2019-12

LOCK IT DOWN: IMPROVING FEDERAL SPECIFICATIONS FOR PHYSICAL SECURITY WITH A SYSTEMS ENGINEERING APPROACH

Finklea, Darren

Monterey, CA; Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

LOCK IT DOWN: IMPROVING FEDERAL SPECIFICATIONS FOR PHYSICAL SECURITY WITH A SYSTEMS ENGINEERING APPROACH

by

Darren Finklea

December 2019

Thesis Advisor: Robert Semmens
Second Reader: Walter E. Owen

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2019	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE LOCK IT DOWN: IMPROVING FEDERAL SPECIFICATIONS FOR PHYSICAL SECURITY WITH A SYSTEMS ENGINEERING APPROACH	**5. FUNDING NUMBERS**
6. AUTHOR(S) Darren Finklea	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

Implementation of systems engineering processes to improve design and performance requirements in physical security equipment federal specifications is a concept worth investigating. The Department of Defense composes federal specifications to supply the warfighter with approved products that are essential for the protection of classified information. In the past, it was common for physical security equipment specifications to require multiple amendments due to insufficient requirements or a lack of complete knowledge in end user needs. The thesis examines four physical security equipment specifications and develops an approach based on systems engineering methodologies to reduce the occurrence of amendments and deliver products that fully satisfy end user needs. The identification of problem statements and operational requirements, along with the execution of a stakeholder analysis, functional analysis, and subject matter expert interviews, found that a systems engineering approach can establish a more complete and standardized process to formulate equipment requirements. The General Services Administration will review the findings for possible implementation for future physical security equipment specifications.

14. SUBJECT TERMS physical security, performance requirement	**15. NUMBER OF PAGES** 103
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89) Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

LOCK IT DOWN: IMPROVING FEDERAL SPECIFICATIONS FOR PHYSICAL SECURITY WITH A SYSTEMS ENGINEERING APPROACH

Darren Finklea
Civilian, Department of the Navy
BS, University of California - Irvine, 2009

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS ENGINEERING MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
December 2019

Approved by: Robert Semmens
Advisor

Walter E. Owen
Second Reader

Ronald E. Giachetti
Chair, Department of Systems Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Implementation of systems engineering processes to improve design and performance requirements in physical security equipment federal specifications is a concept worth investigating. The Department of Defense composes federal specifications to supply the warfighter with approved products that are essential for the protection of classified information. In the past, it was common for physical security equipment specifications to require multiple amendments due to insufficient requirements or a lack of complete knowledge in end user needs. The thesis examines four physical security equipment specifications and develops an approach based on systems engineering methodologies to reduce the occurrence of amendments and deliver products that fully satisfy end user needs. The identification of problem statements and operational requirements, along with the execution of a stakeholder analysis, functional analysis, and subject matter expert interviews, found that a systems engineering approach can establish a more complete and standardized process to formulate equipment requirements. The General Services Administration will review the findings for possible implementation for future physical security equipment specifications.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

DoD	Department of Defense
GSA	General Services Administration
IACSE	Interagency Committee on Security Equipment
QPL	qualified products list
SME	subject matter expert
TPM	technical performance measurement

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

The Department of Defense composes federal specifications to supply the warfighter with approved products essential for the protection of classified information. Currently, the Interagency Committee on Security Equipment (IACSE) examines the government needs, formulates a viable solution, documents the requirements in a completely new specification or an amendment to an existing specification, and submits for General Service Administration (GSA) approval. The process has resulted in viable products implemented in the field for decades, but GSA distributed several amendments and new federal specifications during that period to satisfy end user needs. Also, future technological advancements present the possible need for physical security equipment that has yet to be manufactured or even designed. Thus, the thesis examined the implementation of a systems engineering approach to standardize and document the federal specification requirements development process.

This research analyzed four current specifications: FF-L-2740 *Locks, Combination, Electromechanical*, FF-L-2890 *Lock Extensions (Pedestrian Door Lock Assembly Preassembled, Panic and Auxiliary Deadbolt)*, FF-P-110 *Padlock Changeable Combination (Resistant to Opening by Manipulation and Surreptitious Attack)* and AA-F-358 *Filing Cabinet, Legal and Letter Size, Uninsulated, Security*. The appropriate systems engineering methods were determined to be problem statement identification, stakeholder and needs analysis, subject matter expert interviews, operational requirements analysis, and functional analysis. The methods represent a detailed step-by-step decomposition of end user needs into the required functions of the locking systems that provide a complete framework for all design and performance specification requirements. The functional analysis was the final step in the approach because either established policy or the discretion of GSA dictates quantitative values for specifications. However, the functions are critical to providing the incorporation of all necessary elements in the requirements.

The research initially thought to improve the requirements development process by identifying missing functions that GSA could further examine. Unfortunately, without complete access to end users for observation and interviews with all stakeholders, absolute

detailed needs were unable to be gathered so all functions could not be confirmed. However, the unexpected value of the systems engineering approach was the recognition of additional tools that IACSE could incorporate in future requirements development. The inclusion of a needs analysis, testing documentation, and classified supplemental testing requirements along with the utilization of the analyses detailed in the research offer GSA an avenue to fully decompose and document specification requirements.

The systems engineering approach added value to the requirements development by offering a structured framework from identifying and subsequently decomposing end user needs into functions that correlate into design and performance requirements manufacturers can design to. The intended improvements will decrease the amount of requirements required alterations and produce locking systems that fully meet end user needs. The results and recommendations will be presented to GSA for possible formal implementation.

ACKNOWLEDGMENTS

The publication of this thesis would not have been possible without the much-appreciated efforts of my thesis advisor, Professor Robert Semmens, and the subject matter experts consulted in the physical security equipment field. The information, guidance, and support provided throughout the process were invaluable. Also, a resounding thank you is in order for my wife, June Finklea, who showered me with support, assisted whenever available, and picked up my slack during the months of dedicated writing.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Product design can begin with fantastical ideas that creatively solve a problem or meet an existing need, such as the invention of a retina-scanning lock to secure all doors protecting classified information. However, before any design, much thought and analysis must be considered during the conceptual phase to ensure all functions are satisfied, proper design or performance requirements are established, all stakeholder needs are examined, and the design is feasible, along with other essential components. Experience has demonstrated that applying substantial effort in developing requirements based on end user needs and feasibility results in a higher quality product. Systems engineering approaches provide a project engineer with a standardized process and set of tools for effective requirements development for complex systems such as assault aircraft, amphibious vehicles, naval ships, and drones. However, this research examined the possible utilization of such an approach in other fields that produce essential equipment for the government.

A. BACKGROUND

In the 1950s, the government identified the need to store classified material but faced an obvious dilemma: how to qualify physical security equipment for use. Two options were the government manufacturing its product to meet all safeguarding requirements or industry producing equipment with government oversight. The solution was determined to be federal specifications, under the control of the General Services Administration (GSA), which documented all requirements for physical security equipment storing classified information. The first federal specification introduced for this purpose was AA-F-357, *Filing Cabinet, Steel, Legal and Letter Size Insulated, Security*, which addressed Executive Order 10501 requirements for storing "official" information. The specification detailed protection requirements such as 30 person-minutes against surreptitious entry, ten person-minutes against forced entry, 20 person-hours against radiological techniques, 1-hour against fire damage to contents, along with other material, testing, configuration and usability requirements (General Services Administration 1954). Since, GSA has published federal specifications for vault doors, vault systems, information

processing system storage, weapons storage, mechanical and electromechanical combination locks, pedestrian door lock extensions, and changeable combination padlocks, all for securing sensitive national information.

Product manufacturing process is as follows: manufacturers submit the product to meet all requirements listed in the specification for testing, the designated GSA testing facility determines whether the product passes or fails based on the specification, and the product is included on the qualified products list (QPL) upon passing testing. The government can then procure the qualified product from GSA or the Defense Logistics Agency (DLA), which establishes contracts with the manufacturers on the QPL. Another key factor in the procurement of physical security equipment is policy and, for this research, the Department of Defense (DoD) policy. A policy like DoD Manual 5200.01 Volume 3, "DoD Information Security Program: Protection of Classified Information," mandates the use of storage and locking systems meeting the GSA federal specifications. For example, "except as provided elsewhere in this Volume, combination locks on vault doors, secure rooms, and security containers protecting classified information shall conform to Federal Specification FF-L-2740" (Under Secretary of Defense (Intelligence) 2013, 35). Thus, policy requirements may dictate end user (military, government civilians, and contractors) needs.

GSA relies on the Interagency Committee on Security Equipment (IACSE) to create, review, update, and provide recommendations on enforcement of all physical security equipment federal specifications. This research paper examines the formal process for the reviews, tools utilized to document the actions through subject matter expert interviews, and how systems engineering can play a role in physical security equipment federal specification development.

B. PROBLEM

Researchers have defined systems engineering in various ways, but one common thread is systems engineering offers "a better and more complete effort regarding the initial definition of system requirements, relating these requirements to specific design criteria and the follow-on analysis effort to ensure the effectiveness of early decision making in

the design process" (Blanchard and Fabrycky 2011, 18). The systems engineering approach, which has advanced over the decades, can pay major dividends in the creation of product requirements that encompass a specification. The approach emphasizes the detailed analysis of all elements incorporated in requirement development to ensure complete coverage of all stakeholder needs and technical feasibility. From that perspective, physical security equipment federal specifications seem like an appropriate platform to implement systems engineering processes. Federal specifications must incorporate end user, policymaker, manufacturer and testing facility needs, while not limiting design but also ensuring enough clarity is present to produce a viable security system. Thus, it is common for a specification to undergo many amendments and edition changes. The challenge is apparent: how much detail should the government include in the specifications, what stakeholders should be involved or considered during development, how are the evolving needs of the government accounted for, and what constitutes an effective specification?

C. SCOPE

The research paper examines four federal specifications recommended by GSA: FF-L-2740 "Locks, Combination, Electromechanical," FF-L-2890 "Lock Extensions (Pedestrian Door Lock Assembly Preassembled, Panic and Auxiliary Deadbolt)," FF-P-110 "Padlock Changeable Combination (Resistant to Opening by Manipulation and Surreptitious Attack)" and AA-F-358 "Filing Cabinet, Legal and Letter Size, Uninsulated, Security." After review of available systems engineering methods and tools, the following were determined to be optimal for implementation: problem statement identification, stakeholder and needs analysis, subject matter expert interviews, operational requirements analysis, and functional analysis. This process of analysis is commonly utilized when developing requirements for complex systems and applies to equipment development as well, especially equipment with the important objective of protecting classified information. The designs and functions of specific products on the specification QPLs will not be examined in this research, just the expert opinion on the current product available. The research will strive to answer the question: Can implementation of systems

engineering processes improve current design and performance requirements in physical security equipment federal specifications?

D. RESEARCH DESIGN

The first step of the process was the identification of the problem statements for each specification. The task seems simple, but it is vital to properly identify the appropriate problem to ensure the solution meets the true need. A misconstrued problem can lead to a product that does not satisfy the government's needs. Then a stakeholder analysis identified all interested and affected parties involved with the specification and the needs associated with each. Throughout the initial phases of the research, subject matter expert interviews provided valuable knowledge on the requirements development process and any current issues with the four federal specifications. From there, the completed formulation of operational requirements specified the mission definition, performance and physical parameters, operational distribution, operational life cycle, utilization requirements, and environmental factors (Blanchard and Fabrycky 2011). The functional analysis completed the process detailing exactly what sub-functions should be included in each specification. With the data generated, recommendations on possible tools and approaches for future specification fabrication were supplied to GSA.

II. METHODS

A. RESEARCH DESIGN

The research conducted for this thesis is unique in the sense that it applies a new approach to an established field. The U.S. government has produced physical security equipment protecting classified information since 1954 with oversight from GSA. However, physical security equipment federal specifications have yet to implement a systems engineering approach to develop design and performance requirements. Thus, considerable brainstorming and planning were involved in determining the course of completion that would yield the most beneficial findings. The execution of the research validates if a systems engineering approach applies to physical security equipment requirements development, what systems engineering processes best fit such development, and if fabrication of standardized tools for future specifications is possible.

Physical security equipment federal specifications are a hybrid of performance and design requirements. The documents detail the physical features, testing, performance, and design requirements to obtain GSA approval and are placed on a QPL for procurement eligibility by government agencies. As it turns out, requirements development is an essential aspect of a systems engineering approach. Throughout the evolution of systems engineering, a few varying definitions of the approach have been offered for product development—as described by Blanchard and Fabrycky (2011)—which list requirement definition as the first action. For example, three of the more iconic models are the Winston Royce waterfall model (Figure 1) applied to software systems, Barry Boehm's risk-driven software development spiral model, and the Kevin Forsberg and Harold Mooz "Vee" model that links system development with verification. All three models begin with either requirements analysis, systems requirements determination, or definition of system requirements. The models point to the fact that the definition of needs at the system conception level is the commencement for determining end user requirements and constructing design criteria (Blanchard and Fabrycky 2011, 38). The requirements for physical security equipment delineate the functions that formulate a unified design goal and the true problem that is to be resolved by the product. Ensuring that the problem

definition reflects the true customer requirements is essential. Optimal requirement formulation is an extensive process that implements in-depth analyses that incorporates input from all product stakeholders.

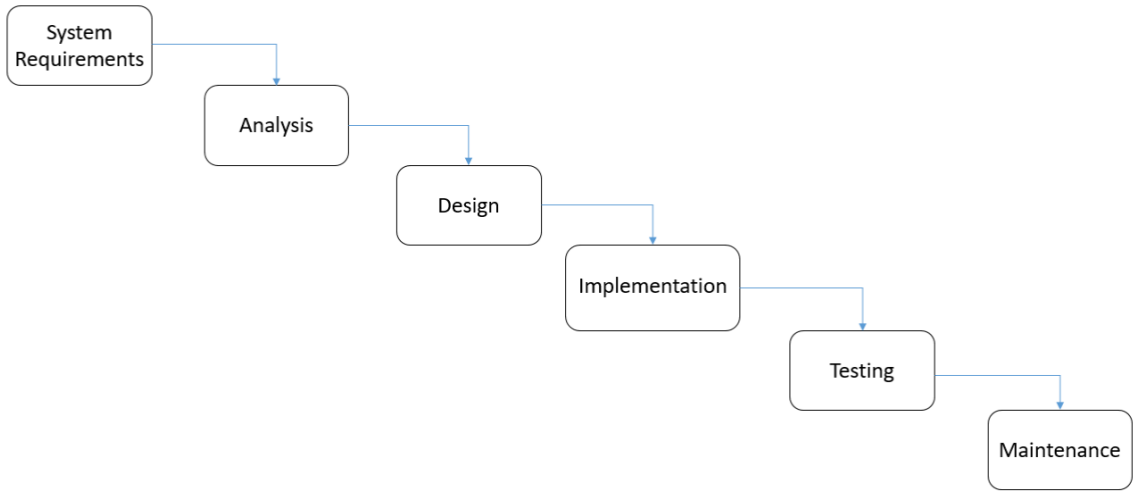

Figure 1. Winston Royce Waterfall Model Illustration

B. PROCEDURE

The initial action of the research project was to define the intended problem each specification addresses. Generating the problem reduces the probability of developing a product to a perceived need rather than the actual operational need. From there, a stakeholder analysis ensured all parties with interest in the products are considered throughout the specification composition. Stakeholder analysis is a process or action research methodology used to explore the opinions different stakeholders may have on potential outcomes and their influence (Flicker 2014, 713). Physical security equipment affects the end users who store the classified material, policymakers concerned with effectiveness and feasibility, manufacturers of the product, and the approving agency, to name a few. All of these entities examine the federal specifications for different purposes. Effective requirements examine all perspectives to avoid missing critical design elements. The analysis consists of identifying all stakeholders associated with each specification,

ranking the influence and impact on each, and determining the specific need of each. The analysis will supply all essential needs the requirements must satisfy.

The defined needs were then translated into a set of operational requirements. The systems engineering and analysis approach formulated the system's operational requirements that should be identified early, carefully, and as completely as possible (Blanchard and Fabrycky 2011, 61). For each specification, the following seven factors were identified and documented: mission definition, physical and performance parameters, operational deployment or distribution, operational life cycle, utilization requirements, effectiveness factors, and environmental factors (Blanchard and Fabrycky 2011). The operational requirements act as a guideline for the development of technical performance measurements (TPM), the quantitative values that describe system performance. For this research project, the TPMs consist of estimated, predicted, and measured quantitative values assigned to the operational requirements. As stated in *Systems Engineering and Analysis*, "the objective is to influence the system design process to incorporate the right attributes/characteristics to produce a system that will ultimately meet customer requirements effectively and efficiently" (Blanchard and Fabrycky 2011, 82).

A critical element throughout the thesis project was the review by subject matter experts (SMEs) in the physical security field. The cooperative SMEs were involved with the development, reinforcement, testing, or review of all the specifications covered in the project in some capacity. Furthermore, the SMEs participated in preliminary interviews that established their evaluation of the effectiveness of the specifications, whether the current products meeting the specifications were adequate, and any recommended specification improvements. The interviews were vital in steering the project in an appropriate direction by supplying valuable knowledge of the current specification effectiveness and evaluating the validity of the project since the experts have a vast knowledge of the specifications.

