Security Modeling for Advanced Nuclear Facility Design

M. Jordan Parks, Benjamin B. Cipiti, Ben Stromberg, Todd Noel, and Ryan Knudsen

Sandia National Laboratories
P.O. Box 5800 MS 0779
Albuquerque, NM 87185-0747 USA
bbcipit@sandia.gov

Abstract

Several decades ago, the design of Physical Protection Systems (PPS) was typically done after a nuclear facility was completed. The evaluation of the PPS would occur using path analysis and tabletop exercises to identify deficiencies. Today, single analyst modeling and simulation tools dominate the field and allow for much more rapid and efficient design and analysis of a PPS. These tools also allow security requirements to be considered from the beginning of the facility design process in order to develop optimized and cost-effective protection strategies (Security by Design). The Material Protection, Accounting, and Control Technologies (MPACT) working group is demonstrating Safeguards and Security by Design (SSBD) for a generic electrochemical reprocessing facility as part of a 2020 Milestone. The Scribe3D© and PathTrace© tools have been used for PPS design and analysis to support this milestone. The PPS design process will be described along with the tools and analytical results. Security by Design recommendations are highlighted.

Introduction

The MPACT working group, funded through the U.S. Department of Energy, Office of Nuclear Energy, conducts research on technologies and concepts to improve safeguards and security in the civilian nuclear fuel cycle. The MPACT program recently completed a 2020 Milestone to develop a Virtual Facility Distributed Test Bed to demonstrate advanced SSBD. A generic electrochemical facility was used for the demonstration due to recent research and development on related technologies. The Virtual Test Bed is described in more detail in the overview paper accompanying this special issue.

The "Virtual Facility" aspect of the milestone refers to the use of systems-level modeling tools to design the plant and monitoring systems. The security design and modeling work is described here. The Material Control and Accountancy (MC&A) system and the PPS are typically kept separate for division of responsibilities which helps to minimize the insider threat.

This paper describes the PPS design process and steps through the iterative nature of PPS design for a new facility. The modeling and simulation tools are emphasized. The results section highlights performance metrics achieved for the baseline design. Security by Design recommendations are provided.

PPS Design Process

In the physical protection world, DEPO (Design and Evaluation Process Outline) [1] has been used for several decades for the design of a PPS. The DEPO process is shown in Figure 1. The process begins by defining the PPS requirements which involves defining regulatory requirements, characterizing the facility, identifying targets, and identifying the threat. From there, the PPS is designed with appropriate elements for detection, delay, and response. Then various tools are used to evaluate the PPS including both path analysis and performance testing. These tools have increasingly moved toward single-analyst modeling capabilities. Based on performance and identified gaps or vulnerabilities, the PPS will be redesigned. One revision that has been made to the original DEPO process is to include Security by Design (SBD) recommendations. SBD means not just adding more guns, guards, and gates, but considering security aspects early in the design process to help optimize facility costs. The PPS design will be iterated until satisfactory results (from performance tests) are obtained.

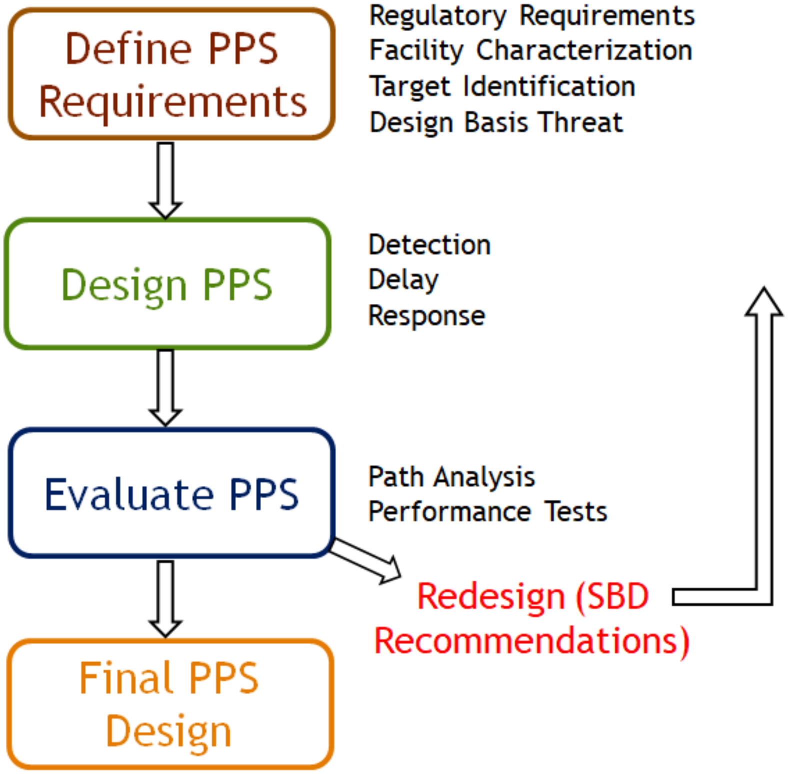


Figure 1. DEPO process[1]

Regulatory Requirements

The process for designing a security system for a new facility begins with regulatory requirements. In the U.S., physical protection of plants and materials is outlined in the Code of Federal Regulations (CFR)[2] 10 CFR Part 73. The regulations follow a graded approach depending on the category of the facility. Any commercial reprocessing facility would be a Category I facility.

10 CFR Part 73 covers all aspects of the design of the PPS including general performance capabilities. Key points are highlighted here. The facility must maintain at least one security member on site and contain a tactical response team of at least five members at all times. At least 2 guards must be present at each access control point. The two-man rule is required for any material access areas. Vital and material access areas must be located in a protected area, and the functions of a Perimeter Intrusion Detection and Assessment System (PIDAS) are required around the protected area. At least two barriers are required around vital areas. Several other requirements are called out including use of isolation zones, lighting, communication, and protection of digital systems amongst others.

The design of the PPS is also heavily informed by the Design Basis Threat (DBT), which can vary significantly for different types of facilities or locations (eg. those located in the vicinity of known terrorist cells or other well-documented threats). The DBT defines the adversary threat including number of adversaries, outsider versus insider, capabilities, and equipment. This information is sensitive and as such is not included here; instead, the physical protection analysis considered a range of outsider threats to develop a general PPS strategy that is robust to the scenarios of interest.

10 CFR Part 74 does not include specific performance metrics that must be met due to the more subjective nature of analysis techniques, particularly from several decades ago. However, a good practice is to achieve a probability of neutralization greater than 80% using modeling and simulation tools for a variety of theft and sabotage scenarios. There is also flexibility in the language of the regulation to allow for alternative designs if a case can be made to justify the performance.

Electrochemical Facility Characterization

The electrochemical reprocessing facility baseline flowsheet is described in detail in an accompanying article in this issue[3] and will not be repeated here. This information helps to define the targets, but a baseline facility layout was also needed. A high-level diagram of an electrochemical facility design was described in reference 4, and reference 5 was used to help fill in gaps. The high-level diagram was used as a starting point, but the building was modified in order to include all necessary support functions and to include realistic geometries. A 3D building model was created using the Blender[6] tool, which was then also used for the path analysis and force-on-force modeling. Figure 2 shows the layout of the main processing level (ground floor) with the air hot cell and argon hot cell shown in the middle. The shipping/receiving high bay, central alarm station, control room, generator room, and entry control point are also pointed out.

