SAND2020-10051R

SANDIA REPORT
SAND20XX-XXXX
Printed September 2020

Sandia National Laboratories

Physical Security Model Development of an Electrochemical Facility

Benjamin B. Cipiti, M. Jordan Parks, Ryan Knudsen, Todd G. Noel, Benjamin 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 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. Two theft scenarios (an outsider attack and insider diversion) as well as a sabotage scenario were examined in order to optimize the security design. Security metrics are presented. This work fits into a larger Virtual Facility Distributed 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 (DOE), Office of Nuclear Energy (NE).

CONTENTS

1. Introduction 15
   1.1. Background 16
   1.2. MPACT 2020 Milestone 16
   1.3. Electrochemical Facility Design References 17
2. PPS Design Process 21
3. Regulatory Requirements 23
4. Overview of Vulnerability Assessment 25
   4.1. Purpose and Objectives of the Assessment 25
   4.2. Scope of Assessment 25
   4.3. VA Process 25
   4.4. Modeling Tools 26
      4.4.1. Blender 26
      4.4.2. EASI ..... **Error! Bookmark not defined.**
      4.4.3. PathTrace © and EASI - Path Analysis Tool 26
      4.4.4. Scribe3D© – Tabletop Recorder and Automated Tabletop Data Tool 27
   4.5. System Effectiveness Analysis Assumptions 27
5. Electrochemical Facility Design and Operations 29
   5.1. Processing Level 29
      5.1.1. High-Bay 30
      5.1.2. Air Cell/Hot Cell 31
      5.1.3. Control Room 32
      5.1.4. Central Alarm Station/Guard Force Staging Area/Entry Control Point 33
      5.1.5. Server Room/Warehouse/Storage/Machine Shop 35
   5.2. Basement Level 35
      5.2.1. U/TRU Vault and Vault Control Room 37
      5.2.2. Subcell Transfer Tunnels 37
   5.3. Top Floor – Process Cell Equipment Service Floor 37
      5.3.1. Hot Repair/Glovewall/Mock-Up Areas/Secondary Alarm Station 38
6. Target Characterization 41
   6.1. Target Identification and Quantities 41
      6.1.1. Spent Nuclear Fuel 41
      6.1.2. Oxide Reduction 41
      6.1.3. Electrorefiner 41
      6.1.4. Uranium Metal Product 42
      6.1.5. U/TRU Metal Product 42
      6.1.6. Noble Metal, Cladding, and Fission Product Wastes 42
      6.1.7. Backup Generator 43
7. Facility Physical Security System 45
   7.1. PPS Overview 45
      7.1.1. Perimeter Physical Security System 45
      7.1.2. Entry Control Point 46
      7.1.3. Facility Interior Security System Design 47
   7.2. Response Force 54
      7.2.1. Response Force Assumptions 54

7.2.2. Central Alarm Station (Supervisor/Management) 56
8. Threat Spectrum 57
8.1. Varied Threat 57
8.2. Outsider Assumptions 58
9. Vulnerability Analysis of Facility Design 59
9.1. Definition of Adversary Path 59
9.2. Probable Detection Point 59
9.3. Adversary Task Times 59
9.4. Delay Focused Design Features – U/TRU Vault 60
10. Analysis Scenario Outline 61
11. Theft Attack Results 63
11.1. Outsider Theft Attack Scenario - Path 63
11.1.1. Outsider Theft Path Analysis Results EASI 64
11.1.2. Outsider Theft Path Analysis Results PathTrace© 65
11.1.3. PathTrace Theft Path Analysis Results Discussion 66
11.2. Theft PN Analysis Simulation and Analysis Overview 67
11.2.1. Response Force Win Criteria 67
11.2.2. Scenario Results Description – Theft 68
11.2.2.1. TRU Theft Scenario - Time Zero – 00:00-00:30 Simulation start 68
11.2.2.2. Time 30s – 00:30-01:06 Adversary Enters Facility 68
11.2.2.3. Time 01:06-02:25 Adversaries Begin Vault Breach 69
11.2.2.4. Time 02:25 – 10:00 – Vault Breach and RF Containment Positions 70
11.2.2.5. Time 10:00-16:20 - Adversary Attempts Escape 71
11.2.3. Results Outsider Theft – Baseline 72
11.2.3.1. Baseline Scribe3D© Results – Outsider Theft 72
11.3. Outside/Insider Collusion Scenario Theft of U/TRU Material 73
11.3.1. Collusion Path Analysis Results – Pathtrace© 74
11.3.2. Outsider/Insider Collusion Scenario Attack Timeline 74
11.4. Insider/Outsider PN Collusion Results – Theft 75
11.4.1. Inside/Outsider Collusion - Time 00:00-00:30 75
11.4.1.1. Time 00:40-01:30 Adversary Enters Facility and Secures Corners 75
11.4.1.2. Time 01:30-02:40 Adversaries Breach Stairwell Doors 76
11.4.1.3. Time 02:40-06:50 Adversaries Acquire Target Material 77
11.4.2. Results Collusion Theft – Baseline 77
11.4.2.1. Scribe3D© PN Collusion Theft Results – Baseline 77
11.4.3. Collusion Theft – Upgrade 1 – Mantraps 78
11.4.3.1. Scribe3D© PN Collusion Theft Results – Upgrade 1 Mantraps 78
11.4.4. Collusion Theft – Upgrade 2 – Mantraps + Shifting exterior patrols 79
11.4.4.1. Scribe3D© PN Collusion Theft Results – Upgrade 2 Mantraps + Patrol Relocation 79
11.4.5. Collusion Theft – Upgrade 3 – Extended Detection, Exterior Delay, Hardened Garage 80
11.4.5.1. Extended Detection – Fused Radar and Video Motion Detection Using the Deliberate Motion Algorithm (DMA)8 81
11.4.5.2. Ankle Breaker Anti-Transit Landscaping 81
11.4.5.3. Hardened Fighting Positions at Quicker Building Access Points 81

11.4.5.4. Scribe3D© PN Collusion Theft Results – Upgrade 3 Extended Detection, Transit Rocks, HFPs....82
11.4.6. Theft Results Summary....84
12. Sabotage Attack Results....85
12.1. Outsider Sabotage Scenario - Path....85
12.1.1. Sabotage Scenario Task Timeline....85
12.1.2. Sabotage Scenario Path Analysis Results....86
12.2. Sabotage PN Analysis Simulation and Analysis Overview....87
12.2.1. Response Force Win Criteria....87
12.2.1.1. Sabotage P_N Results Description – Sabotage....87
12.2.1.2. Hot Cell Sabotage Scenario – Time 00:00-00:30 Simulation Start....87
12.2.1.3. Time 00:40-02:00 Adversary Enters Facility Begins Sabotage....88
12.2.1.4. Time 02:00-06:00 Adversary Enters Facility Begins Sabotage....89
12.2.2. Results Sabotage – Baseline....89
12.2.2.1. Scribe3D© PN Sabotage Results – Baseline....89
12.2.3. Results Sabotage - Upgrade 1 - Mantraps and Response Changes....90
12.2.3.1. Scribe3D© PN Sabotage Results – Upgrade 1 - Mantraps....91
12.2.4. Results Sabotage – Upgrade 2 – Mantraps Plus Shifting Exterior Patrols....92
12.2.4.1. Scribe3D© P_N Sabotage Results – Upgrade 2 – Mantraps Plus Shifting Patrol 92
12.2.5. Results Sabotage – Upgrade 3 – Extended Detection, Exterior Delay, Hardened Garage....93
12.2.5.1. Scribe3D© PN Sabotage Results – Upgrade 3 Extended Detection, Transit Rocks, HFPs....93
12.2.6. Sabotage Results Summary....94
13. Conclusion....95

LIST OF FIGURES

Figure 1. Electrochemical Facility 2/3D Images....11
Figure 2. Theft Results Summary....12
Figure 3. Sabotage Scenario Upgrade Results....12
Figure 4. Virtual Facility Distributed Test Bed....17
Figure 5. Electrochemical Flowsheet [6]....19
Figure 6. DEPO Process [1]....21
Figure 7. Processing Level Facility Overview....29
Figure 8. Processing Level facility 3D Model – Blender Screenshot....30
Figure 9. High Bay Area....31
Figure 10. Air and Argon Hot Cells....32
Figure 11. Control Room....33
Figure 12. CAS (left) and ECP (right)....34
Figure 13. ECP Security Layout....34
Figure 14. Warehouse (left), Machine Shop (upper right), and Server Room (lower right)....35
Figure 15. Basement Level Facility Overview....36
Figure 16. Basement Level 3D Model....36
Figure 17. U/TRU Vault (right) and Vault Control Room (left)....37
Figure 18. Basement Transfer Tunnels....37

Figure 19. Top Level Facility Overview 38
Figure 20. Top Level 3D Model 38
Figure 21. Hot Repair Area 39
Figure 22. Building Exterior Security Features 46
Figure 23. EChem Processing Building, Operating Floor, and Conceptual PPS Design Layout 48
Figure 24: EChem Processing Building, Basement Level, and Conceptual PPS Design Layout 49
Figure 25: EChem Processing Building, Hot Repair Area, and Conceptual PPS Design Layout 50
Figure 26. Response Force Starting Locations 55
Figure 27. Ground Floor Adversary Attack Path (left) Basement Attack Path (right) 63
Figure 28 – PathTrace© path on ground floor for Outsider TRU Vault Theft Scenario 66
Figure 29 – PathTrace© path in basement for Outsider TRU Vault Theft Scenario 66
Figure 30. Time 00:00 Scenario configuration 68
Figure 31. Adversary Enters Facility 69
Figure 32. Adversaries Begin Vault Breach 70
Figure 33. Vault Breach and RF Containment 71
Figure 34. Adversary Attempts Escape 72
Figure 35. Collusion Path to Material Stashed by Insider 74
Figure 36 - Time 00:00 Collusion Theft Scenario configuration 75
Figure 37 - Time 00:40 Building Entry and Secure Corners 76
Figure 38 - Time 01:30-02:40 Adversaries breach upper and lower stairwell doors 76
Figure 39. Adversaries breach and acquire target material – Collusion 77
Figure 40. Ankle Breaker Rock Example (left); High Bay Hardened Fighting Position (right) 81
Figure 41. Upgrade 3 Component Locations with Path A and Path B 82
Figure 42. Theft Results Summary 84
Figure 43. Sabotage Scenario 85
Figure 44. Sabotage Scenario Path Analysis Results 86
Figure 44 - Time 00:00 Sabotage Scenario Configuration 88
Figure 45 - Time 00:40 Building Entry and begin sabotage 88
Figure 46 - Time 02:00 Sabotage and Interdiction 89
Figure 48. Baseline Sabotage, Probability of Neutralization for Four-to-Eight Attackers 90
Figure 49. Mantrap Upgrade and Response Force Configuration 91
Figure 50. Sabotage Scenario Upgrade Results 94

LIST OF TABLES

Table 1. Detail and Legend for Figure 23 through Figure 25 51
Table 2. Response Force Overview 55
Table 3. Outsider High-Level Design Basis Threat Used for Assessment 57
Table 4. Adversary Uninterrupted Attack Timeline 63
Table 5. Path Analysis Results 65
Table 6. PathTrace Probability of Interruption Results 67
Table 7. Baseline Scribe3D © Simulation Results – Outsider Theft 73
Table 8. Collusion Scenario Timeline and Probability of Interruption 74
Table 9. Adv Target Acquisition Insider Collusion 77
Table 10. Scribe3D © Simulation Results – 4 Adversary Collusion Theft – Baseline 78
Table 11. Scribe3D © Simulation Results – Collusion Theft – Upgrade 1 79
Table 12. Scribe3D © Simulation Results – Collusion Theft – Upgrade 2 80
Table 13. Response Force Attrition Rate Reduction vs. Baseline 80

Table 14. Scribe3D © Simulation Results – Collusion Theft – Upgrade 3 – Path A 83
Table 15. Scribe3D © Simulation Results – Collusion Theft – Upgrade 3 – Path B 84
Table 16. Sabotage Scenario Path Analysis Results 86
Table 17. Sabotage Scenario Path Analysis Results 87
Table 18. Scribe3D © Simulation Results – Sabotage – Upgrade 1 91
Table 19. Scribe3D © Simulation Results – Sabotage – Upgrade 2 92
Table 20. Scribe3D © Simulation Results – Sabotage – Upgrade 3 – Path B 93
Table 21. Remaining Response Strength Upgrade 3 95

This page left blank

EXECUTIVE SUMMARY

A suite of tools, including Scribe3D and Blender, were used to model 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 further stress the system, a sabotage scenario was designed to cause a release from the argon hot cell. Additionally, an insider/outsider collusion scenario was designed such that an insider would stash material over time and then move it to a more advantageous position for outsider theft.

To understand the security performance of the system design, a vulnerability assessment was performed across all three attack scenarios. Using a threat spectrum (4/5/6/7/8 adversaries), the scenarios were modeled to test the system. The baseline design was able to achieve very high detection and assessment and adequate delay in order to achieve a probability of interruption of 0.99 across all scenarios. Utilizing a containment strategy, the baseline is able to keep material from being stolen from the EChem facility design 75% of the time or greater 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 (DBT)

in order to secure system effectiveness. However, for theft with insider assistance and sabotage, system performance was much lower. Various upgrade packages were designed to increase performance across all scenarios. Figure 2 and Figure 3 show how performance improved across each upgrade package. Several low-cost upgrades, adding mantraps and shifting response strategy (Upgrade 1), and moving exterior patrols to the interior of the facility (Upgrade 2) made major improvements, as can be seen in Upgrade 1 and 2 results. More extreme upgrades such as extending detection beyond the site perimeter, transit impeding landscaping, and hardened fighting positions at key access points make Upgrade 3 a formidable task for even the largest threat group studied. For Upgrade 3, system effectiveness was 90% or greater across all scenarios and threat configurations. This study provides a spectrum of design features, which if incorporated early in the design phase should be effective in improving security in a cost-effective manner.

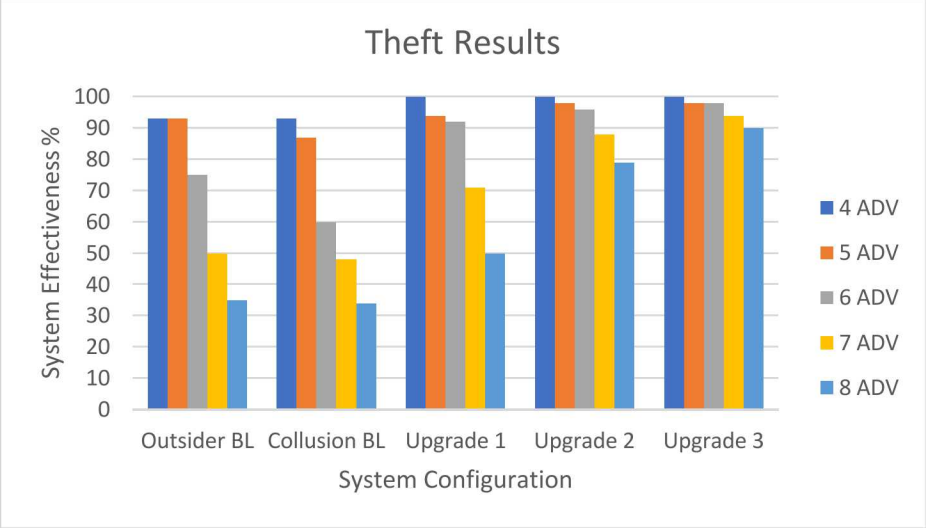

Figure 2. Theft Results Summary

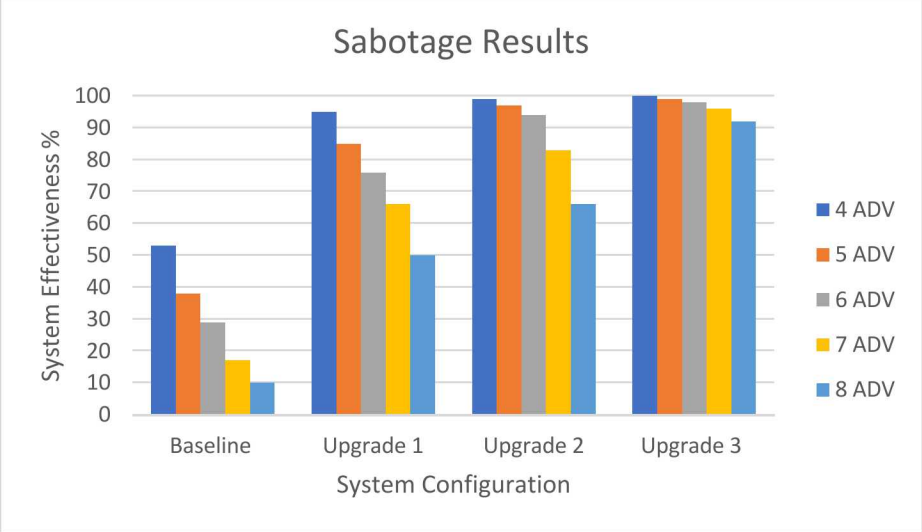

Figure 3. Sabotage Scenario Upgrade Results

ACRONYMS AND DEFINITIONS

Abbreviation	Definition
AC&D	Alarm Control and Display System
ADV	Adversary
CAS	Central Alarm Station
CAT-I	Category I
C/S	Containment/Surveillance
DA	Destructive Analysis
DBT	Design basis threat
DEPO	Design and Evaluation Process Outline
DMA	Deliberate motion algorithm
DOE	Department of Energy
EASI	Estiamate of Adversary Squence Interruption
ECP	Entry control point
ER	Electrorefiner
EMX	Emergency exit
FP	Fission Products
FOV	Field of view
IAEA	International Atomic Energy Agency
IED	Improvised explosive device
KIA	Killed in action
LCC	Liquid Cadmium Cathode
LEU	Low-enriched uranium
LLEA	Local Law Enforcement Agency
MBA	Material Balance Area
MC&A	Material Control & Accountability
MGs	Machine guns
MIR	Material Inspection Room
MOU	Memorandum of Understanding
M&P	Military and Police
MPACT	Material Protection, Accounting, and Control Technologies
MT	Metric Tons
MTR	Material Transfer Room
MUF	Material Unaccounted For
MVP	Most vulnerable paths

Abbreviation	Definition
NDA	Non-Destructive Analysis
NE	Office of Nuclear Energy
NRC	Nuclear Regulatory Commission
PDP	Probable detection point
PIDAS	Perimeter intrustion detection and assessment system
P_E	System effectiveness
P_I	Probability of interruption
P_N	Probability of neutralization
PPS	Physical Protection System
RF	Response Force
RFT	Response force time
RPG	Rocket propelled grenade
SBD	Security by design
SME	Subject matter expert
SNF	Spent Nuclear Fuel
SNL	Sandia National Laboratories
SNM	Special nuclear material
SSBD	Safeguards and Security by Design
SSPM	Separation and Safeguards Performance Model
STAGE	Scenario Toolkit and Generation Environment
SWAT	Special Weapons and Tactics
TRU	Transuranics
USG	United States Government
U/TRU	Uranium/Transuranics
VA	Vulnerability assessment

1. INTRODUCTION

Nuclear facilities in the U.S. face stringent requirements for security, particularly for facilities that process highly 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 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 under 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 site layout model. Next, the physical protection elements are described. Finally, multiple scenarios are presented with results. Building on the work conducted in 2019, This report describes the detailed analysis and design work that results in multiple PPS design packages created to fully optimize the site PPS.

1.1. Background

1.2. MPACT 2020 Milestone

The MPACT campaign is working toward the goal of developing and demonstrating the next generation of SSBD for future civilian nuclear facilities. The 2020 milestone is developing a Virtual Facility Distributed Test Bed that 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.

Error! Reference source not found. shows the Virtual Test Bed Concept. There are three 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. The security modeling work described in this report is the last modeling component and is used to design and analyze a PPS. A 3D facility model is used for the plant layout. 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 built with 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.

