NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

CYBER-DEFENSE RETURN ON INVESTMENT FOR NAVFAC ENERGY TECHNOLOGIES

by

Brian J. Adams
Cameron C. Hartner

December 2017

Thesis Advisor: Eva Regnier
Co-Advisor: Bryan Hudgens

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** December 2017	**3. REPORT TYPE AND DATES COVERED** Master's thesis	
4. TITLE AND SUBTITLE CYBER-DEFENSE RETURN ON INVESTMENT FOR NAVFAC ENERGY TECHNOLOGIES		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Brian J. Adams and Cameron C. Hartner			
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. IRB number NPS.2017.0070-IR-EM2-A			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.		**12b. DISTRIBUTION CODE**	

13. ABSTRACT (maximum 200 words)

This study was conducted in support of a Department of Defense (DOD) effort to improve cyber-security in relation to DOD installation control systems. Space and Naval Warfare Systems Command (SPAWAR) is developing programs to assist decision-making for the selection of cyber-security products for U.S. naval installations and infrastructure. We interviewed a sample of Naval Facilities Engineering Command employees utilizing the Value-Focused Thinking technique developed by Dr. Ralph Keeney in the 1990s. The interviews revealed various means objectives and fundamental objectives that we compiled into a network. The network organizes values into means and fundamental objectives and also helps to clarify terminology often used within cyber-security communities. Our goal is for, through organization and the clarification of terms, this study to serve as an initial step to the identification of objective performance measurements, which can inform the decision making-process.

14. SUBJECT TERMS return on investment, ROI, value-focused thinking, VFT, cyber, Space and Naval Warfare Systems Command, SPAWAR, energy, microgrid, control systems, Supervisory Control and Data Acquisition, SCADA, energy resilience, energy security			**15. NUMBER OF PAGES** 61
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** 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.

CYBER-DEFENSE RETURN ON INVESTMENT FOR NAVFAC ENERGY TECHNOLOGIES

Brian J. Adams
Captain, United States Marine Corps
B.A., University of California, Los Angeles, 2011

Cameron C. Hartner
Captain, United States Marine Corps
B.A., University of Texas at Dallas, 2010

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF BUSINESS ADMINISTRATION

from the

NAVAL POSTGRADUATE SCHOOL
December 2017

Approved by: Eva Regnier
Thesis Advisor

Bryan Hudgens
Co-Advisor

Donald Summers
Academic Associate
Graduate School of Business and Public Policy

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This study was conducted in support of a Department of Defense (DOD) effort to improve cyber-security in relation to DOD installation control systems. Space and Naval Warfare Systems Command (SPAWAR) is developing programs to assist decision-making for the selection of cyber-security products for U.S. naval installations and infrastructure. We interviewed a sample of Naval Facilities Engineering Command employees utilizing the Value-Focused Thinking technique developed by Dr. Ralph Keeney in the 1990s. The interviews revealed various means objectives and fundamental objectives that we compiled into a network. The network organizes values into means and fundamental objectives and also helps to clarify terminology often used within cyber-security communities. Our goal is for, through organization and the clarification of terms, this study to serve as an initial step to the identification of objective performance measurements, which can inform the decision making-process.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

C-SEC	Cyber-SCADA Evaluation Capability
CS	Control System
DOD	Department of Defense
DOE	Department of Energy
DON	Department of the Navy
EPA	Environmental Protection Agency
ESTEP	Energy Systems Technology and Evaluation Program
GMI	Grid Modernization Initiative
IRB	Institutional Review Board
JBPHH	Joint Base Pearl Harbor-Hickam
MODA	Multi-objective Decision Analysis
NAVFAC	Naval Facilities and Engineering Command
NBSD	Naval Base San Diego
NPS	Naval Postgraduate School
ONR	Office of Naval Research
ReCIst	Resilient Critical Infrastructures through Secure and Efficient Microgrids
ROI	Return on Investment
SCADA	Supervisory Control and Data Acquisition
SPAWAR	Space and Naval Warfare Systems Command
SSC Pacific	SPAWAR System Center Pacific
VFT	Value-Focused Thinking

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

We would like to thank our advisors, Dr. Eva Regnier and Mr. Bryan Hudgens, for their committed guidance and direction. Thank you to Mr. Jose Romero-Mariona, Mrs. Maxine Major, Mrs. Megan Kline, and the rest of the ReCIst team at SPAWAR for assisting in our efforts. Thank you to NPS Institutional Review Board and Mrs. Rikki Nguyen for making the human subject research approval process expeditious. Thank you to everyone within the NPS Graduate School of Business and Public Policy who contributed hours to edit and transcribe in support of this project. Finally, we would like to offer a special thank-you to all who participated as subjects for sharing your time, partaking in the methodical questions, and putting up with our post-it notes. The data that you provided was paramount to our research and analysis. Cheers!

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROJECT CONTEXT

Top naval commanders have acknowledged the need to increase cybersecurity for their control system networks and to reduce vulnerabilities to cyber threats in the future (Lyngaas, 2016). Space and Naval Warfare Systems (SPAWAR) Center Pacific's Resilient Critical Infrastructures through Secure and Efficient Microgrids (ReCIst) project is developing a tool to help Naval Facility and Engineering Command (NAVFAC) energy management teams measure the return on investment (ROI) of cybersecurity investments to protect their energy control systems (Lyngaas, 2016; Romero-Mariona, 2016). ReCIst is leading an effort to help NAVFAC energy management teams make the best cybersecurity decision for their installation's infrastructure (Romero-Mariona, 2016), defined as adding the most value to the stakeholders. This thesis is designed to aid the ReCIst team in the development of their return-on-investment (ROI) tool by determining and defining what impacts of cybersecurity investments are important to stakeholders and therefore should be included in the ROI measure.

B. WHAT IS THE PROBLEM AND WHOM DOES IT AFFECT?

The Department of Defense (DOD) is taking steps to make its energy systems more efficient and resilient by investing in and developing microgrids (Broekhoven, Judson, Galvin, & Marqusee, 2013; Nekoui, 2014) and other control systems at its installations. A microgrid is a stand-alone network that "can be islanded from the local utility grid and function in stand-alone mode" (Broekhoven et al., 2013, p.41). A microgrid has the ability to supply power to consumers independent of the commercial grid, sometimes with the use of alternative sources of energy such as solar and other fuels (Broekhoven et al., 2013). Microgrids have the potential to secure the energy supply in times of natural disaster or commercial power outages (Lantero, 2014; Ortiz, 2015). Microgrids require a network of computerized control systems (CS) in order to function and allow energy managers to monitor activity (Broekhoven et al., 2013). Control systems are networks of computer software and hardware used to control and monitor infrastructure functions such as

electrical voltage from the commercial grid to the microgrids, sewage, and building functions such as air conditioning (Nekoui, 2014).

The network of control systems raises concerns over the vulnerability to cyber threats (Broekhoven et al., 2013). The ReCIst team states, control systems and their "microgrids can increase the potential cyberattack surface by offering new entry points that could be used to target larger Smart Grids and ultimately compromise critical infrastructures" (Romero-Mariona, 2016, p.3). Previous research has provided numerous examples where hackers infiltrated control system networks, disrupted energy capabilities, and stole data (Adametz, Groesbeck, & Quibilan, 2016). A recent example is the compromise of customer credit card information from the retail company Target in 2014 (Adametz et al., 2016). Recently, Equifax and nearly half of the U.S. population fell victim to a cyberattack through a weakness in an online support tool. Also, in October 2017, a U.S. cybersecurity company reported "hackers linked to North Korea recently targeted U.S. electric power companies with spearphishing emails" (Mitchell & Dilanian, 2017). There is a considerable cybersecurity threat that will not fade or retreat on its own (Wattles & Larson, 2017).

The Navy has taken steps to invest resources to research, develop, and purchase cybersecurity products across all naval functions (Keller, 2017). Investing implies stakeholders will receive some sort of measurable return on their asset in the future, but it is very difficult to precisely measure that return or guarantee 100% security for connected networks (Hubbard & Seiersen, 2016).

The ReCIst team and this thesis project attempt to tackle this challenge and bridge the gap between business measures and operational considerations for Navy installation energy systems (Romero-Mariona, 2016; Romero-Mariona et al., 2017). This thesis project seeks to inject stakeholder input into the SPAWAR ReCIst ROI tool. Stakeholder input is important to properly develop a tool that reflects the legitimate concerns of those who routinely design, operate, and use control systems. NAVFAC energy management teams will ultimately use the ROI tool to make decisions on cybersecurity investments for these systems. The users of the tool will input information about their specific control system

and select information on cybersecurity products they would like to add, and the tool will measure the ROI for that product.

C. PROJECT GOALS

This project's purpose is to assist the SPAWAR ReCIst team with developing the ROI tool by collecting important end user inputs. While the SPAWAR ReCIst team has developed the capability for the model to represent an end user's system, one of the important remaining issues is how to measure ROI as a function of the performance of the system. Our goals, based on the SPAWAR ReCIst team's needs, are as follows:

- Identify and clearly define stakeholder values for control system cybersecurity.
- Produce understandable and usable information for the ReCIst team.

