ABSTRACT

Title of Thesis: APPLICATIONS OF MODEL-BASED SYSTEMS ENGINEERING IN PERFORMANCE-BASED VULNERABILITY ASSESSMENT

Soroush Bassam, Master of Science, 2015

Directed By: Associate Professor Jeffrey W. Herrmann, Mechanical Engineering Department and Institute for Systems Research (ISR)
Associate Professor Linda C. Schmidt, Mechanical Engineering Department

This thesis discusses the use of a model-based systems engineering (MBSE) approach for physical protection systems (PPS) evaluation. We discuss the role of requirements analysis in Vulnerability Assessment (VA). Then, we discuss different tools that are being used for requirement analysis and demonstrate how requirements modeling tools can be used in analyzing requirements for VA. Next, we review the steps in vulnerability assessment (VA) and describe the use of SysML models in these steps. The thesis presents examples of SysML models that can be used when conducting VA. Such models can enable the development and integration of other VA tools and reduce the time and cost of conducting VA, which will lead to safer facilities.

APPLICATIONS OF MODEL-BASED SYSTEMS ENGINEERING IN PERFORMANCE-BASED VULNERABILITY ASSESSMENT

By

Seyed Soroush Bassam

Thesis submitted to the Faculty of the Graduate School of the
University of Maryland, College Park, in partial fulfillment
of the requirements for the degree of
Master of Science
2015

Advisory Committee:
Associate Professor Linda C. Schmidt, Chair
Associate Professor Jeffrey W. Herrmann
Associate Professor Mark Austin

© Copyright by
Seyed Soroush Bassam
2015

Dedication

This work is dedicated to my parents, Sharareh and Vahid, for their unconditional love and support.

Acknowledgements

I would like to extend my sincerest word of gratitude to my advisors, Dr. Jeffrey Herrmann and Dr. Linda Schmidt, for their continuous support during my research. This thesis would not have been possible without their encouragement and patience. I would also like thank Dr. Mark Austin for serving on my thesis committee.

Finally, I would like to thank the National Institute of Standards and Technology (NIST) for their financial support.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction

Physical Protection Systems (PPS) are intended to protect assets and facilities. A PPS is composed of people (e.g., a response force), procedures (e.g., alarm assessment), and elements (e.g., closed-circuit television (CCTV) cameras, sensors, and locks) that contribute to protecting assets against malevolent human operations such as theft and sabotage [1]. Assets include people, information, and property. Human actions and natural occurring threats can cause serious damage and are particularly important when it comes to critical infrastructure. For instance, losing information technology (IT) infrastructure for nine or more days can bankrupt an organization [2]. Therefore, mitigating the impact of damage to a business's critical infrastructure is a high priority. Today there is heightened awareness of the possibility of damage to an organization's assets from malicious actors, domestic and foreign. From 1970 to 2010, 98,000 cases of high-profile international and domestic terrorist attacks and disrupted plots occurred [3].

A PPS performs three functions: detect, delay, and respond. The PPS detects a threat (e.g., an intruder) by observing and identifying it. Elements in the PPS delay the threat by increasing the time needed for it to reach its target, which provides enough time for interruption. The PPS responds by intercepting and neutralizing the threat. A state-of-the-art PPS includes sophisticated sensor systems, automated responses, and modern communication and information technology.

In many occasions a PPS needs to be evaluated. Some enterprises with critical assets require such evaluations on a regular basis. External rules and regulations may require periodic assessments of PPS. Oftentimes an assessment is performed on the

PPS when a facility was recently under attack [4]. Various methods have been used to evaluate PPS. Vulnerability assessment (VA) (discussed in more detail in Chapter 2) is a process in which a PPS is evaluated. Garcia [4] described two distinct approaches for the analysis step in VA: compliance-based and performance-based. A compliance-based approach uses checklists and a site survey to verify the presence of specified security elements. A PPS is compliant if the correct equipment is installed in the right places. A performance-based approach, on the other hand, uses information about the performance of the security elements to estimate the PPS effectiveness by evaluating a quantitative model. The criticality of the assets and the desired level of protection determine which approach is most appropriate for evaluating a PPS. A compliance-based approach is appropriate when the loss of the asset has low consequences for the stakeholders. When dealing with more valuable and critical assets, however, a performance-based approach is more appropriate.

As PPS have become more complex, so have the approaches and tools available for conducting VA. Proprietary techniques and a lack of standards make sharing information between these tools difficult, however.

Systems engineering can be considered as a discipline, a process, and an approach [5]. As a discipline, it concerns with the system as a whole. It applies a holistic approach to the system and covers all socio-technical aspects of the system. In other words, it studies the interaction of the system within its context. Systems engineering is also a process. Estefan defined a process as a "logical sequence of tasks" [6]. Systems engineering has an iterative development process which consists of a sequence of tasks starting from requirements analysis, through detail design,

validation and verification. Moreover, systems engineering is an interdisciplinary approach, meaning it considers various aspects of the system, from different costumer and technical needs, to various stages of a system's lifecycle. Garcia [4] stated that vulnerability assessment follows basic Systems Engineering principles. Particularly, the performance-based VA process is founded on basic stages of the system development process, i.e. requirements analysis, design, and test [4] [5]. Therefore, the methods that are currently being used in systems engineering practices may be valuable to vulnerability assessment as well. This idea has been the main driver of conducting this research.

One method that is used in the systems engineering domain is Model-based Systems Engineering (MBSE). INCOSE defined MBSE as "the formalized application of modeling to support system requirements, design, analysis, verification and validation activities beginning in the conceptual design phase and continuing throughout development and later life cycle phases" [7]. When adopted, MBSE approaches result in higher productivity and less development risk compared to traditional document-based approaches [8]. Therefore, document-centered systems engineering processes will be replaced by model-based systems engineering processes [7], [8]. In MBSE, a set of interconnected models are built, instantiated, and used throughout the design process [8]. MBSE software enables the user to check these models for consistency. There are several benefits to modeling such as cost reduction and enhanced knowledge transfer [8]. MBSE facilitates the design and evaluation of a PPS by representing data about the facility, assets, PPS, and threats in a way that aids model-based VA approaches. Moreover, the use of a common modeling language used in

systems engineering (e.g. SysML) can provide the foundation for standards and tool integration in the future.

In this thesis, we review the VA process and show how the SysML models commonly used in MBSE can be used for VA The main research question is how we can use MBSE approach in performance-based VA. This thesis addresses what models can be used to store critical information throughout the VA evaluation process.

In Chapter 2, we review works that have been done on vulnerability assessment, requirement analysis, and model-based systems engineering. In Chapter 3, we discuss different methods and tools used in Requirement Analysis. Also, we provide a requirements modeling framework that can be used for requirement analysis in the context of performance-based VA. In chapter 4, we demonstrate the use of MBSE in VA by developing SysML diagrams for an example facility. In chapter 5, we describe future work that can extend this research.

Chapter 2: Literature Review

In this chapter, we provide some insights into the context of this research by reviewing relevant works that have been done in the past. First, we review the main concepts of security systems. Then, we address the process in which a security system is evaluated. Next, we point out some notes about MBSE.

2.1. Physical Protection Systems (PPS)

Physical Protection Systems (PPS) are intended to protect assets and facilities. A PPS is composed of people (e.g., a response force), procedures (e.g., alarm assessment), and elements (e.g., sensors, and locks) that contribute to protecting assets against malevolent human operations such as theft and sabotage [4]. People, including users, customers, and stakeholders, are involved with PPSs on different levels. A user may maintain or operate the system, e.g. response force. A customer is someone who owns the system. A stakeholder is someone who is involved in issues related to security of the entity and may impose requirements on the security system.

Another component of PPSs is procedure. It is important to distinguish between procedure, process, and tool. Estefan [6] provided the following definitions:

- Process: a logical sequence of tasks performed to achieve a particular objective.
- Method: a set of techniques for performing a task, in other words, it defines the "HOW" of each task. (In this context, the words "method," "technique," "practice," and "procedure" are often used interchangeably.)

- Tool: an instrument that, when applied to a particular method, can enhance the efficiency of the task; provided it is applied properly and by somebody with proper skills and training. [6]

A procedure is concerned with how each task is done. In the context of PPS, a procedure defines how people (e.g. response force) accomplish a task. An example of such a procedure is alarm assessment. Alarm assessment begins after a potential threat is detected. The objective is to determine if an actual threat has triggered the alarm. The second objective is to obtain information if it is a threat [4].

2.2. Vulnerability Assessment

Vulnerability Assessment (VA) is a process in which a PPS is evaluated. VA for a facility includes three key steps: determining the PPS objectives, evaluating the PPS design, and analyzing the PPS design. In the first step, one defines the PPS objectives by characterizing the facility and describing its specifications, defining potential threats, and identifying the assets that are potential targets. In the second step, one evaluates the PPS design by collecting information about PPS capabilities in functional areas of detection, delay, and response. In the third step, one analyzes the PPS design under scenarios likely within the set of threats to determine if it meets the objectives (that is, does it stop likely threats). If the PPS is inadequate, it should be redesigned. Otherwise, it is considered as the final PPS design (Figure 1) [4].

There are two types of vulnerability assessment: compliance-based and performance-based. In the compliance-based approach, one verifies the presence of PPS elements.

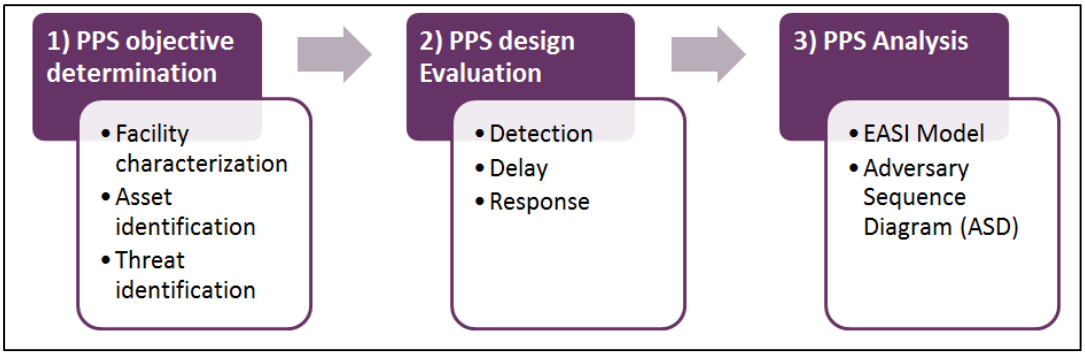

Figure 1 PPS evaluation process

In the performance-based approach, one not only addresses the presence of PPS elements but also evaluates the PPS overall performance. In the compliance-based approach checklists are used to document the information, whereas in the performance-based approach rigorous tools such as modeling and simulation are utilized. Factors that determine which approach should be adopted include threat level, criticality of assets, and the consequence of loss.

2.2.1. Objective Determination

Determining the objectives for a PPS requires collecting data about the facility, its assets, and potential threats. It is crucial to properly gather, organize, and represent the collected data [4].

Facility characteristics include its physical features and its operations. Garcia [4] provided a site description form that can be used to characterize the site, including the site boundary and buildings, room locations, entry points, and existing physical protection features. Physical protection features include fences, sensors, CCTV cameras, alarm communication and display (AC&D) systems, barriers, response force availability, and the response force response time. Also required is information about

the facility operations, including the major products, the processes that support these products, the work hours, emergency operations, and type and number of employees.

Facility characterization

Facility characterization is the first task in PPS objective determination. The core activity in this stage is data collection. Data collection is an essential part of VA for it enables quantitative analysis of PPS performance. Techniques and methods of data collection range from facility tours to document reviews to interviews with personnel. In a site tour, a VA team locates PPS components in the facility. It also collects information regarding the building physical characteristics, facility operations, facility states, etc. Document review is another way to collect information about PPS characteristics, and it is used to verify information gathered from other methods. Furthermore, interviews with personnel provide insight into facility operations and how the security system actually works. This information can be compared to PPS documents to see how differently the system functions. Testing is another method of data collection which provides information about functionality, operability, and performance of various PPS components.

Facility characteristics include its physical features and its operations. Garcia [4] provided a site description form that can be used to characterize the site, including the site boundary and buildings, room locations, entry points, and existing physical protection features. Physical protection features include fences, sensors, CCTV cameras, alarm communication and display (AC&D) systems, barriers, response force availability, and the response force response time. One important factor in facility characterization is facility states. Facility states may include normal operating hours,

non-operational hours, shift changes, and emergency situations. The PPS of a facility may have different behaviors in different states. For example, a CCTV's performance during the day might differ from its performance at night due to lighting variation. Also required is information about the facility operations, including the major products, the processes that support these products, the work hours, emergency operations, and type and number of employees.

The site description data sheet provided by Garcia [4] is organized in six sections:

- Facility characterization: includes physical conditions, facility operations, facility policies and procedure, regulatory requirements, legal issues, safety considerations, and facility goals and objectives.
- Physical facility condition
- Infrastructure details
- Physical site conditions
- Physical protection features
- Facility operations
- Supporting functions

AVERT modeling and simulation tools can be utilized to characterize the facility [9]. An AVERT model contains information about elevation, terrain, and building locations.

Threat definition

One step in determining the PPS objective is threat definition. At this step, one collects and organizes information about potential threats. This is an important step as the severity of threats determines the level of the protection needed. A threat is

defined by the adversary class, goal, motivation, and capability. The threat class includes insider, and outsider. An insider is classified as passive, irrational, rational nonviolent, and rational violent. A passive insider usually provides critical information needed to an outsider adversary. An adversary's goal ranges from theft to sabotage based on the facility's operational concept and its assets. Capabilities of an adversary include weapons and tools, transportation and technical expertise. This information is gathered using historical data, reports of previous incidents, etc. Information is then organized to be used later in the analysis process. Garcia [4] provided a sample data sheet for this purpose where threat information is organized in two tables. In the first one, information about the outsider threat is listed. Attributes of the table includes theft, sabotage, ideological, economic, personal, number, weapons, equipment tools, transportation, technical expertise, and insider assistance. In the second table, insider information is listed. An insider's role includes PPS designer, control, operator, maintenance, guard, and manager. For each role, information about the access to asset, access to PPS, access to vital equipment, theft opportunity, sabotage opportunity, and collusion opportunity is listed.