The next step in the approach was the functional analysis that translated system requirements into detailed design criteria. "The purpose of 'functional analysis' is to present an overall integrated description of the system's functional architecture, and to

provide a foundation from which all physical resource requirements are identified" (Sadraey 2013, 27). Furthermore, functional analysis ensures all necessary components are documented and that no unnecessary components are included in the specifications. The analysis broke down all functions related to the specific product from a top-level function into sub-level functions. The decomposition of levels depicted by a functional flow block diagram continued until it was determined the adequate sub-level was reached, as seen in Figure 2. The sub-level functions rendered the attributes each product must have to meet the federal specifications. Thus, requirements can be developed and documented based on the functions identified in the analysis.

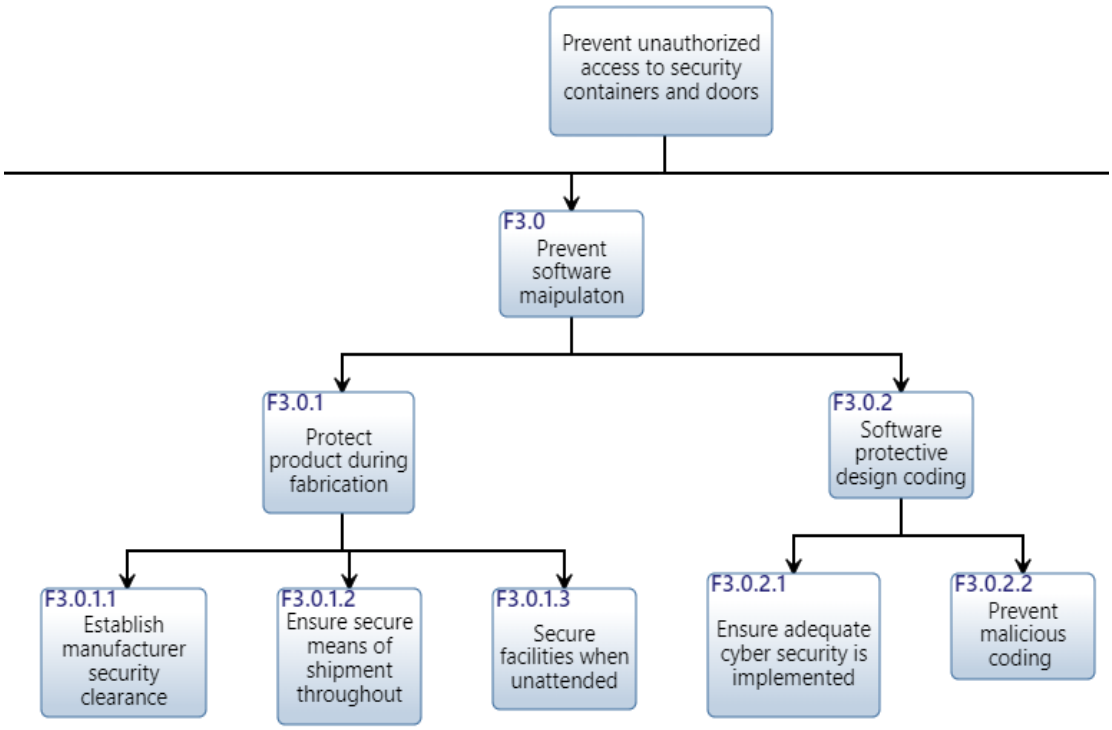

Figure 2. FF-L-2740 Functional Analysis Example

The research provides lessons learned for implementing future requirement developmental procedures for other federal specifications. As stated previously, requirements development for specifications based on committee decisions has been quite effective. However, a more standardized and thorough approach may lead to time saved,

reduction in amendments due to more comprehensive initial requirements, and higher quality products that completely satisfy the needs of all stakeholders. Supplying the government with a comprehensive standardized approach to establishing requirements for equipment used to store national classified information was the goal and driving force behind this research.

THIS PAGE INTENTIONALLY LEFT BLANK

III. RESULTS

A systems engineering approach to constructing physical security equipment federal specifications has never been executed in the past, which lends no reference to the best practice of completion. However, as discussed in the Methods section, the following analysis tools were determined to be the most useful for this case: subject matter expert interviews, problem statement development, stakeholder/needs analysis, operational requirements analysis, and functional analysis of each specification. The analyses are typically utilized in the beginning phases of complex systems to fully and accurately define the requirements. The results of each analysis provided insight into the need and effectiveness of the federal specifications.

A. PROBLEM STATEMENT IDENTIFICATION

A problem statement describes the system capability need in enough qualitative and quantitative terms to justifying progressing to the next step (Blanchard and Fabrycky 2011). For physical security equipment, in particular, the statement must include the protection function of the product and what the product is to protect. The problem statement must be accurate because it acts as the foundation of the need for product fabrication. Thus, if the statement is inaccurate, the product will not satisfy the true need from the field.

A few components were utilized to piece together the problem statements for each specification. First, as the DoD Lock Program subject matter expert, the extensive experience on the use of the products through fieldwork over the years has provided much insight as to how the current products are utilized and the needs of the end users through dialog and observation. Furthermore, review and evaluation of the current specifications supplied perspective on the intent of the government regarding the final product desired. Lastly, a physical security equipment subject matter expert was consulted for a review of the drafted statements. The comments supplied added key elements to each statement. The statement must be detailed enough to relay the foundational need without supplying too much detail to restrict possible solutions (Blanchard and Fabrycky 2011).

1. Electromechanical Combination Lock

The first specification examined was the FF-L-2740 *Locks, Combination, Electromechanical* (General Services Administration 2011). An initial view of the need for the product can be obtained from the currently implemented government policy. DoD policy, in particular, DoD Manual 5200.01, Volume 3 (Undersecretary of Defense (Intelligence) 2013), mandates that all hard copy classified information be stored securely using locks meeting FF-L-2740. One can identify that the government requires a deadbolt mechanism to store classified information. Remember, the problem statement should not contain any detailed performance or design requirements. Therefore, the problem statement reads as follows:

The U.S. government requires a deadbolt mechanism to secure the storage component of classified information while unattended.

Statement elements:

- The product is to be used by all agencies of the U.S. government and no foreign government.
- The "storage component" is purposefully vague. The secured component should not be limited to safes, containers, or any other specific equipment.
- Specifying a deadbolt is required because no other mechanism shall be used to secure the storage component.
- The material under protection is classified information.
- The deadbolt is to provide protection when the storage element is unattended, meaning it must be capable of being locked and opened only by the appropriate personnel.

2. Pedestrian Door Assembly

FF-L-2890 *Lock Extensions (Pedestrian Door Lock Assembly Preassembled, Panic, and Auxiliary Deadbolt)* (General Services Administration 2019) is unique in that

one event initiated the creation of the specification by identifying new priorities in security. The physical security world through the 1990s focused on the integrity of the locking systems and the ability to protect an area that may house classified information and arms, ammunition, and explosives. However, the tragic occurrence of hijacked airplanes crashing into the Twin Towers in 2001 emphasized the need for life safety components in all facilities, even those storing classified information. If a physical security product did not provide ease of exiting a facility, lives might be lost in an emergency. The government supplied guidance that life safety is a priority in all designs. The pedestrian door assemblies must secure areas while offering ease of egress. The problem statement for the specification is as follows:

The U.S. government requires a pedestrian door assembly to secure a restricted area and incorporate life safety and accessibility components.

Statement elements:

- The product is to be used by all agencies of the U.S. government and no foreign government.
- Pedestrian door assemblies characterize the need for locking systems on doors in high traffic areas.
- The door assembly must still only allow access to those granted access, which is encompassed by “secure.”
- “Restricted areas” refer to any areas that restrict access (e.g., Sensitive Compartmented Information Facility [SCIF], Special Access Program [SAP])
- “Life safety” refers to the ease of exit from the facility, egress, which will be defined later.
- Accessibility refers to the ease of entrance by those physically handicapped.

3. Combination Padlock

FF-P-110 *Padlock, Changeable Combination (Resistant to Opening by Manipulation and Surreptitious Attack)* (General Services Administration 1997) is one of the oldest specifications that has undergone the least amount of major changes. The need derived from the use of classified equipment classified due to the ability of threats to access the equipment and gain classified information such as protective distribution systems (PDS) boxes that contain wireline and fiber-optics telecommunication systems for classified networks. The government determined to ensure forced entry resistance into such equipment is not required, as they accept the risk, but the occurrence of a breach into the equipment must be evident, entailing manipulation resistance. The problem statement is as follows:

The U.S. government requires a manipulation resistant locking system to secure classified equipment in controlled facilities.

Statement elements:

- Manipulation resistance protects against undetectable entrance into the equipment. Manipulation proof would be infeasible or very costly to design.
- The original statement contained “padlock,” but after review, it was determined that the need does not restrict the use of any other locking system. Therefore, a locking system is utilized.
- The equipment will always be located in controlled facilities with layers of security surrounding the equipment.

4. Security Cabinet

AA-F-358 *Filing Cabinet, Legal and Letter Size, Uninsulated, Security* (General Services Administration 2010) is also an older specification. However, unlike FF-P-110, it has undergone significant changes over the years. The need for the product derived from Executive Order 10501 by President Eisenhower stating the requirements for safeguarding

"official" information (The White House 1953). The government produces an extreme number of classified documents through the vast amount of sensitive projects that require protection when unattended. It is important to note that within any facility accredited to execute classified projects, many different projects can be ongoing in one area, but not all personnel may have a need-to-know for all projects. Therefore, securing documents within the facility is required instead of the alternative, open storage. With that in mind, the problem statement is as follows:

The U.S. government requires a six-sided container system capable of accepting a deadbolt lock to store hard copies of classified information while unattended securely.

Statement elements:

- The system must be able to protect from the entrance at every angle that is encompassed by a "six-sided container system."
- The system must be capable of utilizing a deadbolt to provide access to the documents.
- The system must still only allow access to those granted access, which is encompassed by "securely store."
- The container is to provide protection when unattended, meaning it must be capable of being locked and opened only by authorized personnel.

5. Summary

The balance of creating problem statements containing enough information to ensure all vital elements of the product were addressed through design without too much detail to restrict design was accomplished through multiple iterations and coordination with subject matter experts. Through the process, a few lessons learned were gained. For example, do not identify a specific locking system into the statement (such as a padlock), address all relevant needs with stakeholders, consider feasibility (i.e., manipulation resistant vs. manipulation proof) and do not solely rely on products or requirements that

already exist because current requirements may not meet the particular need. Table 1 shows the finalized problem statements.

Table 1. Finalized Problem Statements

Federal Specification	Problem Statement
FF-L-2740	The U.S. Government requires a deadbolt mechanism to secure the storage component of hard copy classified information while unattended.
FF-L-2890	The U.S. Government requires a pedestrian door assembly to secure a restricted area and incorporate life safety and accessibility components.
FF-P-110	The U.S. Government requires a manipulation resistant locking system to secure classified equipment in controlled facilities.
AA-F-358	The U.S. Government requires a six-sided container system capable of accepting a deadbolt lock to store hard copies of classified information while unattended securely.

B. STAKEHOLDER AND NEEDS ANALYSIS

Physical security equipment federal specifications affect many organizations and individuals to varying degrees ranging from the DoD policy authorities to manufacturers, and government end users to commercial locksmiths. All parties influenced or impacted by the specifications are considered stakeholders for this research. The argument could be made the stakeholders are the most important element of the requirements because it is their needs that must be satisfied. To effectively prioritize all needs, every stakeholder must be identified, and their need accurately documented, and quantify the influence and impact of each while accurately documenting each stakeholder need (Blanchard and Fabrycky 2011). The tasks seem rudimentary, but human factors are always involved. The stakeholder must provide the need, but the responsibility falls on the entity fabricating the specification, in this case, GSA. This research executed the stakeholder analysis using my experience gained from years on the IACSE committee as well as input from other subject matter experts.

1. Stakeholder Analysis

The first step of a stakeholder analysis is to identify all stakeholders involved in the system, or this case, involved in the specification requirements development process. The identification process examined key elements to product development, manufacturing, and support such as: who influences policy for the physical security equipment, who delivers the initial need, who produces the equipment, who supports the equipment approval, who supplies training, and who supplies ongoing field support? These considerations resulted in four categories that encompass all of the stakeholders detailed in Table 2.

Table 2. Federal Specification Stakeholders

Stakeholder Category	Stakeholder
End user	Department of Defense (DoD), Department of Energy (DoE), State Department, Department of Justice (DoJ), Federal Bureau of Investigation (FBI), National Security Agency (NSA), National Reconnaissance Office (NRO), Department of Homeland Security (DHS), Government Contractors, Non-Title 50 Agencies, National Intelligence Community (NIC)
Program Support Agencies	Information Security Oversight Office (ISOO), Defense Security Service (DSS), Interagency Committee on Security Equipment (IACSE), General Services Administration (GSA), DoD Lock Program Field Support, DoD Lock Program Testing Facility, GSA Certified Technicians & Inspectors
GSA Approved Training	Lockmasters Security Institute, MBA USA, Inc.
Container/Lock/Vault Door/Accessory Manufacturers	Container Manufacturers, Lock Manufacturers, Vault Door Manufacturers, Accessory Manufacturers

The stakeholder analysis identified the influence and impact each has on the specification (ranked by low, medium, or high). Utilizing the respective levels of impact and influence, the stakeholders were plotted on an Influence (Power) and Interest Grid for Stakeholder Prioritization (Thompson n.d.), Figure 3. The grid categorizes the data points into four quadrants based on the rankings. The grid assisted with recognizing to what degree the stakeholders shall be included in the requirements development process spanning from manage closely (keeping engaged and ensuring needs are satisfied) to monitor (kept updated but no significant effort required). The grid and categories were:

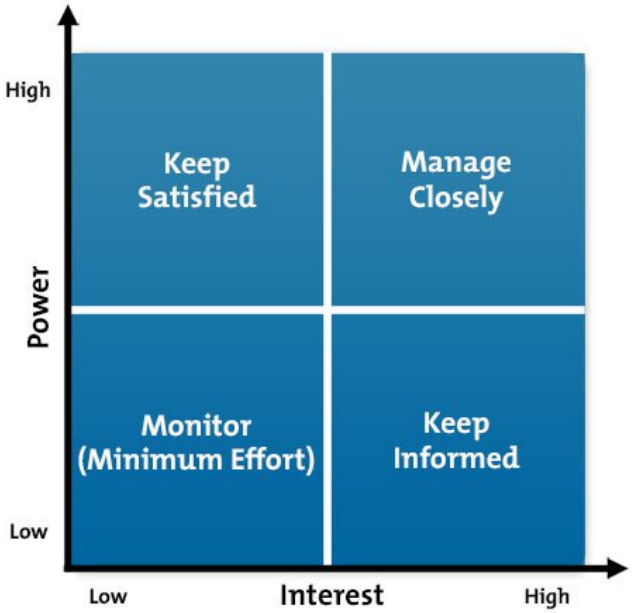

Figure 3. Power/Interest Grid for Stakeholder Prioritization. Source: Thompson (n.d.).

- Manage Closely (high influence, high interest): must fully engage and expend significant effort to satisfy.
- Keep Satisfied (high influence, low interest): keep updated but do not over communicate.

- Keep Informed (low influence, high interest): adequately inform and ensure no issues arise with these stakeholders.
- Monitor (low influence, low interest): monitor needs, but not too much communication is required.

The categorization of stakeholders required criteria to assess whether the stakeholder's interest and influence in the federal specification were low, medium, or high. The criteria was developed with the consultation of GSA and subject matter experts (see Table 3) and with considerations that included the amount invested in the particular physical security equipment, the level of involvement in the requirements development process, and the percentage of labor hours or business invested in support of the equipment.

Table 3. Stakeholder Analysis Criteria

Grading Criteria	Low	Medium	High
End user	-	-	-
Impact	Invests less than $1 million annually in product meeting specification ($100K for FF-P-110J)	Invests $1 to $5 million annually in product meeting specification ($100K - $500K for FF-P-110J)	Invests more than $5 million annually in product meeting specification (more than $500k for FF-P-100J)
Influence	Rare participant in specification fabrication	Occasional participant in specification fabrication	Active participant in specification fabrication
Program Support Agencies	-	-	-
Impact	GSA-approved product support accounts for 15% or less of labor hours	GSA-approved product support accounts for 15%-50% of labor hours	GSA-approved product support accounts for more than 50% of labor hours
Influence	Rarely supplies feedback, completes tasks necessary to GSA-approval	Occasionally supplies feedback, completes tasks necessary to GSA-approval	Consistently supplies feedback, completes tasks necessary to GSA-approval

Grading Criteria	Low	Medium	High
GSA Approved Training Centers	-	-	-
Impact	Accounts for 15% or less of training offered	Accounts for 15%-50% of training offered	Accounts for more than 50% of the training offered
Influence	Rarely supplies end user feedback, recommendations	Occasionally supplies end user feedback, recommendations	Consistently supplies end user feedback, recommendations
Container/Lock/ Vault Door/Accessory Manufacturers	-	-	-
Impact	Product accounts for 15% or less of company profits	Product accounts for 15%-50% of company profits	Product accounts for more than 50% of company profits
Influence	Rarely provides feedback, recommendations, new product capabilities	Occasionally provides feedback, recommendations, new product capabilities	Consistently provides feedback, recommendations, new product capabilities

The analysis results were consistent across all four specifications with the exemption of one case (recognized the National Intelligence Community "monitor" in FF-P-110 but as "monitor closely" in the other three specifications). Figure 4 depicts the results of the analysis is graphical form encompassing all four specifications. The results in tabular and graphical form for each specification are located in Appendix A.