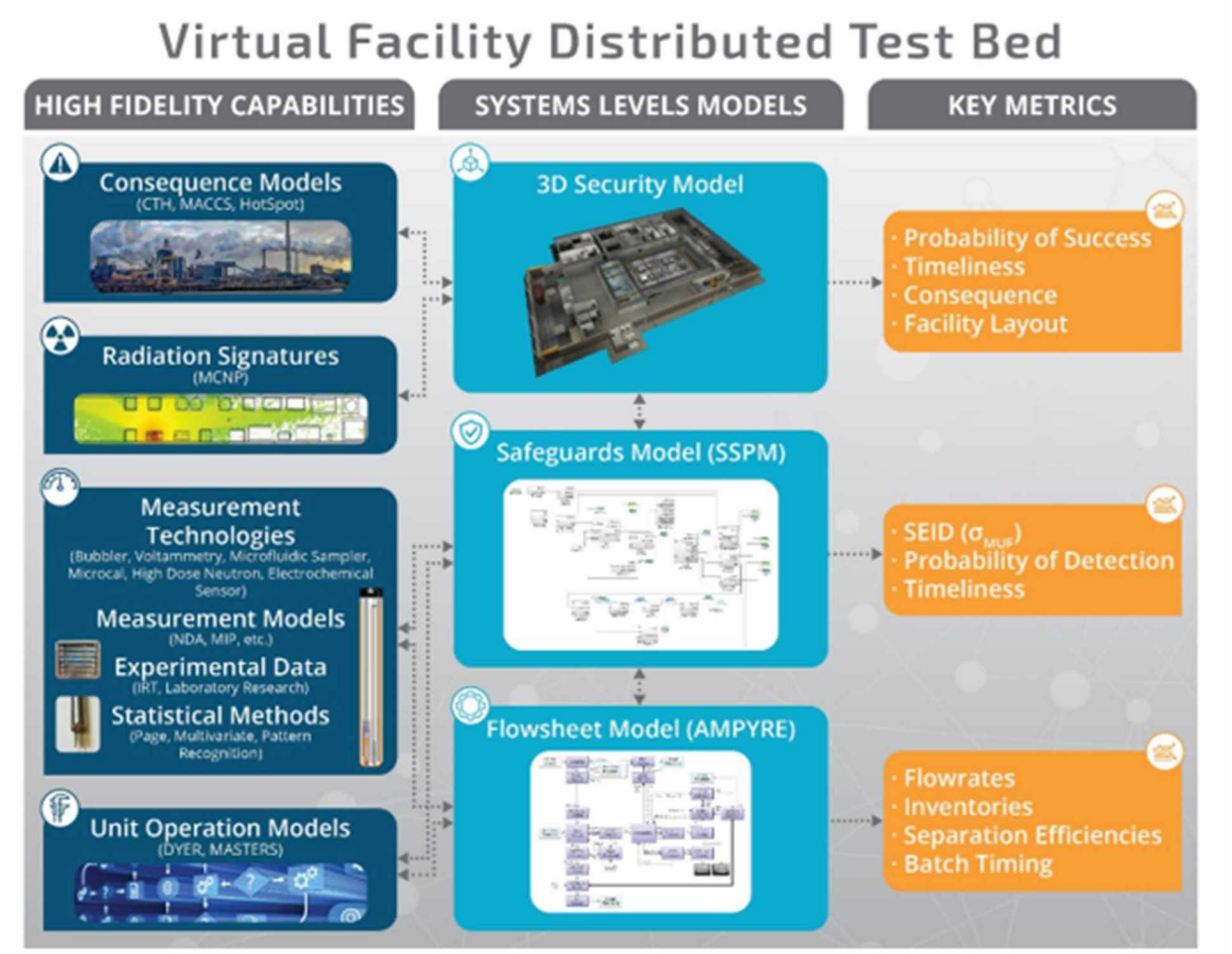

Figure 4. Virtual Facility Distributed Test Bed

The security model was developed in 2018-2019 based on the generic flowsheet and safeguards model. Preliminary security designs were implemented and tested against example attack scenarios. In FY20 the analyses were formalized more to develop an optimal security design and provide the results of the analysis against a variety of attack scenarios.

1.3. Electrochemical Facility Design References

The generic electrochemical facility design was based on references [5] and [6]. 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 (SMEs) 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 5. 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. These operations occur in the air hot cell in Material Balance Area (MBA) 1. 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 (MBA 2). 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 0 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.

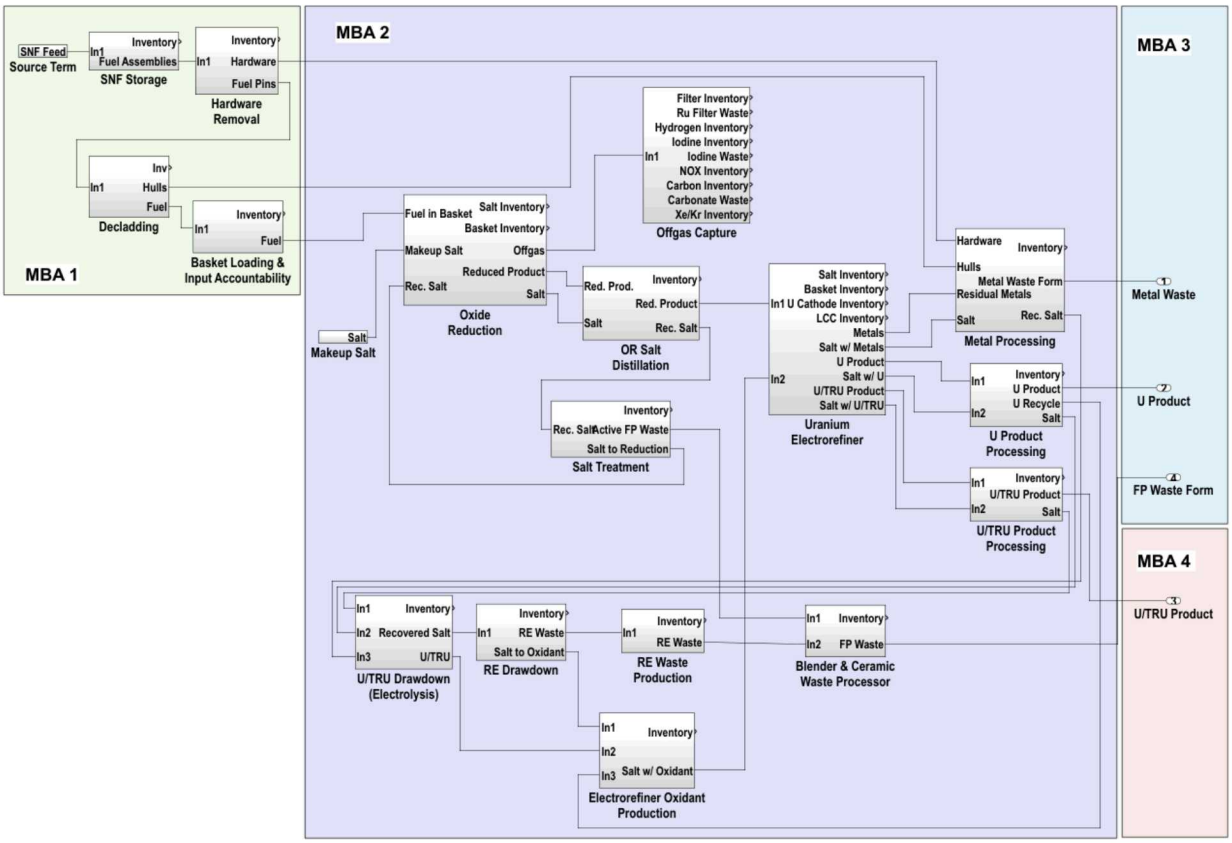

Figure 5. Electrochemical Flowsheet [6]

Page left blank

2. PPS DESIGN PROCESS

In the physical protection world, DEPO (Design and Evaluation Process Outline) has been used for several decades for the design of a PPS [1]. The DEPO process is shown in Figure 6. 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 addition that has been made to the original DEPO process is to include Security by Design (SBD) recommendations. This means not just adding more guns, guards, and gates, but developing optimized PPS designs that may request changes to the facility or process design early in the design process. The PPS design will be iterated until satisfactory results (from performance tests) are obtained.

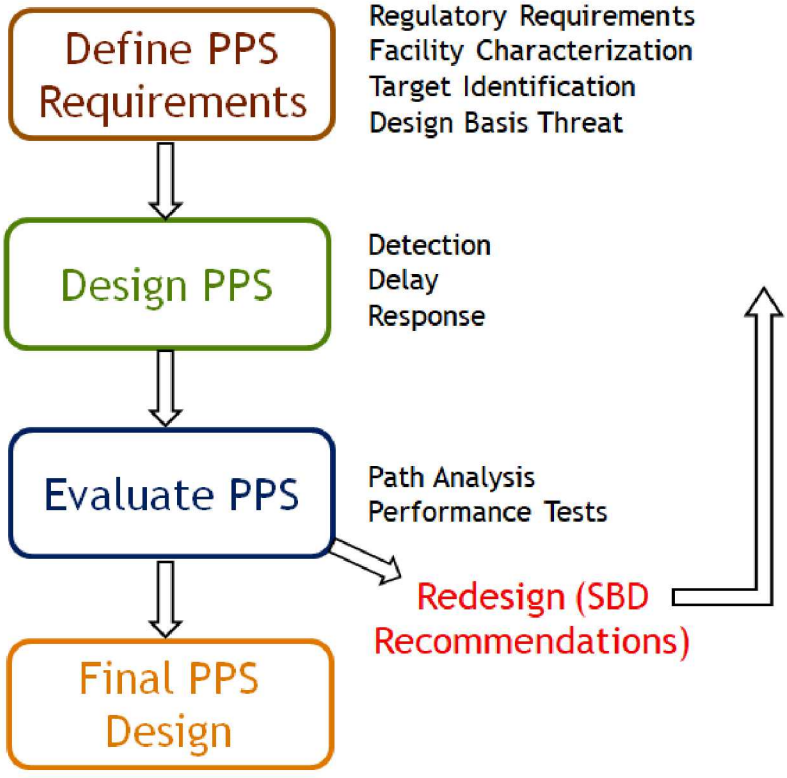

Figure 6. DEPO Process [1]

Page left blank

3. 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 [2]. 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 two 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 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, among others

For this facility, the goal was to design an effective system without use of a PIDAS. The PIDAS of a facility is generally the single most expensive piece of security infrastructure, so achieving desired effectiveness without a PIDAS should reduce security costs during construction, and over the lifetime of the site.

The design of the PPS is also heavily informed by the DBT, which can be different for different types of facilities. The DBT defines the adversary threat including number of adversaries, outsider versus insider, capabilities, and equipment. This information is sensitive and so is not included here. The physical protection analysis instead considered a range of outsider threats to develop a general PPS strategy that is robust to the scenarios of interest.

Page left blank

4. OVERVIEW OF VULNERABILITY ASSESSMENT

4.1. Purpose and Objectives of the Assessment

The purpose of this vulnerability assessment (VA) is to estimate the system effectiveness of the site's PPS against the theft and sabotage of nuclear material given a range of threats. To achieve this result, several objectives must be met:

- Identify metrics and define assumptions that form the basis for a vulnerability assessment
- Characterize the current nuclear processes and operations, identify target assets (facilities, items, materials, etc.) that are high-consequence targets, and identify and characterize the existing PPS elements and strategies used to protect these targets at the site
- Evaluate the PPS, estimate its effectiveness against the defined threats, and identify any weaknesses or vulnerabilities in the PPS; estimate the current system effectiveness (reported as a value between 0.0 and 1.0)

The VA examines specific attacks and their effects on site security. Vulnerabilities from both insider and outsider adversaries are assessed.

4.2. Scope of Assessment

This VA is intended to provide the best understanding of the effectiveness of the proposed designs and PPS in preventing the theft of special nuclear material (SNM) from a hypothetical EChem processing facility.

This VA establishes a baseline system effectiveness of the site's PPS under proposed conditions for use as an advisory document when judging the need and extent of possible future PPS upgrades or replacements.

Cyber/control system attack scenarios were not considered for this site. It is expected that a review of this VA, as well as updates, would be required during any subsequent PPS upgrade design reviews or in the case of a higher-level threat.

The threat used for this report covers a spectrum of adversaries and is not meant to replicate that defined by any United States Government (USG) agency.

4.3. VA Process

The evaluation of an existing or proposed 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 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 may vary with the threat. As the threat capability increases, performance of individual security elements or the system may 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 literally been 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:

- Selects a path that exploits vulnerabilities in the system and
- 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.

4.4. Modeling Tools

4.4.1. Blender

Blender is a free and open source 3D creation suite that is widely used throughout the 3D modeling community [7]. 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.

4.4.2. PathTrace © and EASI - Path Analysis Tool

For validation purposes, the Estimate of Adversary Sequence Interruption tool (EASI) was first used for path calculations. EASI is a simple-to-use calculational tool that quantitatively illustrates the effect of changing physical protection parameters along a specific path. The program uses detection, delay, response, and communication values to compute the probability of interruption. However, since EASI is a single path-level model, it is necessary to use another model to observe all possible paths and determine which are the most vulnerable.

PathTrace is a tool that allows a user to explore and analyze entry paths in two dimensions and determine which paths are most vulnerable. 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 the amount of time it would take to breach these barriers, as well as the probability that they would be detected in doing so. The tool allows for the drawing of detection areas (a distinction between areas of a facility where an adversary may walk slower or be detected more easily due to the nature of existing in that area [sensors, patrols, etc.]). Finally, the user may specify the kinds of tools the adversary may be carrying, and their effects on the time to defeat a barrier, as well as their probability of detection. Once the user has mapped out the entire facility, they can analyze the entry paths into the facility with a variety of methods, given the PPS Response Force Time (RFT) and an Adversarial Strategy. The user will receive data visually or textually representing the:

- Adversarial task time
- Total probability of detection
- Critical detection point
- Time after the critical detection point
- Probability of interruption
- Probability of detection, delay, and defeat time of every barrier
- Detection area that the adversary has encountered

The final data allows the user to fully explore their facility and any potential vulnerabilities in a simple fashion.

4.4.3. Scribe3D© – Tabletop Recorder and Automated Tabletop Data Tool

Scribe3D© is a 3D tabletop recording and scenario visualization software created by Sandia National Laboratories (SNL). It was developed for use by other National Laboratories, government organizations, and international partners [8]. 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 [8].

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 Scribe3D© 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.

4.5. 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 response force (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, analysis is conducted conservatively with the advantage weighted toward the adversary
- Adversaries and RF are assumed to be equal with regard to training and combat ability
- Adversaries are willing to die to achieve their mission
- RF strategy is containment only

5. ELECTROCHEMICAL FACILITY DESIGN AND OPERATIONS

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

The electrochemical processing building is protected by a robust PPS 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 of 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.

5.1. Processing Level

The main processing level includes the high bay for shipping and receiving, air and argon hot cells, control room, entry control point (ECP), and central alarm station (CAS). Additional rooms are included to support various facility needs (office space, locker rooms, meeting rooms, etc.) Figure 7 shows an overhead view of the main processing level, and Figure 8 shows the 3D view.

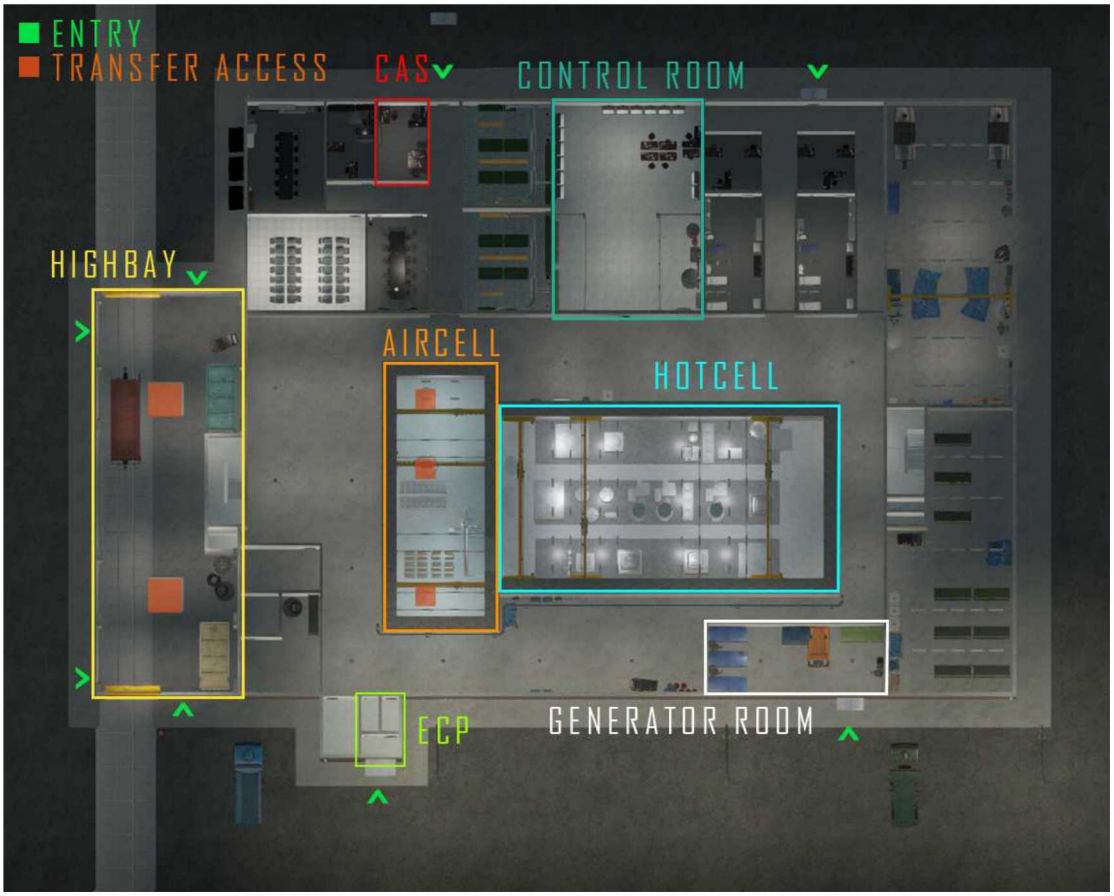

Figure 7. Processing Level Facility Overview

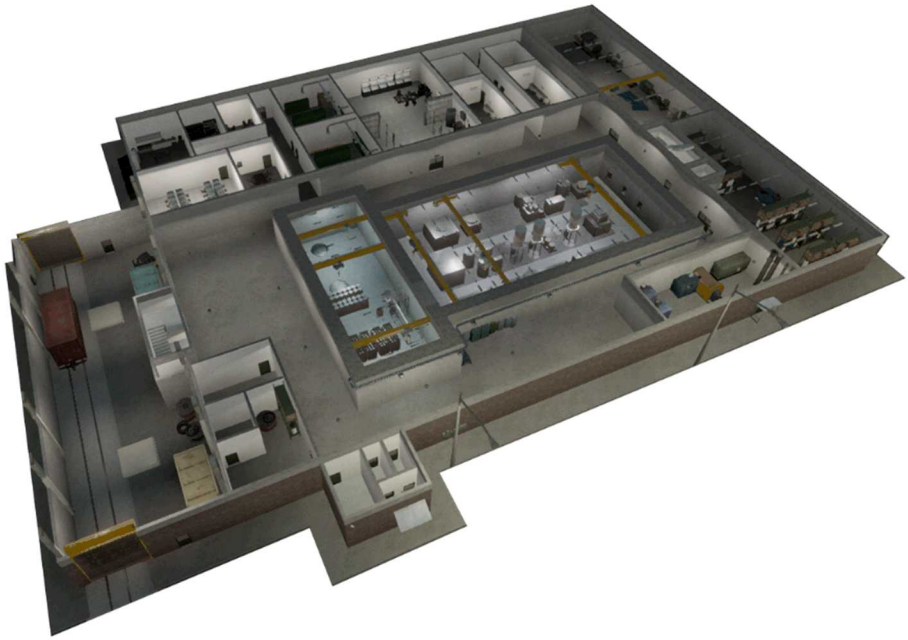

Figure 8. Processing Level facility 3D Model – Blender Screenshot

5.1.1. High-Bay

The high bay area (see Figure 9) 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 9. High Bay Area

5.1.2. 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 that will be used for electrorefining operations. At some point while in the air cell, the spent fuel will be measured for input accountancy.

