An Integrated Framework for the Vulnerability Assessment of Complex Supply Chain Systems

by

Sarah Maria Rovito

B.S.E. Systems and Control Engineering, Case Western Reserve University, 2007
M.S. Systems Engineering, The George Washington University, 2010

Submitted to the Institute for Data, Systems, and Society in partial fulfillment of the requirements for the degree of

Master of Science in Technology and Policy

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

June 2016

Author.....
Institute for Data, Systems, and Society
May 12, 2016

Certified by.....
Donna H. Rhodes
Principal Research Scientist, Sociotechnical Systems Research Center
Director, Systems Engineering Advancement Research Initiative
Thesis Advisor

Accepted by.....
Munther A. Dahleh
William A. Coolidge Professor of Electrical Engineering and Computer Science
Acting Director, Technology and Policy Program
Director, Institute for Data, Systems, and Society

An Integrated Framework for the Vulnerability Assessment of Complex Supply Chain Systems

by

Sarah Maria Rovito

Submitted to the Institute for Data, Systems, and Society on May 12, 2016
in Partial Fulfillment of the Requirements for the Degree of Master of Science in Technology and Policy

ABSTRACT

Supply chains are critical to delivering components and products safely, affordably, and securely. However, these complex networks of suppliers, manufacturers, and customers are vulnerable to internal and external disruptions and subject to exploitation. This can result in adverse impacts to the system and inhibit value delivery. This thesis proposes a generic electronics supply chain model that can guide a user through different vulnerability assessment techniques and reveal information regarding system vulnerabilities as well as opportunities for decision-makers to intervene. The model draws upon a previously-developed Cause-Effect Mapping (CEM) analytic technique and assists with making decisions affecting complex systems, including those operating in resource-constrained environments. Elements of System Security Engineering (SSE) and Trusted Systems and Networks (TSN) analysis are taken into consideration, and leading indicators are utilized to provide a greater understanding of security concerns and impacts to a supply chain focusing on electronics for the defense industry. The model, adaptable to a diversity of systems and capable of recognizing non-obvious sources of vulnerability, can be used by systems engineers to provide a holistic view of a complex supply chain. The model facilitates the communication of information regarding supply chain vulnerabilities to decision-makers and other individuals.

Thesis Supervisor: Donna H. Rhodes
Title: Principal Research Scientist, Sociotechnical Systems Research Center
Director, Systems Engineering Advancement Research Initiative

ACKNOWLEDGEMENTS

There are many extraordinary people I would like to thank:

- To my advisor Dr. Donna Rhodes. Thank you for sticking with me during my transition from project manager to academic researcher, for sharing your wealth of systems engineering knowledge, and for motivating me to explore and expand my interests.

- To Dr. Adam Ross and my SEAri colleagues. Thank you for being a source of research insight, ideas, and inspiration.

- To everyone at Draper, especially Alex Edsall, Dan Keating, and Sandra Kassin-Deardorff. Thank you for providing me opportunities both as an MIT Research Assistant and Draper Laboratory Fellow. Without your constant and generous support, this thesis would not be possible.

- To Dr. Dava Newman, Dr. Frank Field, Barb DeLaBarre, Ed Ballo, and my TPP classmates. Thank you for challenging my thinking and enriching my MIT experience.

- To everyone at DC Road Runners, Community Running, and Turnstyle Cycle and my long run partner Theodora Skeadas. Thank you for instilling in me the tenacity and endurance to make it to the finish line of two marathons, one literal (New York) and one figurative (this thesis).

- To my parents Debbie and Tony Rovito and brothers Dr. R.J. and Tom Rovito. Thank you for your unwavering support of my educational and professional endeavors. I hope I made you proud.

- To my dear friends Eileen Searle and Brennan Scott for giving me a home in between leases and getting me away from campus on occasion; and Stephanie Davis and Dr. Marianne Lalonde for checking in on my abandoned husband and listening to me vent from afar. I cannot thank the four of you enough.

- To my husband Jim Piotrowski. Thank you so much for encouraging me to seize the chance to be a part of the MIT community and for sending me videos of fuzzy baby alpacas on bad days. I am in awe of your patience and insistence that I discover my hidden potential. I cannot wait to come home to Silver Spring and embark on many more adventures with you.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

AG	Attack Graph
AHP	Analytic Hierarchy Process
AIA	Aerospace Industries Association
ARM	Accelerated Requirements Method
ASIC	Application-Specific Integrated Circuit
ATA	Attack Tree Analysis
ATLIST	Attentive Listener
AURUM	Automated Risk and Utility Management
BCP	Business Continuity Planning
BIS	Bureau of Industry and Security
BN	Bayesian Network
CACP	Coalition Against Counterfeiting and Piracy
CAPEC	Common Attack Pattern Enumeration and Classification
CARVER	Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognizability
CBP	Customs and Border Patrol
CEM	Cause-Effect Mapping
CEM-VA	Cause-Effect Mapping for Vulnerability Analysis
CERL	Construction Engineering Research Laboratory
CJA	Crown Jewels Analysis
CP-IPT	Counterfeit Parts-Integrated Project Team
COG	Center Of Gravity
CONOPS	Concept of Operations
COTS	Commercial Off-The-Shelf
CPT	Conditional Probability Table
CREF	Cyber Resiliency Engineering Framework
CRRA	Cyber Risk Remediation Analysis
CTL	Center for Transportation and Logistics
C-TPAT	Customs-Trade Partnership Against Terrorism
CTSA	Cyber Threat Susceptibility Analysis

CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
DAG	Directed Acyclic Graph
DARPA	Defense Advanced Research Project Agency
DFAR	Defense Federal Acquisition Regulation
DFARS	Defense Federal Acquisition Regulation Supplement
DHS	Department of Homeland Security
DLA	Defense Logistics Agency
DMEA	Defense Microelectronics Activity
DoD	Department of Defense
DoDI	Department of Defense Instruction
DOE	Department of Energy
DOJ	Department of Justice
DVSS	Dynamic Vulnerability Scoring System
ERDC	Engineer Research and Development Center
FAA	Federal Aviation Administration
FAR	Federal Acquisition Regulation
FBI	Federal Bureau of Investigation
FDFI	Fault Detection/Fault Isolation
FMEA	Failure Mode and Effects Analysis
FMECA	Failure Mode, Effects and Criticality Analysis
FPGA	Field Programmable Gate Array
FTA	Fault Tree Analysis
GAO	Government Accountability Office
GEN	Good Expansion Network
GIDEP	Government Industry Data Exchange Program
GSA	Government Services Administration
HW	Hardware
IA	Information Assurance
IBIS	Issue-Based Information Systems

IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IPS	Intrusion Prevention System
ISR	Intelligence, Surveillance, and Reconnaissance
IVA	Integrated Vulnerability Assessment
JAD	Joint Application Development
JCTD	Joint Command Technology Development
LOE	Lines Of Effort
LOO	Lines Of Operation
MAE	Mission Assurance Engineering
MBSE	Model-Based Systems Engineering
MEII	Minimum Essential Information Infrastructure
MSHARPP	Mission, Symbolism, History, Accessibility, Recognizability, Population, and Proximity
MULVAL	Multihost, Multistage Vulnerability Analysis
NASA	National Aeronautics and Space Administration
NAVAIR	Naval Air Systems Command
NDAA	National Defense Authorization Act
NETSPA	Network Security Planning Architecture
NIPP	National Infrastructure Protection Plan
NIST	National Institute for Standards and Technology
NSA	National Security Agency
OCM	Original Component Manufacturer
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
OECD	Organisation for Economic Co-Operation and Development
OEM	Original Equipment Manufacturer
PPP	Program Protection Planning
PRO-IP	Prioritizing Resources and Organization for Intellectual Property
RAMBO	Resilient Architectures for Mission and Business Objectives
RFP	Request For Proposal
SA	Situation Awareness

SAE	Society of Automotive Engineers
SASC	Senate Armed Services Committee
SCEM	Supply Chain Event Management
SCRM	Supply Chain Risk Management
SEI	Software Engineering Institute
SHIELD	Supply Chain Hardware Integrity for Electronics Defense
SLA	Service Level Agreement
SME	Subject Matter Expert
SOA	Service-Oriented Architecture
SoS	System of Systems
SOW	Statement Of Work
SPIDERS	Smart Power Infrastructure Demonstration for Energy Reliability and Security
SQUARE	Security Quality Requirements Engineering
SRD	System Requirements Document
SSE	Security Systems Engineering
SSE	System Security Engineering
STAMP	Systems-Theoretic Accident Model and Process
STPA	Systems-Theoretic Process Analysis
SW	Software
TARA	Threat Assessment and Remediation Analysis
TSN	Trusted Systems and Networks
TTP	Tactics, Techniques, and Procedures
TVA	Topological Analysis of Network Attack Vulnerability
TVA	Topographical Vulnerability Analysis
USPS	U.S. Postal Service
VAM	Vulnerability Assessment & Mitigation
VAM	Vulnerability Assessment Method
VAMPG	Vulnerability Assessment Method Pocket Guide
VPN	Vulnerability Priority Number
WTO	World Trade Organization

CHAPTER 1: INTRODUCTION

"Vulnerable systems are likely to transition from stability to instability. Like a pencil on its tip, a vulnerable system will collapse if it experiences a sufficiently large deviation. By contrast, a stable system can restore itself to its equilibrium state when perturbed, like a pendulum. A system that is normally stable can become functionally unstable due to changes in global conditions or in relationships between the system's constituent elements" – Vedant Misra, Dion Harmon, and Yaneer Bar-Yam (Misra et al., 2010).