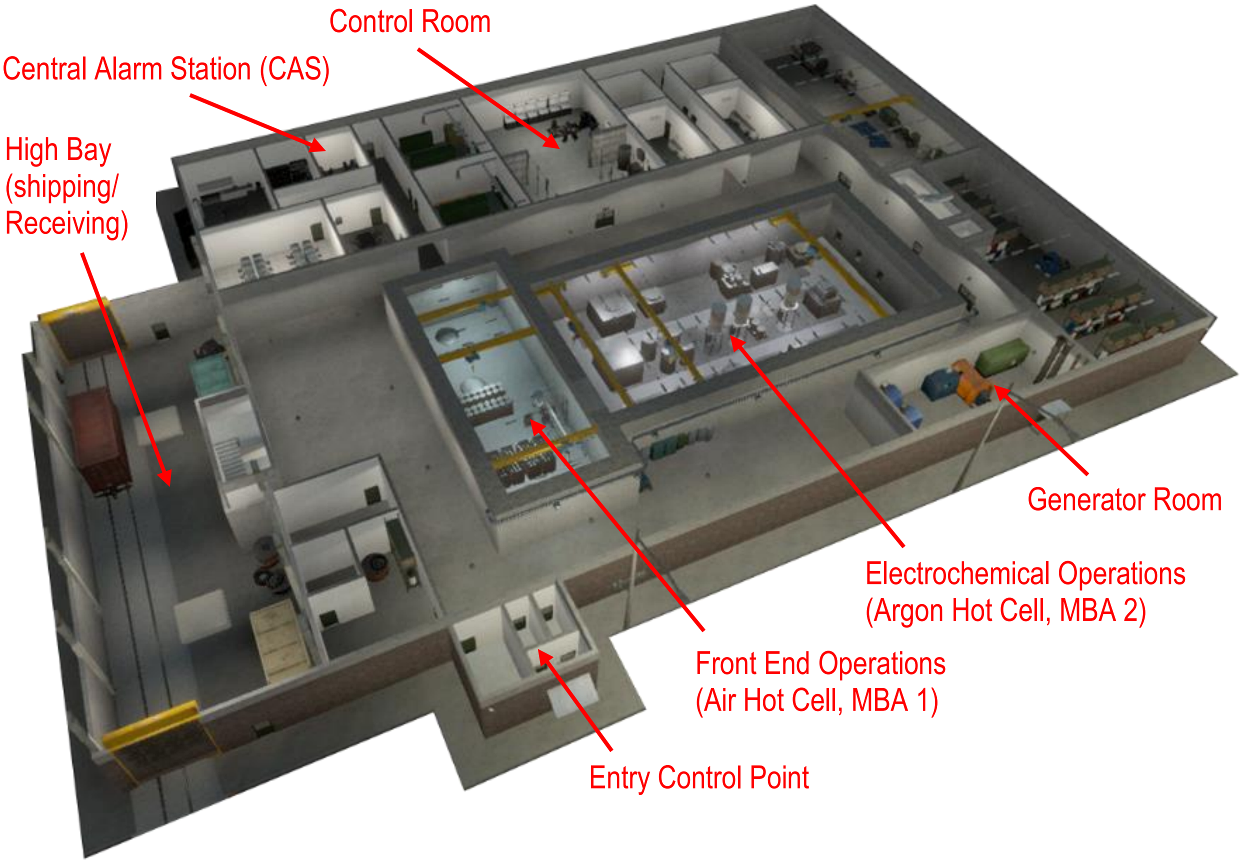


Figure 2. Electrochemical facility processing level

The electrochemical facility has a top floor which provides access to the hot cells for hot repair and maintenance operations. For brevity, it is not shown here. The basement contains the uranium and transuranic (U/TRU) storage vault and transfer tunnels that move material from the high bay into the process cells. Figure 3 shows the basement level.

The security aspects of electrochemical facilities are not significantly different than at any other nuclear facility, and in some cases the nature of the process provides opportunities that benefit the PPS. Many of the processing materials (like dendrites or molten salt) would be difficult to work with or remove from the facility.

The thick walls of the hot cell, along with an argon environment (which contains the bulk of the electrochemical processing equipment), provide barriers to access, and this is taken into account in the design of the PPS. The U/TRU ingots produced by the process are the most attractive target for theft, so protection of this material needs to be a central part of the security design. Security analyses are usually done on a case-by-case basis.

Identification of vulnerabilities and the subsequent mitigations put in place are part of the analysis and design.

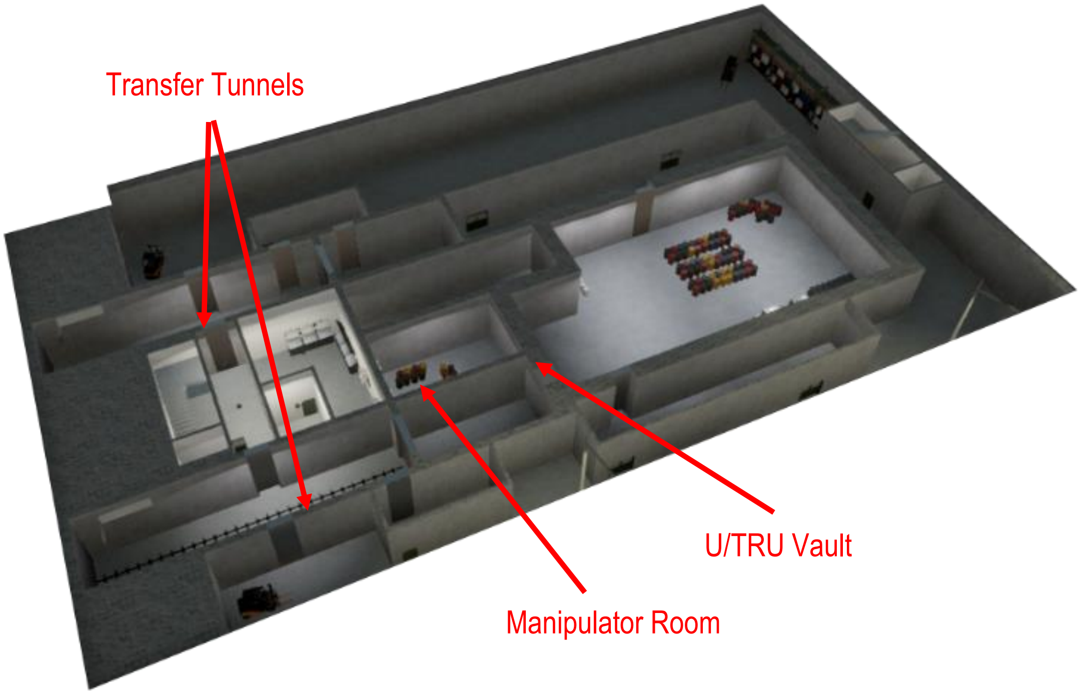


Figure 3. Electrochemical facility basement level

Target Characterization

The material types and forms were evaluated to generate a list of theft and sabotage targets. Material transfers into and out of the facility are assumed to occur with compensatory measures in place. Nuclear material is transferred into and out of the hot cell through underground tunnels, and while in the hot cells, the thick shield walls provide an additional security barrier. U ingot and waste forms will be stored in a different building but contain large plugs above underground storage. The following provides a summary of the targets considered:

Spent Nuclear Fuel – SNF is present as whole assemblies, in smaller pieces during disassembly and de-cladding, and as small pieces when it is loaded into the baskets for processing. SNF is a less attractive theft target due to the dilute form, presence of fission products, and handling difficulties; however, criticality events should be considered from a sabotage perspective. Approximately 4-5 kg of Pu are contained per fuel assembly or processing basket.

Oxide Reduction – During oxide reduction, the fuel converts to metallic forms but stays within the basket. The salt is contaminated with active metal fission products, so theft from this location would be less attractive. The salt itself does not contain fissionable material but could potentially be the target of a sabotage event to attempt to disperse radioactive material. Approximately 4-5 kg of Pu are contained per basket.

Electrorefiner – The ER salt may contain between 50-100 kg of Pu, but it is diluted in about 9000 kg of salt. Roughly 1000 kg of molten salt would need to be removed in a theft scenario. The U and U/TRU cathodes would not be considered theft targets since theft after cathode processing would be more attractive. The ER salt also contains high amounts of rare earth fission products, so could be a target for sabotage to disperse radioactive material.

U Metal Product – Pu content in the U ingot is negligible, and the U-235 content is about 1%. The U ingots also contain very little fission products. Therefore, the attractiveness for theft or sabotage is very low.

U/TRU Metal Product – The U/TRU ingot contains a roughly equal mix of U and Pu along with other minor actinides. The higher Pu content and limited amounts of fission products make this the most desirable theft target in the facility. Theft from the hot cell or storage vault is difficult but should be considered. Criticality events should also be considered from a sabotage perspective. Approximately 4-5 kg of Pu are contained in each ingot.

Metal and Fission Product Waste Forms – The waste forms contain very little actinides but include activation and fission products. They could be considered for sabotage scenarios or theft for a dirty bomb. However, biological dose is dominated by actinides, and fission products present less of an actual consequence in terms of dose to the public. These wastes contain kg quantities of fission products.

Backup Generator – A generator is required to keep the salts molten should the facility lose off-site power. Loss of the generator would not cause an accident but could cause economic damage to the operator. The generator is considered a vital area and may be a target in a plant sabotage scenario.

Threat

The threat used for this study covers a spectrum of adversaries and is not meant to replicate the DBT as defined by any U.S. government agency. The study was parametric in that a range of number and characteristics were considered. Adversary numbers were varied from 4-8 to study robustness of the system against a range of threats. Table 1 describes the adversary capabilities used for the study.

Table 1. Adversary capabilities

Adversary Capabilities Studied

Motivation		Ideological; cause public terror (regionally and internally)
Goals		Theft and/or sabotage of nuclear materials/items
Capabilities and Attributes	Numbers	4 - 8
	Weapons	Automatic or Semiautomatic Rifles
	Explosives	Commercial and military explosives (assume sufficient amounts to complete objective)
	Tools	Hand tools, power tools, bridging/breaching equipment, chains, ladders, ropes, cutting torches, radios
	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	Assume full facility knowledge, security system (people, equipment/technology, and procedures), and mission-critical operations
	Technical Skills	Military training, demolition, information technology, general and site-specific engineering
	Funding	High – regional and international support
	Passive Insider Collusion	Planning, local cell structure, safe-havens, sympathetic population, logistics
	Active Insider Collusion	Ability to manipulate material processes, move material around the hot cell, into the vault, and transport hatch
	Support Structure	One insider (both passive and active roles considered)

PPS Design

The PPS design process starts once the facility characterization was complete. The PPS design is shown in the next several sections, and the analysis led to design changes which are described in subsequent sections. The modeling tools used for the design and analysis are described below.