D. PROJECT SCOPE AND APPROACH

1. Scope

This project focuses on the eventual end users of the ReCIst ROI tool—engineers and managers in various roles at Naval Facilities and Engineering Command (NAVFAC)-run installations. While the tool may be useful to a broader set of end users, NAVFAC engineers and managers are the target audience, and are the focus of the development effort. NAVFAC engineers' and managers' decisions affect a much broader group of stakeholders. The stakeholders are also their customers and the NAVFAC end users have internalized stakeholders' values with respect to NAVFAC industrial systems, which our results confirm.

2. Approach

The methodology is based on value-focused thinking (VFT), which uses stakeholder values to support the best possible decisions in many contexts (Keeney, 1996). Stakeholder values were identified in qualitative interviews. The interviews were conducted with potential end users of the tool such as energy managers and subject matter experts. The data is synthesized into a means-ends objective network (Keeney, 1996)

which offers a perspective on the values and trade-offs that should be captured in the ReCIst ROI tool, how characteristics of cybersecurity products contribute value, as well as specific objectives that the ReCIST team can seek to measure.

E. SUMMARY

Cyberattacks are a concern to the U.S. Navy energy infrastructure because it has the potential to inhibit successful military missions and operations. The Navy is striving to protect their infrastructure by investing in cybersecurity, but measuring the financial return on those investments is difficult. The SPAWAR ReCIst team is attempting to make quantifying cybersecurity ROI easier by developing a tool for NAVFAC energy management teams. Our project's objectives are to support the SPAWAR ReCIst team by determining stakeholder values and mapping them to measurable impacts. In Chapter II, we discuss background information on naval micogrids, control system networks, cyber threats, and ROI. In Chapter III, we discuss the methodology behind VFT and our research. In Chapter IV, the results of the VFT-interviews are revealed in the form of means and fundamental objectives. We provide the analysis of what the results mean for our project in Chapter V, and in Chapter VI, we provide project conclusions.

II. BACKGROUND

Starting with the rising connectivity of automated systems and the corresponding prevalence of cyber threats, and response at multiple levels of the U.S. federal government, this chapter illustrates the purpose of the ReCIST ROI tool. In addition, it describes the research approach and the reasons for choosing it in this context.

A. WHAT ARE MICROGRIDS AND CONTROL SYSTEM NETWORKS?

The world, including the DOD, increasingly relies on automated systems that are linked to intranet and Internet devices. In 2001, the number of devices connected to the Internet was around 400 million (Department of Energy [DOE], 2017c). Less than 15 years later, that number was estimated to have grown to 25 billion in 2015 (DOE, 2017c). Control systems (CSs) are quickly modernizing as part of this trend. While there are many reasons for this trend, the efficient and reliable functioning of energy systems is a key contributor. The Department of Energy (DOE) is seeking to improve the resiliency, reliability, security, affordability, flexibility, and sustainability of the United States' electrical grid through the Grid Modernization Initiative (DOE, 2017a). A major element of GMI is the implementation of Smart Grids, which drastically increase a power grid's reliability, resiliency, and efficiency (DOE, 2017b). Supervisory Control and Data Acquisition (SCADA), also known as control systems, are critical for the smart grid implementation.

Modern control systems are used across industrial organizations to transmit real time data and controls, which assist an organization's ability to respond efficiently (Inductive Automation, 2017). Advances in control systems have changed reactive monitoring to proactively identifying developing situations and solving problems before they inhibit operations or safety (Clouser, 2013). Control room operators are no longer just monitoring, they now have the ability to control industrial machinery through dispatching based on need rather than arbitrary schedules (Clouser, 2013). The ability to proactively solve issues and make decisions in order to prevent problems adds to the overall efficiency of an organization through its efficient use of manpower (Clouser, 2013). Ultimately,

modern control systems allow fewer people to control more assets and do so more efficiently (Clouser, 2013).

Microgrids are local power grid systems that can operate with autonomy by unplugging from commercial grid systems (Lantero, 2014). Although many microgrids operate concurrently with the commercial grids, the capability of the system to function independently is beneficial because it can provide power during times when the commercial grid is unable to provide power (Lantero, 2014). This benefit was demonstrated in 2012 during Hurricane Sandy (John, 2012). While entire commercial grids were shut down, pockets of installations maintained their own power (John, 2012). Although the key aspect is the ability to operate independently, microgrids provide much more than just backup power. Another important aspect of microgrids is in the efficient use of power and the translation into cost savings (Lantero, 2014). A microgrid's use of alternative fuels lessens the reliance on a commercial grid's power distribution (Lantero, 2014).

B. WHAT IS THE NATURE OF THE CYBER THREAT?

Cyber threats have risen alongside the rise of the online systems and the reliance on control systems. Cyberattacks are becoming more sophisticated, militarized, and targeted. The number of data breaches in the first six months of 2017 has increased by 164% compared to all of 2016 (Graham, 2017).

Interoperability between control systems is increasing and therefore the possibilities for cyberattacks expand (Idaho National Laboratory, 2016). Russia, Iran, and China, along with non-state actors such as hacker groups and terrorist organizations, are continuing to seek methods to disrupt the U.S. energy grid through cyberattacks (Idaho National Laboratory, 2016). The utilities responsible for implementing security measures often lack a full-spectrum perspective of their cyber vulnerabilities (Idaho National Laboratory, 2016). North Korea is also becoming a more serious cybersecurity threat. As recently as October 10, 2017, FireEye, a private cybersecurity company, reported that North Korea had launched phishing emails in an attempted breach of U.S. electrical companies.

Based on its assessment of vulnerabilities in the energy grid infrastructure, the DOE judges that Russia and China pose the greatest threat with regards to capability and intent of cyberattack (Idaho National Laboratory, 2016). In 2009, Russia and China were involved in the infiltration and attempted mapping of the U.S. energy grid, and even went as far as to leave behind malicious programs aimed to disrupt power distribution (Gorman, 2009). In 2015, Ukraine was hit by a cyberattack that completely shut off the power for 250,000 citizens and left the power systems to be operated manually for months. The coordinated attack is largely suspected to have been conducted or financed by the Russian government and is believed to be a precursor to future attacks on the U.S. electrical infrastructure (Zetter, 2016).

C. WHAT IS THE DEPARTMENT OF THE NAVY'S CONCERN?

The importance of uninterrupted electrical power cannot be understated. The U.S. government, economy, and citizens rely on electrical power in every facet of life. Commerce, transportation, health and emergency services, communications, and national defense are dependent on reliable uninterrupted power (Center for Naval Analysis Military Advisory Board, 2015). Even short outages can be detrimental to the nation or region affected. In 2012, Superstorm Sandy caused widespread outages across the northeastern United States. The communication systems used by emergency services were dependent on commercial power and when the back-up generators stopped providing power, the ability of recovery crews to respond diminished (Center for Naval Analysis Military Advisory Board, 2015).

The DOD is the largest electrical consumer in the United States and an estimated 91% of the DOD's critical infrastructure is reliant on the commercial grid (DOE, 2017c). In 2013, the Department of the Navy (DON), via the Office of Naval Research (ONR), established the Energy Systems Technology and Evaluation Program (ESTEP). The goal of ESTEP is to "focus on energy technologies that reduce costs, increase energy security, and ultimately increase the reach and persistence of the warfighter" (DON, 2015). ESTEP implements its research goals through the Naval Postgraduate School (NPS), Naval Facilities Engineering Command (NAVFAC), Space and Naval Warfare Systems

Command (SPAWAR), and other organizations (Asia-Pacific Technology and Education Partnership, 2017). According to the APTEP website, ESTEP funds research for educational purposes though NPS; installation construction, operations, and maintenance purposes though NAVFAC; and energy network operations and security purposes though SPAWAR (Asia-Pacific Technology and Education Partnership, 2017).

D. WHAT IS THE ReCIst ROI TOOL?

SPAWAR Systems Center Pacific's (SSC Pacific) Resilient Critical Infrastructures through Secure and Efficient Microgrids (ReCIst) project is part of ESTEP. The ReCIst team is developing a return-on-investment (ROI) tool to assist decision-making on what cybersecurity measures fit particular installation circumstances. It will build on the team's earlier work, specifically, the Cyber-SCADA Evaluation Capability (C-SEC; Nekoui, 2014). C-SEC is a program under SPAWAR that focuses on energy system security with the goal of improving the overall protection of control systems (Nekoui, 2014). The ROI model will eventually be implemented as a third part of the ReCIst program. According to team members at SPAWAR, the ReCIst program will be comprised of three sections. These will include the ROI tool, a derivative of the C-SEC program that measures the functionality of cybersecurity products, and the energy efficiency of the control system. Like traditional ROI tools, the objective is to analyze the costs and benefits of an investment, and provide capability for evaluating and comparing multiple investment options (Investopedia, 2003). Using the system model in the C-SEC, the ROI tool is intended to evaluate the performance of the system with the addition of a cybersecurity project under consideration. The ReCIst team aims to capture—and quantify—the cost savings provided by security measures due to cyberattack identification and prevention. The tool will utilize inputs that consider the cost of potential cyberattacks and the cost of implementing a particular security product or measure. According to the team, the tool will provide a quantifiable monetary analysis that will better assist in the decisions over which security measures to implement.