"Our committee's report makes it abundantly clear that vulnerabilities throughout the defense supply chain allow counterfeit electronic parts to infiltrate critical U.S. military systems, risking our security and the lives of the men and women who protect it. As directed by last year's Defense Authorization bill, the Department of Defense and its contractors must attack this problem more aggressively, particularly since counterfeiters are becoming better at shielding their dangerous fakes from detection" – U.S. Senator John McCain (United States Committee on Armed Services, 2012).

1.1. Summary

Predicting and mitigating system vulnerabilities and designing appropriate interventions can lead to the development of more resilient systems, capable of delivering a sustained level of value. This is especially important in the supply chain field, as supply chains are complex and vulnerable to both internal and external disruptions. A generic model focusing on electronics is developed incorporating features from Cause-Effect Mapping (CEM), an analytic technique that has been validated in previous research as a promising method for identifying cascading failures and system intervention points. The model is designed to address sources of supply chain risk identified through System Security Engineering (SSE), as well as to implement vulnerability analysis requirements specified through Trusted Systems and Networks (TSN) Analysis. A set of leading indicators for threats and susceptibility is developed as a redundant design feature to encourage further discovery of system weaknesses subject to exploitation. The model, able to be adapted to systems of interest by a wide range of individuals, provides insight into parts of the supply chain where an existing vulnerability can lead to mission failure, or the inability to deliver secure, reliable electronic components.

1.2. Motivation

An ideal supply chain ensures that materials or components can move safely, securely, and quickly to their intended destination at low cost. Managers are frequently tasked with making supply chains even more efficient, and this pressure has resulted in new methods and initiatives (Waters, 2011). These new methods, however, often introduce unexpected sources of vulnerability and unforeseen problems into a supply chain. One factor causing this to occur is the employment of lean initiatives and subsequent removal of slack within a supply chain, yielding a more inflexible, rigid supply chain than before. Vulnerability highlights how prone a supply chain is to be affected by risky events (Waters, 2011).

The supply chain utilized by the U.S. Department of Defense (DoD) is one of the largest, most complex, wide-reaching, and operationally volatile supply chains globally (Gansler et al., 2014). The DoD supply chain, which employs more than one million personnel, is responsible for the management of five million stock numbers across thousands of customer activities and information systems, all at a reported value of $98 billion dollars as of September 2013 (Parlier, 2011; Farahani et al., 2009; Government Accountability Office, 2015b). A typical component can travel from an Original Equipment Manufacturer (OEM) to an assembler, independent distributor or broker, prime contractor, subcontractor, or government depot before reaching its intended destination. Risk, ranging from "minimally consequential" to "potentially catastrophic" can arise from factors such as globalization, terrorism, and cyber warfare and numerous existing and potential security threats (Gansler et al., 2014). Risk resulting from the exploitation of vulnerabilities within a supply chain can affect the flow of physical products and materials as well as the flow of information and can compromise missions, endanger lives, or threaten national security (Van de Voort et al., 2007; Gansler et al., 2014).

Investigating vulnerabilities and how and where supply chains can be susceptible and exploited for financial and adversarial gain is of the utmost importance. Defense-related supply chains often rely upon Commercial Off-The-Shelf (COTS) products, which have their own complex supply chains; having in-depth knowledge of all component origins is nearly impossible. This is especially concerning given the multiplicity of inter-organizational relationships within a supply chain and the fact that systems engineers must account for the security of the system and the security of the supply chain (Farahani et al., 2009; Popick & Reed, 2013). COTS products may

be more likely to be vulnerable to attack and to contain counterfeit parts due to the unknown origins of internal components. It is worth noting the impact and prevalence of counterfeit parts, which jeopardize the security and reliability of complex systems and have adverse economic effects.

First and foremost, there is a lack of a holistic understanding of vulnerability as the concept pertains to complex systems. Furthermore, research has indicated a dearth of support tools providing analytical or methodological support capable of enabling companies to identify and account for vulnerability and resilience in their supply chains (Centre for Logistics and Supply Chain Management at the Cranfield School of Management, 2003). The research area has the potential for further exploration of system performance with respect to minimizing the impact of system perturbations, disruptions, and disturbances and for the development of new frameworks to address supply chain vulnerability and resilience (Nowakowski et al., 2015). This thesis seeks to contribute to resilient systems, through both the prevention and mitigation of vulnerabilities.

1.3. Research Approach

A multi-faceted research approach was adopted for the development of the generic model as shown in Figure 1-1. This approach considers inputs from previous research, literature, expert guidance, and existing methodologies for the assessment of system risk and vulnerability. These inputs inform CEM and allow for a targeted vulnerability analysis to be performed on case applications. The initial SPIDERS case application in Chapter 2 served as an introduction to the application of CEM, highlighting the level of effort required in order to fully understand a system and to perform a thorough analysis as well as testing CEM as a useful analytic technique. The supply chain case study in Chapter 5 involved a higher level of detail and analysis with a focus on socio-technical factors and extended the research to incorporate System Security Engineering (SSE), Trusted Systems and Networks (TSN) Analysis, and a derived set of leading indicators in addition to findings from expert judgment. This rendered an updated generic model capable of assessing system vulnerability and providing decision-makers with critical insights and information.

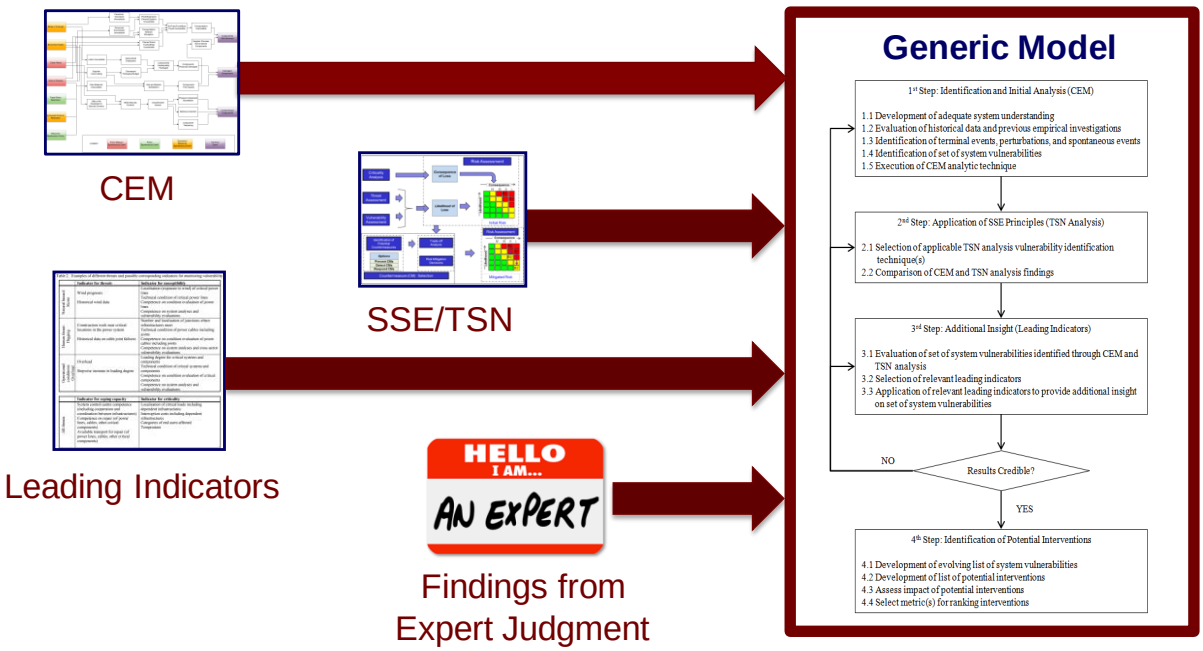


Figure 1-1. Research Approach.