Asset identification

At this step, one identifies and prioritizes assets. This determines different levels of protection as assets may be of different value to an enterprise. Assets can be prioritized by the consequence of loss.

Once information about threat and asset is gathered, one can use a threat/asset matrix in order to compose and demonstrate the data. In a threat/asset matrix, columns represent consequence of loss and rows represent the probability of attack. Each cell

demonstrates a threat level, an associated consequence of loss, and the probability of attack.

2.2.2. PPS Design Evaluation

The main activity when evaluating PPS design is collecting data about PPS elements. This part of the VA evaluation process is divided into three subsections based on PPS functionalities: detection, delay, and response.

PPS Detection

Detection is defined as "notifying an unauthorized action" [1]. Detection is a sequence of functions; an authorized action is detected, an alarm is communicated to response force, and the alarm is assessed. The detection function involves sensors, alarm assessment, entry control, and alarm communication subsystems.

Sensor

Sensors are classified into two types: exterior sensors, and interior sensor. Exterior sensors have the following attributes:

- Passive or active
- covert or visible
- line-of-sight or terrain-following
- volumetric or line detection
- application

Metrics that define exterior sensors are probability of detection, Nuisance Alarm Rate (NAR), and vulnerability to defeat. Probability of detection is the probability that a sensor detects an unauthorized action. NAR is the number of nuisance alarms (i.e. alarms that are not caused by an unauthorized action) over a period of time.

Vulnerability to Defeat is the sensor's deficiency against bypassing and spoofing. Interior sensors have the following attributes:

- Passive or active
- covert or visible
- volumetric or line detection
- application

Interior sensors measures are the same as exterior sensors: Probability of detection, NAR, and Vulnerability to Defeat. More detailed information about sensors is provided by Garcia [1].

Alarm Assessment

An essential part of detection function is assessment. Probability of Assessment (PAs) determines the speed and accuracy of assessment and is the measure of performance. Assessment is done either by security personnel or by CCTV. Using CCTV is preferred as assessment by personnel is not as effective in terms of time. The following parameters are metrics that define video assessment capabilities:

- minimum time between alarm and video display
- assessment zone
- the ability to classify target
- vertical field-of-view
- continuous operation
- sensitivity to environmental conditions
- obscuration of the assessment zone
- camera field-of-view

Garcia explained these parameters in more detail [1]. A video assessment system is composed of the following:

- cameras and lenses (Pan-Tilt-Zoom (PTZ) vs Fixed; Black and White vs. color)
- camera housing
- camera mounting
- lighting
- signal transmission
- recording and storage
- monitors
- procedures

Entry Control

An entry control system aims to distinguish between an authorized person and an intruder. It is usually installed on the facility's boundary and gives access to authorized persons. Main functions of an entry control system include giving permission to authorized person, and preventing passage of contraband materials. Metrics for entry control system performance are throughput and error rate. Throughput is defined as "the rate at which an authorized person pass through an entry control system." Error rate is determined by: 1) rejection of authorized person and 2) acceptance of unauthorized person. Personnel entry control is processed using personal identification number, credentials (e.g. photo identification badge), or biometrics (e.g. fingerprints). Moreover, contraband detection is done using manual search, metal detector, explosive detection, etc. Using locks is another way to control

the entrance. It is important to choose a lock that is on the same level of performance as the whole barrier. This principle is called balanced protection. Two major elements of a lock are fastening device (e.g. latch), and the coded mechanism (e.g. key).

PPS Delay

After an adversary is detected, there should be enough time for response force to arrive at the location. For a successful interruption, the time it takes the adversary to accomplish the attack should be more than the time it takes for the response force to arrive. So, a major functionality of the PPS is to provide delay. PPS components that aim to provide delay include perimeter barrier, structural barrier, and dispensable barrier. Perimeter barriers are installed on the facility's perimeter and build the first layer of protection. Fences, gates, and vehicle barriers are different types of perimeter barrier. Structural barrier includes the elements in the facility's structure such as walls, doors, windows, utility ports, roofs, and floors. Dispensable barrier adds more protection when it is required, e.g. when there is an attack. There are two types of dispensable barriers: active and passive. Passive dispensable barriers are less costly than active barriers. On the other hand, active barriers accept commands.

PPS Response

Response function begins when an alarm is processed. Main measures of performance associated with response are response time and neutralization. Response time is defined as "the time between alarm verification and interruption." Neutralization is the ability to defeat the adversary, given the interruption. Response time will be used to estimate the probability of interruption. Together with probability of interruption,

probability of neutralization gives the PPS effectiveness, which is the overall PPS performance measure.

2.2.3. PPS Analysis

PPS analysis is the third and last step of the PPS evaluation process. All information gathered in PPS objective determination and PPS design phases is used in the analysis. At this step one determines the overall PPS effectiveness and compares it to the requirements of the system. If the existing model meets the criteria stated in the requirements, it is considered as the final PPS design. Otherwise, one considers redesigning the PPS and starts the evaluation process over. In this chapter, we first introduce measures and parameters that will be used in the analysis. Then we introduce tools and techniques used throughout the process.

Quantitative analysis process

Analysis procedure starts from estimating performances using information about functional areas of detection, delay, and response. Next, a path analysis is conducted to identify possible pathways to different assets. Then, scenarios are generated for each path and defeat tactics is reviewed. The output of this analysis is the probability of interruption and the probability of neutralization. In order to come up with a more accurate estimate of neutralization capability more analysis is needed. At the analysis step, one can look at a facility and its security system from different points of view.

In what follows, we summarize steps in the analysis process.

Facility Description

At this step we organize the information about the facility (discussed in section 2.2.1).

Path Analysis

In the path analysis, one determines the weaknesses of PPS. To do so, one needs to compose collected data on the facility, PPS, and adversary. When composed, the data shows all possible pathways to an asset. Several factors are important in defining pathways. A threat chooses a pathway based on based on his tactics, tools, etc. Also, the criticality of a path is related to the probability of detection of PPS components along the path. Other factor that may be considered in pathway analysis is the time of adversary as daylight affects PPS components' performance.

An Adversary Sequence Diagram (ASD) is a tool used in pathway analysis to graphically depict pathways. An ASD consists of physical area (such as sites, buildings, etc.), protection layers in between them, and the adversary path. An ASD helps an analyst identify various possible pathways and is useful in multiple pathway analysis [10]. An ASD shows the different areas along the path as well as security elements. In order to transit from one area to another an adversary has to break through or overcome a security element that connects two areas.

An ASD shows where the attack starts, what PPS components an adversary needs to pass, and what area he needs to enter to reach the target asset.

Scenario Analysis

In the pathways analysis, we identified pathways with low interruption probability to different assets. . We also graphically showed pathways to a specific asset as well as protection layers and physical areas along the pathway. This gives information required to initially estimate the performance parameters for an attack. However, factors such as varying tactics for a pathway have not been taken into consideration.

In other words, one needs to consider effect of threat's characteristics as well as facility states on a pathway. Through scenario analysis, one can come up with a more accurate estimate of PPS performance. Pathway analysis provides input information for scenario analysis. In a scenario analysis, one incorporates information about threat capabilities and facility states (e.g. closed or open) into the pathway analysis. Then, the procedure refines the performance estimate in the pathway analysis. One writes descriptions for each task, which provide detailed information that will be used later for performance calculations. These refinements are then used by the pathway analysis. One should document all assumptions made throughout the process. Adversary task timeline is a table used in scenario analysis to document information [4]. For each adversary task, task time, cumulative task time, and assumptions and descriptions are listed in the table.

In the scenario analysis, one uses the aforementioned information to reduce the set of possible pathways to those that are credible. For example, if two pathways share the same detection element, an adversary will choose the one that is farthest from the location of the response force because that increases the time until interruption.

Estimate Neutralization

The probability of neutralization is defined as the probability that the response force defeats the adversary in a face-to-face engagement [10] [1]. Factors that impact neutralization includes threat characteristics (such as numbers, weapons, training, and tactics), response force capabilities (numbers, weapons, training, response) and detection and delay elements [10].

System Effectiveness

The most critical pathway is chosen in the previous analyses. Now, one can estimate the probability of interruption, which will be used later in calculating the overall PPS effectiveness. One of the main tools used in this part is The Estimate of Adversary Sequence Interruption (EASI).

Developed by Sandia National Laboratories, EASI is a quantitative analysis tool that determines the PPS performance for a specific threat and attack scenario [1] [4]. The EASI model uses performance characteristics of security elements and parts of the building structure, including probability of detection (the probability that a security item detects the adversary) and delay (the time it takes for the adversary to pass a security element). The time required for a response force to stop an adversary is also an important factor. The EASI model can also determine a PPS's Critical Detection Point (CDP), which is the last point at which, if the PPS detects the adversary, the response force can stop the adversary before the attack is completed [10].

Optimizing the PPS design includes increasing the likelihood of detecting the adversary before the CDP and increasing the delays afterwards. So, identifying the CDP plays a key role in PPS design and optimization. There are multiple pathways that an adversary can use to reach an asset. Each pathway has its own CDP because a pathway has different security elements with different characteristics. For each pathway, one could use EASI model to determine the CDP and consequently, probability of interruption. An example of applying the EASI model is shown in Chapter 4. Equations 1, 2, and 3 describe the calculations that take place within the

EASI model. The output of the model is the value of the probability of interruption which is used to determine the PPS effectiveness.

Let J be the number of PPS elements along an adversary's path where timely detection can occur [10]. Let P_j^D be the probability of detection for item j, j = 1, …, J. Let β_j^D be the non-detection probability of the component j:

$$\beta_j^D = 1 - P_j^D \tag{1}$$

Let β_D be the probability of non-detection, which is the probability that the adversary is not detected by multiple independent elements:

$$\beta_D = \prod_{j=1}^{J} \beta_j^D \tag{2}$$

The probability of interruption is the probability that the response force interrupts the attack. Let P_I be the probability of interruption:

$$P_I = 1 - \beta_D = 1 - \prod_{j=1}^{J} \left(1 - P_j^D\right) \tag{3}$$

The probability of neutralization is the probability that the security response force can successfully confront and stop the threat given they are notified timely. Let P_N be the probability of neutralization, and let P_E be the system effectiveness, which measures the level of adequacy of the PPS for a defined threat:

$$P_E = P_I \cdot P_N \tag{4}$$

The EASI model's advantage is that deviations associated with RFT and adversary task times are included in the calculations whereas tools like Analytic System and Software Evaluating Safeguards and Security (ASSESS) rank vulnerabilities using mean time only [10] [1].

The EASI model inputs are PPS performance in areas of detection, delay, and response. Detection capabilities of the PPS appear as probabilities while delay and response appear as mean times and standard deviations. As discussed earlier, Probability of detection is a measure of detection capability of PPS. Many factors contribute in the probability of detection such as threat attributes, assessment, sensing, and transmission. P_D can be calculated as

$$P_D = P_D \times P_T \times P_A$$

Where P_S is the probability that a sensor will sense an intrusion, P_T is the probability of successful transmission of an alarm, and P_A is the probability of successful alarm assessment.

Response Force Time (RFT) is a measure of PPS's response capabilities. It is the time it takes to interrupt an intrusion. It includes time it takes to communicate and assess the alarm, plus time for guard communication, preparation, travel, and deploy [4] [10]. Moreover, adversary task time is the time it takes an adversary to perform a specific task. Since there is an uncertainty associated with these parameters, they are represented as mean times and standard deviations.

Another important factor in EASI calculation is the sequence in which detection and delay are performed. Each adversary task in EASI is labeled as *B*, *M*, or *E*. When detection is performed before delay during a task, a *B* label is used. When detection is performed after delay, an *E* label is used. The *M* label indicates that both functions are performed simultaneously.

It is important to understand the goal of an attack as it affects the estimations. In a sabotage, the attack ends when the adversary reaches and destroys the asset, whereas

in a theft an adversary needs to exit the facility to be successful. That means PPS components along the path have to be defeated twice.

2.3. Model-Based Systems Engineering

In a model-based systems engineering approach, one develops models that express the structure and behavior of the system. In a structure model information about features of system components as well as relationships among them is stored. A behavior model shows various states of system components and the sequence of actions within the system.

The Unified Modeling Language (UML) is a general-purpose graphical modeling language that is used in various stages of software development. It provides a standard framework to generate models that describe the underlying software [11]. The Systems Modeling Language (SysML) is a specialized version of UML that exists to customize UML to better support modeling systems engineering processes [8]. SysML can be used to build models that describe a system's structure and behavior. This thesis describes the use of SysML structure diagrams (e.g., block definition diagrams or BDDs) to describe a facility and its security system. We also describe behavior diagrams (e.g., activity diagrams) for modeling a threat attack scenario. Moreover, we use requirements diagrams to analyze requirements within the context of VA. Although SysML is partially model-oriented, it has not improved UML model orientation significantly. For example, the nature of requirements modeling in SysML is still textual [12].

Extensive works have been done on VA. Garcia [1] [4] provided valuable insight into compliance-based as well as performance-based VA. However, there is a little work

done on applications of MBSE in performance-based VA. Since the VA process is based on the systems development processes that are used in systems engineering [4], it may be valuable to investigate potential application of MBSE in this domain.

This research is intended to address this gap. In the following chapter, we study potential applications of MBSE on VA processes defined in the literature.

Chapter 3: Requirements Analysis for Vulnerability Assessment

Requirement analysis plays a key role in performing VA. Through requirement analysis, the needs of users, stakeholders, and customers are identified. In fact, the requirements determine whether or not PPS effectiveness is sufficient. In order to evaluate a PPS, one needs to validate performance characteristics of the PPS against requirements. Sources of requirements range from stakeholder's needs to standards and regulations. In general, requirements can be classified as follows:

Functional Requirements. Functional requirements are the needs and expectations of the user in terms of system's functionalities. Functional requirements can be traced back to higher level requirements, also known as business requirements [13]. In VA, functional requirements refer to the user, customer, and stakeholder needs [4]. A high level requirement for every PPS is "PPS shall protect assets from threats [4]." Therefore, in order to derive functional requirements, one needs information regarding assets and threats. As discussed in chapter 2, this information is gathered and organized in PPS Objective Determination phase of PPS evaluation process. Use case diagrams are recommended to use for capturing high-level functional requirements [8].