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 10 shows an overhead view of the hot cells and an internal view of the air cell (upper left) and argon cell (upper right).

Figure 10. Air and Argon Hot Cells

5.1.3. Control Room

The control room (see Figure 11) 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 use 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 11. Control Room

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

The CAS contains the alarm control and display system (AC&D). All alarms and camera feeds are monitored here. A two-person RF 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 given time (see Section 6).

The personnel 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 mantrap, personnel present credentials, and only once verified, are they allowed entry or exit. Ingress traffic is checked for metal via metal detection portals. Egress traffic is checked for SNM. Figure 12 shows both the CAS and the ECP, and the ECP security layout is captured in Figure 13.

Figure 12. CAS (left) and ECP (right)

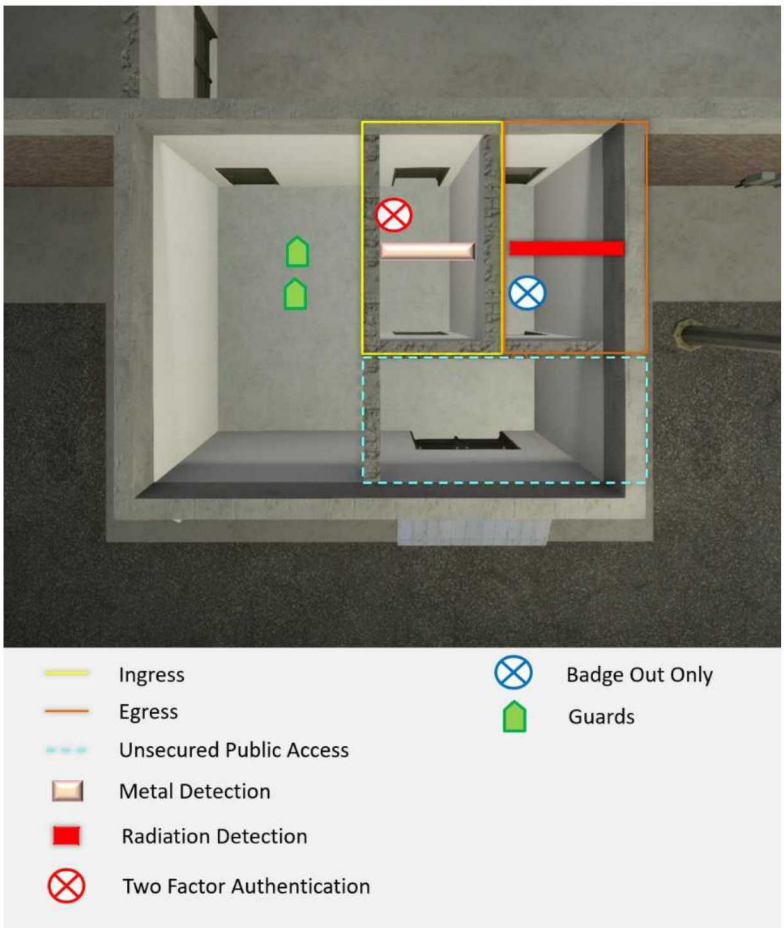

Figure 13. ECP Security Layout

5.1.5. Server Room/Warehouse/Storage/Machine Shop

Other facilities included on the processing floor are the server room, warehouse, machine shop, and storage areas. Figure 14shows 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 14. Warehouse (left), Machine Shop (upper right), and Server Room (lower right)

5.2. 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 15 shows an overview of the basement, and Figure 16 shows a 3D view.

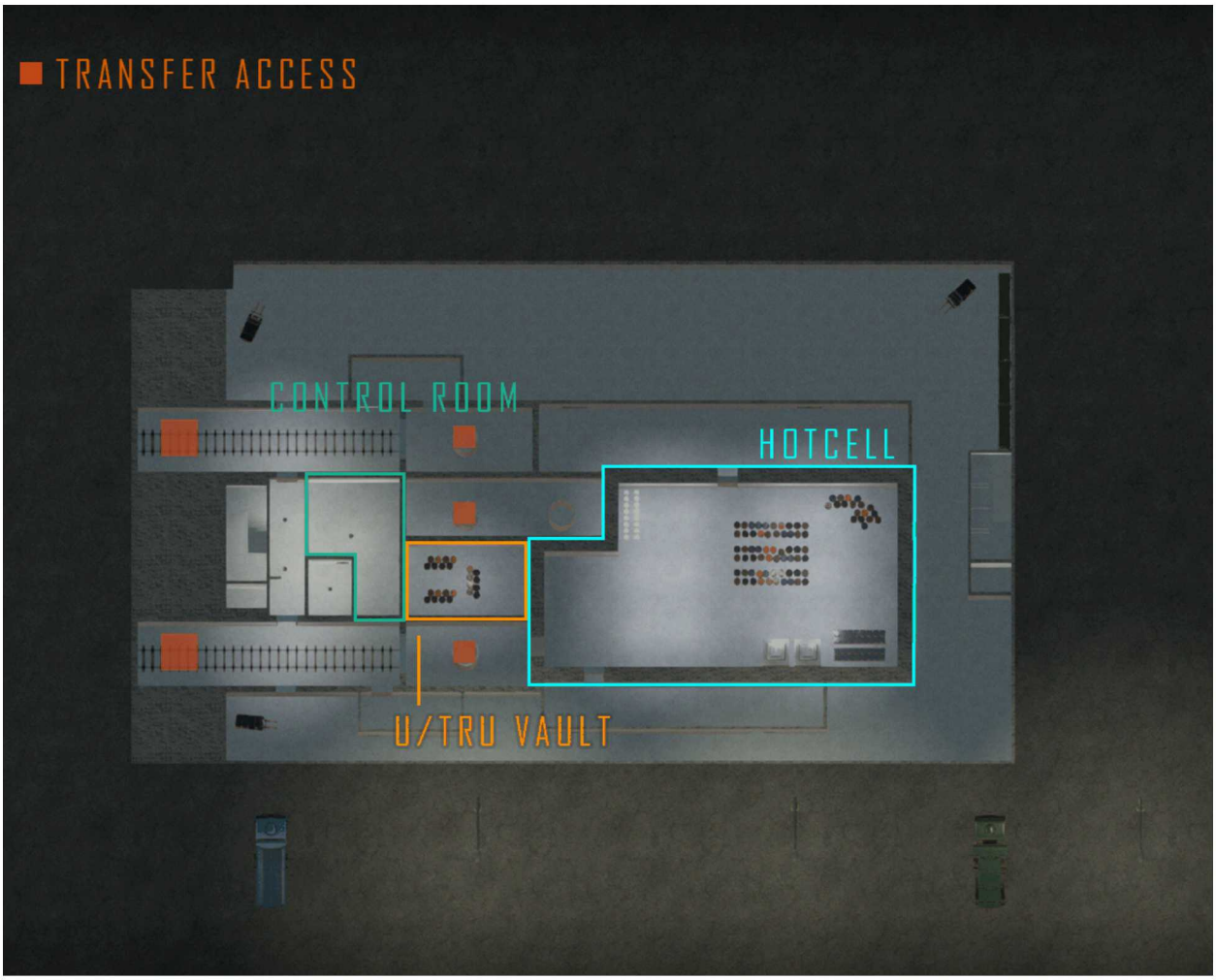

Figure 15. Basement Level Facility Overview

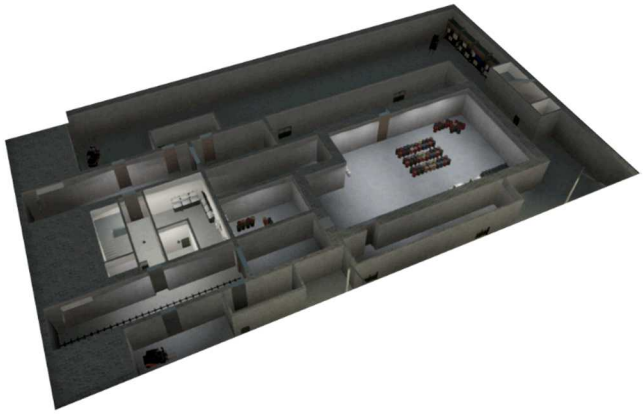

Figure 16. Basement Level 3D Model

5.2.1. 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 is the most attractive. 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 17. U/TRU Vault (right) and Vault Control Room (left)

5.2.2. 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 18 shows pictures of the basement area (left) and transfer tunnel (right).

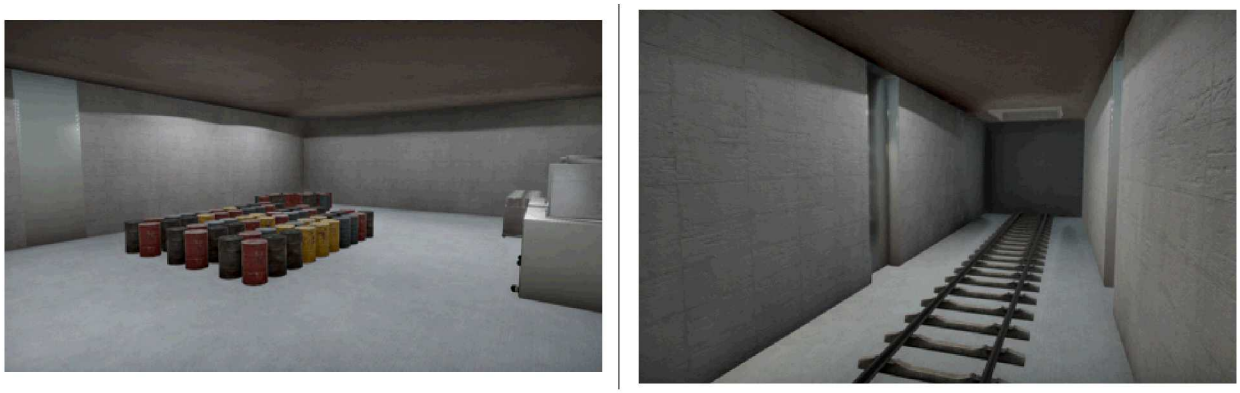

Figure 18. Basement Transfer Tunnels

5.3. 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 19 shows a top-level view of the top floor, and Figure 20 shows a 3D view.

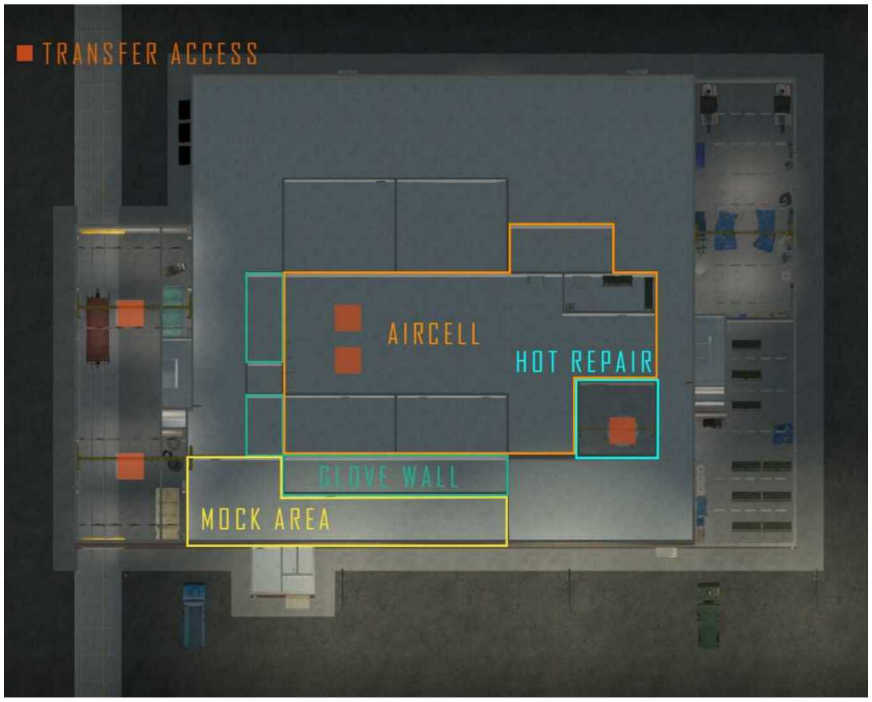

Figure 19. Top Level Facility Overview

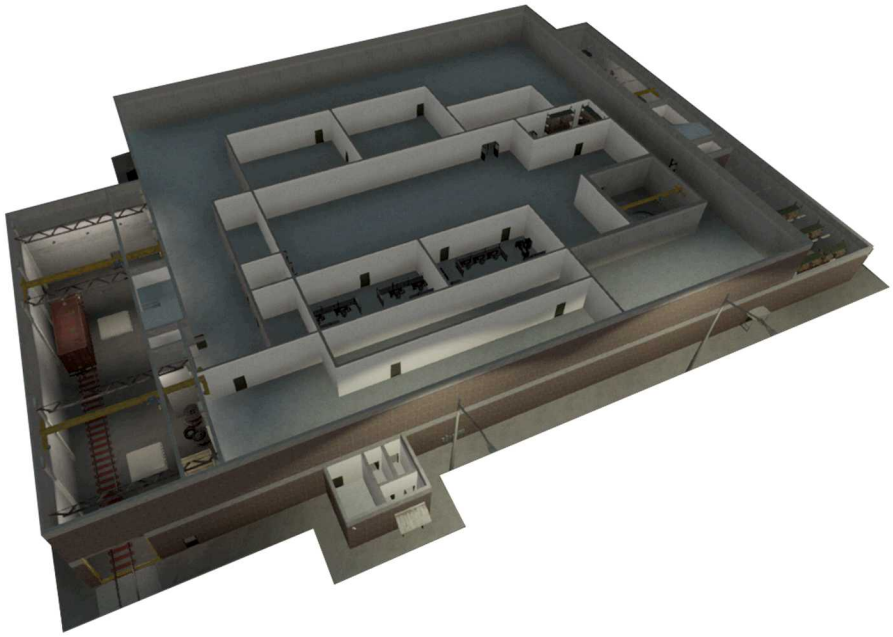

Figure 20. Top Level 3D Model

5.3.1. 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 RF personnel. Figure 21 shows the hot repair area with transfer hatch.

Figure 21. Hot Repair Area

Page left blank

6. TARGET CHARACTERIZATION

6.1. Target Identification and Quantities

Based on the generic electrochemical processing facility design, the following describes the targets and target locations of interest for the VA. These targets consider both theft and sabotage.

6.1.1. Spent Nuclear Fuel

Spent fuel exists in multiple forms throughout the process and will be contained in various locations. Fuel assemblies will arrive on-site in the main processing building and are transferred into the air hot cell for storage. When an assembly begins to be processed, it is disassembled, declad, and chopped or shredded. The shredded fuel is placed in porous metal baskets and then awaits transfer into the argon hot cell to begin the electrorefining process. Compensatory measures will likely be in place during shipment and transfers. Thus, the spent fuel is either contained as whole assemblies, within process units as it is being declad, or in the porous baskets in the air and argon hot cell. The hot cells contain a number of inherent security features due to the thick walls and limited number of penetrations. Fuel assemblies and shredded fuel are not as attractive since they contain fissionable fuel in a dilute form, and fuel assemblies are difficult to move. Once inside the processing cell, the oxide fuel is a much less attractive target than other material contained within the cell.

Quantities: 4-5 kg of Pu per fuel assembly (solid, item form, roughly 500 kg per assembly) and 4-5 kg of Pu per basket (shredded/powder form, roughly 500 kg bulk mass per batch).

6.1.2. Oxide Reduction

The spent fuel in baskets is typically transferred into an argon hot cell for all remaining electrorefiner operations. The processing cell provides a significant barrier to theft of material due to the thickness of the walls for radiation shielding, the argon environment, and the high radiation environment. The spent fuel is no more attractive in oxide reduction as compared to earlier in the process. Once processing begins, the material is contaminated with salt that contains active fission products, so the attractiveness of the material for theft would further decrease. The salt does not contain actinides during normal operations. Therefore, this area does not contain attractive theft targets. The OR salt contains significant radioactivity due to the collection of active metal fission products (like Cs), so this salt could be a sabotage target.

Quantities: 4-5 kg of Pu per basket (shredded/powder form, roughly 500 kg bulk mass per batch).

6.1.3. Electrorefiner

The electrorefiner salt contains larger quantities of Pu, depending on the time during the cycle. However, the actinides are fairly diluted in the salt. Roughly 35kg of Pu and 70 kg of U may be contained in approximately 9,000 kg of salt. Thus, it would take a diversion of about 2,000 kg of ER salt in order to remove one IAEA-significant quantity (8 kg) of Pu. The U cathode contains large amounts of depleted U. The U/TRU cathode (liquid cadmium cathode) contains the concentrated product. All these materials are in a difficult form to remove and would require significantly altered operations in order to remove material. Due to the protections of the hot cell, the likely numerous safeguards in place around the electrorefiner, and the molten form of the material, the material in this location would be very difficult to steal for an outsider adversary. The ER salt also contains significant radioactivity from the buildup of fission products, so the processing unit could be a sabotage target.

Quantities: Pu content in the salt: 35 kg total per 9000 kg salt.

6.1.4. Uranium Metal Product

The uranium dendrites are scraped from the cathode outside of the ER vessel. The dendrite material has salt entrained on it and contains only low-enriched uranium (LEU), so this material would not be an attractive theft target. After distillation and forming of the uranium product, the ingots are likely to be transferred to another building for storage. Due to the metallic form and limited radioactivity, it also would not make an attractive target for radiological sabotage after the ingots are removed from the hot cell.

Quantities: Pu content negligible, 40-50 kg of U per ingot.

6.1.5. U/TRU Metal Product

The U/TRU extraction on the liquid cadmium cathode goes through distillation to remove the salt and cadmium. The U/TRU ingot is produced in the processing cell and then will be transferred to a storage vault in the basement level of the facility for storage for future use. This is the most attractive material for theft in the facility due to the presence of Pu. Theft of the product while in the processing cell seems less likely due to the barriers of the hot cell. Theft during a transfer of material out of the hot cell (depending on the design) seems more likely since the environment will be easier to deal with. Any U/TRU storage will need to be adequately protected from theft. In addition, radiological sabotage should be considered since criticality is a possibility.

The U/TRU product was found to be the 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, removal of the material from the TRU storage vault was the analyzed pathway.

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, they 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.

Quantities: 4-5 kg of Pu per ingot.

6.1.6. Noble Metal, Cladding, and Fission Product Wastes

The various waste products from the process all contain little or no actinides, so they are not attractive from a theft standpoint. Some could potentially be stolen for use in a dirty bomb or be the target of radiological sabotage, so that should be considered in a PPS design. It should be noted that biological dose rates from radiological sabotage are dominated by the presence of actinides, so the

limited actinide content will lead to poor sabotage targets. However, any dispersal of radioactive material on a site would lead to considerable economic impact, regardless of the actual dose to the public. After the waste forms are generated, the wastes are likely to be removed from the main process building and stored below ground in a co-located facility on-site.

Quantities: Negligible Pu content, but kg quantities of radioactive fission products.

6.1.7. Backup Generator

The electrorefining process requires power to keep the systems operational, in particular to keep the salt molten should the facility loose grid power. This may be important both for safety and for protecting the equipment in the plant. Complete loss of power likely would not lead to a potential radioactivity release, but it would have an economic consequence for the operator due to loss of equipment and extended downtime. The generator will be considered a vital area for these reasons so adversary attack could be considered.

Page left blank

7. FACILITY PHYSICAL SECURITY SYSTEM

The proposed system was first created with physical security best practices in mind, but with an emphasis on the reduction of security costs. An initial system was designed, and then tested against a range of threats in both theft and sabotage settings. Based on the results of the analysis, upgrades were designed to approve system performance. Section 7 describes the baseline system, and its underlying assumptions and philosophy.