1.4. Research Design

As shown in Figure 1-2, a research design emphasizing knowledge capture and synthesis was initially employed. An empirical approach was undertaken, studying past events to facilitate comprehension of current infrastructure dependencies and allowing for the identification of patterns of interest to policy and decision-makers (Johansson & Hassel, 2010). This can provide valuable information, such as the frequency at which failures cascade between infrastructures and the extent to which society is impacted by infrastructure failures (Johansson & Hassel, 2010). Requirements gathering, or using elicitation processes to collect system requirements from stakeholders and Subject Matter Experts (SMEs), drove the development of the integrated model framework and ultimately the pilot use of the generic model.

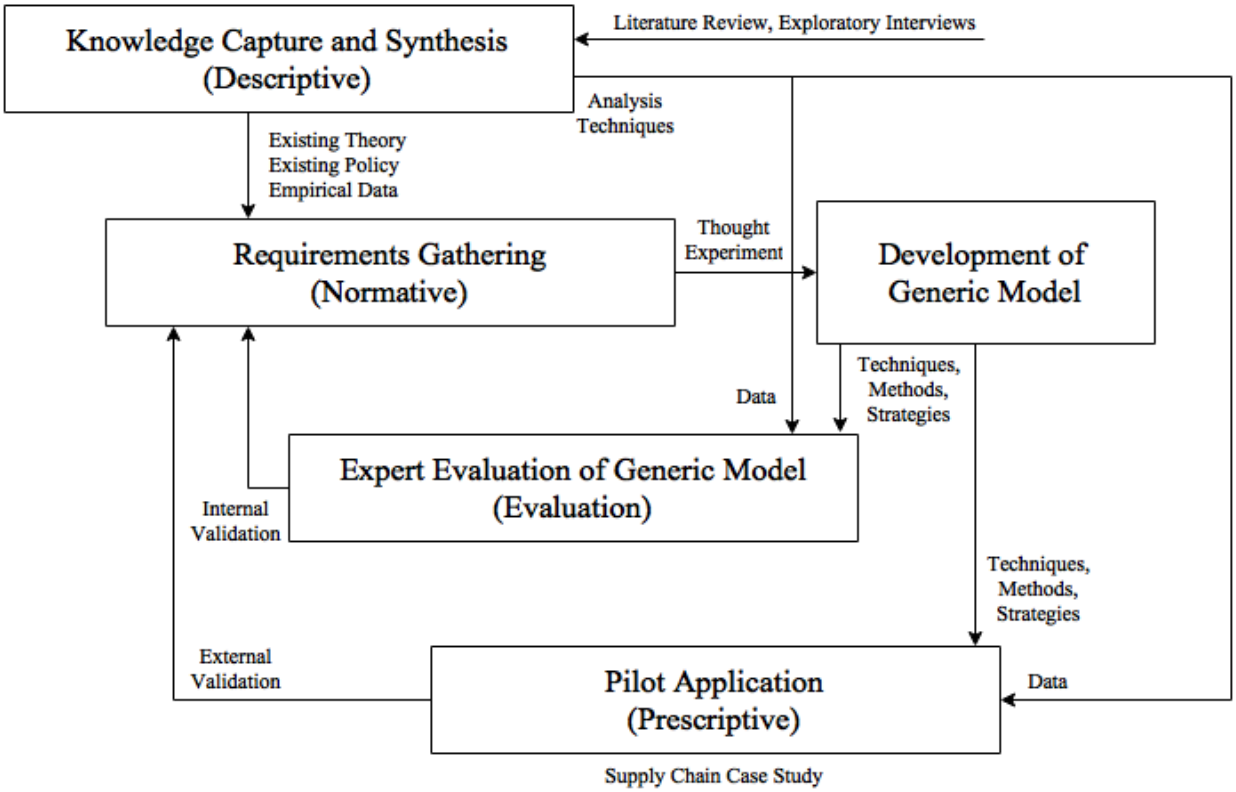


Figure 1-2. Research Design.

1.5. Research Questions

The focus of this thesis is to better understand where and how complex systems are vulnerable with the goal of better facilitating decisions allowing stakeholders to intervene and implement proper interventions. As such, this thesis is guided by three central research questions:

1. How can vulnerability assessment be defined within a complex engineering systems context?

2. What strategies can system architects use to identify "intervention points," or places within the system where causal chains can be disrupted to reduce or prevent vulnerabilities?

3. How can a comprehensive framework for vulnerability assessment facilitate better decisions with respect to uncertainty, resource constraints, and policy implications?

1.6. Research Contribution

The research contribution of this thesis is the in-depth exploration of vulnerability and vulnerability assessment as pertaining to complex systems and the development of a generic model capable of imparting holistic system-level understanding and of formulating a list of system vulnerabilities along with associated interventions allowing for informed decisions. In addition, a set of leading indicators is tailored and applied to a system as a means to uncover further sources of supply chain vulnerability. The sum of these contributions imparts the development of more resilient systems, which in turn has significant economic implications.

1.7. Thesis Structure

Chapter 2 provides an overview of complex systems and the previously-developed Cause-Effect Mapping analytic technique capable of identifying cascading failures and system intervention points (Mekdeci et al., 2012). Chapter 3 provides a survey of vulnerability and vulnerability assessment and explores a breadth of existing frameworks and methodologies. Chapter 4 expands into supply chain vulnerability and the development of the generic model (Rovito & Rhodes, 2016). Chapter 5 details the pilot application of the generic model. Chapter 6 presents an overview of policy issues surrounding risk and vulnerability assessment, taking into consideration both legislation and regulation. Chapter 7 recaps research findings, addresses the research questions presented above, and proffers recommendations for future work.

CHAPTER 2: COMPLEX SYSTEMS AND CAUSE-EFFECT MAPPING

Modern-day infrastructure systems are becoming increasingly complex and reliant on an ever-expanding network of components and suppliers (Nowakowski & Werbińska-Wojciechowska, 2014). These systems are designed with the expectation of delivering a constant level of value; however, they frequently encounter changing operational environments among other internal and external disruptions. A disruption, or instant, discontinuous change in state, can itself have a disastrous impact on a system and has the potential to yield a disturbance, or prolonged, continuous change in state (Mekdeci, 2013). An example of a disruption would be the sudden failure of a jet engine, while an example of a disturbance would be flying without an engine (Mekdeci et al., 2012). Both disruptions and disturbances are considered perturbations, or an unintentional change in state of a system's form, operations, or context that could put the system's value delivery in question (Mekdeci et al., 2012). Disruptions and disturbances in a system typically occur due to hazards and threats. These can stem from natural events, accidents or technical factors, market factors, policy factors, and human factors and result in the uncovering of system weaknesses and exploitation of system vulnerabilities (Kröger & Zio, 2011). Non-technical vulnerabilities, such as those concerning people and operations or those concerning a lack of clear policies and procedures, are especially important to take into consideration when assessing system viability.

2.1. Complex Systems

The resilience of complex systems to internal and external disturbances is of particular interest. A complex system can be thought of as a network, with the existence of paths (such as power lines or a transport route) between nodes (often a representation of physical components). These paths, or connections, are instrumental for the system to function properly. Removal of nodes or links, due to the malfunctioning of components or impact of disturbances, increases the length of a given path and can impede system performance. Systems exhibit different levels of resilience to such disturbances, and it is imperative to determine critical components necessary for the system to function (Latora & Marchiori, 2005).

Survivability is the ability of a system to minimize the effect of disturbances of finite duration on value delivery (Mekdeci et al., 2012). In this thesis, survivability is concerned with minimizing

the impact of a disruption (an instant, discontinuous change in state) as opposed to a disturbance (prolonged, continuous change in state) (Mekdeci et al., 2012). Focusing on the immediate shock or hazard to a system allows system architects to use appropriate design principles to influence the system's response and recovery and to restore value as quickly as possible (Mekdeci et al., 2012). The nature of disruption and the dynamics associated with a respective system's response can be characterized by eight phases as shown in Figure 2-1:

1. Preparation: In some scenarios, preventative measures can be taken to stave off disruption and to minimize system impacts.
2. The Disruptive Event: The event occurs, whether it involves a natural disaster, adversarial attack,
3. First Response
4. Initial Impact
5. Full Impact
6. Recovery Preparations
7. Recovery
8. Long-Term Impact (Blackhurst et al., 2005; Sheffi, 2007).