Garcia [4] listed a set of generic functional and non-functional requirements. Requirements are classified based on their corresponding subsystems: Communications, Event Annunciation, Display Console Interface, Video, Access Control, Redundancy, Configuration Information Management, Printing/Logging, System Privileges/Password Control, Sensor Mode Control, Device Control, Ergonomics, Power, Maintenance, Archive/Backup, and System Software.

Non-functional Requirements. Also known as constraints, or implementation requirements, non-functional requirements impose limitations on functional requirements [13]. Non-functional requirements address quality, implementation, and life cycle issues [13]. In VA, different sources including regulations, legal liabilities, standards, organization's policies and procedures, and operational environment may impose constraints [4]. When performing VA, one must consider conformance of the PPS with non-functional requirements.

Performance Requirements. These requirements state the expected level of performance for a system and are derived from stakeholder's need statements (i.e. functional requirements) [4] [5]. Measures of Performance (MOPs) are used to quantify the system's performance characteristics [5]. Example of performance requirements in VA include probability of detection, delay, probability of interruption, and earned value [4]. Deriving performance requirements requires information about threat capabilities. As discussed in chapter 2, this information is gathered through the first phase of PPS evaluation process, PPS objective determination.

Figure 2 is a context diagram that shows the role of requirement analysis in the context of VA.

3.1. Requirements analysis tools

Various approaches in requirement analysis include text-based requirements management and requirements modeling. Different tools have been designed for each approach. These tools include requirements management tools and requirements

modeling tools. A requirements management tool uses a database that facilitates storing information related to requirements and their relationships [8].

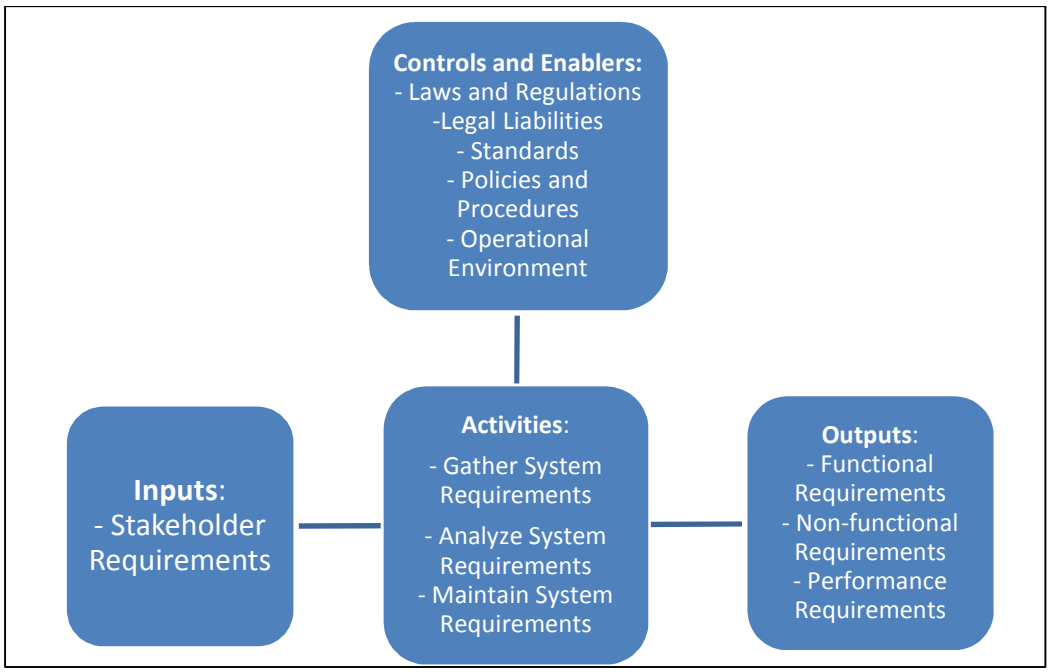

Figure 2 Context Diagram for Requirements Analysis in VA

A requirements modeling tool acts as a liaison between a requirement management tool and system models [8]. Requirements modeling tools ensure that the requirements stored in a requirements management tool are consistent with system model elements. Also, these tools provide the user with an ability to trace text-based requirements stored in the database to system model elements throughout the system development process [8], [14]. IBM Rational DOORS, a requirements management tool developed by IBM, is an example of a database tool. It provides the user with a spreadsheet to store requirements.

Furthermore, one may use requirements modeling software tools such as MagicDraw [15]. MagicDraw enables modeling in UML and SysML languages [15]. In SysML

language, there is a diagram specifically designed for the purpose of requirements analysis.

Requirements management tools can play a key role when it comes to handling a large set of requirements (e.g. PPS and facility requirements). They also facilitate conformation with requirements analysis standards. Moreover, they enable users to export requirements to word processor software. On the other hand, requirements modeling tools link requirements to models. They provide a graphical representation of requirements and their relationship through a standard notation [14]. They graphically show what requirements are imposed to each system component. Furthermore, SysML formally defines interfaces between subsystems and finds conflicts between them, whereas in a requirements management tool it is hard to detect such conflicts.

A VA specialist needs to gather requirements, store them, and use them in justifying performance of PPS. For storing requirements, requirements management tools such as IBM Rational DOORS seem to be appropriate. Also, a requirements modeling tool such as SysML requirements diagram facilitates analyzing PPS structure and behavior.

3.2. Comparing Requirements Analyses

As mentioned before, there are two techniques in VA: compliance-based and performance-based. In this section we will study the role of requirements analysis in each of these approaches and point out the differences. Then, a requirements analysis framework for performance-based VA will be proposed.

3.2.1. Requirements Analysis in Compliance-Based VA

In a compliance-based approach, one relies on checklists to keep track of PPS element presence. These documents mostly address functional and–in some cases– non-functional requirements. However, there is little indication of performance requirements and MOPs. In other words, compliance to non-functional requirements derived from standards and regulations appears in the form of presence. In this technique, requirements are based on policies, and the MOP is replaced by considering a component's presence.

3.2.2. Requirements Analysis in Performance-Based VA

A performance-based VA technique considers not only the presence of PPS elements but also their performance against various conditions and scenarios. In this technique, requirements are based on the PPS overall performance (i.e. System Effectiveness). In other words, all forms of requirements are considered. In fact, performance-based VA includes requirements analysis as it is founded on system development process [4].

3.3. A Modeling Framework for Requirements Analysis

As shown in Figure 2, the main source of requirements analysis is the stakeholder's needs. Also, standards, rules and regulations (modeled as controls) play an important role. Figure 3 shows an overview of requirements hierarchy.

A requirements diagram in SysML may contain several individual requirements and their relationships. Each requirement is represented as a "requirement" block and consists of the following parts:

- Title

- ID
- Text

A set of attributes may be defined for each requirement in order to facilitate assessment throughout the evaluation process [13]. Typical examples of these attribute include source, priority, Validation and Verification (V&V) criteria, ownership, and absolute reference [13]. Attributes should be defined based on the context of project [13].

Requirements relationships in SysML include containment, derivation, satisfaction, verification, refinement, and trace [8]. A containment relationship is used to decompose a high-level requirement to a set of low-level requirements. A derivation relationship relates a source requirement to a derived requirement. A satisfaction relationship relates a requirement to a model element that satisfies it. The relationship between a requirement and a test case that verifies it is depicted through the verification relationship. A refinement relationship links a model element to a requirement to reduce ambiguity. A trace relationship can be used to link a requirement to a document [8].

Figure 3 is a high level overview of performance requirements modeling framework for performance based VA. As shown in Figure 3, the performance requirement at the highest level is derived from functional requirement package diagram. This requirement maps the desired level of security stated in the functional requirement package to a level of PPS System Effectiveness. As discussed earlier, System Effectiveness is the product of interruption probability and neutralization probability

(equation 4). Therefore the system effectiveness requirement must contain a requirement for interruption capabilities as well as neutralization capabilities.

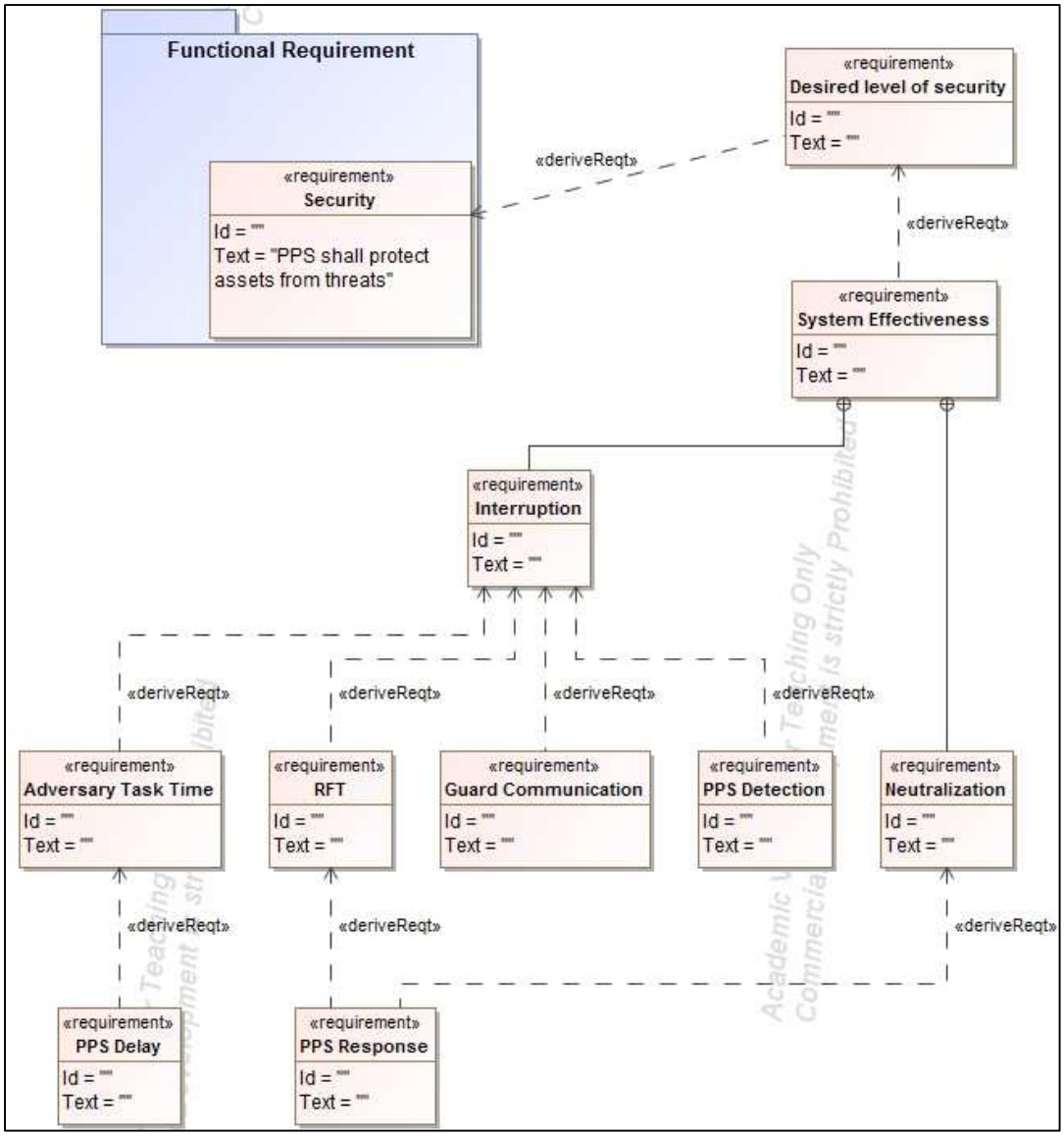

Figure 3 Requirements modeling framework for VA

3.4. Characteristics of a "good" requirement

Various guidelines have been generated for requirements analysis. SMART requirements propose the following characteristics: Specific, Measurable, Attainable,

Realisable, and Time-bounded [16]. INCOSE [5] indicated the following as characteristics of a "good" requirement:

- **Necessary**: Since writing and maintaining requirements are costly and time-consuming, one should avoid unnecessary requirements. Requirements that are covered by other requirements and unnecessary design specifications are examples of unnecessary requirements.
- **Implementation Independent**: Requirements should not specify design, i.e., they should state what are the expectations from a system, not how a system meets those expectations.
- **Clear and Concise**: A requirements should be interpreted in only one way. Using "and", "or", and commas are discouraged as it may cause ambiguity.
- **Complete**: As an input for the designer, a requirement must convey all necessary information in terms of expected characteristics.
- **Consistent**: Consistency of requirements is an important factor as many different sources (such as industry standards) may impose requirements on the same specification.
- **Achievable**: Implementing designers must ensure the achievability of requirements. Other parties that may be involved in this include manufacturers, customers, and users.
- **Traceable**: One must ensure that a requirement traces to higher level requirements.
- **Verifiable**: Requirements should be verifiable through one of the following methods: inspection, analysis, demonstration, or test.

The University of Maryland's Office of Facilities Management published the Design Criteria/Facilities Standards [17], which provides guidelines for the design of the university's existing and new buildings. This document contains requirements for building security systems that shall be applied to all new construction and renovation projects [17]. Section 1.08 of the document specifically addresses the intrusion detection aspect of security systems. Requirements in this section were evaluated based on engineering judgement against the criteria identified by INCOSE. The degree to which each requirement meets the criterion was indicated by YES (the criterion is met), NO (the criterion is not met), and PARTIALLY (the criterion is partially met). The results are shown in Appendix A. Although the selected requirements generally meet most of the criteria, 8 of the 16 requirements fail to meet the "clear and concise" criterion.

