenario two, the adversary team uses a cybersecurity attack to disable the DMA on the south and west side of the plant, the PTZ on responder two and four towers and developed a fake coded credential to use on the badge and PIN readers to gain access to the facility. The purpose of taking down the PTZs and DMA was to disable detection and to decrease the response force's ability to engage and neutralize the adversary force. The adversary team chose to create a fake coded credential to use on the badge and PIN readers that allow access through the shark cages on personnel doors and doors entering into the reactor buildings. The adversary team goal is to enter into the western reactor building and sabotage systems inside the western reactor building.

The cyber attack is again facilitated through the wireless connection between the CAS and SAS. Instead of DoS attacking the DMA, the cyber attackers operate a stealthy attack which forces the DMA system to replay old data. There are at least 3 ways to execute this attack, either performing a MitM on the DMA system to alter data in transit, attacking the video servers which processes the DMA information, or attacking the individual devices. A MitM attack was selected as it would likely be the most effective against the majority of device vendors. The PTZ cameras were defeated by

attacking the Linux operating system of the cameras and locking them in a direction which is the most advantageous for the adversaries. New badges were also added to the access control system by attacking the biometric readers and configuring them with a new badge. The network targets of the cyber-attack can be seen in Figure 12.



Interface	Status	Protocol Description
Fa1/2	Up	ECP Controller 10.5.54.12
Fa1/3	Up	DMA Camera 3 10.5.55.154
Fa1/4	Up	Biometric Device 10.5.54.20
Gi1/1	Up	CAS-NCS01 Gi2/16
Gi1/2	Down	CAS-NCS02 Gi 2/17

Interface	Status	Protocol Description
Fa1/2	Up	Building 1 Controller 10.5.54.11
Fa1/3	Up	DMA Camera 1 10.5.55.152
Fa1/4	Up	DMA Camera 2 10.5.55.153
Gi1/1	Up	CAS-NCS01 Gi2/14
Gi1/2	Down	CAS-NCS02 Gi 2/15

Interface	Status	Protocol Description
Fa1/2	Up	Controller 10.5.54.13
Fa1/3	Up	Camera 5 10.5.55.161
Fa1/4	Up	Camera 6 10.5.55.162
Fa1/5	Up	Camera 7 10.5.55.163
Fa1/6	Up	Camera 8 10.5.55.164
Fa1/7	Up	Camera 10 10.5.55.166
Fa1/8	Up	Camera 15 10.5.55.171
Fa1/9	Up	Camera 16 10.5.55.172
Fa1/10	Up	PTZ Camera 1 10.5.55.197
Fa1/11	Up	DMA Camera 10.5.55.153
Gi1/1	Up	CAS-NCS01 Gi2/18
Gi1/2	Down	CAS-NCS02 Gi 2/19

Interface	Status	Protocol Description
Fa1/2	Up	Controller 10.5.54.14
Fa1/3	Up	Camera 11 10.5.55.167
Fa1/4	Up	Camera 12 10.5.55.168
Fa1/5	Up	Camera 13 10.5.55.169
Fa1/6	Up	Camera 14 10.5.55.170
Fa1/7	Up	Camera 17 10.5.55.173
Fa1/8	Up	Camera 18 10.5.55.174
Fa1/9	Up	Camera 19 10.5.55.175
Fa1/10	Up	Camera 20 10.5.55.176
Fa1/11	Up	Camera 21 10.5.55.177
Fa1/12	Up	Camera 22 10.5.55.178
Fa1/13	Up	Camera 29 10.5.55.179
Gi1/1	Up	CAS-NCS01 Gi2/20
Gi1/2	Down	CAS-NCS02 Gi 2/21

Interface	Status	Protocol Description
Fa1/2	Up	Controller 10.5.54.15
Fa1/3	Up	Camera 23 10.5.55.179
Fa1/4	Up	Camera 24 10.5.55.180
Fa1/5	Up	Camera 25 10.5.55.181
Fa1/6	Up	Camera 26 10.5.55.182
Fa1/7	Up	Camera 28 10.5.55.184
Fa1/8	Up	Camera 30 10.5.55.186
Fa1/9	Up	PTZ Camera 3 10.5.55.199
Fa1/10	Up	PTZ Camera 4 10.5.55.200
Fa1/11	Up	DMA Camera 4 10.5.55.155
Fa1/12	Up	Camera 22 10.5.55.178
Fa1/13	Up	Camera 29 10.5.55.185
Gi1/1	Up	CAS-NCS01 Gi2/22
Gi1/2	Down	CAS-NCS02 Gi 2/23

Interface	Status	Protocol Description
Fa1/2	Up	CAS Workstation 10.5.54.8
Fa1/3	Up	Camera 33 10.5.55.189
Fa1/4	Up	Camera 35 10.5.55.191
Fa1/5	Up	Camera 36 10.5.55.192
Fa1/6	Up	Camera 37 10.5.55.193
Fa1/7	Up	Camera 40 10.5.55.196
Fa1/8	Up	PTZ Camera 2 10.5.55.198
Fa1/9	Up	DMA Camera 5 10.5.55.156
Gi1/1	Up	CAS-NCS01 Gi2/24
Gi1/2	Down	CAS-NCS02 Gi 2/25

Figure 12: Scenario 2 cyber attack network targets.

In this scenario adversaries one and two are using the tree line west of the facility for cover to be able to suppress the response force towers if needed. Adversaries three, four, five and six move to the OCA fence line. The adversary breaches through the OCA fence line, moves up to the PA fence line and breaches the PA fence line. Due to the nighttime attack and the lack of DMA and PTZs at the facility, the adversaries are able to move to this location without being detected or visualized by the response force. During the TTX, it was assumed that there would be a five-percent chance that responders two and four would be able to visualize the adversaries before they reach the shark cage to the reactor building. The start of scenario two can be seen in the figure below.