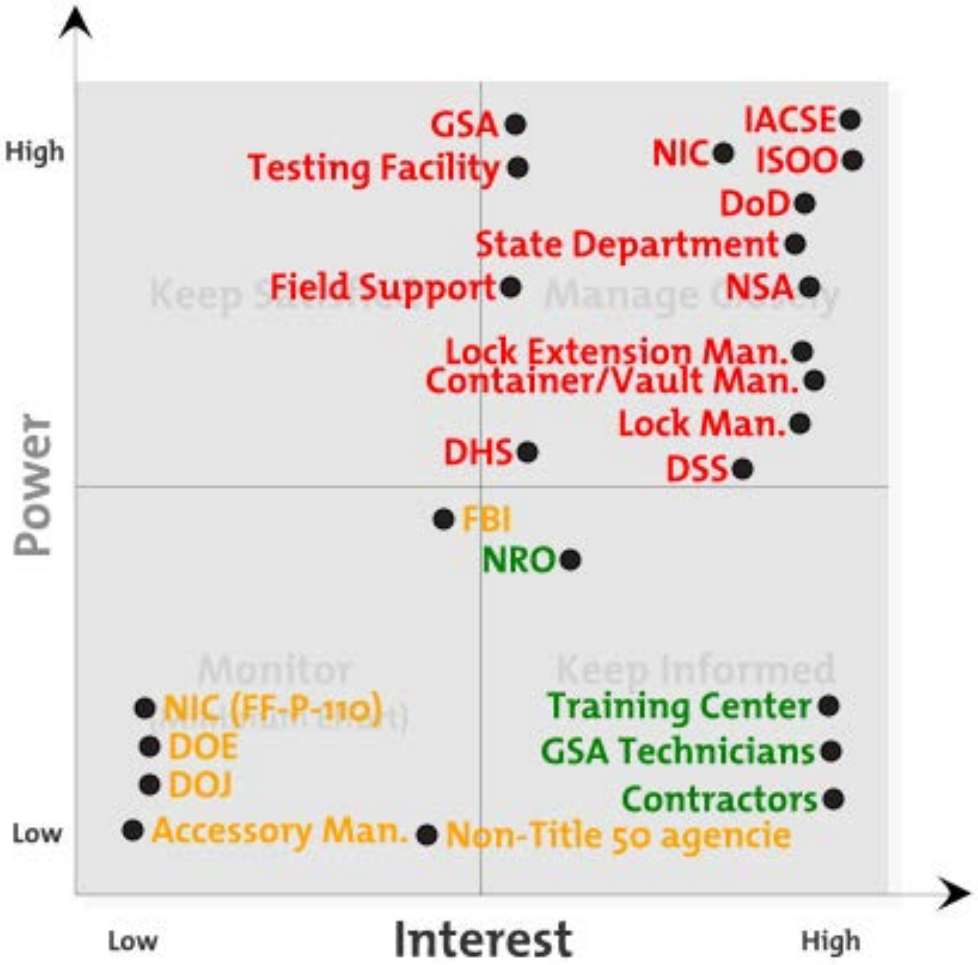

Figure 4. Stakeholder Prioritization Grid for all Specifications. Adapted from Thompson (n.d.).

a. Summary

The analysis examined all stakeholders with interest or influence in the specification to determine the level of communication that should be established for each. The categorization of each organization provided GSA with an idea of how to fabricate the communications plan for each specification. The analysis found that throughout each specification, the resulting category for each stakeholder remained the same. Table 4 details the cumulative results. Note: no stakeholder was identified in the Keep Satisfied category because all stakeholders that have high to moderate power tended to have high interest.

Table 4. Categorized Stakeholder Chart

Communications Category	Stakeholders
Manage Closely	• IACSE • National Intelligence Community • GSA • ISOO • DoD • State Department • NSA • Field Support/Testing Facility • Container Manufacturer • Lock Manufacturer • DHS • DSS
Keep Informed	• NRO • Training Center • GSA Technicians • Contractors
Monitor	• FBI • DOE • DOJ • Accessory Manufacturers

2. Needs Analysis

The objective of the needs analysis was to detail each stakeholder need to ensure inclusion in the requirements development. If one entity were left out, important requirements impacting that element of the specification could go unaddressed, leading to amendments or an ineffective product. The accuracy of the needs analysis is very significant, and as the tables will show, each stakeholder need varies. The needs for a particular stakeholder was the same throughout the four specifications due to the similarity in product capabilities. Therefore, Table 5 incorporates the needs for all specifications.

Table 5. Stakeholder Needs Analysis Results

Stakeholder	Needs
End user	
Department of Defense, Department of Energy, State Department, Department of Justice, Federal Bureau of Investigation, National Security Agency, National Reconnaissance Office, Department of Homeland Security, Government Contractors, Non-Title 50 Agencies, National Intelligence Community	Protection of classified information and secured areas, user-friendly product (usability, reliability), clear requirements
Program Support Agencies	
Information Security Oversight Office (ISOO)	Feasible and clear requirements, meets ISOO intent, delivers reliable product
Defense Security Service	Secure storage of classified information, user-friendly product (usability, movability, reliability), clear requirements
Interagency Advisory Committee on Security Equipment (IACSE)	Ensure end user needs are met, intent reflected in requirements, secure storage of classified information
General Services Administration	Responsible for specification, user-friendly product (usability, reliability), protection of classified information
DoD Lock Program Field Support	Viable procedures available, clear requirements
DoD Lock Program Testing Facility	Clear performance, design and testing requirements, feasible requirements, clear submittal requirements
GSA Certified Technicians & Inspectors	Clear GSA-approval requirements

Stakeholder	Needs
National Laboratories	Clear performance, design and testing requirements, feasible requirements, clear submittal requirements, specialized testing
Defense Logistics Agency	Viable procedures available, clear requirements
GSA Approved Training Centers	
Lockmasters Security Institute, MBA USA, Inc.	Clear performance, design requirements to guide students
Lock Manufacturers	
Kaba Mas, Sargent and Greenleaf	Clear performance, design requirements, feasible requirements, rapid access to updates, profitable/market
Container Manufacturers	
Alpha Safe and Vault, Inc., Hamilton Products Group, Inc., Will-Burt Company, A&H Security Cabinets, Inc., American Made Safe & Security, LLC.	Clear performance, design requirements, feasible requirements, rapid access to updates
Vault Door Manufacturers	
Will-Burt Company, Overly Manufacturing Co., Hamilton Products Group, Inc., International Vault, Inc., Brown Safe Manufacturing	Clear performance, design requirements, feasible requirements, rapid access to updates
Accessory Manufacturers	
Lockmasters	Clear performance, design requirements, feasible requirements, rapid access to updates

C. SUBJECT MATTER EXPERT INTERVIEWS

The physical security community relies heavily on the guidance of experts in the field when deriving new specifications, making recommendations on policy, or evaluating proposed needs. Those involved with federal specifications for more than 20 years can provide valuable insight into not only how requirements have been developed but also have a historical perspective on how decisions were made. The accumulated knowledge base of these experts is more valuable than any documentation available because they know the circumstances surrounding the determination of needs and requirements. For example, it is not documented that the events of September 11th contributed to the reinforcement of federal specification FF-L-2890 due to life safety concerns, but experts readily supply that information, "Then you add in in the life safety issues post 911 becomes very complicated. I say that because a lot of people don't realize that 911 and what went on in those towers significantly impacted the life safety requirements in the United States requirements," as claimed by Participant 5 (retired physical security specialist) in the discussion, July 21, 2019. Thus, expert insight on the subject of this research is extremely beneficial.

Five experts in the field of physical security equipment were asked to participate in interviews, all of which are members of IACSE. The selectees were chosen for the current role in federal specification development and the experience with physical security equipment. For this paper to conform to IRB protocols, names will not be associated with the results. Instead, the individuals are identified as "Participant" 1 through 5. Participants 1 through 4 were interviewed in person, and Participant 5 was interviewed over the phone. Each conversation was recorded and transcribed. The transcriptions were exported into the qualitative analysis tool, QDA Miner Lite, to establish patterns and assist with interpretation of the data provided by experts. The software was selected due to its ability to code text and analyze the code frequency among all transcripts. The interview questions are listed in Appendix B.

1. Participant Description

A brief description of each participant provides insight into the knowledge base incorporated in the supplied responses. The participants were selected based on their vast experience in the field and the different perspectives they offer.

- Participant 1: Involved with physical security at the field operator level during Naval career from 1982 through 2004 from which retired to join the DoD Lock Program as a team lead and manager. Currently fills a prominent role in the IACSE.

- Participant 2: A member of the DoD Lock Program for eighteen years and involved with reviewing, developing, interpreting, and implementing specifications. Currently an active IACSE committee member.

- Participant 3: A member of the GSA-approved testing facility for ten years where he has tested numerous products to the federal specifications for approval. Currently an active IACSE committee member.

- Participant 4: Involved in the development and testing of the physical security equipment for 20 years as a GSA employee. Currently fills a prominent role in the IACSE.

- Participant 5: Involved with physical security for over 40 years, having direct involvement with federal specifications for 25 years. An active IACSE committee member and currently the primary specification drafter.

2. Qualitative Data Analysis

The qualitative analysis executed for this research paper consisted of coding all relevant topics present in the cases, establishing the coding frequency, then analyzing the significance of the codes. “Coding” refers to the grouping or labeling of commentary into subgroups, and “cases” are the individual interviews imported into the software. The analysis can be categorized as “content analysis” because it classifies and summarizes the comments documented from the interviews. The difficult aspect of the analysis was

determining how to categorize the results in a manner that would identify themes across interviews. However, a deep examination of the data revealed relations consistent with all the codes.

The codes embodied four high-level categories that related lifecycle stages with subject matter expert observations: *Development, Evaluation, Deficiencies, and Improvements*. All the codes present in every case linked to the four recognized categories. For example, one high-level code was identified as *Development* for codes related to the characteristics and causes for specification development with sublevels: *Events, Federal Specification Manual, IACSE Review, Manufacturers Offer New Product, New Need, No Submissions, Unknown Procedure, Policy, and Sustained Development*. The "Analyze" function of the software supplied a "Code Frequency" output that tallied the code mentions in a tabular format. The tools provided in Table 8 detailing the "Category," "Code," "Description," "Count," and "Cases." The results of codes mentioned at least twice in two separate interviews are listed in Appendix B. The eight most mentioned codes are listed with descriptions below (minimum of five counts and four cases).

- **Code**: Clarity; **Category**: Evaluation; **Count:** 15; **Cases**: 5

  Description: Subject matter experts emphasized the importance of specifications to be written clearly to ensure the intended interpretation from all stakeholders involved. For example, end users rely on the specification to develop policy for appropriate use of the security equipment, while manufacturers rely on the requirements for accurate product development.

- **Code**: Changing Needs; **Category**: Evaluation; **Count:** 13; **Cases**: 4
  Description: Experts detailed the importance of monitoring changes in end user needs, which has led to past federal specification amendments and revisions. Needs naturally evolve due to technological advancements, policy alterations or tactical developments, which must be incorporated in physical security equipment requirements.

- **Code**: Need Met; **Category**: Evaluation; **Count:** 10; **Cases**: 4

Description: Experts highlighted the satisfaction of stakeholders' needs as one of the main objectives of the federal specifications. Talking points included meeting policy, end user, manufacturer, and technician needs to ensure the product is effectively implemented to protect classified information.

- **Code**: Sustained Development; **Category**: Development; **Count:** 8; **Cases**: 4

  Description: Experts mentioned that not only is the initial development of federal specifications important to produce valid equipment but also the sustained development of requirements. Requirements must be continually reviewed and evaluated for effectiveness in current applications.

- **Code**: New Need; **Category**: Development; **Count:** 6; **Cases**: 5
  Description: The identification of a new stakeholder need was identified as a major factor for amendment or revision initiation. Currently, new needs are informally introduced to the IACSE committee for review.

- **Code**: NSA Lock Need; **Category**: Deficiencies; **Count:** 6; **Cases**: 3
  Description: Three experts mentioned the current situation with NSA introducing a capabilities gap in what is required in the field versus what the FF-P-110 offers to the IACSE. All experts stated not enough requirements have been supplied to the IACSE to move forward with revisions to current specifications.

- **Code**: Classified Testing; **Category**: Improvements; **Count:** 6; **Cases**: 2
  Description: Two experts commented on the benefits of a supplemental classified testing procedure for surreptitious, covert, and forced entry tests. To avoid entry methods falling into the wrong hands, the supplement must be classified at the appropriate level. The testing procedure will allow for technique development and ensure each article is tested to the same standards.

- **Code**: Needs Analysis; **Category**: Improvements; **Count:** 5; **Cases**: 4 **Description**: All but one expert mentioned how a formalized needs analysis would assist the program in identifying needs, validating viability, and determining a path forward. Currently, there is not a formalized analysis established by the IACSE.
- **Code**: Technique Change; **Category**: Development; **Count:** 5; **Cases**: 4 **Description**: Testing and attack techniques naturally evolve with the availability of new tools and methods. Four experts mentioned the importance of the specifications and committee to stay up to date in these areas.

D. REQUIREMENTS ANALYSIS

The problem statements, stakeholder identification, needs analysis, and data gathered from the subject matter experts established the necessary foundation for the operational requirements analysis. The Blanchard and Fabrycky (2011) approach was implemented for this research to assist with the complete inclusion of all vital elements. This called for the identification of seven operational factors: mission definition, physical and performance parameters, operational deployment or distribution, operational life cycle, utilization requirements, effectiveness factors, and environmental factors. The process of developing the factors incorporated review of each specification, analysis of end user needs through observation and inquiry, and calibration with subject matter experts due to the importance of high-level accuracy for the results. Operational requirements were the basis for the functional analysis conducted later which will establish the requirements documented in the final specifications. If the requirements analysis were incomplete or inaccurate, the resulting system would have a high probability of not meeting end user needs.

Therefore, it is essential to include consideration of operational requirements at a great depth and to do so early in the system life cycle when the specification of such requirements has the greatest impact on the design. The questions to answer for each

operational factor as stated in the *Systems Engineering and Analysis* textbook are as follows:

- Mission definition: Identification of the prime and alternate or secondary missions of the system. What is the system to accomplish? How will the system accomplish its objectives? The mission may be defined through one or a set of scenarios or operational profiles. The dynamics of system operating conditions must be identified to the extent possible.
- Performance and physical parameters: Definition of the operating characteristics or functions of the system (e.g., size, weight, speed, range, accuracy, flow rate, capacity, transmit, receive, throughput, etc.). What are the critical system performance parameters? How are they related to the mission scenario?
- Operational deployment or distribution: Identification of the quantity of the equipment, software, personnel, facilities, and so on and the expected geographical location to include transportation and mobility requirements. How much equipment and associated software is to be distributed, and where is it to be located, and for how long? When does the system become fully operational?
- Operational life cycle (horizon): Anticipated time that the system will be in operational use (expected period of sustainment). What is the total inventory profile throughout the system life cycle? Who will be operating the system, and for what time?
- Utilization requirements: Anticipated usage of the system and its elements (e.g., hours of operation per day, percentage of total capacity, operational cycles per month, facility loading). How is the system to be used by the customer, operator, or operating authority in the field?
- Effectiveness factors: System requirements specified as figures-of-merit (FOMs) such as cost/system effectiveness, operational availability (Ao), readiness rate, dependability, logistic support effectiveness, mean time between maintenance (MTBM), failure rate (λ), maintenance downtime (MDT), facility utilization (in percent), operator skill levels and task accomplishment requirements, and personnel efficiency. Given that the system will perform, how effective or efficient is it? How are these factors related to the mission scenario?
- Environmental factors: Definition of the environment in which the system is expected to operate (e.g., temperature, humidity, artic or tropics, mountainous or flat terrain, airborne, ground, or shipboard). This should include a range of values as applicable and should cover all transportation, handling, and storage modes. How will the system be handled in transit? To what will the system be subjected during its operational use, and for how long? A complete environmental profile should be developed. (Blanchard and Fabrycky 2011, 61)

The analysis results for each specification are described in the following sections. Each section underwent multiple iterations to reach the final product. The objective was to complete the analysis using the program manager's perspective to evaluate how effective the tool could be.

1. Electromechanical Combination Lock

- Mission definition: The lock shall secure classified material using a hand-operated deadbolt mechanism installed on security containers and pedestrian doors. The lock must require an established combination to retract the bolt.

- Physical and performance parameters: The lock must incorporate a self or battery-powered display, or graduated dial enabling manual bolt retraction with a minimum of 1,000,000 different combinations and dual combination capabilities. The locking system must resist 20 man-hours of manipulation and radiological attack, 30 man-minutes of covert entry, and 20 man-hours of surreptitious entry. The lock body must fit the "magic module footprint" (3.343" x 2.397") with specified mounting hole diameter and locations.

- Operational deployment or distribution: The locks shall be located on assets securing classified information (i.e., security containers and doors to open storage areas). Product meeting the specification will be shipped all over the world and used by the government and its contractors CONUS and OCONUS.

- Operational life cycle: Locks must operate for 10,000 cycles (based on 20-year use operated twice daily).

- Utilization requirements: The locks will secure containers or facilities when unattended with unlimited use during daily operations and used by personnel with basic operation knowledge.

- Effectiveness factors: The locks shall require no more than annual maintenance, have a failure rate of less than 10% during testing, require no more than a two-day training course to certify personnel on maintenance, repair, and installation of the product, and be operable by personnel with limited experience based on provided instructions.