7.1. PPS Overview

A major cost for most Category I (CAT-I) facilities is a PIDAS. An initial goal of the baseline PPS was to eliminate the need for a PIDAS and establish the skin of the building as the site first line of detection. Though required by NRC Regulation 10 CFR 73, this effort seeks to reduce security costs wherever possible, and the PIDAS is the most costly feature present at most sites, outside of manpower.

7.1.1. Perimeter Physical Security System

The processing facility features a single passive fence for limiting public access 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 system cost as much as possible while still providing a robust protection from theft and sabotage. The typical use of a two-fence PIDAS is likely not needed since all the material of concern is located inside one building. The building exterior acts as a 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.

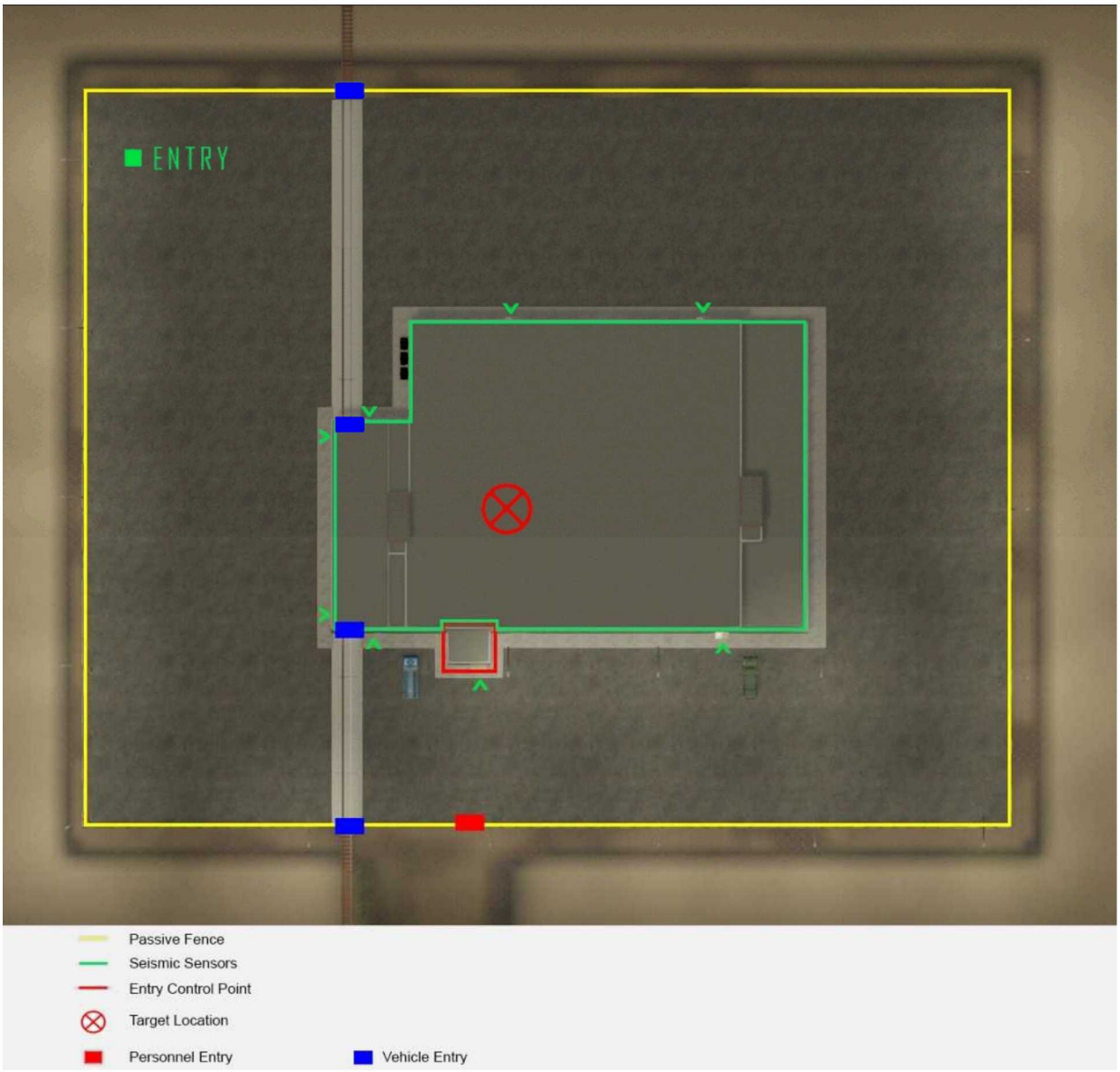

Figure 22. Building Exterior Security Features

7.1.2. Entry Control Point

The ECP 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.

7.1.3. Facility Interior Security System Design

The interior physical security system for the processing level is characterized in Figure 23. As mentioned above, all exterior doors are protected with magnetic locks and balanced magnetic switches and are assessed by dedicated camera systems. Interior doors that 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 24. 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 25. Main areas of concern are the secondary alarm station (SAS)/RF room. Other sensitive areas include the hot maintenance area, due to safety concerns.

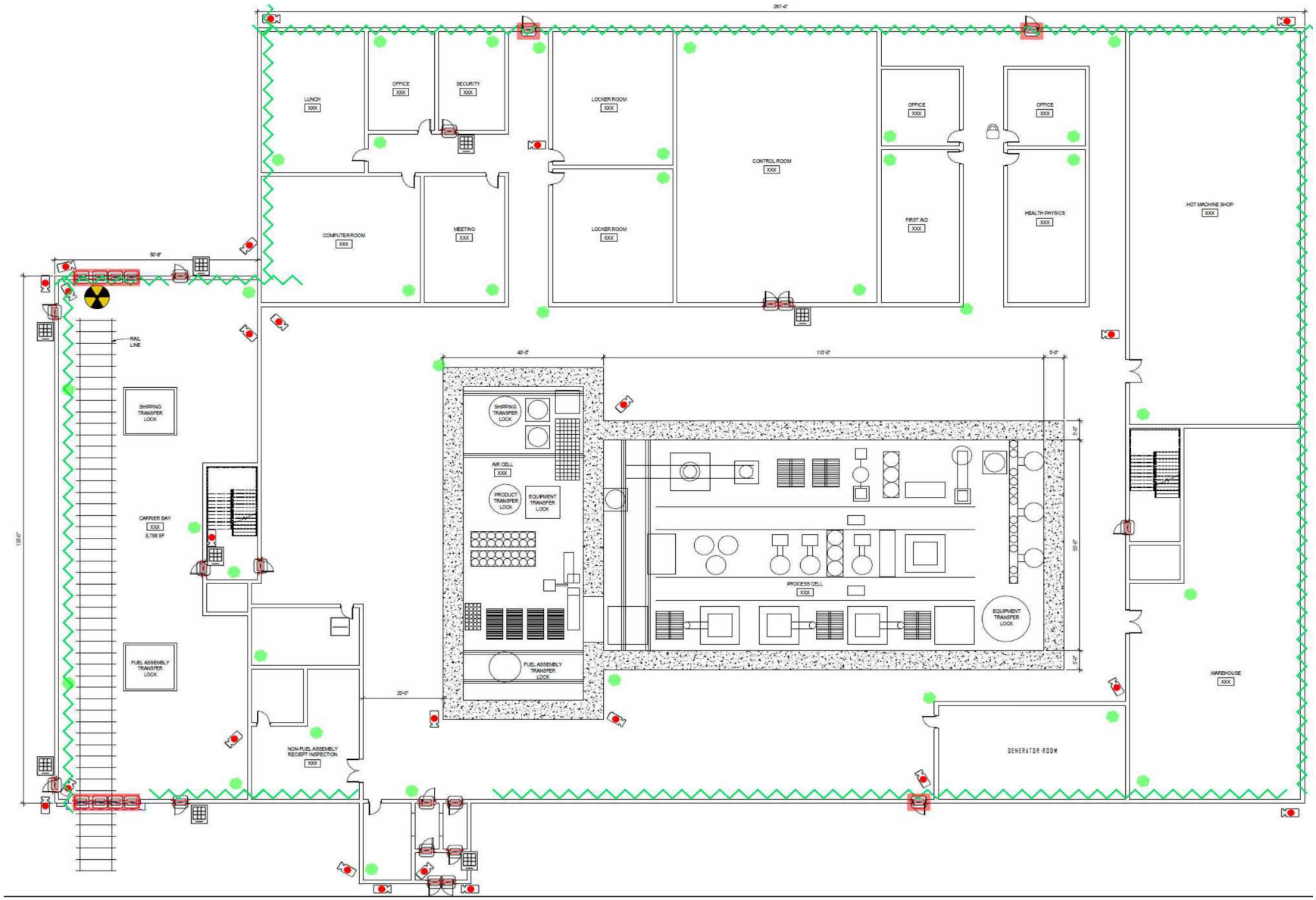

Figure 23. EChem Processing Building, Operating Floor, and Conceptual PPS Design Layout

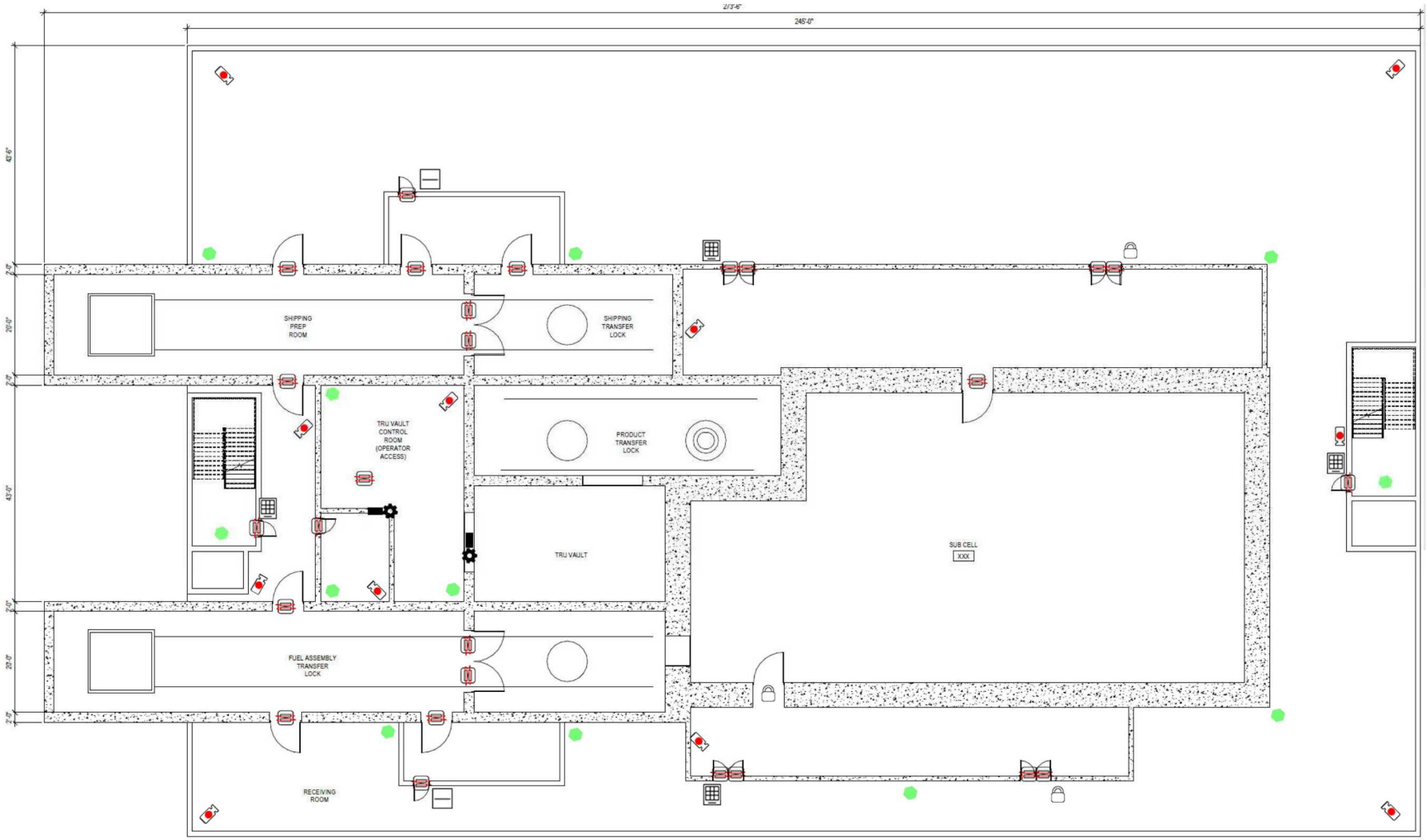

Figure 24: EChem Processing Building, Basement Level, and Conceptual PPS Design Layout

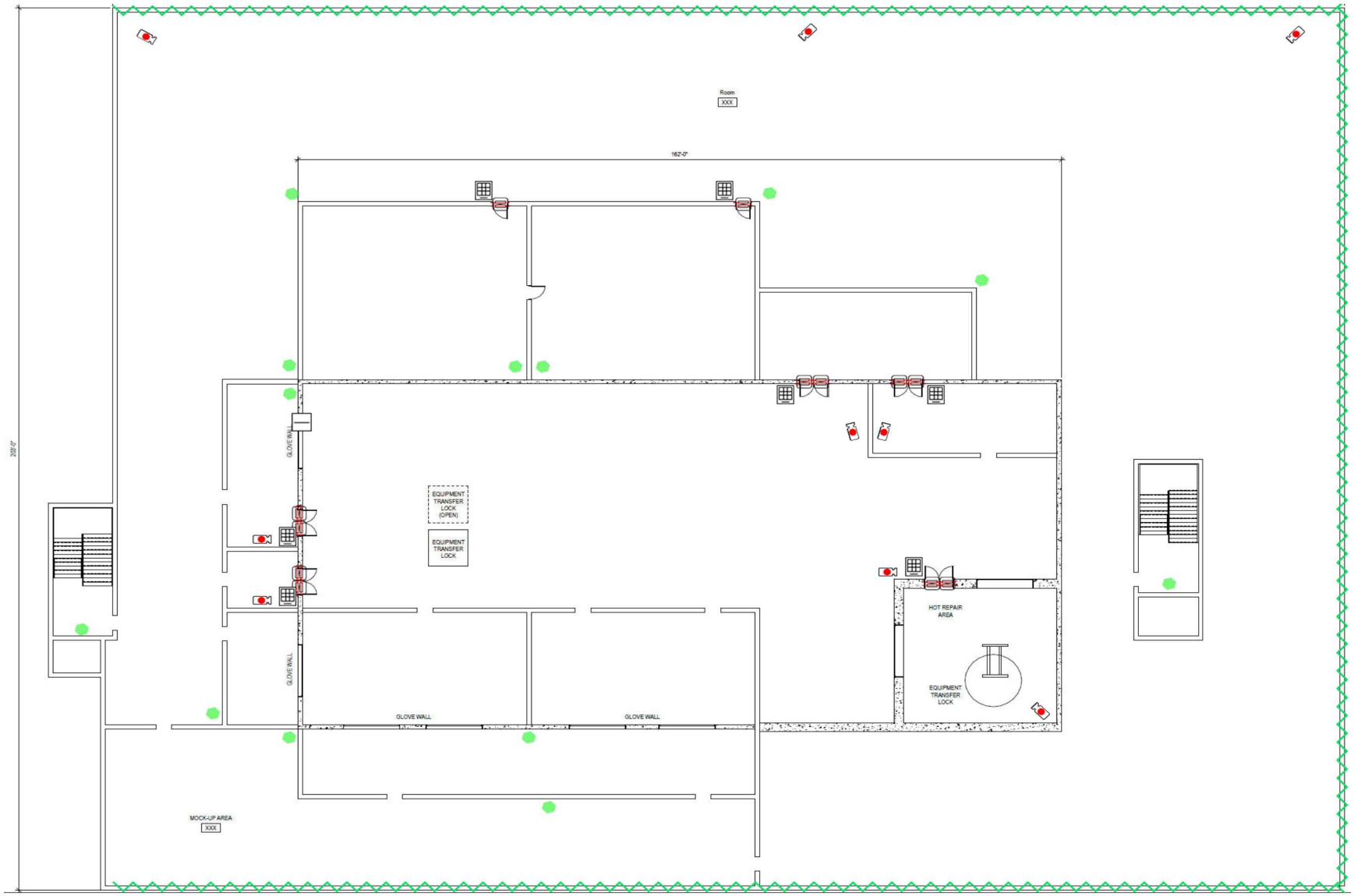

Figure 25: EChem Processing Building, Hot Repair Area, and Conceptual PPS Design Layout

Table 1. Detail and Legend for Figure 23 through Figure 25

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 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:	

Sub-Task	System/ Comp Type	Description / Requirement	Team Notes
		• Upon entry, the entry turnstile will be unlocked by a 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	

7.2. Response Force

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, 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 may be necessary to use in the event of an adversary attack. Weaponry and equipment may include, but is 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.

7.2.1. Response Force Assumptions

Given the current status of the facility design, little is established regarding the RF 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 two-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. After initial detection, a 30-second alarm assessment and communication time occurs before the RF muster times 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.

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 26 shows the positions of the RF at the beginning of the scenario.

Figure 26. Response Force Starting Locations

7.2.2. 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 CAS. The primary functions of the CAS include:

- Oversight of all security-related emergency activities and support
- Responsible to maintain protection of all onsite nuclear material
- 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 communication with the Command and Control Center

8. THREAT SPECTRUM

The concept of the 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 CAT-I facility, and therefore warrants the use of a high-level outsider threat. Outsider adversary groups differ in their capabilities to defeat a PPS. For the current analysis, it is assumed that an insider is providing facility knowledge for the outsider threat group.

8.1. Varied Threat

To test a broader threat landscape, a threat spectrum was used. Numbers of attackers were varied from four to eight.

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, commercial and military explosives (assume sufficient amounts to complete objective)
	Tools	Hand tools, power tools, bridging/breaching equipment, chains, ladders, ropes, cutting torches, radios, 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	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
	Insider Collusion	Planning, local cell structure, safe-havens, sympathetic population, logistics
	Support Structure	One passive insider providing information; active non-violent placing material in a more advantageous location

8.2. 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 a 7.62 mm rifle, or 7.62 mm 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.])
- Access to two four-wheel drive vehicles in scenarios involving vehicles
- 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 RF element (e.g., roving patrol) was within visual range of the initial breach. They would also avoid hardened and manned response positions, if possible.

9. VULNERABILITY ANALYSIS OF FACILITY DESIGN

Vulnerability assessment (VA) results are based on an analysis of the physical paths that the adversary follows to achieve their 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 and mitigate the system's greatest vulnerabilities to theft.

9.1. 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 the dedicated RF 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).

9.2. 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 on a reliable detection technology component rather than detection by guards (because of the human factor).

9.3. Adversary Task Times

Non-sensitive data was used for all door and fence breaches. For the detailed breaches, data was summed across steps so as to not 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 eight seconds, then the minimum task time is four seconds, and the maximum is 12 seconds.

9.4. Delay Focused Design Features – U/TRU Vault

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 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, it was determined that the 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.

10. ANALYSIS SCENARIO OUTLINE

The following scenarios were studied:

1. Outsider Theft
2. Insider/Outsider Collusion Theft
3. Sabotage

Based on the results of the baseline analysis, upgrades were designed into the system to increase overall system effectiveness to levels greater than or equal to 80%. The upgrades resulted in the following scenario configurations, which will be covered in detail in Section 11 and Section 11.4.5.4:

1. Upgrade 1 – Mantraps at emergency exit doors plus modification to RF behavior
2. Upgrade 2 – Mantraps plus shifting exterior patrol to the building interior
3. Upgrade 3 – Mantraps, interior patrol, plus extended detection, exterior building delay, and hardened positions in probable entry ways

The Outsider Theft scenario presents the lowest threat due to its longer attack timeline; the collusion and sabotage scenarios both have shorter timelines and are harder to defeat. For this reason, upgrade cases were only run against the collusion scenario and the sabotage scenario. This results in the following scenario matrix of 45 individual scenarios:

1. Outsider Theft
    a. Baseline Scenario – Four-to-eight attackers
2. Collusion Theft
    a. Baseline Scenario – Four-to-eight attackers
    b. Upgrade 1 – Four-to-eight attackers
    c. Upgrade 2 – Four-to-eight attackers
    d. Upgrade 3 – Four-to-eight attackers
3. Sabotage
    a. Baseline Scenario – Four-to-eight attackers
    b. Upgrade 1 – Four-to-eight attackers
    c. Upgrade 2 – Four-to-eight attackers
    d. Upgrade 3 – Four-to-eight attackers

Path Analysis is only run against the baseline system for each scenario (outsider theft, collusion theft, and sabotage), because this system produces an extremely high probability of interruption across all scenarios. Therefore, adding upgrades to the system will not improve the probability of interruption, only the probability of neutralization.