E. WHO ARE THE STAKEHOLDERS?

The potential users for the ROI tool are those who would utilize it in order to make decisions on the security of their NAVFAC installation. Specifically, primary stakeholders are energy installation managers, control system engineers, utilities managers, and others who have direct involvement or responsibility to the security of the networks.

The group of stakeholders is much broader. The potential damage caused by cyberattacks on military installations' electrical power would negatively affect the DOD's ability to carry out its mission, thus anyone involved in that mission or depending on that mission is a stakeholder. One of the key goals within the mission of the DOD is to "protect the security of our country" (DOD, 2017). Any degradation of that protection would negatively affect the citizens and other residents.

F. WHAT IS A RETURN ON INVESTMENT?

ROI tools are commonly used in financial decisions to evaluate the forecasted impact of different investments. The ROI metric can be applied to anything that has a cost with the potential to produce gains (Calculator.net, n.d.). The fundamental ROI formula is displayed in Equation (1). Note that the formula assumes that both cost and gains are summarized in a unidimensional measurement scale and, moreover, that they use the same scale, i.e., the same units—usually monetary. Because control systems and cybersecurity provide many different types of benefits, and many types of costs, a fundamental challenge to calculating an ROI is summarizing multidimensional benefits (and costs) in a single scale. The return-on-investment tool that SPAWAR is developing aims to measure benefits of security measures in the form of cost savings, or in equivalent monetary value. Unlike most financial investments where the "gain on investment" would be referred to as profit, the SPAWAR ROI tool will attempt to quantify cost savings of attack prevention, while capturing any other benefits or costs that are important to the stakeholders.

$$ROI = \frac{\text{Gain on investment - Cost of investment}}{\text{Cost of investment}} \tag{1}$$

THIS PAGE INTENTIONALLY LEFT BLANK

III. METHODOLOGY

To support SPAWAR's ReCIst ROI tool and per this project's goals in Chapter I, section C., the team used the value-focused thinking (VFT) methodology (Keeney, 1996) to identify what NAVFAC energy management teams value from their control system networks and from protection in the form of security products for control systems. In particular, the team elicited values and objectives from stakeholders in structured interviews, explicitly defined the objectives, and organized them into a means-ends network, identifying the fundamental (also known as "ends") objectives and showing the relationships among objectives.

A. WHY USE VALUE-FOCUSED THINKING?

Keeney (1996) states that decision problems are not necessarily "problems," but decision opportunities. In SPAWAR's ROI tool, the decision opportunity is *which cyber product(s) do I buy to protect my control system and microgrid?* The VFT method identifies values that stakeholders might not have otherwise considered. Our team hopes that VFT will reveal additional values previously not thought of by analysts and decision makers. The focus on end objectives and values will eventually lead to a better decision and a better ROI tool.

VFT also clarify values and provide structure for measuring costs and benefits. Doing so will eliminate redundant objectives and explicitly define values so that they may be measured. For example, clarifying and standardizing the term *resilience*—if you define it as "time until power is restored," you have something that's at least potentially measurable. If metrics are not standardized the effects and expectations of the cybersecurity products will be different across the DOD.

Another important contribution of VFT, in the SPAWAR ROI context, is clarifying and communicating (for example, Figure 4) why various metrics are important. This can allow one to not measure a seemingly important objective if you can measure higher level objectives instead. For example, in a manufacturing plant, if you measure the production objectives between "maximize quantity of units produced" and "minimize total costs," it

may become unnecessary to track the amount of material used to produce the units. Of course, this example depends on the level of management. VFT can also help stakeholders with competing objectives—for example, trade-offs between a "more secure" control system versus a "more functional" control system. VFT aims to identify how various stakeholder preferences interact with other legitimate but conflicting preferences.

Keeney's VFT separates itself from other decision-making methodologies by teasing out previously unknown or unthought-of alternatives (Keeney, 1996). Decision makers often only compare and make decisions based on a limited selection of alternatives. While these alternatives will probably solve their problem, they do not necessarily offer the best outcome (Keeney, 1996). For example, you may choose between three restaurants to eat lunch due to proximity, even though you are willing to drive further if there were a *better* option. In the future, you will tend to decide lunch options between only those three restaurant menus. Keeney addresses this issue by having the stakeholder identify the *values*, or "what they care about," in relation to the decision opportunity (Keeney, 1996). The identified values stimulate additional alternatives and eventually lead to a better outcome (Keeney, 1996). For example, assume you performed VFT and you value low-sodium and vegan options, and after a little research, these values led you to find four more restaurants in reasonable proximity that meet these preferred nutritional values. You would then have better, but previously unthought-of, lunch options for the future.

Alternatives intended to be revealed through VFT methodology are already going to be represented in SPAWAR's ROI tool as various cybersecurity products. SPAWAR and the DON may have the opportunity to identify and select products they would not have otherwise identified as a result of this method. The products will be an output of the ROI tool, but not identified while using the tool or while doing VFT.

B. DATA COLLECTION EFFORTS

The VFT methodology has five basic steps as depicted in Figure 1: identify stakeholders, determine values, convert values to objectives, distinguish between means and ends objectives, and construct the means-ends objective network (Keeney, 1996; Maitland, Barclay, & Kweku-Muata, 2013). Figure 1 illustrates the VFT methodology

using various values, related objectives, and ultimately means-ends networks. For example, the value "not need car" translates to an objective "have necessary goods and services nearby." The figure illustrates the same process using several other projects as guides to execute the first five VFT methodology steps.

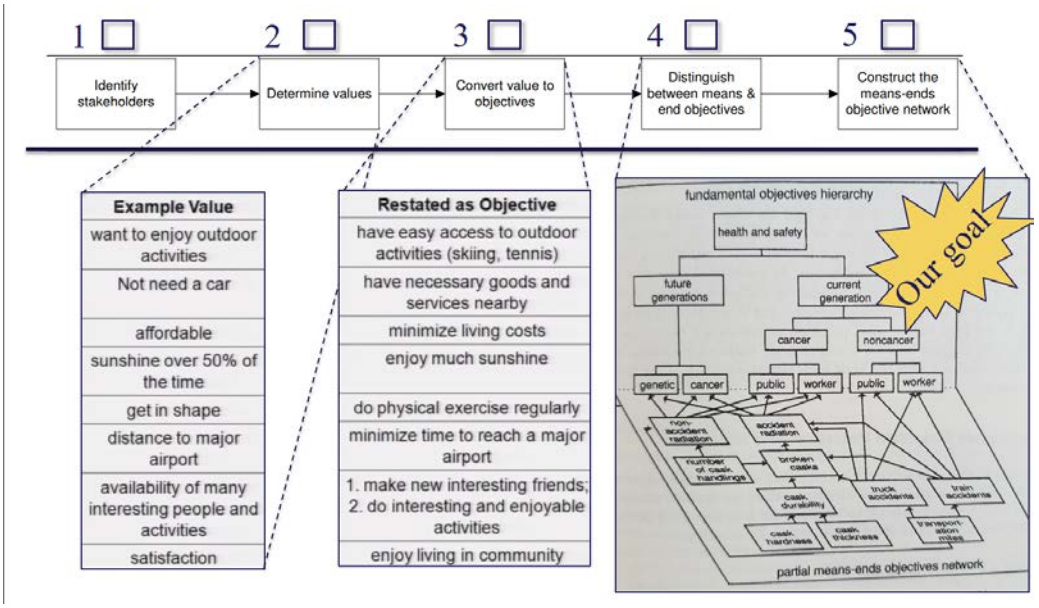

Figure 1. Value-Focused Thinking Process. Adapted from Keeney (1996), Maitland et al. (2013), and Siebert (2013).

1. Identify Stakeholders

Values "should come from individuals interested in and knowledgeable about [the] situation" (Keeney, 1996; Maitland et al., 2013). For this project, the stakeholders were NAVFAC energy managers, engineers, and program managers, as detailed in Table 1. The stakeholders were contacted and recruited in accordance with NPS Institutional Review Board (IRB) human subjects research guidance.

We obtained subjects by first identifying which commands operationally supported the energy mission and worked with control systems. The NAVFAC website has its organization easily delineated by function and location, and has contact information. We also decided to select commands in relatively close proximity to the NPS. We also made selections based on news articles. For example, NAVFAC Miramar was selected to be

contacted based on an online news article about its innovative renewable energy microgrid construction plan.