Requirement analysis is a crucial activity in VA. Using requirements modeling tools such as the SysML Requirement Diagram can be valuable. A requirements model facilitates traceability [13] [8]. One can easily examine how a requirement is related to other requirements in the hierarchy. Also, it facilitates consistency where requirements from different sources are imposed to a system component. When integrated with other models such as PPS and Facility model, one can show what components of the PPS satisfy a particular requirement.

Chapter 4: Using SysML for Vulnerability Assessment[1]

This chapter illustrates the use of SysML models for VA by considering the example of a Secure Cargo Area (SCA) facility that was presented by Garcia [4] , who provided a detailed layout of the facility (Figure 7). The SysML models generated in this chapter are based on the information provided by Garcia. It is not the purpose of this chapter to verify the completeness of that information but to use SysML models to store available data.

In this chapter, we apply performance-based VA to an example facility. First, we perform requirements analysis through requirements modeling, as discussed in

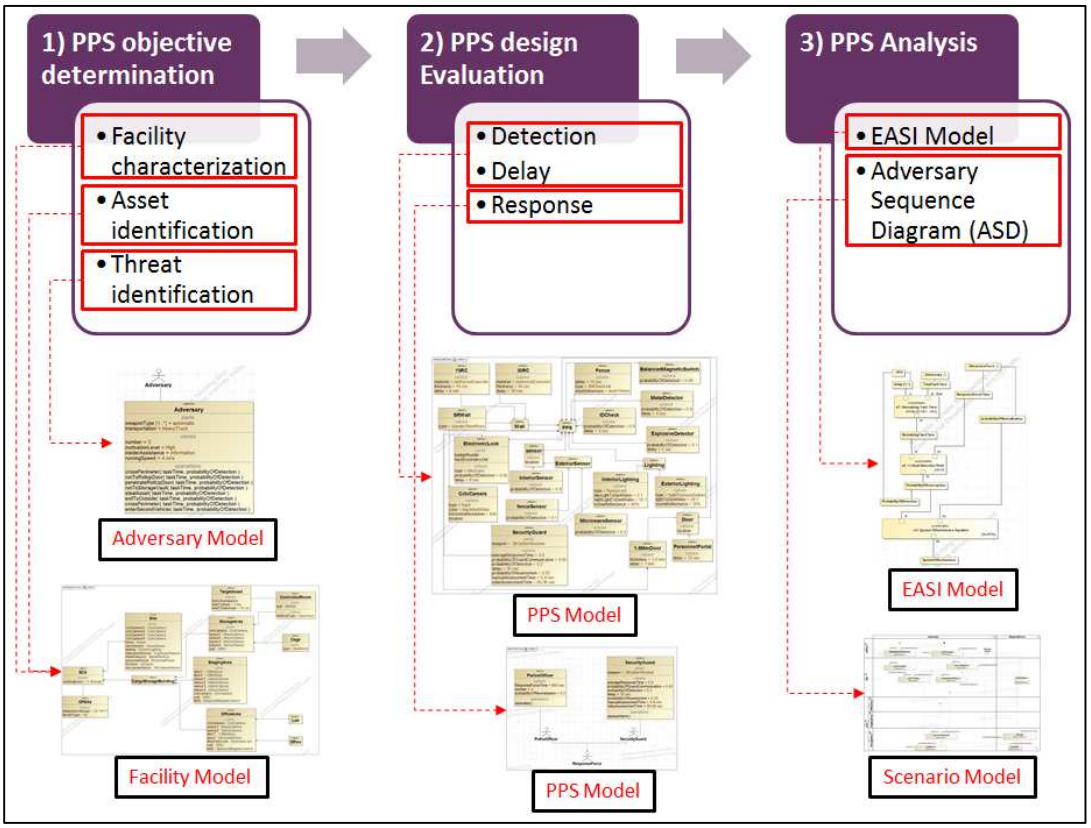

Figure 4 VA evaluation process and corresponding SysML Models

[1] Parts of this chapter have been previously published and presented in 2015 CSER conference.

Chapter 3. Then, we use the VA evaluation process discussed in Chapter 2.

For each step in the process, we develop SysML models to store the information. Figure 4 shows how these models are associated with steps in evaluation process. As indicated, for objective determination step, BDD diagrams are developed to store the information about the facility, asset, and the adversary. Next, BDD diagrams are created to represent PPS structure. Finally, a parametric diagram as well as an activity diagram is used in the PPS Analysis phase.

4.1. Requirements analysis

Requirements were derived from the information provided by Garcia. Figure 5 illustrates a portion of functional requirements. As discussed earlier, performance requirements are derived from functional and non-functional requirements. In this example we determine PPS's performance requirement based on stakeholder's requirement on risk level.

One can map a risk level to a corresponding level of PPS effectiveness using the following equation:

$$R = P_A \times (1 - P_E) \times C$$

Where R is the expected level of risk (determined by stakeholders), P_A is the probability of an adversary attack (determined based on previous attack data) and C is a normalization factor. Since Garcia [4] did not provide stakeholder's expectation as well as history of previous attacks, we assumed that the stakeholders expect a risk level of 0.1 which is mapped to a corresponding PPS effectiveness of 0.6.

This mapping is an indication that performance requirements were derived from functional requirements (Figure 6).

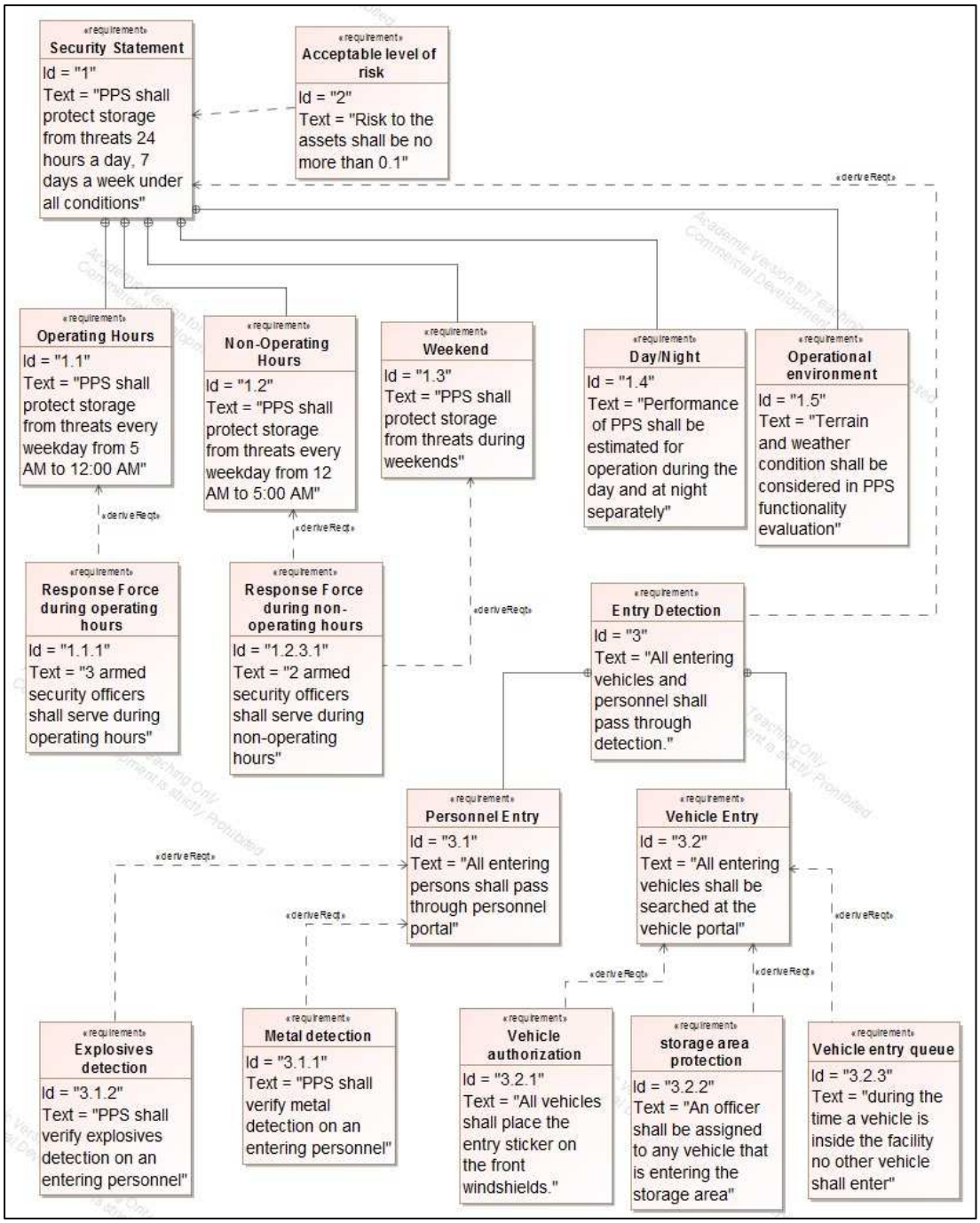

Figure 5 Functional and non-functional requirements representation using SysML Requirement Diagram

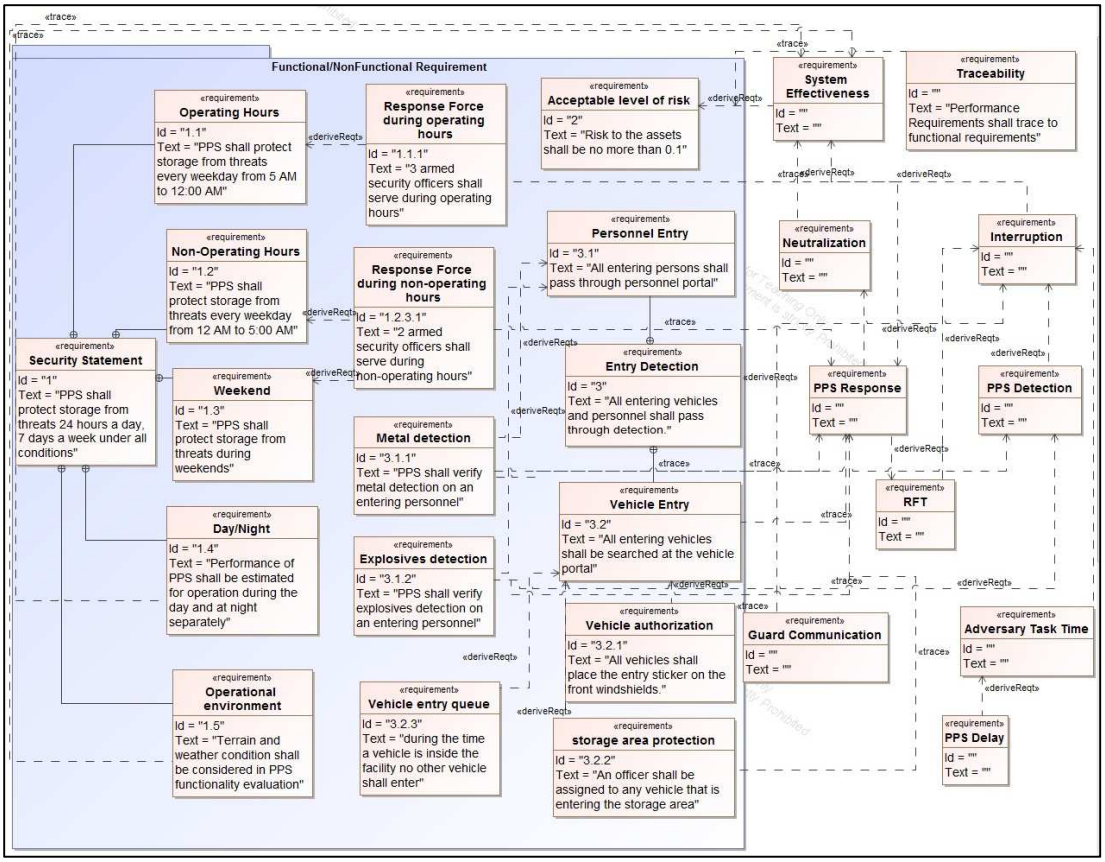

Figure 6 Performance requirements derived from functional/non-functional requirements

4.2. PPS objective determination for SCA facility

4.2.1. SCA facility characterization and asset identification

The building is in the middle of a rectangular plot that is surrounded by the facility perimeter fence; a gate in the perimeter allows vehicles to enter the facility. The main building has a staffing area, a storage area, and a staging area. Engineers, clerks, and security managers work in rooms in the staffing area. In the storage area, cargos are stored in cages, and environmental chambers and sensitive cargos are stored in a separated controlled room, where the asset is located. A portal connects these two areas. The storage area is connected to the staging area by a second portal through which cargo are moved.