Page left blank

11. THEFT ATTACK RESULTS

11.1. Outsider Theft Attack Scenario - Path

The first scenario considered was the outsider theft attack against 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 scenario is captured in story board form in Figure 27.

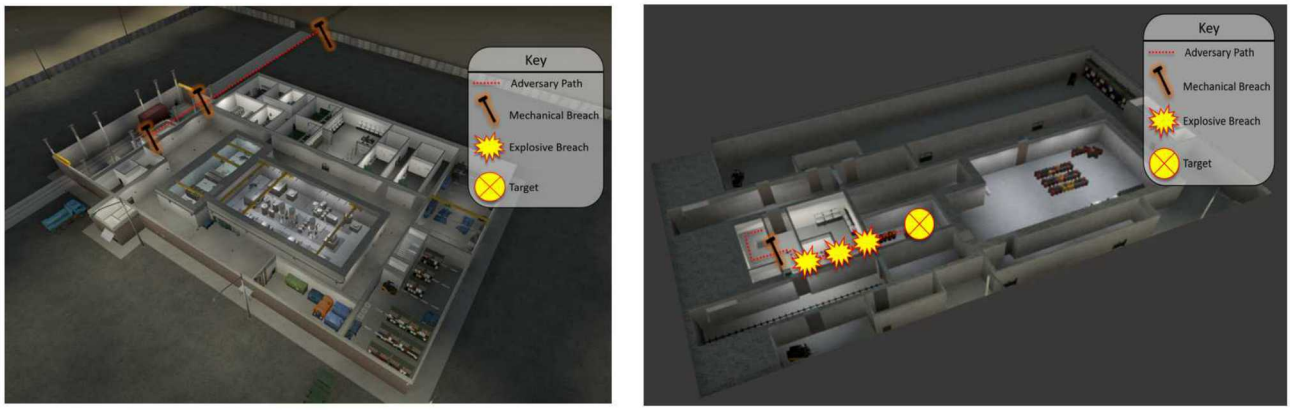

Figure 27. Ground Floor Adversary Attack Path (left) Basement Attack Path (right)

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 (50 m)	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 and 1/8-inch steel back plate) in front of Material Transfer Room (MTR) 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 and 1/8-inch steel back plate) in front of gap in TRU Vault Wall for hoist passage	273^	388
13	Climb step ladder ~10 ft then crawl through square hole ~2 ft x 2 ft	30	418
14	Adversary in Vault receives portable light sources, manual chain hoist, beam clamp, lifting straps & small toolkit through I-beam hole between 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 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 MTR	12.5	898
24	Adversaries exit MIR	12.5	910
	*Critical Detection Point **Total**		(15:10 min)
^Denotes values that are sums of the steps preceding that have " --" for their delay value			

11.1.1. Outsider Theft Path Analysis Results EASI

EASI is a pathway tool where the user specifies a given path, and the spreadsheet calculates P_I along that path. It does not calculate the most vulnerable path. Given that there are two mobile teams on foot patrol in full gear, the RFT is very short. These teams are able to begin moving to response positions within 30 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

				Delays (in Seconds):	Total Time(s)
Task	Description	P(Detection)	Location	Mean:	
1	Breach outer passive fence	0.02	M	30	30
2	Engage foot patrol	0.1	M	10	40
3	Move to building exterior (50 m)	0.02	M	15	55
4	Breach Emergency Exit Door	0.95	E	30	85
5	Move to Stairwell Door	0.8	M	5	90
6	Breach Upper Stairwell	0.8	E	30	120
7	Move down to Lower Stairwell door	0.02	M	15	135
8	Breach Lower Stairwell Door	0.8	E	30	165
9	Move to Basement Hall Door	0.02	M	5	170
10	Breach Basement Hall Door	0.8	E	30	200
11	Move to Vault Door at TRU Vault Control Room	0.02	M	5	205
12	Breach Vault Door	0.8	E	--	--
13	Move to Shield Wall at TRU Vault	0.02	M	--	--
14	Breach Shield Wall at TRU Vault	0.8	E	--	--
15	Move to inner Shield Wall	0.02	M	--	--
16	Breach Inner Shield Wall	0.8	E	273	478
17	Set up and Climb step latter into TRU Vault	0.02	M	--	--
18	Retrieve target material	0.02	M	497	975
19	Exit Site	0.02	M	30	1005
				Total	16:45
	Probability of Interruption:	.99			
	^Denotes values that are sums of the steps preceding that have " --" for their delay value				

11.1.2. Outsider Theft Path Analysis Results PathTrace©

PathTrace was used to validate the results from the timeline path analysis conducted with EASI. Using EASI, the team selected a path manually and built it out, dictating what elements would be crossed to the software. PathTrace examines all possible paths to the target, and then provides the lowest PI path, or the most vulnerable path (MVP). The PathTrace software identified the same path as that used in EASI as most vulnerable. Figure 28 and Figure 29 show the path the adversary takes to the vault. Further, the EASI path P_I and the PathTrace P_I are equivalent at 0.99. The total path timeline was 1,005 seconds for EASI and 1,035 seconds for PathTrace. This 30-second difference is most likely due to travel time differences between the tools. PathTrace measures precise distances the adversary must travel over the path. EASI requires that the analyst measure each distance manually and manually calculate transit time over the path. As a result, the PathTrace results are most likely more accurate.

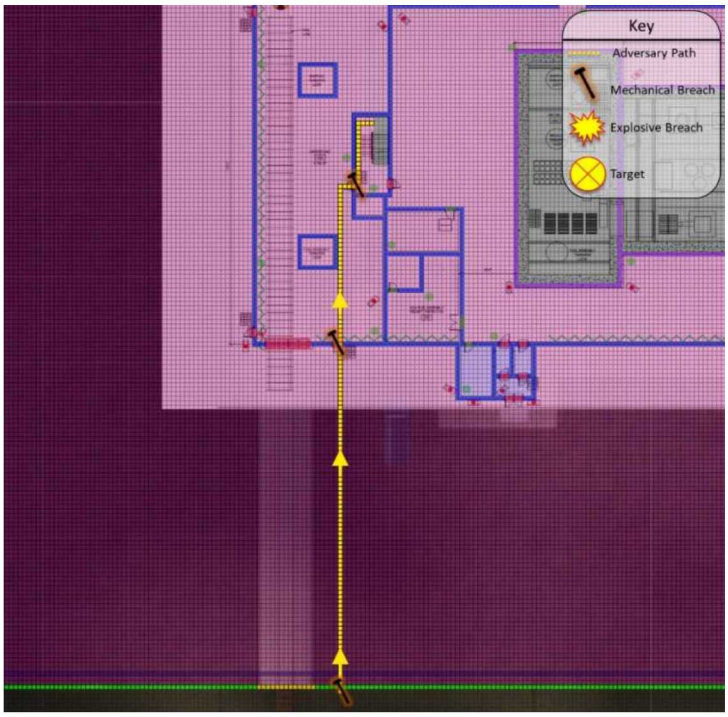

Figure 28 – PathTrace© path on ground floor for Outsider TRU Vault Theft Scenario

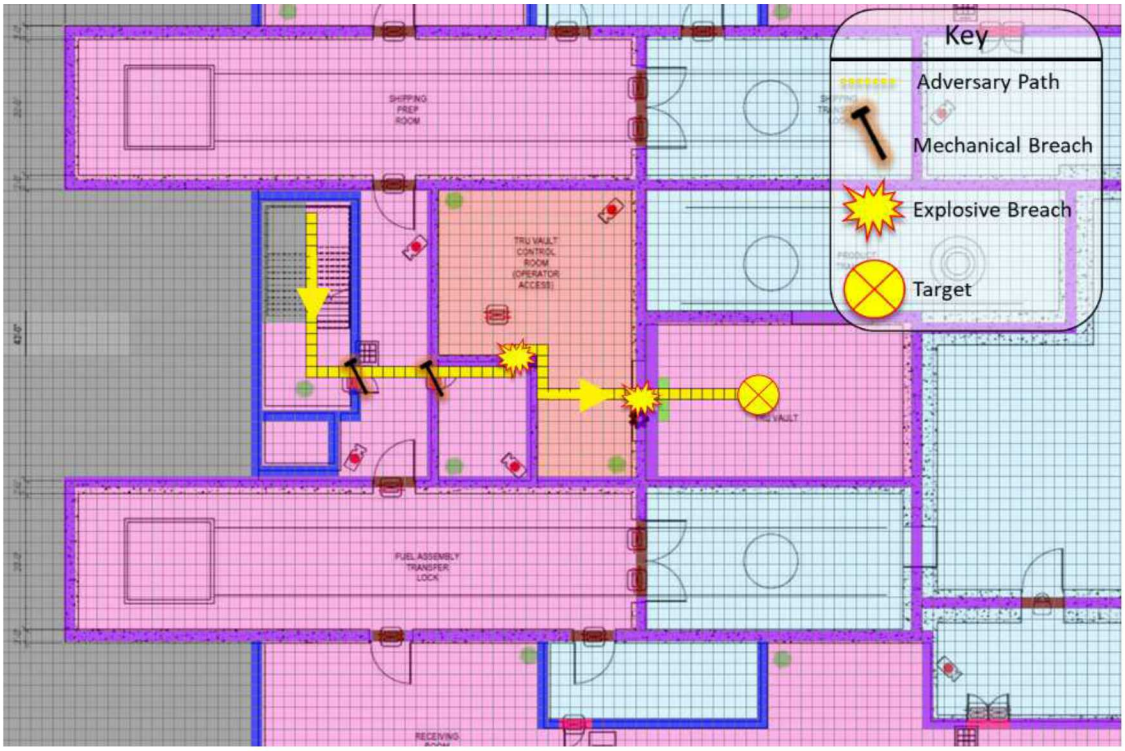

Figure 29 – PathTrace© path in basement for Outsider TRU Vault Theft Scenario

11.1.3. PathTrace Theft Path Analysis Results Discussion

Table 6 shows that the adversary is interrupted at an extremely high rate (P_I =.99). Total scenario time is 1,035 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 6. PathTrace Probability of Interruption Results

Task	Description	P(Detection)	Delay (mean seconds)	Task End Time (seconds)
1	Breach outer passive fence	0.02	30	30
2	Engage foot patrol	0.02	10	40
3	Move to building exterior (50m)	0.02	11.94	51.94
4	Breach Emergency Exit Door	0.8	30	81.94
5	Move to Stairwell Door	0.02	5.96	87.9
6	Breach Upper Stairwell	0.8	30	117.9
7	Move down to Lower Stairwell door	0.02	5.54	123.4
8	Breach Lower Stairwell Door	0.8	30	153.4
9	Move to Basement Hall Door	0.02	0.99	154.4
10	Breach Basement Hall Door	0.8	30	184.4
11	Move to Vault Door at TRU Vault Control Room	0.02		
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	286^	470.4
16	Set up and Climb step latter into TRU Vault	0.02	30	500.4
17	Move to Target Material	0.02	1.32	501.8
18	Retrieve Target Material	0.02	468	969.8
19	Exit Site	0.02	65.33	1035
	Probability of Interruption:	.99		

^Indicates combined step times

11.2. Theft PN Analysis Simulation and Analysis Overview

A simplistic simulation was conducted in Scribe3D© in order to gauge the rough effectiveness of the process site interior response teams. 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.

11.2.1. Response Force Win Criteria

At the end of each simulation, an RF win is awarded in the event the adversary is unable to successfully complete their theft objective due to attrition of adversary personnel and/or lack of

required equipment to complete necessary breaches. For Sabotage, all adversaries must be neutralized before the full sabotage attack is carried out.

11.2.2. Scenario Results Description – Theft

Section 11.1 describes the uninterrupted scenario timeline for the adversary, while Section 7.2 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.

11.2.2.1. TRU Theft Scenario - 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 (**Error! Reference source not found.**).

Figure 30. Time 00:00 Scenario configuration

Upper left—OP3 Adv engages outer patrol; Middle—Time 00:00 configuration; Upper right—Adv. Breach outer door

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

Upon completion of 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 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 31).

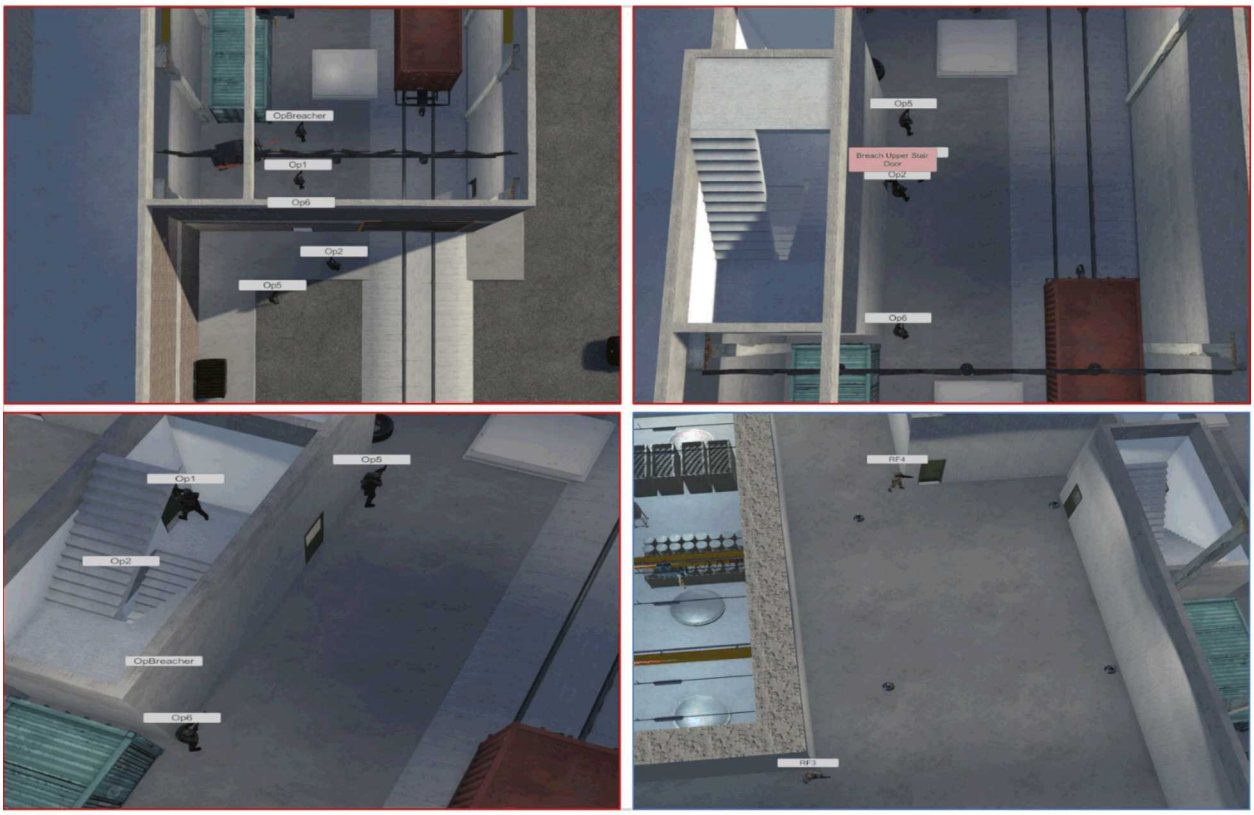

Figure 31. Adversary Enters Facility

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

11.2.2.3. 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 32).

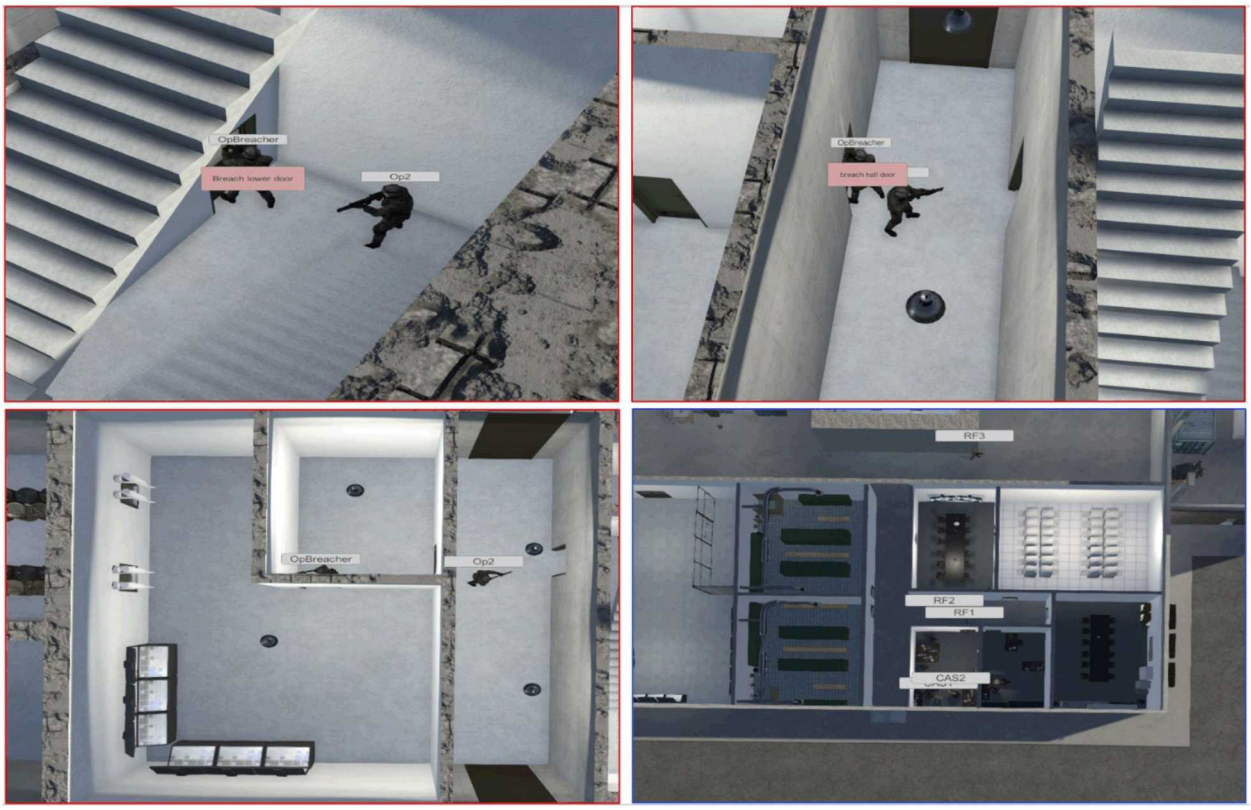

Figure 32. Adversaries Begin Vault Breach

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 RF2 move to containment positions

11.2.2.4. 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 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 10 minutes after the initial alarm, the LLEA first responders arrive and set up facility containment positions (see Figure 33).

Figure 33. Vault Breach and RF Containment

Upper left—RF1 1 RF2 engage Adv. outside building; Upper right—TRU Vault Breach in Progress; Lower left—Remaining RF in containment; Lower right—LLEA responds in containment positions

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

Roughly 15 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 riflemen are killed or all responders are killed. Either way, once the engagement is complete, the adversary 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.