Modeling Tools

Blender – Blender[5] is a free and open source 3D creation suite that is widely used throughout the 3D modeling community. It is designed to create efficient, highly detailed 3D models that can be ingested by any engine. The Blender toolset allows for the creation of detailed, to-scale models of facilities, vehicles, and equipment that can then be used for visualization, analysis, and training.

PathTrace© – Pathtrace is a tool that allows a user to explore and analyze entry paths in two dimensions. Given an aerial photo or detailed drawings of the facility, the user draws barriers such as walls, fences, windows, doors, and any user created material on top of the image of the facility, specifying delay times and detection probabilities for protection elements. Once the user has mapped out the entire facility, they can then analyze the entry paths into the facility with a variety of methods, given the PPS Response Force Time (RFT) and an adversarial strategy. The final data allows the user to fully explore their facility and any potential vulnerabilities in a simple fashion.

Scribe3D© - Scribe3D is a 3D tabletop recording and scenario visualization software, created by Sandia National Laboratories. It was developed using the Unity[7] game engine for use by other national laboratories, government organizations, and international partners. Scribe3D© is used to create, record, and play back scenarios developed during tabletop exercises or as a planning tool for performance testing, force-on-force, or other security analysis related applications. Transcript reports are automatically generated from the recorded data. The automated functions of Scribe3D allow for recorded scenarios to be run in a Monte Carlo method (i.e. numerous iterations with random sampling of certain variables), to collect large quantities of data for analysis and optimization purposes, after initial scenarios are defined in the traditional tabletop exercise.

PPS Site and Building Design

The electrochemical reprocessing facility features a single passive fence for limiting public access only. It has no sensors or detection. One of the Security by Design recommendations found in doing this work is to eliminate a Perimeter Intrusion Detection and Assessment System (PIDAS) and instead equip the building skin with seismic vibration sensors to detect breaching of the building walls and emergency exit doors. The elimination of the PIDAS (but replacement with wall sensors) will save considerable costs and is possible due to the single building design, thick shield walls, argon atmosphere, and underground vault storage. Due to the lack of an extended radius PIDAS around the facility, accurate detection and rapid response are necessary to balance cost with system effectiveness. A single entry control point (ECP), staffed with 2 response force (RF) officers, is the only authorized personnel entry point to the facility. All building doors feature magnetic locks and balanced magnetic switches (BMS).

The ECP, seen in the bottom of Figure 4 extending outward from the exterior wall of the building, is equipped with a mantrap formed by two metal doors and the ECP walls. Both doors are equipped with a BMS and remote-controlled lock. The inner door is equipped with a door closing device, proximity card reader, and PIN pad for entry and exit. A personal portal monitor is also installed to detect metal and radioactive substances.

The interior PPS for the processing level is characterized in Figures 4 and 5 (the main processing level and basement level). As mentioned above, all exterior doors are protected with magnetic locks and BMS's and are assessed by dedicated camera systems. Interior doors which lead to protected areas as well as stairwell doors are protected in the same way.

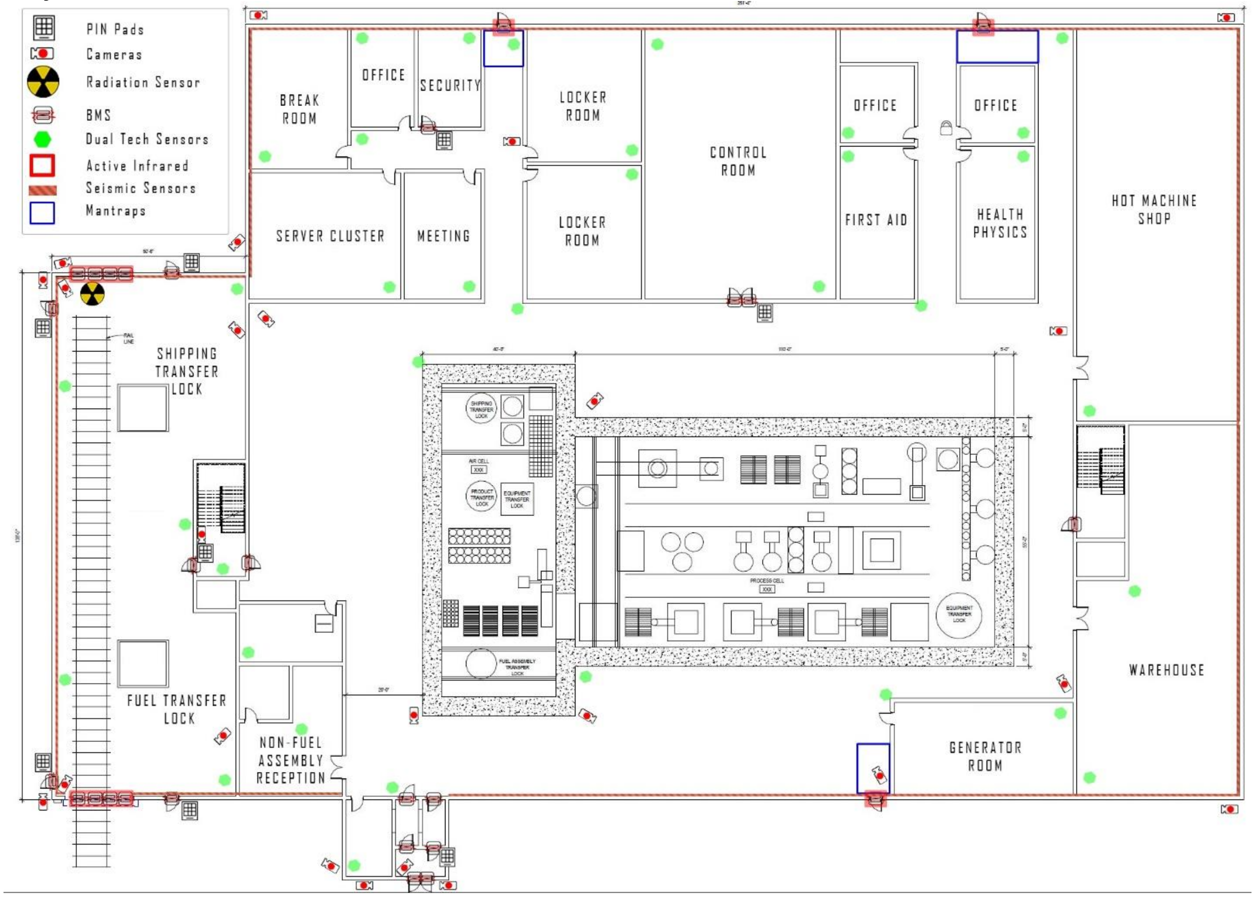


Figure 4. Processing level PPS elements

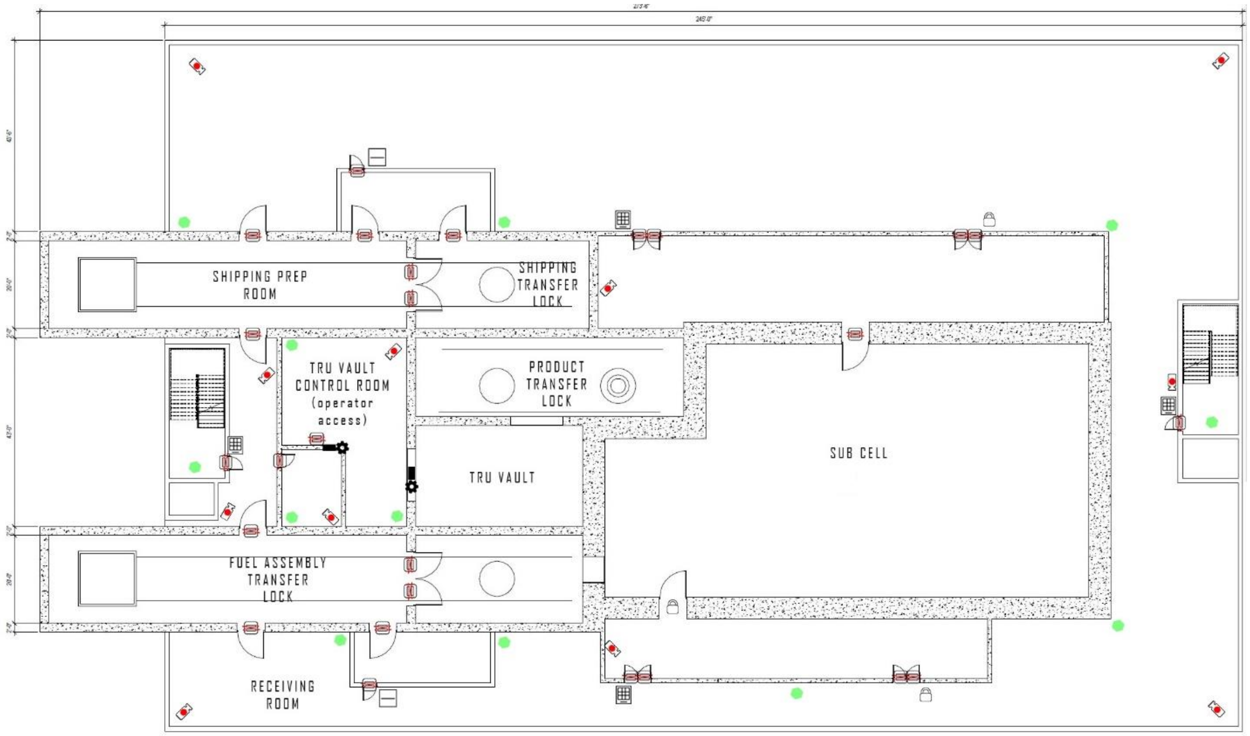


Figure 5. Basement level PPS elements

Doors leading from the stairwell and into the U/TRU manipulator room in the basement are protected with magnetic locks and BMS's and are assessed by dedicated camera systems. The door leading directly into the manipulator room is protected by a GSA Class 5 Vault door for increased security. An additional area of concern is the Central Alarm Station (CAS)/RF room, identified as the Security room in Figure 4. Another sensitive area is the hot maintenance room on the top level of the facility due to it being the location of the Secondary Alarm Station (SAS) and for safety concerns.