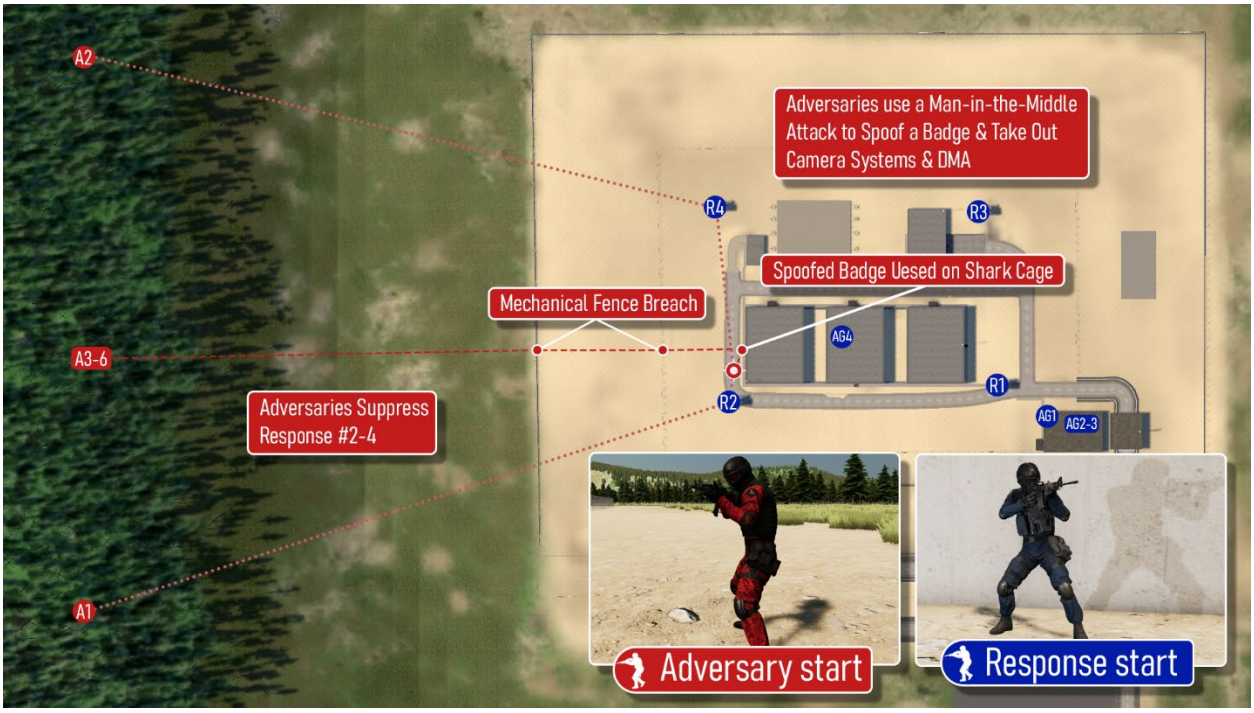


Figure 13 Attack Scenario Two – Beginning

After reaching the shark cage, the adversary team is able to open the shark cage door using the coded credential for the shark cage. As the adversary team opens the shark cage door, two adversaries inside the PA begin to suppress responders two and four, and adversaries one and two begin to suppress responders two and four. The suppressive fire on the BBRE towers are the first notification of an adversary attack on the facility. The breacher from the adversary team enters into the shark cage and begins to try and breach into the facility door. At this point in the scenario responder two and four begin to engage and neutralize adversaries three, four, five, and six at the shark cage to the reactor building. One of the reasons for this is that the responders must now respond to the shark cages based on where they are receiving suppressive fire from. The security feature of having access control devices on the shark cage door that must use a proximity badge and then a door that must have a proximity badge, PIN, and facial recognition force the adversary team to breach through the inner door. This allows responders one and two to engage and neutralize adversaries three, four, five and six. This portion of the TTX can be seen in the figure below.

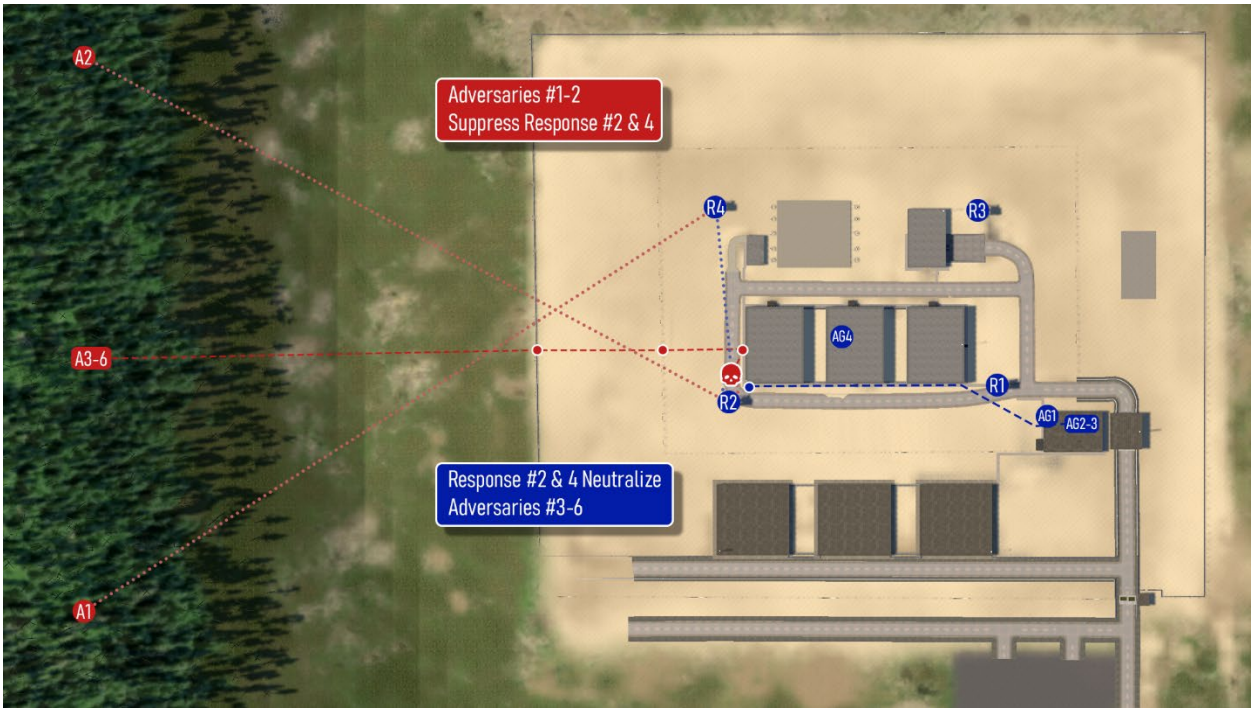


Figure 14 Scenario Two - Adversaries 3-6 Neutralized

Once the responders are able to communicate with the response team lead (RTL), the RTL dispatches two of the ASOs from the PA ECP toward the western reactor building. The adversary team consists of two members who can still continue the act of sabotage at the facility. During the engagement adversary one and two begin to move up to the OCA and the PA and toward the western door to enter into the reactor building. At this point, adversary two attempts to body breach the reactor door. Adversary two decides to body breach the door at this point to ensure that adversary one is able to make entry into the reactor building to complete sabotage inside of the reactor building. As adversary two body breaches the door, responders two, for and the armed security officers begin to engage and neutralize adversary one. This can be seen in the figure below.