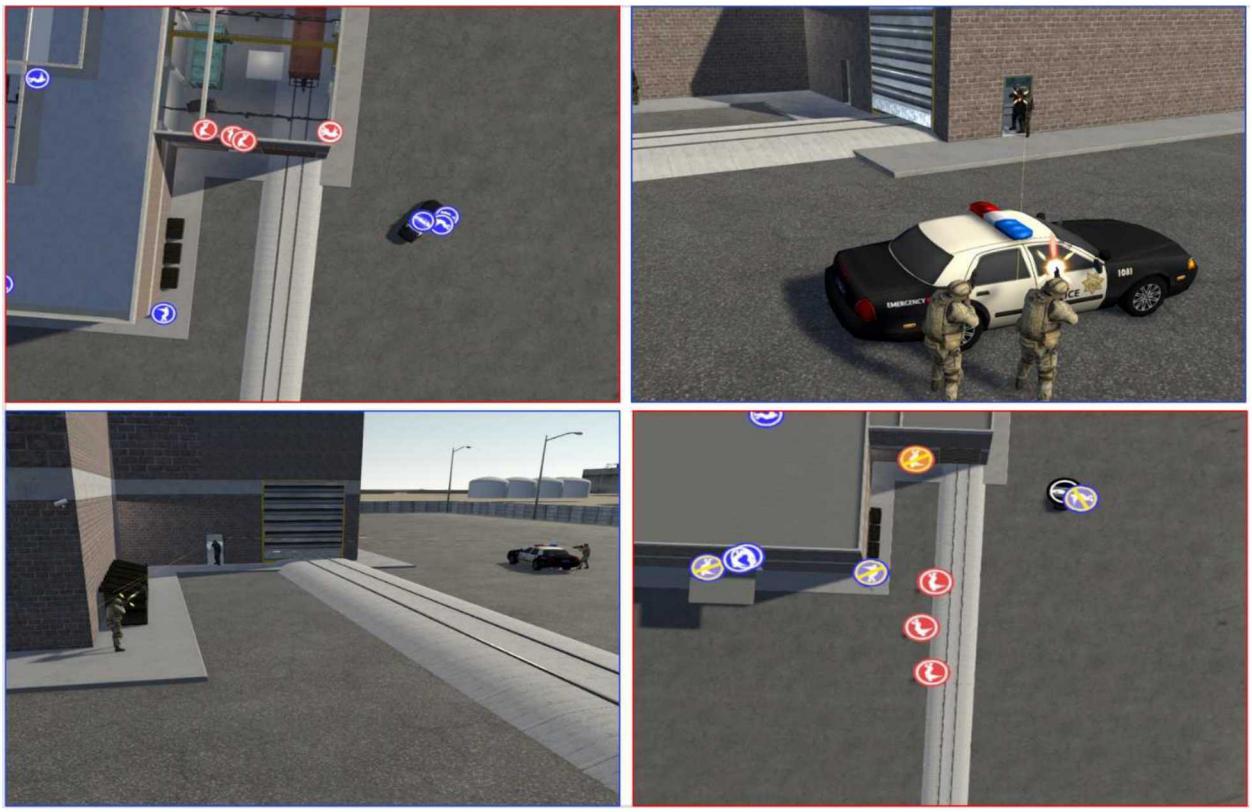

Figure 34. Adversary Attempts Escape

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—Adv.e escaping with material

11.2.3. Results Outsider Theft – Baseline

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.

11.2.3.1. Baseline Scribe3D© Results – Outsider Theft

Table 7 describes the outcomes of the attack scenario with four-to-seven adversaries. Overall, the RF was successful versus only four and five adversary attackers (P_N=93% for both). The system maintains some effectiveness versus six attackers (75%), but performance drops considerably versus seven adversaries. The eight-adversary scenario was not modeled due to low system performance versus seven adversaries. It was already clear that upgrades would be necessary. Average scenario times ranged from 15:05 to 16:08, showing that the containment strategy employed allows the adversaries a great deal of time onsite to deal with system delay, but it also allows LLEA to arrive to support the onsite response force. The number of engagements (how many times any individual

fired a weapon) scaled with the number of adversaries present in the scenario, as would be expected. However, the number of killed in action (KIA) engagements increased, but not dramatically. This overall low success rate in engagement is largely due to most entities being in cover when taking fire. Both Blue and Red KIA increased as Red numbers increased as well. Overall, the system performs well, but there is room for improvement versus higher adversary numbers.

Table 7. Baseline Scribe3D © Simulation Results – Outsider Theft

Name	4 ADV	5 ADV	6 ADV	7 ADV
Number of Runs	100	100	100	100
Blue Wins	93	93	75	50
Red Wins	7	7	25	50
Probability of Neutralization (P_N)	93%	93%	75%	50%
Prevent Material Out of Building	93	90	75	53
Average Time (s)/(mm:ss)	950/(15:50)	966/(16:06)	964/(16:04)	968/(16:08)
Average Engagements	20	29	33	39
Average KIA Engagements	7	8	9	9
Blue Force Count	12	12	12	12
Average Blue KIA	2.98	3.56	3.84	4.86
Average Blue KIA in Win	2.75	3.38	3.12	3.72
Red Force Count	4	5	6	7
Average Red KIA	3.76	4.7	4.88	4.32
Average Red KIA in Win	0.57	1.52	1.52	1.64

11.3. Outside/Insider Collusion Scenario Theft of U/TRU Material

In order to further test the system, an insider collusion theft scenario was designed. In this scenario, the insider is a site operator with access to the manipulator arms in the hot cell, U/TRU vault, and transfer hatches. This scenario assumes an insider operator is able to covertly acquire small quantities of the U/TRU product in the hot cell. Once a significant quantity was acquired, the insider moved the material from the hot cell to the north transfer hatch in conjunction with an outsider force attack

to obtain the target material in the transfer hatch. The effect of this action is that a large portion of the delay seen in the U/TRU vault theft scenario is mitigated.

11.3.1. Collusion Path Analysis Results – Pathtrace©

The result of the insider having moved the material from the U/TRU vault to the north transfer hatch is visible in the path analysis results. Rather than breaching the pedestrian door into the high bay, the adversary breaches the southeast emergency exit door and proceeds down the eastern stairwell, through the service room and into the transfer hatch. The major effect of this action is that a large portion of delay is removed, which results in offsite responders being unable to reach the site before the theft is complete. Figure 35 shows the adversary path.

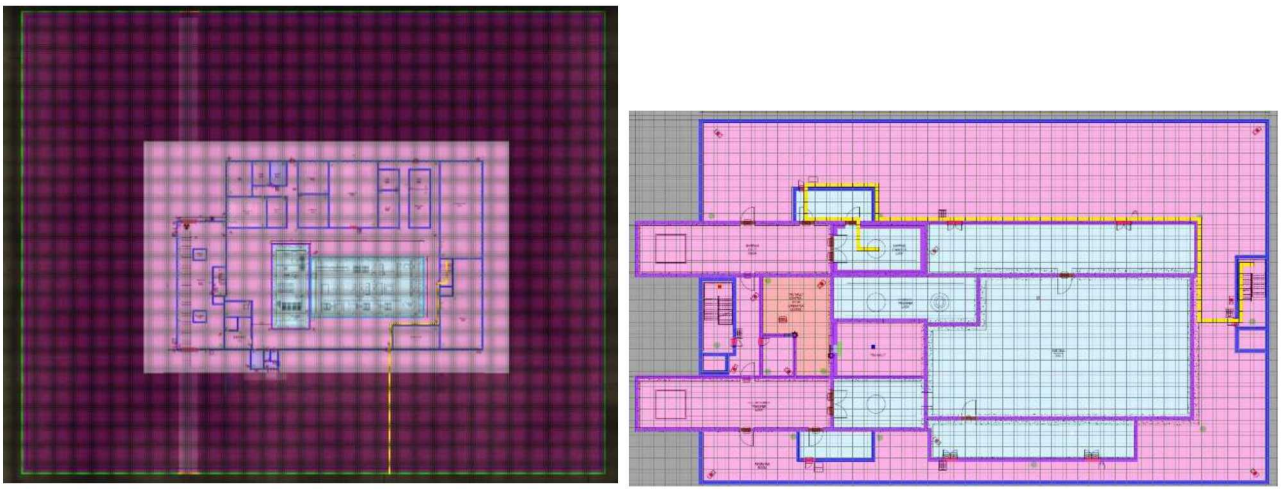

Figure 35. Collusion Path to Material Stashed by Insider

11.3.2. Outsider/Insider Collusion Scenario Attack Timeline

Table 8 shows that the system is still highly effective in interrupting the adversary. Similar to the non-collusion scenario, P_I is 0.99, however delay is cut roughly in half (from 956 to 452). As mentioned above, this reduces response effectiveness because only onsite responders are timely and can engage the adversary.

Table 8. Collusion Scenario Timeline and Probability of Interruption

Task	Element Crossed	P(Detection)	Delay (s)
1	Breach outer passive fence	0.02	20
2	Move to building exterior [50m]	0.02	11.6
3	Engage foot patrol	0.2	10
4	Breach Exterior Emergency Exit Door	0.8	30
5	Move to Stairwell Door	0.02	11.4
6	Breach Upper Stairwell	0.8	30
7	Move down to Lower Stairwell Door	0.02	5.7
8	Breach Lower Stairwell Door	0.8	30
9	Move to Service Room Shield Door	0.02	--
10	Breach Service Room Shield Door	0.8	--
11	Move to Transfer Hatch Door	0.02	--

12	Breach Transfer Hatch Door	0.8	--
13	Retrieve Insider Theft Target	0.02	240^
14	Exit Site with Target	0.02	63.3
		P(Interruption)	**Total Time**
		0.99	**452**

11.4. Insider/Outsider PN Collusion Results – Theft

Section 11.3 describes the uninterrupted scenario timeline for the adversary, while Section 7.2describes the response force timeline to muster and respond to attack. This section will describe the results of the intersection of these two timelines and step through how the scenario unfolded in the Scribe3D© simulation.

11.4.1. Inside/Outsider Collusion - Time 00:00-00:30

The neutralization timeline begins at the probable detection point. The path analysis conducted showed the adversaries would most likely be detected as they breached the emergency exit door of the facility. In the simulation, this occurred after the adversaries breached the outer passive fence and moved to the building exterior on the southeast side of the facility. Adversary 3 took a concealed position at the corner of the building and subsequently engaged the patrol from cover as the breach team completed the exterior breach (Figure 34).

Figure 36 - Time 00:00 Collusion Theft Scenario configuration

Left—Adversaries Approach the Facility; Middle—Breach the Emergency Exit; Right— Engage the Patrol

11.4.1.1. Time 00:40-01:30 Adversary Enters Facility and Secures Corners

Upon completion of outer breach, the adversaries entered the facility and moved toward the eastern stairwell. The adversary forces split up and took positions at the corners of the hot cell to secure

both the eastern stairwell door and theeventual exit path out the breached emergency door. Early response forces on patrol inside the building at the time of the exterior breach engaged these corner adversaries from their respective locations while the onsite quick response team mustered in response to the attack.

Figure 37 - Time 00:40 Building Entry and Secure Corners

11.4.1.2. Time 01:30-02:40 Adversaries Breach Stairwell Doors

Adversaries, on their way to obtain the target in the basement transfer hatch, breached the upper door to the eastern stairwell. As the adversaries breached the lower stairwell door and moved to the basement shield door, the onsite quick response team finished mustering. Response forces moved toward the eastern stairwell door and engaged cover adversaries with a containment strategy focused on preventing the removal of the theft target from facility.

Figure 38 - Time 01:30-02:40 Adversaries breach upper and lower stairwell doors

Left—Upper stairwell breach; Right—lower stairwell breach

11.4.1.3. Time 02:40-06:50 Adversaries Acquire Target Material

Adversaries breached the shield door, the door to the transfer hatch, and finally acquired the target material left by the insider. Upon receipt of material, the adversaries left the site.

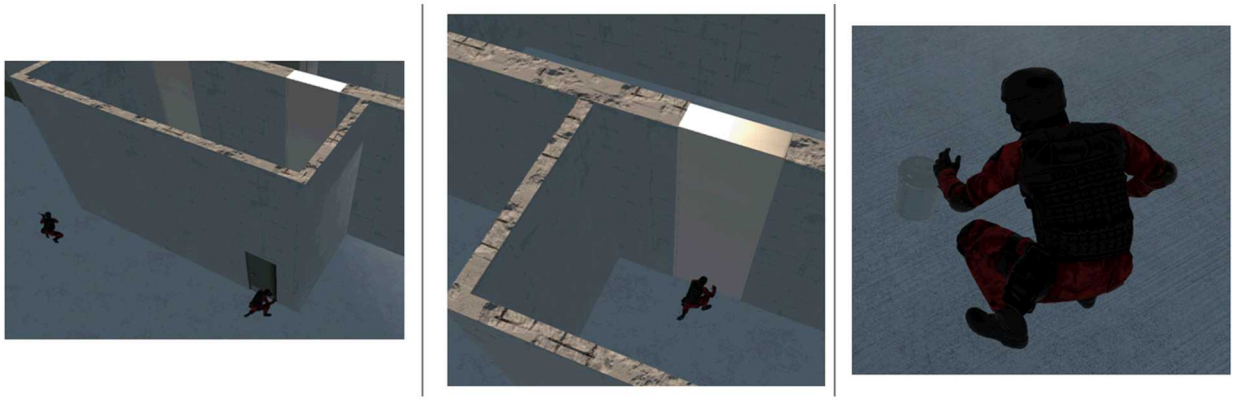

Figure 39. Adversaries breach and acquire target material – Collusion

11.4.2. Results Collusion Theft – Baseline

A total of 100 simulations were conducted for each scenario to evaluate the success of an insider/outsider collusion theft. In all engagements, the adversary was successful in breaching the plant perimeter and entering the facility through a breached emergency exit door.

Table 9. Adv Target Acquisition Insider Collusion

Adv #s	Acquire Target
4	85
5	90
6	98
7	100
8	100

Table 9 shows adversaries were able to acquire the target at a very high rate proportional to the number of attacking adversaries. As noted in the above timeline, response forces attempted to set up in a containment strategy off of the eastern stairwell door rather than assaulting the adversaries in the basement. This resulted in favorable outcomes for keeping the material onsite but also all but guaranteed the adversary would get their hands on the target material.

11.4.2.1. Scribe3D© PN Collusion Theft Results – Baseline

Table 10 describes the outcomes of the attack scenario with four-to-eight adversaries (Blue: Response Forces, Red: Adversaries). Overall the response forces were only successful versus four and five adversary attackers (P_N=93% and 87% respectively). The system maintained limited effectiveness versus six attackers (60%), but performance drops below 50% for seven and eight adversaries. Average scenario time ranged from 6:29 to 7:34, which showed the significant impact of the insider on bypassing system delay and prevented the offsite LLEA from arriving in time to

support the onsite response forces. The number of engagements (how many times any individual fired a weapon) scaled with the number of adversaries present in the scenario, as would be expected. However, the number of KIA engagements increased, but not dramatically. This overall low success rate in engagements is largely due to most entities being in cover when taking fire. Both Blue and Red KIA increased as Red numbers increased. Overall, the system performs well versus lower adversary numbers, but there is significant room for improvement versus higher adversary numbers.

Table 10. Scribe3D © Simulation Results – 4 Adversary Collusion Theft – Baseline

Theft Data	4 ADV	5 ADV	6 ADV	7 ADV	8 ADV
Number of Runs	100	100	100	100	100
Blue Wins	93	87	60	48	34
Red Wins	7	13	40	52	66
Average Time (s)	390	411	444	451	455
Average Engagements	40.9	49.9	58.3	65.5	70.1
Average KIA Engagements	7.26	8.42	8.8	9.42	9.43
Blue Force Count	10	10	10	10	10
Average Blue KIA	3.5	3.93	4.62	5.13	5.35
Average Blue KIA in Win	3.31	3.62	3.72	4.19	4.09
Red Force Count	4	5	6	7	8
Average Red KIA	3.77	4.52	4.29	4.42	4.19
Average Red KIA in Win	0.71	100	1.73	2.04	2.23

11.4.3. Collusion Theft – Upgrade 1 – Mantraps

The mantraps upgrade was proposed in response to findings in the sabotage scenario analysis, covered in detail in section 12.2.3. The rationale behind the upgrade was two-fold: 1) more delay would allow the inner patrol response force time to move to more advantageous positions of cover from which to engage adversaries and 2) that additional delay would enable the onsite quick response team to muster and engage adversaries in conjunction with the inner patrol response forces instead of as two separate and smaller engagements.

11.4.3.1. Scribe3D© PN Collusion Theft Results – Upgrade 1 Mantraps

Table 11 describes the outcomes of the attack scenario with four-to-eight adversaries. Overall, the response force was highly successful versus four-to-six adversary attackers (P_N=100%, 94%, and 92% respectively). The system maintains limited effectiveness versus seven attackers (71%), but performance drops to 50% at eight adversaries. This simple upgrade universally and significantly improved system performance as it allowed the inner patrol response forces more time to prepare and take cover before the adversaries enter the building. The additional delay was still not enough to

facilitate complete mustering of all response forces prior to adversary entry, however, which leaves room for improvement either in earlier detection, further delay, or more rapid muster.

Table 11. Scribe3D © Simulation Results – Collusion Theft – Upgrade 1

Theft Data	4 ADV	5 ADV	6 ADV	7 ADV	8 ADV
Number of Runs	100	100	100	100	100
Blue Wins	100	94	92	71	50
Red Wins	0	6	8	29	50
Average Time (s)	245	359	381	424	459
Average Engagements	25.9	34.6	39.3	52.5	59
Average KIA Engagements	6.43	7.93	8.97	9.49	9.84
Blue Force Count	10	10	10	10	10
Average Blue KIA	2.49	3.22	3.4	4.11	4.77
Average Blue KIA in Win	2.49	3.04	3.18	3.34	3.54
Red Force Count	4	5	6	7	8
Average Red KIA	4	4.79	5.69	5.53	5.28
Average Red KIA in Win	NaN	1.5	2.13	1.93	2.56

11.4.4. Collusion Theft – Upgrade 2 – Mantraps + Shifting exterior patrols

Across all scenarios previously studied it was observed that the exterior patrol was being ambushed and neutralized over 90% of the time. This upgrade therefore involved moving the exterior patrol inside the facility, paired up with existing inner patrol response force, where they would not be ambushed. Moving the patrol to the interior and relying on camera systems for exterior surveillance would therefore improve overall system performance and reduce response force attrition by allowing these response force members to engage adversaries.

11.4.4.1. Scribe3D© PN Collusion Theft Results – Upgrade 2 Mantraps + Patrol Relocation

Table 12 describes the outcomes of the attack scenario with four-to-eight adversaries. Overall, the response force was highly successful versus four-to-seven adversary attackers (P_N=100%, 98%, 96%, and 88% respectively). The system maintains limited effectiveness versus eight attackers (79%). The combination of the mantrap, which allowed the response force time to better prepare for the adversaries, and doubling the fighting strength at each corner facing adversary entry greatly improved system performance.

Table 12. Scribe3D © Simulation Results – Collusion Theft – Upgrade 2

Theft Data	4 ADV	5 ADV	6 ADV	7 ADV	8 ADV
Number Of Runs	100	100	100	100	100
Blue Wins	100	98	96	88	79
Red Wins	0	2	4	12	21
Average Time (s)	168	215	212	276	315
Average Engagements	27.1	37.6	42.5	52.1	67.9
Average KIA Engagements	4.94	6.24	7.18	8.6	9.82
Blue Force Count	10	10	10	10	10
Average Blue KIA	0.97	1.38	1.35	2.29	2.98
Average Blue KIA in Win	0.97	1.29	1.16	1.78	2.18
Red Force Count	4	5	6	7	8
Average Red KIA	4	4.91	5.86	6.39	6.95
Average Red KIA in Win	NaN	0.5	2.5	1.92	3

Response survivability increased significantly as well across the two upgrade cases as can be seen in Table 13. This table shows the reduction (in terms of Average KIA) versus the baseline configuration for Upgrades 1 and 2.

Table 13. Response Force Attrition Rate Reduction vs. Baseline

Config.	4 ADV	5 ADV	6 ADV	7 ADV	8 ADV
Upgrade 1	29%	18%	26%	20%	11%
Upgrade 2	72%	65%	71%	55%	44%

11.4.5. Collusion Theft – Upgrade 3 – Extended Detection, Exterior Delay, Hardened Garage

As noted in prior scenarios, the onsite quick reaction response force had been unable to be alerted and mustered prior to adversary entry. To facilitate a complete response force and maximize system effectiveness for the given numbers of responders and adversaries, this final upgrade case involved three additional security measures. It included pushing the detection point in the scenario far outside the building, making the adversary travel a circuitous or perilous route, and hardening the quickest access points in the building. Each upgrade will be discussed in detail below.