The CAS provides oversight of emergency activities and maintains protection of all nuclear material onsite. All alarms, assessment, and dispatch is handled here.

Response Force (RF)

Notional requirements are used as a first step to define the RF roles and responsibilities. In an actual design, the roles and responsibilities will be based on the facility's regulations and site requirements. It is assumed that the on-site special RF is staffed with ten officers during each day, night, and swing shifts. Officers are equipped with rifles, and typical law enforcement equipment.

The onsite RF will consist of 10 officers divided into multiple teams and placed at different locations within the building based on roles and to prevent losing them to a preemptive attack. There is also a 2-person offsite response team consisting of Local Law Enforcement Agency (LLEA) personnel. It is assumed that no other response personnel would be able to respond before the conclusion of the adversary timeline. **Error! Reference source not found.** shows RF numbers, starting locations, and muster times. RF times are purely notional and represent possible times but are not based on any existing facility or posture.

Table 2. Response Force Overview

Team	#	Location	Muster Time (s)	Responsibility
Outer Patrol	2	Outside Building	30	Protected Area Containment, Alarm Assessment
Inner Patrol	2	Inside Building	30	Protected Area Containment, Alarm Assessment
Entry Control	2	Main Entrance	NA	Entry Control, Operating Floor Containment (does not respond)
CAS	2	CAS	NA	Provide Command and Control (does not respond)
QRT1	2	GF Room, CAS, Operating Floor	90	On Duty Quick response team
Offsite LLEA	2	Offsite Response	600	Offsite Containment
Total	12	6 Onsite Responders, 2 Offsite Responders, 2 Entry Control, and 2 Command Control		

After initial detection, a 30 second alarm assessment and communication time occurs before the muster times of all RF begin. Offsite responders will be dispatched per the plant Memorandum of Understanding (MOU) in the event additional resources are needed to neutralize the adversary/event.

Vulnerability Assessment of the Facility PPS

Vulnerability Assessment (VA) results are based on an analysis of the physical paths that the adversary follows to achieve their objective. The performance capabilities of detection, assessment, delay, and response are used in path analysis to determine probability of interruption (P_I). Key performance measures included in estimating P_I are the probability of detection (P_D), delay time, and RF time (RFT). There are many possible combinations of ways to get to a target location; therefore, all possible adversary paths should be considered. The following are the steps taken in this analysis to determine system effectiveness (and ultimately system vulnerability) and facility risk:

1. An Adversary timeline was constructed and all physical protection elements in the system were identified.
2. Detection and delay values for each protection layer and path element in the Adversary Sequence Diagram were incorporated.
3. The Most Vulnerable Paths (MVPs) were identified by analyzing the effectiveness of detection and delay along each possible path.
4. Scenarios of concern were developed, response timeliness and effectiveness were evaluated, and system effectiveness was determined.

After completing the system effectiveness analysis, the VA team examined the paths and scenarios that had lower-than-desired system effectiveness (i.e., high vulnerability). The goal was to identify the system's greatest vulnerabilities to theft and sabotage so that they could be mitigated.

Outsider Theft Scenario

The first scenario that was considered was a brute force attack by an outside adversary group to steal material from the U/TRU vault. The adversary path is direct from the passive perimeter to the TRU Vault. Direct assaults against RF positions were considered but deemed unlikely to succeed due to time constraints on the adversary to begin their task before the RF can muster and interrupt. The adversary will breach an emergency exit door, proceed downstairs and breach the multiple shield doors on their way through the transport port in the TRU vault. The path is captured in Figures 6 and 7, which show the facility model overlaid with colors identifying barriers, regions, and paths.

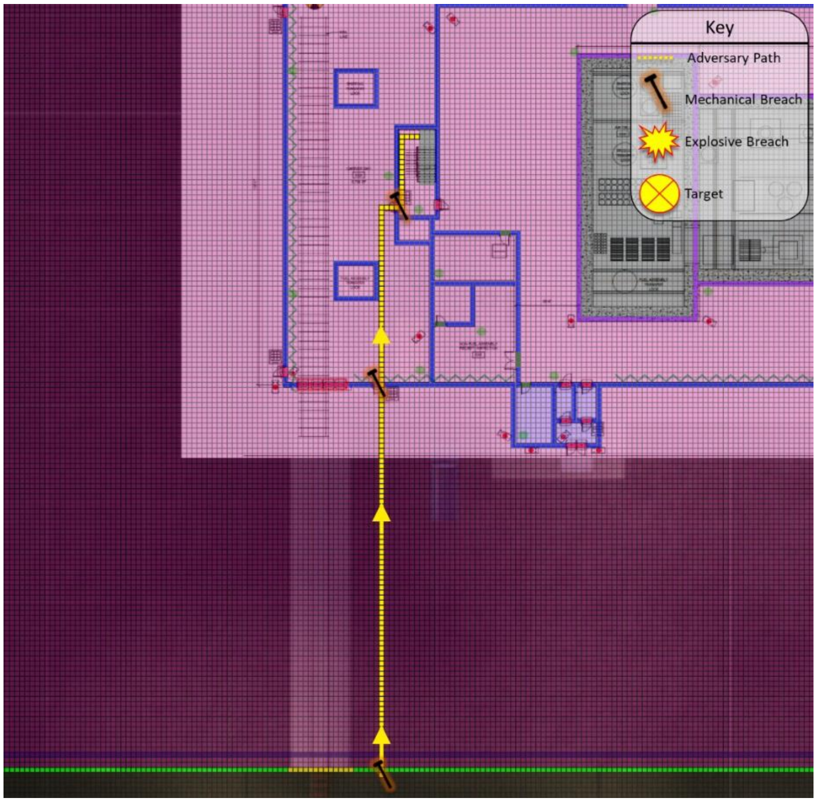


Figure 6. PathTrace path on ground floor for outsider TRU vault theft scenario

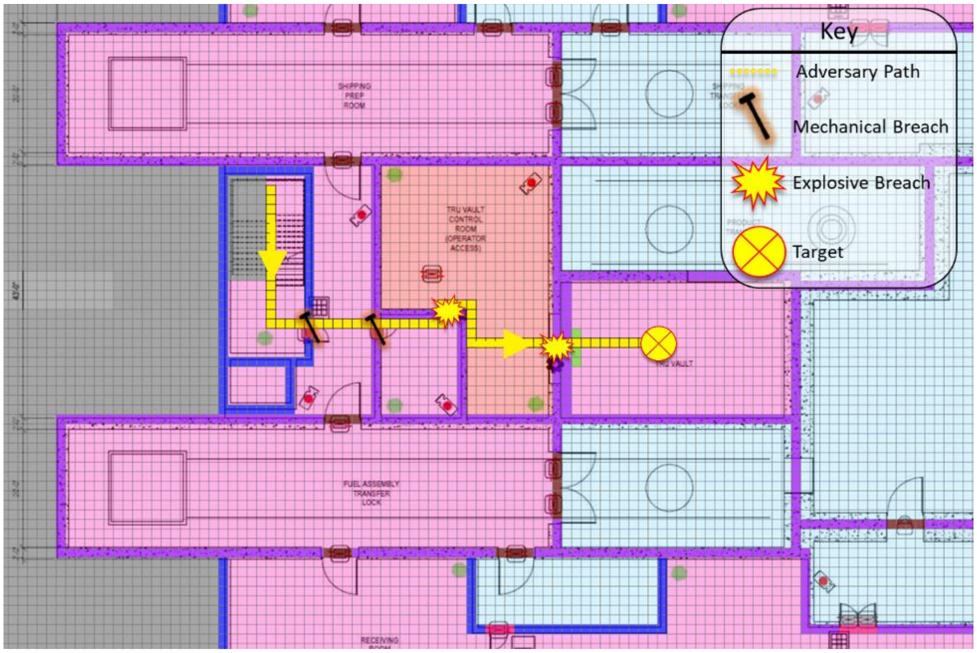


Figure 7. PathTrace path in basement for outsider TRU vault theft scenario

Outsider Theft Path Analysis Results

Generic data is used for detection and delay elements on the way to the target to avoid issues with sensitive information. Table 3 shows that the adversary is interrupted at an extremely high rate (P_I =.99). Total scenario time is 956 seconds. The adversary penetrates several doors with high detection probabilities using explosives, so detection is virtually guaranteed. The timeline is very long due to the long breach time of the TRU vault.