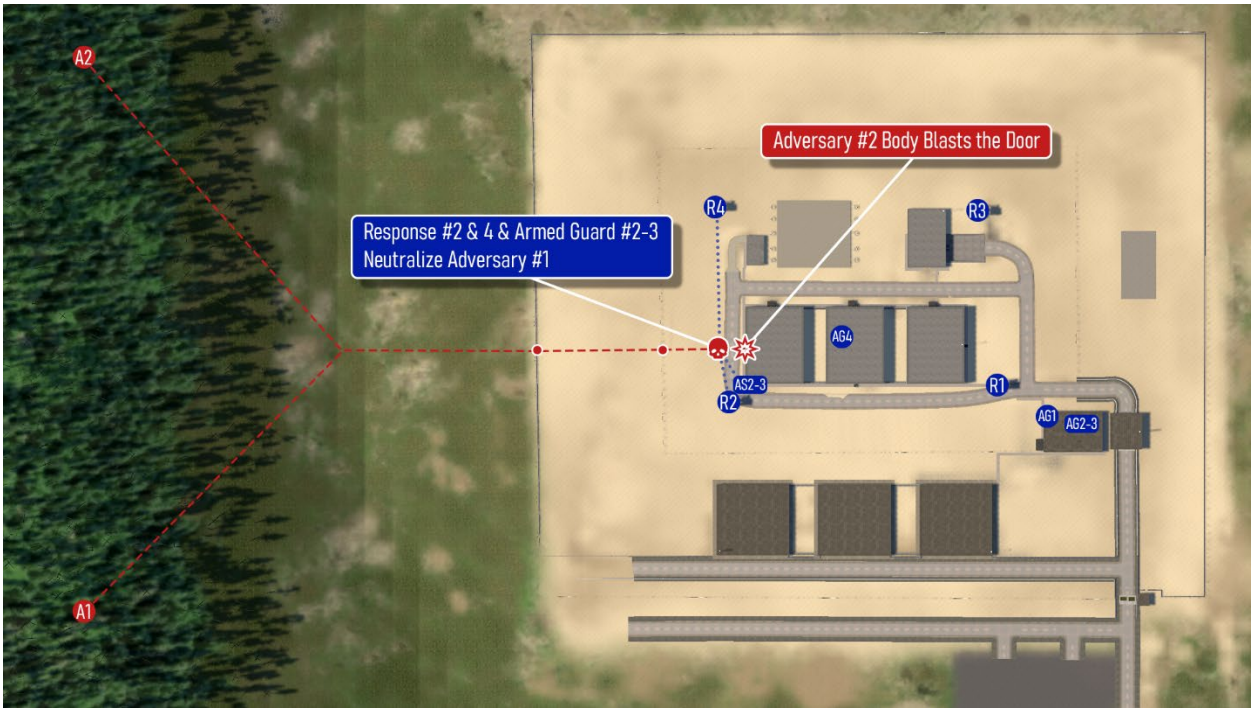


Figure 15 Scenario Two – End

This adversary attack scenario results in the PPS and the response force effectively neutralizing and mitigating the adversaries. There are many compounding factors that allowed the PPS and responders to effectively neutralize the adversaries and mitigate the adversary attack scenarios. The first factor is that the adversary team in this tabletop did not move all eight available adversaries into the PA to attack the facility. The adversary team initially thought that multiple points of suppressive fire would be beneficial and confusing to the responders in the BBREs and disrupt the response force strategy for the facility. However, because the response force strategy was decided that initial response and initial observation from response towers should focus on doorways to enter into the reactor buildings rather than along the perimeter of the PA or OCA. Because of these factors, the response force was able to quickly begin to engage and neutralize the initial group of adversaries aiming to breach into the reactor building. The second competing factor in this scenario is that the ASOs are flexible enough to respond to certain scenarios based on timelines and communication to the ASOs to move to a location where they are able to contribute to interrupting and neutralizing the adversary force.

4.3. Attack Scenario Three

The third adversary attack scenario considered the adversary team using a cybersecurity attack to disable the DMA on the south and west side of the plant, the PTZ on responder two and four towers and developed a fake coded credential to use on the badge and PIN readers to gain access to the facility. Functionally the cyber portion of the attack is the same as attack scenario two. This disabled the ability of the CAS operator and the RTL to effectively determine where the adversary team was attacking the facility from. The adversary team leaves one adversary team member outside of the OCA to help suppress responders two and four with a sniper rifle. The remaining five adversaries approach the OCA, breach the OCA fence mechanically and proceed to the PA fence line. At the PA fence line, one adversary member mechanically breaches the fence and allows two

adversaries to proceed through the fence line breach. These two adversaries proceed through the breach and attempt to place linear shape charges on two legs of the BBRE towers. Once the adversaries are able to place the shape charges, the remaining adversaries start providing suppressing fire on BBRE towers two and four. As the suppressive fire begins, this is the first instance that all security personnel become aware of an adversary attack on the facility. The suppressive fire alerts responders three and one to shift focus to the west of the facility and allows them to engage both adversaries attempting to place the charges. Responder three was able to engage and neutralize the adversary attempting to take down BBRE tower four, while responder one was unable to neutralize BBRE tower two. This portion of the adversary attack can be seen in the figure below.

