SAND2019-4377

SANDIA REPORT

SAND2019-
Printed May 2019

Sandia National Laboratories

Physical Security Model Development of an Electrochemical Facility

Benjamin B. Cipiti, M. Jordan Parks, Ryan Knudsen, Todd G. Noel, Tam Dang Le, and Stephen J. Stromberg.

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

Issued by Sandia National Laboratories, operated for the United States Department of Energy by National Technology & Engineering Solutions of Sandia, LLC.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@osti.gov
Online ordering: http://www.osti.gov/scitech

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Rd
Alexandria, VA 22312

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.gov
Online order: https://classic.ntis.gov/help/order-methods/

ABSTRACT

Nuclear facilities in the U.S. and around the world face increasing challenges in meeting evolving physical security requirements while keeping costs reasonable. The addition of security features after a facility has been designed and without attention to optimization (the approach of the past) can easily lead to cost overruns. Instead, security should be considered at the beginning of the design process in order to provide robust, yet efficient physical security designs. The purpose of this work is to demonstrate how modeling and simulation can be used to optimize the design of physical protection systems. A suite of tools, including Scribe3D and Blender, were used to model up a generic electrochemical reprocessing facility. Physical protection elements such as sensors, portal monitors, barriers, and guard forces were added to the model based on best practices for physical security. One outsider theft scenario was examined with 4-8 adversaries to determine security metrics. This work fits into a larger Virtual Test Bed 2020 Milestone in the Material Protection, Accounting, and Control Technologies (MPACT) program through the Department of Energy (DOE). The purpose of the milestone is to demonstrate how a series of experimental and modeling capabilities across the DOE complex provide the capabilities to demonstrate complete Safeguards and Security by Design (SSBD) for nuclear facilities.

ACKNOWLEDGEMENTS

This work was funded by the Materials Protection, Accounting, and Control Technologies (MPACT) working group as part of the Nuclear Technology Research and Development Program under the U.S. Department of Energy, Office of Nuclear Energy.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

This page left blank

EXECUTIVE SUMMARY

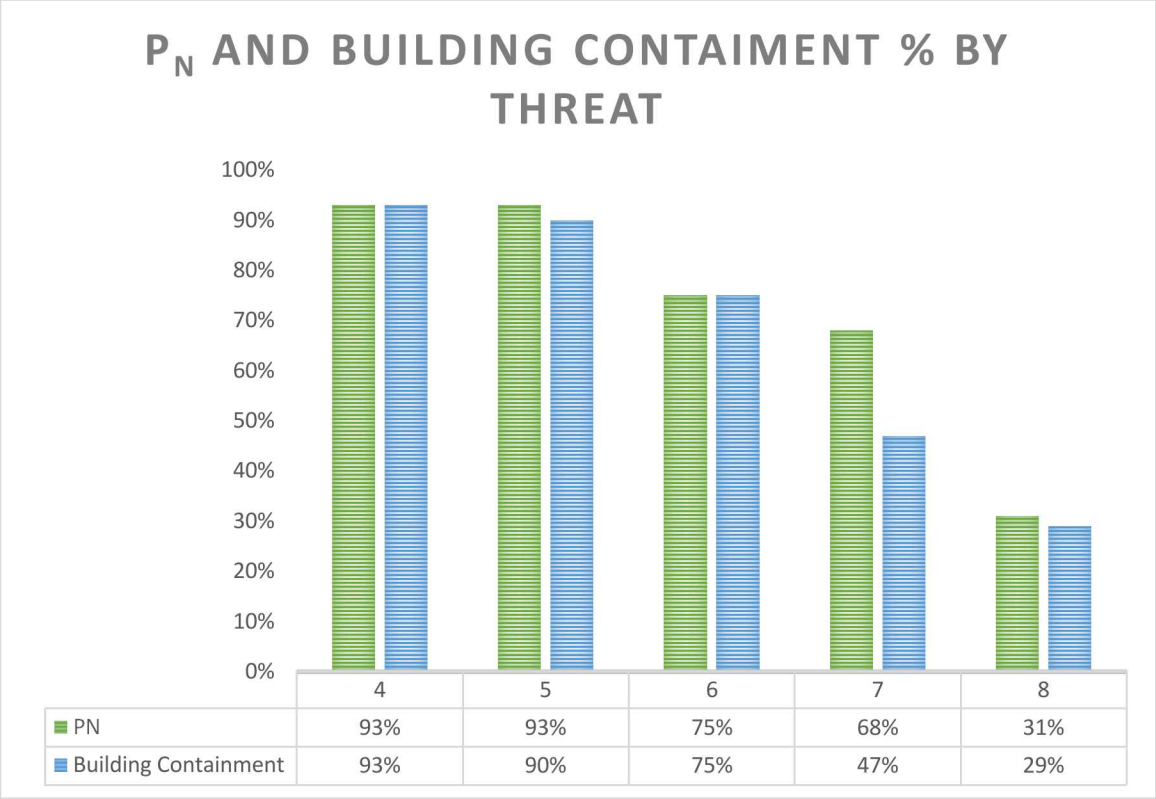
A suite of tools, including Scribe3D and Blender, were used to model up a generic electrochemical reprocessing facility (see Figure 1). This modeling capability is one aspect of a Virtual Facility Distributed Test Bed concept to demonstrate Safeguards and Security by Design (SSBD) for future nuclear facilities. The Virtual Test Bed is a 2020 Milestone in the DOE NE MPACT program. The modeling work presented here allows an analyst to optimize a security design for a new facility to avoid the high cost of retrofitting security elements to a facility after the design is complete. Physical protection elements such as sensors, portal monitors, barriers, and guard forces were added to the model based on best practices for physical security.

Given the nature of the processes within the facility, the only viable theft target is in a hardened vault within the basement of the facility. The location of the vault in the basement greatly increases the amount of time necessary to breach it. The confined nature limits the explosive weight of any adversary breaching charge, allowing responders ample time to set up facility containment.

Figure 1. Electrochemical Facility 2/3D Images

In order to understand the security performance of the system design, a vulnerability assessment was performed. Using a threat spectrum (4/5/6/7/8 adversaries), an outsider theft scenario was modelled to test the system. Utilizing a containment strategy, the response is able to keep material from being stolen from the eChem facility design 75% of the time or great for threats of six (6) or lower (see Figure 2). This is while only

maintaining a security staff of 10 responders on site, and assuming a single offsite local law enforcement agency (LLEA) team of two (2) responders in 10 minutes. General best practice is to maintain a 3-to-1 ratio between responders and design basis threat in order to secure system effectiveness. Results for threat levels higher than six (6) were 68% effectiveness at seven (7) adversaries and 31% effectiveness at eight (8) adversaries, revealing that the system fails gradually, rather than suffering a steep drop off at any single step. This is a useful data point when considering the possibility of attacks that may exceed the design basis threat. The system, as designed, overs some protection against large scale threats.



	4	5	6	7	8
PN	93%	93%	75%	68%	31%
Building Containment	93%	90%	75%	47%	29%

Figure 2. Combined Results by Threat

ACRONYMS AND DEFINITIONS

Abbreviation	Definition
ADV	Adversary
CAS	Central Alarm Station
C/S	Containment/Surveillance
DA	Destructive Analysis
ER	Electrorefiner
FP	Fission Products
IAEA	International Atomic Energy Agency
LCC	Liquid Cadmium Cathode
LLEA	Local Law Enforcement Agency
MBA	Material Balance Area
MC&A	Material Control & Accountability
MPACT	Material Protection, Accounting, and Control Technologies
MT	Metric Tons
MUF	Material Unaccounted For
NDA	Non-Destructive Analysis
NRC	Nuclear Regulatory Commission
PPS	Physical Protection System
RF	Response Force
SNF	Spent Nuclear Fuel
SSPM	Separation and Safeguards Performance Model
STAGE	Scenario Toolkit and Generation Environment
SWAT	Special Weapons and Tactics
TRU	Transuranics
U/TRU	Uranium/Transuranics

1. INTRODUCTION

Nuclear facilities in the U.S. face stringent requirements for security, particularly for facilities that process high enriched uranium or plutonium. Even for power reactors that have less attractive material, the security requirements are significant due to the concerns over theft and sabotage. This places nuclear at a disadvantage compared to other energy sources since it requires more upfront and operating costs in maintaining physical protection systems (PPS) and protective forces. Future nuclear facilities will need to incorporate Safeguards and Security by Design (SSBD) early in the design process in order to optimize these costs as much as possible.

The purpose of this work is to demonstrate how modeling and simulation can be used to quickly and efficiently design and analyze a PPS for a nuclear facility. A generic electrochemical reprocessing facility was modeled using the Scribe3D and Blender tools. The value of these types of modeling tools are that they allow a single analyst to design a PPS system and rapidly perform scenario analyses in order to optimize the design. This saves costs during the design phase and also reduces upfront and operational security costs for the facility.

The tools fully model up the facility building in 3D, along with a complete site layout. Physical protection elements are added to the models to represent portal monitors, surveillance, guard forces, locks on doors, barriers, etc. Adversary forces, both outsider and insider, can be set up for certain theft or sabotage scenarios to evaluate how the PPS design and guard forces respond. Multiple iterations are run to develop statistics for particular scenarios, and then the designs are modified until acceptable security metrics are obtained.

The modeling capability presented here is one part of a Virtual Test Bed 2020 Milestone in the MPACT program in DOE NE. The Virtual Test Bed ties together experimental and modeling capabilities across the laboratory complex to provide a one-stop-shop for SSBD. The long-term goal of this work is to provide a source for consulting when future facilities are built in order to prevent overly conservative designs and cost overruns due to safeguards and security.

In the following sections, the reference electrochemical reprocessing plant design will be described. An overview of the modeling tools is provided followed by the process building and physical security model. Finally, an outsider attack scenario is presented along with modeling results for a range of adversary numbers. This report is focused on describing the model and modeling capabilities, but the next year will focus on a more thorough scenario analysis and creation of an optimized PPS design.

2. BACKGROUND

2.1. MPACT 2020 Milestone

The MPACT campaign is working toward the goal of developing and demonstrating the next generation of Safeguards and Security by Design (SSBD) for future civilian nuclear facilities. The 2020 Milestone is developing a Virtual Facility Distributed Test Bed which ties together testing and modeling capabilities for safeguards and security analyses [1,2,3]. The demonstration is initially focused on electrochemical processing facilities, but many of the capabilities can be applied to other fuel cycle facilities.

Figure 3 shows the Virtual Test Bed Concept. There are four key systems level modeling capabilities that are used for safeguards and security analysis. Starting at the bottom and moving up, the flowsheet modeling work defines the process parameters and feeds into the above modeling capabilities. The safeguards model is built using the flowsheet and is used to design and analyze the safeguards measurements and overall safeguards system. Key metrics include overall measurement uncertainty and probability of detection of diversion or misuse. A 3D facility model is used to layout the plant design and determine batch timing—safeguards and security considerations are taken into account. The security modeling work described in this report is the last modeling component and is used to design and analyze a physical protection system. Key metrics include probability of adversary success and timeliness for various attack scenarios.

While the modeling capabilities allow for analysis of safeguards and security designs for new facilities, the models have been informed by a significant amount of experimental work as well as higher fidelity modeling capabilities. These high-fidelity capabilities are shown on the left of the figure and include the wealth of past and current work in the MPACT program on new measurement technologies, experimental data from test beds at the various national laboratories, measurements models, statistical methods, unit operation models, radiation signatures, and consequence modeling.

The overall purpose of the 2020 Milestone is to tie together all these capabilities more to provide a one-stop shop for SSBD. For example, if a future reprocessing facility were to be built and had unique features, the modeling capabilities would work together to help the vendor optimize the facility, safeguards, and security system design. If specific materials accountancy challenges are identified, one of the laboratory test beds may be used to develop a measurement system that will work under operating conditions. The latest developments in measurements, sensors, and data analytics would be applied to provide designs that meet regulatory requirements in a cost-effective manner.

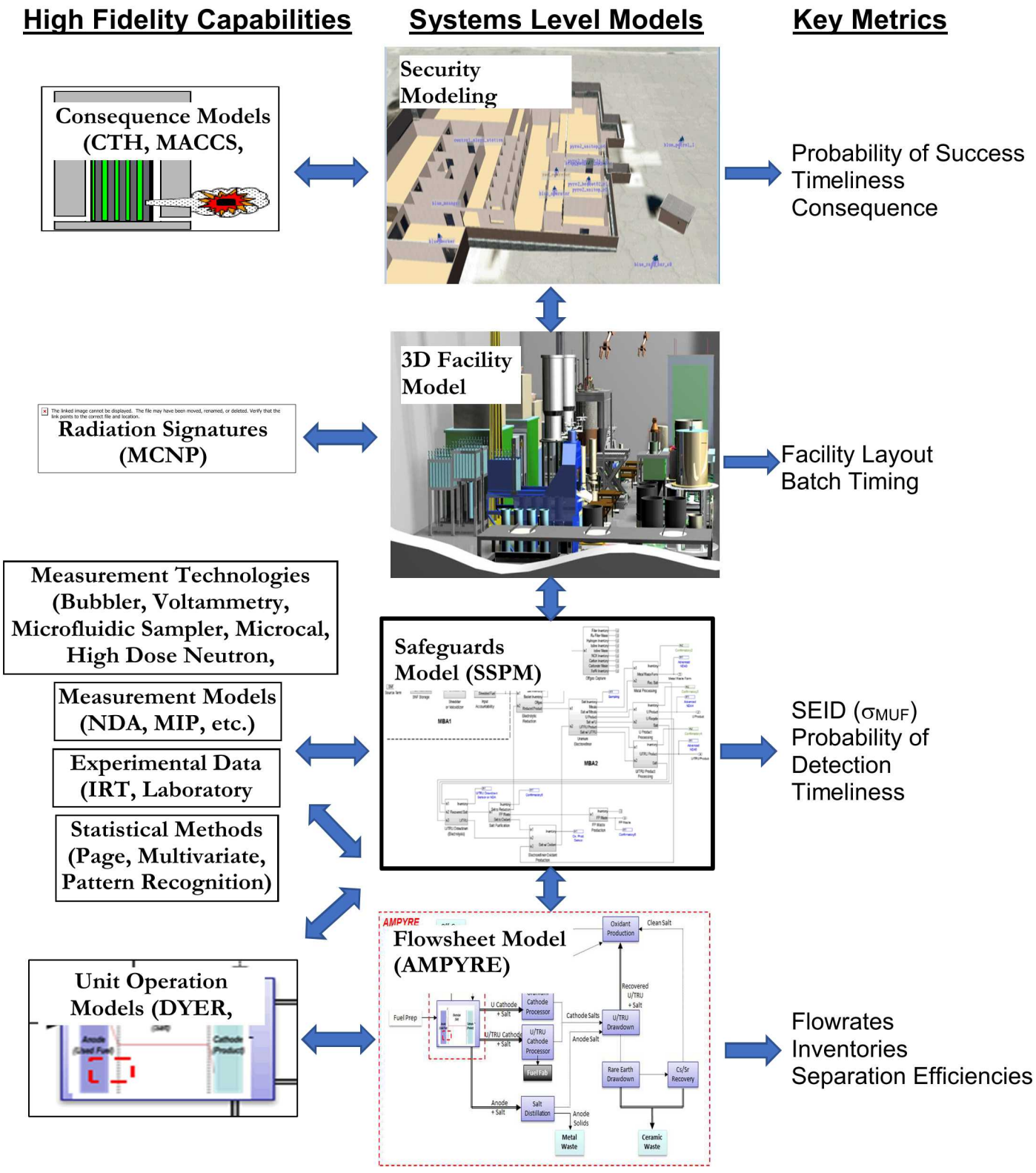


Figure 3. Virtual Facility Distributed Test Bed

The focus of the security modeling (described in this report) in 2018-2019 has been to develop a physical security model of a generic electrochemical processing facility. This model is based on the generic flowsheet and safeguards model. Preliminary security designs have been implemented and tested against example attack scenarios. For the rest of 2019 and moving into 2020, the analyses will be formalized more to develop an optimal security design and provide the results of the analysis against a variety of attack scenarios.