Table 3 - PathTrace path results (^indicates combined times)

Task	Description	P(Detection)	Delay (mean seconds)
1	Breach outer passive fence	0.02	20.00
2	Engage foot patrol	0.02	10.00
3	Move to building exterior (50m)	0.02	11.94
4	Breach Emergency Exit Door	0.8	30.00
5	Move to Stairwell Door	0.02	5.96
6	Breach Upper Stairwell	0.8	30.00
7	Move down to Lower Stairwell door	0.02	5.54
8	Breach Lower Stairwell Door	0.8	30.00
9	Move to Basement Hall Door	0.02	0.99
10	Breach Basement Hall Door	0.8	30.00
11	Move to Vault Door at TRU Vault Control Room	0.02	1.15
12	Breach Vault Door	0.8	
13	Move to Shield Wall at TRU Vault	0.75	
14	Breach Shield Wall at TRU Vault	0.8	
15	Breach Inner Shield Wall	0.8	283^
16	Set up and Climb step latter into TRU Vault	0.02	
17	Move to Target Material	0.02	
18	Retrieve Target Material	0.02	468.00^
19	Exit Site	0.02	65.33
			Total Time
	Probability of Interruption:	**0.99**	**956**

Outsider Theft Attack Scenario

The path analysis conducted showed that the adversary would most likely be detected as they breach the emergency exit door of the facility near the loading bay. In the simulation, it is assumed that the adversary has cut the outer passive fence and advanced to the exterior of the building. As the breach team is completing the exterior breach, the exterior RF patrol is engaged from cover. There are no other exterior RF patrols to detect this engagement if successful by the adversary. Upon completion of the outer breach, the adversary enters the facility, and moves to the stairwell in the transportation high bay. The adversary breaches the outer door and moves downstairs. The adversary team makes its way downstairs and breaches the inner stairwell door. They then move to the U/TRU vault control access area outer door and breach it. Next, they move to the vault door leading into the U/TRU vault control room and begin their breach. Meanwhile, the RF team in the CAS has met its muster time and begins moving to containment positions outside the building. Approximately ten minutes after the initial alarm, the LLEA first responders arrive and set up facility containment positions. Roughly fifteen minutes into the scenario, the adversary has acquired the target and attempts to leave the site, see Figure 8.

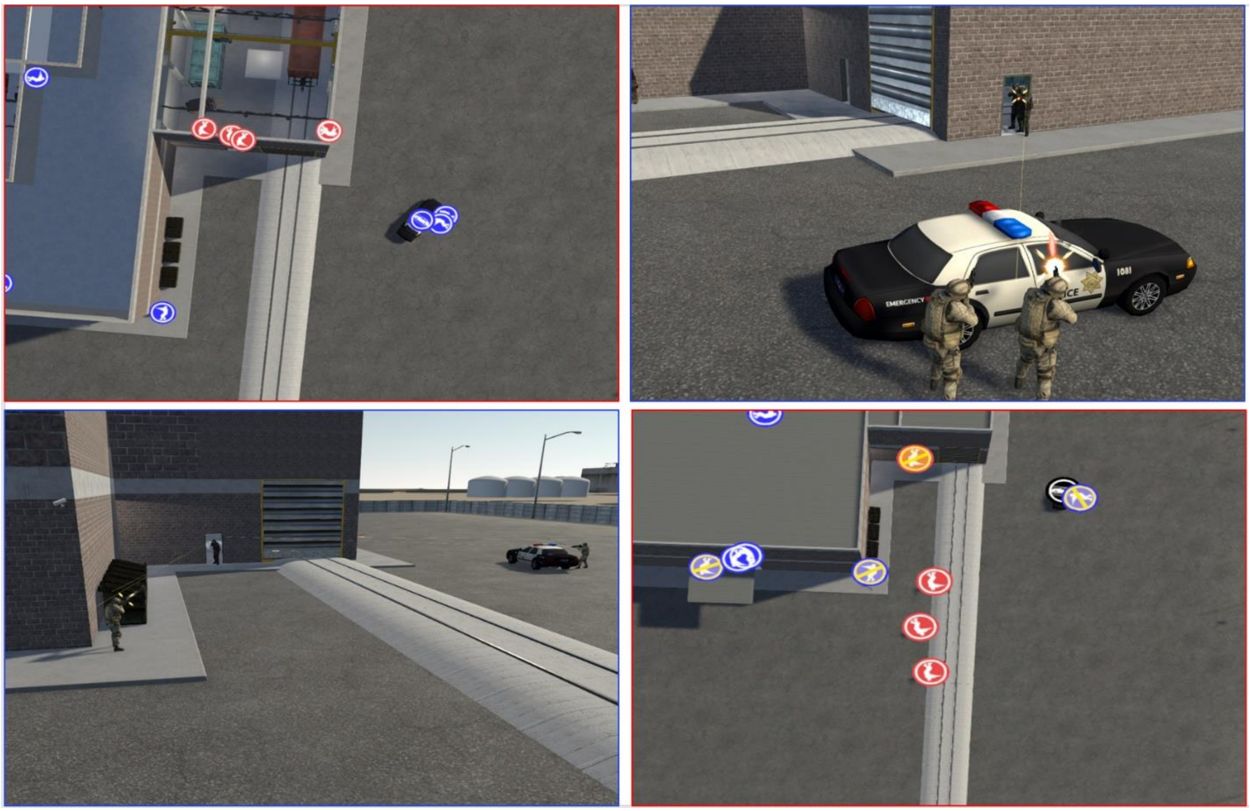


Figure 8. Adversary attempts escape: upper left – adversary sets up to exit the building with riflemen at two exit doors; upper right – LLEA and adversary engagement; lower left – RF and adversary engagement; lower right - adversary escaping with material

Outsider Theft Scenario Neutralization Analysis Results

The scenario was run 100 times, for threat groups ranging from 4-8 individuals, using the automated features of Scribe3D. The RF was able to prevent the theft over 90% of the time versus 4 and 5 individuals, and over 75% of the time versus 6 individuals. The gradual system degradation as adversary numbers increase shows robustness. The inherent delay of the vault's underground construction forces the adversary to perform numerous smaller explosive breaches, leaving the enclosed vicinity of the blast each time, which greatly extends the adversary timeline and allows offsite local law enforcement agencies (LLEA) to respond.

A theft scenario with insider collusion was also examined, and the system effectiveness was similar to the outside only theft scenario. Despite good results against 4-5 individuals, upgrades were considered to improve the overall system effectiveness. Reference 8 provides more detail on the upgrades. Upgrade 1 included mantraps on all exterior doors to increase delay for the adversary entering the facility. Upgrade 2 included mantraps plus shifting the exterior patrol to the interior of the building. Upgrade 3 included extended detection around the facility utilizing a Fused Radar and Video Motion Detection using the Deliberate Motion Algorithm, ankle-breaking anti-transit landscaping, and hardened fighting positions in the building. Figure 9 shows the results of the neutralization analysis for the two baseline theft cases along with the results for the collusion scenario after the upgrades are applied. The upgrades provide the facility options to create an extremely well-secured design with progressively more robust protections. A facility designer can utilize this information to determine an optimal design based on upgrade costs and the perceived threat as outlined in the DBT.