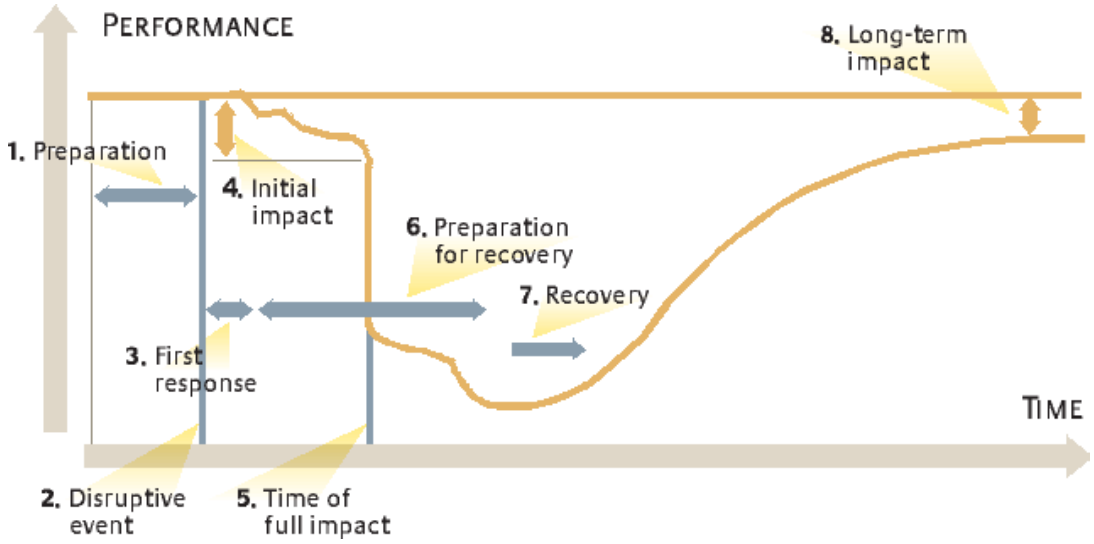


Figure 2-1. System Disruption Profile (Sheffi & Rice Jr., 2005).

This approach is similar to the three-phased approach for system survivability emphasizing avoidance, survival, and recovery from a disturbance as shown in Figure 2-2 (Richards, 2009). Three ways in which a system can be enhanced to ensure greater survivability include:

1. Decreasing the probability that the system will be impacted by a disturbance, otherwise referred to as a system susceptibility;
2. Decreasing the amount of value reduction directly attributable to the disturbance;
3. Increasing the ability of the system to recover in a timely manner, otherwise referred to as system resilience (Westrum, 2006).

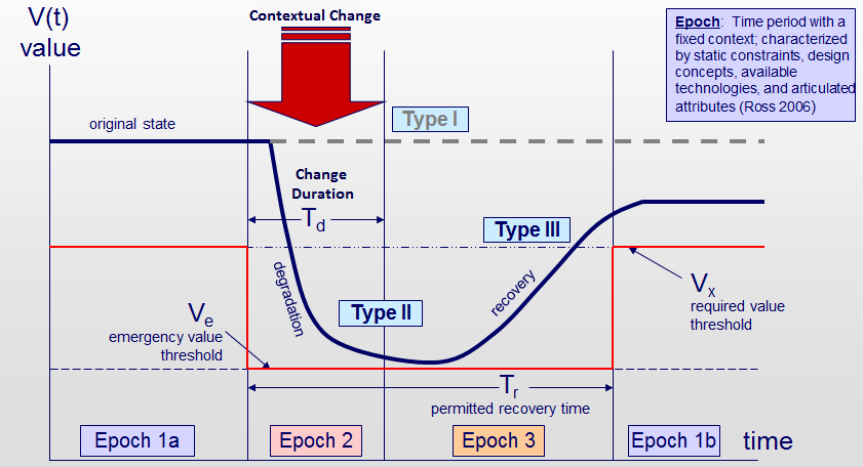


Figure 2-2. Definition of Survivability (Richards, 2009).

2.1.1. Existing Analysis Frameworks

Many techniques are currently used for reliability and safety analysis, including Fault Tree Analysis (FTA), Failure Mode and Effects Analysis (FMEA), and Failure Mode, Effects and Criticality Analysis (FMECA). The intent of FTA, first used to evaluate the Minuteman Launch Control System in 1961, is to translate the behavior of a physical system given failure into a visual diagram and logic model (Ericson, 1999). FTA is a top-down approach that utilizes Boolean algebra along with reliability and probability theory to analyze a system and establish the cause of a single failure, or effect (Fenelon et al., 1994). Since FTA is a deductive approach, starting with a failure state and working backwards towards individual events that may have been responsible, it does not always find all possible initiating faults.

Failure Mode Effects Analysis (FMEA) and closely-related Failure Mode, Effects and Criticality Analysis (FMECA) provide a standardized and systematic evaluation of potential failures through the employment of a bottom-up approach and focus on the loss of function of a component or capability rather than operational or human failures. FMEA/FMECA looks at initiating faults and attempts to determine their immediate and subsequent effects ("failures") on the overall system. Each system component is examined for possible things that could go wrong before the fact, rather than retroactively. FMEA/FMECA describes failure as the loss of an intended function of a device under stated conditions, which addresses component/capability failures but does not address operational perturbations (Langford, 1995).

FMECA takes the FMEA approach further by ranking each failure mode per severity classification and probability of occurrence (Hampl, 2010). In particular, FMECA lists single point failures and estimates the criticality of these failures. FMEA/FMECA does not consider human/software failures or combined (non-single point) failures (Federal Aviation Administration, 2004). Present methods focus on the technical system rather than considering the entire socio-technical system and fail to adequately visualize complex relationships.

Table 2-1. Comparison of CEM with Other Hazard Analysis Methods (Federal Aviation Administration, 2000; Hampl, 2010; Yu, 2011).

	Cause-Effect Mapping	**FTA**	**FMEA/FMECA**
Focus	Entire system	Failure outcome	Each system component
Methodology	Linkage of causes to perturbations to effects	Deductive, top-down method	Inductive, bottom-up method
Specialty	Identification of cascading failures and intervention points	Analyzing effects of initiating faults	Analyzing effects of single component or function failure
Strengths	Exposing causal flows	Showing system resistance to initiating faults, consideration of external events	Classifying initiating faults and identifying local effects
Weaknesses	Approach not yet mature	Finding all possible initiating faults	Examining multiple failures and effects at system level, lack of consideration of external events

Finally, Systems-Theoretic Accident Model and Process (STAMP) and Systems-Theoretic Process Analysis (STPA) are an accident model and hazard analysis technique, respectively, that both view safety as a dynamic control issue, not a component failure problem (Leveson, 2011). STAMP and STPA emphasize that failures can be prevented from the enforcement of safety constraints and promote the safety-driven design of systems. STAMP and STPA take causal factors leading to hazards into consideration through a chain-of-event causality model (Leveson, 2013). STPA can ultimately yield a larger set of causes, including those unrelated to failure or reliability and takes particular care to identify and analyze component interaction accidents.

2.1.2. Causality and Cascading Failures

Causality is said to apply whenever the occurrence of one event is expected within reason to lead to the incidence of another. A causal relationship is one in which the occurrence of a first event is a sufficient condition for the occurrence of a later event (Heise, 1975). Causes are related to effects by specifiable structures with precise locations in time and space, and the principle of causal inference is based on the logical implication involved in causality (Heise, 1975).

More formally, an event, C, causes another event, E, if and only if:

a. An operator exists which generates E, which responds to C, and which is organized so that the connection between C and E can be analyzed into a sequence of compatible components with overlapping event fields;
b. Occurrences of event C are coordinated with the presence of such an operator – such an operator exists within the field of C;
c. When conditions (a) and (b) are met, when the operator is isolated from the fields of events other than C, and neither C nor E is present to begin with, then occurrences of C invariably start before the beginning of an occurrence of E.
d. When conditions (a) and (b) are met, C implies E; that is, during some time interval occurrences of C are always accompanied by occurrences of E, though E may be present without C or both events may be absent (Heise, 1975).