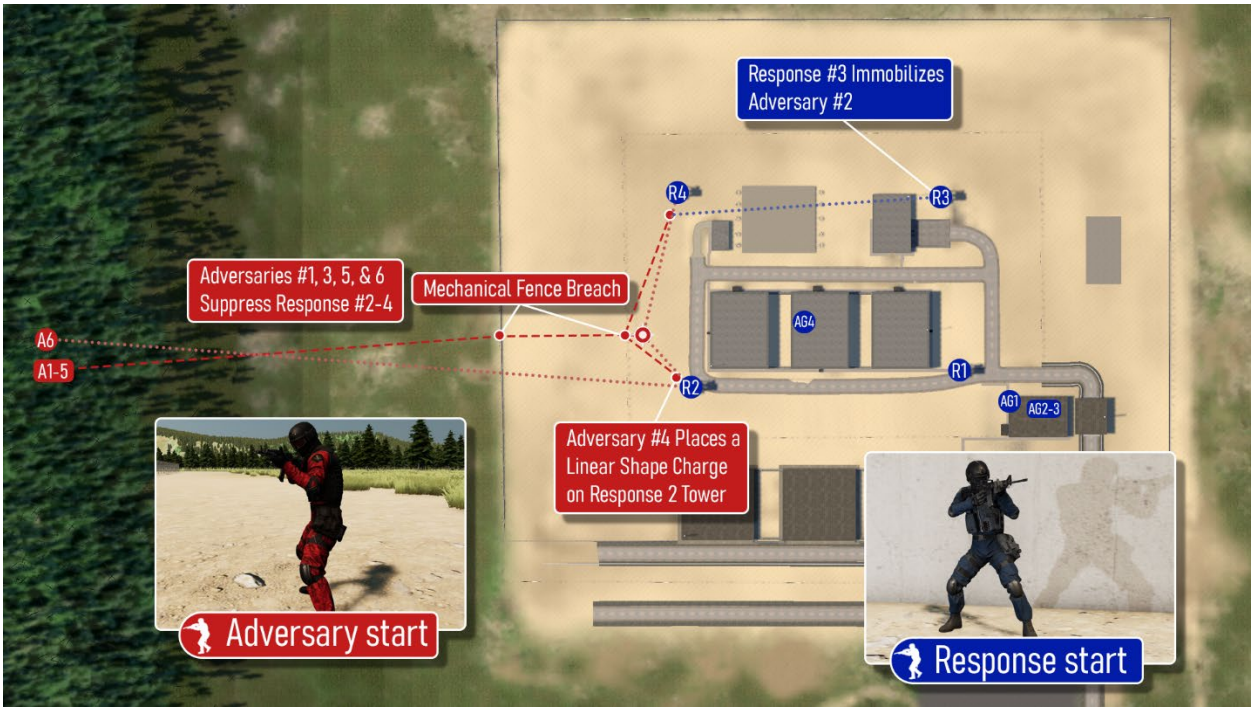


Figure 16 Scenario Three - Scenario Start

Responder one was unable to neutralize the adversary attempting to breach and take down BBRE tower two. This allows the adversary to detonate both linear shape charges and take down the BBRE tower. This portion of the adversary attack scenario results in one tower for the response force and one responder being neutralized and two adversaries are neutralized. At this time the RTL decides to send armed security officers from the entry control point building to interrupt the adversary team before they can make entry into the western reactor building.

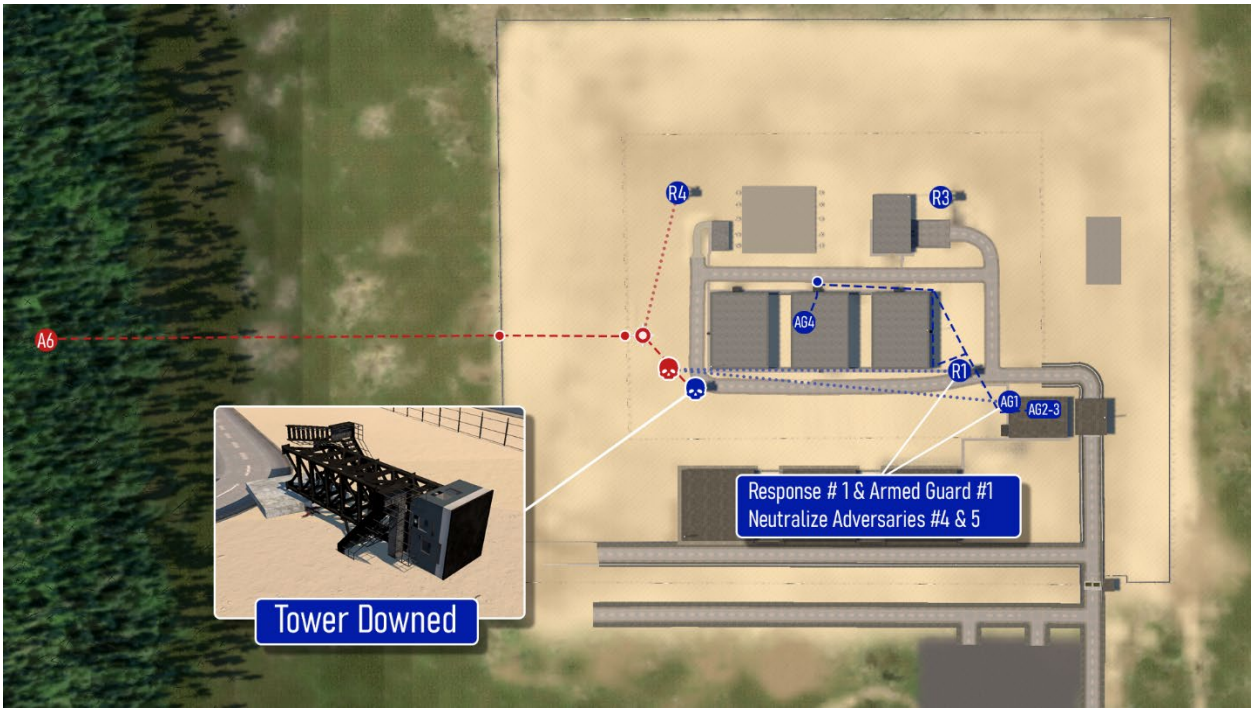


Figure 17 Scenario Three - Downed Response BBRE Tower

Once the adversary tower was disabled there are four remaining adversaries capable of continuing the attack. One adversary is outside of the OCA and three remaining adversaries are insider of the PA. The responder in BBRE tower four is suppressed by three of the adversaries as they continue to move toward the western reactor building and the western entrance to the reactor building. During this time responders in BRRE towers four and three are able to neutralize two of the adversaries. During this time armed security officers are moving toward the reactor buildings. One ASO enters the eastern building, one ASO enters the middle reactor building, and one ASO positions themself on the northwest corner outside of the western reactor building. This ASO is able to position themself to engage and neutralize one of the adversaries inside of the PA. The final adversary attempts to move through the OCA and PA to breach into the western reactor building. Due to the long travel distance and open terrain this remaining adversary must cross, the responder in BBRE tower three is able to engage and neutralize the adversary entering the PA. This final step in the scenario can be seen in the figure below.