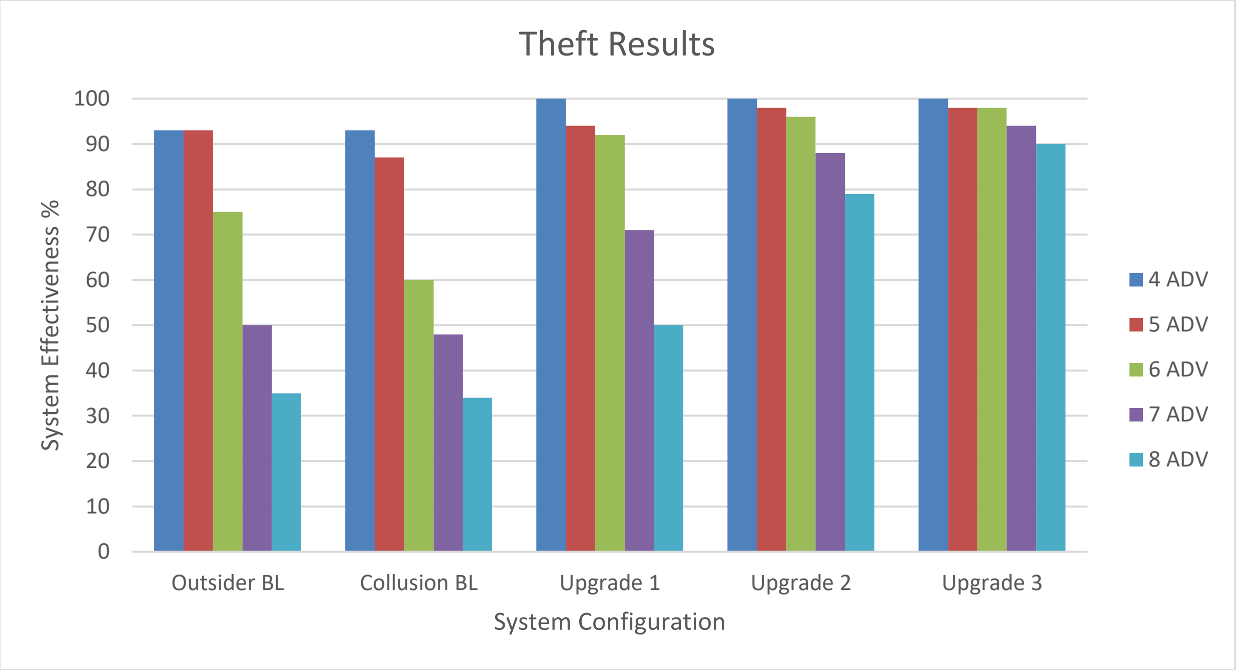
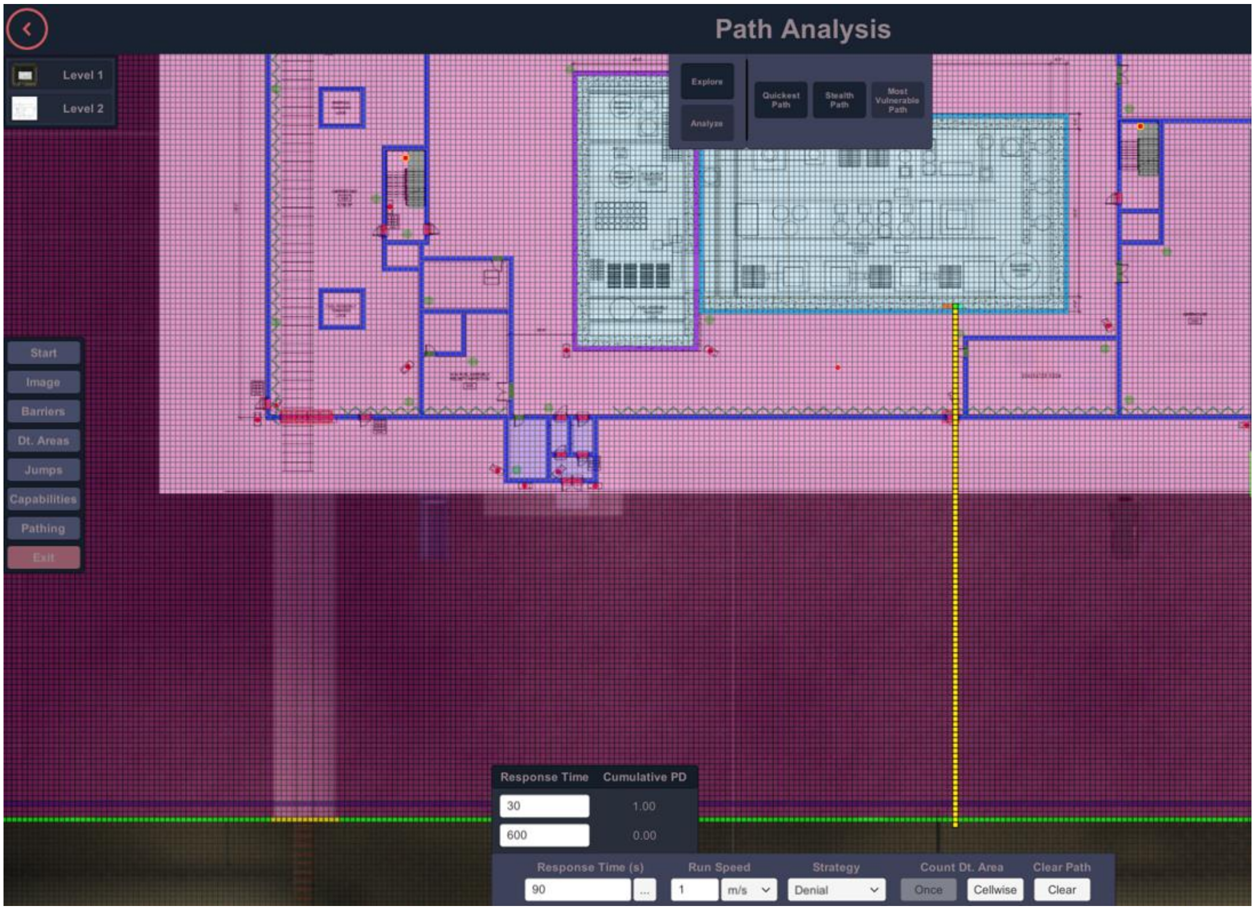


Figure 9. Probability of neutralization - outsider theft scenarios with upgrades

Hot Cell Sabotage Scenario

In order to fully test the PPS of the facility, a notional sabotage scenario was also examined. In this scenario, the adversary attempts to breach the argon hot cell in order to halt operations, create an international incident, and/or trigger material release. The hot cell sits just inside several emergency exits which provide quick access. The adversary will conduct a multi-phase sabotage attack where they penetrate the wall of the hot cell, then place follow-on charges through the initial penetration. Figure 10 below shows how short the path is (identified as yellow blocks), from offsite to the hot cell, as this design only features one barrier with reliable detection. This results in rapid, easy access to the hot cell wall for the adversary.



Response Time	Cumulative PD
30	1.00
600	0.00

Response Time (s): 90
Run Speed: 1 m/s
Strategy: Denial
Count Dt. Area
Clear Path

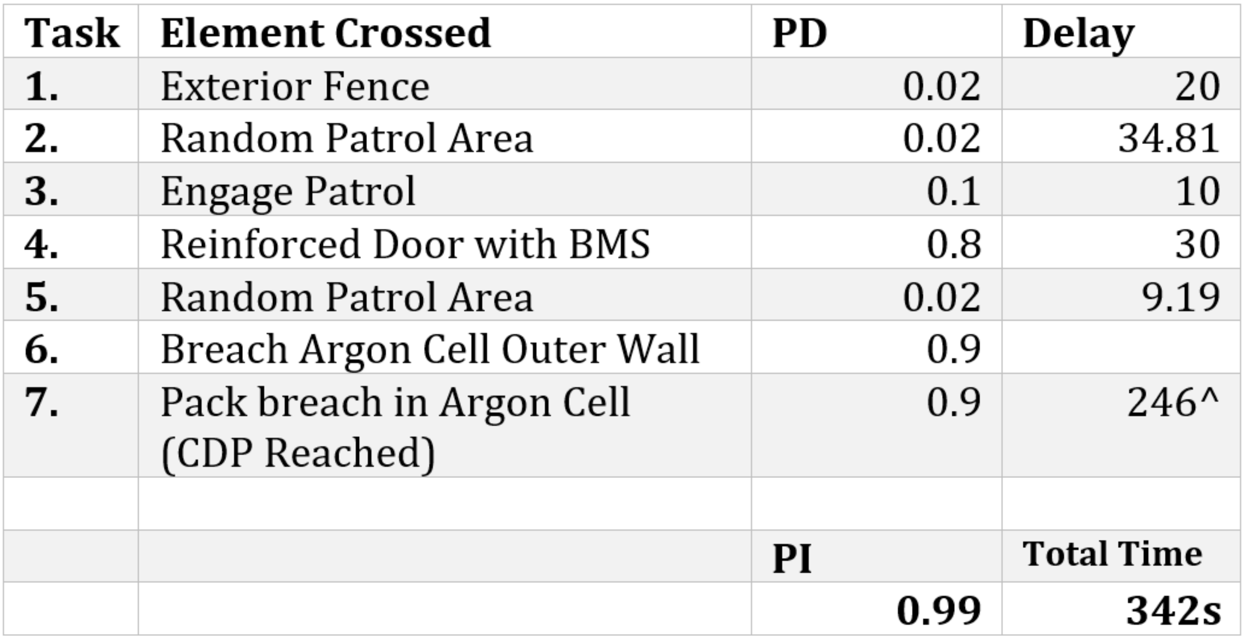
Figure 10. Sabotage scenario path analysis results

Sabotage Scenario Path Analysis Results

The actual sabotage attack, which begins with the adversary reaching the hot cell wall, features a multi-stage breach event. The adversary much first use an explosive charge to penetrate the wall of the hot cell, and then use a follow-on charge to further disperse the hot cell contents.

Generic data is used for detection and delay elements on the way to the target. Table *4* shows that the adversary is interrupted at an extremely high rate (P_I =.99). Total scenario time is 342 seconds. This time allows for all onsite RF to muster and interrupt the adversary but is too short for offsite LLEA to arrive prior to completion of the sabotage attack. Detection is largely driven by the BMS on the emergency exit door which triggers an alarm in the CAS in addition to the multiple explosive breaches along the adversary path.