- Environmental factors: Locks shall operate in primarily habitable indoor conditions but also limited outdoor conditions exposed to high and low temperatures, salt spray, moisture, UV rays, debris, and shock over a 20-year life cycle.

2. Pedestrian Door Assembly

- Mission definition: The pedestrian door lock extension must provide single egress with configurations including capabilities of housing a magic module footprint deadbolt, lock integrating with existing facility access control, incorporating built-in access control, providing secondary door access (no lock meeting FF-L-2740) and incorporating permanently deadbolt exit only egress.

- Physical and performance parameters: The lock extensions must be American Disabilities Act (ADA), Architectural Barriers Act (ABA), Uniform Federal Accessibility Standards (UFAS), International Build Code (IBC), National Fire Protection Association (NFPA) and International Fire Code (IFC) compliant and resist 20 man-hours of surreptitious entry.

- Operational life cycle: Lock extensions must operate for 500,000 cycles without replacement of any component.

- Utilization requirements: The lock extensions will secure facilities when unattended with unlimited use during daily operations and used by personnel with basic operation knowledge.

- Effectiveness factors: The lock extensions shall require no more than annual maintenance, have a failure rate of less than 10% during testing, require no more than a two-day training course to certify personnel on maintenance, repair, and installation of the product, and be operable by personnel with limited experience based on provided instructions.

- Environmental factors: Locks shall operate in primarily habitable indoor conditions but also limited outdoor conditions exposed to high and low temperatures, salt spray, moisture, UV rays, debris, and shock over a 20-year life cycle.

3. Combination Padlock

- Mission definition: The padlock must secure with a shackle and grant access only with an appropriate combination.

- Physical and performance parameters: The padlock must have a minimum of 30,000 different combinations, a ¼-dial number dialing tolerance, at least three combination wheels and cam. “The outside dimensions across the shackle shall be of 1.5 inches ±0.125-inch (38.1 millimeters (mm) ±3.175 mm), and the space under the shackle shall be of sufficient size to fasten around a 0.75-inch (19.05 mm) diameter bar. The diameter of the shackle shall be 0.31-inch -0.00, +0.02-inch (7.938 mm -0.00, +0.55 mm). The length of the padlock, when locked, shall be 4.375 inches (111.125 mm) maximum. The width or thickness shall not exceed 2.75 inches (69.85 mm)” (General Services Administration 1997, 5).

- Operational life cycle: Padlock must operate for 5,000 cycles without replacement of any component.

- Utilization requirements: The padlock will secure classified equipment when unattended with unlimited use during daily operations and used by personnel with basic operation knowledge.

- Effective factors: The locks shall require no more than annual maintenance, have a failure rate of less than 10% during testing, require no more than a one-day training course to certify personnel on maintenance, repair,, and installation of the product, and be operable by personnel with limited experience based on provided instructions.

- Environmental factors: Locks shall operate in primarily habitable indoor conditions but also limited outdoor conditions exposed to high and low temperatures and moisture over a 20-year life cycle.

4. Security Cabinet

- Mission definition: The six-sided cabinet shall secure classified material by utilizing a combination lock meeting with the magic module footprint. Depending on the configuration, the cabinet is to protect hard copy classified documents, weapons, or other classified material with dimensions that will enable storage.

- Physical and performance parameters: The cabinets must resist “20 man-hours surreptitious entry, 30 man-minutes covert entry, and ten man-minutes forced entry” (General Services Administration 2010, 1) (forced entry requirements only for Class 5). The required configurations include those with multiple control drawers (drawers mounted with lock), single control drawer, styles with varying sizes, and capable of storing weapons and being mounted.

- Operational life cycle: Cabinet must operate for 50,000 cycles without replacement of any component.

- Utilization requirements: The cabinet will secure classified material when unattended with unlimited use during daily operations and used by personnel with basic operation knowledge.

- Effective factors: The cabinet shall require no more than annual maintenance, have a failure rate of less than 10% during testing, require no more than a one-day training course to certify personnel on maintenance, repair, and installation of the product, and capable of being operated by personnel with limited experience based on provided instructions.

- Environmental factors: Cabinets shall operate in primarily habitable indoor conditions but also limited outdoor conditions for particular mountable configurations exposed to shock and vibration.

5. Summary

The analysis examines the precise needs by assigning quantitative values, which allows for confirmation by end users and serves as a feasibility check. The quantitative data is essential for the development of general operational requirements to be further decomposed via the functional analysis. The following functional analysis will include all operational requirements while ensuring the inclusion of an adequate decomposition of sub-levels.

E. FUNCTIONAL ANALYSIS

Functional analysis decomposes the top-level function of a system or in this case, physical security equipment, into all the required sub-level functions in detail. The sub-level functions provide the last piece in the requirements development process as needs were boiled down from general problem statements to function diagrams addressing each functional component. The analysis was completed with the operational requirements as the baseline and utilized the review of security experts. The current specifications were referenced, but not relied on for descriptions of all functions as an examination of the equipment's physical requirements went beyond what is currently available. For each specification, the top-level functions were decomposed until it was determined an adequate sub-level was reached using a hierarchy diagram. The function diagrams were composed on Innoslate, a systems engineering tool supporting the integration of requirements analysis

and management, functional analysis and allocation, solution synthesis, test/evaluation, and simulation (Innoslate 2017).

Functions refer "to a specific or discrete action that is necessary to achieve a given objective" (Blanchard and Fabrycky 2011, 86). Thus, the specific detailed requirements addressing the values associated with the functions are derived from the function hierarchical diagram. For example, "withstand exposure to high temperatures" is the function the product must execute. However, the requirement the system is to execute associated with the function could be "The lock shall operate in a temperature range of -10ºF to 158ºF (-23.3ºC to 70.0ºC). Locks shall be tested for compliance with this requirement in accordance with 4.6.10" (GSA 2011). The analysis assists program management in identifying all the functional needs of the system, which are then correlated to requirements based on an existing policy, product specifications, anticipated system environment, and other factors. The next sections will present the functional analysis results of the four specifications in the tabular format. Appendix A includes the hierarchy charts.

1. Electromechanical Combination Lock

Below are the results of the FF-L-2740 *Locks, Combination, Electromechanical* functional analysis. The functional hierarchy diagram can be found in Appendix C.

Table 6. FF-L-2740 Functional Analysis Results

Prime Function	1st Level	2nd Level	3rd Level
0.0 Prevent unauthorized access to security containers and doors	1.0 Secure with deadbolt	1.1 Fit all applications	1.1.1 Fit one precise footprint including thickness
		1.2 Remain attached through all uses	1.2.1 Mount to all applications adequately
	2.0 Delay physical manipulation	2.1 Resist electromagnetic pulse exposure	2.1.1 Expose to a determined level of electromagnetic pulse

Prime Function	1st Level	2nd Level	3rd Level
			2.1.2 Operate after exposure
		2.2 Resist electrostatic charge	2.2.1 Expose to a determined level of electrostatic charge
			2.2.2 Operate after exposure
		2.3 Delay surreptitious entry	2.3.1 Expose to determined surreptitious techniques
			2.3.2 Prevent extraction of material in the allotted time
		2.4 Delay covert entry	2.4.1 Expose to determined covert entry techniques
			2.4.2 Prevent extraction of material in the allotted time
		2.5 Retract bolt only with the correct input	2.5.1 Enable storage of a determined amount of codes
			2.5.2 Enable change of combination with a correct combination input
	3.0 Prevent software manipulation	3.1 Product during fabrication	3.1.1 Establish manufacturer security clearance
			3.1.2 Ensure secure means of shipment throughout
			3.1.3 Secure facilities when unattended

Prime Function	1st Level	2nd Level	3rd Level
		3.2 Software protective design coding	3.2.1 Ensure adequate cybersecurity is implemented
			3.2.2 Prevent malicious coding
	4.0 Withstand environmental impact	4.1 Withstand long-distance shipping	4.1.1 Withstand incurred vibrations
			4.1.2 Withstand incurred temperatures
			4.1.3 Withstand incurred pressures
		4.2 Continue operation in a corrosive environment	4.2.1 Withstand salt spray and moisture
		4.3 Continue operation in high temperatures	4.3.1 Withstand determined exposure to high-temperature environments
		4.4 Continue operation in low temperatures	4.4.1 Withstand determined exposure to low-temperature environments
	5.0 Operate through the anticipated life cycle	5.1 Display limited failures during testing	5.1.1 Pass predetermined percentage of tests
		5.2 Operate through daily demand	5.2.1 Pass determined amount of cycles
		5.3 Operate with limited maintenance required	5.3.1 Pass determined amount of cycles
		5.4 Operate by personnel relying solely on instructions	5.4.1 Operate by individuals without formal training

Prime Function	1st Level	2nd Level	3rd Level
	6.0 Install by certified technicians	6.1 Train technicians in a reasonable duration	
		6.2 Administer certificates by manufacturers	6.2.1 Administer training directly by the manufacturer
			6.2.2 Administer training by approved training facility (curriculum supplied by the manufacturer)

2. Pedestrian Door Assembly

Below are the results of the FF-L-2890 *Lock Extension (Pedestrians Door Lock Assembly Preassembled, Panic, and Auxiliary Deadbolt)* functional analysis. The functional hierarchy diagram can be found in Appendix C.

Table 7. FF-L-2890 Functional Analysis Results

Prime Function	1st Level	2nd Level	3rd Level
0.0 Delay unauthorized access to a secure area	1.0 Provide single egress and access	1.1 Allow for single-hand egress	1.1.1 Comply with all applicable codes
		1.2 Allow for single-hand access	1.2.1 Comply with all applicable codes
	2.0 Secure with pedestrian door	2.1 Configure with building access control for day use	2.1.1 Allow the extension to open with credentials
			2.1.2 Compatible with access control
			2.1.3 Secure with deadbolt retracted and no credential input
		2.2 Secure with separate deadbolt when unattended	2.2.1 Compatible with FF-L-2740 combination lock

Prime Function	1st Level	2nd Level	3rd Level
			2.2.2 Interface with the door assembly
			2.2.3 FF-L-2740 included in the deliverable
	3.0 Delay physical manipulation	3.1 Delay surreptitious entry	3.1.1 Expose to determined surreptitious entry techniques
			3.1.2 Delay bypass of locking mechanism
	4.0 Withstand environmental impact	4.1 Withstand long-distance shipping	4.1.1 Withstand incurred vibrations
			4.1.2 Withstand incurred temperatures
			4.1.3 Withstand incurred pressures
		4.2 Continue operation in high temperatures	4.2.1 Withstand determined exposure to high-temperature environments
		4.3 Continue operation in low temperatures	4.3.1 Withstand determined exposure to low-temperature environments
	5.0 Operate through the anticipated life cycle	5.1 Operate through daily demand	5.1.1 Pass determined amount of cycles
		5.2 Operate with limited maintenance required	5.2.1 Pass determined amount of cycles
		5.3 Operate by personnel relying solely on instructions	5.3.1 Operate by individuals without formal training

Prime Function	1st Level	2nd Level	3rd Level
	6.0 Install by certified technicians	6.1 Train technicians in a reasonable duration	
		6.2 Administer certificates by manufacturers	6.2.1 Administer training directly by the manufacturer
			6.2.2 Administer training by approved training facility (curriculum supplied by the manufacturer)

3. Combination Padlock

Below are the results of the FF-P-110 *Padlock, Changeable Combination (Resistant to Opening by Manipulation and Surreptitious Attack)* functional analysis. The functional hierarchy diagram can be found in Appendix C.

Table 8. FF-P-110 Functional analysis results

Prime Function	1st Level	2nd Level	3rd Level
0.0 Prevent unauthorized access to classified equipment	1.0 Secure with shackle	1.1 Physically fit desired applications	1.1.1 Fit through hasp being secured
			1.1.2 Fit around hasp being secured
	2.0 Delay physical manipulation	2.1 Resist radiographic techniques	2.1.1 Expose to a determined level of radiographic techniques
			2.1.2 Delay unlatching of the shackle
		2.2 Delay surreptitious entry	2.2.1 Expose to determined surreptitious entry techniques

Prime Function	1st Level	2nd Level	3rd Level
			2.2.2 Delay unlatching of the shackle
			2.2.3 Demonstrate tamper signs
		2.3 Delay manipulation	2.3.1 Expose to manipulation techniques
			2.3.2 Delay unlatching of the shackle
		2.4 Unlatch shackle only with access	2.4.1 Enable storage of a determined amount of codes
			2.4.2 Enable change of code with correct code without formal training
	3.0 Withstand environmental impact	3.1 Operate in humid environments	3.1.1 Withstand moisture
		3.2 Operate in high temperature	3.2.1 Withstand determined exposure to high temperature
		3.3 Operate in low temperatures	3.3.1 Withstand determined exposure to low temperature
	4.0 Operate through the anticipated life cycle	4.1 Operate through daily demand	4.1.1 Operate after determined cycles
		4.2 Operate with limited maintenance	4.2.1 Operate after determined cycles
		4.3 Operate only utilizing instructions	4.3.1 Operate and install by personnel with no formal training

4. Security Cabinet

Below are the results of the AA-F-358 *Filing Cabinet, Legal and Letter Size, Uninsulated* functional analysis. The functional hierarchy diagram can be found in Appendix C.

Table 9. AA-F-358 Functional Analysis Results

Prime Function	1st level	2nd level	3rd level
0.0 Prevent unauthorized access to classified material	1.0 Secure classified material	1.1 Store classified material	1.1.1 Allow access to material with deadbolt retracted
			1.1.2 Provide space for classified documents
			1.1.3 Allow for compartmentalized storage
		1.2 Secure with a separate deadbolt	1.2.1 Interface locking components with deadbolt
			1.2.2 Deadbolt mechanism to meet FF-L-2740
			1.2.3 FF-L-2740 included in the deliverable
	2.0 Delay physical manipulation	2.1 Delay forced entry (Class 5)	2.1.1 Expose to forced entry techniques
			2.1.2 Delay extraction of classified material
		2.2 Delay surreptitious entry	2.2.1 Expose to surreptitious entry techniques
			2.2.2 Delay extraction of classified material

Prime Function	1st level	2nd level	3rd level
		2.3 Delay covert entry	2.3.1 Expose to covert entry techniques
			2.3.2 Delay extraction of classified material
	3.0 Secure classified material on mobile platforms	3.1 Include mountable configuration	3.1.1 Include mountable surface separate but attached to the system
			3.1.2 Mountable solely utilizing instructions
		3.2 Withstand shock and vibration	3.2.1 Withstand incurred shock and vibration from all mobile platforms
	4.0 Operate through the anticipated life cycle	4.1 Operate through daily demand	4.1.1 Operate after determined cycles
		4.2 Operate with limited maintenance	4.2.1 Operate after determined cycles
		4.3 Operate only utilizing instructions	4.3.1 Operate and install by personnel with no formal training

F. SUMMARY

The systems engineering analyses implemented in this section provide a detailed incremental approach to developing requirements for complex systems. However, the tools correlate well to specification requirements development. The executed analyses ensured examination of specification problem statements, identification and ranking of all stakeholders and needs, the inclusion of subject matter expert inputs, the examination of operational requirements, and development of function hierarchy chart. The functional analysis provides the responsible party the necessary foundation to develop requirements

for specification input. The results demonstrate a systems engineering approach can be implemented with physical security federal specifications, which were only an assumption prior. The next section discusses the value and possible future use of the systematic approach outlined in this research with physical security equipment specifications.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. DISCUSSION

GSA has published 14 federal specifications that have delivered physical security equipment currently used to secure national classified information and arms, ammunition, and explosives (AA&E). However, all specifications administer amendments, with some experiencing up to ten complete revisions. Subject matter expert interviews revealed that the cause of specification updates are due to stakeholder need changes, lack of complete understanding of stakeholder needs or misguided system function identification. GSA implements a "feature-based approach" to specification development that can be characterized as informal brainstorming lists of requirements. While subject matter experts complete the brainstorming sessions via the IACSE Committee, the execution is not standardized nor documented. "The feature-based approach enables developers to quickly elicit and collect requirements inputs with a minimal effort" (Wasson 2005, 344). However, as stated in the textbook *System Analysis, Design and Development*, the approach is prone to resulting in "missing, misplaced, conflicting or contradictory and duplicated requirements", which is consistent with the number of specification revisions (Wasson 2005, 343).

These analyses intend to demonstrate an improvement in physical security equipment specification requirements development through the implementation of a systems engineering approach. A definitive indication of such an improvement was the identification of requirements missing from current specifications. Due to a lack of resources, the research could not complete the necessary analysis to detail all required specifications. The research could not obtain complete involvement from stakeholders such as the manufacturers, GSA, the IACSE committee or the DoD Lock Program because funding is not allocated for such an effort. Thus, no insight from manufacturers, detailed analysis from IACSE, or access to testing procedures was included in the research. However, a particular value of the approach was evident. Although all existing requirements could not be validated, the approach offers tools that will lead to fewer amendments and improved documentation if adopted in the current process. This section

will illustrate how each tool supplies value to the development process and what future actions from GSA can take to improve the current process.

A. PROBLEM STATEMENT

The problem statement identification ensures the program manager truly understands the reason for the design of a system acting as the solution. Lessons learned were discovered during the construction of the statements for each specification. We realized that the tendency to add too much detail to the statement could restrict the design of the system. For example, stating a system "must prevent physical manipulation" implies an absolute condition that may not be feasible. "Prevent" implies the system shall not allow physical manipulation at all, no matter the duration. In reality, there are security measures set in place that resist identified threats within a certain period so the correct nomenclature is "delay" in this case. Also, existing specifications cannot be solely relied on to recognize the problem. This initial action in the approach is vital because a system cannot satisfy end user needs when it solves an inaccurate problem.