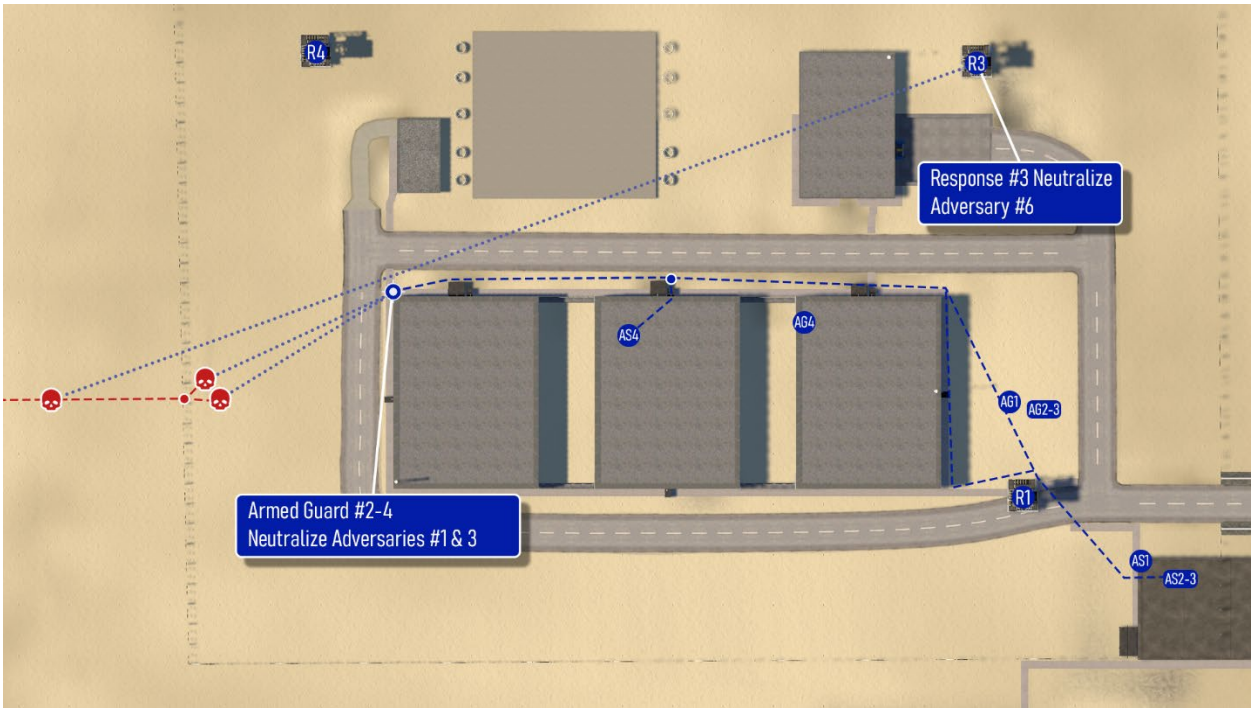


Figure 18 Scenario Three - Neutralization of All Adversaries

The results from this scenario show that the PPS and response force are able to effectively interrupt and neutralize the adversary force. However, in this scenario the response force loses one responder and a BBRE tower due to the adversary attack path and the tactics used by the adversary team. One large lesson learned from this specific tabletop scenario is that an adversary team that has more time and capabilities to perform surveillance and reconnaissance may have been effective at breaching into the reactor building and potentially causing a radiological sabotage event at this facility. The distances and line-of-sight provided to the responders in the BBRE towers are effective at allowing the response force to have adequate lines-of-sight to engage and neutralize the adversary force. If the adversary team was able to plan for longer periods of time they may have been able avoid some of these lines-of-sight and stay alive longer in the attack scenario. Additionally, if the adversary team had decided to use both adversaries to detonate the towers and themselves instead of trying to survive, the adversary team may have been more successful and been able to funnel more adversaries to a protected location to survive and neutralize the adversary force. Finally, if the adversary team had been able to cause a diversion or attack the PA ECP to disable or neutralize the ASOs in the PA ECP.

4.3.1. Attack Scenario Three with Cybersecurity Operations Center

This third adversary was again analyzed but the hypothetical SMR facility was equipped with a cybersecurity operations center (CSOC). The CSOC is dedicated to monitoring the PPS network, the safety system networks, and other critical networks on the facility. In this scenario, the CSOC monitors cyber intrusions to the PPS network.

Due to the addition of a CSOC, the analysts in the CSOC were able to identify unusual network activity from the adversary team attempting to gain access to the network and disable the DMA sensors, the PTZ cameras and the access control system. Due to this early identification, the CSOC

was able to discuss this with the security shift supervisor and response team lead (TRL) and place the PPS in a heightened state of security to prepare for a potential future attack. This attack scenario followed the same adversary attack scenario as discussed above. However, because the adversary team was unable to disable the DMA and the PTZs on the response BBRE towers. Because of this, the response force was able to engage and neutralize the adversaries immediately after they breach the OCA fence line. Responders in BBRE towers two, three and four are able to visualize and engage the adversary force. This scenario and the result of this scenario show that the PPS is able to neutralize the adversary team earlier and not result in the loss of a responder.

4.4. Beyond-DBT Attack Scenario

The fourth scenario considered a beyond-DBT attack scenario. The beyond-DBT capabilities allowed the adversaries to have a kinetic UAS with a 1-kilogram explosive charge that could be used to attack the facility or the response BBRE towers. Additionally, the adversary team was also given an active non-violent insider to use and facilitate the attack of the facility.

The adversary attack started with a cyber attack that disabled all of the DMA stations and the PTZ located on the response BBRE towers. This cyber attack follows the same pattern as attack scenario two. As soon as the DMA stations and PTZs are disabled, one adversary team member moving a large box-truck of explosives through the OCA ECP. The adversary team used their active non-violent insider to allow the vehicle through the ECP while the other ASO was not present. This would have violated the security policy requiring two ASOs to conduct a vehicle search for large explosives. Once this vehicle passed through the OCA entry point, the vehicle and adversary proceeded to the PA ECP. As the vehicle pulls up to the PA ECP the adversary red team begins breaching the PA barrier. At this point the adversary detonates the VBIED at the PA ECP. This results in all ASOs in the ECP being neutralized. The start of this attack scenario can be seen in the figure below.