Table 4. Sabotage scenario path analysis results (^indicated combined times)



Task	Element Crossed	PD	Delay
1.	Exterior Fence	0.02	20
2.	Random Patrol Area	0.02	34.81
3.	Engage Patrol	0.1	10
4.	Reinforced Door with BMS	0.8	30
5.	Random Patrol Area	0.02	9.19
6.	Breach Argon Cell Outer Wall	0.9	
7.	Pack breach in Argon Cell (CDP Reached)	0.9	246^
		PI	**Total Time**
		0.99	**342s**

Sabotage Scenario Neutralization Analysis

Scribe3D was used for the neutralization analysis. In this scenario, the adversary breaches the outer perimeter fence, moves to the nearest emergency exit, and engages a RF patrol from cover. The adversary then breaches the emergency exit and moves to the hot cell to begin the multistep sabotage attack (Figure 11). Depending on the threat size, the adversary takes up cover positions around the sabotage location (Figure 12). When the interior patrolling RF hear the breaches, they take up defensive positions at the corners of the hot cell and wait for backup to muster. Once all onsite RF has mustered, they move as a unit and attempt to neutralize the adversary (Figure 13).

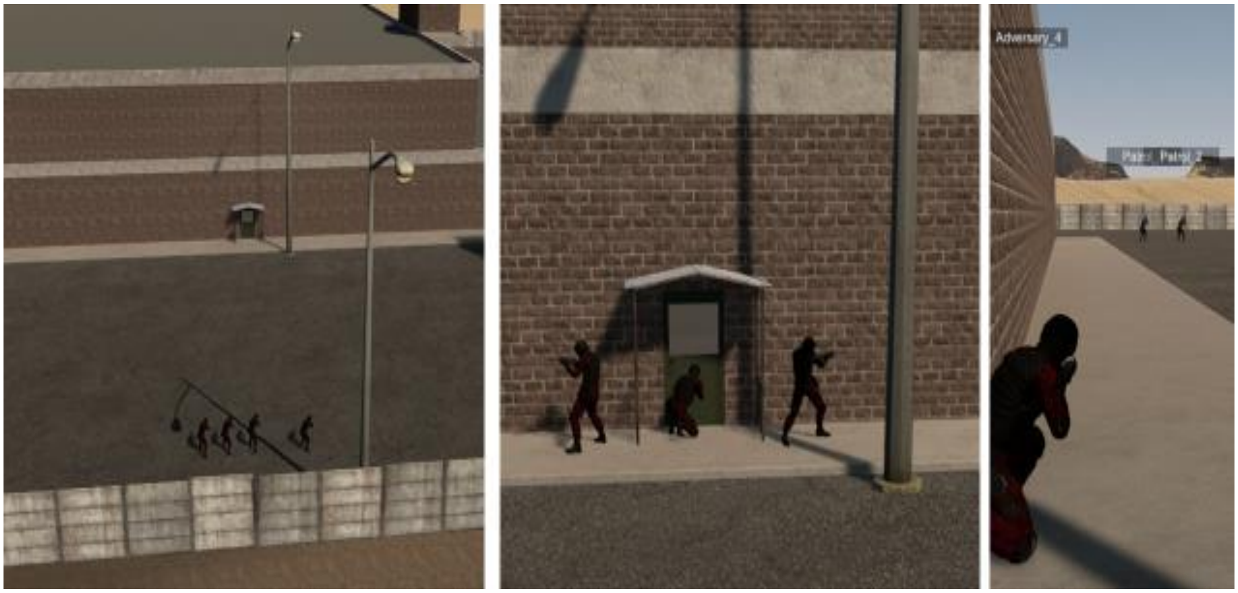


Figure 11. Adversaries approach the facility (left), breach the emergency exit (center), and engage the patrol (right)

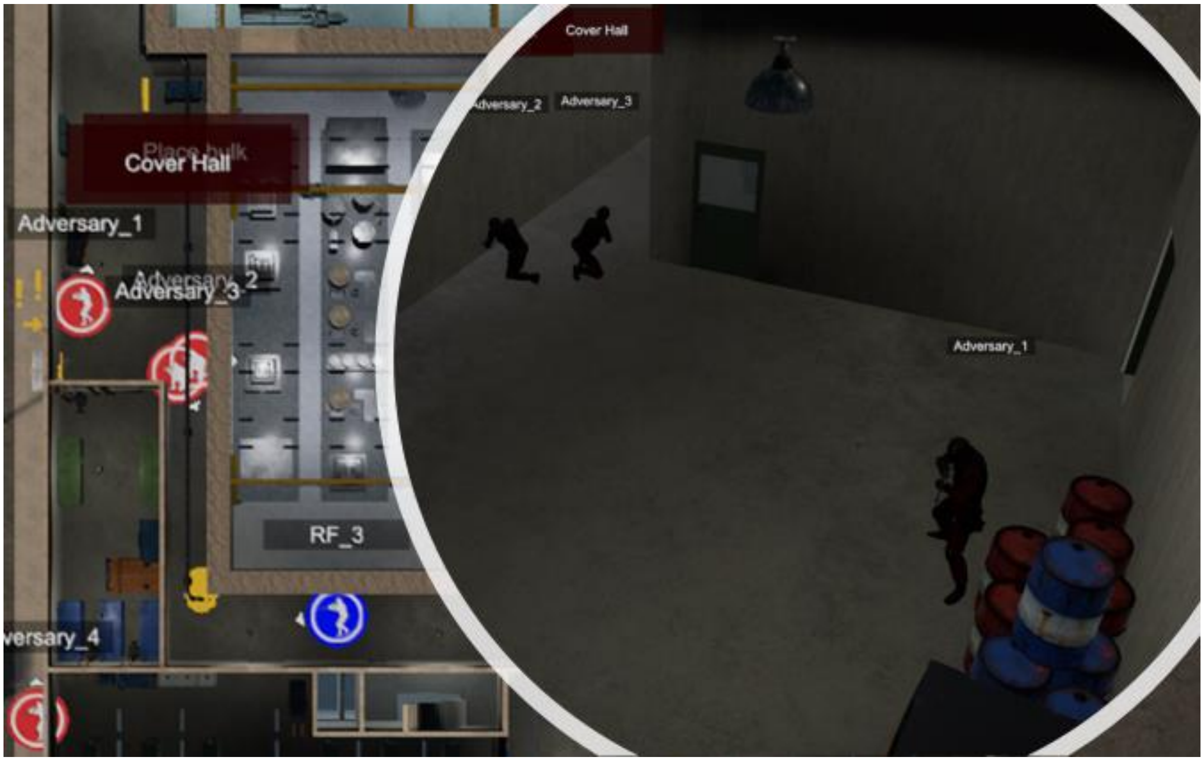


Figure 12. Adversaries attempt to sabotage the hot cell

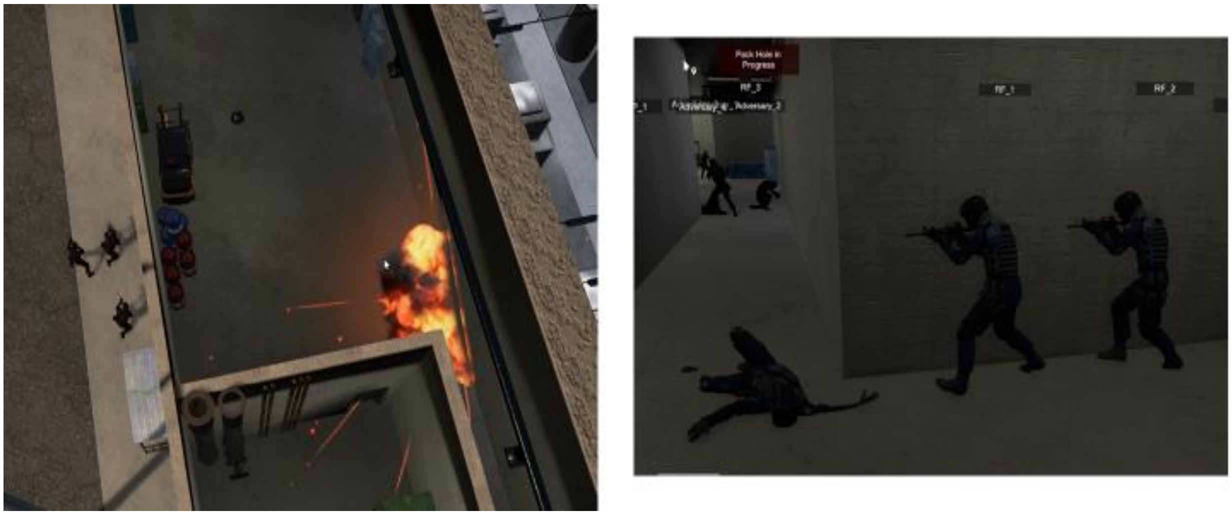


Figure 13. Charges detonate on hot cell (left), and RF try to engage adversaries (right)

The scenario was run 100 times, for threat groups ranging from 4-8 individuals, using the automated features of Scribe3D. The RF was only able to prevent the sabotage about 50% of the time in the 4 individual sabotage scenarios. Adversary numbers greater than 4, as expected, showed worse system performance for the facility. Lack of early detection and a substantial RF mustering delay allowed the adversary to get to the target as well as positions of cover before the RF response. The adversary usually takes out the exterior patrol, and the remaining onsite responders must fight with fewer numbers, not to mention without offsite LLEA response. This results in very low success rates for the RF.