Table 1. Interview Locations

Date	Location	Interviews
14 Sep 17	NAVFAC, Miramar	3
15 Sep 17	NAVFAC, NBSD	2
18 Sep 17	NAVFAV, JBPHH	1
19 Sep 17	NAVFAV, JBPHH	1
20 Sep 17	NAVFAV, JBPHH	2

2. Identify Values

Researchers probe the stakeholders with questions and have open discussions to identify their values in context to the decision problem (Keeney, 1996). In this project, the team conducted structured interviews with the identified stakeholders. The following list represents a menu of questions that could have been asked in any given interview to identify values. These questions were created based on previous research in Maitland et al. (2013) and a literature review on cybersecurity concerns, microgrids, and control systems. Due to time constraints (the interviews were limited to approximately one hour) we averaged three menu questions, 1, 2, and 3. We selected these questions due to the volume and variation of answers they might invite. Stakeholder answers were written on a Post-It note and placed on a wall or white board with elaboration in response to interviewer questions, and with their relationships identified as described in steps 3 and 4 of Figure 1,

1. List what is important to you regarding the performance of CS networks.

2. Describe the ideal performance of a microgrid under a cyberattack (or electrical grid if no microgrid).

3. List the consequences of a worst-case scenario (within reason).

4. List what is important to you regarding cybersecurity performance for CS networks.

5. What are your current concerns relating to security threats on CS networks?

6. What can be done to raise awareness of cybersecurity threats on CS networks? (Maitland et al., 2013)

7. What are some of the issues that prevent the effectiveness of CS networks? (Maitland et al., 2013)

8. How would you evaluate cybersecurity threats on CS networks?

9. How would you evaluate your vulnerability to cyber threats?

10. What would you tell other energy engineers to do to maintain cybersecurity, CS networking performance?

11. What can the owners of commercial-run power plants do to increase safety against cybersecurity threats?

3. Restating Values as Objectives

The third step in the process is to restate the values as objectives using a verb-noun format (Keeney, 1996; Siebert, 2013). Keeney (1996) explains, “An objective is a statement of something someone desires to achieve” (p. 34).

Steps 2, 3, and 4 were sometimes conducted simultaneously and produced raw data, as illustrated in Figures 2 and 3. Converting the interview answers into objective statements would prove to be one of the simplest of all the steps. Most of the time this was done while the questioning was taking place. These figures show the answers written on yellow post-it notes placed on a white board. The subsequent writing with accompanying arrows are a

result of “why is that important?” and “what do you mean by that?” questioning per Step 4. Each interview’s raw data was recorded with a picture and compiled to complete Step 5.

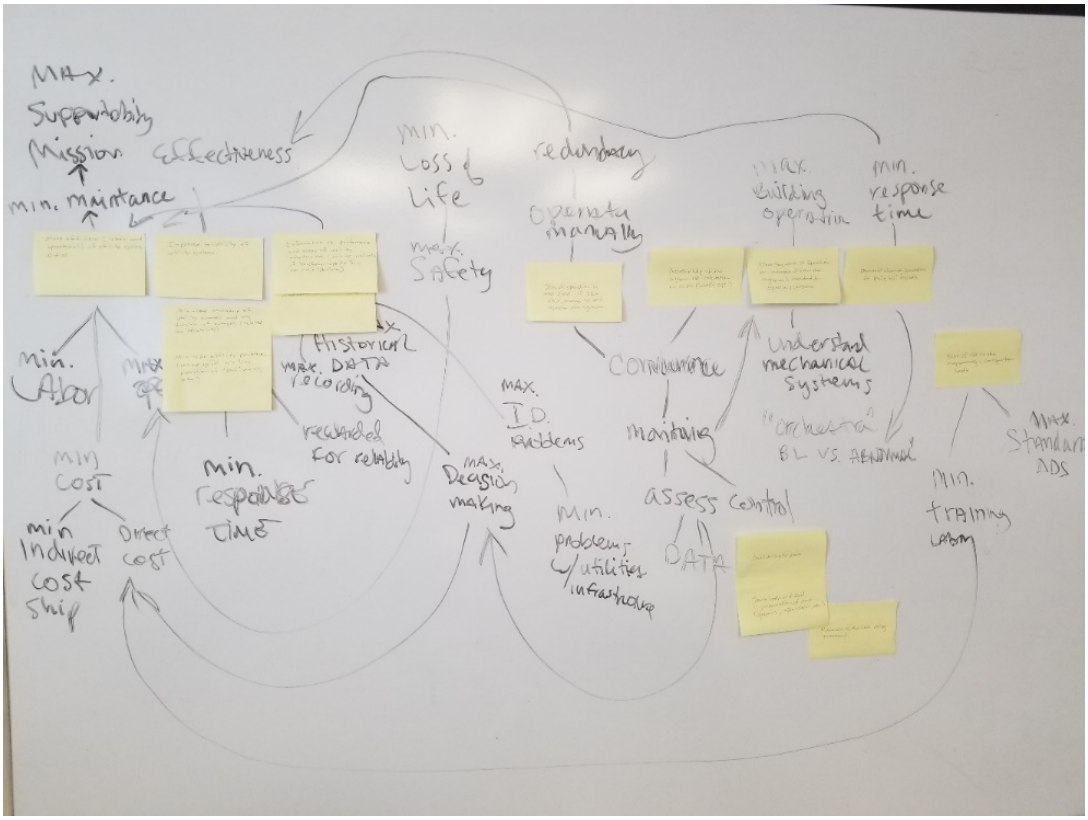

Figure 2. Example of Interview Results 1

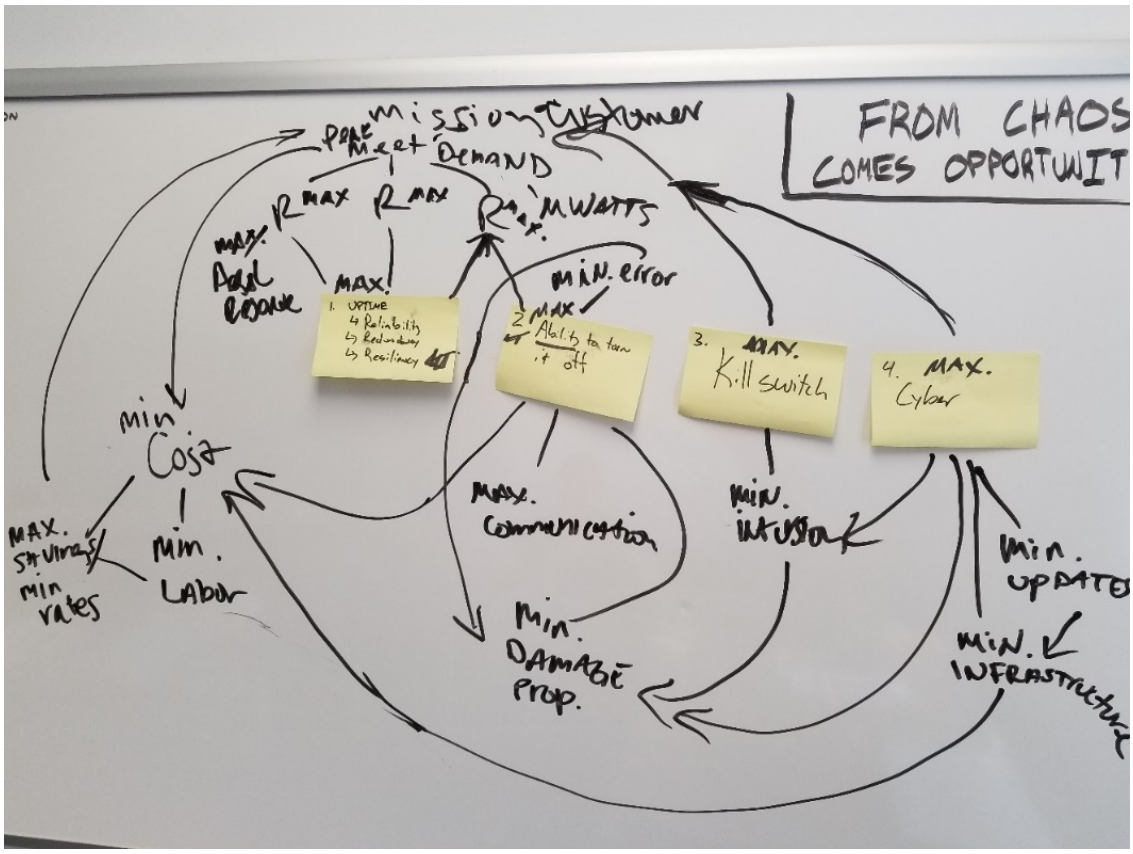

Figure 3. Example of Interview Results 2

4. Delineate Means and Fundamental Objectives

Keeney (1996) says, “A fundamental objective characterizes an essential reason for interest in a decision situation” (p. 34). Means objectives lead to the accomplishment of fundamental objectives (Keeney, 1996). Step 4 is accomplished by asking the “why is that important?” question, which leads to fundamental values or the “what do you mean by that?” question, which could lead to more detailed means objectives (Keeney, 1996; Maitland et al., 2013). For example, a frequently written answer to the question “List the consequences of a disaster” was death or casualties as a result of an electrical surge or breaker trip. After questioning, the interviewee clarified the value to “minimize casualties.” When asked, “why is that important?” the interviewee explained that while casualties may prevent NAVFAC from accomplishing its mission, casualties were important even absent an effect on the mission, revealing that minimizing casualties is a fundamental objective. As Maitland et al. (2013) noted, “If an objective is found to be important because it helps

achieve another objective, it is categorized as a means objective; otherwise it is a fundamental objective" (p. 7). After several interviews it was clear that "minimize causalities" was a fundamental objective. The "what do you mean by that?" question also helped clarify industry buzzwords like "resilient." For example, almost all interviewees valued "maximize resiliency." Interviewees defined *resiliency* as the amount of time to return to normal operation, or the minimum amount of time it took to restore power. This helped to clarify that resiliency is not the same as durability or flexibility. Flexibility is preventative and resiliency is reactionary to a specific event such as an unplanned outage. This clarification greatly simplifies the identification of appropriate measures of resiliency that may be included in ROI calculations.