2.2. Electrochemical Facility Design References

The generic electrochemical facility design was based on references 4 and 5. Reference 4 provided a high level summary of more detailed design work at Argonne National Laboratory. This reference provided a layout of facility operations in the hot cell along with a 3D rendering of the building design. Reference 5 is a much more detailed electrochemical fuel processing design report. It provides more detail on the building layout and unit operations. These two references were used to extrapolate a facility model and overall site layout. Subject matter experts in both electrochemical operations and security system design provided input into the generic design that was developed here.

The electrochemical facility is based on the flowsheet that is currently being used to support the MPACT 2020 Milestone. The overall flowsheet is shown in Figure 4. The process begins with receipt and storage of spent fuel. Typically fuel assemblies are delivered via rail and transferred underground into the hot cells for processing. An electrochemical process is performed in a hot cell using manipulators. The process is broken up into an air cell and an argon cell.

Front end operations, such as decladding, fuel chopping, possibly voloxidation, and input accountancy can be done in an air atmosphere hot cell. The reference flowsheet assumes that spent fuel is shredded and loaded in baskets. The baskets are thin and porous to allow increased surface area during contact with the molten salts. After the fuel is loaded in baskets, the baskets are transferred into an argon hot cell for processing. The molten salt chemistry of the hot cell requires an argon atmosphere.

All electrochemical extractions, distillation of the products, fission product removal, and product processing is performed in the argon hot cell. The extraction processes remove uranium in a mostly pure form along with a mixed uranium and transuranic (U/TRU) product. Fission products are removed through continuous processing of the recycle salt. In addition to the U and U/TRU products, the process also produces a metal waste and one or more fission products wastes (depending on the design).

From a security perspective, there are advantages to the requirement of thick walls for shielding and the argon atmosphere. These design features provide additional barriers to theft. Material is usually transferred through underground tunnels, and the U/TRU products are stored in an underground vault. Because the processing operations are isolated in a single building, it is possible to use the building exterior for perimeter intrusion detection instead of building a larger and costly Perimeter Intrusion and Detection and Assessment System (PIDAS).

Section 3 describes the processing building and facility layout in more detail. Some aspects of the building are estimations since a full plant design was not available. Attention was focused on the geometry of the building to make sure that spacing is self-consistent. (For example, realistic spacing in hallways and stairwells is required so that the modeling of attacker and guard movement is correct.) Best practices for the location of PPS elements were used.

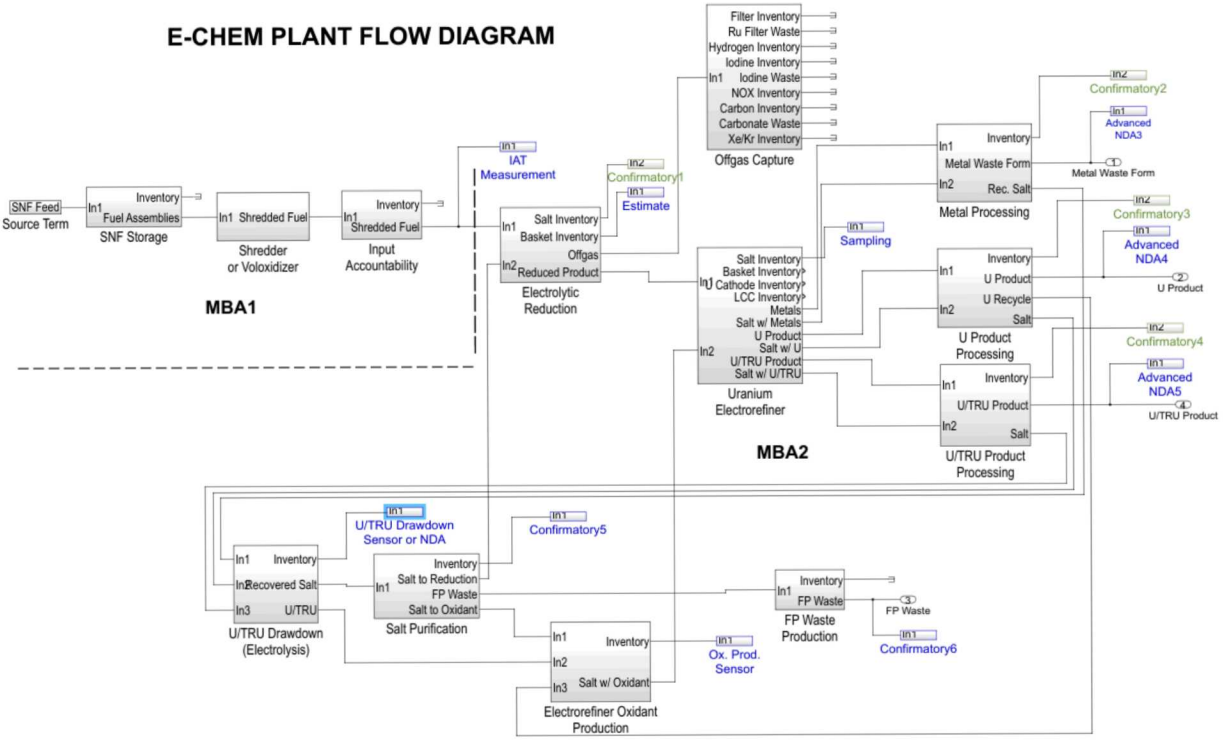


Figure 4. Electrochemical Flowsheet [6]

3. OVERVIEW OF VULNERABILITY ASSESSMENT

The evaluation of an existing or proposed Physical Protection System (PPS) requires a methodical approach in which the ability of the security system to meet defined protection objectives is measured. Without this kind of careful assessment, valuable resources might be wasted on unnecessary protection or, worse yet, fail to provide adequate protection of material against a theft attack by the defined threat. The Vulnerability Assessment (VA) methodology was developed to implement performance-based physical security concepts at nuclear sites and facilities.

The measure of overall security effectiveness is described as system effectiveness and expressed as a probability, P_E. P_E is determined using two terms: the probability of interruption (P_I) and the probability of neutralization (P_N). Analysis techniques are based on the use of adversary paths, which assume that a sequence of adversary actions is required to complete an attack on an asset. It is important to note that P_E will vary with the threat. As the threat capability increases, performance of individual security elements or the system as a whole will decrease.

Interruption is defined as the probability of arrival by the security force at a deployed location to halt adversary progress. Interruption may lead to the initiation of a combat event; however, it does not mean that the task has been literally interrupted, simply that security forces have arrived before completion of the adversary task.

Neutralization is defined as the defeat of the adversaries by the security forces in a combat engagement or by other means. P_N is a measure of the likelihood that the security force will be successful in overpowering or defeating the adversary given interruption. This defeat could take many forms; it could mean the adversaries are rendered task incapable because a vital vehicle is disabled or key personnel are neutralized. It could mean that all adversaries are neutralized. Neutralization is simply the ability of the security force to prevent the adversary from completing its mission.

These probabilities are treated as independent variables when the defined threat:

1. Selects a path that exploits vulnerabilities in the system and
2. Is willing to use violence against the security forces.

In this case, the effectiveness of the system (P_E) against violent adversaries, expressed as the probability of interrupting and neutralizing the adversaries, is calculated by the following formula:

$$P_E = P_I x P_N$$

It is important to stress the conditional probability. Interruption (P_I) is meaningless without neutralization (P_N). If a system has a very high probability of interruption but lacks the firepower to respond to the given threat, then the system fails. Conversely, if the system

lacks the timely detection to get responders to the fight, it does not matter how well staffed and armed the response is.

3.1. Modeling Tools

3.1.1. STAGE

STAGE is used to assist in the determination of the P_N of the existing (baseline) facility along specific paths outlined in the path analysis section. STAGE is a virtual simulation software that models a facility and its PPS under adversary attack in 3D. The model uses artificial intelligence along with detailed information about a facility's buildings, utilities, and landscape; PPS performance characteristics; and tactics and weapons for both the adversary and the RF.

STAGE simulations concentrate on an adversary sabotage scenario, which takes into account the varying tactics and configuration of response forces. Typically a Design Basis Threat is used to define the adversary capabilities and attributes, but for this work the adversary definition is parametric.

In previous analysis, STAGE was used to assist in the determination of the P_N of the facility. However, STAGE proved to be overly complex, labor intensive, and time consuming for simple neutralization analysis. Therefore, neutralization analysis was performed in Scribe3D©, which lacks complex behavioral logic, but is much easier to implement. Models are created in Blender. Then the models are used in Scribe3D© to create scenarios, conduct table-top exercises, and collect neutralization data.

3.1.2. Blender

Blender [7] is a free and open source 3D creation suite that is widely used throughout the 3D modeling community. It supports the entirety of the 3D pipeline and 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. For this project, Blender was used to create the facility 3D model.

3.1.3. Scribe3D© – Table Top Recorder and Automated Tabletop Data Tool

Scribe3D© is a 3D tabletop recording and scenario visualization software, created by Sandia National Laboratories. It was developed using the Unity [8] game engine for use by other National Laboratories, government organizations, and international partners. Unity is a commercial game engine built for developers and non-developers to create a wide variety of games and applications. It features a fully customizable framework and set of development tools. Unity was used to build Scribe3D© and many other training and analysis tools within the DOE complex.

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. The tools offered by Scribe 3D can help open discussions and capture their results, visualize consequences, collect data, and record events, as well as help make decisions while users develop scenarios. Data can be viewed in 2D or 3D and be played back in real-time or at various speeds. 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 fashion to collect large quantities of data for analysis purposes, after initial scenarios are defined in the traditional tabletop exercise.

3.2. System Effectiveness Analysis Assumptions

The vulnerability assessment process uses the following assumptions:

- Pathways are determined using table-top analysis and SME judgement.
- The target areas and operational states are all accurately identified.
- Adversary acts are planned and executed at a time that provides maximum opportunity for success for the adversary.
- Facility security features function as designed, and RF respond as defined.
- Appropriate threat attributes and capabilities are identified.
- Current protection strategies evaluated in this analysis are assumed.
- When data are limited or missing and the analyst must rely on subjective expert opinion, the analysis is conducted conservatively, with the advantage weighted toward the adversary.
- Adversaries and response force are assumed to be equal with regard to training and combat ability.
- Adversaries are willing to die to achieve their mission.
- Only theft scenarios are analyzed.
- RF strategy is containment only.

4. ELECTROCHEMICAL FACILITY DESIGN AND SECURITY ANALYSIS

For the notional Electrochemical (EChem) facility a baseline operational state was studied. This baseline state of the standard physical protection system includes intrusion detection, assessment, access control to restricted areas, and on-site response.

The electrochemical processing building is protected by a robust physical protection system designed to stop outsider attacks. The facility consists of three floors. The main processing floor sits at ground level and is where most facility activity occurs. The main floor includes shipping and receiving and the main electrochemical processing unit operations which are contained within two hot cells. This floor is supported by the basement level, which mainly consists of shielded pass throughs for which material travels into and out the process cell. The basement also contains a vault for the U/TRU product until it is shipped. (This generic plant design assumes that the final product is a U/TRU ingot that would be sent to another facility for fuel fabrication.) The top floor allows for maintenance and repair of any equipment from the process cell. Additional rooms are located throughout the facility to support various day to day operations.

4.1. Processing Level

The main processing level includes the highbay for shipping and receiving, air and argon hotcells, control room, entry control point, and central alarm station. Additional rooms are included to support various facility needs (office space, locker rooms, meeting rooms, etc.) Figure 5 shows an overhead view of the main processing level, and Figure 6 shows the 3D view.