B. STAKEHOLDER AND NEEDS ANALYSIS

The stakeholder analysis provides a means of documenting and prioritizing all parties which impact and influence the system. Currently, members of the IACSE have the experience and history of knowing how each stakeholder affects the requirements development process, but there is no formalized approach or plan for coordination. The stakeholder analysis ranked the groups into the categories *manage closely, keep satisfied, keep informed* and *monitor* which allows GSA to consider communication strategies. The results of the analysis were expected based on the current inclusion of stakeholders in the decision processes. However, one entity in the *manage closely* category is not engaged to the appropriate degree. The Information Security Oversight Office (ISOO) is responsible for disseminating policy on the procurement of physical security equipment and impacts the specifications by dictating the use of certain products. For example, ISOO Notice 2014-02 states GSA-approved security containers and vault doors must be procured through the GSA supply center rather than directly from container manufacturers (ISOO 2014). The analysis showed the stakeholder is one of the most impactful and influential parties but

does not have an active role in the IACSE. Thus, ISOO is not consistently informed of the committee decisions and the thought process behind the decisions. Based on the findings of the analysis, the composition of a communication plan is suggested for GSA to document the detailed actions of inclusion for all stakeholders. GSA could use the provided analysis as a baseline for development.

The needs analysis detailed the general needs of each stakeholder recognized to have an impact and/or influence over the federal specifications. However, due to time and resource constraints, the analysis did not include input from each entity. Consequently, the results are based solely on experience within the IASCE and collaboration with subject matter experts. A more inclusive analysis may render information directly from stakeholders that have not yet been considered. For example, manufacturers may offer suggestions on how to detail requirements that do not limit the possibilities of viable configurations. Other inputs not present in the research include end user, installer, training facility, testing facility, and field support perspectives on the adequacy and effectiveness of current federal specifications. Thus, it is recommended that GSA conduct a needs analysis for each specification to further detail considerations for future specifications resulting in a complete document. However, out of all the recommendations, the needs analysis for every stakeholder is the least vital because GSA has a considerably accurate view of each need with the immense experience gained from past interactions.

C. SUBJECT MATTER EXPERT INTERVIEWS

The subject matter expert interviews were particularly valuable. The strategic selection of interviewees offered a range of perspectives resulting in a complete description of the specification development process and what may be missing. Consistencies amongst the five interviews were apparent, but each also offered unique insight on how the requirement development process could be improved. The qualitative data analysis categorized the transcript codes into four themes: *Development, Evaluation, Deficiencies, and Improvements*. The top five codes identified, *Clarity* (15), *Changing Needs* (13), *Need Met* (10), *Sustained Development* (8), and *New Needs* (6), represent the reflections of the evaluation and development process of the specifications. The importance of clear

requirements, addressing changing, and newly discovered needs, fully satisfying end user needs and continually developing requirements were reflected in all of the interviews.

The high-volume mention of clarity is not surprising due to the number of varying stakeholders that rely on the specifications. End users must ensure they meet the storage requirements of classified information. Manufacturers must ensure products satisfies all standards. Misinterpretation of the requirements has led to incorrect storage of material, disputes on how to store material, and ineffective products submitted for testing. The recognition of changing, new, and satisfying needs is also apparent in the results, which lends insight to amendments and revisions. IACSE prioritizes the identification of need when initiating new specifications or amendments to existing specifications. The revision to FF-L-2890 is an example of a changing need addressed by the committee. FF-L-2890C includes four new "types" of pedestrian door assemblies that cover secondary door and exit only door applications, which do not include combination deadbolt locks (General Services Administration 2019). The need was informally introduced to the committee by government agencies who are increasing the size of secured areas. The greater secured area footprint requires more exits to meet life safety requirements. Also, IACSE emphasizes the specifications cannot be stagnant. Sustained development or continually review of the documents must be completed to identify elements overlooked in the past. The next three most mentioned codes understand deficiencies and recommended improvements from the subject matter experts, which were relevant and consistent with the systems engineering approach.

First, three of the five experts noted an issue with receiving a detailed need from stakeholders, in particular, the need for a lock to secure classified network cables. Currently, locks meeting FF-P-110 do not satisfy end user needs due to usability and inability to withstand outdoor environments, but the IACSE is unsure of what exactly the need is. "For instance, when I was mentioning earlier with the National Security Agency (NSA) issue, we haven't seen any white paper or anything written from their agency pushed up the chain to DoD or OUSDI asking for changes to a spec or creating a new spec to meet someone's actual needs and requirements," as claimed by Participant 2 (physical security specialist) in discussion on July 19, 2019. Therefore, the experts mentioned the creation of

descriptive documentation as a supplement to aid the specification development. A needs analysis directed by GSA to identify the true base operational needs through agency and end user interviews and written input would provide essential documentation for requirements development.

Furthermore, the documentation would act as reference material to answer future inquiry into each requirement. All the experts also asserted the lack of supplemental documentation for testing requirements in some manner. Two supplementals emerged: a classified supplemental to detail the testing requirements for entry tests (forced, covert and surreptitious entry) and complete overall testing requirements for each specification. The supplement detailing testing procedures for the entry tests must be classified because public knowledge of entry techniques is accessible to enemy threats that could implement the techniques for unauthorized access to protected classified information. For this reason, it is recommended GSA establish supplemental unclassified and classified testing requirements for each specification. This would ensure consistency for tested products, letting manufacturers with the appropriate clearance to know how the product is tested, and comprehensive supplemental testing requirements. The supplements would allow the testing facility to defend determinations if questioned by submitting the manufacturer and solidify the program. The official recommendation backed by the interviews will act as the driving force for improvement.

D. OPERATIONAL REQUIREMENTS AND FUNCTIONAL ANALYSIS

The execution of the operational requirements and functional analysis were thought to identify requirements in the four specifications that are currently not present. However, the inability to collaborate with experts for each product did not make full inclusion of all requirements possible. Nevertheless, the execution of complete requirements and functional analysis would, at the very least, provide documentation on how the requirements were formulated. Currently, if a question as to why a particular requirement was included in a specification arises, the IACSE can only answer based on memory or expert reference. Documenting this knowledge would decrease the probability of the committee committing the same error in requirement development. Thus, we recommend

that GSA designate a team of experts to complete functional analysis for each specification as supplemental documentation. The analyses will act as working documents for the IACSE.

V. RECOMMENDATIONS AND CONCLUSION

Physical security equipment has been developed through the implementation of federal specifications since 1954, resulting in reliable locking and storage systems for classified information. Nonetheless, specifications undergo numerous amendments and revisions to satisfy further end user needs that sometimes do not change but rather are not identified during the conception of specification requirements. The goal of the "system engineering approach is to justify these resource requirements through a top-down approach and to ensure the proper development of each through a fully integrated system" (Blanchard and Blyler 2016, 22). So, this research strived to answer the question: Can implementation of systems engineering processes improve the development of current design and performance requirements in physical security equipment federal specifications?

The method to formulate a viable answer was to select four federal specifications, identify the most appropriate systems engineering tools for application, execute the systems engineering approach for each specification, analyze the results and determine whether the approach improves the requirements development process. As referenced in the discussion, the revealing of missing requirements was thought to be the concrete evidence required to confirm improvements. However, due to lack of resources and the direct involvement from the IACSE, the requirements and functional analysis could not be executed with all necessary inputs. Expert involvement for each locking and storage system would be required and is feasible if implemented by the governing agency, GSA. Nonetheless, the research did discover process improvements through the analyses and interviews.

A. RECOMMENDATIONS

The IACSE implements an effective specification requirements process and produces specifications that provide the warfighter with systems to secure classified information. This research has uncovered that the process is lacking formal analysis, procedural documentation, and a structure, which is the major advantage of the system

engineering approach. Thus, the simulation of the approach for the four specifications revealed the application of the following tools which will improve the process by providing documentation for reference, in-depth analysis of vital components leading to the accurate identification of stakeholder needs and a structured method for consistency in requirements development:

- Establish a well-defined problem statement for each federal specification that clearly defines the end user need. The statement can be fluid based on the changing demands experienced in the field driven by advancements in technology.

- Develop a communications plan for internal use to ensure all stakeholders are involved to the appropriate level through the requirements development process.

- Create a needs analysis template (document or process within its own) to be administered when an agency contacts IACSE with the need for an alteration to an existing product or a new product. The tool will identify the true need through analysis rather than hearsay from an agency representative.

- Develop detailed test plans for each specification, including classified supplemental for entry tests to document how each requirement is tested and promote consistency in testing. The plans should be working documents and evolve as new equipment or techniques are discovered.

- Develop a functional analysis template for implementation on each specification that will supply a basis for all generated requirements. The analysis will provide IACSE a documented and visual aid to ensure the incorporation of all functions.

The five recommendations have been presented to GSA and have received positive feedback thus far. Questions as to how to administer and who will be responsible for the actions will need to be finalized with input from the IACSE. The execution of the new

approach will, at the least, provide documentation, which is currently not available for GSA to reference when future development is required. Therefore, the research identified systems engineering tools that will improve the physical security equipment requirements development process.

B. CONCLUSION

The systems engineering approach implemented in the research is not only beneficial for the four specifications identified, but for all GSA owned physical security equipment specifications. The adoption of the methodology by GSA would take considerable time and effort, but the documentation and standardized approach would lead to a more exhaustive examination of requirements development. Comprehensive implementation includes involvement from a designated project manager and insight from end users, technicians, manufacturers, and all support components. Furthermore, GSA owns seven hundred and ninety federal specifications. Consideration of the methodology can be applied to federal specifications determined to be high priority products such as those that protect classified information. The inclusion of a systems engineering approach to government product requirements development is worth implementation.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. STAKEHOLDER ANALYSIS RESULTS

A. ELECTROMECHANICAL COMBINATION LOCK

Below are the results of the FF-L-2740 *Locks, Combination, Electromechanical* stakeholder analysis.

Table 10. FF-L-2740 Stakeholder Analysis Results

Stakeholder	Impact	Influence	Category
End user	-	-	-
Department of Defense	High	High	Manage Closely
Department of Energy	Low	Low	Monitor
State Department	High	High	Manage Closely
Department of Justice	Low	Low	Monitor
Federal Bureau of Investigation	Medium	Medium	Monitor
National Security Agency	High	High	Manage Closely
National Reconnaissance Office	Medium	Medium	Keep Informed
Department of Homeland Security	Medium	Medium	Manage Closely
Government Contractors	High	Low	Keep Informed
Non-Title 50 Agencies	Medium	Low	Keep Informed
National Intelligence Community	High	High	Manage Closely
Program Support Agencies			
Information Security Oversight Office (ISOO)	High	High	Manage Closely
Defense Security Service	High	Medium	Manage Closely
Interagency Advisory Committee on Security Equipment (IACSE)	High	High	Manage Closely
General Services Administration	Medium	High	Manage Closely
DoD Lock Program Field Support	Medium	High	Manage Closely
DoD Lock Program Testing Facility	High	High	Manage Closely
GSA Certified Technicians & Inspectors	High	Low	Keep Informed
National Laboratories	Low	High	Keep Informed
Defense Logistics Agency	Low	Low	Monitor
GSA Approved Training Centers	-	-	-
Lockmasters Security Institute	High	Low	Keep Informed
MBA USA, Inc.	High	Low	Keep Informed
Lock Manufacturers	-	-	-

Stakeholder	Impact	Influence	Category
Kaba Mas	High	Medium	Manage Closely
Sargent and Greenleaf	High	Medium	Manage Closely
Container Manufacturers	-	-	-
Alpha Safe and Vault, Inc.	High	Medium	Manage Closely
Hamilton Products Group, Inc.	High	Medium	Manage Closely
Will-Burt Company	High	Medium	Manage Closely
A&H Security Cabinets, Inc.	High	Medium	Manage Closely
American Made Safe & Security, LLC.	High	Medium	Manage Closely
Vault Door Manufacturers	-	-	-
Will-Burt Company	High	Medium	Manage Closely
Overly Manufacturing Co.	High	Medium	Manage Closely
Hamilton Products Group, Inc.	High	Medium	Manage Closely
International Vault, Inc.	High	Medium	Manage Closely
Brown Safe Manufacturing	High	Medium	Manage Closely
Accessory Manufacturers	-	-	-
Lockmasters	Low	Low	Monitor

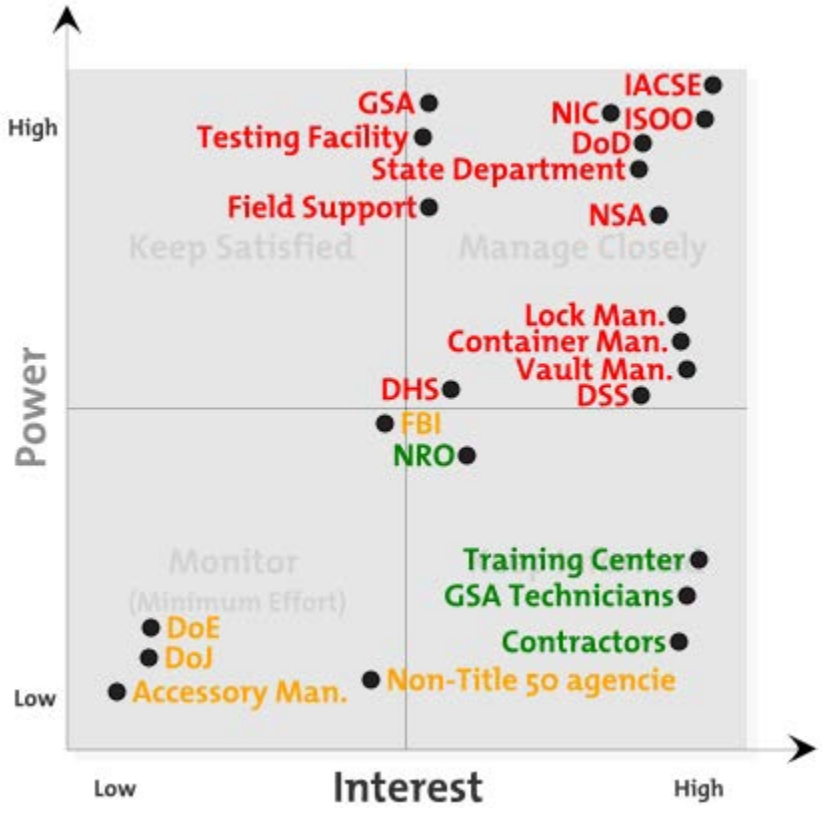

Figure 5. FF-L-2740 Stakeholder Prioritization Grid. Adapted from Thompson (n.d.).

B. PEDESTRIAN DOOR ASSEMBLY

Below are the results of the FF-L-2890 *Lock Extension (Pedestrians Door Lock Assembly Preassembled, Panic, and Auxiliary Deadbolt)* stakeholder analysis.

Table 11. FF-L-2890 Stakeholder Analysis Results

Stakeholder	Impact	Influence	Category
End user	-	-	-
Department of Defense	High	High	Manage Closely
Department of Energy	Low	Low	Monitor
State Department	High	High	Manage Closely
Department of Justice	Low	Low	Monitor
Federal Bureau of Investigation	Medium	Medium	Monitor
National Security Agency	High	High	Manage Closely
National Reconnaissance Office	Medium	Medium	Keep Informed
Department of Homeland Security	Medium	Medium	Manage Closely
Government Contractors	High	Low	Keep Informed
Non-Title 50 Agencies	Medium	Low	Monitor
National Intelligence Community	High	High	Manage Closely
Program Support Agencies			
Information Security Oversight Office (ISOO)	High	High	Manage Closely
Defense Security Service	High	Medium	Manage Closely
Interagency Advisory Committee on Security Equipment (IACSE)	High	High	Manage Closely
General Services Administration	Medium	High	Manage Closely
DoD Lock Program Field Support	Medium	High	Manage Closely
DoD Lock Program Testing Facility	High	High	Manage Closely
GSA Certified Technicians & Inspectors	High	Low	Keep Informed
Defense Logistics Agency	Low	Low	Monitor
GSA Approved Training Centers	-	-	-
Lockmasters Security Institute	High	Low	Keep Informed
MBA USA, Inc.	High	Low	Keep Informed
Lock Manufacturers	-	-	-
Kaba Mas	High	Medium	Manage Closely
Sargent and Greenleaf	High	Medium	Manage Closely

Stakeholder	Impact	Influence	Category
Lock Extension Manufacturers	-	-	-
Kaba Mas	High	Medium	Manage Closely
Lockmasters	High	Medium	Manage Closely
Sargent and Greenleaf	High	Medium	Manage Closely

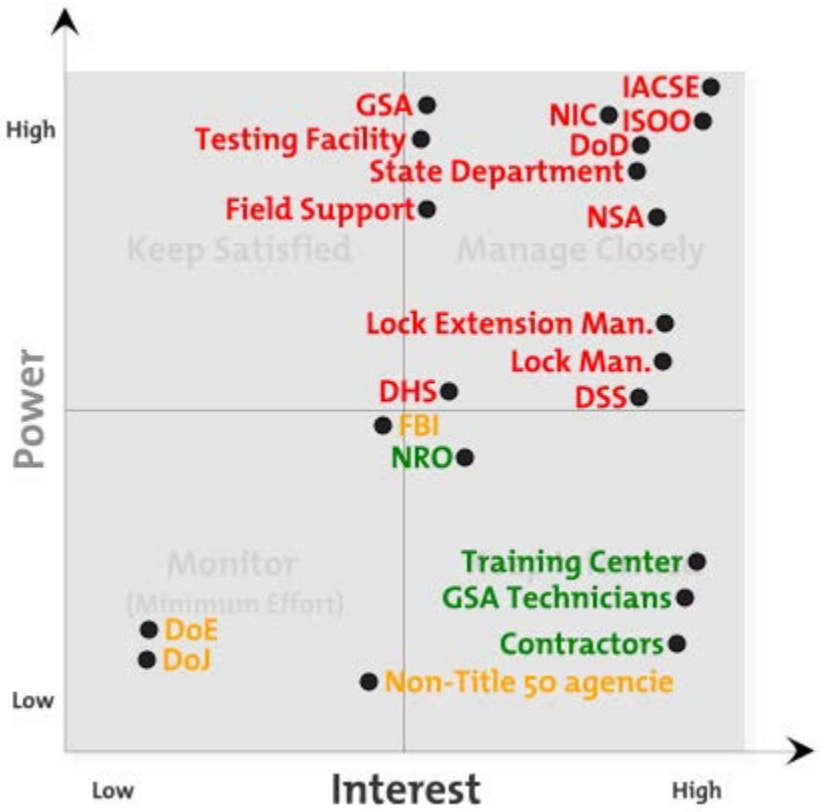

Figure 6. FF-L-2890 Stakeholder Prioritization Grid. Adapted from Thompson (n.d.).