Due to time constraints, Step 4 was also performed after the interviews. A difficult aspect of this step is knowing when to expand upon vague objective statements. "Maximize efficiency" is an example of an objective given by interviewees that is not well defined, or not defined identically by all. Efficiency is a ratio used to measure relationships between specified numerators and denominators (for example, "production efficiency" is a common ratio used in a manufacturing plant). The numerator in this ratio is total costs and the denominator quantity of products produced, with the goal to minimize costs and maximize the quantity of products manufactured—to produce more products with less material and costs. In our case, "efficiency" was often described as the relationship between performing the best quality services while striving for lower costs. "Services" was defined as supporting the effort to deliver constant power to the customer and other base functions. "Maximize efficiency" would eventually break out into two or more fundamental objectives such as "maximize reliability," "maximize resilience," and "minimize costs."

5. Means-Ends Network

Step 5 is to structure objectives into a means-ends objective network (Keeney, 1996; Maitland et al., 2013). Three main aspects to the network include identifying the highest-level fundamental objectives, relationships among objectives, and the size and scope of the network (Keeney, 1996). The means-ends network is a graphic depiction of all of the interview answers and is presented in Chapter IV. The means-ends network

represents a formula shell where performance metrics could be developed reflecting each node (objective) in the network. Means objectives contribute to fundamental objectives (i.e., fundamental objective measurements could be calculated as a function of the means objectives).

The means-ends network also helps identify the relationships between competing objectives, such as more cybersecurity versus system functionality—where additional steps to improve the security of the control system may restrict its maximum potential to function. The potential to lose functionality of the control system as a result of adding security measures was a constant theme expressed throughout the interviews.

Ideally, preference trade-offs are evaluated using fundamental objectives (Keeney, 2002). In our case, the trade-offs between security and system functionality should be evaluated between the effects of the fundamental objectives identified in Chapter IV. For example, based on Keeney (2002), an appropriate question to elicit fundamental value trade-offs in this context would be: Suppose it costs $1 billion annually to maintain 50% cybersecurity, and suppose it costs $6 billion annually to obtain 60% cybersecurity. Is a 10% gain in cybersecurity worth an additional $5 billion annually? This is distinct from asking: Is it worth $1M to have a kill switch? The ReCIst ROI tool could calculate relationships between the means and fundamental objectives; for example, the relationship between “enable kill switch” (means) and “maximize resilience” (ends).

THIS PAGE INTENTIONALLY LEFT BLANK

IV. RESULTS

From the interviews, we were able to consolidate fundamental and means objectives into a network illustrated in Figure 4. The fundamental objectives were common to all interviews, and are arranged in a hierarchy (each lower-level objective has only one parent) at the top of Figure 4. here was one overarching objective that all subjects agreed was paramount: The ability to provide mission support to end users of their services. This objective is shown in the top left of Figure 4. Various means objectives were discussed with certain subjects emphasizing differing aspects of those characteristics. Not every means objective was raised in every interview. Means objectives, are shown in a network (each means objective may contribute to more than one higher-level objective) in the lower portion of Figure 4. This chapter explains each fundamental and means objective and how it contributes to the ability of NAVFAC to support end users.

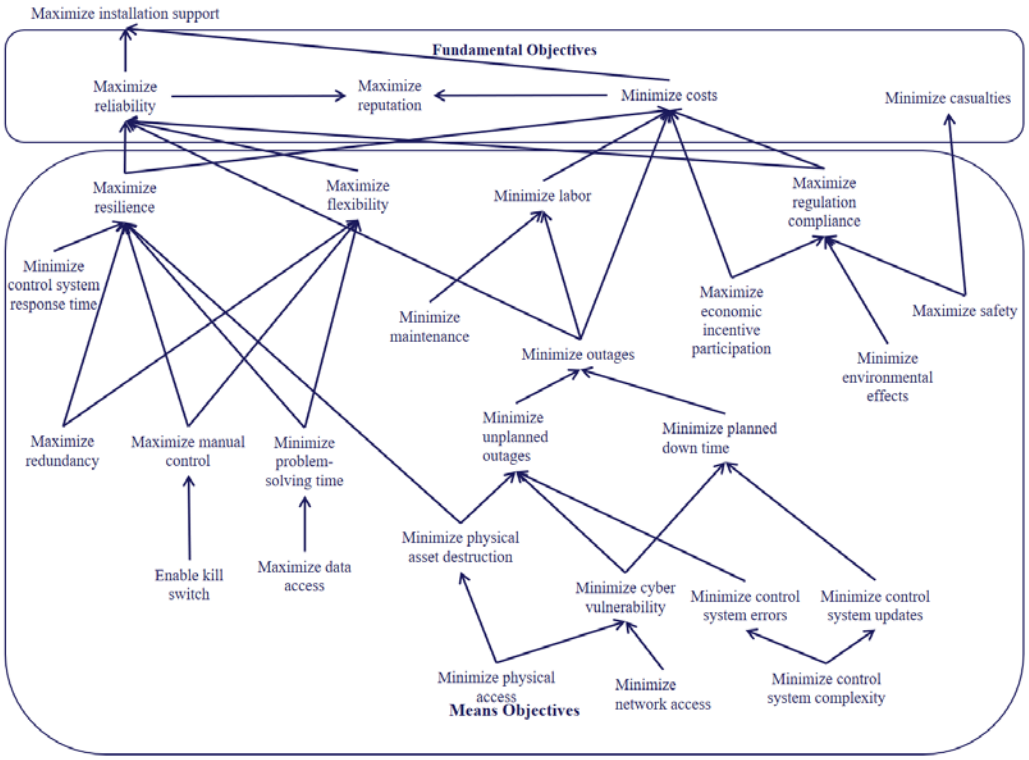

Figure 4. Means-Ends Objective Network

A. FUNDAMENTAL OBJECTIVES

Based on the interviews, the most common responses led to four fundamental objectives: to maximize reliability, maximize reputation, minimize costs, and minimize casualties. Combined, these fundamental objectives led to one overarching objective: maximize installation support. For each NAVFAC entity, maximization of installation support was meant to allow end users the best possible energy support needed to accomplish their mission.

1. Maximize Reliability

Universally, according to all those who participated in the study, reliable energy was an essential value and a crucial aspect of the mission. Depending on which level the subjects worked at and the specificity of the NAVFAC facility mission, "reliable energy" was defined by the subjects differently. However, the term was consistently used to refer "to the ability of an energy production system to provide consistent and expected levels of energy under stated conditions for a specified period of time" (Energy-101.org, 2017). Objectives like minimizing outages, maximizing regulation compliance, maximizing resilience, and maximizing flexibility of the control systems were all mentioned within the interviews as important means to the maximization of reliability. By minimizing the number of outages occurring, the system is naturally able to provide more consistent and therefore reliable energy. A facility department's ability to comply with regulation ensures that there will be no government interference in regards to the system's operation and therefore supply of power. Resilience ensures that the system is able to recover and is therefore more reliable under stress. Flexibility adds to reliability as the system's ability to adjust and respond to differing circumstances helps to provide optimal service. In relation to sustaining the ability to provide reliable energy, the subjects had differing outlooks as it pertained to cybersecurity. An energy installation manager explained that while cybersecurity is important, there are immediate issues when it comes to providing adequate manpower to support the systems. In regards to his manpower concerns, this subject explained more thoroughly that he felt it more probable that they could potentially have a system that nobody knew how to use and that was more threatening than the current cyber

vulnerabilities. Contrary to that opinion, a subject that oversaw a more extensive network expressed concerns over the potential cyberattacks could have in disrupting the reliable energy. This subject felt that there was a realistic hacking threat that could allow adversarial control over electrical breakers.

2. Maximize Reputation

The ability to provide reliable energy was directly related to the fundamental objective to maximize reputation. Subjects felt that the ability to provide low cost, reliable energy helps to bolster the facility's reputation. Across all installations involved in the study, the subjects expressed a general concern for NAVFAC's reputation. Much like public and private companies, a federal agency's reputation is of great importance. Public trust is a fundamental component that is necessary for the success of government actions (Organization for Economic Co-Operation and Development [OECD], 2017). One of the ways to build a good reputation is to improve the ability of an organization to meet expectations (Eccles, Newquist, & Schatz, 2007). The DOD is expected to protect American security (DOD, 2017). The DON's ability to protect their control systems is part of that mission. A disruption to a CS that degrades the ability of the Navy to function in turn degrades the expectation that the DOD can keep America safe. As Benjamin Franklin is quoted, "It takes many good deeds to build a good reputation, and only one bad one to lose it" (Goodreads, n.d.).

3. Minimize Costs

Costs are what is paid or given up in order to get or achieve something. This study defines *costs* as an expenditure of resources or opportunity. Resources include labor, materials, time, and monetary funds. In the context of the control systems, the resources would be manpower, physical assets, time, and budgetary discretion.