11.4.5.1. Extended Detection – Fused Radar and Video Motion Detection Using the Deliberate Motion Algorithm (DMA)8

This upgrade component uses a combination of radar and video motion detection to reach far beyond the facility perimeter. The deliberate motion algorithm (DMA) is able to decipher motion moving toward the facility while minimizing nuisance alarms from weather or traffic in the area. Assumptions for the technology are that detection begins between 200 and 300 meters from the walls of the facility. This would result in a total mobilization of response force prior to adversary entry.

11.4.5.2. Ankle Breaker Anti-Transit Landscaping

This upgrade component involves covering the non-essential pathways into the site with 8-12" diameter rough cut stones. These stones make walking through these areas much more perilous, slowing transit. The site would still require roads and paths without these stones for normal facility operations; however, adversaries would be delayed by the stones or funneled through specific access pathways and circuitous routes. Similar rocks can be seen in Figure 40.

Figure 40. Ankle Breaker Rock Example (left); High Bay Hardened Fighting Position (right)

11.4.5.3. Hardened Fighting Positions at Quicker Building Access Points

The final upgrade component for this upgrade case involves reinforcing the quickest path that the adversary would take in order to avoid traversing the ankle breaker rocks. This quickest access path is along the road into the facility's high bay, which is required for normal operations and would not have any rocks placed along it. The two response force members who were previously external patrol are placed in hardened fighting positions inside this now most-likely breach location in order to engage adversaries the minute they enter as seen in Figure 40.

Additionally, Figure 41 shows the overall layout of the respective security upgrades as well as the two adversary paths that were generated to fully qualify this upgrade case. One path (Path A) entered through the high bay against the hardened fighting positions. After collecting the extremely effective data for Path A, a second path (Path B) was analyzed to ensure the design was sound if the adversary avoided the hardened positions in the high bay. Path B involved the adversaries using the

sidewalks around the building to navigate to the same emergency exit door, as observed in previous scenarios.

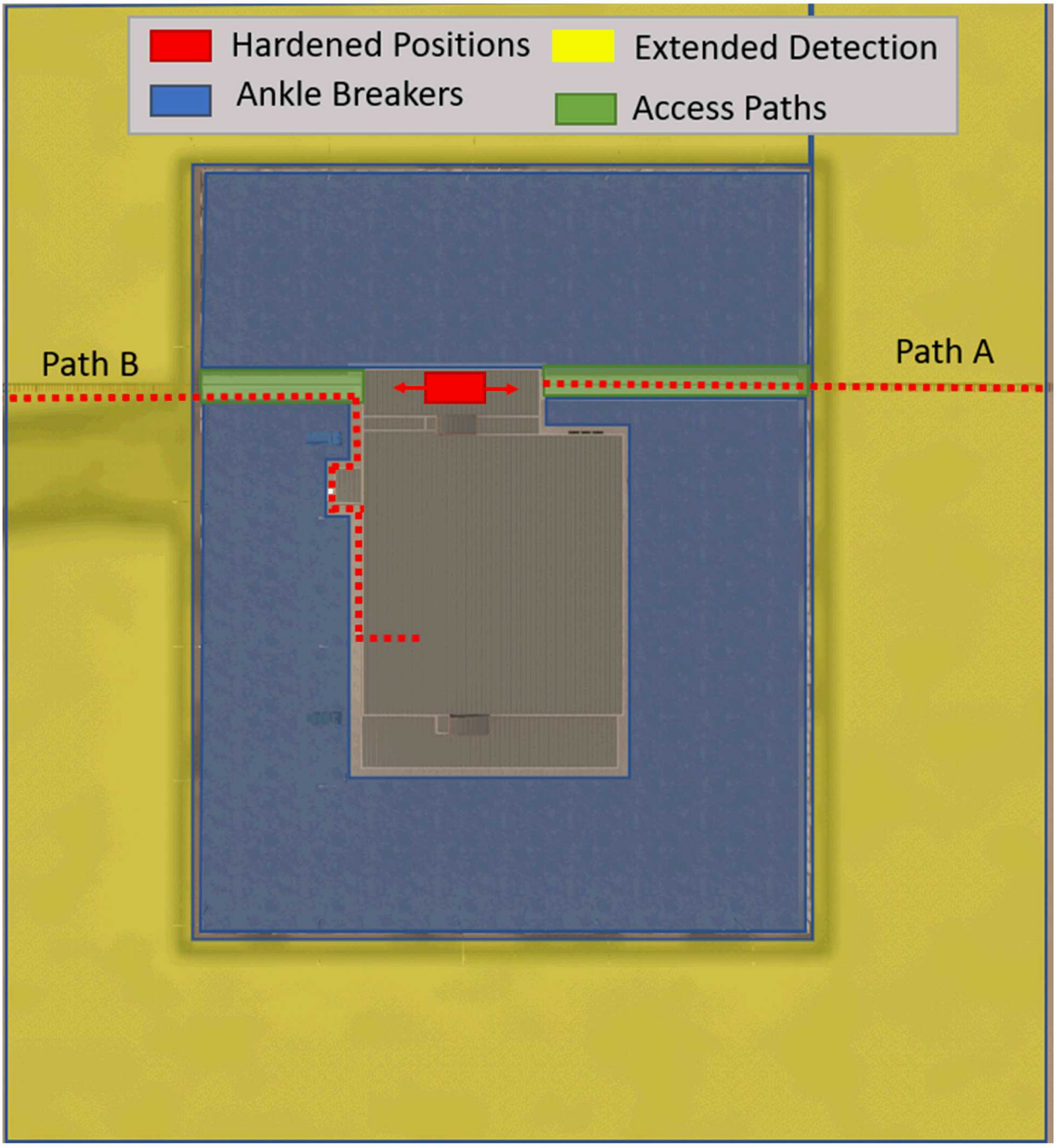

Figure 41. Upgrade 3 Component Locations with Path A and Path B

11.4.5.4. Scribe3D© PN Collusion Theft Results – Upgrade 3 Extended Detection, Transit Rocks, HFPs

Table 14 describes the outcomes of the attack scenario with four-to-eight adversaries, wherein the adversaries take Path A through the high bay. Overall, the response force was highly successful with

only a single adversary win across the entire run set (499/500). Adversaries were detected early in their approach by the extended detection system, forced into the high bay by the ankle breaker delay features, and then were overcome by the hardened manned fighting positions. The additional delay also enabled the remainder of the response force to muster and take up covered positions from which to engage adversaries. Scenario time is cut in half, which identifies that in almost all cases the adversaries do not even get close to the target.

Table 14. Scribe3D © Simulation Results – Collusion Theft – Upgrade 3 – Path A

Theft Data	4 ADV	5 ADV	6 ADV	7 ADV	8 ADV
Number of Runs	100	100	100	100	100
Blue Wins	100	100	99	100	100
Red Wins	0	0	1	0	0
Average Time (s)	175	179	190	190	196
Average Engagements	13.5	18.6	27.6	34.9	42.3
Average KIA Engagements	4.21	5.37	6.76	7.85	9.17
Blue Force Count	10	10	10	10	10
Average Blue KIA	0.22	0.43	0.97	1.06	1.55
Average Blue KIA in Win	0.22	0.43	0.92	1.06	1.55
Red Force Count	4	5	6	7	8
Average Red KIA	4	5	5.97	7	8
Average Red KIA in Win	NaN	NaN	3	NaN	NaN

Table 15 describes the outcomes of the attack scenario with four-to-eight adversaries, wherein the adversaries take Path B to avoid the high-bay hardened fighting positions. The adversaries skirted around the building on the sidewalk and entered through the emergency exit and subsequent mantrap doors used in previous scenarios. Overall, the response force was highly successful with a probability of neutralization at 90% or higher in every scenario. Even though the adversaries avoided the garage, they still were detected at sufficient range and delayed such that all response personnel were well positioned at the corners of the hot cell to immediately engage adversaries upon entry. Scenario time is cut significantly, showing that in almost all cases the adversaries do not even get close to the material; however, the results are slightly worse than for Path A listed above.

Table 15. Scribe3D © Simulation Results – Collusion Theft – Upgrade 3 – Path B

Theft Data	4 ADV	5 ADV	6 ADV	7 ADV	8 ADV
Number of Runs	100	100	100	100	100
Blue Wins	100	98	98	94	90
Red Wins	0	2	2	6	10
Average Time (s)	238	252	264	270	296
Average Engagements	27.6	37.2	46.2	58.1	66
Average KIA Engagements	4.76	6.18	7.72	9	10.5
Blue Force Count	10	10	10	10	10
Average Blue KIA	0.8	1.27	1.83	2.37	3
Average Blue KIA in Win	0.8	1.17	1.74	2.14	2.67
Red Force Count	4	5	6	7	8
Average Red KIA	4	4.97	5.91	6.67	7.59
Average Red KIA in Win	NaN	3.5	1.5	1.5	3.9

11.4.6. Theft Results Summary

Results show a linear progression in terms of system effectiveness from the baseline system design to upgrade packages 1, 2, and 3 (Figure 42). Depending on the threat level that the facility faces, upgrades 1 or 2 may be adequate for system performance. Overall, the elements added in upgrade 3 create an extremely well secured design that would require a highly trained force larger than any analyzed in this report to even potentially steal material.

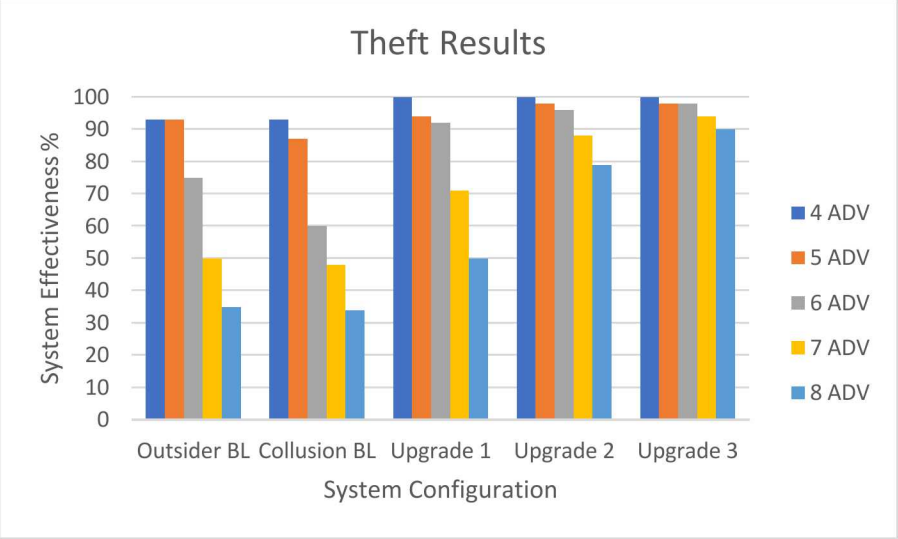

Figure 42. Theft Results Summary

12. SABOTAGE ATTACK RESULTS

12.1. Outsider Sabotage Scenario - Path

In order to fully test the PPS of the facility, a notional sabotage scenario was designed. In this scenario, the adversary has attempted to breach the argon hot cell in order to halt operations, to create an international incident, and/or to trigger material release. The hot cell sits just inside several emergency exits, which provide quick access. The adversary conducted a multi-phase sabotage attack where they penetrated the wall of the hot cell, then placed follow-on charges through the initial penetration. Figure 43shows how short the path is from offsite to the hot cell. As this design only featured one barrier with reliable detection, specifically the exterior emergency exit door, it was an attractive target that provided adversaries rapid access.

Figure 43. Sabotage Scenario

12.1.1. Sabotage Scenario Task Timeline

The sabotage attack began with adversaries breaching the exterior passive fence and advancing to the building exterior. The adversaries then engaged external response force patrols at the same time the exterior door was breached, and the initial stage of the argon cell breach began. After an explosive charge penetrated the wall of the hot cell, a follow-on charge was placed to further disperse hot cell contents, at which time adversaries leave the facility. The task time once the adversary reaches the hot cell is just over four minutes with a total attack time under six minutes, which precluded response by an offsite LLEA who would have required 10 minutes to respond.

Figure 44. Sabotage Scenario Path Analysis Results

12.1.2. Sabotage Scenario Path Analysis Results

Generic data is used for detection and delay elements on the way to the target.

Table 16. Sabotage Scenario Path Analysis Results

Task	Element Crossed	P(Detection)	Delay (s)
1	Breach outer passive fence	0.02	20
2	Move to building exterior [50m]	0.02	34.81
3	Engage foot patrol	0.1	10
4	Breach Exterior Emergency Exit Door	0.8	30
5	Move to Argon Cell	0.02	9.19
6	Breach Argon Cell Outer Wall	0.9	-
7	Pack breach in Argon Cell (CDP Reached)	0.9	246^
		P(Interruption)	**Total Time**
		0.99	**342**

Task	Element Crossed	P(Detection)	Delay (s)

1	Breach outer passive fence	0.02	20
2	Move to building exterior [50 m]	0.02	34.81
3	Engage foot patrol	0.1	10
4	Breach Exterior Emergency Exit Door	0.8	30
5	Move to Argon Cell	0.02	9.19
6	Breach Argon Cell Outer Wall	0.9	-
7	Pack breach in Argon Cell (CDP Reached)	0.9	246^
		P(Interruption)	**Total Time**
		0.99	**342**

Table 16. Sabotage Scenario Path Analysis ResultsTable 16 shows that the adversary was interrupted at an extremely high rate (P_I =.99). Total scenario time is 342 seconds. Detection was largely driven by the balanced magnetic switch on the emergency exit door, but also occurs as the result of multiple explosive breaches along the path timeline.

Table 17. Sabotage Scenario Path Analysis Results

Task	Element Crossed	P(Detection)	Delay (s)
1	Breach outer passive fence	0.02	20
2	Move to building exterior [50 m]	0.02	34.81
3	Engage foot patrol	0.1	10
4	Breach Exterior Emergency Exit Door	0.8	30
5	Move to Argon Cell	0.02	9.19
6	Breach Argon Cell Outer Wall	0.9	-
7	Pack breach in Argon Cell (CDP Reached)	0.9	246^
		P(Interruption)	**Total Time**
		0.99	**342**

12.2. Sabotage PN Analysis Simulation and Analysis Overview

A simulation was conducted in Scribe3D© in order to gauge the rough effectiveness of the onsite response teams for the process site. The goal of this analysis was to provide a high-level understanding of the effectiveness of the proposed locations for responders at an early design phase. The scenario was conducted from the outer passive perimeter fence through completion of the sabotage event.

12.2.1. Response Force Win Criteria

At the end of each simulation, a response force win was awarded in the event the adversary was unable to successfully complete its full sabotage objective due to attrition of adversary personnel and/or lack of required equipment to complete necessary breaches. Both argon hot cell charges must have been detonated for a response force loss.

12.2.1.1. Sabotage P_N Results Description – Sabotage

Section 11.4.5.4 describes the uninterrupted scenario timeline for the adversary, while Section 7.2 describes the RFT. This section will describe the results of the intersection of these two timelines and step through how the scenario unfolded in the Scribe3D© simulation. The overall results for 100 individual scenarios were recorded to report an overall probability of neutralization of the adversaries (i.e. response force victory), where a successful system had a $P_N > 80\%$.

12.2.1.2. Hot Cell Sabotage Scenario – Time 00:00-00:30 Simulation Start

The neutralization timeline began at the probable detection point; 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 adversaries had already breached the passive exterior fence and advanced to the building exterior. Adversary 3 took a concealed position at the corner of the building and as the breach team completed the exterior breach, Adversary 3 engaged the patrol from cover (Figure 45).

Figure 45 - Time 00:00 Sabotage Scenario Configuration

Left—Adversaries approach the facility; Middle—Breach the Emergency Exit; Right--Engage the patrol

12.2.1.3. Time 00:40-02:00 Adversary Enters Facility Begins Sabotage

After the outer door breach and patrol ambush, adversaries entered the facility and moved to the hot cell. An initial charge was placed on the hot cell wall while remaining adversaries advanced to hot cell corners to engage response forces from cover and protect breaching team.

Figure 46 - Time 00:40 Building Entry and begin sabotage

12.2.1.4. Time 02:00-06:00 Adversary Enters Facility Begins Sabotage

Adversaries placed and detonated an initial charge designed to puncture the hot cell wall, followed by an additional bulk charge designed to increase damage inflicted and material dispersal. While the second charge was being placed, the quick reaction team finished mustering and, in conjunction with the inner patrol response force, engaged adversaries to stop the attack.

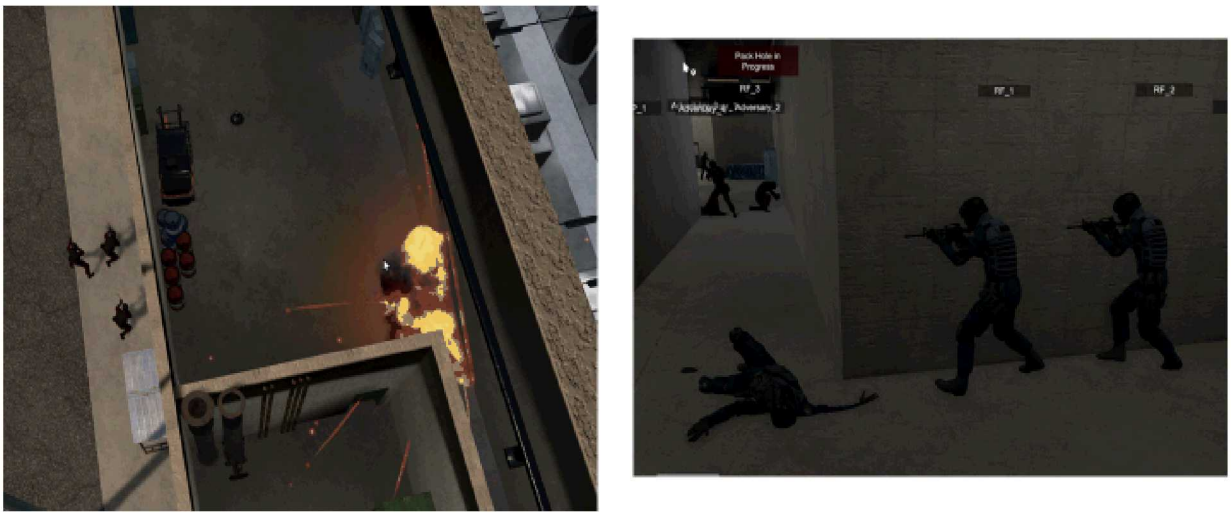

Figure 47 - Time 02:00 Sabotage and Interdiction

Left—Charges detonate on Hot Cell; Right—RF Try to Engage Adversaries

12.2.2. Results Sabotage – Baseline

A total of 100 simulations were conducted for each scenario, to evaluate the success of an adversary sabotage attack against the argon hot cell. In all engagements, the adversary was successful in breaching the plant perimeter, entering the facility through an emergency exit door, reaching the hot cell wall, and detonating an initial charge. Due to the nature of the attack, a containment strategy was not an option, and the response forces must take an active denial approach. Upon hearing the initial outer breach and the subsequent alarm communication from the CAS, response forces regroup and move en force to stop the adversary. This approach proved overall to be more effective and resulted in fewer response force casualties than responders rushing to individually engage the adversaries.

12.2.2.1. Scribe3D© PN Sabotage Results – Baseline

The scenario was run 100 times for threat groups ranging from four-to-eight adversaries, using the automated features of Scribe3D. Figure 48. Baseline Sabotage, Probability of Neutralization for Four-to-Eight AttackersFigure 48shows the results in which the response force was only able to prevent the sabotage about 50% of the time in the four adversary scenario. Numbers greater than foud adversaries declined linearly in performance. Lack of early detection and a substantial response delay allowed the attackers to get to the target and positions of cover before response force engagement. The adversaries eliminated the outer patrol in most simulation runs, which forced remaining onsite responders to fight with reduced numbers. In conjunction with the adversary having established cover and minimal separation, this resulted in overall very low system performance and as such, results are not presented in detail.