C. COMBINATION PADLOCK

Below are the results of the FF-P-110 *Padlock, Changeable Combination (Resistant to Opening by Manipulation and Surreptitious Attack)* stakeholder analysis.

Table 12. FF-P-110 Stakeholder Analysis Results

Stakeholder	Impact	Influence	Category
End user	-	-	-
Department of Defense	High	High	Manage Closely
Department of Energy	Low	Low	Monitor
State Department	High	High	Manage Closely
Department of Justice	Low	Low	Monitor
Federal Bureau of Investigation	Medium	Medium	Monitor
National Security Agency	High	High	Manage Closely
National Reconnaissance Office	Medium	Medium	Keep Informed
Department of Homeland Security	Medium	Medium	Manage Closely
Government Contractors	High	Low	Keep Informed
Non-Title 50 Agencies	Medium	Low	Monitor
National Intelligence Community	Low	Low	Monitor
Program Support Agencies			
Information Security Oversight Office (ISOO)	High	High	Manage Closely
Defense Security Service	High	Medium	Manage Closely
Interagency Advisory Committee on Security Equipment (IACSE)	High	High	Manage Closely
General Services Administration	Medium	High	Manage Closely
DoD Lock Program Field Support	Medium	High	Manage Closely
DoD Lock Program Testing Facility	High	High	Manage Closely
GSA Certified Technicians & Inspectors	High	Low	Keep Informed
GSA Approved Training Centers	-	-	-
Lockmasters Security Institute	High	Low	Keep Informed
MBA USA, Inc.	High	Low	Keep Informed
Lock Manufacturers	-	-	-
Sargent and Greenleaf	High	Medium	Manage Closely

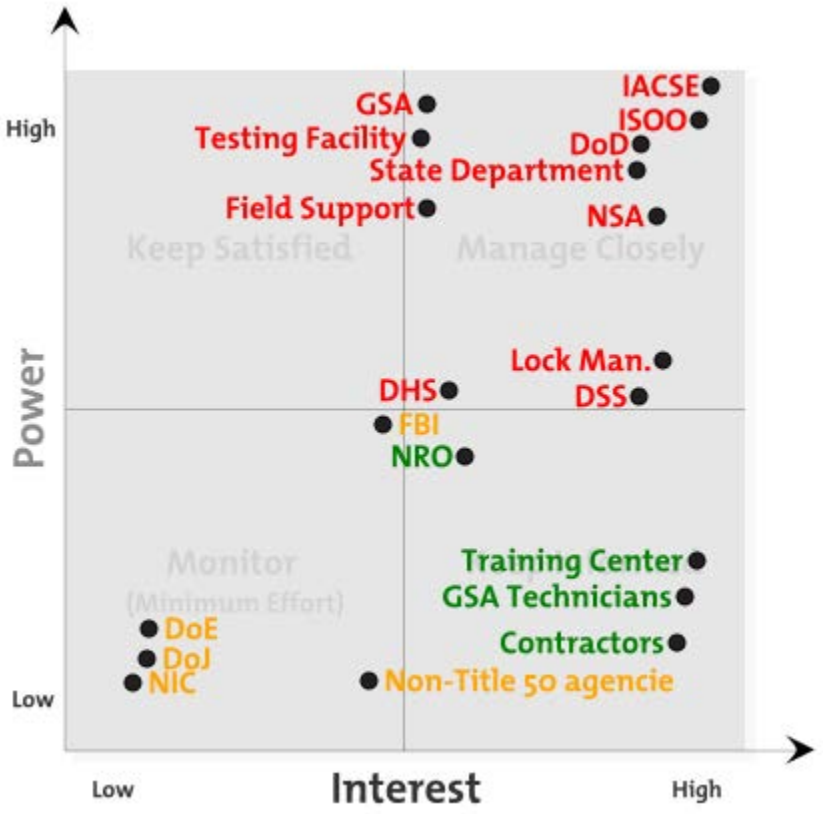

Figure 7. FF-P-110 Stakeholder Prioritization Grid. Adapted from Thompson (n.d.).

D. SECURITY CABINET

Below are the results of the AA-F-358 *Filing Cabinet, Legal and Letter Size, Uninsulated* stakeholder analysis.

Table 13. AA-F-358 Stakeholder Analysis Results

Stakeholder	Impact	Influence	Category
End user	-	-	-
Department of Defense	High	High	Manage Closely
Department of Energy	Low	Low	Monitor
State Department	High	High	Manage Closely
Department of Justice	Low	Low	Monitor
Federal Bureau of Investigation	Medium	Medium	Monitor
National Security Agency	High	High	Manage Closely
National Reconnaissance Office	Medium	Medium	Keep Informed
Department of Homeland Security	Medium	Medium	Manage Closely
Government Contractors	High	Low	Keep Informed
Non-Title 50 Agencies	Medium	Low	Monitor
National Intelligence Community	High	High	Manage Closely
Program Support Agencies	-	-	-
Information Security Oversight Office (ISOO)	High	High	Manage Closely
Defense Security Service	High	Medium	Manage Closely
Interagency Advisory Committee on Security Equipment (IACSE)	High	High	Manage Closely
General Services Administration	Medium	High	Manage Closely
DoD Lock Program Field Support	Medium	High	Manage Closely
DoD Lock Program Testing Facility	High	High	Manage Closely
GSA Certified Technicians & Inspectors	High	Low	Keep Informed
Container Manufacturers	-	-	-
Alpha Safe and Vault, Inc.	High	Medium	Manage Closely
Hamilton Products Group, Inc.	High	Medium	Manage Closely
Will-Burt Company	High	Medium	Manage Closely
A&H Security Cabinets, Inc.	High	Medium	Manage Closely
American Made Safe & Security, LLC.	High	Medium	Manage Closely
GSA Approved Training Centers	-	-	-
Lockmasters Security Institute	High	Low	Keep Informed
MBA USA, Inc.	High	Low	Keep Informed
Lock Manufacturers	-	-	-
Kaba Mas	High	Medium	Manage Closely
Sargent and Greenleaf	High	Medium	Manage Closely
Accessory Manufacturers	-	-	-
Lockmasters	Low	Low	Monitor

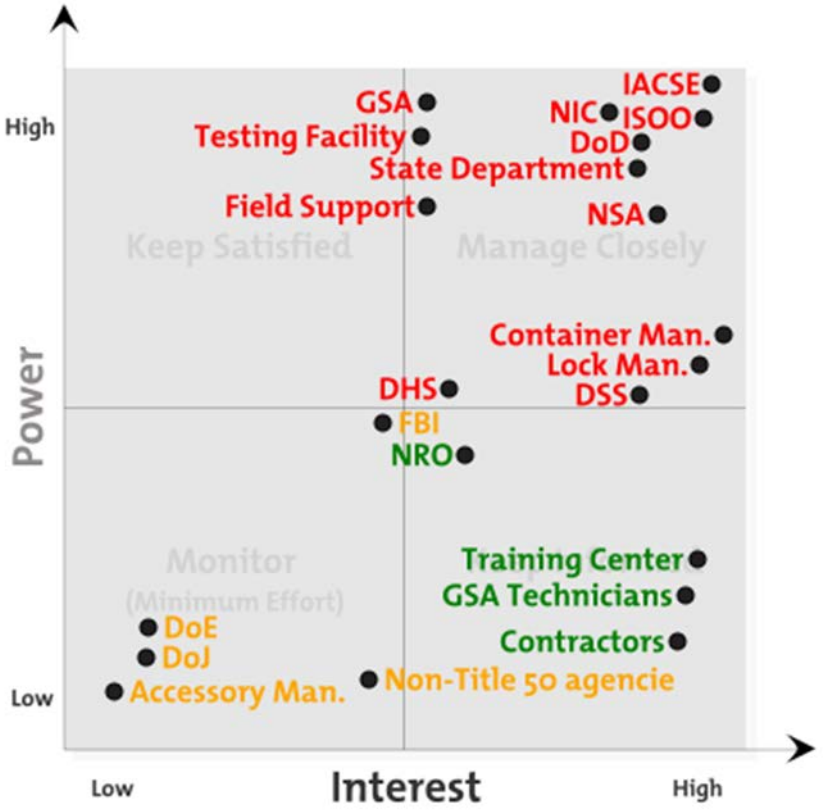

Figure 8. AA-F-358 Stakeholder Prioritization Grid. Adapted from Thompson (n.d.).

APPENDIX B. INTERVIEW QUESTIONS AND QUALITATIVE ANALYSIS RESULT

General Questions:

1) How would you characterize an effective physical security equipment specification?

2) What typically prompts the creation of a new specification?

3) What typically prompts a modification to a current specification?

4) What is the established procedure for developing physical security equipment specifications?

5) How would you improve the specification development process?

6) What data could be utilized to determine specification effectiveness?

7) How could improvements to a specification be measured?

Specification Specific Questions:

8) To what extent does (FF-L-2740, FF-L-2890, FF-P-110, AA-F-358) currently satisfy end user needs? Score from 1 to 5.

   1 being does not satisfy, 5 being fully satisfies.

   Why is the highest-ranked that way?

   Why is the lowest-ranked that way?

9) To what extent does (FF-L-2740, FF-L-2890, FF-P-110, AA-F-358) specification provide adequate detail? Score from 1 to 5.

   1 being inadequate amount, 5 being the optimal amount.

   Why is the highest-ranked that way?

Why is the lowest-ranked that way?

10) To what extent has (FF-L-2740, FF-L-2890, FF-P-110, AA-F-358) produced an adequate product? Score from 1 to 5.

1 being inadequate products, 5 being an optimal product.

Why is the highest-ranked that way?

Why is the lowest-ranked that way?

11) To what extent does (FF-L-2740, FF-L-2890, FF-P-110, AA-F-358) require any immediate improvements? Score from 1 to 5.

1 being requires little to no improvements, 5 being requires immediate improvements.

Why is the highest-ranked that way?

Why is the lowest-ranked that way?

Table 14. Qualitative Data Analysis Code Frequency Output. Adapted from Provalis Research (n.d.)

Category	Code	Description	Count	Cases
Evaluation	Clarity	The specification requirements must be clear.	15	5
Evaluation	Changing Needs	Evolving needs from the field must be continuously evaluated.	13	4
Evaluation	Need Met	It is determined essential for the specification to meet the end user need effectively.	10	4
Development	Sustained Development	Modifications are natural through sustained development, which has resulted in viable products.	8	4
Development	New Need	A new need provided by the field prompts the creation and modification of a specification.	6	5
Deficiencies	NSA Lock Need	NSA requires a new padlock that has not been formally communicated. The requirements are not detailed.	6	3
Improvements	Classified Testing	Add a classified testing plan as a supplemental to each specification.	6	2

Category	Code	Description	Count	Cases
Improvements	Need Analysis	Implementation of a needs analysis would improve specification development.	5	4
Development	Technique Change	Change in testing or attack techniques can prompt specification modification.	5	4
Evaluation	Data Query from End users	End user input from the DoD Lock Program hotline can be used to measure effectiveness.	5	3
Development	Policy	Policy changes or new policy prompts the creation or modification of specifications.	5	3
Development	IACSE Review	IACSE is responsible for the review of the need, determines the validity, and prompts modification or creation of specification.	5	3
Deficiencies	White Paper	Agencies verbally communicate need instead of submitting a formal white paper.	5	2
Deficiencies	Unclear Testing Requirements	Some performance or design requirements are unclear in current specifications.	4	2
Deficiencies	Lack of Manufacturers	Lack of manufacturers submitting to specifications, which results in a lack of product options.	3	3
Deficiencies	Newer Specification	New specifications undergo natural iterations due to a lack of exposure to the field.	3	3
Development	Federal Standardization Manual	Federal Standardization Manual utilized for the structure for specification development.	3	2
Evaluation	Number of Product Used/Sold	The number of products sold can determine the effectiveness of a specification.	3	2
Development	Events	An event prompts the development of the specification.	3	2
Deficiencies	Needs Statement	Need end users do not supply a statement.	3	2
Deficiencies	Too Restrictive	Requirements may be too detailed, restricting the possibility of viable designs.	3	2
Development	Unknown Procedure	A formal procedure for specification development is unknown.	2	2
Deficiencies	Unclear Design or Performance Requirements	Some performance or design requirements are not clear in current specifications.	2	2