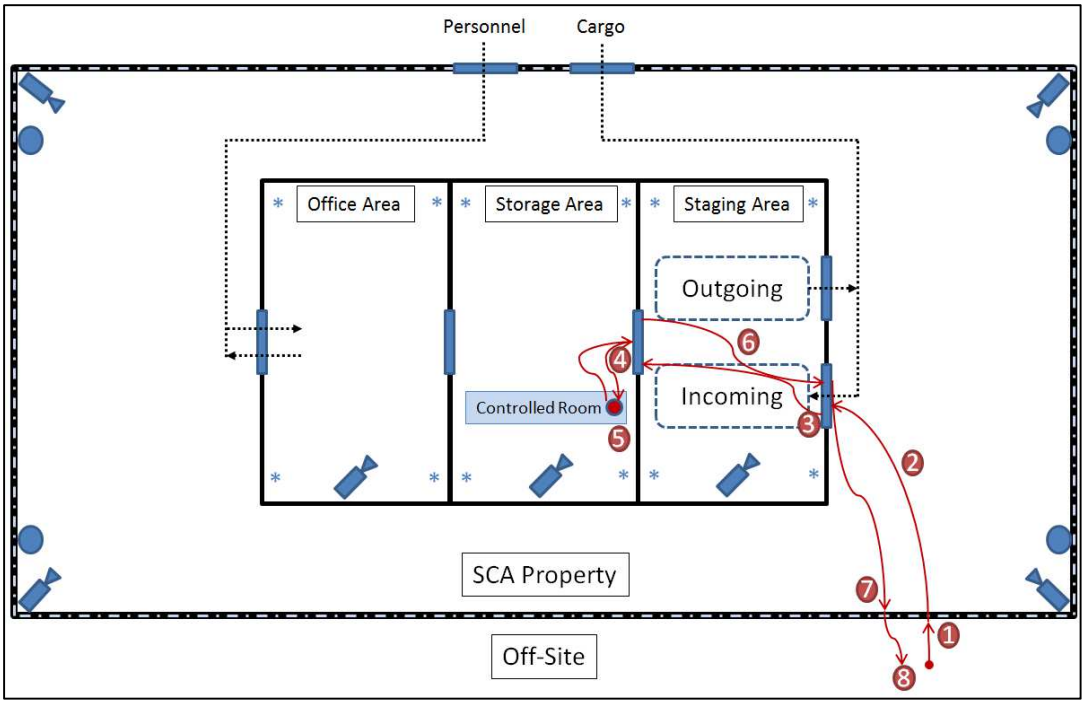

Figure 7 Layout of the SCA facility (adapted from Garcia [4])

Table 1 List of elements used in the layout of the SCA facility

Element	Icon
Fence	
Exterior Sensor	
CCTV	
Light	
Gate/Roll-Up Door	
Interior Sensor	*
Wall	
Personnel/Cargo flow	
Asset	
Adversary Path	
Adversary Task	

The staging area has two sections: outgoing staging and incoming staging. Cargo is moved to this area through a corridor that is connected the entrance gate. The layout of the facility is shown in Figure 7. Table 1 lists the symbols used in the figure. Figure 8 is a BDD of the facility.

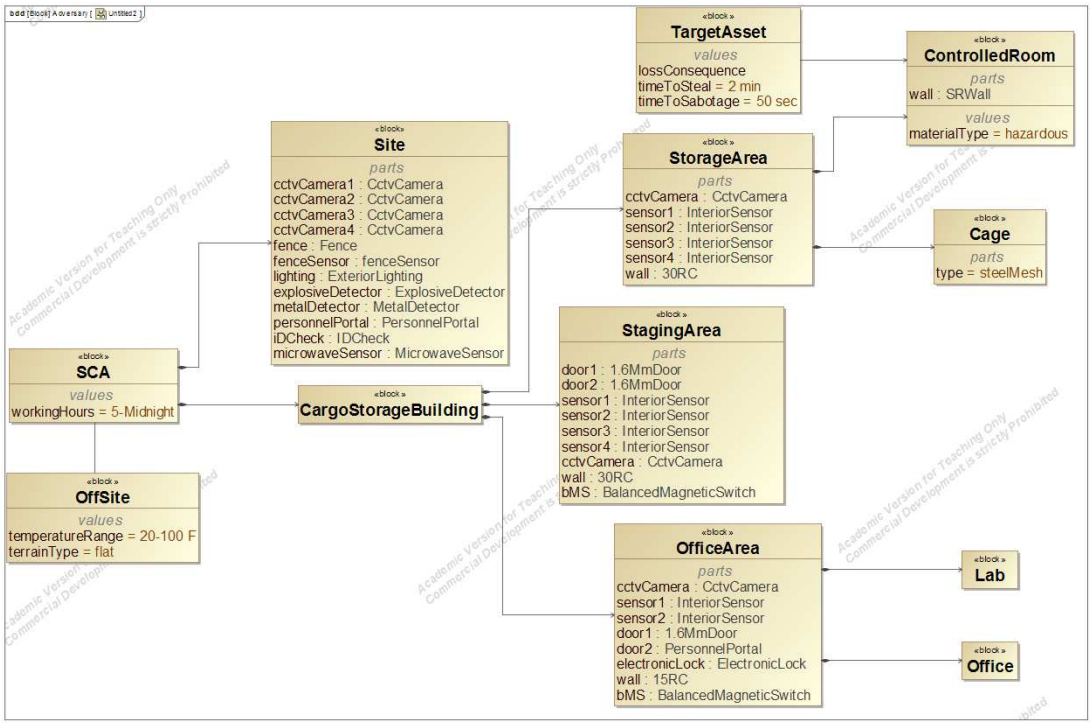

Figure 8 BDD for facility characterization and target (asset) identification

4.2.2. Threat identification

Figure 9 is a BDD for the threat. Attackers are equipped with power tools and weapons. They have received information from an insider and planned their attack based on that information. The three attackers are highly motivated, competent and able to run 4 meters/second.

4.3. PPS Design Evaluation

Since detection and delay functions are closely related, we address both at the same time.

4.3.1. PPS detection and delay

A fence located on the facility's perimeter separates the facility property from adjoining areas. There is a set of vibration sensors installed on the fence. Also, at each

corner there is a fixed CCTV as well as two exterior lights to provide visibility. To further increase to detection capability at the perimeter, several microwave sensors are installed. The entrance gate is equipped with metal and explosive detectors. In the staffing area, there are two interior microwave sensors at the end of the hallway as well as a fixed CCTV.

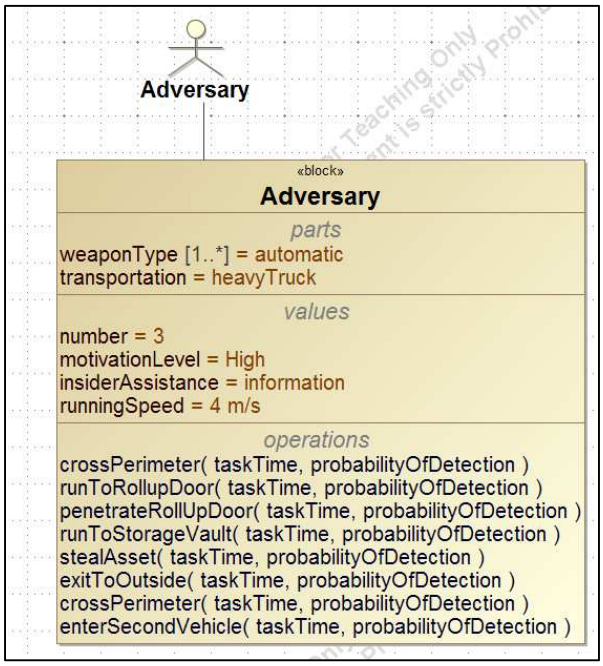

Figure 9 BDD diagram for threat identification

The wall of the staging area is 30-cm reinforced concrete. The wall of the staffing area is 15-cm reinforced concrete wall. The staging area and the storage area are protected by four interior microwave sensors and a CCTV. The PPS elements are shown in Figure 10.

4.3.2. PPS response

As discussed earlier, a BDD stores the information of system components as well as relationship amongst them. As an example, the BDD shown in Figure 11 indicates that the security guard and the police officer actors are types of the more general

model for response force actor. A security guard assesses alarms. He also has a weapon, which is modelled as a part property. Also, different parameters are related to the security guard such as the average response time and the assessment time and are stored in the block.

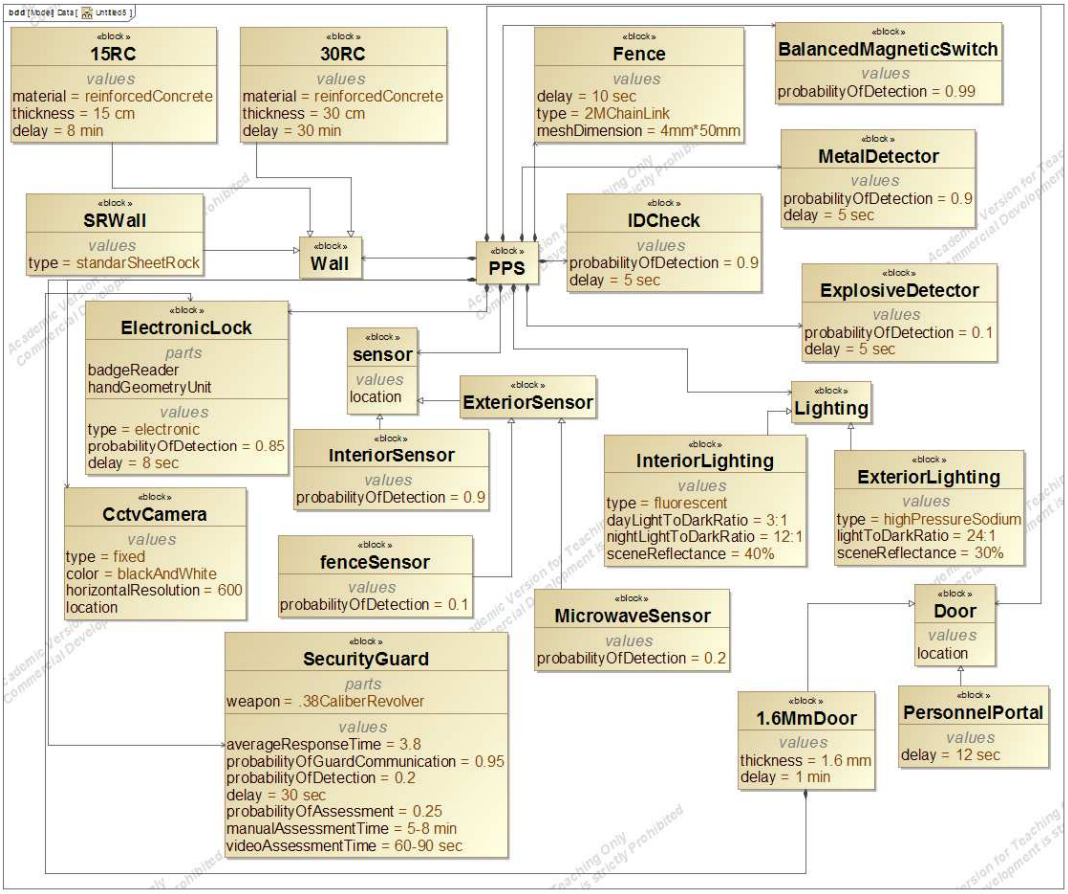

Figure 10 BDD for PPS detection and delay functions

Note. It is important to distinguish between a block and its instances. A block is a representation of an entity and describes some of its characteristics [8]. While instances of a block have these characteristics, they may differ in the values of some characteristics [11] [13]. For example, in the BDD corresponding to the SCA facility, the part "cctvCamera1" in the block "Site" indicates that the CCTV Camera 1 in the site is an instance of the block "CctvCamera" in the PPS BDD diagram. In other

words, there are four CCTV cameras in the site which are instances of the CCTV block in the PPS diagram. That means they share common characteristics indicated in the PPS diagram, i.e., type, color, and horizontal resolution, but they are installed in different locations.

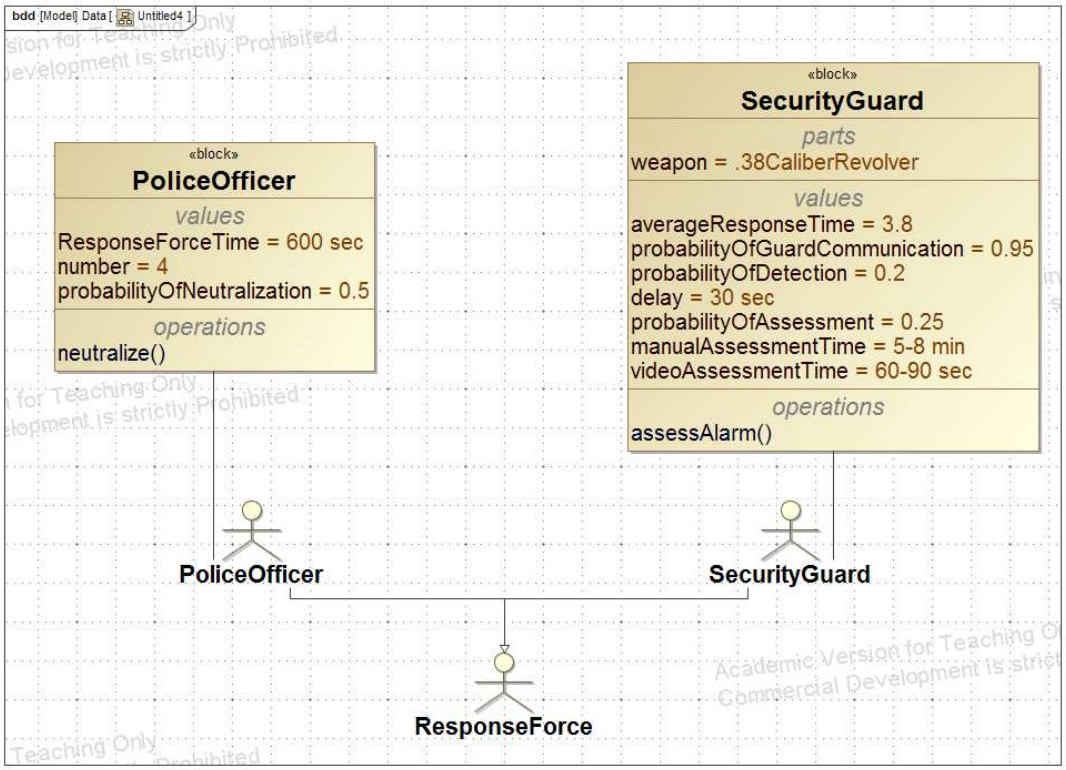

Figure 11 BDD for PPS response function

4.4. PPS Analysis

In the previous section, we developed SysML models to store and present information required for evaluating PPS design. In the PPS analysis step, we use those models to analyze the PPS performance. As discussed in chapter 2, PPS analysis includes the following steps:

- Facility description (discussed in section 4.2.1)
- Path analysis

- Scenario analysis
- Estimate Neutralization
- System effectiveness
- Upgrade analysis

4.4.1. Path analysis

There are various pathways to the target asset. As discussed earlier, an ASD diagram provides a better understanding of different possible pathways to the target asset. Figure 12 shows various areas such as off-site, the SCA property, and the cargo storage building as well as protection layers in between them. Also, the pathway corresponding to the attack scenario is shown in the figure with a dotted red line.