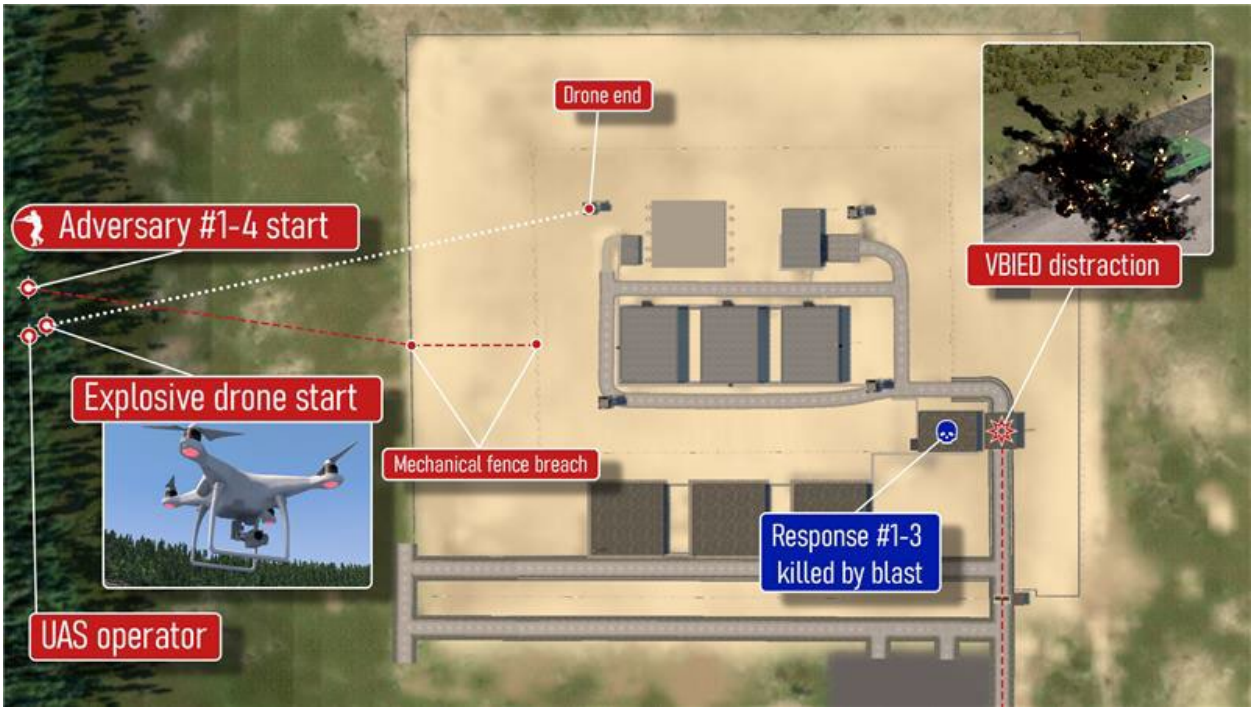
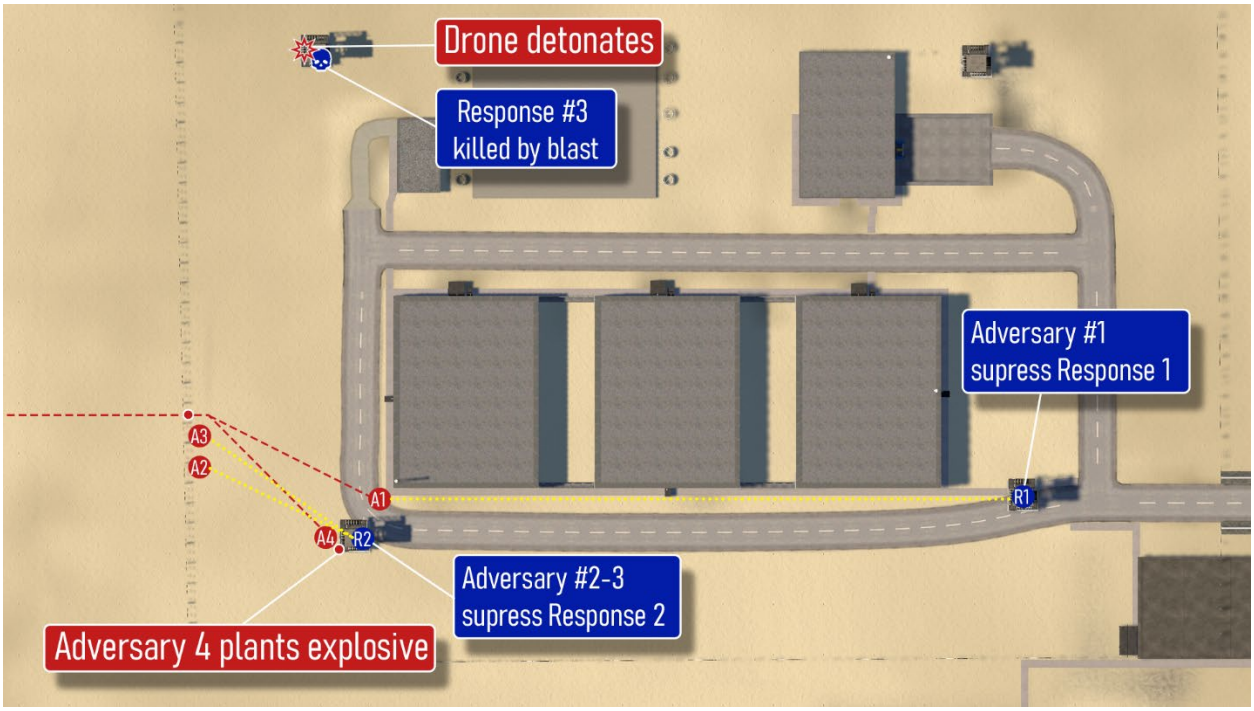


Figure 19 Scenario Four - Scenario Initiation

Once the detonation has gone off at the PA ECP, the four adversaries split into two teams. Adversary one and two move up the BBRE tower two. Here, adversary two begins to place linear shape charges on the legs of the BBRE towers and adversary one moves up to the corner of the reactor building and begins to suppress responder one. The adversary team chose to suppress responder one to ensure that adversary two could successfully cause the downing of the response towers. At the same time, the UAS operator flies the UAS over the responder three tower and detonates the UAS. This blast neutralizes the responder in the BBRE tower. This can be seen in the figure below.



Adversaries two and three begin suppressing the BBRE tower at this point. The responder in BBRE tower two decides to engage the adversary team and is able to neutralize adversary two and three. Once the kinetic UAS explosive detonates at BRRE tower three, adversary two detonates the explosives on BBRE tower two. This causes the collapse of the BBRE tower, neutralizing the responder in the tower. The blast detonated by the adversary also neutralized adversaries one and two due to the explosive blast radius and the charges used by the adversaries to ensure that the tower could be brought down. The UAS operator notices from their position that the rest of the adversary team is neutralized and decides to attack the facility from their position outside of the OCA. At this time the RTL dispatches responder one and four from the BBRE towers to the west reactor building. The final adversary who was controlling the UAS decides to continue the attack on the facility. The adversary is able to collect explosives off of the neutralized adversaries while moving toward the western reactor building. This adversary is able to breach through the reactor building door and make entry into the reactor building. At this time, responder four has made entry into the reactor building and is holding the pathway to the below-grade entrance in the reactor building. The adversary team member, not knowing that a responder is in the building decides to throw a fragmentation grenade into the reactor building to neutralize any adversaries and clear the above-grade floor of the reactor building. This fragmentation grade neutralizes responder four. After the fragmentation grenade detonation has gone off, the adversary is able to make entry into the reactor building. Once inside the building,

the adversary proceeds to the below-grade entry point and places a breaching charge on the door that enters the below-grade portion of the facility where the adversary could attempt a sabotage event on the reactor to cause a potential radiological release. This part of the adversary attack can be seen in the figure below.