Costs were discussed in all forms in every interview that we conducted. The control system's ability to minimize labor requirements was one of the most prominent means objective related to keeping costs low. With more automated functions and less time taken to fix or perform maintenance, the control systems are able to save resources. This also helps to minimize planned or unplanned outages. Planned outages may occur as the result

of regular maintenance or as system updates are installed. Unplanned outages occur for various reasons such as weather disruptions, breaker overloads, or physical depreciation of the systems.

Costs were a concern for all subjects interviewed, however one subject elaborated on the importance of keeping energy costs low. This subject explained that by lowering the costs of energy they could in turn charge the users on the installation less and this would allow them more discretionary freedom in their budget. Budgetary discretion for NAVFAC customers frees up funds they can allocate towards other uses in order to better perform their missions. This subject described a scenario in which NAVFAC was able to participate in economic incentive programs. The incentives of the local economic program came in the form of decreasing monetary costs of commercial grid electricity. On the other hand, violations of economic regulatory compliance often result in fines that increase costs.

4. Minimize Casualties

All who were interviewed felt that death and casualties were potential consequences of worst case scenarios. In accordance with the NAVFAC safety policy, the NAVFAC personnel felt that safety was a vital enabler of the support to the operational position and warfighter's readiness (Naval Facilities and Engineering Command, 2013). Concerns for the realistic danger of working with industrial systems and the potential for casualties due to disruptions within control systems were expressed by all interviewed. Universally, all of the subjects expressed a need to maximize safety of the operating environment and the control system in order to minimize casualties. Deaths or casualties that occur in relation to control systems are contrary to the DON's mission "to maintain, train, and equip combat-ready naval forces capable of winning wars, deterring aggression, and maintaining freedom of the seas" (United States Navy, 2017). According to the Bureau of Labor Statistics (2016), an average of over 150 deaths per year occurred in relation to electrical systems between the years of 2011 and 2015.

B. MEANS OBJECTIVES

The means objectives contribute to fundamental objectives. We have extracted the most common means objectives from the interviews and tied them to their fundamental

objective(s) as shown in Figure 4 above. The VFT methodology used in the interviews included identifying what connections were most prominent, as described in Section III.B.5. The following section offers brief descriptions of the means objectives, how they relate to NAVFAC operations, and their ties to fundamental objectives.

1. Maximize Resilience

As a key means objective to ensure reliability, the ability to restore power quickly was considered a key objective by all of those interviewed. The term resilience is used in several different ways. The DOE defines *energy resilience* as the ability to prepare, prevent, and recover from disruptions that impact the mission of government installations (DOE, 2017d). In this study, we differentiate it from other commonly used terminology such as "reliability." Referencing an etymological study of the word *resilience*, this study uses the word to mean to recover from a disruption (Clark-Ginsberg, 2016), so maximizing resilience means minimizing the time to restore required energy services following a disruption.

Three of the subjects explained that the ability of a control system to respond to a disruption was an integral part of the system's use. Minimizing control system response time to an incident directly correlates with the resilience of the system overall. One of the engineers further explained that the control system could pinpoint where a disruption had occurred and explain what had happened. This data allowed the operator to save time and resources by ensuring that he brought along the correct tools and knew exactly where to locate the problem, and by minimizing problem solving time, the time to restore power is reduced. Maximizing data access, in turn, reduces problem-solving time.

Resilience is also achieved through maximizing redundancy. The redundancy provided by alternative energy sources such as renewable energy, that are enabled by microgrids and stand-alone generators that are strategically placed to carry critical loads allow an installation to provide more resilient energy. The physical security of these redundant assets remains critical to ensure that they are ready when needed. Therefore, the ability to for a facility to minimize physical asset destruction directly contributes to their ability to maximize resilience. While one of control systems' key features is automation, it

was stressed to us that the ability to shut off the system and provide manual control was also an integral component of a resilient system. In the case that the control system is no longer functioning at a desired level, the personnel expressed a need for the option to go off-line and perform manual controls. According to one of our subjects the ability to maximize manual control was an essential aspect that was needed in order to maximize resilience.

2. Minimizing Labor

As discussed in the previous means objective, the subjects explained how the control system automates controls and lessens the necessity for manual controls. In addition, modern control systems provide the ability to monitor, protect, and control equipment within a distributed system (Electrical Technology, 2015). Benefits of this technology lessen the time required for maintenance and include the replacement of manual labor and manpower (Weinberger, 2010). The automated functions that modern control systems feature minimize maintenance required on the systems. Less manpower is required to perform maintenance and the system provides data that help operators determine optimal times for maintenance to occur. Reductions in manpower and labor directly impact cost savings and were considered essential to all subjects within this study.

3. Maximizing Regulation Compliance

One of our subjects explained the costs and benefits of the regulatory compliance specific to the laws the Environmental Protection Agency (EPA) enacts. The DON develops and partakes in various environmental, energy, and climate change initiatives (DON, 2017). Environmentally compliant operations are stressed within these initiatives. Facilities are to remain compliant with all "applicable environmental regulations and polices" (DON, 2017). By minimizing environmental effects ensures that the NAVFAC facility is compliant and avoids penalties. Violations of environmental regulations lead to fines. In September 2016, the DON paid a fine of nearly $100,000 due to a violation of an EPA regulation on Joint Base Pearl Harbor. The EPA regulation that denied federal installations to utilize large-capacity cesspools had been violated ("Navy Pays EPA Fine," 2017). Violations of regulations increase costs and degrade the Navy's mission. The

subject went on to discuss some of the energy sharing initiatives that could be used to receive cost savings. Maximizing economic incentive participation enables, NAVFAC facilities to lower the costs of their energy and better support the Navy's mission. In addition, compliance with regulations reduces risks to life and health and therefore casualties.

4. Maximize Flexibility

As a means to providing reliable energy, the subjects discussed how the control system was important in its ability to meet the fluctuations in energy usage. Energy flexibility is the ability for a control system to maintain its distribution while experiencing fluctuations in the energy supply or demand (Papaefthymiou, Grave, & Dragoon, 2014). As the use of renewable energy sources, such as hydroelectricity and solar, increase, energy systems have an increased need for flexibility (Papaefthymiou et al., 2014).

One subject interviewed discussed the trade-off of automated systems and user control. This subject expressed the need to enable a kill switch for an authorized person to turn the system over to manual controls. This subject had experienced issues when attempting to shut off an automated system. As a result, the system was no longer operational.

All subjects discussed how redundancy was a key part of an installation's energy flexibility. The continued use of strategically placed generators in order to back up critical loads was a common example of redundancy. The ability for a system to collect data quickly and then allow user access was stressed as an important aspect to minimizing problem-solving time. By maximizing data access, operators are able to make sound and timely decisions that adds to the systems overall flexibility.

5. Minimize Cyber Vulnerability

The subjects all admitted that vulnerabilities in control systems exist within the architecture of the system. However, the same level of concern over those vulnerabilities was not universally shared. One subject felt the 2015 Ukraine cyberattack that resulted in a prolonged outage was not an unrealistic scenario, but one that could potentially occur

against NAVFAC installations. Within this example, the subject discussed the vulnerabilities that exist when systems have complex networks with multiple entry points. By minimizing physical and network access, the system can decrease its cyber and physical vulnerabilities. Hacking and the potential to obtain authorized power to operate the control system was said to be a significant threat that should not be taken casually.

6. Minimize Control System Complexity

As a means objective to both the minimization of control system errors and the minimization of control system updates, the minimization of control system complexity was described as essential to decrease both unplanned and planned outages. One of the subjects that we interviewed expressed concern over the number of outages that occurred due to system updates and thought that a less-complex system would potentially avoid that problem. In addition to the increased number of planned outages, unplanned outages were described as more prevalent within more complex systems. A control system engineer explained that the more connections that a control system had to outside systems directly increased the amount of possibilities for disruptions.

C. TRADE-OFFS

1. Functionality versus Security

The most commonly discussed trade-off was between the functionality of the system and security. The interviews showed that all subjects had similar understandings of the relationship between functionally and security, but there was no universal agreement on how it should be balanced. It was clear that variables such as billet responsibility, installation location/mission, and historical experience all weighed in as factors that ultimately resulted in differing perspectives and values. When interviewing a single control system engineer, the concern over the security of the system was described as someone else's concern. This is in stark contrast to the perspective of another subject who was responsible for more than one installation. The subject responsible for multiple installations expressed personal beliefs that security was essential at all levels, and that without security the potential for widespread disaster over the supplied area was probable. Another subject who oversaw an installation felt that security was being implemented in a more than

adequate manner and that more security would potentially be a waste of resources. This subject felt that the ability to use the system was more critical and that resources ought to be allocated in a way to support the functions of the system. As for the risk of cyberattack, another subject explained that he was more worried about the rat that could chew through vital cables and explained that they had experienced an entire critical circuit go down after a gecko was electrocuted on a wire. Although we encountered different perspectives and thoughts on the importance of security, a common theme across all subjects was the need for balance between functionality and security. One subject said it this way: “The most secure system is one that doesn’t work.”