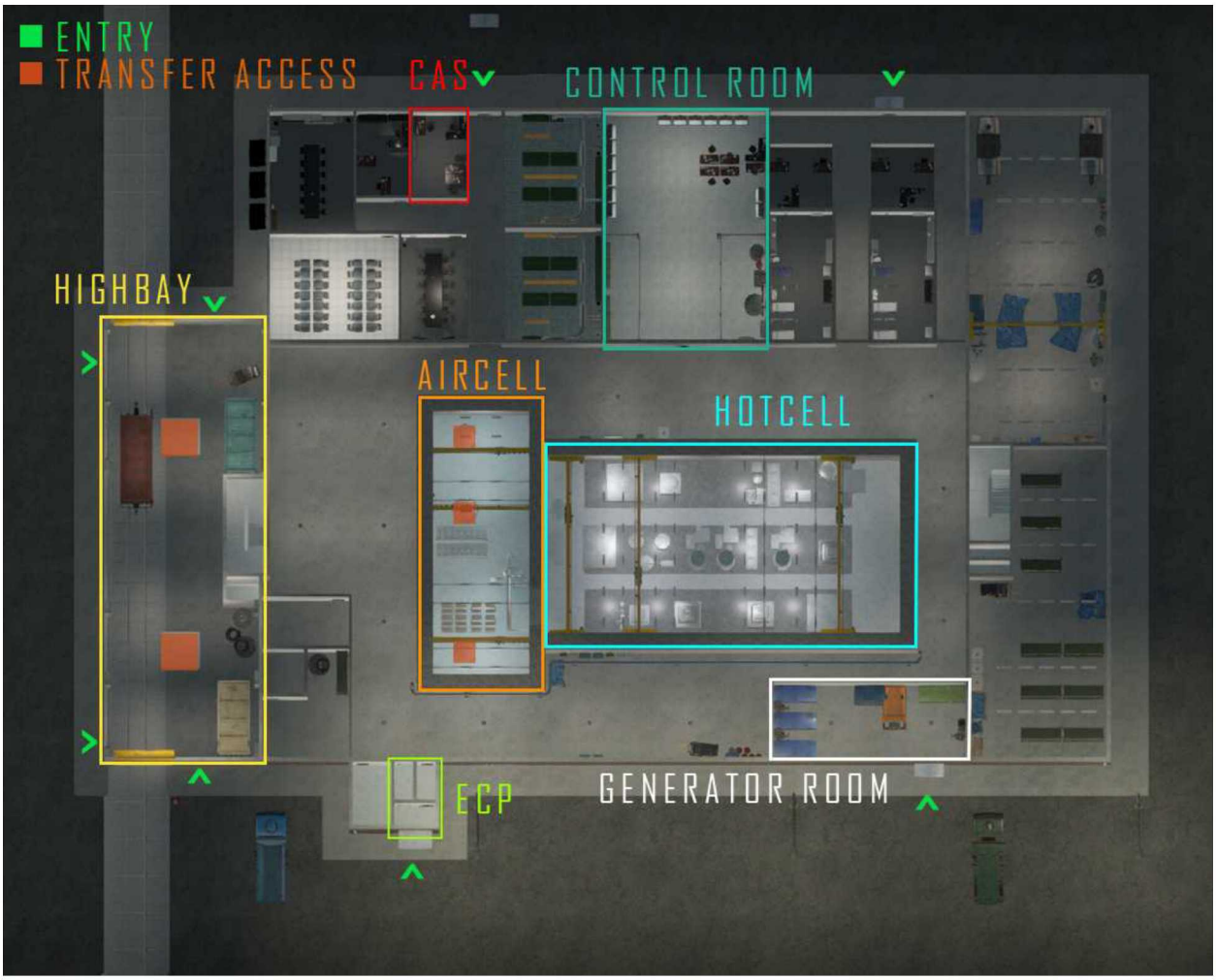


Figure 5. Processing Level facility overview

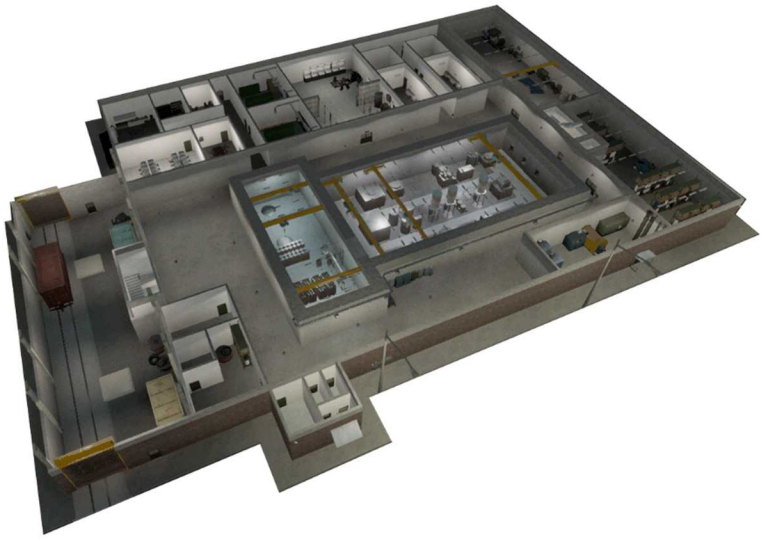


Figure 6. Processing Level facility 3D Model – Blender Screenshot

4.1.1. High-Bay

The high bay area (see Figure 7) serves as the transfer point for material entering and exiting the facility. It features rail entry through large roll-up doors and contains a large gantry crane for unloading fuel rods from incoming rail casks. The floor of the facility features two pass-through hatches into the below-grade material transfer tunnel. One hatch is used to move material into the facility, while the other hatch is used to remove final products as well as waste products from the facility.

The high bay will provide the following functions:

- Provide an enclosed area that transportation carriers and casks, either rail or legal weight truck, can be moved into in preparation for unloading and loading.
- Provide an overhead crane for unloading the cask from the transport carrier and moving the cask to the receiving transfer cart or shipping transfer cart.
- Provide temporary protection around the transportation casks during loading and unloading.

Figure 7. High Bay Area

4.1.2. Air Cell/Hot Cell

The air cell is a shielded hot cell with an air atmosphere that is used for front end operations. Spent fuel assemblies are transferred into the air cell from the high bay area through the underground passage. The air cell contains a storage location for spent fuel assemblies. Once processing begins, the assembly hardware is removed, and the fuel is

chopped or shredded and loaded into thin, porous metal baskets which will be used for electrorefining operations. At some point while in the air cell, the spent fuel will be measured for input accountancy. The details of that measurement are not worked out yet.

Once the baskets are loaded and input accountancy measurements are complete, the baskets are transferred into an argon atmosphere hot cell for the electrorefining separation process. Oxide reduction, electrochemical separations, cathode processing, and product and waste processing are all performed in this location. The final products of the process include uranium ingots, U/TRU ingots, metal waste forms, and one or more fission product waste forms. The U/TRU product is stored in the basement level, and the rest of the products/wastes would be shipped out of the facility for waste storage. Figure 8 shows an overhead view of the hot cells and an internal view of the air cell (upper left) and argon cell (upper right).

Figure 8. Air and Argon Hot Cells

4.1.3. Control Room

The control room (see Figure 9) contains the operating consoles for the hot cell and air cell. It also houses high voltage components, safety system controls, and critical diagnostic equipment. Large scale electrochemical plants do not exist currently, but it is likely that they would automate operations as much as possible. Current research-scale operations utilize manipulators and operators to carry out electrorefining operations. Some level of operator-run manipulators will probably still be required, but most of the process will be automated if possible.

Figure 9. Control Room

4.1.4. Central Alarm Station/Guard Force Staging Area/Entry Control Point

The Central Alarm Station (CAS) contains the alarm control and display system (AC&D). All alarms and camera feeds are monitored here. A two-person response force team is stationed in the staging area 24/7 along with a single CAS operator. As will be described later, a total of ten responders are assumed to be on site at any time (see Section 5).

The personnel entry control point (ECP) allows for processing personnel in and out of the facility. Two responders are stationed here as well. The ECP features ingress and egress "man-traps", which consist of a set of hardened doors. Once inside the man-trap, personnel present credentials, and only once verified, are allowed entry or exit. Ingress traffic is checked for metal via metal detection portal. Egress traffic is checked for special nuclear material (SNM). Figure 10 shows both the CAS and the ECP, and the ECP security layout is captured in Figure 11.

Figure 10. CAS (left) and ECP (right)

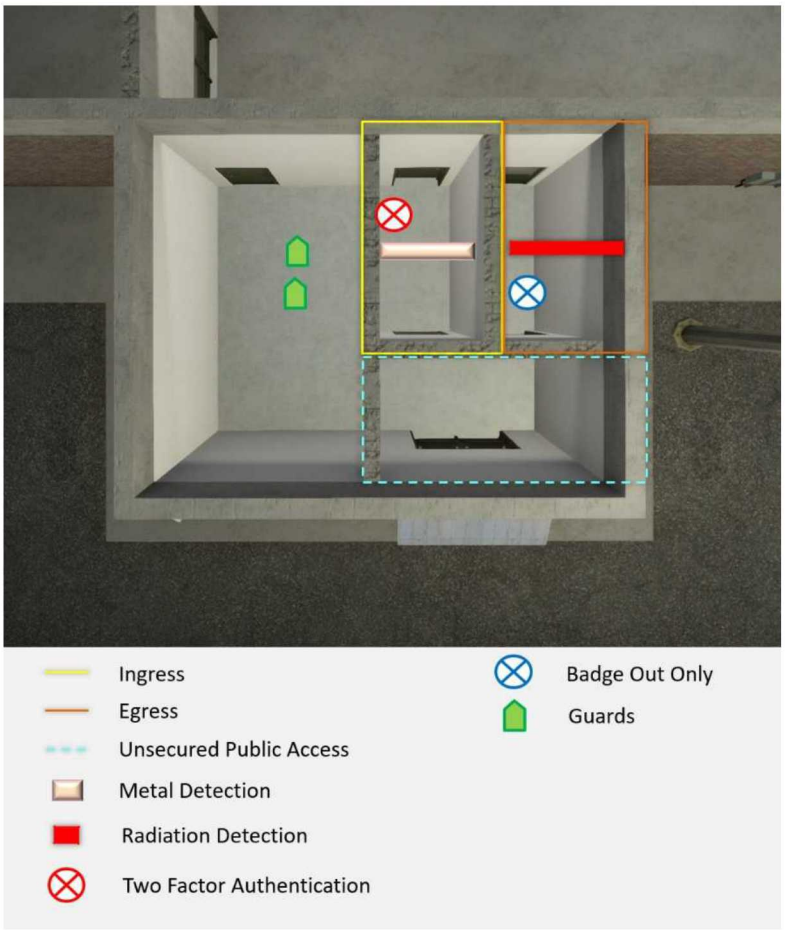


Figure 11. ECP Security Layout

4.1.5. Server Room/Warehouse/Storage/Machine Shop

Other facilities included on the processing floor are the server room, warehouse, machine shop, and storage areas. Figure 1 shows a few of these rooms. Other rooms include office space, conference rooms, locker rooms, etc. These areas support the main functions of the facility and are generally of low security concern.

Figure 12. Warehouse (left), Machine Shop (upper right), and Server Room (lower right)

4.2. Basement Level

The basement of the facility mainly contains the transfer tunnels to move material from one location to another and the U/TRU vault for storage of the key product. Other rooms may be required for access below the hot cell, though specific functions are not called out. Figure 13 shows an overview of the basement, and Figure 14 shows a 3D view.

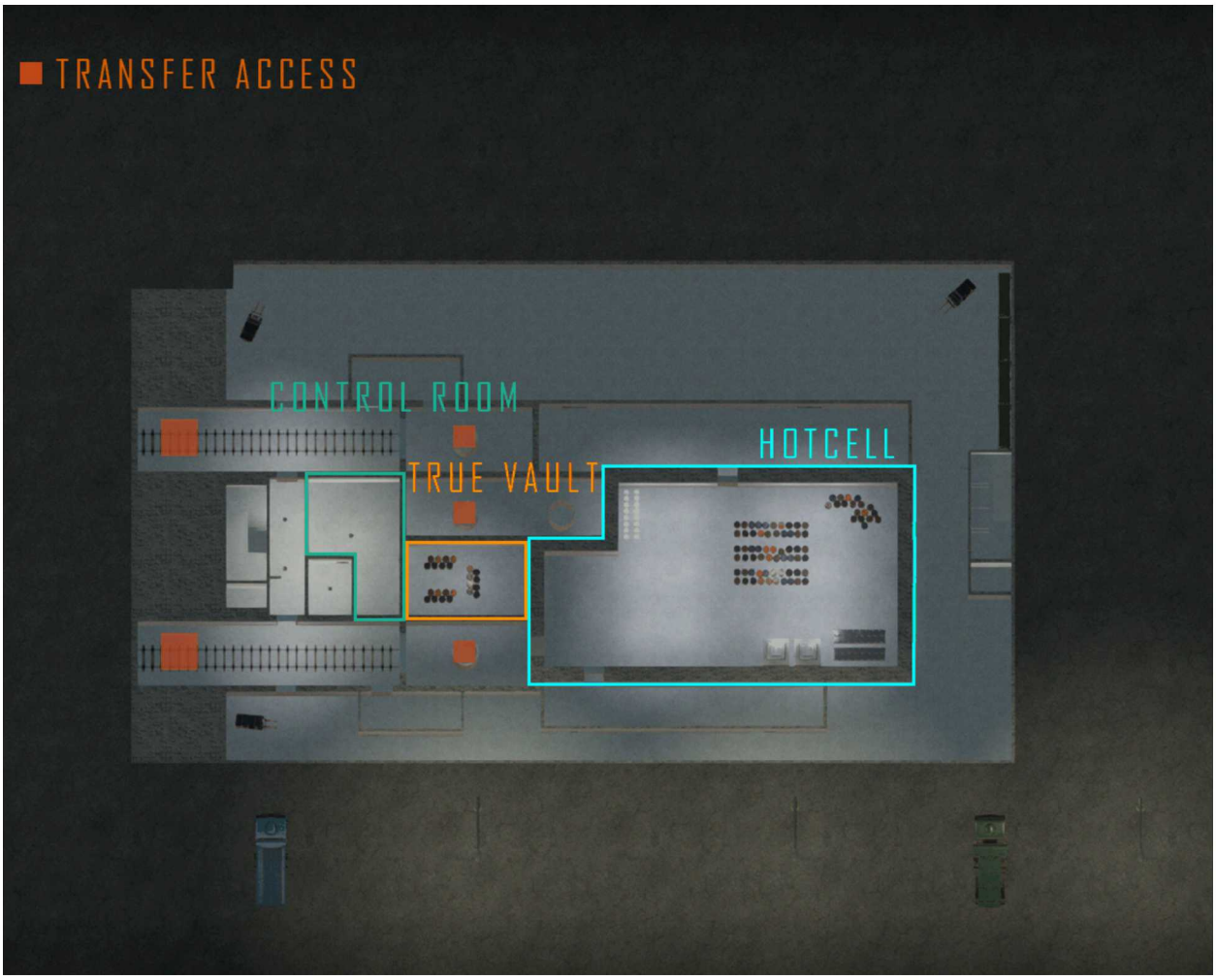


Figure 13. Basement Level Facility Overview

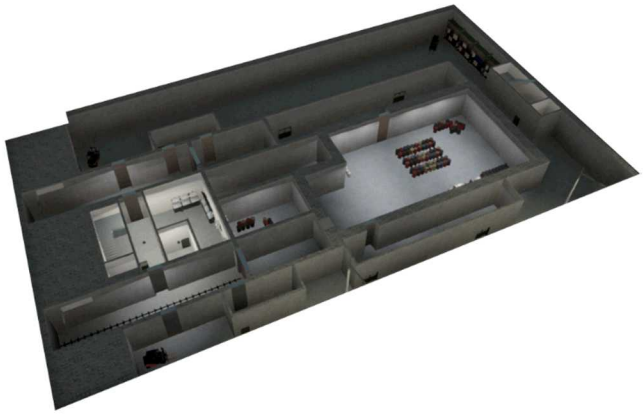


Figure 14. Basement Level 3D Model

4.2.1. U/TRU Vault and Vault Control Room

The U/TRU Vault is where finished products are stored, awaiting transport off site. It is one of the main target areas of concern for the facility since the U/TRU material has the most attractiveness. The only other location of U/TRU material is in the hot cell which is very difficult to access. The U/TRU vault control room shares an adjacent wall and contains the controls and manipulators to move products into and out of the vault for storage and transport. The U/TRU ingots from the process cell would be transferred through the underground hatches into the vault.