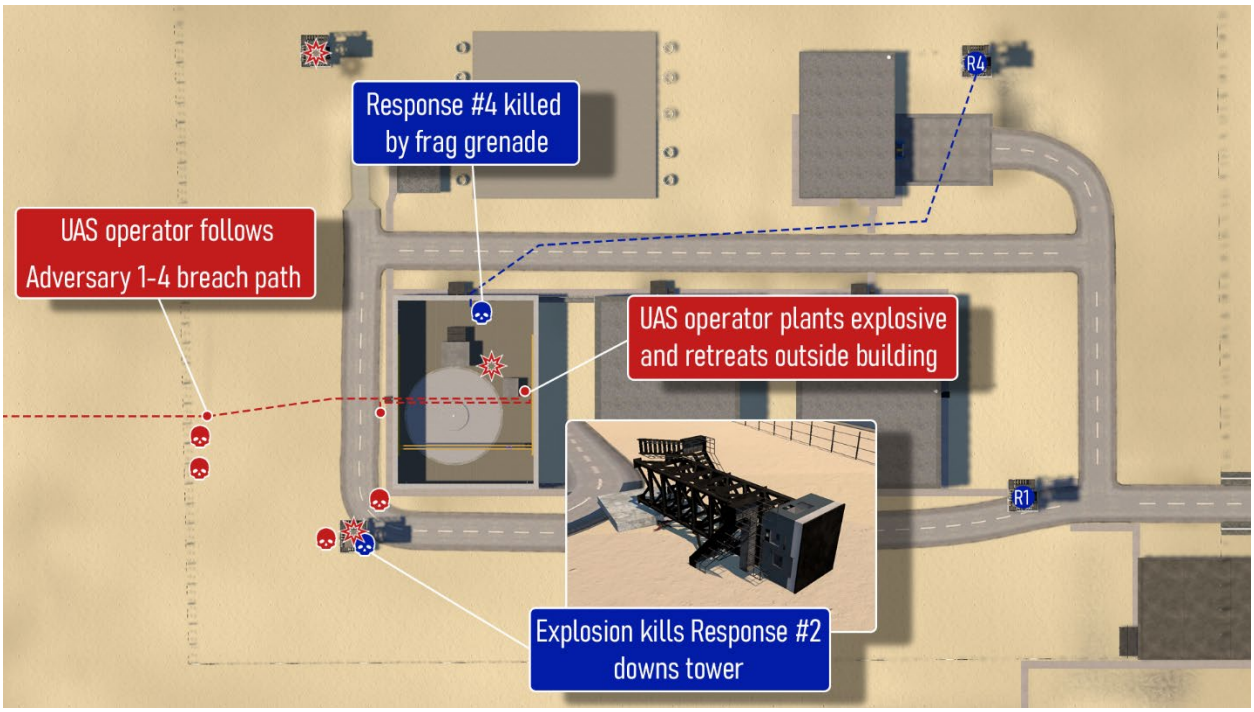


Figure 20 Scenario Four - Adversaries and Responders Neutralized

Once the adversary places the breaching charge on the doorway to enter the below-grade portion of the building, the adversary must retreat out of the building to survive the blast. After the explosive has gone off, the adversary and responder one (who was moving from the BBRE tower) enter the building at the same time. The responder engages the adversary and neutralizes the adversary causing an end to the scenario. This can be seen in the figure below.

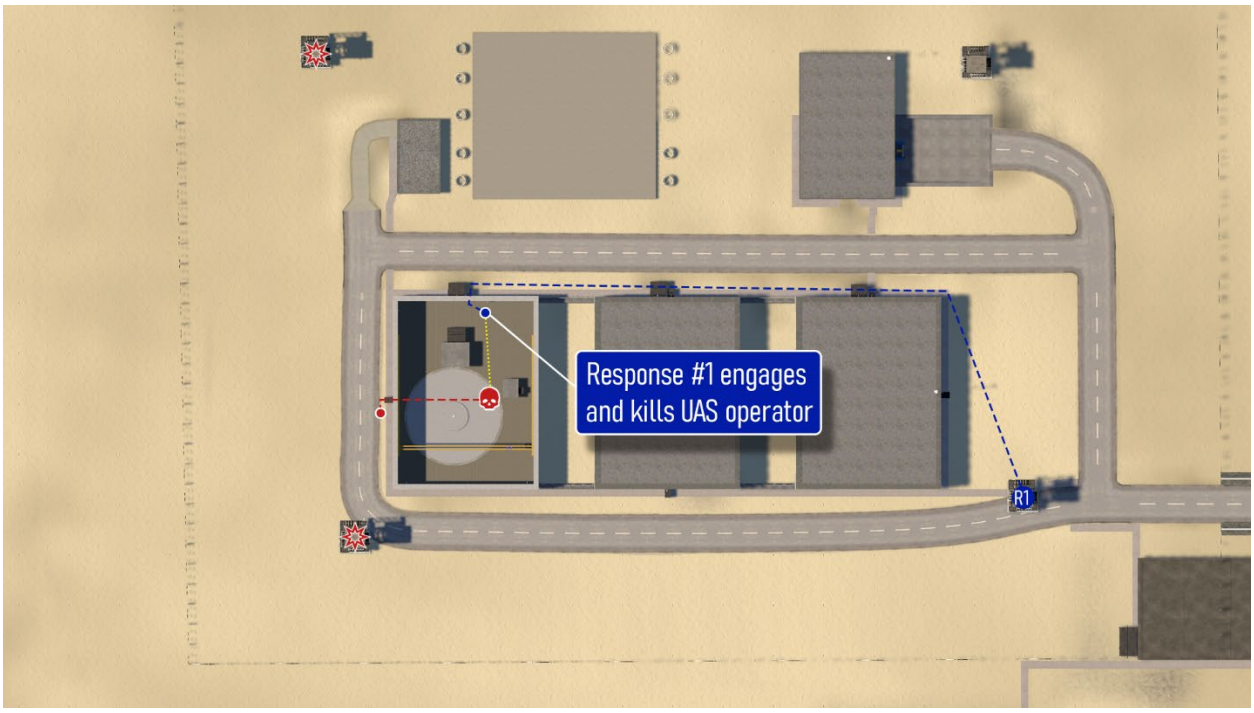


Figure 21 Scenario Four - Scenario End

This adversary attack scenario ultimately resulted in the neutralization of the adversary team before a potential radiological release could have occurred onsite. However, this scenario results in the loss of three ASOs and three armed responders, as well as the loss of two BBRE towers. The operational impact of this loss would be very costly and damaging for the plant's overall ability to operate in the future. However, the results from this tabletop and scenario show that the overall PPS design is robust and creates many effective layers that the adversary must successfully breach and clear before they can achieve a radiological release from this facility.

5. TABLETOP RESULTS AND RECOMMENDATIONS FOR VENDORS

This tabletop set out to identify answers to many of the challenges that SMR vendors may have when considering cyber-physical attacks against a PPS. This evaluation of this facility is not conclusive, and it would require further examination to qualify cyber-robustness. Below are results for questions discussed in the introduction section based on the limited example evaluation of the design detailed in this report.