2. User versus Automated Controls

This trade-off was not universally discussed; however, one installation did find it important enough to emphasize more than once. While most of the interviews contained praise for control systems’ ability to automate functions, subjects at one installation expressed concern over a control system’s inability to be shut down and assume manual controls. The reason for this concern was given through the explanation of a relatively recent issue that had occurred with the microgrid. Once the microgrid malfunctioned, it would not respond and would not turn off. This resulted in damaged assets and the suspension of the microgrid’s use.

THIS PAGE INTENTIONALLY LEFT BLANK

V. ANALYSIS AND CONCLUSION

A. WHAT DO THE RESULTS TELL US?

NAVFAC stakeholders value customer support and ensuring that customers have the power to perform mission critical tasks. A varying degree of value was placed specifically on cyberdefense among stakeholders—some stakeholders felt that it was very important, while others placed less emphasis on it. Those who felt that cybersecurity was less important favored functionality and connectivity. They expressed the opinion that potential disruption due to cyberattack did not pose an immediate threat to their mission. However, those stakeholders who assigned less value to cybersecurity did not find it unimportant. For example, the end user stakeholders generally praised "Big Navy" and cyber-focused employees for researching ways to minimize the cyber threat. With this research, we found that the NAVFAC employees who felt this way generally believe that enough is being done at higher levels to combat cyber-related threats. These interviewees expressed that their specific installations had more pressing issues like manpower and systems' compatibility.

As Marine officers conducting this study, we can provide a similar example from our personal experiences. It is common for military personnel in the non-combat military occupations to perceive the threat of enemy contact as less probable compared to those who serve within the infantry community. Despite the Marine Corps stressing that all Marines must be riflemen first, there are many within non-combat military occupational specialties that become consumed with the immediate issues within their jobs and assume that the infantry will take care of the combat. The problem is not visible until the effects are experienced. However, the majority of those interviewed expressed that cybersecurity was essential to their mission and an integral component to ensure mission support.

B. FUTURE RESEARCH

Chapter III is based on Keeney's value-focused thinking; however, Chapter III is only one of several steps to completing the decision analysis. According to Keeney, the means-ends network should first represent a summary of all stakeholder's objectives

(Keeney, 1996; Siebert, 2013). The means-ends network for this problem is Figure 4. The means-ends network may inspire the stakeholders to create new alternatives or "potential choices to pursuing your [means] objectives," which in turn would increase the odds of achieving their fundamental objectives (Siebert, 2013).

To complete this VFT-based project, the NAVFAC participants must think of solutions that will drive improvements in their fundamental objectives. Using each objective in turn to brainstorm alternatives could result in potentially more solutions outside the scope of cybersecurity (Siebert & Keeney, 2015). These could be hardware, software, policy, or other operational changes. The DOD is currently pursuing antivirus and security software programs as the alternatives to "minimize network access" and "minimize cyber vulnerability" (Defense Information Systems Agency, 2017).

Alternative brainstorming should not be restrictive. The stakeholders strive to develop as many options as possible no matter how unrealistic they may seem. Keeney states that stakeholders are to evaluate the alternatives with three criteria: usefulness, feasibility, and creativity. This step is designed to assist stakeholders in the determination of which best alternatives to pursue. There is a possibility that it could result in other alternatives aside from firewalls and software development for cyber-defense. It is possible that the results could promote a completely different approach to energy security.

Keeney discusses the reactionary nature of decision problems. He defines *decision problems* as problems caused by other people, belligerents, or happenstance. For example, the Navy's network *has been* hacked and we must react to the situation. These problems have already occurred. In the context of our thesis and SPAWAR's ReCIst team's project, the decision problem is caused by hackers or anyone who *has* obtained unauthorized access to naval control system networks. Fortunately, we do not have a decision problem, or at least an unclassified one— we have a decision opportunity. Keeney states a decision opportunity is proactive, or that a potential problem has been identified but has not occurred yet. In the context of our thesis and SPAWAR's ReCIst team, the decision opportunity is, "which cyber-defense product do I buy to prevent control system infiltration by unauthorized users?" This is the question the SPAWAR ReCIst team is ultimately attempting to measure, cost out, and decide.

C. THE NEED TO STANDARDIZE PERFORMANCE MEASURES

There is the potential that a future project could be useful in the attempt to standardize performance measurement for the ends and means objectives found within this study. According to Gregory et al. (2012), there are three types of performance measurements: natural, constructed, and proxy. There are five categories for identifying and selecting each type of performance measurement for an objective: complete and concise; unambiguous; understandable; direct; and operational (Gregory et al., 2012, p.96-97). Gregory et al. (2012) explain what each category means and clarifies how to determine if the proposed performance metric is satisfactory. Without standardization, performance measurements could incorrectly evaluate or insufficiently weigh information. For example, counting the number of deaths to measure the objective "minimize casualties" may be too vague. Questions regarding the measurement may include the following: Is there a consistent time frame? Are the deaths recorded per outage? Is the causality civilian or military? In order to maintain accuracy, several different measurements may need to be recorded simultaneously. Such an approach would seek to accurately determine the performance of the "minimize casualties" objective. A future project could focus on finding the metrics for the objective "minimize cyber vulnerability" and all other objectives. These measurements could be consolidated by the research team and given back to stakeholders for feedback.

D. HOW CAN MULTI-OBJECTIVE DECISION ANALYSIS HELP?

This thesis project was focused on qualitative modeling using VFT to identify control system end user values, objectives, and alternatives. Multi-objective decision analysis (MODA) is the quantitative means to analyze the qualitative results. As Dillon-Merrill, Parnell, Buckshaw, Hensley, and Caswell (2008) put it, MODA is a method "for evaluating complex alternatives by systematically examining decisions and focusing on multiple, conflicting objectives" (p. 6). According to Parnell (2007), MODA is the method used to take VFT-qualitative data and analyze the best alternatives oriented toward achieving stakeholder values. MODA is specifically useful in analyzing conflicting objectives where a trade-off would normally occur (Parnell 2007). For example, a

commonly cited example throughout our interviews was the perceived trade-off between having uncertain cybersecurity results with above average control system network connectivity or having 100% cybersecurity results with no control system network connectivity at all. Both are extreme scenarios, unless electrical engineers can design a microgrid that does not need a control system and can run perfectly. The point is that MODA will take uncertainties and analyze the best alternative results for the stakeholders (Parnell, 2007).

VI. CONCLUSION

While mission support was a universally shared fundamental objective among the participants in this research study, not all subjects agreed on which means objectives should be stressed in order to achieve it. The network hierarchy that this project has provided is a compilation of the commonly shared values along with a few means that were stressed by a subset of the participants. It is reassuring that all participants of this study did agree on the need for balance between functionality and security. An ROI tool that allows end users the ability to weigh values and enter their own values at their own specification would help to ensure that the tool does not rigidly support a particular set of preferences particular to one group of stakeholders or type of installation or mission. User specificity in preference trade-offs will be essential in order to best capture the variables associated with an installation, its control system, and the environment. Threats exist in all forms and the potential for disruptions caused by obscure reasons, such as geckos interrupting critical loads, will only be thought of by the end user. We believe that the subject matter experts on the ground are in the best position to make critical decisions on how to balance security. As universally expressed throughout this study, balance between trade-offs will remain key. This study concludes that the end users have the control to strike that balance between trades-offs, however supervision must carefully monitor whatever trade-off is decided. As Oscar Wilde is quoted, “Everything in moderation, including moderation” (Goodreads, n.d.).

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Adametz, J., Groesbeck, D., & Quibilan, R. (2016, September). *Navy strategy for cybersecurity of industrial control systems: Analysis and recommendations* (Capstone Project report). Monterey, CA: Naval Postgraduate School.

Asia-Pacific Technology and Education Partnership. (2017). Energy Systems Technology Evaluation Program. Retrieved from https://www.aptep.net/partners/estep/

Broekhoven, S. V., Judson, N., Galvin, J., & Marqusee, J. (2013). Leading the charge: Microgrids for domestic military installations. *IEEE Power and Energy Magazine*, *11*(4), 40–45. doi: 10.1109/MPE.2013.2258280

Bureau of Labor Statistics. (2016, December 16). *National census of fatal occupational injuries in 2015*. Washington, DC: Bureau of Labor Statistics. Retrieved from https://www.bls.gov/news.release/pdf/cfoi.pdf

Calculator.net. (n.d.). Return on investment (ROI) calculator. Retrieved November 1, 2017, from http://www.calculator.net/roi-calculator.html

Center for Naval Analysis Military Advisory Board. (2015, November). *National security and assured U.S. electrical power*. Arlington, VA: can. Retrieved from https://www.cna.ocanCNA_files/PDF/National-Security-Assured-Electrical-Power.pdf

Clark-Ginsberg, A. (2016, March). *What's the difference between reliability and resilience?* Washington, DC: U.S. Department of Homeland Security. Retrieved from https://ics-cert.us-cert.gov/sites/default/files/ICSJWG-Archive/QNL_MAR_16/reliability%20and%20resilience%20pdf.pdf

Clouser, G. (2013, April 1). *SCADA getting smarter*. Retrieved from https://www.schneider-electric.com/solutions/ae/en/med/691367152/application/pdf/2414_scada-getting-smarter-_-midstream-business-ap.pdf