Figure 15. U/TRU Vault (right) and Vault Control Room (left)

4.2.2. Subcell Transfer Tunnels

The transfer tunnels provide shielded transfer from the high-bay to the air cell, hot cell, and U/TRU vault. They allow material to move both into and out of the facility. The exact design of these are not specified. Large, heavy transfers (like spent fuel assemblies) will likely be placed on some type of cart and travel via rail. Other materials may move through a different mechanism. Figure 16 shows pictures of the basement area (left) and transfer tunnel (right).

Figure 16. Basement Transfer Tunnels

4.3. Top Floor – Process Cell Equipment Service Floor

The equipment service floor serves as a maintenance level for the process and air cells. New equipment is tested and qualified prior to installation, and hot equipment is serviced or decontaminated or prepared to be disposed as a waste. Figure 17 shows a top level view of the top floor, and Figure 18 shows a 3D view.

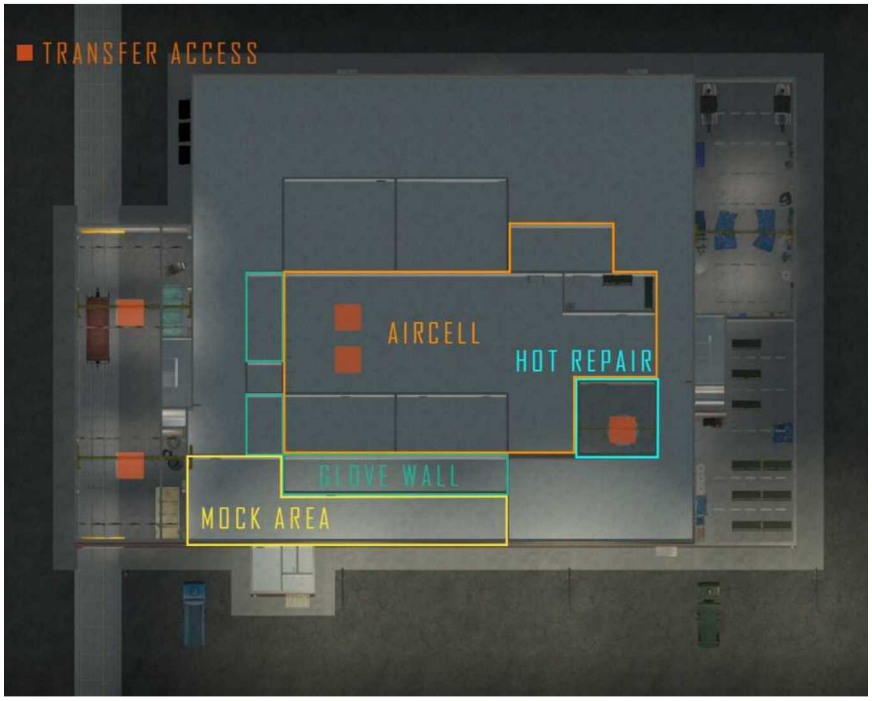


Figure 17. Top Level facility overview

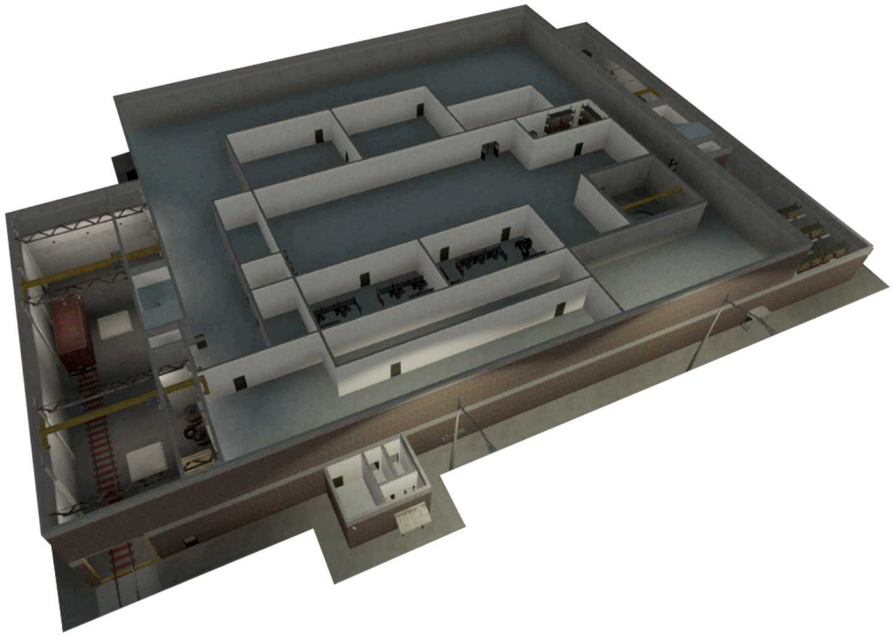


Figure 18. Top Level 3D Model

4.3.1. Hot Repair/Glovewall/Mock-Up Areas/Secondary Alarm Station

Located above the process cells, the functions of the hot repair area will be to provide decontamination, repair and maintenance capabilities for the in-cell equipment and modules. The glovewall area is used for hot maintenance of process cell equipment as well. The mock-up area is used for testing, and qualification of new equipment as well as in preparation of installation within the process cell. The secondary alarm station is also located on the equipment maintenance level. It serves as a back-up for alarm monitoring, features a reduced CAS, and also houses two response force personnel. Figure 19 shows the hot repair area with transfer hatch.

Figure 19. Hot Repair Area

4.4. Facility Physical Security System

In order for the path analyzed to be valid given the lack of a perimeter intrusion detection and assessment system (PIDAS), it is assumed that the facility walls are equipped with seismic sensors to detect attempts at penetration, and has dedicated cameras to assess alarms from said sensors. The skin of the building is the first protection layer since the adversary could breach the walls to avoid being detected by the BMSs on the doors. It is assumed that each of the doors breached along the adversary path is equipped with a balanced magnetic switch (BMS) to detect unauthorized entry. This sensor is assumed to have a detection probability no less than 80%. In the material inspection area, it is assumed there is a dual-tech volumetric sensor which features a probability of detection no less than 90%.

4.4.1. Perimeter Physical Security System

The processing facility features a single passive fence for limiting public assess only. It has no sensors or detection. The skin of the building features seismic vibration sensors designed to detect breaching of the building walls. Each wall of the facility features at least one dedicated assessment camera tied to the seismic sensors for that wall section and/or the respective emergency exit doors. The entry control point is the only authorized personnel entry point. The facility features several emergency exits for personnel. These all feature magnetic locks and balanced magnetic switches.

One of the key aspects of Security by Design is to optimize security systems as much as possible while still providing a robust protection from theft and sabotage. The typical use of a two-fence Perimeter Intrusion Detection and Assessment System (PIDAS) is likely not needed since all the material of concern is located inside one building. The building exterior acts as a the PIDAS. This approach also takes into account the fact that the thick shield walls of the hot cell, basement, and vault areas along with the high radiation environment and argon atmosphere make it difficult for an adversary to access these areas.

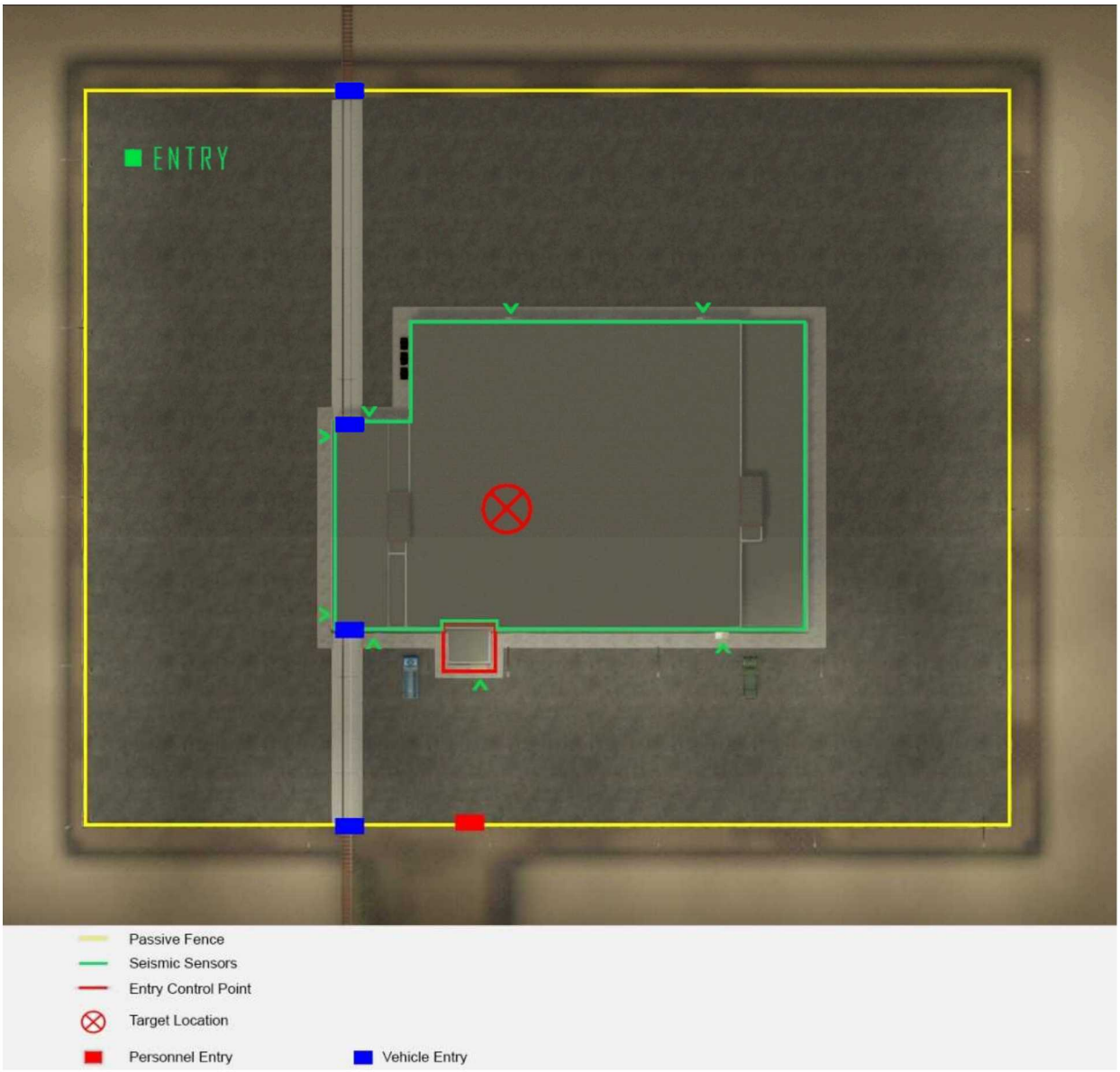


Figure 20. Building Exterior Security Features

4.4.2. Entry Control Point

The Entry Control Point is the only authorized site entrance/exit under normal conditions. It includes a person-on-duty room and a mantrap for personnel passage.

For authorized access to the site, the ECP is equipped with a mantrap, formed by two metal doors and ECP walls. The ECP exterior door is equipped with a balanced magnetic switch and a remote-controlled lock. The inner mantrap door is equipped with balanced magnetic switch and remote-controlled lock with door closing device, a proximity card reader and PIN pad for entry and a PIN pad for exit.

To detect the presence of metal items and radioactive substances, a personal portal monitor is installed in the mantrap. In special circumstances, personnel can be checked with handheld metal detectors, explosive detectors, and SNM detectors.

4.4.3. Facility Interior Security System Design

The interior physical security system for the processing level is characterized in Figure 21. As mentioned above, all exterior doors are protected with magnetic locks and balanced magnetic switches and are assessed by dedicated camera systems. Interior doors which lead to protected areas are also protected in the same way. Doors leading into the stairwells are protected as well.

The interior physical security system for the basement level is characterized in Figure 22. Doors leading from the stairwell and into the TRU control room are protected with magnetic locks and balanced magnetic switches and are assessed by dedicated camera systems. The door leading directly into the control room is protected by a GSA Class 5 Vault door for increased security.

The interior physical security system for the equipment processing level is characterized in Figure 23. Main areas of concern are the SAS/Response force room. Other sensitive areas are the hot maintenance area due to safety concerns.