Causal relationships can be linear or non-linear in nature. A linear causal relation is one in which events can be assessed in terms of magnitudes, effects due to different sources can be combined additively, and levels of effect are proportional to levels of cause after allowing for a constant

additive correction (Heise, 1975). Being able to capture a causal relationship in a linear manner permits the translation of variables into a form that depicts a relation between changes in values. However, not all causal relationships can be described as linear. Non-linear causal relationships can take the form of feedback loops and can be promulgated by system phenomena including oscillation, growth, decay, amplification, and control (Heise, 1975). Multiple causation, or when the value of an effect is determined by other causes in addition to the cause of interest, and multiple effects, or when one cause leads to a series of consequences, can further complicate causal relationships.

Infrastructure systems also are subject to cascading failures, or when the failure of one component propagates and leads to the failure of multiple components (Kröger & Zio, 2011). Applying this concept at the system-of-systems level, the failure of one system can lead to the failure of multiple systems. These failures result from the level of interconnectedness or dependency between two nodes or systems; the more tightly coupled, the more likely a failure is to propagate. An increased number of links can render a network or system more resistant to cascading failures but involves increased cost and complexity (Kröger & Zio, 2011). Recent disasters attributable to cascading failures include the Northeast Blackout of 2003, the Fukushima Daiichi nuclear plant disaster in 2011, and Hurricane Sandy in 2012.

2.2. Cause-Effect Mapping Analytic Technique

Cause-Effect Mapping (CEM) is an analytic technique for identifying cascading failures and system intervention points (Mekdeci et al., 2012). Causal chains, terminal conditions, and intervention points are employed to model a system and illustrate pathways where causes and effects of small failures or attacks (perturbations) can propagate and interact. This can lead to critical system failures. CEM is capable of highlighting the complex, non-linear relationships between causes and effects of perturbations and serves as a mechanism for system architects to identify intervention points, or places within the system where causal chains can be disrupted to reduce vulnerabilities. At these places in the system, decision makers can enact strategies to prevent the occurrence of terminal events through the avoidance and mitigation of and recovery from the root-cause perturbations (Mekdeci, 2013). CEM is intended to complement and address gaps within other techniques such as FTA and FMEA/FMECA and to be useful to systems at any level of abstraction.

A brief overview of taxonomy is required before launching into discussion of CEM. A spontaneous event is an event that occurs outside of a system's control, typically without warning. Spontaneous events can be exogenous (natural disaster, terrorist attack) or endogenous (operator error, component failure) in nature. These initiating events can also be characterized as a disruption, or a discontinuous state change that is unintended and instantaneous; or as a disturbance, or a continuous state change that is unintended and of finite duration (Mekdeci et al., 2012). A perturbation is a change in state of the operation, form, or context of a system and has the potential to adversely impact value delivery. Both disruptions and disturbances are considered perturbations and jeopardize system functionality. Moreover, a terminal event results from one or a series of perturbations and involves reaching a set of conditions that is not survivable for the system.

CEM takes advantage of the fact that anything causing a reduction in system value has at least one cause and one effect. Each cause is a set of conditions that leads to a perturbation, which in turn leads to an effect, or direct change in context and/or the system. The ability to separate perturbations into cause and effect is "critical" since it permits systems architects to focus on causes and effects having the greatest impact on system survivability (Mekdeci et al., 2012). CEM provides the capability to consider multiple causes of a perturbation as well as multiple effects. While FTA and FMEA/FMECA typically draw upon knowledge gleaned from existing designs, CEM has the added capability to find all possible initiating faults and consider human/software and combined failures (Mekdeci, 2013). Finally, a system designer must be conscious of the "unknown unknowns," or the fact that the exact cause of a perturbation may not be known. Often, unknown unknowns are best addressed in a system through robust solutions to known problems.

CEM is used to develop a list of perturbations of interest and to determine possible points of intervention where strategies can be applied. A CEM traces the multiple causes and effects of perturbations from spontaneous events (those outside of the system's control), through intermediate events, to terminal conditions. Spontaneous events are often exogenous (i.e., outside system boundary), such as changes in the weather or the action of an outside entity. Spontaneous events can also be endogenous, such as a random component failure or operator error. Spontaneity is not absolute, but rather is relative to the system.

Conducting a CEM typically begins with a terminal event, which is one that results in unacceptable and unrecoverable loss of system value delivery. The causes of that event are added to the map as perturbations of interest and a single arrow from each of the causes to terminal event is drawn. If any of the causes of the terminal event are not spontaneous events, then their causes, along with appropriate arrows, are added to the map as additional perturbations of interest. Next, each perturbation of interest is examined for additional causes and effects. Arrows are drawn to any causes and effects already on the map and new perturbations are added, as necessary. This process continues until each perturbation is indicated as being caused by a spontaneous event, and eventually traces to a terminal event. If a perturbation cannot eventually lead to a terminal event, then it is not worth considering and should be removed from the CEM.

CEM is useful for system architects to determine intervention points where the system or supporting enterprise can implement strategies that prevent terminal events from occurring by avoiding, mitigating and recovering from the perturbations that cause them. In particular, system architects should try to intervene and break reinforcing loops to prevent cascading failures. Similarly, because it is harder to recover from perturbations that have multiple effects, emphasis on prevention and mitigation of these perturbations would be advised. Like causal diagrams used in system dynamics, CEM includes consideration of non-linear relationships, including reinforcing loops.

Since a system is unlikely to be able to address all perturbations under consideration, CEM is useful for prioritizing certain perturbations based on whether they have multiple effects and/or are part of reinforcing loops. With such an analysis, even trivial perturbations, such as setting an incorrect waypoint for a UAV, can be shown to have a large impact. This analysis also allows the prioritization of intervention strategies by allowing them to be qualitatively compared based on where in the causal map they are effective. For example, a CEM analysis might show increasing the level of technology seems to be a potential solution to many perturbations, and therefore may be more valuable overall than an intervention that only addresses a single perturbation. Causal diagrams also help system architects deal with “unknown unknowns,” or perturbations that are not explicitly considered. Sometimes the solution to a known problem is also the solution to an unknown problem. For example, an authentication procedure for an e-commerce website can not only protect against fraud or other security compromises, but also

may prevent unintentional purchases by legitimate users (i.e., errors). Instead of focusing on the causes, it may be more fruitful to focus on the effects, specifically the main effects.

Potential uses of CEM include the following:

- Showing multiple causes and multiple effects.
- Identifying perturbations that could result in cascading failures.
- Prompting system architects to recognize relationships that may not have been obvious.
- Augmenting traditional hazard analysis methods, such as FTA/FMEA/FMECA.
- Identifying similar perturbations that could be mitigated using same/similar strategies.
- Guiding top-down and bottom-up tracing of causal chains that end in terminal events.
- Encouraging system architects to think about causal chains beyond technical factors to include multiple facets such as social, political, cyber-operations, etc.

2.3. CEM-VA Process

CEM highlights dynamics regarding how perturbations within a system propagate and enables system architects to visually discern possible intervention points. In these spots, strategic action can be taken to avoid, mitigate, or survive a given perturbation. Systems architects tend to operate in resource-constrained environments, however, and must be selective in the strategies ultimately chosen for implementation. Special attention should be paid to the amount of time, money, and other resources involved with a potential mitigation; design constraints and boundary conditions may be factors as well.

Finding interventions to avoid perturbations that result from multiple causes as well as perturbations that result in multiple effects is a top priority for system architects. The identification of and intervention against reinforcing loops is of critical importance, as perturbations in such a loop can lead to cascading failures. Finally, CEM can assist systems architects in addressing "unknown unknowns," or perturbations that cannot be anticipated or planned for. On occasion, mitigations addressing known causes and effects of perturbations can be helpful in reducing the impact of unknown causes and effects as well.

A four-step process, *Cause-Effect Mapping for Vulnerability Analysis* (CEM-VA), was developed for an individual with basic knowledge of a system to apply CEM and identify intervention points. This process assists a user in performing analysis and is exclusive to the application of CEM, an analytic technique. The process is shown in Figure 2-3.

The first step of applying CEM-VA focuses on knowledge gathering and investigation, along with defining the scope of the assessment upon the system of interest. Literature review, discussion with Subject Matter Experts (SMEs), and experiential learning serve as inputs and lead to the identification of the system of interest along with a set of terminal events.

Step 2 of CEM-VA takes the terminal events and uses backwards induction to develop a set of intermediate perturbations and spontaneous events.

All of the knowledge necessary to perform a comprehensive CEM has been acquired at this point, and Step 3 of CEM-VA leads the user task-by-task to create a CEM diagram.