As a result of the poor performance against the sabotage scenarios, similar upgrades to those noted above in the theft scenarios were once again considered. Reference 8 provides more detail on the upgrades. Upgrade 1 included mantraps on all exterior doors and RF changes to tactics inside the building. Upgrade 2 included mantraps plus shifting the exterior patrol to the interior of the building. Upgrade 3 included extended detection around the facility utilizing a Fused Radar and Video Motion Detection using the Deliberate Motion Algorithm, ankle-breaking anti-transit landscaping, and hardened fighting positions in the building. Figure 14 shows the results of the neutralization analysis for the baseline sabotage case along with the results after the upgrades are applied. As before, the upgrades provided progressively more robust protections for the facility, and a facility designer can use this information to determine an optimal design based on upgrade costs and the perceived threat as outlined in the DBT.

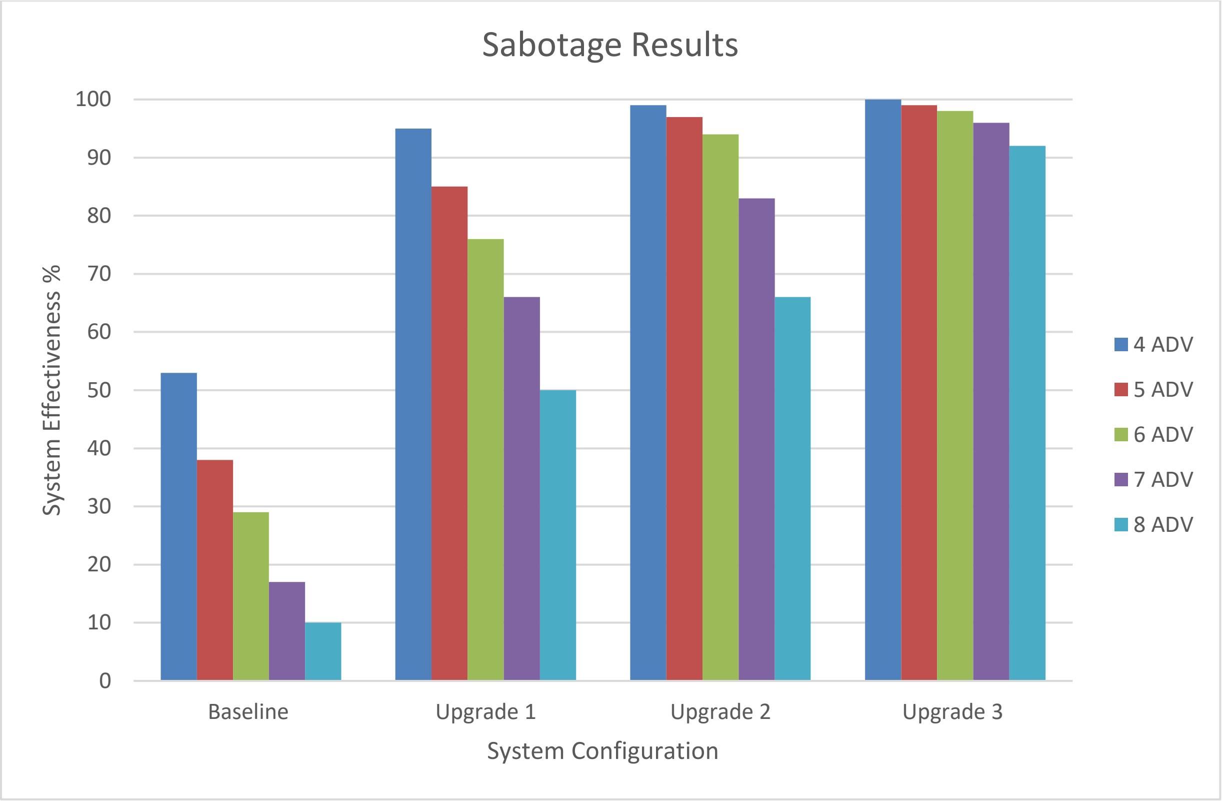


Figure 14. Baseline sabotage and upgrade configurations, probability of neutralization for 4-8 attackers

Conclusion

The baseline facility design showed a significant vulnerability to sabotage scenarios due to the rapid access to the hot cell from nearby emergency exit doors. Against only 4 attackers, the RF were only able to achieve a P_N of 53%. Performance decreased for all larger threat sizes. As a result, upgrade options were considered to produce a more robust design. The baseline theft scenarios, both with and without collusion, performed better than the sabotage scenarios for the same respective number of attackers. This was due to the longer adversary timelines, however identical upgrade options were considered as well. A finalized facility design will depend on the cost-benefit of the upgrades and design basis threat.

The following Security by Design insights were gleaned from this work:

- Underground siting extends adversary timelines not only because the adversary must travel further and through very specific pathways, but also because the adversary is limited in the size of explosive charge they can detonate underground due to the potential of facility collapse. This limitation forces the adversary to conduct multiple smaller breaches, rather than one big one, which greatly extends the attack timeline.

- Upgrades may need RF policy changes in order to see value. The initial mantrap upgrade did not show value without changes to how the RF respond. At no additional cost beyond the mantraps, changing the RF plan allowed for major improvements that worked in concert to utilize the time gained with the delay upgrades.
- For the baseline design, the PIDAS was replaced with perimeter intrusion on the building exterior walls, which helps to reduce overall security costs. However, the use of new technologies can provide greater value by extending detection range, and subsequently effective response time, without the cost of a full PIDAS.

The upgrades considered in this work to reduce vulnerability while keeping security costs low included:

- Elimination of exterior patrols (all RF are inside the building)
- Mantraps on all building exits
- Hardened fighting positions at key interior locations
- Extended detection features
- Additional RF configurations
- Additional delay barriers (anti-transit exterior barriers)
- Combinations of upgrades

The PPS modeling presented here is one of three systems level modeling capabilities that are part of the Virtual Facility Distributed Test Bed concept. These tools were used to develop, test, and iterate on a PPS design for a generic electrochemical reprocessing facility. The design would need to be further iterated for an actual facility, but the concepts presented here provide a baseline PPS design and demonstrate the value of the SSBD approach.

Keywords

Electrochemical; Security; Safeguards and Security by Design; PPS; Pyroprocessing;

Acknowledgements

This work has been supported by the Fuel Cycle Technologies program through the U.S. Department of Energy. Sandia National Laboratories is a multi-mission 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, SAND2020-8171R.

Author Biographies

Jordan Parks is a Principle Member of the Technical Staff at Sandia National Laboratories. He holds a MA in Organizational Psychology from Claremont Graduate University and BAs in Psychology and Sociology from the University of New Mexico.

Ben Cipiti is a Principle Member of the Technical Staff at Sandia National Laboratories. He holds a PhD in Nuclear Engineering from the University of Wisconsin-Madison and BS in Mechanical Engineering from Ohio University.

Ben Stromberg is a Senior Member of the Technical Staff at Sandia National Laboratories. He holds a BS in Electrical Engineering from the University of New Mexico.

Ryan Knudsen is Principle Computer Aided Design and Drafting Technologist at Sandia National Laboratories. He holds a BA in Fine Arts with a Focus in 3D Modeling from the University of New Mexico.

Todd Noel is a Senior Member of the Technical Staff at Sandia National Laboratories. He holds a BS in Computer Science from the University of New Mexico.

References

1. Garcia, M.L. 2008. Design and Evaluation of Physical Protection Systems, 2nd edition, Sandia National Laboratories.
2. NRC Regulations, Title 10, Code of Federal Regulations. 2020. https://www.nrc.gov/reading-rm/doc-collections/cfr/.
3. Maggos, L.E., Williamson, M.A., and Pereira, C. 2021. Flowsheet and Facility Design to Support Safeguards and Security by Design (SSBD) for Future Nuclear Fuel Cycle Facilities, *J. Nucl. Mater. Manage,* Vol. X, No. X.
4. Frigo, A.A., Wahlquist, D.R., and Willit, J.L. 2003. A conceptual Advanced Pyroprocess Recycle Facility. Global 2003, New Orleans, LA.
5. Burns and Roe Electrochemical Fuel Processing Design Report. 1995.
6. Blender. 2019. available at www.blender.org/about/.
7. Unity. 2019. available at unity3d.com/unity.
8. Parks, M.J. et al. 2020. Physical Security Model Development of an Electrochemical Facility. SAND2020-10051R, Sandia National Laboratories.