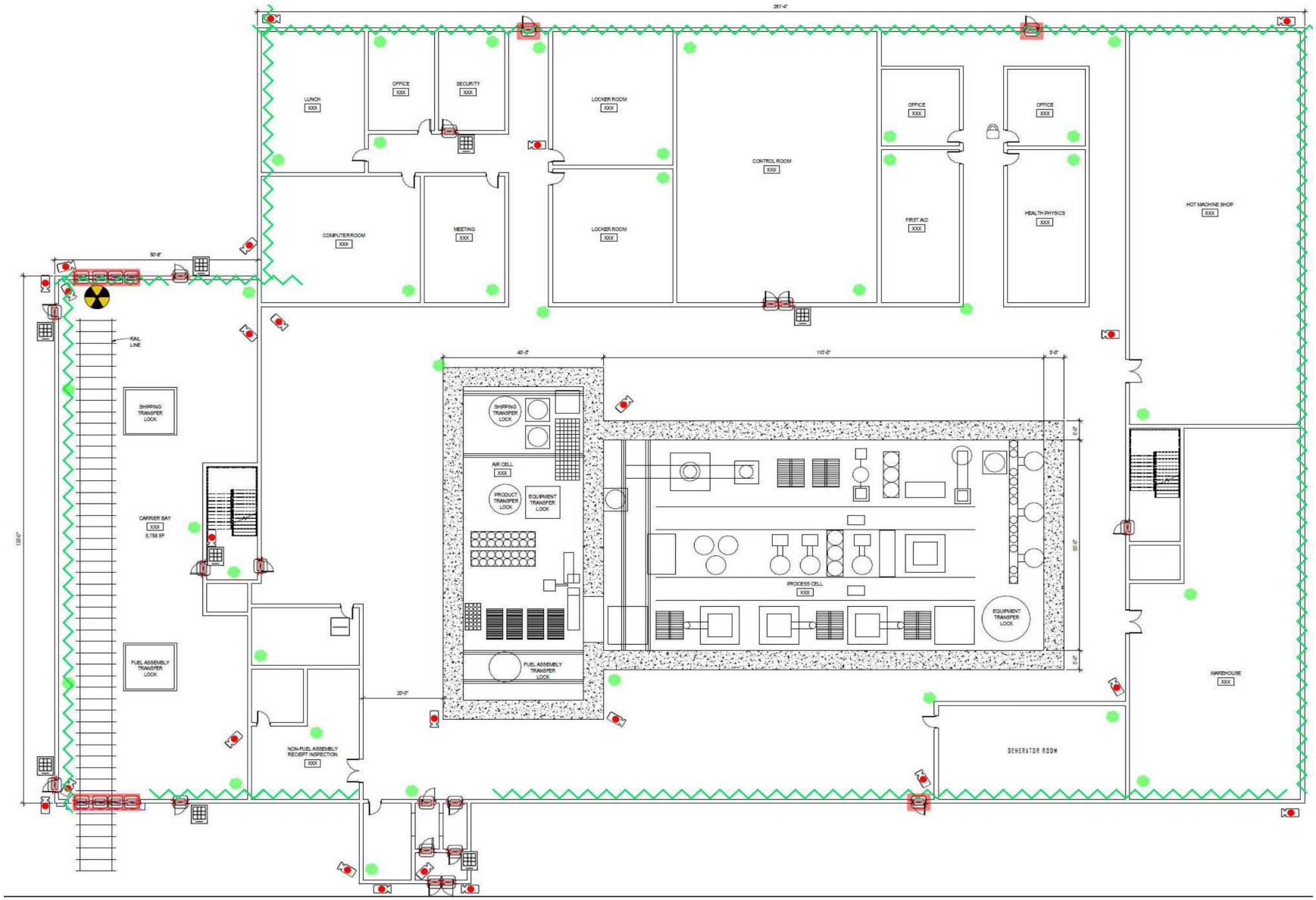


Figure 21. EChem Processing Building, Operating Floor Level, and Conceptual PPS Design Layout

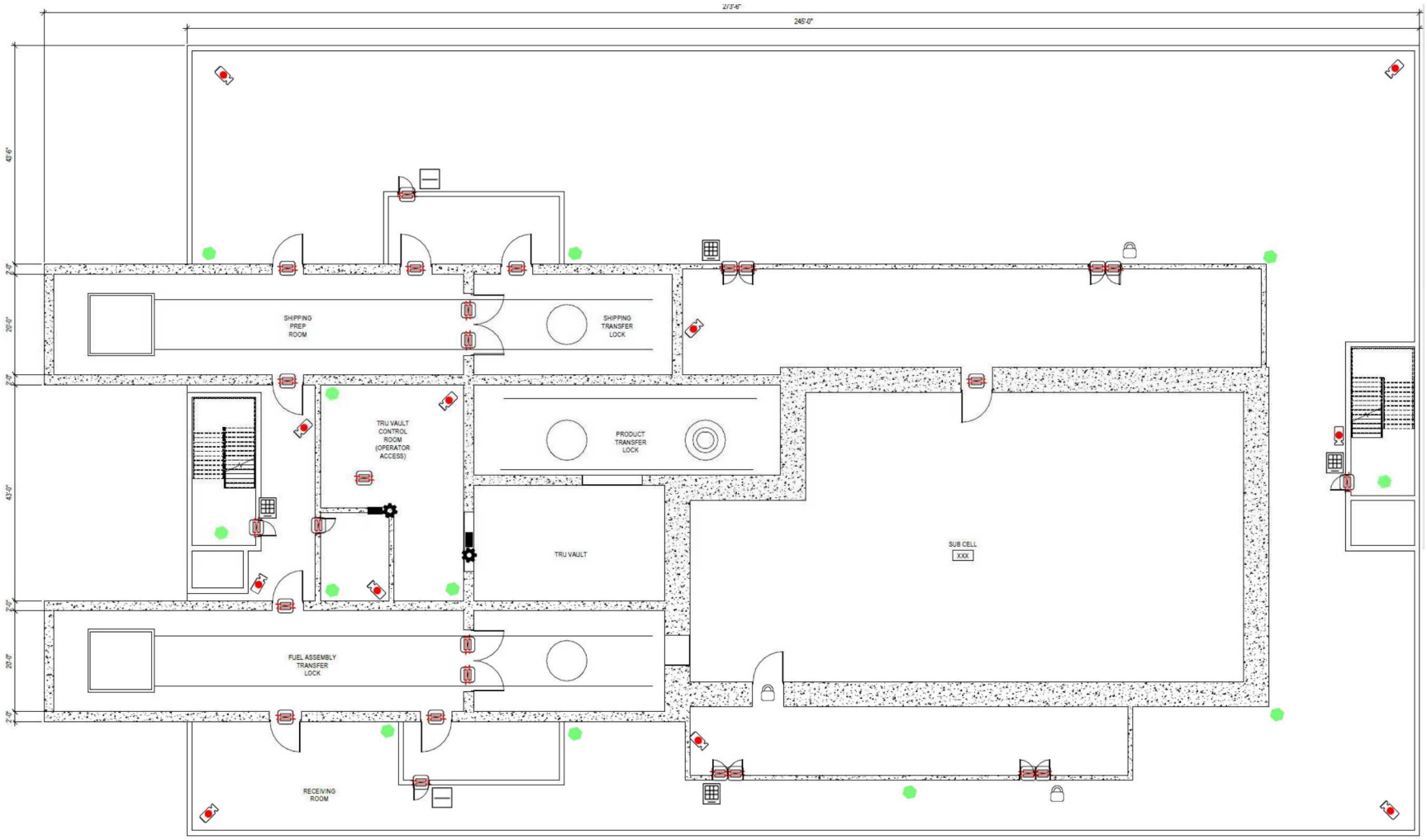


Figure 22: EChem Processing Building, Basement Level, and Conceptual PPS Design Layout

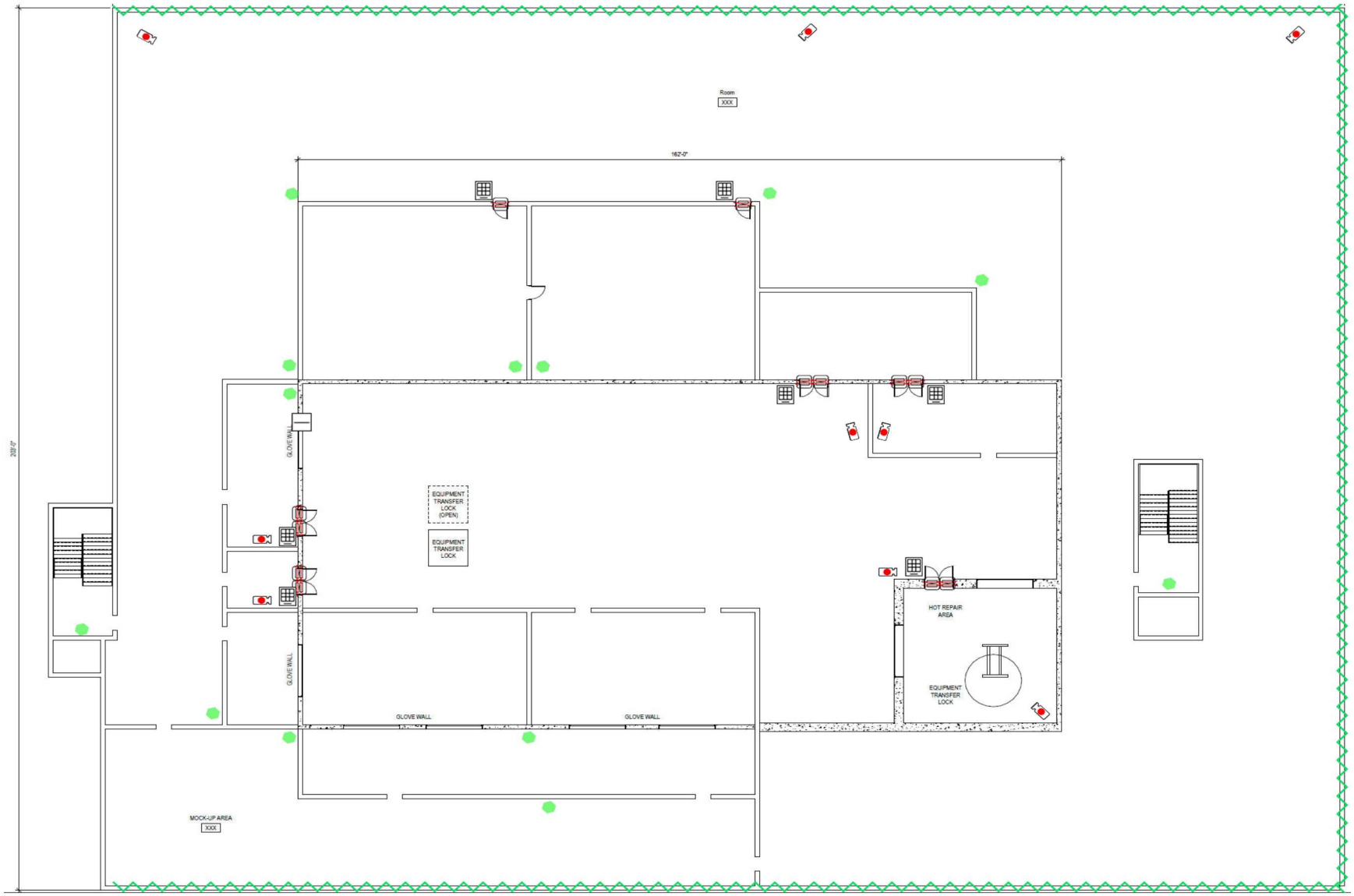


Figure 23: EChem Processing Building, Hot Repair Area Level, and Conceptual PPS Design Layout Icons

Table 1. Detail and Legend for Figure 21 through Figure 23

Sub-Task	System/ Comp Type	Description / Requirement	Team Notes
Outer Building Perimeter			
1.	Intrusion Detection System 	**Balanced Magnetic Switch (BMS)** Install a high security triple-biased BMS on the secure side of the door.	BMS alarms shall annunciate as: Door Held (after 30 seconds) and Door Forced (immediately); and each door alarm shall indicate its specific location.
2.	Intrusion Detection 	**Dual Tech Sensors** Installed in interior hallways and vault areas,	Will be placed in access during operations.
3.	Intrusion Detection 	**Active Infrared** Placed at all emergency exit doors as well as transport area roll up doors.	
4.	Intrusion Detection System 	**Emergency Exit (EMX) / Door Exit Camera** • Install a camera covering the emergency exit (EMX) doors, on the exterior side of the EMX doors as indicated; use a wide-angle lens to capture as much of the portal as possible in the field of view (FOV).	Camera images shall be used for 15-second pre/post assessment of alarm event.
5.	Access Control System 	**Card Swipe Access Control** Install card swipe access controls for personnel door for building entrance. • Card swipe access control will only allow entrance for personnel cleared to enter facility per the access list.	

Sub-Task	System/ Comp Type	Description / Requirement	Team Notes
6.	Seismic Sensors 	**Embedded Seismic Sensors in Exterior Walls** • Detect penetration of wall surfaces	
7.	Contraband Detection System 	**Radiation Sensor** Install an area gamma radiation sensor above and near the rail exit, for security purposes, to provide indication of illicit removal of nuclear fuel material. • Sensor shall indicate an alarm if the background dose rate increases above a threshold security limit (not safety). • The sensor shall be located within the field of view (FOV) of an existing assessment camera. If possible, the sensor shall be programmed to report radiation level readings to the CAS (preferred), or to another location (such as the director's computer) at the time of an alarm.	
8.		GSA Class 5 Vault Door or equivalent • High security reinforced Vault Door	
9.	Access Control System	**Personnel Turnstile** Install a one-way turnstile for the entry and exit portals. Both turnstiles will be locked: Upon entry, the entry turnstile will be unlocked by a	

Sub-Task	System/ Comp Type	Description / Requirement	Team Notes
		successful/accepted Card Swipe; On exit, the turnstile will unlock if no radiation or metal detector sensor activates.	
10.	Access Control System 	**Card Swipe Access Control** Install card swipe access controls for personnel door for building entrance. Card swipe access control will only allow entrance for personnel cleared to enter facility per the access list.	
11.	Access Control System 	**Card Swipe and Keypad Access Control** Install card swipe and keypad (i.e., proximity/swipe card reader, and PIN with silent duress code capability) at the Entry Control door of the facility. Install audible door held-open warning buzzer/toner. • Silent duress alarms shall annunciate as: Duress; and shall annunciate the specific location of the duress alarm.	

5. TARGET CHARACTERIZATION

The U/TRU product was found to be most attractive. Normally, U/TRU is most vulnerable to theft during shipping, which is why compensatory measures are in place during transfer of U/TRU ingots from the TRU Vault to the loading dock at the Waste Storage Facility. Although U/TRU also exists in the hot cell, the thick walls, difficult material handling forms, and argon environment make the hot cell a particularly difficult target. Therefore, the pathway analyzed was to remove material from the TRU storage vault.

Each U/TRU ingot is cylindrical in shape, with a mass of about 10 kg. The Pu content is between 3 and 4 kg, and a single U/TRU ingot is the theft target quantity. For now, the analysis is focused on theft, but it should be noted that criticality concerns should be taken into account in future work to examine sabotage scenarios.

In order to transfer a U/TRU ingot, a person (operator or adversary) must be in the U/TRU Vault control room, the controls must have power, and TRU Vault lighting and cameras must have power and be operational. (The PPS is assumed to have lockouts for cranes or manipulators that may be used for material transfer. If the adversary cannot operate the TRU Vault controls, he must enter the TRU vault and remove the TRU ingots manually. The adversary's task is to get a U/TRU ingot out of the TRU Vault (via crane or explosive), open it and extract the material, and remove the ingot from site. The adversary will attempt to steal two ingots.

6. RESPONSE FORCE

Notional requirements are used as a first step to define the response force 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 response force is staffed with ten officers during each day, swing, and graveyard shifts. Each officer receives training to ensure they are current with mandated training requirements. Officers are required to complete certification and training on selected weaponry and equipment that maybe necessary to use in the event of an adversary attack. Weaponry and equipment may include, but not limited to:

- Handguns with approximately 40 rounds i.e. Smith and Wesson Military and Police (M&P) .45 caliber pistol
- Access to shoulder-fired weapons i.e. 9mm caliber H&K MP-5s, 12-gauge shotguns, and 5.56mm M-4 type rifles
- Batons
- Pepper Spray
- Handcuffs with key
- Handheld Radios.

The EChem Facility will have general orders and procedures in place that outline the roles and responsibilities for each officer.