1. Cyber Attack Effectiveness
    a. How much did the cyber attack contribute to delaying detection?
        i. The cyber attack played a significant role in delaying detection by disabling or falsifying early warning systems (PTZ cameras, radar sensors, alarm logs). However, it did not completely prevent detection, as all attacks were ultimately discovered once kinetic engagement began (e.g., suppressive fire, truck bomb detonation).
        ii. Scenarios 1-3: Cyber attacks delayed detection but did not prevent it because the attackers had to engage the guard towers, which provided a fallback detection mechanism.
        iii. Scenario 4: The cyber attack enabled stealth entry up to the shark cage, but the truck bomb itself was the detection event, meaning cyber manipulation didn't change the ultimate outcome—only when the attack was noticed.
        iv. Key Takeaway: The cyber attack was instrumental in delaying the security response but did not lead to complete failure of the PPS
    b. Did the cyber attack remove any security layers, or did it just delay engagement with the attacking force?
        i. The cyber attack disabled sensing elements (cameras, radar, alarm logs).
        ii. However, it did not remove the final layers of security:
            1. Response towers (independent of cyber systems).
            2. Lighting (not cyber-controlled).
            3. Physical barriers (shark cage, PA fencing).
        iii. While the cyber attack allowed attackers to reach the PA undetected, it did not remove the need for physical engagement, meaning the guard towers still functioned as the primary defensive response mechanism.
        iv. Key Takeaway: The cyber attack removed early warning capabilities but did not remove the final protective layers.
    c. If the cyber attack did not exist, how much sooner would the response force have detected and engaged the attackers?
        i. At the OCA breach instead of the PA or breach (due to functional PTX camera and observant responders)

1. With real time assessment rather than only discovering the attack rather than due to direct engagement from the adversary against the BBRE towers

ii. Without the cyber attack, the response force would have detected the attackers significantly earlier

iii. Key Takeaway: The cyber attack allowed the adversaries to get closer to the reactor building but did not remove the final protective layer (I.e. shark cage at reactor building entrance).

d. Was there a critical point of failure in cyber defenses that made the attack more effective (e.g. shared credentials, flat network)?

i. Yes, the cyber attack was effective due to several critical cyber security weaknesses:

1. The flat network architecture allowed the adversary to laterally move across the entire PPS network once access was granted

a. Scenario 1: attackers used a wireless access point to gain entry and find core switches to the PPS network and disable DMA and PTZ cameras

b. Scenario 4: the Insider (vendor) disabled both access controls and sensors by compromising core switches and completely blinded the PPS except for physical visual observation

2. Shared administrator credentials allowed for complete PPS network compromise once a single password was found

a. Scenario 1: The same credentials were used across all PPS network core switches and enabled the attackers to take down multiple security layers at once

3. Lack of network monitoring: No ability for the blue force to detect or block malicious activity on the PPS network.

4. Key Takeaway: Providing network segregation and not using shared administrator credentials could minimize access points for an adversary and improve the resiliency of the security system to defend against cyber-physical attacks.

2. Physical Protection System Resilience to Attack

a. What PPS elements (response towers, lighting, humans performance) made the biggest difference in stopping the attack?

i. The PPS element that made the largest difference was the shark cages on all reactor building entry door and the overlapping fields-of-fire provided by the response force design.

ii. **Key Takeaway: SMR designers and utilities must identify critical components in the PPS. This can be done by conducting traditional TTXs and cyber-physical TTXs.**

b. How did the engineering of response positions influence the outcome?

    i. The BBRE response towers and their positioning directly influenced all scenario outcomes positively. These response force positions provided overlapping field-of-fire and the flexibility of the ASOs allowed for flexible responses to various adversary attack scenarios.

    ii. **Key Takeaway: The BBRE tower positions and flexibility to deploy ASOs allowed for effective neutralization of adversaries.**

c. If the response force were compromised (fatigued, understaffed, disorganized), would any of these attacks have succeeded?

    i. Response force compromise cause adversary success in certain scenarios given the cyber capabilities and current PPS network configuration.

        1. SMR designers and utilities should consider detailed plans and communication check-ins between the response team lead and the CAS operator. In combination with regular rotations can ensure the response force is able to continually due their assigned job responsibilities.

        2. Understaffing the response force could lead to fatigue and potentially not enough responders and armed security officers being on shift to effectively neutralize an adversary force.

    ii. **Key Takeaway: SMR designers and utilities should ensure programs and trainings are in place to ensure the response force can be effective at their job duties to properly neutralize an adversary force.**

d. Are delay barriers on door entrances a critical delay mechanism, or were they just a minor obstacle?

    i. Shark cages proved to be critical delay barriers in their current design and configuration.

    ii. **Key Takeaway: Delay barriers with proper magnetic lock mechanisms and physical locking mechanisms in the event of compromise can improve the PPS effectiveness in the event of cyber-physical attacks.**

3. Identifying Insights for Cyber-Physical Security Integration

    a. Did the cyber attacks play a critical role or was the resilience of the physical protection system the deciding factor?

        i. Based on the scenarios identified and analyzed through the tabletop exercises, it was shown that the resilience of the PPS was the deciding factor in mitigating these adversary scenarios from completing an act that would lead to a radiological release. These exercises evaluated only four adversary attack scenarios, and other attack scenarios may exist that could impact these outcomes.

    b. If the attackers had purely relied on physical breach techniques, would the outcome have been different?

i. Based on scenario three with the inclusion of the CSOC to the hypothetical facility, if the adversary team was unable to complete a cyber attack they would be neutralized before they could breach through the first shark cage into the reactor building. This does show that a cyber-physical attack was more advantageous to the adversary than a physical attack. However, the adversary team could not successfully complete their mission in a direct physical attack or using a cyber-physical attack.

c. How can a PPS be designed so that cyber compromise does not lead to a radiological release from an act of sabotage?

   i. This analysis shows that a PPS design that includes many robust layers of delay and response can effectively neutralize an adversary before they can complete an act of radiological sabotage. The design of this PPS allowed for the response force to have effective fields-of-fire to engage and neutralize an adversary.

   ii. PPSs should be designed with various electronic security systems to include sensors, locks, and access control features that not only increase adversary task time and the complexity of an adversary attack but also increase the difficulty of a cyber attack and reduce the likelihood that an adversary will be able to successfully disable all electronic security measures used in a PPS

   iii. **Key Takeaway: A PPS design should include multiple layers of detection, delay, and response that can be allow the response force to effectively interrupt and neutralize adversaries without the inclusion of electronic security measures.**