Figure 13 is an activity diagram that shows the activities of an adversary and the response force. It stores information about the location of each adversary task, sequence of actions, and involvement of different actors.

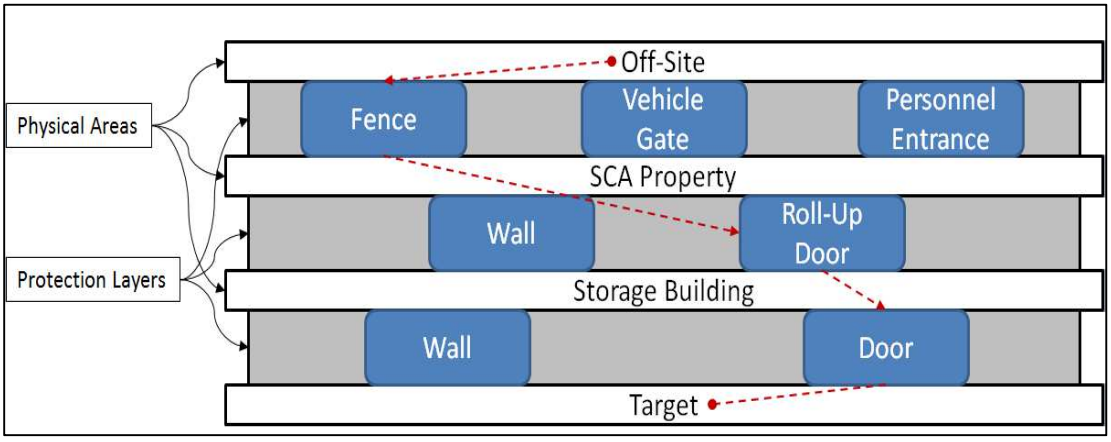

Figure 12 ASD diagram for the example attack scenario. The dotted red line is the adversary pathway. (adapted from Garcia [4])

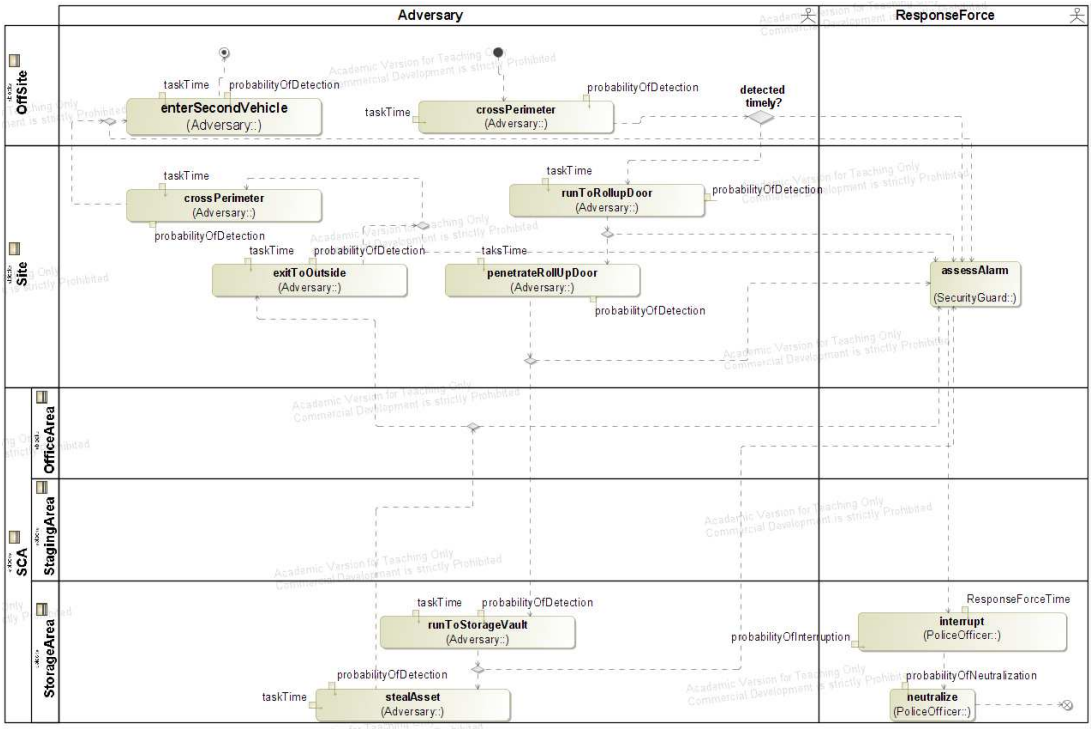

Figure 13 Activity diagram for scenario analysis

4.4.2. Scenario analysis

Three outsiders attack the facility using a large truck at night during operating hours. The target asset is located in the controlled room. The adversary tasks include the following:

- Crossing the perimeter
- Running to the roll-up door
- Penetrating through the roll-up door
- Running to the storage vault
- Stealing the asset
- Exiting to outside
- Crossing the perimeter
- Entering the second vehicle (Figure 7).

4.4.3. Estimate neutralization

Garcia provided information about how one can estimate the probability of neutralization [4]. In this example, we assume the neutralization probability for current response force is 0.9. This estimate will be used in calculating the overall PPS effectiveness (P_E).

4.4.4. System effectiveness

Table 2 shows an EASI model for the attack scenario. As indicated in the figure, the adversary requires 550 seconds to accomplish the attack after completing task 3. This time is less than the RFT (which is 600 seconds). Therefore, in this scenario, task 2 is the CDP, and the interruption probability equals 0.41. A SysML parametric diagram can be used to represent the necessary parameters and these relationships.

Table 2 EASI model for the example attack scenario

	A	B	C	D	E
1	Task No.	Adversary Task	Task Time (s)	Time Delay Remaining	PoD
2	Task 1	Cross Perimeter	30	712	0.4
3	Task 2	Run to Roll-Up Door	12	682	0.02
4	Task 3	Penetrate Roll-Up Door	120	670	0.5
5	Task 4	Run to Storage Vault	120	550	0.02
6	Task 5	Steal Asset	240	430	0.5
7	Task 6	Exit to Outside	120	190	0.02
8	Task 7	Cross Perimeter	60	70	0.4
9	Task 8	Enter Secon Vehicle	10	10	0
10					
11		Total Task Time	712		
12		RFT	600		
13		CDP	**Run to Roll-Up Door**		
14					
15					
16		**PoI**	**0.41**		
17		**PoN**	**0.90**		
18		**Effectiveness**	**0.37**		

A parametric diagram enables us to integrate the detection, delay, and response capabilities of the PPS into a set of equations. The parameters used in the equations link the PPS and the facility model. The parametric model shows which components in the model affect the equations that determine PPS performance. Figure 14 is the corresponding parametric model for the quantitative analysis. This model shows how elements of different models affect the system effectiveness. For example, it is indicated in the figure that the RFT, a parameter in the response force model, is an input to CDP calculation.

4.4.5. Upgrade analysis

At this phase one compares the PPS effectiveness estimate to the requirements. If the requirements are not met, an upgrade analysis is necessary. As discussed earlier, the required level of PPS effectiveness is 0.6; however, the estimated PPS effectiveness for the attack scenario is 0.37. Thus, the PPS shall be redesigned.

In this section, we perform sensitivity analysis for the example facility (shown in Figure 7) to better understand the effect of each parameter on the PPS effectiveness. PPS functional performance can be defined in areas of detection, delay, and response. The PPS detection function at each adversary task is indicated by probability of detection. Also, PPS delay can be associated with task time for each adversary task. Moreover, Response Force Time (RFT), and the Probability of Neutralization represent PPS Response function in the model.

The baseline case for the sensitivity analysis specified in the previous section is listed in Table 2. It is important to note that the PPS delay at each task is equivalent to the

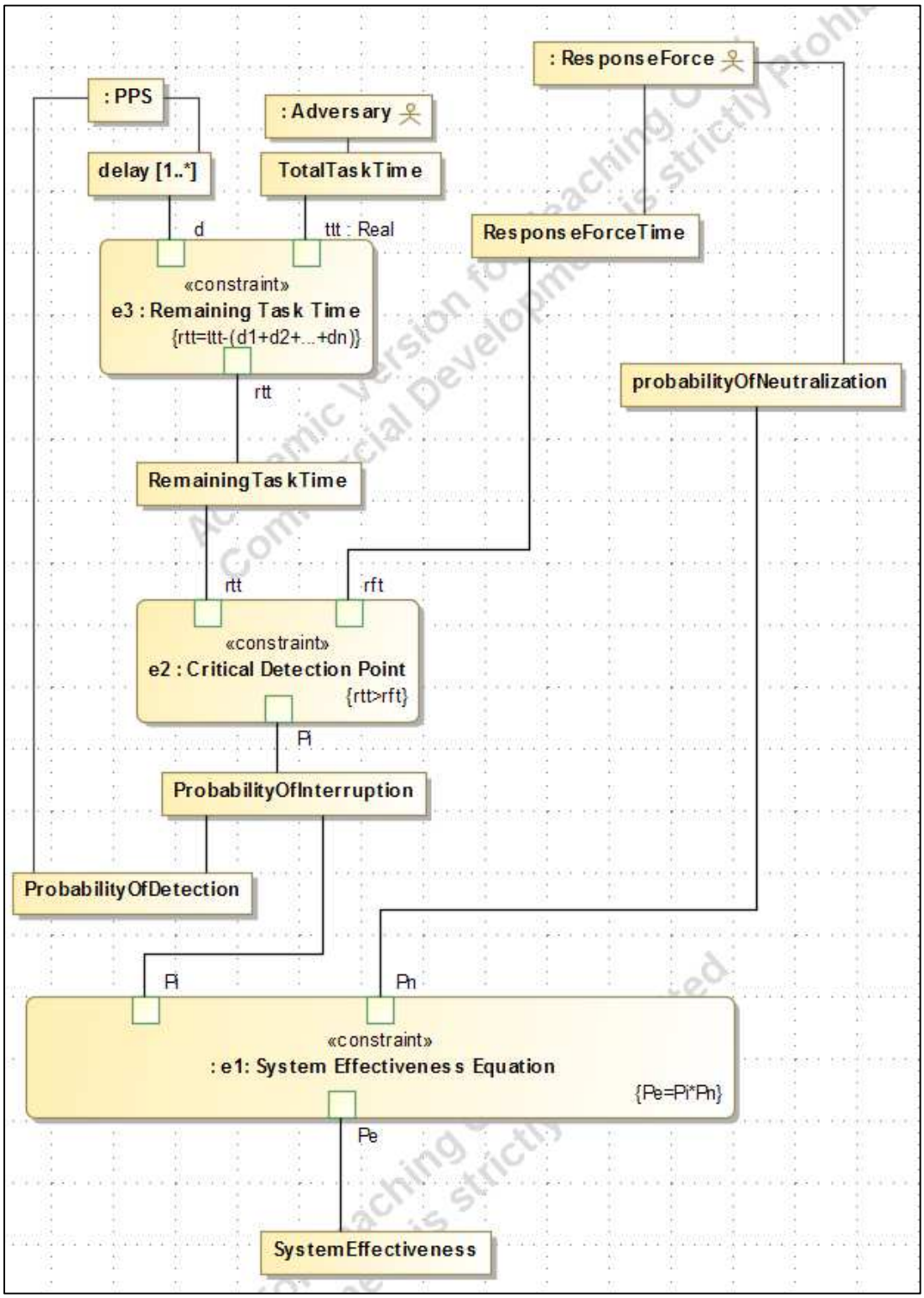

Figure 14 SysML parametric representation of EASI model

corresponding task time. The adversary tasks timeline shown in Figure 15, indicates that the RFT is greater than the sum of task time associated with task 4 through task 8. Therefore, the last point where a timely detection can happen is task number 2: Running to the roll-up door. It is important to note that detection during the task 3 is considered ineffective as it may happen after RFT (i.e. from 550 seconds to 600 seconds). Thus, assuming the probability of neutralization to be 0.9, we can calculate the PPS Effectiveness using equation 4:

$$P_E = P_I \cdot P_N = [1 - (1 - 0.4)(1 - 0.02)](0.9) = 0.37$$

Changes in PPS effectiveness with the probability of detection for each task is shown in Figure 16. One can observe that increasing the probability of detection only for task 1 and task 2 increases the PPS Effectiveness. This is consistent with the fact that a detection after CDP (in this case task 2) is ineffective. Also, since the line corresponding to task 1 has a greater slope, one can observe that changing P_D for task 1 increases the PPS effectiveness at a higher rate compared to task 2.