Defense Information Systems Agency. (2017). Anti-virus/anti-spyware solutions. Retrieved from http://www.disa.mil/Cybersecurity/Network-Defense/Antivirus

Department of Defense (DOD). (2017, January 27). About Department of Defense. Retrieved from https://www.defense.gov/About/

Department of Energy (DOE). (2016, September). *Distribution automation: Results from the smart grid investment grant program–Distribution automation summary report*. Retrieved from https://energy.gov/sites/prod/files/2016/11/f34/Distribution%20Automation%20Summary%20Report_09-29-16.pdf

Department of Energy (DOE). (2017a). About the Grid Modernization Initiative. Retrieved from https://energy.gov/under-secretary-science-and-energy/about-grid-modernization-initiative

Department of Energy (DOE). (2017b). Grid modernization and the smart grid. Retrieved from https://energy.gov/under-secretary-science-and-energy/about-grid-modernization-initiative

Department of Energy (DOE). (2017c, January). *Valuation of energy security for the United States*. Retrieved from https://energy.gov/sites/prod/files/2017/01/f34/Valuation%20of%20Energy%20Security%20for%20the%20United%20States%20%28Full%20Report%29_1.pdf

Department of Energy (DOE). (2017d). *Department of defense installation energy resilience* [PowerPoint slides]. Retrieved from https://energy.gov/sites/prod/files/2017/06/f34/5_Storage%20and%20Microgrids%20Panel%20-%20Ariel%20Castillo%2C%20DoD.pdf

Department of the Navy (DON). (2015). *ONR program evaluates emerging energy technologies at Naval facilities*. Retrieved from http://greenfleet.dodlive.mil/files/2015/10/Fall15_ONR_Energy_Technologies.pdf

Department of the Navy (DON). (2017). About Us. Retrieved November 14, 2017, from http://greenfleet.dodlive.mil/home/

Dillon-Merrill, R., Parnell, G., Buckshaw, D. L., Hensley, W. R., & Caswell, D. J. (2008). Avoiding common pitfalls in decision support frameworks for Department of Defense analyses. *Military Operations Research*, *13*, 19–31. https://doi.org/10.5711/morj.13.2.19

Eccles, R. G., Newquist, S. C., & Schatz, R. (2007, February 1). Reputation and its risks. Retrieved from https://hbr.org/2007/02/reputation-and-its-risks

Electrical Technology. (2015, September 14). SCADA systems for electrical distribution. Retrieved from https://www.electricaltechnology.org/2015/09/scada-systems-for-electrical-distribution.html

Energy-101.org. (2017). Reliable. Retrieved November 14, 2017, from http://www.energy-101.org/topics/choose-topic/definitions/reliable

Goodreads. (n.d.). Benjamin Franklin [Quotes]. Retrieved November 14, 2017, from https://www.goodreads.com/quotes/66761-it-takes-many-good-deeds-to-build-a-good-reputation

Goodreads. (n.d.). Oscar Wilde [Quotes]. Retrieved December 6, 2017, from https://www.goodreads.com/quotes/22688-everything-in-moderation-including-moderation

Gorman, S. (2009, April 8). Electricity grid in U.S. penetrated by spies. *Wall Street Journal*. Retrieved from https://www.wsj.com/articles/SB123914805204099085

Graham, L. (2017, September 20). Cyberattacks are surging and more data records are stolen. Retrieved from https://www.cnbc.com/2017/09/20/cyberattacks-are-surging-and-more-data-records-are-stolen.html

Gregory, R., Failing, L., Harstone, M., Long, G., McDaniels, T., & Ohlson, D. (2012). *Structured decision making: A practical guide to environmental management choices*. West Sussex, UK: Wiley-Blackwell. Retrieved from https://ebookcentral.proquest.com/lib/ebook-nps/reader.action?docID=862851

Hubbard, D. W., & Seiersen, R. (2016). *How to measure anything in cybersecurity risk*. Hoboken, NJ: John Wiley & Sons.

Idaho National Laboratory. (2016, August). *Cyber threat and vulnerability analysis of the U.S. electric sector*. Retrieved from https://energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf

Inductive Automation. (2017). What is SCADA? [Commerical]. Retrieved from https://inductiveautomation.com/what-is-scada

Investopedia. (2003). Return on investment—ROI [Wiki]. Retrieved November 1, 2017, from http://www.investopedia.com/terms/r/returnoninvestment.asp

John, J. S. (2012, November 20). How microgrids helped weather Hurricane Sandy. Retrieved from https://www.greentechmedia.com/articles/read/how-microgrids-helped-weather-hurricane-sandy

Keeney, R. L. (1996). *Value-focused thinking a path to creative decisionmaking*. Cambridge, MA: Harvard University Press. Retrieved from https://ebookcentral.proquest.com/lib/ebook-nps/reader.action?docID=3300726#

Keeney, R. L. (2002). Common mistakes in making value trade-offs. *Operations Research, 50*(6), 935–945. doi: 10.1287/opre.50.6.935.357

Keller, J. (2017, March 13). Navy SPAWAR chooses four companies for research into cyber security tests and technologies. Retrieved from http://www.militaryaerospace.com/articles/2017/03/cyber-security-emerging-technologies.html

Lantero, A. (2014, June 17). How microgrids work. Retrieved from https://energy.gov/articles/how-microgrids-work

Lyngaas, S. (2016, February 25). Top naval commanders asks Carter to include SCADA on cyber scorecard. Retrieved from https://fcw.com/articles/2016/02/25/commanders-cyber-pentagon.aspx

Maitland, N., Barclay, C., & Kweku-Muata, O.-B. (2013, December 14). A value focused thinking (VFT) analysis to understanding users' privacy and security dynamics in social networking services. In *Proceedings of SIG GlobDev Sixth Annual Workshop*. Milan, Italy: Special Interest Group for ICT in Global Development. Retrieved from http://globdev.org/files/proceedings2013/paper_19.pdf

Mitchell, A., & Dilanian, K. (2017, October 10). Experts: North Korea targeted U.S. electric power companies. Retrieved from https://www.nbcnews.com/news/north-korea/experts-north-korea-targeted-u-s-electric-power-companies-n808996

Navy pays EPA Fine to settle cesspool case. (2017, April 11). Honolulu Star-Advertiser. Retrieved from http://www.military.com/daily-news/2017/04/11/navy-pays-epa-fine-settle-cesspool-case.html

Naval Facilities and Engineering Command. (2013). *Safety Plan 2013*. Retrieved from https://navfac.navy.mil/content/dam/navfac/NAVFAC%20Atlantic/NAVFAC%20Southwest/PDFs/SF_docs/sw_sf_2013_safety_plan.pdf

Nekoui, A. (2014, October 22). Improving secure networks for national infrastructure. Retrieved from http://www.doncio.navy.mil/CHIPS/ArticleDetails.aspx?ID=5645

Organization for Economic Co-Operation and Development (OECD). (2017). Trust in government. Retrieved from http://www.oecd.org/gov/trust-in-government.htm

Ortiz, E. (2015, October 20). Microgrids sustain power during natural disasters. Retrieved from http://www.govtech.com/dc/articles/Microgrids-Sustain-Power-During-Natural-Disasters.html

Papaefthymiou, G., Grave, K., & Dragoon, K. (2014, March 10). *Flexibility options in electricity systems*. Berlin, Germany: ECOFYS. Retrieved from https://www.ecofys.com/files/files/ecofys-eci-2014-flexibility-options-in-electricity-systems.pdf

Parnell, G. S. (2007). Value-focused thinking using multiple objective decision analysis. *Methods for conducting military operational analysis: Best practices in use throughout the Department of Defense*, 619–656.

Romero-Mariona, J. (2016, July 22). *ESTEP program review: Resilient critical infrastructures through secure and efficient micro grids (ReCIst)[PowerPoint Slides]*. Email from Professor Eva Regnier.

Romero-Mariona J. et al. (2017) An Approach to Organizational Cybersecurity. In: Chang V., Ramachandran M., Walters R., Wills G. (eds) Enterprise Security. Lecture Notes in Computer Science, vol 10131. Springer, Cham, 203–222.

Siebert, J. (2013, July 30). Ralph Keeney´s (Duke University) talk on value-focused thinking at the University of Bayreuth [Video file]. Retrieved from https://www.youtube.com/watch?v=5nhBDgvjOy4

Siebert, J., & Keeney, R. L. (2015). Creating more and better alternatives for decisions using objectives. *Operations Research, 63*(5), 1144–1158.

United States Navy. (2017). Mission. Retrieved from https://www.navy.com/about/mission.html

Wattles, J., & Larson, S. (2017, September 16). How the Equifax data breach happened: What we know now. Retrieved from http://money.cnn.com/2017/09/16/technology/equifax-breach-security-hole/index.html

Weinberger, J. (2010, November 11). SCADA benefits without SCADA costs. Retrieved from www.wwdmag.com/analytical-equipment/scada-benefits-without-scada-costs

Zetter, K. (2016, March 3). Inside the cunning, unprecedented hack of Ukraine's power grid. Retrieved from https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California