6.1. Response Force Assumptions

Given the current status of the facility design, little is established regarding the response force for this facility, therefore many assumptions will be made for the security analysis. The onsite response force will consist of 10 officers divided into multiple teams and placed at multiple locations within the building to prevent losing them to 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. Table 2 shows RF numbers, starting locations, and muster times. Figure 24 shows the positions of the response force at the beginning of the scenario.

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
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	10 Onsite Responders and 2 Offsite		

Figure 24. Response Force Initial Positions

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.

6.2. Central Alarm Station (Supervisor/Management)

The shift supervisor and/or management develop schedules and post orders. They ensure procedures and policies are met and make command decisions in the event of a security related situation to raise or lower response levels. The supervisor and/or management work directly with the Central Alarm Station (CAS). The primary functions of the CAS include:

- Oversight of all security related emergency activities and support.
- Responsibility to maintain protection of all nuclear material onsite.
- Handle all alarm annunciation, assessment and dispatch of all alarms to the officers at the facility.
- Responsible to manage command, control, and communications for all security related emergency events.
- Remain in constant communications with the Command and Control Center.

7. DESIGN BASIS THREAT

The concept of the Design Basis Threat (DBT) is used to establish the expected threat to a facility. For this study, (a notional facility with a notional threat), a DBT will not be used. Rather, the section below will characterize the threat spectrum used for the security study. In this vulnerability assessment, only the outsider adversary threat is analyzed. The eChem Facility is designated as a Category One facility, and therefore warrants the use of the high-level outsider threat. Outsider adversary groups differ in their capabilities to defeat a physical protection system. For the current analysis, it is assumed that an insider is providing facility knowledge for the outsider threat group.

describes the capabilities and attributes for the outsider DBT in this assessment.

7.1. Varied Threat

To test a broader threat landscape, a threat spectrum was used. Numbers of attackers were varied from 4-8.

Table 3. Outsider High-Level Design Basis Threat Used for Assessment

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

7.2. Outsider Assumptions

The adversary team members were assumed to have the following characteristics:

- Equally trained.
- Able to perform any of the tasks needed to steal critical assets.
- Armed with an 7.62mm rifle, or 7.62mm belt-fed machine-guns (2), a pistol, ammunition, grenades, satchel charges containing bulk high explosives (HE, not to exceed 10 kg total), detonators, bolt cutters, and miscellaneous other tools.
- Able to each carry a man-portable load (29.5 kg [65 lb.]).
- In scenarios involving vehicles, the adversary team has access to two four-wheel drive vehicles.
- Adversaries have the tactical capability to divide forces and coordinate attacks from multiple vectors

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

8. VULNERABILITY ANALYSIS OF FACILITY DESIGN

Vulnerability assessment (VA) results are based on an analysis of the physical paths that the adversary follows to achieve its objective. The protection functions (detection and delay) along the paths are important in determining the adversary attack scenarios most likely to succeed. There are many possible combinations of ways to get to a target location and steal the asset(s); 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 so that they can be mitigated.

8.1. Definition of Adversary Path

An adversary path is an ordered series of actions against a facility that, if completed, will result in a successful theft event. Protection elements along the path potentially detect and delay the adversary, so that the dedicated response force can interrupt the series of events. 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 response force time (RFT).

8.2. Adversary Task Times

Table 4 and Table 5 feature delay times for the steps require to steal material from the TRU Vault. Non-sensitive data was used for all door and fence breaches. For the detailed breaches at the TRU Vault area, data was summed across steps so as not to reveal the specific breach times for any one step. Therefore, times given may contain travel times, breach times, and other steps not specifically listed.

All task times used in this analysis are mean times; maximum and minimum times are plus and minus 50% of the mean time, respectively. For example, if the mean time shown for

the Adversary Task Time in a scenario is 8 seconds, then the minimum task time is 4 seconds, and the maximum is 12 seconds.

8.3. Probable Detection Point

The path analysis for all outsider attacks focuses on when the adversary team arrives at the most Probable Detection Point (PDP) within the PPS. For the baseline analysis, the PDP is defined as a PPS element that reliably provides a high level of P_D (>0.50); also, the PDP in the analysis depends upon a reliable detection technology component rather than detection by guards (because of the human factor).

8.4. Delay Focused Design Features

Given the nature of the processes within the facility, the only viable theft target is in a hardened vault within the basement of the facility. The location of the vault in the basement greatly increases the amount of time necessary to breach it. The confined nature limits the explosive weight of any adversary breaching charge, allowing responders ample time to set up facility containment. If the adversary were to try to breach the reinforced concrete wall of the TRU Vault, the charge required would likely cause the building to collapse and bury the target material. Therefore the adversary would have to use multiple smaller charges to breach the way, and then cut rebar in between charge detonations. In addition, the concrete debris and dust would severely limit visibility further lengthening the timeline. For all of these reasons, if was determined that adversary would be forced to breach the multiple layers of steel vault doors and protective shutters that sperate the TRU Vault control room from the TRU vault itself.

8.5. Adversary Attack Scenario

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 breech the multiple shield doors on their way through the transport port in the TRU vault. The scenario is captured in story board form in Figure 25.

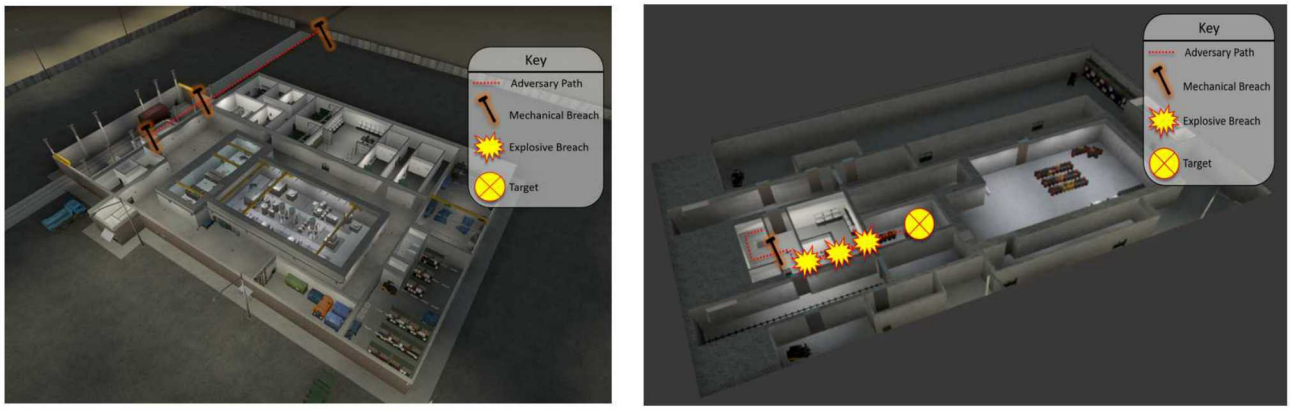


Figure 25. Ground Floor Adversary Attack Path (left) Basement Attack Path (right)

Table 4 presents the uninterrupted adversary attack timeline. It does not consider any potential disruption of the attack by the response force. All times are mean times, and cumulative time begins at the probable detection point (Step 3).

Table 4. Adversary Uninterrupted Attack Timeline

Task #	Adversary Task Description	Task Time (Sec)	Running Task Time Total (Sec)
1	Breach Passive Fence	30	--
2	Move to building exterior (50m)	15	--
3	Breach emergency exit (solid core steal door) on North wall	30*	--
4	Travel to stairwell door	5	5
5	Breach sold core steel door into stairwell down	30	35
6	Travel down staircase to inner stairwell door	15	50
7	Breach solid core steal door at inner stairwell area	30	80
8	Travel to door into work area	5	85
9	Breach solid core steal door, into work area	30	115
10	5.5 lbs Tamped HE Charge to breach GSA Class 5 Vault Door (< 1 inch steel plate) to enter Material Inspection Room (MIR)	--	--
11	5.5 lbs Tamped HE Charge to breach Movable Shield Wall (assumed cross section is 3/4 inch steel face plate with 3 inch insulation with 1/8 inch steel back plate) in front of Material Transfer Room Entry Door	--	--
12	5.5 lbs Tamped HE Charge to breach Movable Shield Wall (assumed cross section is 3/4 inch steel face plate with 3 inch insulation with 1/8 inch steel back plate) in front of gap in TRU Vault Wall for hoist passage	273^	388
13	Climb step ladder ~10ft then crawl through square hole ~2ft x 2ft	30	418
14	Adversary in Vault receives portable light sources, manual chain hoist, beam clamp, lifting straps & small toolkit through I-beam hole between Material Transfer Room (MTR) and Vault	--	--
15	Attach portable manual hoist to I beam	150^	568
16	Connect hoist lifting hooks to the top lifting hooks of a target container	--	--

17	Use the manual hoist to lift a target container to above the level of the rest of the containers (~23-25 inches)	--	--
18	Lower target container such that it pivots over and lays on its side	--	--
19	Lift base of container with hoist and lifting strap such that the ingot is able to slide out of the top	--	--
20	Pass ingot thru I-beam hole in TRU Vault Wall to Adversary in Material Transfer Room (MTR)	143.75^	712
21	Repeat Steps 16-20 to get 2nd Ingot to MTR	143.75	855
22	Adversary climbs through I-beam hole into MTR	30	885
23	Adversaries exit Material Transfer Room	12.5	898
24	Adversaries exit Material Inspection Room	12.5	910
	*Critical Detection Point **Total**		(15:10 min)
^Denotes values that a sums of the steps preceding which have " --" for their delay value			

8.6. Path Analysis Results

Given that there are two mobile teams on foot patrol in full gear, the response force timeline is very short. These teams are able to begin moving to response positions within thirty seconds of the breach on the emergency exit door. Interruption is virtually assured given that all building services have multiple complimentary sensors with dedicated, fixed assessment cameras (P_I = 99%). Table 5 shows the detection and delay values at each step. The "location" column indicates where in the step the detection is likely to occur (B = beginning, M = middle, E = end).

Table 5. Path analysis results

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:
1	Breach outer passive fence	0.02	M	15
2	Engage foot patrol	0.10	M	10
3	Move to building exterior (50m)	0.02	M	15
4	Breach Emergency Exit Door	0.95	E	30
5	Move to Stairwell Door	0.80	M	5
6	Breach Upper Stairwell	0.80	E	30
7	Move down to Lower Stairwell door	0.02	M	15
8	Breach Lower Stairwell Door	0.80	E	30
9	Move to Basement Hall Door	0.02	M	5
10	Breach Basement Hall Door	0.80	E	30
11	Move to Vault Door at TRU Vault Control Room	0.02	M	5
12	Breach Vault Door	0.80	E	--
13	Move to Shield Wall at TRU Vault	0.02	M	--
14	Breach Shield Wall at TRU Vault	0.80	E	--

15	Move to inner Shield Wall	0.02	M	--
16	Breach Inner Shield Wall	0.80	E	283^
17	Set up and Climb step latter into TRU Vault	0.02	M	30
18	Retrieve target material	0.02	M	468
19	Exit Site	0.02	M	30

Probability of Interruption:	.99
^Denotes values that a sums of the steps preceding which have " -- " for their delay value	

9. SIMULATION AND ANALYSIS OVERVIEW

A simplistic simulation was conducted in Scribe3D© in order to gauge the rough effectiveness of the interior response teams of the process site. The goal of this analysis was to provide a high-level understanding of the effectiveness of the proposed locations for interior responders at an early design phase. The scenario was conducted from the outer passive perimeter through acquisition of the target material. Given that the target material is in the basement in a vault, sabotage was not considered. Adversaries must transport material offsite.

9.1. Response Force Win Criteria

At the end of each simulation, a RF win is awarded in the event the adversary is unable to successfully complete its theft objective due to attrition of adversary personnel and/or lack of required equipment to complete necessary breaches.

9.2. Scenario Results Description

Section 8.5 describes the uninterrupted scenario timeline for the adversary, while Section 8.6 describes the response force timeline. This section will describe the results of the intersection of these two timelines, and step through how the scenario unfolded in the Scribe3D© simulation.

9.2.1. Time Zero – 00:00-00:30 Simulation start

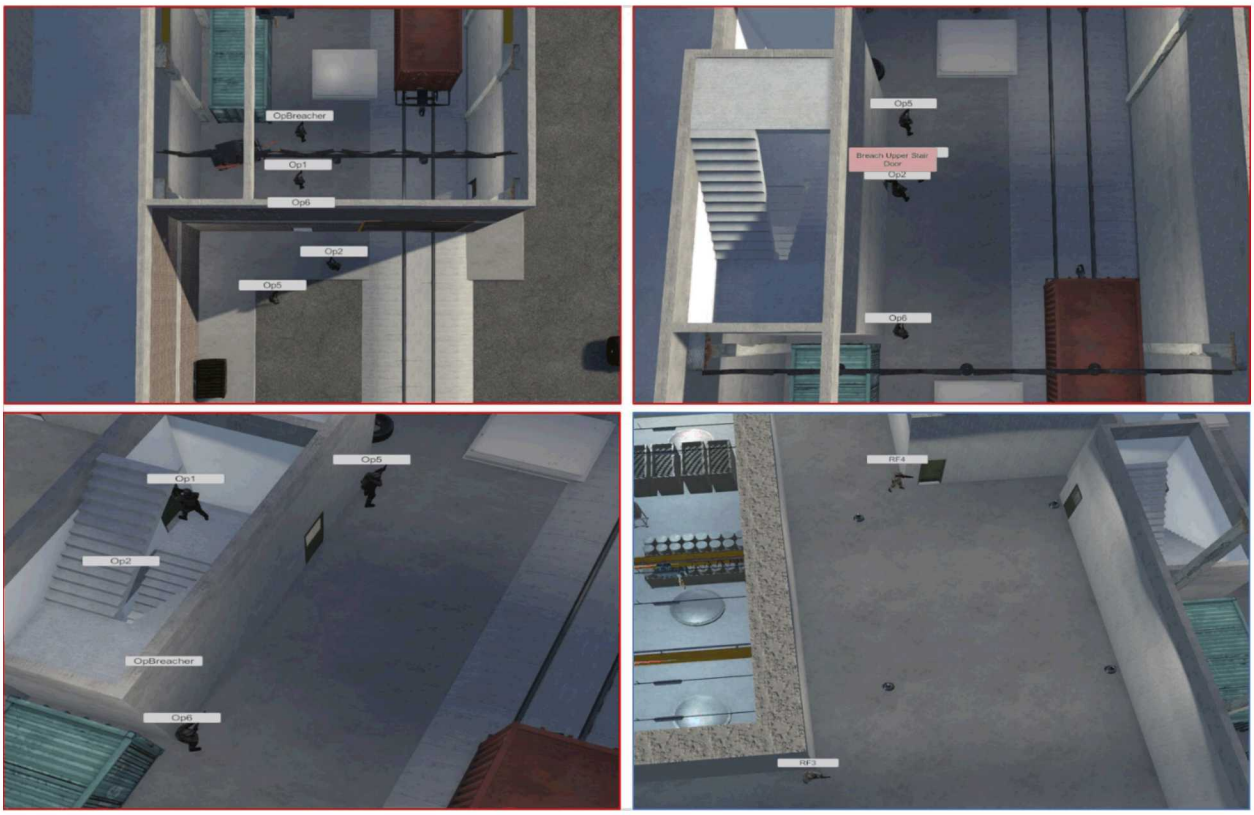
The neutralization timeline begins at the probable detection point. The path analysis conducted showed that the adversaries would most likely be detected as they breached the emergency exit door of the facility. In the simulation, it is assumed that the adversary has cut the outer passive fence and advanced to the exterior of the building and is preparing to breach. Op3 has taken a concealed position at the corner of the building. As the breach team is completing it the exterior breach, Op3 engages the patrol from cover, see (Figure 26).