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C. FUNCTIONAL ANALYSIS HIERARCHY DIAGRAMS

A. ELECTROMECHANICAL COMBINATION LOCK

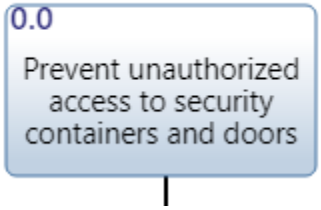

Figure 9. FF-L-2740 Prime Function

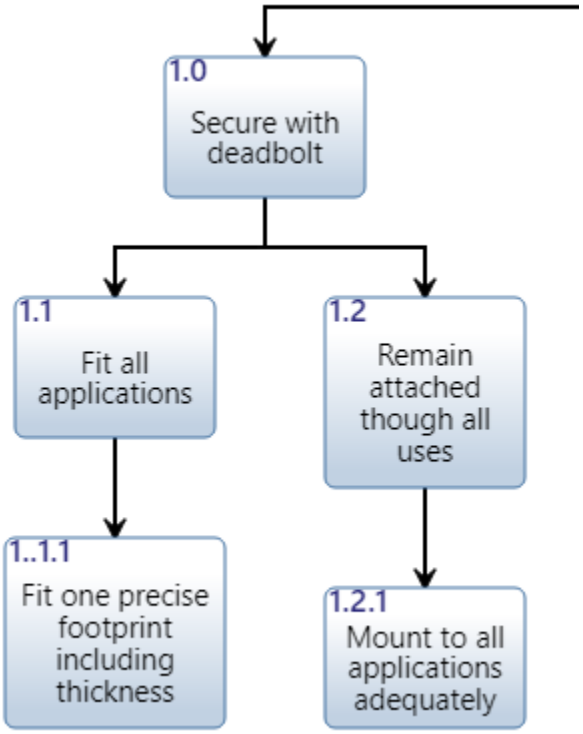

Figure 10. FF-L-2740 1.0 Function Diagram

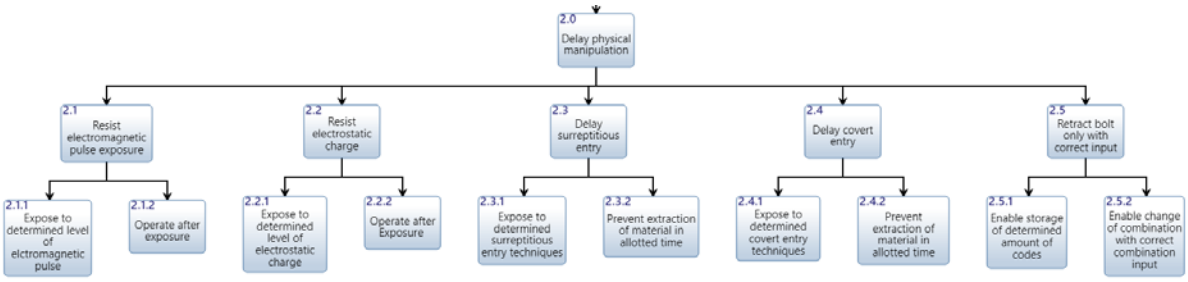

Figure 11. FF-L-2740 2.0 Function Diagram

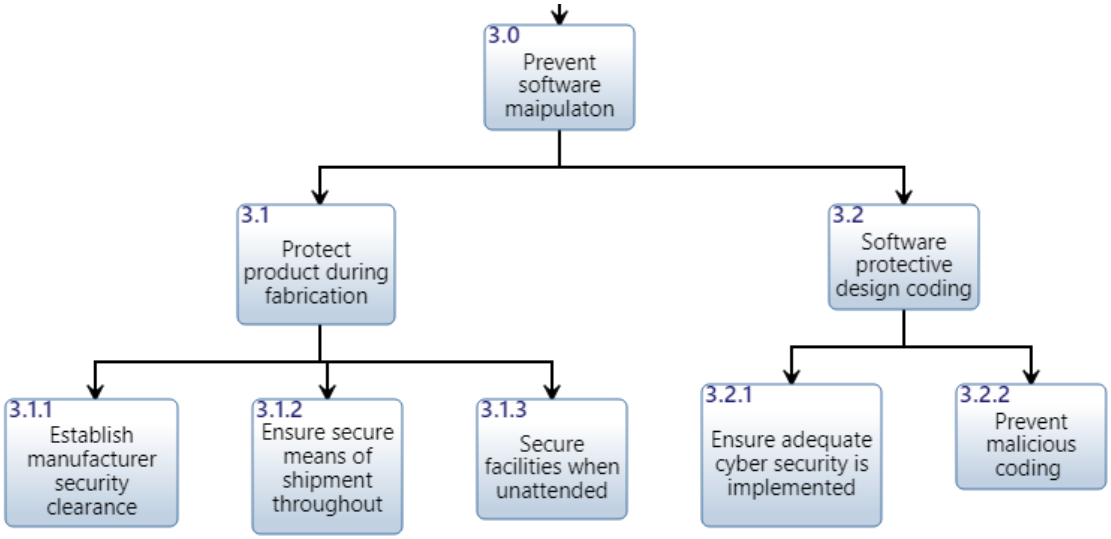

Figure 12. FF-L-2740 3.0 Function Diagram

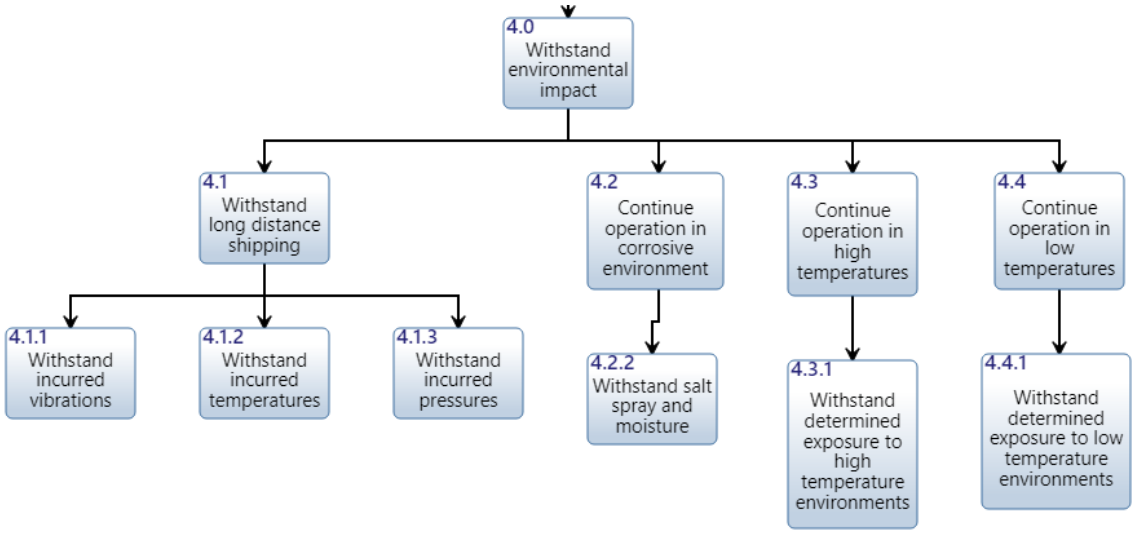

Figure 13. FF-L-2740 4.0 Function Diagram

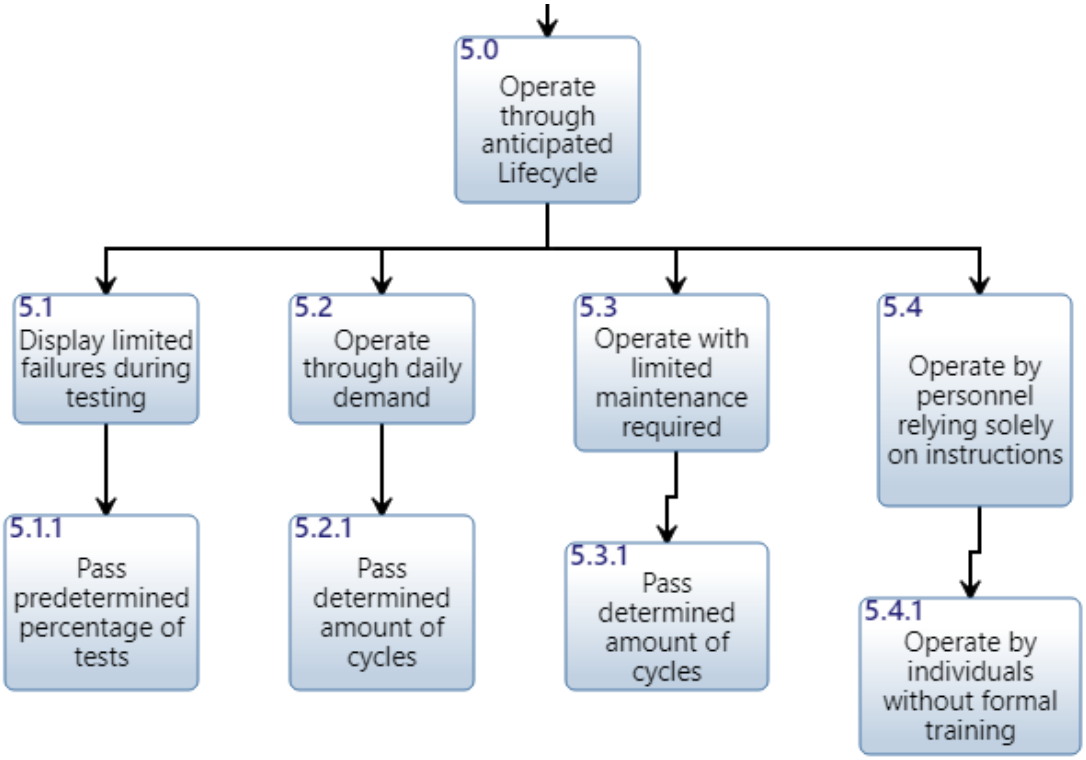

Figure 14. FF-L-2740 5.0 Function Diagram

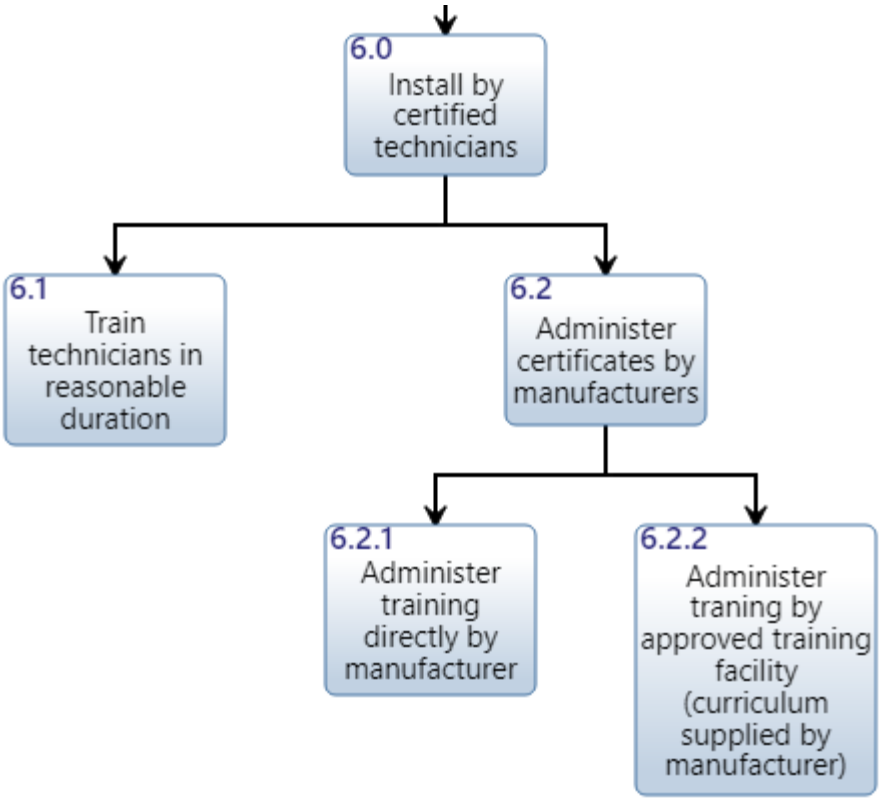

Figure 15. FF-L-2740 6.0 Function Diagram

B. PEDESTRIAN DOOR ASSEMBLY

Figure 16. FF-L-2890 Prime Function

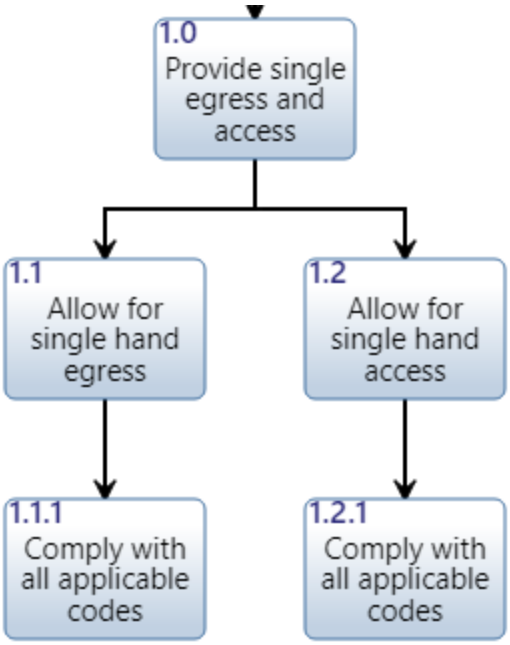

Figure 17. FF-L-2890 1.0 Function Diagram

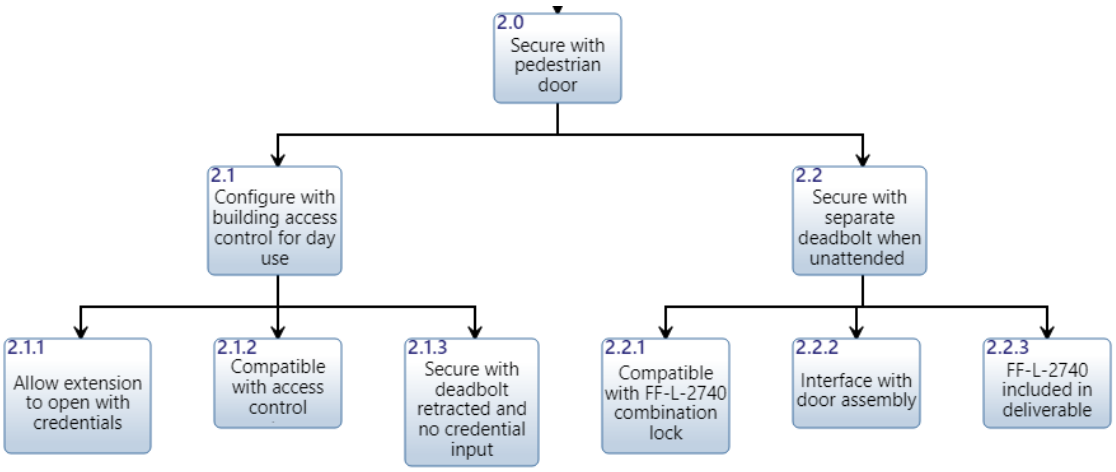

Figure 18. FF-L-2890 2.0 Function Diagram

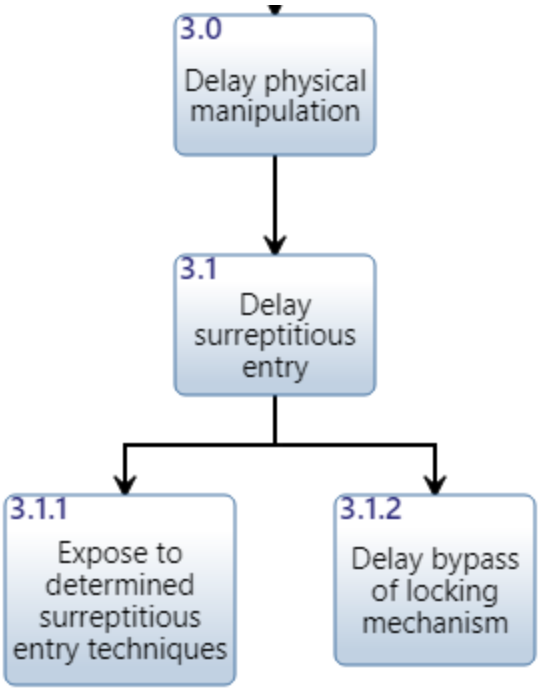

Figure 19. FF-L-2890 3.0 Function Diagram

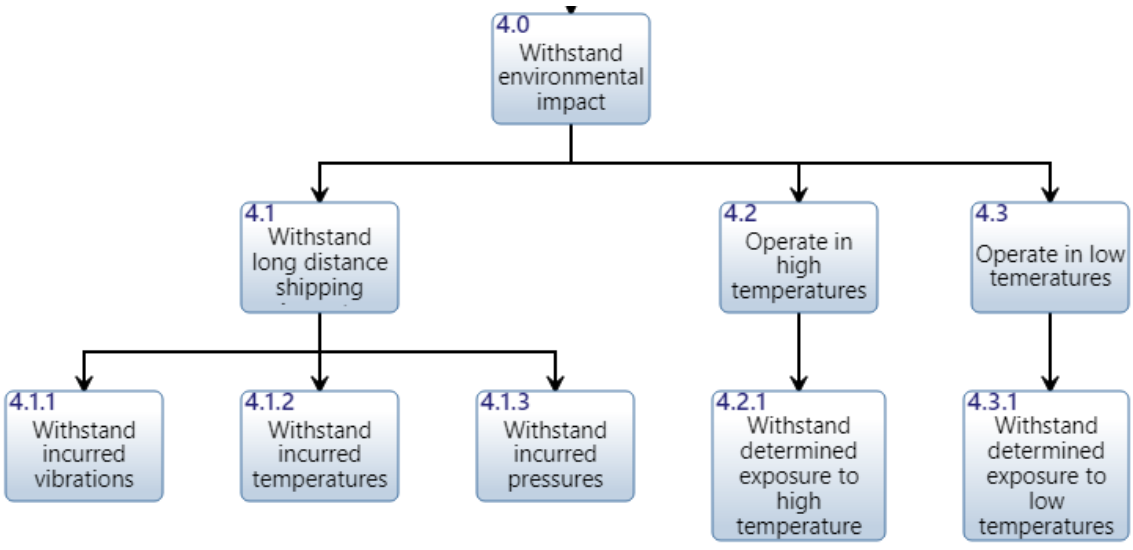

Figure 20. FF-L-2890 4.0 Function Diagram

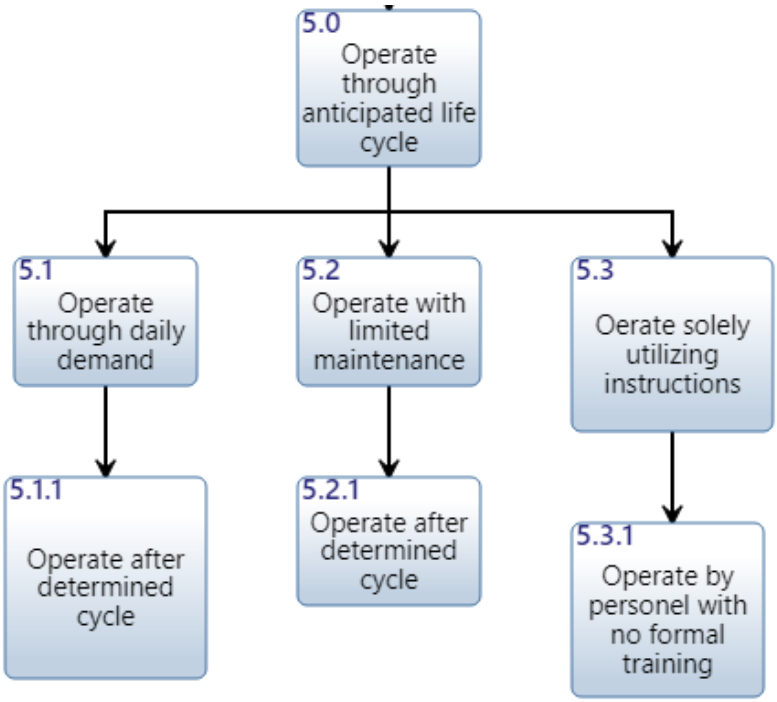

Figure 21. FF-L-2890 5.0 Function Diagram

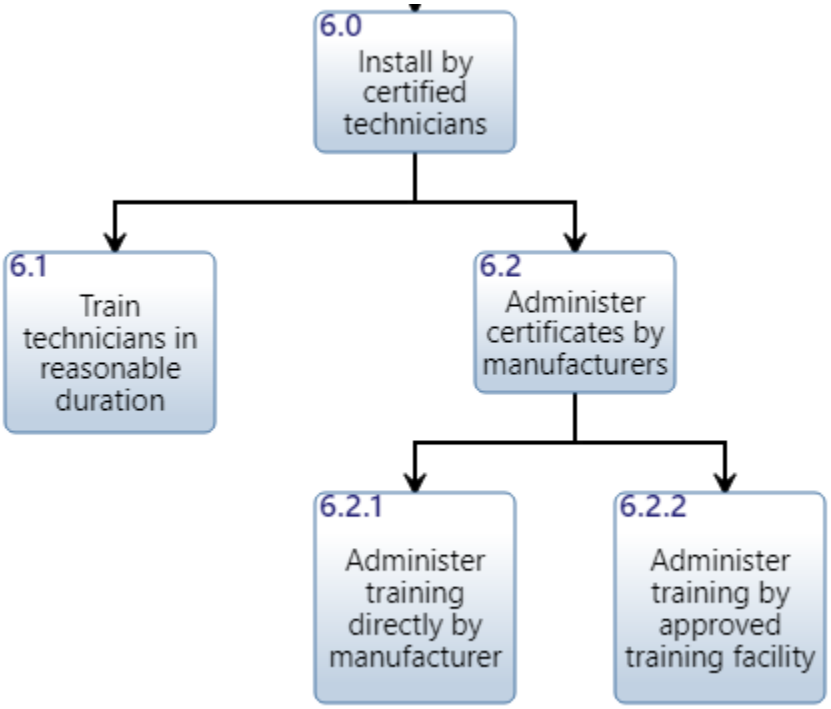

Figure 22. FF-L-2890 6.0 Function Diagram

C. COMBINATION PADLOCK

Figure 23. FF-P-110 Prime Function

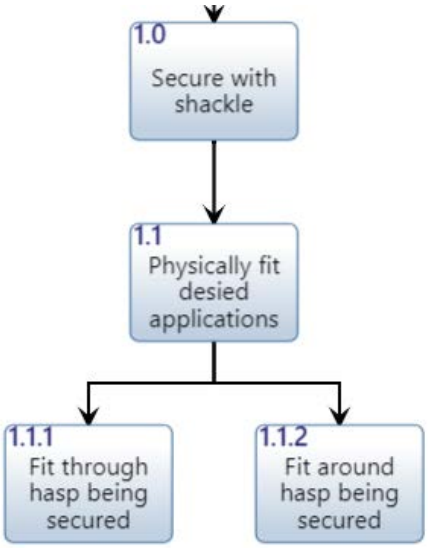

Figure 24. FF-P-110 1.0 Function Diagram

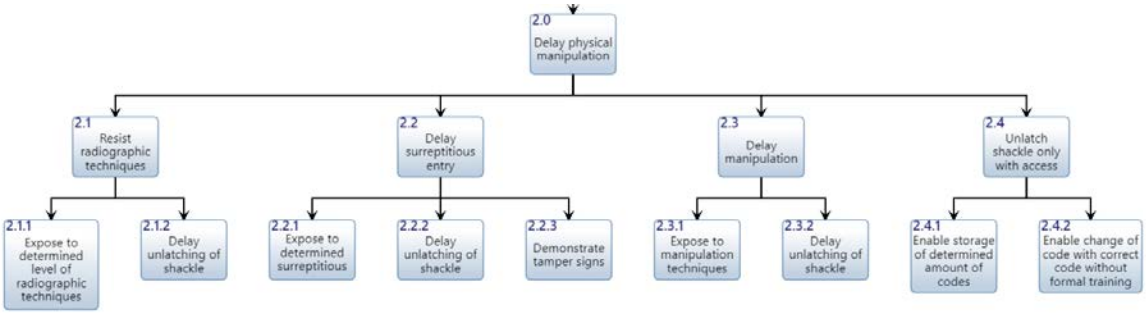

Figure 25. FF-P-110 2.0 Function Diagram

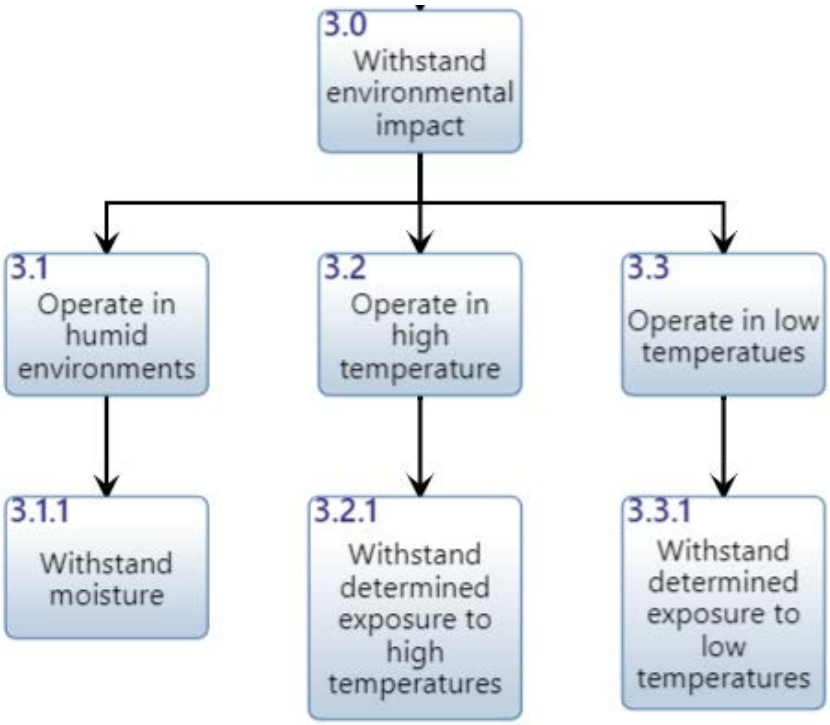

Figure 26. FF-P-110 3.0 Function Diagram

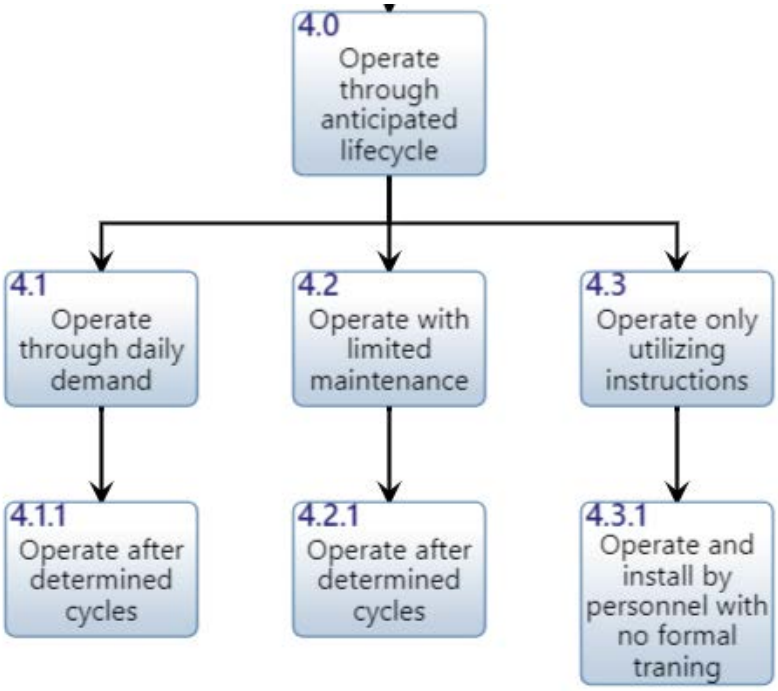

Figure 27. FF-P-110 4.0 Function Diagram

D. SECURITY CABINET

Figure 28. AA-F-358 Prime Function

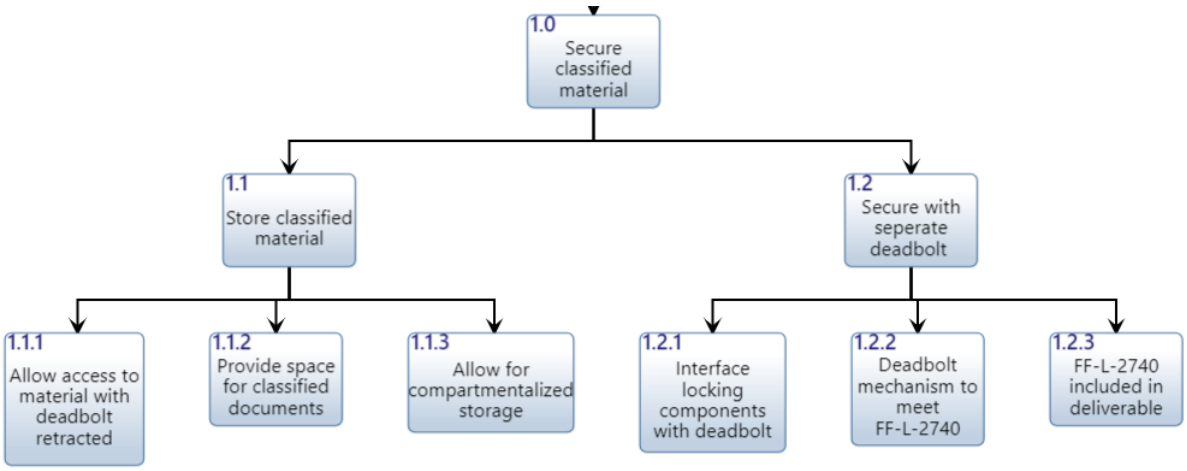

Figure 29. AA-F-358 1.0 Function Diagram

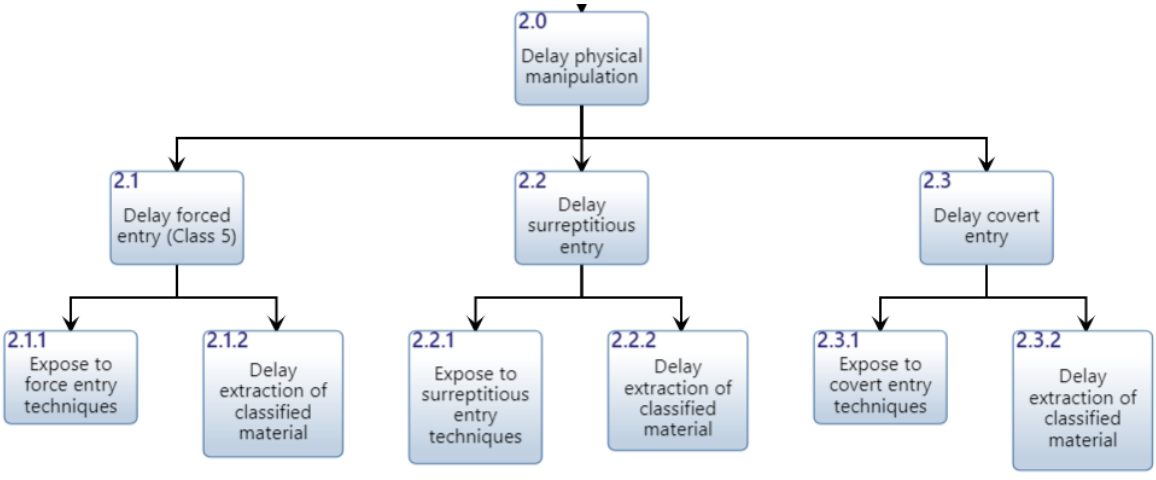

Figure 30. AA-F-358 2.0 Function Diagram

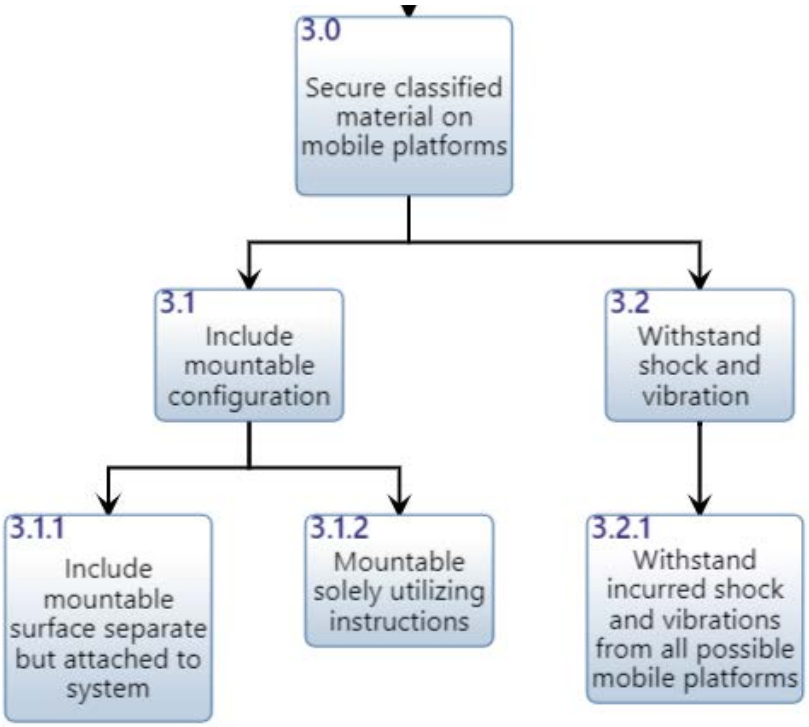

Figure 31. AA-F-358 3.0 Function Diagram

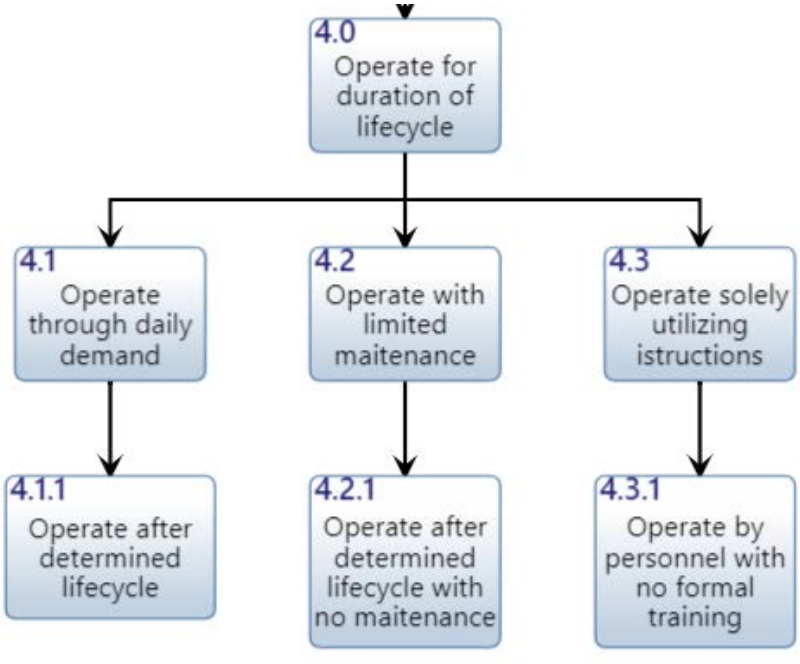

Figure 32. AA-F-358 4.0 Function Diagram

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Blanchard, Benjamin, and John Blyler. 2016. *System Engineering Management*, 5th Edition. Hoboken, NJ: John Wiley & Sons, Inc.