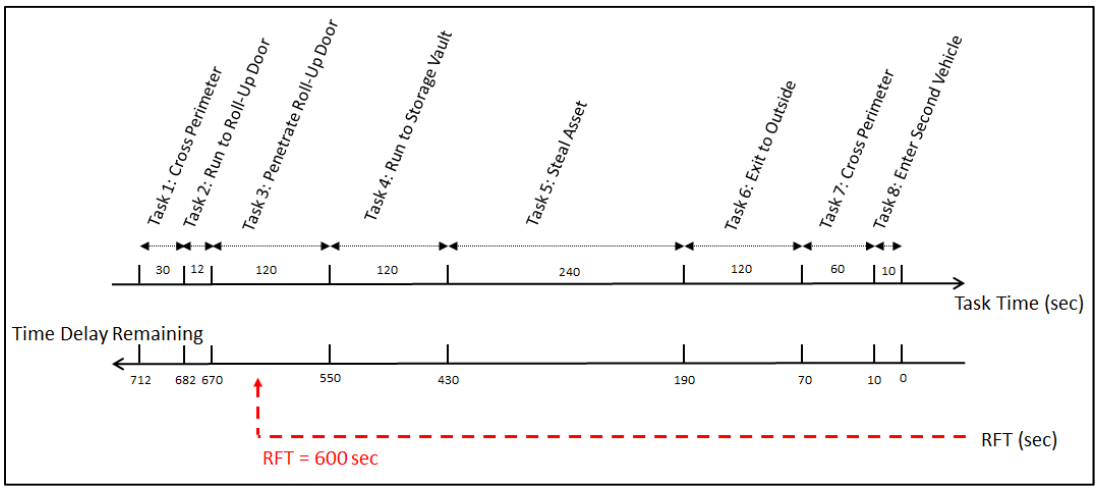

Figure 15 Adversary tasks timeline and the RFT for the baseline case

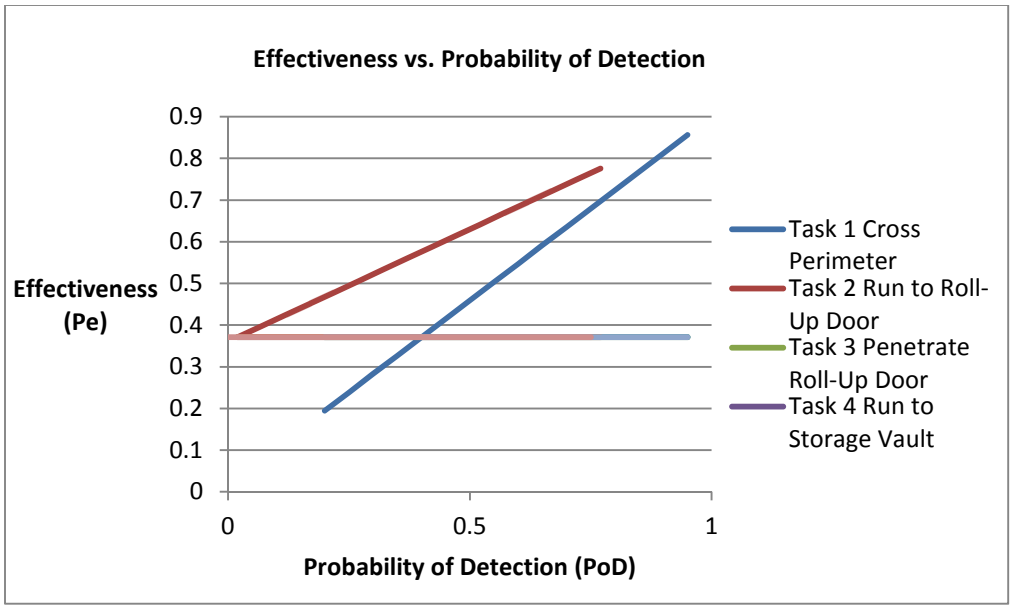

Figure 16 Sensitivity of the PPS effectiveness on the probability of detection for each task

Figure 17 shows the PPS effectiveness variation with increase in PPS delay (and thus, adversary task time). One can simply observe that increasing delay for tasks 4, 5, 6, 7, and 8 can effectively increase the PPS effectiveness. The reason is when determining the CDP, one compares the RFT to the time delay remaining (Column D in Table 2) which only includes delay times from the CDP to the last adversary task (In this case task 2 through task 8).

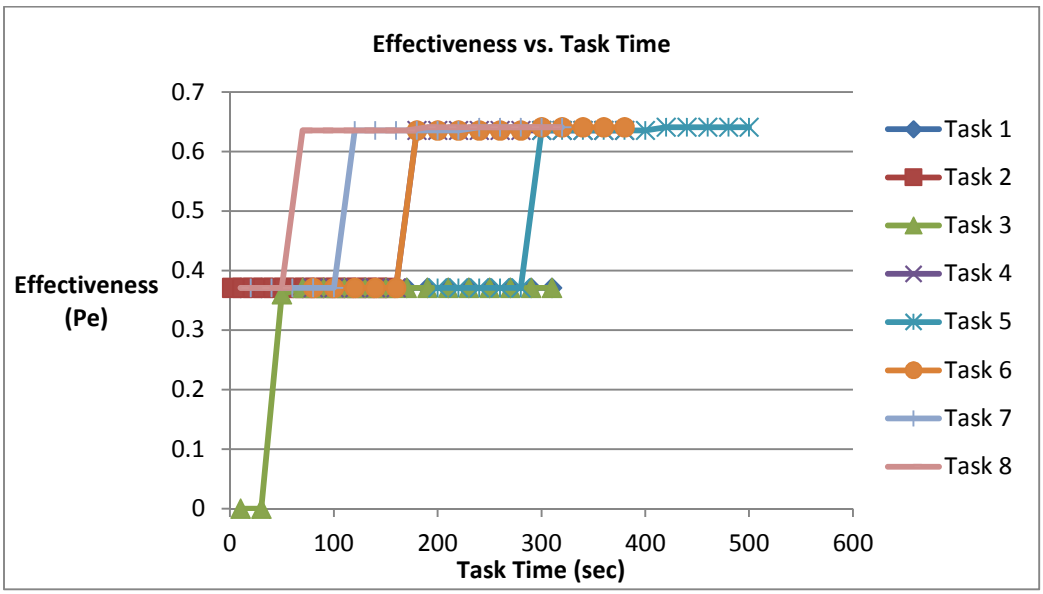

Figure 17 Sensitivity of the PPS effectiveness on the task time for each task

One can conclude from Figure 16 and Figure 17 that increasing probability of detection for tasks before the CDP is effective while increasing delay affects the PPS effectiveness only if applied after CDP.

Figure 18 illustrates changes in the CDP with the RFT. As we increase the RFT, CDP moves toward the beginning of the adversary sequence. As mentioned earlier, RFT is less than the time that an adversary requires to accomplish the attack. Therefore, as we increase RFT, CDP moves to the previous tasks where there is enough time for the response force to respond. For example, in the base line case, where the RFT is 600 seconds, as we increase the value to 670 seconds, task 2 is no longer the CDP. In this case, task 1 will be the CDP. Figure 19 illustrates the changes in PPS Effectiveness with RFT. In the baseline case, the value of RFT and PPS Effectiveness are, respectively, 600 seconds and 0.37. As we increase the RFT, PPS effectiveness first remains unchanged then at a certain RFT value it sharply decreases to 0. The reason for this behavior is that when RFT is increased to 682 seconds or more, there is no adversary task where a timely detection can happen. Also, as the RFT is decreased to a value between 429 and 550 seconds the PPS effectiveness increases to 0.71, because it moves the CDP farther from the first task along the adversary path; in other words there will be a higher chance to detect the adversary.

Finally, Figure 20 shows how PPS Effectiveness changes as we increase the Probability of Neutralization while we set other parameters constant. One can note that PPS Effectiveness increases linearly with the increase in the Probability of Neutralization.

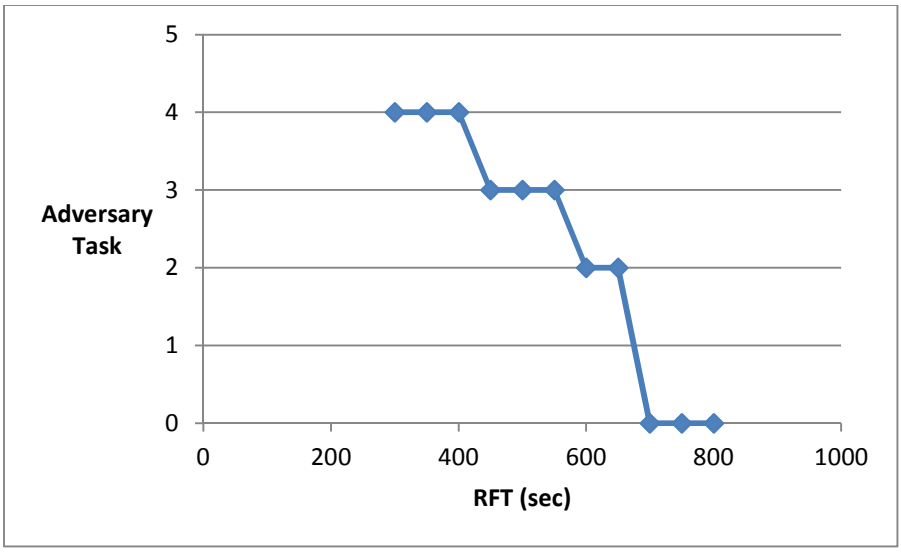

Figure 18 Sensitivity of the CDP on the RFT

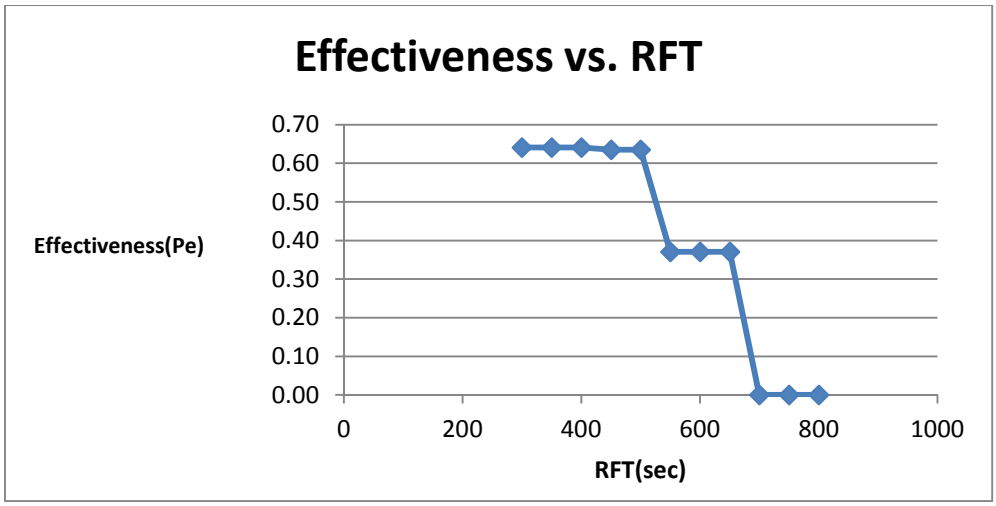

Figure 19 Sensitivity of the PPS effectiveness on the RFT

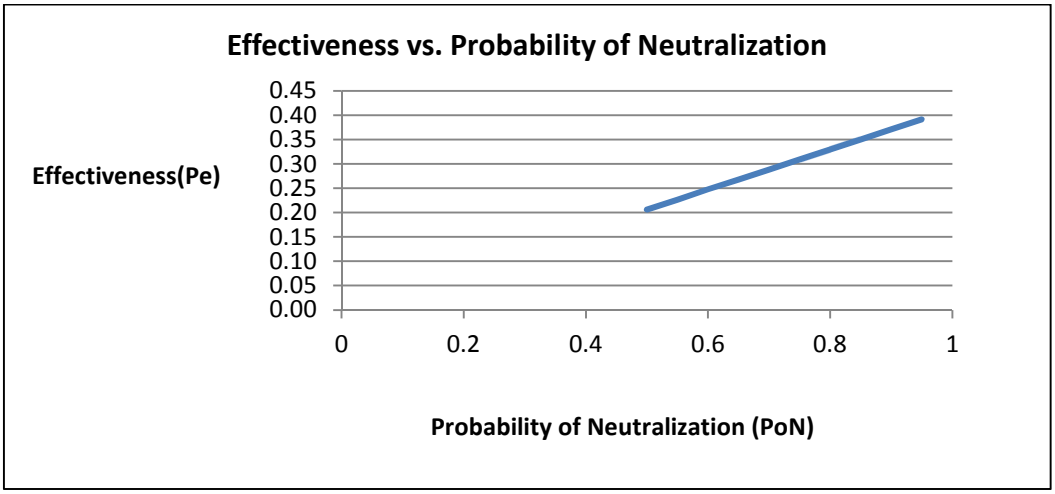

Figure 20 Sensitivity of the PPS effectiveness on the probability of neutralization

4.5. Notes on SysML integrated models

Figure 21 and Figure 22 illustrate the interconnectivity in a set of coherent SysML models that were developed for the SCA facility for a specific threat, asset, and scenario. As shown in the figures, the Activity Diagram that was developed for the scenario is linked to the Adversary BDD, Response Force BDD, and Facility BDD. Moreover, the parametric diagram that was generated for EASI model links the Response Force BDD, Adversary BDD, and PPS BDD to each other.

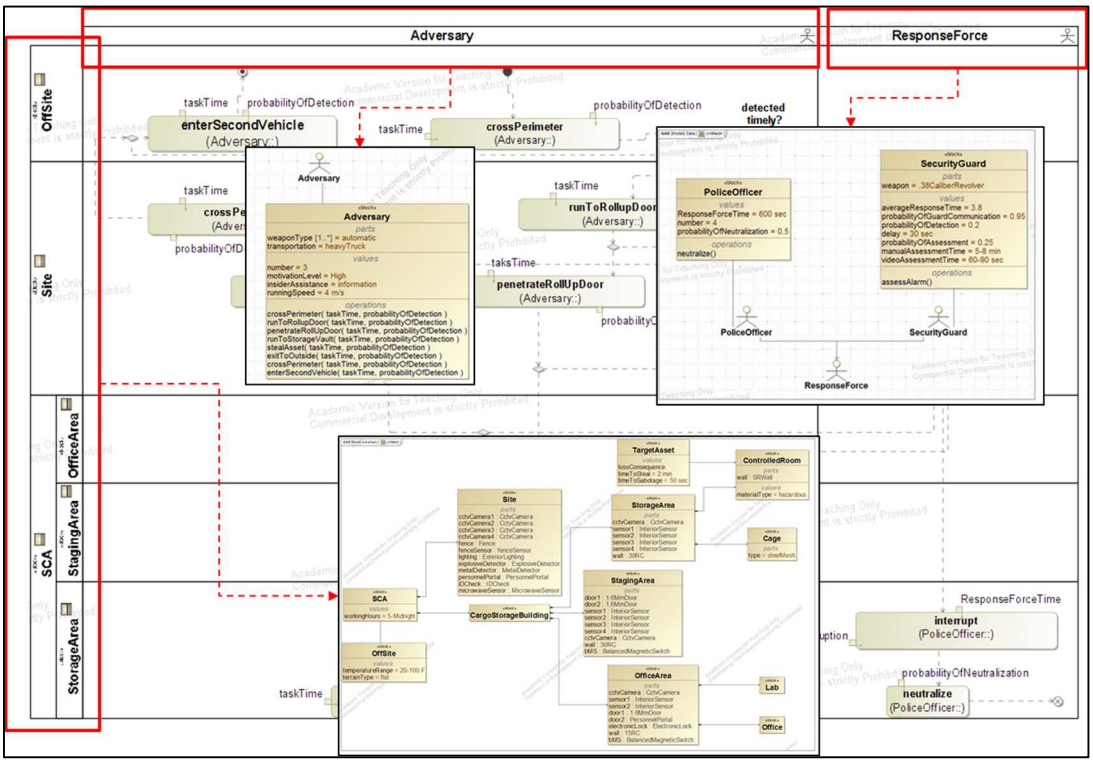

Figure 21 SysML models interconnectivity

Utilizing integrated SysML models is beneficial especially when a change occurs in the PPS because all the generated models are interconnected. Thus, when the value of a parameter in one model changes, the software automatically modifies other models with that element. For instance, if the value of the probability of detection on the fence increases as a result of adding more fence sensors, the MBSE software applies

adjustments to the other models that are involved (such as parametric models of different pathways that have the task “cross perimeter”).