Upper left-Adv engages outer patrol, Middle-Time 00:00 configuration, Upper Right-Adv. Breach outer door

Figure 26. Time 00:00 Scenario configuration

9.2.2. Time 30s – 00:30-01:06 Adversary Enters Facility

Upon completion of outer breach, adversary enters facility, and moves to the stairwell in the transportation highbay. The adversary breaches the outer door and moves downstairs. The adversary team leaves individuals to cover the upper entry into the stairwell. The inner response team responds to the stairwell and provides containment of the inner door leading out of the stairwell (see Figure 27).

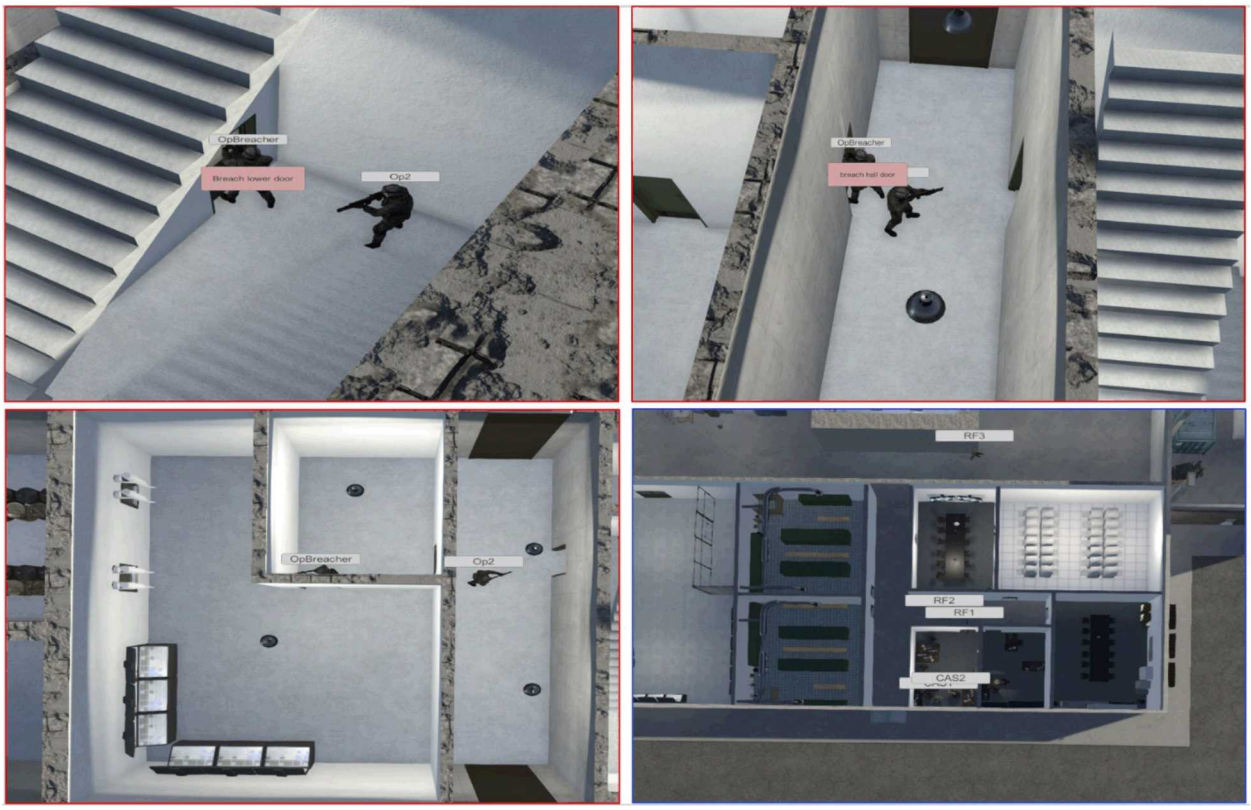


Upper left-Adv. Move through outer breach, Upper right-breach of upper stairwell, Lower left-Adv. Cover stairwell, Lower right- RF containment of inner stairwell

Figure 27. Adversary Enters Facility

9.2.3. Time 01:06-02:25 Adversaries begin Vault Breach

The adversary team makes its way downstairs and breaches the inner stair well door. They then move to the TRU vault control access area outer door and breach it. Next, they move to the vault door leading into the 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 (see Figure 28).



Upper left – Breach of lower stairwell, Upper right- breach of control room access area, Lower left- breach of TRU Vault Control Room, Lower right- RF1 and 2 move to containment positions

Figure 28. Adversaries Begin Vault Breach

9.2.4. Time 02:25 – 10:00 – Vault Breach and RF containment positions

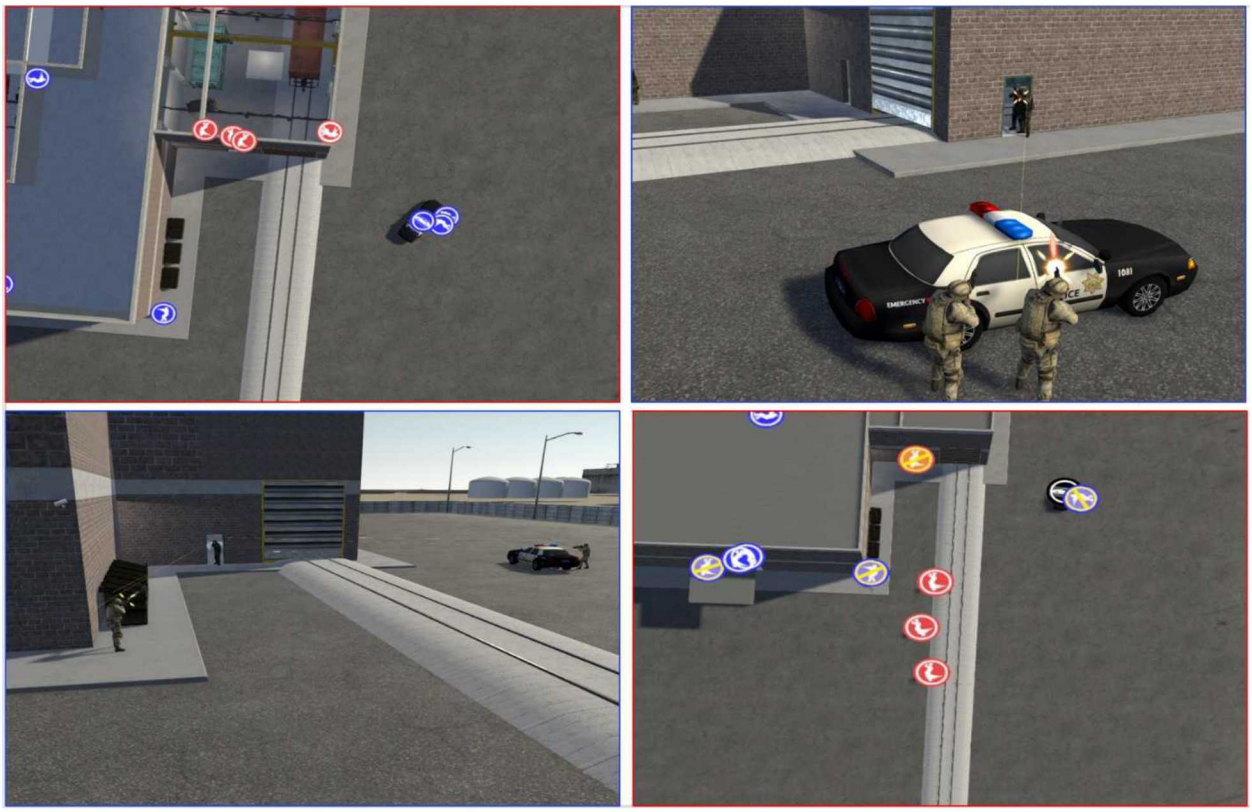
RF1 and RF2 moved outside the building to secure the exterior and take up containment positions on the probable adversary egress routes. Based on camera feeds from the building exterior, they know than an adversary is still outside, and they engage. They move to containment positions near where the adversary entered the facility. The adversary is executing their theft event by breaching the layers of TRU vault hatch. Approximately ten minutes after the initial alarm, the LLEA first responders arrive and set up facility containment positions (see Figure 29).

Upper left – RF 1&2 engage Adv outside building, Upper Right – TRU Vault Breach in Progress, Lower left – Remaining RF in containment, Lower Right, LLEA responds in containment positions

Figure 29. Vault Breach and RF Containment

9.2.5. Time 10:00-16:20 - Adversary Attempts Escape

Roughly fifteen minutes into the scenario, the adversaries have acquired the target and attempt to leave the site. They move upstairs and stack up on the two exit doors on the facility side where the breached occurred. Advance riflemen begin engaging LLEA and RF from both doors simultaneously. At this point, either all adversary rifleman are killed, or all responders are killed. Either way, once the engagement is complete, the adveersary carrying the target material attempts escape. If the adversary is neutralized, the responders are successful, and if no responders remain, the adversary theft is successful.



Upper left – Adv. Sets up to exit the building with riflemen at two exit doors, Upper right – LLEA and Adv engagement, Lower left – RF and ADV Engagement, Lower right, Adversary escaping with material

Figure 30. Adversary Attempts Escape

9.3. Results Theft Timeline Summary – All Scenarios

A total of 100 simulations were conducted for each scenario, to evaluate the success of an adversary attack against the TRU Vault. In all engagements, the adversary was successful in breaching the plant perimeter, entering the facility through an emergency exit door, reaching the basement (service) level, and extracting the material (100/100 scenarios). During the table-top scenario development process, the decision was made to pursue a containment strategy. Therefore, the RF set up a perimeter around the facility rather than try to assault the adversary as they were breaching the TRU Vault. This resulted in favorable outcomes for keeping the material onsite but guaranteed that the adversary would get hands on the target material.

Table 6 shows the average time of completion for events within the timeline. Note that it differs from the uninterrupted scenario timeline (Table 4). This is due to engagements between RF and adversaries as well as contingences that adversaries were forced to carry out due to these engagements. For example, if the breacher carrying the target material

was killed, another adversary would be forced to retrieve the target to get it off site. Because the response force employs a containment strategy, there are very few engagements that take place before the adversary escapes the facility with the material. Therefore; the average timelines are very similar across all scenarios. Note that the times presented only reflect scenarios where the event occurred.

Table 6. Scribe3D © Simulation Results – Average Timeline

Task #	Event	Average Completion Time MM:SS				
		4 ADV	5 ADV	6 ADV	7 ADV	8 ADV
1	Breach Upper Stair Door	0:36	0:36	0:36	0:36	0:36
2	Breach lower door	1:11	1:11	1:11	1:11	1:11
3	breach hall door	1:42	1:42	1:42	1:42	1:42
4	Set Explosives at TRU Vault control room door	2:50	2:50	2:50	2:50	2:50
5	Breach TRU Vault control room door	2:59	2:59	2:59	2:59	2:59
6	Set explosives at outer shield wall	4:30	4:30	4:30	4:30	4:30
7	Breach outer movable shield wall	4:41	4:41	4:41	4:41	4:41
8	Set explosives on inner movable shield	6:14	6:14	6:14	6:14	6:14
9	Breach inner movable shield wall	6:27	6:27	6:27	6:27	6:27
10	Climb step ladder through wall	7:01	7:01	7:01	7:01	7:01
11	Collect material	14:48	14:48	14:48	14:48	14:48
12	Exit Facility with material	15:45	15:45	15:45	15:45	15:45
13	Get material across facility premises	15:48	15:48	15:50	15:49	15:49
14	Exit facility premises with material	16:19	16:19	16:21	16:19	16:19

9.4. Theft Results – 4 Adversaries

Table 7 describes the outcomes of the attack scenario with 4 adversaries. Overall, the RF was successful in 93% of scenarios. Average scenario length (for all scenarios) was 16:06, which was 13 seconds less than the length for successful adversary thefts (16:19). This time is shorter because the adversaries were unsuccessful 93% of the time, so they were unable to complete their timeline. The average run time is also longer than the uninterrupted timeline (15:10), reflecting the impact the RF have in delaying the adversary attack. In the scenario, there were an average of 20 engagements (times any entity fired its weapon), and average of seven (7) of those engagements resulted in combat ineffectiveness in the target (roughly 35%). This overall low success rate in engagement is largely due to most entities being in cover when taking fire. On average, the RF lost 2.98 KIA, which is ~37% of the responders which actively engage in the fight. The adversaries lose 3.76 KIA, which is ~94% of their forces on average. However, in adversary wins, their casualty rate dropped to 0.57 KIA ~14%. Therefore, they were required to be very fortunate in the engagements in order to be successful.

Table 7. Scribe3D © Simulation Results – 4 Adversary Scenario

Name	Results
Number Of Runs	100
Blue Wins	93
Red Wins	7
Probability of Neutralization (P_N)	93%
Prevent Material Out of Building	7
Average Time (s)/(mm:ss)	950/(15:50)
Average Engagements	20
Average KIA Engagements	7
Blue Force Count	14
Average Blue KIA	2.98
Average Blue KIA in Win	2.75
Red Force Count	4
Average Red KIA	3.76
Average Red KIA in Win	0.57

9.5. Theft Results – 5 Adversaries

Table 8 describes the outcomes of the use of 5 adversaries. The RF was again successful in 93% of scenarios. Average scenario length (for all scenarios) was 16:06, which was 13 seconds less than the length for successful adversary thefts (16:19). In the scenario, there were an average of 29 engagements (times any entity fired its weapon), and average of eight (8) of those engagements resulted in combat ineffectiveness in the target (roughly 27%). On average, the RF lost 3.56 KIA, which is almost 50% of the responders which actively engage in the fight. The adversaries lose 4.7 KIA, which is over 80% of their forces on average. However, in adversary wins, their casualty rate dropped to 1.52 KIA or roughly 25%.