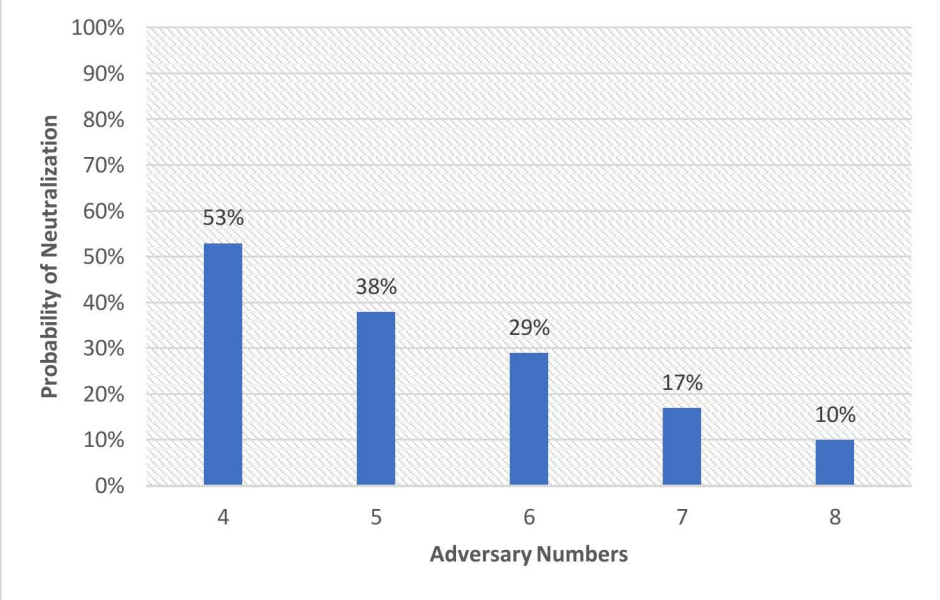

Figure 48. Baseline Sabotage, Probability of Neutralization for Four-to-Eight Attackers

12.2.3. Results Sabotage - Upgrade 1 - Mantraps and Response Changes

When looking at sabotage of the hot cell, several design and procedural changes were considered to improve system effectiveness. Initially it was determined that additional delay at the building exterior might allow the quick reaction response team to get in place with the inner patrol response force before the attackers. This would be achieved with the placement of an additional door at each

emergency exit along the building exterior, forming a mantrap. Both doors would be locked from the outside but would have crash-out bars on the inside to allow for rapid building evacuation in an emergency.

In early testing it was found that the mantrap upgrade did little to help the overall response force performance because the delay provided by the extra doors was not adequate to muster all responders. A change in tactics was proposed wherein, upon hearing the initial outer breach and the subsequent alarm communication from the CAS, inner patrol response forces advanced to advantageous positions of cover along the hot cell corners. From this vantage point, responders would be in cover and able to monitor the alarmed region, while also able to immediately engage adversaries who would enter at a disadvantage into an ambush. In Figure 49, the yellow circles show the positions the responders were able to reach, provided by the extra delay. One of the proposed mantraps is also highlighted by the yellow rectangle.

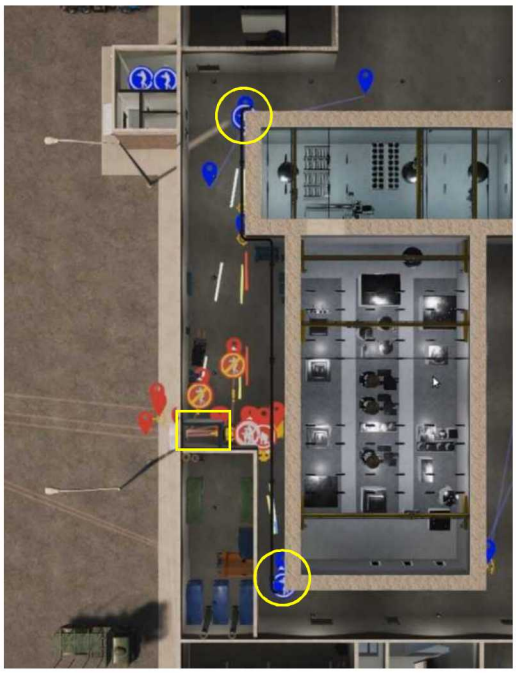

Figure 49. Mantrap Upgrade and Response Force Configuration

12.2.3.1. Scribe3D© PN Sabotage Results – Upgrade 1 - Mantraps

Table 18 describes the outcomes of the sabotage scenario with fou-to-eight adversaries. Overall, the response force was successful versus four and five adversaries (P_N = 95% and 85% respectively). System performance degrades gradually with eight adversaries, still maintaining 50% P_N. This simple upgrade, in conjunction with tactic modification, greatly improved system performance as it gave the response force time to prepare and take cover before the adversaries entered the building.

Table 18. Scribe3D © Simulation Results – Sabotage – Upgrade 1

Sabotage Data	4 ADV	5 ADV	6 ADV	7 ADV	8 ADV
Number of Runs	100	100	100	100	100
Blue Wins	95	85	76	66	50
Red Wins	5	15	24	34	50
Average Time (s)	155	191	222	246	288
Average Engagements	24.9	36.6	42.1	50.3	56.6
Average KIA Engagements	6.2	7.83	8.86	9.58	9.98
Blue Force Count	10	10	10	10	10
Average Blue KIA	2.41	3.43	3.94	4.21	4.84
Average Blue KIA in Win	2.23	2.99	3.3	3.36	3.68
Red Force Count	4	5	6	7	8
Average Red KIA	3.88	4.49	5.02	5.57	5.48
Average Red KIA in Win	1.6	1.6	1.92	2.79	2.96

12.2.4. Results Sabotage – Upgrade 2 – Mantraps Plus Shifting Exterior Patrols

This upgrade case involved shifting the exterior patrol to the interior of the building. The justification for this upgrade was that the exterior patrol was ambushed and neutralized over 90% of the time across all the scenarios studied. Moving the patrol to the interior, paired up with existing inner patrol response forces, and relying on camera systems for exterior surveillance improves system performance and reduces response force attrition.

12.2.4.1. Scribe3D© P_N Sabotage Results – Upgrade 2 – Mantraps Plus Shifting Patrol

Table 19describes the outcomes of the sabotage scenario with four-to-eight adversaries. Overall, the response force was successful versus four-to-seven adversaries (P_N = 99%, 97%, 94%, and 83% respectively). System performance degrades gradually as well with eight adversaries, still maintaining 66% P_N. The external patrol moved inside the building alongside the mantraps addition had a similar impact on the sabotage scenario as it had on the theft scenario detailed earlier in this report, with significant improvements in both response force attrition as well as system effectiveness.

Table 19. Scribe3D © Simulation Results – Sabotage – Upgrade 2

Sabotage Data	4 ADV	5 ADV	6 ADV	7 ADV	8 ADV
Number of Runs	100	100	100	100	100

Sabotage Data	4 ADV	5 ADV	6 ADV	7 ADV	8 ADV
Blue Wins	99	97	94	83	66
Red Wins	1	3	6	17	34
Average Time (s)	123	129	143	175	229
Average Engagements	22.5	32.6	38.9	54.9	68.2
Average KIA Engagements	4.69	6.11	7.22	8.93	9.95
Blue Force Count	10	10	10	10	10
Average Blue KIA	0.73	1.19	1.45	2.49	3.56
Average Blue KIA in Win	0.68	1.04	1.16	1.77	2.3
Red Force Count	4	5	6	7	8
Average Red KIA	3.96	4.92	5.8	6.53	6.48
Average Red KIA in Win	0	2.33	2.67	4.24	3.53

12.2.5. Results Sabotage – Upgrade 3 – Extended Detection, Exterior Delay, Hardened Garage

As noted in prior scenarios, the onsite quick reaction response force had been unable to be alerted and mustered prior to adversary entry. To facilitate a complete response force and maximize system effectiveness for the given numbers of responders and adversaries, this final upgrade case involved three additional security measures. It involved pushing the detection point in the scenario far outside the building, making the adversary travel a circuitous or perilous route, and hardening the quickest access points in the building. These are the same upgrade measures and paths detailed in section 11.4.5for the theft scenario and Figure 40.

12.2.5.1. Scribe3D© PN Sabotage Results – Upgrade 3 Extended Detection, Transit Rocks, HFPs

Path A for Upgrade 3 with respect to sabotage is nearly identical to the theft results, due to the extremely high system effectiveness granted by these upgrades. In the theft results, 99% of the scenario runs did not reach the stairwell where the path between theft and sabotage diverge, so equating these results is reasonable. Refer back to section 11.4.5.4and Table 16for Path A theft results.

Path B, however, provided direct access to the hot cell for sabotage, with significantly less spread of the adversary paths (i.e. setting up for cover near entry point vs. traveling through facility for theft). Therefore Path B was analyzed to ensure system effectiveness remained high. Table 20 describes the outcomes of the sabotage scenario with four-to-eight adversaries, wherein they take Path B to avoid the high-bay hardened fighting positions. The adversaries skirted around the building on the sidewalk and entered through the emergency exit and subsequent mantrap doors used in previous scenarios. Overall, the response force was highly successful, with P_N = 92% or higher in every scenario. Even though the adversaries avoided the high bay, they are still neutralized at an extremely

high rate as the complete response force is mustered, well positioned at the corners of the hot cell, and able to engage the adversaries as they enter the building. Average scenario time is reduced by a third, which shows a marked increase in the ability of the response force to interrupt the adversaries prior to the first argon hot cell charge being detonated, as opposed to always after the first charge detonation in the baseline scenario.

Table 20. Scribe3D © Simulation Results – Sabotage – Upgrade 3 – Path B

Sabotage Data	4 ADV	5 ADV	6 ADV	7 ADV	8 ADV
Number fo Runs	100	100	100	100	100
Blue Wins	100	99	98	96	92
Red Wins	0	1	2	4	8
Average Time (s)	222	226	233	233	249
Average Engagements	16	26	33.6	39.6	49.5
Average KIA Engagements	4.16	5.46	6.67	8.1	9.59
Blue Force Count	10	10	10	10	10
Average Blue KIA	0.16	0.51	0.76	1.27	1.81
Average Blue KIA in Win	0.16	0.45	0.65	1.07	1.45
Red Force Count	4	5	6	7	8
Average Red KIA	4	4.95	5.91	6.83	7.78
Average Red KIA in Win	NaN	0	1.5	2.75	5.25

12.2.6. Sabotage Results Summary

The sabotage results were consistent with the theft results detailed above, which demonstrate a linear progression in terms of system effectiveness from the baseline system design to upgrade packages 1, 2, and 3 (Figure 50). Depending on the threat level that the facility faces, upgrades 1 or 2 may be adequate for system performance. Overall, the elements added in upgrade 3 create an extremely well-secured design that would require a highly trained force larger than any analyzed in this report to successfully sabotage this notional facility.

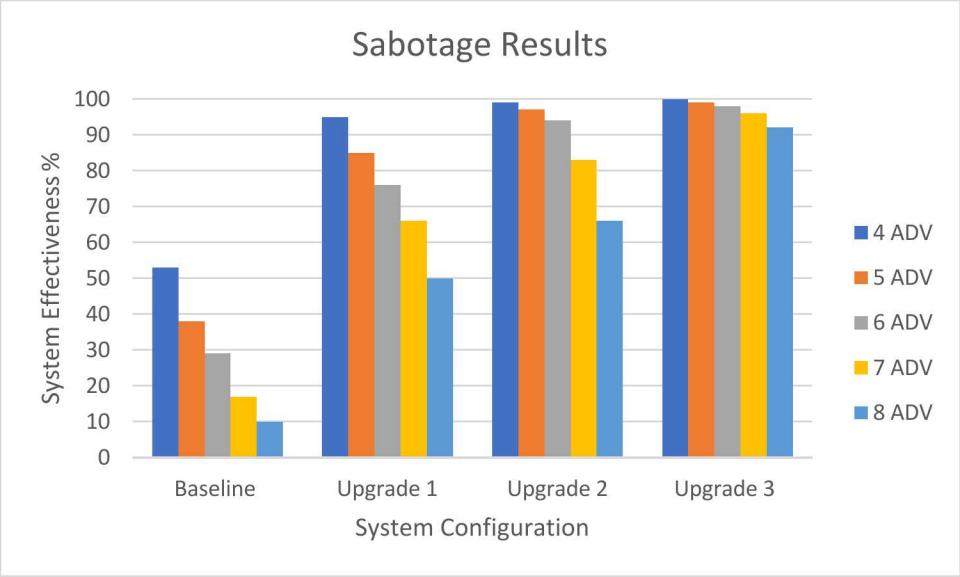

Figure 50. Sabotage Scenario Upgrade Results

13. CONCLUSION

The results of this study show that a facility with a relatively small security force and advanced security technology integrated at the design phase can produce extremely high system performance against a range of adversaries for both theft and sabotage scenarios. The results highlight the importance of how resources are applied to optimize system performance versus cost, and while Upgrade 3 universally provided exceptionally outstanding results, the drastic increases in performance for the limited costs of the Upgrade 1 and 2 packages should be emphasized.

Take, for example, the sabotage scenario and Upgrade 1, with the simple addition of a second door at each pedestrian emergency exit. The baseline scenario without these doors resulted in only a 50% probability of neutralization for the response force (RF), but adding in the mantrap with the second door provided the time and warning to facilitate a change in tactics for the responders and probability of neutralization increased by 45% to 95%,; This approximately 45% increase was consistent across all adversary scenarios. Accurate, effective, and rapid modeling allows these changes to be analyzed in the Design phase, and enables costs to be optimized while still maintaining a secure facility.

Elaborating further, consider the significant cost and/or performance savings identified in the results to Upgrade 2. Recognizing that the external patrols were being neutralized by the adversary the majority of the time demanded a change in procedure by moving them inside the facility or potentially removing the position entirely. Moving those response force members inside now means the costs associated with hiring and training those responders is not wasted.

Upgrade 3 generated universal probabilities of neutralization of over 90% for all scenarios and adversary numbers, and a future study could include looking at what elements could be removed while still maximizing system effectiveness to further refine costs.

The cost of the associated features utilized varies; adding doors during construction is trivial, as is the use of landscaping rock. Hardened fighting positions and advance LIDAR and video analytics are more expensive, but pale in comparison to the cost of security staffing. The overall cost of the security enhancements of this site would be far less than the performance gained by adding additional RF. Operationally, only six onsite responders engage the adversary in this configuration, while others are present manning the CAS and ECP. It is very likely that total staffing could be reduced even further, while maintaining high system performance.

This last upgrade package would most likely maintain high system performance, given the survivability of the guard force based on the added upgrades. Table 21 shows the response strength remaining at the end of the scenarios for Upgrade 3 for both collusion theft and sabotage. In even the worst-case scenario, (eight adversaries, collusion theft) the RF still maintains 50% of their fighting strength. This table is only calculated for those responders who engage the adversary.

Table 21. Remaining Response Strength Upgrade 3

Config	4 ADV	5 ADV	6 ADV	7 ADV	8 ADV
Collusion Theft	87%	79%	69%	60%	50%
Sabotage	97%	91%	87%	79%	70%

Furthermore, the high performance of the system is all without the use of a PIDAS, which is by far the costliest security feature at most high security sites, due to the costs associated with construction

and infrastructure, as well as lifetime maintenance. A PIDAS is most useful as a means of ensuring detection and assessment for a site; it provides little in terms of delay, especially given its high cost. This analysis shows that assessed detection can be achieved at the skin of the building or possibly further out to PIDAS distances, using new technology such as DMA to make extended detection a viable option without constant nuisance alarms.

In addition, modeling and simulation software are powerful and cost-effective tools that allow the security community to experiment with lower cost systems and new technology without impacting operations. However, they provide a limited perspective and should be taken as a single data point in the security conversation. These tools provide bounding conditions for very specific scenarios and should not be taken as ground truth. These tools allow analysts to test the possible and the plausible and provide data-driven answers that cannot be gleaned in any other way in such an affordable manner.

This careful analysis of the data from the study as well as further extrapolation underscores the significant value-added of using the modeling and simulation tools demonstrated in this report for a Virtual Facility Distributed Test Bed. Maximizing efficient Safeguards and Security by Design is enabled by the rapid, accurate, and numerous scenarios that can be generated by a single analyst and optimizing the cost-to-system performance ratio.

APPENDIX A.

NFCSC DOCUMENT COVER SHEET[1]

Name/Title of Deliverable/Milestone/Revision No. M3FT-20SN040105061Physical Security Model Development of an Electrochemical Facility

Work Package Title and Number Security Facility Models – SNL, FT-20SN04010506

Work Package WBS Number FT-20SN04010506

Responsible Work Package Manager Ben Cipiti

(Name/Signature)

Date Submitted

Quality Rigor Level for Deliverable/Milestone[2]	☐ QRL-1 ☐ Nuclear Data	☐ QRL-2	☒ QRL-3	☐ QRL-4 Lab QA Program[3]

This deliverable was prepared in accordance with Sandia National Laboratories

(Participant/National Laboratory Name)

QA program which meets the requirements of

☒ DOE Order 414.1 ☐ NQA-1 ☐ Other

This Deliverable was subjected to:

☐ Technical Review ☒ Peer Review

Technical Review (TR)
Review Documentation Provided

☐ Signed TR Report or,

☐ Signed TR Concurrence Sheet or, Concurrence Sheet or,

☐ Signature of TR Reviewer(s) below Reviewer(s) below

Peer Review (PR)
Review Documentation Provided

☐ Signed PR Report or,

☐ Signed PR

☒ Signature of PR

Name and Signature of Reviewers

Alan Evans

NOTE 1: *Appendix E should be filled out and submitted with the deliverable. Or, if the PICS:NE system permits, completely enter all applicable information in the PICS:NE Deliverable Form. The requirement is to ensure that all applicable information is entered either in the PICS:NE system or by using the NFCSC Document Cover Sheet.*

- *In some cases there may be a milestone where an item is being fabricated, maintenance is being performed on a facility, or a document is being issued through a formal document control process where it specifically calls out a formal review of the document. In these cases, documentation (e.g., inspection report, maintenance request, work planning package documentation or the documented review of the issued document through the document control process) of the completion of the activity, along with the Document Cover Sheet, is sufficient to demonstrate achieving the milestone.*

NOTE 2: *If QRL 1, 2, or 3 is not assigned, then the QRL 4 box must be checked, and the work is understood to be performed using laboratory QA requirements. This includes any deliverable developed in conformance with the respective National Laboratory / Participant, DOE or NNSA-approved QA Program.*

NOTE 3: *If the lab has an NQA-1 program and the work to be conducted requires an NQA-1 program, then the QRL-1 box must be checked in the work Package and on the Appendix E cover sheet and the work must be performed in accordance with the Lab's NQA-1 program. The QRL-4 box should not be checked.*

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, https://www.nrc.gov/reading-rm/doc-collections/cfr/, 2020.

[3] 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).

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

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

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

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

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

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

[10] Light Water Reactor Sustainability Program, "Evaluate Tools and Technologies that Would Benefit the Advancement of Risk-Informed Models" (2020) SAND 202-9055

[11] https://www.milestonematerials.com/wp-content/uploads/sites/12/2019/05/Medium-Boulders-OD2A1730.jpghttps://www.milestonematerials.com/wp-content/uploads/sites/12/2019/05/Medium-Boulders-OD2A1730.jpg

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

DISTRIBUTION

Email—External (encrypt for OUO)

Name	Company Email Address	Company Name
Mike Browne	mcbrowne@lanl.gov	LANL
Mike Reim	michael.reim@nuclear.energy.gov	DOE

Email—Internal

Name	Org.	Sandia Email Address
Sylvia Saltstein	8845	sjsaltz@sandia.gov
Dominic Martinez	6810	dmartin@sandia.gov
Greg Baum	6812	gabaum@sandia.gov
Technical Library	9536	libref@sandia.gov

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.