Blanchard, Benjamin, and Wolter Fabrycky. 2011. *System Engineering and Analysis*, 5th Edition. Upper Saddle River, NJ: Prentice Hall International Series in Industrial & Systems Engineering.

Flicker, Sarah. 2014. "Stakeholder Analysis." *The SAGE Encyclopedia of Action Research*, edited by David Coghlan. Thousand Oaks, CA: SAGE. http://dx.doi.org/10.4135/9781446294406.

General Services Administration. 1954. *Filing Cabinet, Steel, Legal and Letter Size, Insulated, Security*. Federal Specification AA-F-357, Cancelled. Washington, DC: General Services Administration.

———. 1997. *Padlock, Changeable Combination (Resistant to Opening by Manipulation and Surreptitious Attack)*. Federal Specification FF-P-110J. Washington, DC: General Services Administration.

———. 2010. *Filing Cabinet, Legal and Letter Size, Uninsulated*. Federal Specification FF-L-358J. Washington, DC: General Services Administration.

———. 2011. *Locks, Combination, Electromechanical*. Federal Specification FF-L-2740B. Washington, DC: General Services Administration.

———. 2019. *Lock Extension (Pedestrians Door Lock Assembly Preassembled, Panic, and Auxiliary Deadbolt)*. Federal Specification FF-L-2890C. Washington, DC: General Services Administration.

Information Security Oversight Office. 2014. *Procurement of Security Equipment*. ISOO Notice 2014-02. Washington, DC: Information Security Oversight Office.

Provalis Research. n.d. QDA Miner Lite. Montreal, QC. Accessed August 10, 2019. https://provalisresearch.com/products/qualitative-data-analysis-software/freeware/

Sadraey, Mohammad. 2013. *Aircraft Design: A Systems Engineering Approach*. West Sussex, UK: John Wiley & Sons, Ltd.

The White House. 1953. *Safeguarding Official Information in the Interest of the Defense of the United States*. Washington, D.C: The White House.

Thompson, Rachel. n.d. "Stakeholder Analysis: Winning Support for Your Projects." Mind Tools. Accessed August 20, 2019. https://www.mindtools.com/pages/article/newPPM_07.htm.

Under Secretary of Defense (Intelligence). 2013. *DoD Information Security Program: Protection of Classified Information*. DoD-Manual 5200.01 Volume 3. Washington, D.C.: Department of Defense.

Wasson, Charles. 2005. *System Analysis, Design and Development*. Hoboken, NJ: John Wiley & Sons, Inc. https://doi.org/10.1002/0471728241.ch31.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California