Table 8. Scribe3D © Simulation Results – 5 Adversary Scenario

Name	Results
Number Of Runs	100
Blue Wins	93
Red Wins	7
Probability of Neutralization (P_N)	93%
Prevent Material Out of Building	10
Average Time (s)/(mm:ss)	966/(16:06)
Average Engagements	29

Average KIA Engagements	8
Blue Force Count	12
Average Blue KIA	3.56
Average Blue KIA in Win	3.38
Red Force Count	5
Average Red KIA	4.7
Average Red KIA in Win	1.52

9.6. Theft Results – 6 Adversaries

Table 9 describes the outcomes of the use of 6 adversaries. The RF success dropped compared to the other scenarios to 75%. Average scenario length (for all scenarios) was 16:04, which was 17 seconds less than the length for successful adversary thefts (16:21). In the scenario, there were an average of 33 engagements (times any entity fired its weapon), and average of nine (9) of those engagements resulted in combat ineffectiveness in the target (roughly 27%). On average, the RF lost 3.84 KIA, which is almost 50% of the responders which actively engage in the fight. The adversaries lose 4.88 KIA, which is over 80% of their forces on average. However, in adversary wins, their casualty rate dropped to 1.52 KIA or roughly 25%.

Table 9. Scribe3D © Simulation Results – 6 Adversary Scenario

Name	Results
Number Of Runs	100
Blue Wins	75
Red Wins	25
Probability of Neutralization (P_N)	75%
Prevent Material Out of Building	25
Average Time (s)/(mm:ss)	964/(16:04)
Average Engagements	33
Average KIA Engagements	9
Blue Force Count	12
Average Blue KIA	3.84
Average Blue KIA in Win	3.12
Red Force Count	6
Average Red KIA	4.88
Average Red KIA in Win	1.52

9.7. Theft Results – 7 Adversaries

Table 10 describes the outcomes of the use of 7 adversaries. Overall, the RF was successful in 50% of scenarios. Average scenario length (for all scenarios) was 16:08, which was 11 seconds less than the length for successful adversary thefts (16:19). This time is shorter because the adversaries were unsuccessful 50% of the time, so they were unable to complete their timeline. In the scenario, there were an average of 39 engagements (times any entity fired its weapon), and average of nine (9) of those engagements resulted in combat ineffectiveness in the target (roughly 23%). On average, the RF lost 4.86 KIA, which is over 60% of the responders which actively engage in the fight. The adversaries lose 4.86 KIA, which is over 62% of their forces on average. However, in adversary wins, their casualty rate dropped to 1.48 KIA or roughly 21%.

Table 10. Scribe3D © Simulation Results – 7 Adversary Scenario

Name	Results
Number Of Runs	100
Blue Wins	50
Red Wins	50
Probability of Neutralization (P_N)	50%
Average Time (s)/(mm:ss)	968/(16:08)
Prevent Material Out of Building	47
Average Engagements	39
Average KIA Engagements	9
Blue Force Count	14
Average Blue KIA	4.86
Average Blue KIA in Win	3.72
Red Force Count	7
Average Red KIA	4.32
Average Red KIA in Win	1.64

9.8. Theft Results – 8 Adversaries

Finally, Table 11 describes the outcomes of the use of 8 adversaries. Overall, the RF was successful in 31% of scenarios. Average scenario length (for all scenarios) was 16:11, which was 8 seconds less than the length for successful adversary thefts (16:19). In the scenario, there were an average of 36 engagements (times any entity fired its weapon), and average of nine (9) of those engagements resulted in combat ineffectiveness in the target (roughly 25%). On average, the RF lost 5.07 KIA, which is over 63% of the responders

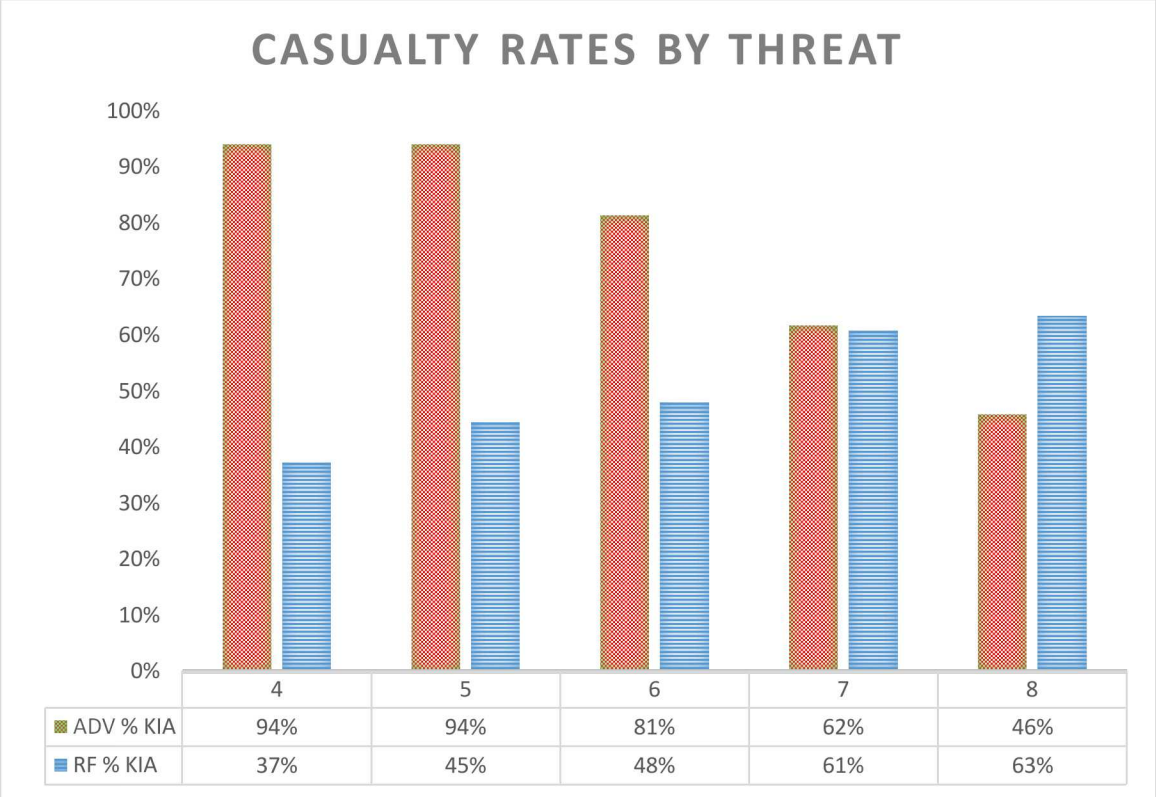
which actively engage in the fight. The adversaries lose 3.67 KIA, which is roughly 46% of their forces on average. However, in adversary wins, their casualty rate dropped to 1.72 KIA roughly 22%.

Table 11. Scribe3D © Simulation Results – 8 Adversary Scenario

Name	Results
Number Of Runs	100
Blue Wins	31
Red Wins	69
Probability of Neutralization (P_N)	31%
Average Time (s)/(mm:ss)	971/(16:11)
Prevent Material Out of Building	29
Average Engagements	36
Average KIA Engagements	9
Blue Force Count	14
Average Blue KIA	5.07
Average Blue KIA in Win	3.26
Red Force Count	8
Average Red KIA	3.67
Average Red KIA in Win	1.72

10. RESULTS DISCUSSION

Initial analysis of the scenario found that trying to engage the adversary while breaching the U/TRU vault led to significant loss of responders since the adversaries set up fighting positions in stairwells. The containment strategy was chosen as a result. Thus, for all the scenarios, the adversary is able to breach the building and acquire material, but unlikely to take the material off-site. Figure 31 shows a summary of the casualty rate for responders (RF) and adversaries (ADV). As could be expected, as adversary threat levels increase, the percentage of adversaries neutralized drops, while the adversary attrition rate increases, although very gradually.



	4	5	6	7	8
ADV % KIA	94%	94%	81%	62%	46%
RF % KIA	37%	45%	48%	61%	63%

Figure 31. Causalty Rate by Threat Level

Utilizing a containment strategy, the response is able to keep material from being stolen from the echem facility design 75% of the time or great for threats of six (6) or lower (see Figure 32). This is while only maintaining a security staff of 10 responders on site, and assuming a single offsite LLEA team of two (2) responders in 10 minutes. General best practice is to maintain a 3-to-1 ratio between responders and design basis threat in order to secure system effectiveness. Results for threat levels higher than six (6) were 68% effectiveness at seven (7) adversaries and 31% effectiveness at eight (8) adversaries, revealing that the system fails gradually, rather than suffering a steep drop off at any single step. This is a useful data point when considering the possibility of attacks that may

exceed the design basis threat. The system, as designed, overs some protection against large scale threats.

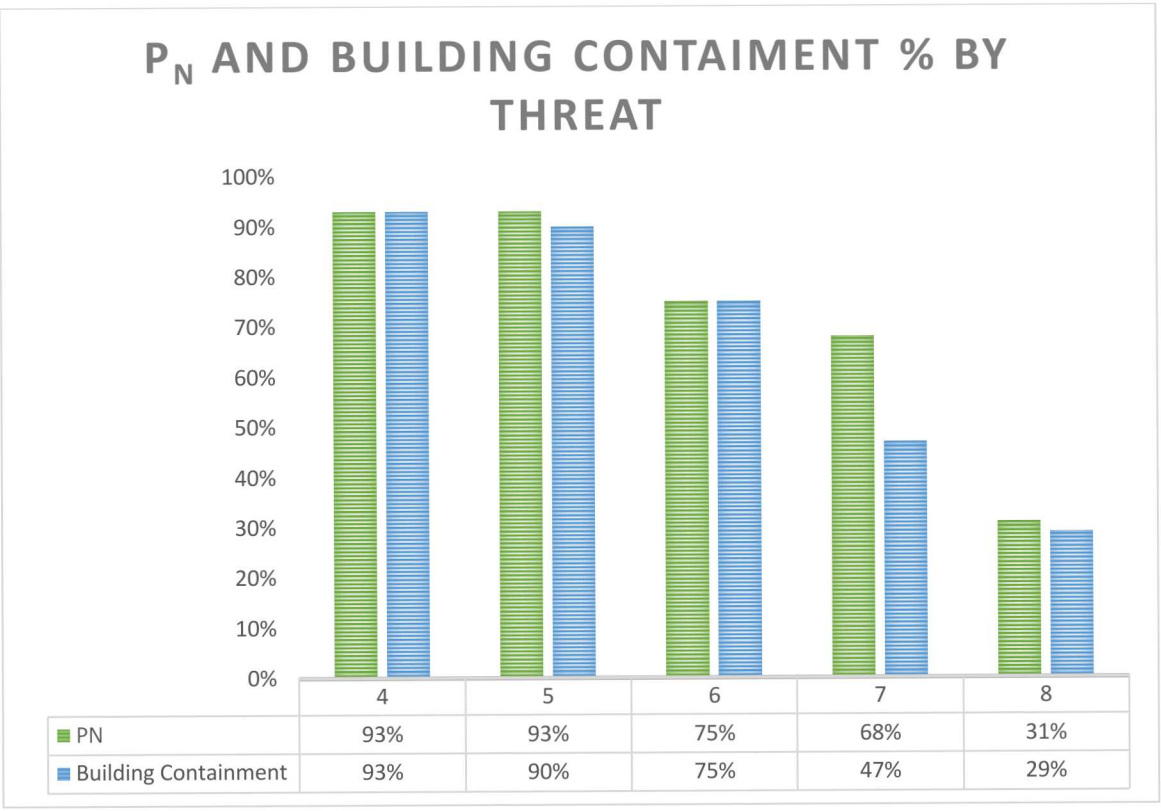


Figure 32. Combined Results by Threat

11. CONCLUSION AND FUTURE WORK

This report demonstrated the use of single-analyst physical protection modeling tools for design and analysis of physical protection systems. An electrochemical reprocessing facility was chosen as the refence facility. In less than one year, a complete building design was modeled using Blender and Scribe3D ©, and initial analyses were completed. While the adversary examined in this work was a notional adversary with a range of numbers, for actual facility designs the analysis would focus on a DBT based on regulatory requirements.

This work is one capability within the DOE NE MPACT program 2020 milestone to develop a Virtual Facility Distributed Test Bed for complete Safeguards and Security by Design. The modeling capabilities presented here work with other tools in the MPACT campaign to develop advanced and optimized safeguards and security

Future work will expand the types of scenarios examined including insider diversion, outsider sabotage, and additional outsider theft scenarios. Future work will also examine design changes to optimize the physical security design while still providing robust protection for the facility.

REFERENCES

[1] B.B. Cipiti et al., "Material Protection Accounting and Control Technologies (MPACT) Implementation Plan: Lab-Scale Demonstration of Advanced Safeguards and Security Systems," INL/EXT-17-43112 (August 2017).

[2] B.B. Cipiti et al., "Material Protection Accounting and Control Technologies (MPACT) Advanced Integration Roadmap," LA-UR-16-27364 (2016).

[3] B.B. Cipiti et al., "Material Protection Accounting and Control Technologies (MPACT) Modeling and Simulation Roadmap," LA-UR-16-26045 (2016).

[4] A.A. Frigo, D.R. Wahlquist, and J.L. Willit, "A conceptual Advanced Pyroprocess Recycle Facility," *Global 2003*, New Orleans, LA (November 2003).

[5] "Burns and Roe Electrochemical Fuel Processing Design Report," (1995).

[6] B.B. Cipiti and N. Shoman, "Pyroprocessing Safeguards Approach," *Advances in Nuclear Nonproliferation Technology and Policy Conference*, Orlando, FL (November 2018).

[7] Blender, available at www.blender.org/about/ (2019).

[8] Unity, available at unity3d.com/unity (2019).

DISTRIBUTION

Email—External

Name	Company Email Address	Company Name
Mike Reim	Michael.Reim@nuclear.energy.gov	Department of Energy
Mike Browne	mcbrowne@lanl.gov	Los Alamos National Lab
Laura Limback	losburn@lanl.gov	Los Alamos National Lab

Email—Internal

Name	Org.	Sandia Email Address
Sylvia Saltzstein	8845	sjsaltz@sandia.gov
Nathan Shoman	8845	nshoman@sandia.gov
Jordan Parks	6835	mjparks@sandia.gov
Tam Le	6835	tdle@sandia.gov
Todd Noel	6835	tgnoel@sandia.gov
Ryan Knudsen	6835	rknudse@sandia.gov
Steven Stromberg	6835	sjstrom@sandia.gov
Dominic Martinez	6835	dmartin@sandia.gov
Technical Library	9536	libref@sandia.gov

This page left blank

This page left blank

Sandia National Laboratories

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