Finally, Step 4 continues the analysis with respect to vulnerability, prompting the user to identify potential intervention points and viability strategies. While a user can go through the four steps once and perform a complete vulnerability assessment using CEM, the process can provide especially optimal results through the incorporation of feedback and additional iteration:

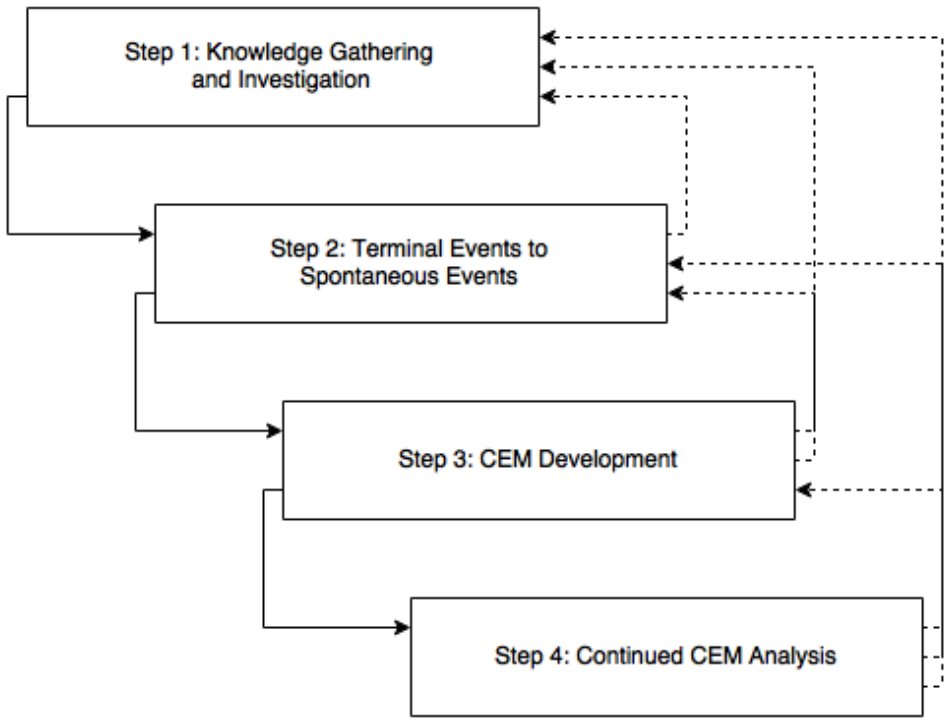


Figure 2-3. CEM-VA Process.

The first step of applying CEM-VA focuses on knowledge gathering and investigation, along with defining the scope of the assessment upon the system of interest. Inputs including literature review, discussion with Subject Matter Experts (SMEs), and experiential learning lead to the identification and scoping of the system of interest and identification of terminal events.

Inputs

- 1.I.1 Literature review.
- 1.I.2 Discussion with Subject Matter Experts (SMEs).
- 1.I.3 Experiential learning (site visits, etc.).

Activities

- 1.A.1 Identify system of interest.
- 1.A.2 Define scope of assessment upon system of interest.
- 1.A.3 Identify terminal events.

Outputs

- 1.O.1 Identification and increased understanding of system of interest.
- 1.O.2 Identification of terminal events.

Once the system of interest has been clearly defined and bounded and terminal events identified, the assessment can shift to using backwards induction to move from the terminal events to spontaneous events through the identification of perturbations. This ultimately provides all of the knowledge necessary to perform CEM:

Inputs

- 2.I.1 Terminal events.

Activities

- 2.A.1 Utilize backwards induction to step from terminal events to identify perturbations and event sequences.
- 2.A.2 Utilize backwards induction to step from perturbations and event sequences to identify spontaneous events.

Outputs

- 2.O.1 Perturbations.
- 2.O.2 Spontaneous events.

CEM can finally take place given the full set of spontaneous events, perturbations, and terminal events. Working backwards to identify connections between the three categories of events will result in the creation of a formal CEM diagram:

Inputs

- 3.I.1 Terminal events.
- 3.I.2 Perturbations.
- 3.I.3 Spontaneous events.

Activities

- 3.A.1 Create diagram with terminal events, perturbations, and spontaneous events.
- 3.A.2 Work backwards to identify connections from terminal events to perturbations.
- 3.A.3 Work backwards to identify connections from perturbations to spontaneous events.
- 3.A.4 Refine and elaborate on interdependencies between initial spontaneous events, perturbations, and terminal events and causal event sequences.
- 3.A.5 Create cause-effect mapping diagram from identified spontaneous events, perturbations, and terminal events and associated event sequences.

Outputs

- 3.O.1 Cause-Effect Mapping Diagram.

Once the CEM diagram is developed, additional analysis is performed in order to identify causal chains, cascading failures, and potential intervention points as well as to formulate possible viability strategies. This completes the objectives of the CEM analytic technique:

Inputs

- 4.I.1 Cause-Effect Mapping Diagram.

Activities

- 4.A.1 Evaluate impact of initial spontaneous events and disruptions on perturbations and system as a whole.
- 4.A.2 Refine and elaborate on interdependencies between initial spontaneous events, perturbations, and terminal events.
- 4.A.3 Examine perturbations from a nested contextual viewpoint.
- 4.A.4 Identify causal chains and cascading failures.
- 4.A.5 Identify potential intervention points.
- 4.A.6 Identify strategies for the avoidance and/or survival of a given perturbation.

Outputs

- 4.O.2 Identification of causal chains and cascading failures.
- 4.O.3 Identification of potential intervention points.
- 4.O.4 Formulation of viability strategies.

The CEM-VA four-step process provides a set of activities with discrete steps allowing for a systems-level analysis. This encompasses the identification of vulnerabilities and intervention points and the implementation of strategies with the potential of increasing system resiliency. The step-by-step process facilitates the implementation of CEM and guides the user in identifying an appropriate scope of a system for analysis, identifying spontaneous through terminal events, and developing a comprehensive CEM for further analysis.

2.4. SPIDERS Case Study Application

CEM and the developed CEM-VA process were applied to a case study focusing on the Smart Power Infrastructure Demonstration for Energy Reliability and Security (SPIDERS) microgrid project to secure military installations. This case study demonstrated the usefulness of CEM as

an analytic technique and laid the foundation for additional vulnerability-analysis related research.

The objective of the SPIDERS Joint Command Technology Development (JCTD) project, an effort involving the United States Department of Energy (DOE), Department of Defense (DoD), and Department of Homeland Security (DHS), is to protect defense critical infrastructure from power loss due to physical disruptions or cyber attack to the bulk electric grid. SPIDERS is working to increase electric power surety through the development of microgrid architectures that can function independently of the commercial electric grid.

SPIDERS is an ideal case to demonstrate the usefulness of CEM since the U.S. electricity grid is critical to DoD mission execution and vulnerable to disruption, whether due to natural events or human factors (Government Accountability Office, 2015a). The commercial electric grid provides ninety-nine percent of DoD's electrical power, and the vast majority of essential functions depend on infrastructure outside of DoD's control (Samaras & Willis, 2013). The absence of a systems approach to energy security has the potential to result in the unavailability of essential capabilities, additional expenses, and unrealized synergies and cost savings.

2.4.1. Background

The aging domestic commercial electricity grid has contributed to prolonged interruptions in service, to which military installations are not immune. DoD facilities have experienced utility disruptions due to hazards including mechanical failure and severe weather resulting in significant operational and fiscal impacts (Government Accountability Office, 2015a). The DoD reported 180 utility disruptions lasting 8 hours or longer in fiscal year 2013, with an average financial impact of $220,000 per day (Government Accountability Office, 2015a). For example, the storm surge from Hurricane Sandy destroyed utility infrastructure at Naval Weapons Station Earle, New Jersey, impacting potable and wastewater service and resulting in almost $26 million dollars in expected repair costs (Government Accountability Office, 2015a). The DoD is also concerned with physical and cyber threats, as a threat similar to the "Stuxnet" computer virus that attacked the nuclear program in Iran in 2010 could affect installations' industrial control systems (Government Accountability Office, 2015a).

Upgrades are needed in order to provide consistent, reliable electricity to the DoD and civilians. The DoD has undertaken several initiatives, including SPIDERS, to better assess and understand infrastructure vulnerabilities and to ensure continued access to utilities (Government Accountability Office, 2015a). SPIDERS seeks to protect defense critical infrastructure from power loss through the deployment of islanded microgrids, enabling a facility to operate independently for extended periods with maximum assurance that cyber security is uncompromised (Government Accountability Office, 2016b). SPIDERS is being implemented in four phases, and the final phase of this project focuses on microgrid and renewable energy technologies transferable to the commercial sector.