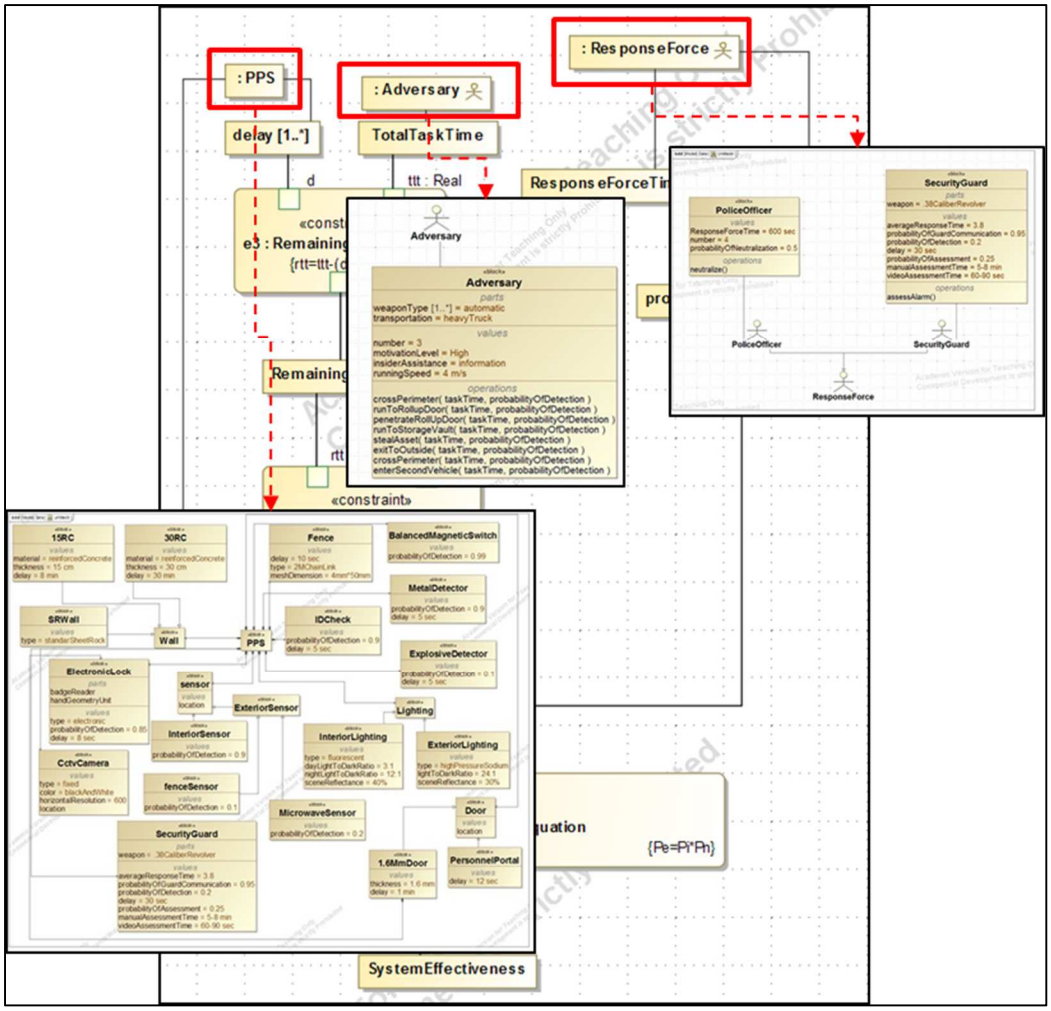

Figure 22 SysML models interconnectivity

In this research, we learned how we can use SysML models when evaluating a PPS using the performance-based VA approach. We first developed a requirements model for gathered functional, non-functional, and performance requirements. Then, we generated BDD models for the facility, threats, and assets to store the information that we gathered in the first step of VA, i.e., PPS objective determination. Next, we developed BDD models for the PPS in the functional areas of detection, delay, and response. We generated an activity diagram for a specific scenario that targets the

asset that we identified earlier. Finally, we constructed a parametric diagram for the third step in performance-based VA, PPS Analysis. In the diagram, we included the parameters that are involved in the EASI calculations. We showed how these parameters link other model elements such as the Adversary, the Facility, and the PPS BDDs.

Chapter 5: Conclusion and Future Work

In this study, we proposed a system modeling framework for evaluating a PPS. We first learned about PPS components including people, procedures, and elements. We studied the PPS elements that contribute to PPS main functionalities, i.e. detection, delay, and response. Then, we studied the evaluation processes that are being used to determine whether a PPS is working properly, i.e. it protects assets from the defined threats. Vulnerability Assessment (VA) evaluates a PPS based on either system compliance or performance. Compliance-based VA focuses on the presence of PPS components and is used when the asset is less critical. When dealing with critical assets, performance-based VA is used. A performance-based VA process includes PPS objective determination, PPPS design evaluation, and PPS analysis. For each task of this process we developed models. In the objective determination, we used SysML Block Definition Diagram to store information about threats, assets, and the facility. In the PPS design evaluation, we generated SysML Block Definition Diagrams to express PPS structure and capabilities in terms of detection, delay, and response. In the PPS analysis, we developed SysML activity diagram to show an attack scenario and different actors that are involved. Also, we generated a parametric diagram that indicates what performance parameters determine the overall PPS performance. We showed how these models are integrated. The modeling framework enables storing, and updating information in a consistent way and thus facilitates VA activities.

This research has shown how SysML models can support PPS vulnerability assessment (VA) and thus enable model-based systems engineering (MBSE) of a

PPS. The VA processes of specification, design, and analysis are essentially a system development process and thus are appropriate activities in which to use SysML models.

This thesis contributes to the development of VA by demonstrating modeling techniques that can enable the development and integration of other VA tools and reduce the time and cost of conducting VA, which will lead to safer facilities.

This thesis also contributes to the development of MBSE by demonstrating that its modeling approaches can be applied to other types of design and evaluation processes. The VA process is part of the larger life cycle of a facility. Although end-to-end, life-cycle use of MBSE is ideal, this thesis demonstrates that, when this is not feasible, the MBSE modeling approach can be applied to a portion of the system life cycle. The implementation of separate approaches could lead eventually to ever-larger integration of developments processes using the principles of MBSE.

This thesis applies MBSE principles to a particular example. We developed a series of models to facilitate the VA process. Future studies will be focused on defining a structured procedure for modeling independent of a particular case.

In the domain of VA, additional work is needed to implement robust specification, design, and analysis tools based on SysML models. The development of standards (similar to those used for building information models [18]) will further simplify VA tool development and use.

SysML enables extensions that support specialized domains [8]. Future studies will be focused on a customization of SysML for performance-based VA domain. A

model library will be generated to store reusable standard models. This will be a step toward establishing a standard security system evaluation framework.

Appendices

A. Evaluation of Intrusion Detection requirements against characteristics of a good requirement

Requirements				Requirements Attributes							
				Necessary	Implementation Independent	Clear and Concise	Complete	Consistent	Achievable	Traceable	Verifiable
1. new Building	1.1. All new research facilities will incorporate the following basic facility design features.	1.1.1. Segregate public access areas from research areas.	1.1.1.1. Locate general access areas (classrooms and conference rooms) on lower floors.	Yes	Yes	Yes	Yes	Yes	Partially	Yes	Yes
			1.1.1.2. Locate research laboratories on upper floors, except for laboratories that may use explosive materials.	Yes	Yes	Yes	Yes	Yes	Partially	Yes	Yes
		1.1.2. Perimeter security	1.1.2.1. Electric locks on all exterior	Partially	Partially	Yes	Yes	Yes	Yes	Yes	Yes

			doors.								
			1.1.2.2 Card readers on all exterior access doors.	Partially	Partially	Yes	Yes	Yes	Yes	Yes	Yes
			1.1.2.3. Security of ground level windows will be achieved by use of either Window grills, or Electronically protected glass in operable windows	Yes	Partially	No	Partially	Yes	Yes	Yes	Yes
			1.1.2.4. Exterior lighting to provide appropriate illuminatio n	Yes	Yes	Yes	No	Yes	Yes	Yes	No
			1.1.2.5. Alarms on roof maintenanc e doors: Automatica	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes

			lly activated at night, deactivated during daytime								
			1.1.2.6. Alarms on roof maintenance doors: Connected to University Police and audible at site	Yes	Yes	No	Yes	Yes	Yes	Yes	Partially
		1.1.3. Elevator/ stairwell security	1.1.3.1. Stairwell doors to public access areas on lower floors will not have locks	Yes	Partially	Partially	Yes	Yes	Yes	Yes	Yes
			1.1.3.2. Card readers and electric locks on stairwell doors to research areas. Under conditions specified by the State	Yes	Partially	Partially	Yes	Yes	Yes	Yes	Yes

			Fire Prevention Code , some stairwell doors must unlock and allow access from the stairwell to the floor when the fire alarm is activated								
			1.1.3.3. Card readers in elevators to research areas.	Partially	Partially	Yes	Yes	Yes	Yes	Yes	Yes
	1.2. All new high risk research facilities (i.e., research facilities that house animals, containment laboratories or greenhouses; store select agents or acute toxins; or involve the use of radiation	1.2.1. Incorporate the basic facility design features set forth in Part I. A.		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
		1.2.2. Incorporate additional security features, on a case-by-		Yes	Yes	Partially	Yes	Yes	Yes	Yes	No

	hazards will [incorporate the following].	case basis, that are identified during planning meetings as necessary by the users, AEC, Building Security Systems, and DES									
2. Existing Buildings	2.1. In conjunction with scheduled renovation, all existing research facilities will be upgraded to incorporate the basic facility design features set forth in Part I.A.			Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	2.2. Prior to renovation users, AEC, Building Security Systems, and DES			Yes	Yes	Partially	Yes	Yes	Yes	Yes	No

	will meet to determine, based on the projected use of the building, whether additional security features are needed.										
	2.3. It is recommended that there be an automatic safety review of renovation plans by appropriate departments, including DES and Building Security System			Yes	Yes	No	Yes	Yes	Yes	Yes	No

Bibliography

[1] M. L. Garcia, The design and evaluation of physical protection systems. 2nd ed., Amsterdam: Elsevier Butterworth-Heinemann, 2008.

[2] P. R. Baker and D. J. Benny, The complete guide to physical security, Boca Raton: CRC Press, 2013.

[3] "Integrated Rapid Visual Screening of Buildings. Building and Infrastructure Series," Department of Homeland Security, 2011. [Online]. Available: http://www.wbdg.org/ccb/DHS/bips_04.pdf. [Accessed 27 4 2015].

[4] M. L. Garcia, Vulnerability Assessment of Physical Protection Systems, Amsterdam: Elsevier Butterworth-Heinemann, 2006.

[5] Systems Engineering Handbook, San Diego, CA: International Council on Systems Engineering (INCOSE), 2010.

[6] J. A. Estefan, "Survey of Model-Based Systems Engineering (MBSE) Methodologies," International Council on Systems Engineering (INCOSE). INCOSE-TD-2007-003-02., Seattle, WA, USA, 2008.

[7] "Systems Engineering Vision 2020," International Council on Systems Engineering (INCOSE): TP-2004-004-02: 2.03, 2007.

[8] S. Friedenthal, A. Moore and R. Steiner, A practical guide to SysML the systems modeling language. 2nd ed, Amsterdam: Elsevier, 2012.

[9] "ARES Security Corporation," 2012. [Online]. Available: http://www.aressecuritycorp.com/learn-more/collateral/. [Accessed 29 4 2015].

[10] "Physical Protection Systems. Nuclear Safeguards Education Portal," [Online]. Available: http://nsspi.tamu.edu/nsep/courses/physical-protection-systems.

[11] G. Booch, J. Rumbaugh and I. Jacobson, The unified modeling language user guide, Reading: Addison-Wesley, 1999.

[12] D. W. Hybertson, Model-oriented systems engineering science: a unifying framework for traditional and complex systems, Boca Raton: CRC Press, 2009.

[13] J. Holt, UML for Systems Engineering: watching the wheels, London: The Institution of Electrical Engineers, 2001.

[14] M. Björkander, "UML and SysML Software Modeling and Requirements Management," 2007. [Online]. Available: http://www.modprod.liu.se/workshop_2007/1.46538/talk8-bjorkander.pdf. [Accessed 27 4 2015].

[15] "MagicDraw," No Magic, Inc., [Online]. Available: http://www.nomagic.com/products/magicdraw.html. [Accessed 29 4 2015].

[16] M. Mannion and B. Keepence, "SMART requirements," *SIGSOFT Softw. Eng. Notes,* vol. 20, pp. 42-47, 1995.

[17] "The 2012 design criteria/facility standards manual," Office of Facilities Management. University of Maryland, 2012.

[18] C. Eastman , P. Teicholz, R. Sacks and K. Liston, BIM handbook: A guide to building information modeling for owners, managers, designers, engineers, and contractors, Hoboken: Wiley, 2008.