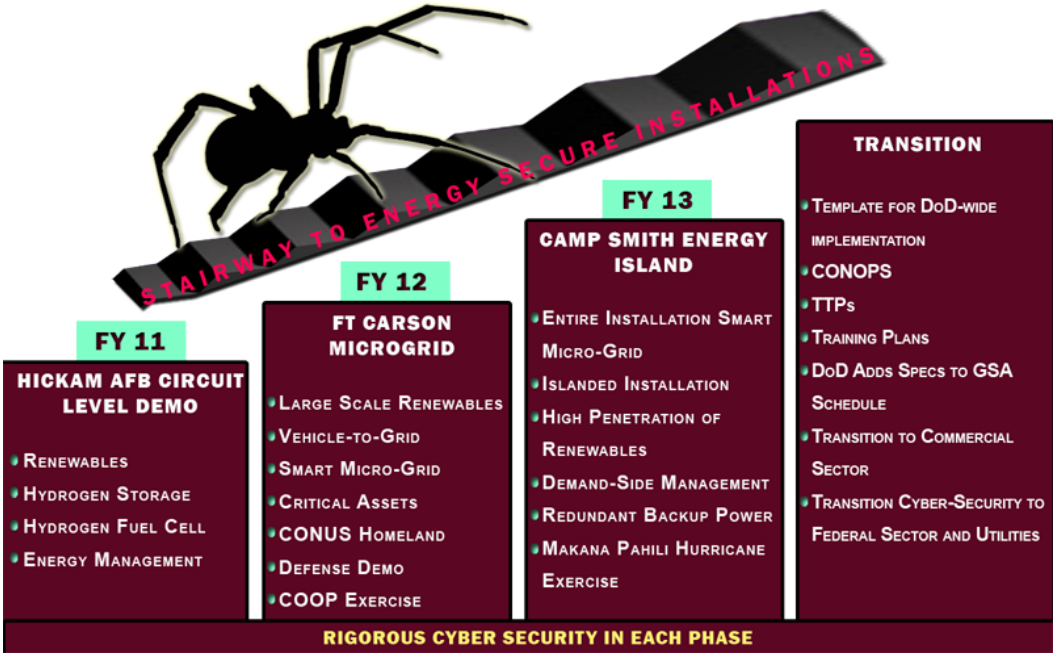


Figure 2-4. SPIDERS Stairway to Energy Secure Installations (Sandia National Laboratories, 2015).

2.4.2. Application of CEM-VA Process

CEM was applied to SPIDERS Phase 2 (the Ft. Carson microgrid installation) with a focus on cybersecurity. The goal of applying this analytic technique is to investigate the ability to maintain operational surety through secure, reliable, and resilient electric power generation and distribution to mission-critical loads. As prescribed in *Step 1: Knowledge Gathering and Investigation*, a thorough literature review was performed on microgrids, and interviews were

conducted with SMEs including Dennis Darcy (Draper Laboratory) and Melanie Johnson (Assistant Technical Manager, U.S. Army Engineer Research and Development Center (ERDC)-Construction Engineering Research Laboratory (CERL)). This led to increased understanding of SPIDERS and the scope of the CEM as well as the identification of Electric Grid Failure as a terminal event.

Step 2: Terminal Events to Spontaneous Events via Backwards Induction enabled the systems analysis to step backwards from the single Electric Grid Failure terminal event to a series of perturbations and ultimately four spontaneous events impacting the system.

Following the recognition of these events, *Step 3: CEM Development* was executed, resulting in the artifacts shown in Figure 2-5 below and Table A-1:

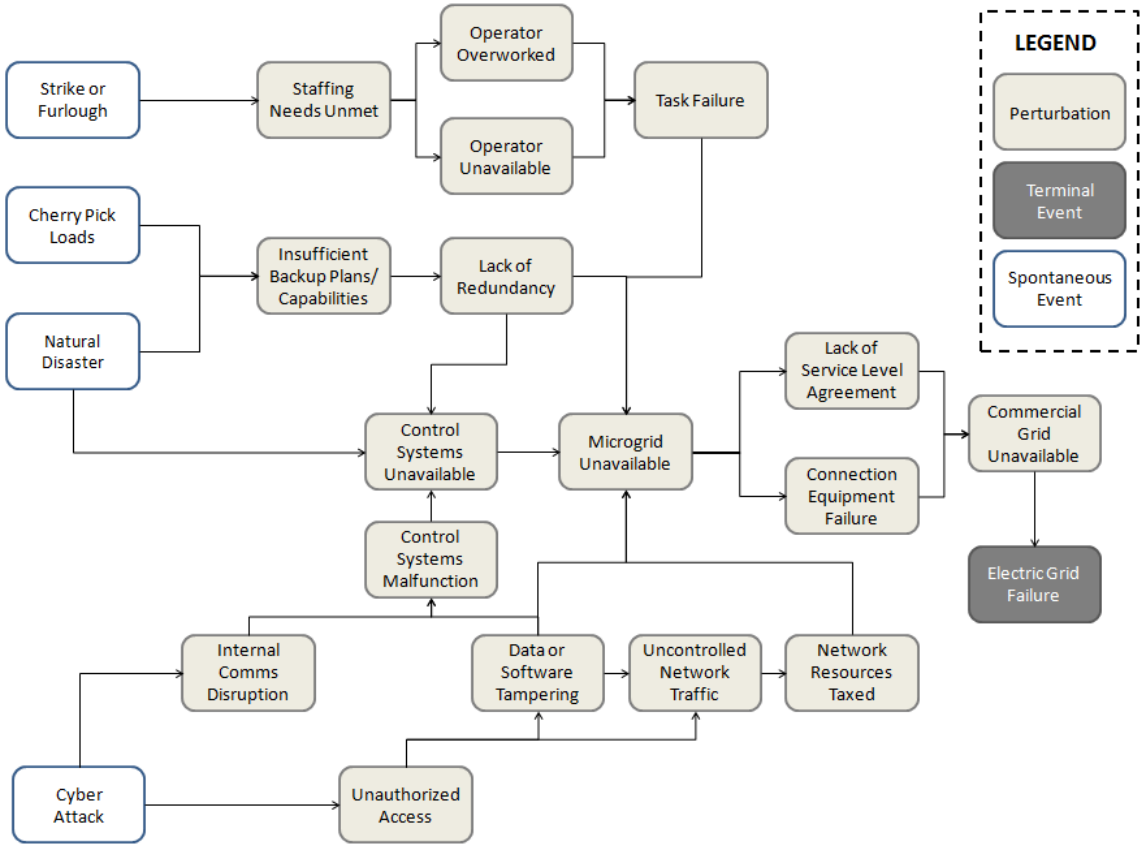


Figure 2-5. Cause-Effect Mapping Diagram of SPIDERS Phase 2.

Step 4: Continued CEM Analysis, provides insight into possible intervention points where strategies can be implemented to prevent terminal events from taking place. These strategies

allow the system to avoid, mitigate, or recover from perturbations. The identification of reinforcing loops (non-linear relationships) is of particular interest, so that these can be broken in an effort to prevent cascading failures. Prevention and mitigation of perturbations with multiple effects is also paramount in this process.

Seven different points for intervention were explored. Five are closely related to cyber security concerns and software, while two are more policy-oriented. Taking simple, straightforward measures to write robust software, ensure proper authentication, secure confidential information, and prevent network sniffing and spoofing attacks can help to prevent Unauthorized Access and Internal Comms Disruptions, along with associated perturbations Data or Software Tampering, Uncontrolled Network Traffic, and Control Systems Malfunction. Backup plans and Service Level Agreements (SLAs) fall to the organization possessing ownership of the microgrid, in this case the U.S. Government.

The seven possible intervention points are identified in the SPIDERS CEM shown in Figure 2-6; a sampling of possible intervention strategies is characterized in Table A-2:

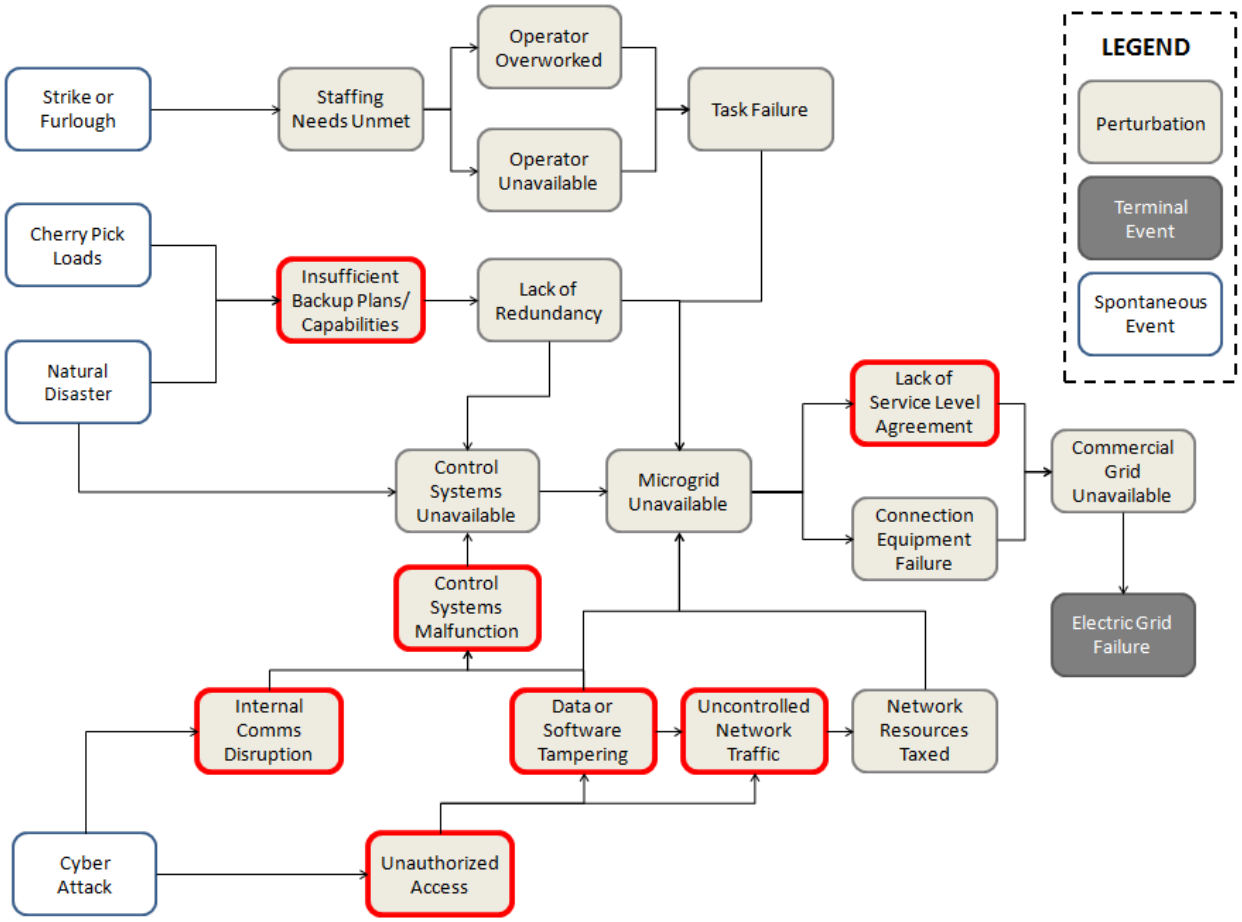


Figure 2-6. Cause-Effect Mapping Diagram of SPIDERS Phase 2 with Intervention Points.

2.5. Findings from Initial CEM Application

The SPIDERS case highlights the potential applications of CEM as well as the need for a systems approach to energy security in order to maintain operational surety through secure, reliable, and resilient electric power generation and distribution to mission-critical loads. Inputs from existing formal vulnerability assessment frameworks, including the Security Quality Requirements Engineering (SQUARE) method and the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Allegro method informed this research, particularly in the areas of defining security goals and developing relevant artifacts. These frameworks will be discussed further in Chapter 3.

Insight can be gained through CEM by examining the resulting mapping, which helps to illustrate the reinforcing loops (non-linear relationships) and potential cascading failures.

Intervention points can be more easily identified, so that strategies can be designed and enacted to prevent terminal events from taking place. These strategies allow the system to avoid, mitigate, or recover from the effects of a given perturbation. The prevention and mitigation of perturbations with multiple effects is imperative, and the CEM diagram provides a means for an analyst to have a big picture, holistic perspective on possible interventions and their impacts.

CEM has the potential to help ensure that a mission remains executable in a resource-constrained environment given an appropriate level of investment in interventions to mitigate vulnerabilities. The implementation of CEM can be facilitated through step-by-step guidance provided by the CEM-VA process. This framework, developed for guiding a user with basic knowledge of a system and the concept of vulnerability, assists the user in identifying an appropriate scope of a system for analysis, identifying spontaneous through terminal events, and developing a comprehensive CEM for further analysis. CEM will continue to evolve given follow-on research and to potentially fill the gap as an effective analytic technique for fostering increased system understanding of vulnerabilities and interventions. This work has set the foundation for further study of the vulnerability analysis of complex systems as demonstrated in Chapters 3 and 4.

CHAPTER 3: VULNERABILITY AND VULNERABILITY ASSESSMENT

3.1. Vulnerability

Both the concept of vulnerability and the current threat landscape continue to evolve (Peck, 2006; Trend Micro, 2015). This thesis adopts Kröger & Zio (2011)'s definition of vulnerability as a flaw or weakness (inherent characteristic, including resilience capacity) in the design, implementation, operation, and/or management of an infrastructure system, or its elements, that renders it susceptible to destruction or incapacitation when exposed to a hazard or threat, or reduces its capacity to resume new stable conditions. Vulnerability focuses on three main elements:

- The degree of loss and damages due to the impact of a hazard.
- The degree of exposure to a hazard.
- The degree of system or component resilience (Kröger & Zio, 2011).

Vulnerability can be thought of as the ability of a system to withstand strains or as a physical feature or operational attribute that renders an entity subject to exploitation or susceptible to a hazard (Johansson & Hassel, 2012; U.S. Department of Homeland Security, 2008). Vulnerabilities can be exploited by a threat to defeat a system's objectives or to significantly degrade performance. All systems, networks, and applications can be vulnerable or possess inherent vulnerabilities; these vulnerabilities can be intentional (implanted logic) or unintentional (capable of being maliciously exploited) (Reed, 2014b; Reed, 2014a). Vulnerability depends not only on the occurrence of or exposure to an event, but the extent to which system reliability is affected as well (Francis & Bekera, 2014).

Awareness of vulnerabilities that could potentially enable malicious activities capable of interfering with a system's operation should be raised through a system's design, development, testing, production, and maintenance (Deputy Assistant Secretary of Defense for Systems Engineering & Department of Defense Chief Information Officer, 2014). Vulnerabilities recognized early in the system design process often can be eliminated or mitigated through simple design changes or procurement constraints at low cost (Deputy Assistant Secretary of Defense for Systems Engineering & Department of Defense Chief Information Officer, 2014). Efforts to mitigate system vulnerabilities later on may require more costly and less effective add-

on protection measures or operational constraints (Deputy Assistant Secretary of Defense for Systems Engineering & Department of Defense Chief Information Officer, 2014).

Quantitatively, vulnerability concerns the degree of damages and losses due to the impact of a hazard, the degree of exposure to the hazards (including the likelihood of being exposed to hazards of a given degree and the susceptibility of a component at the risk of incurring damages and losses), and the degree of resilience (the ability of the system to anticipate, absorb/cope with, resist, and recover from the impact of an adverse event) (Koonce et al., 2008; Zio et al., 2011). The measurement of vulnerability must reflect social processes in addition to material outcomes within systems that appear to be complex and to contain many linkages that are difficult to nail down (Nowakowski et al., 2015). Therefore, vulnerability is not easily reduced to a single metric (Nowakowski et al., 2015; Adger, 2006). Vulnerability can be measured quantitatively on a metric scale, in terms of a specified currency, or qualitatively on a non-numeric scale, based on social values or perceptions (Sterlacchini, 2011; Glade, 2003). For risk assessment within the framework of vulnerability analysis, risk can be quantitatively expressed through a numeric likelihood and consequence (Kröger & Zio, 2011).

Vulnerability is closely related to the concepts of redundancy and resilience (U.S. Department of Homeland Security, 2008; Steen & Aven, 2011; Nowakowski et al., 2015). Redundancy is possessing additional or alternative systems, assets, or processes that can allow a system to maintain a degree of overall functionality given an adverse event or failure (U.S. Department of Homeland Security, 2010). A lack of redundancy can be thought of as a vulnerability that can result in a higher probability of a successful attack, as system functionality will likely be compromised (U.S. Department of Homeland Security, 2010). Resilience is the ability of a system to adapt to changing conditions and to prepare for, survive, and rapidly recover from disruption (U.S. Department of Homeland Security, 2010). Reducing vulnerability entails reducing the likelihood of a disruption and increasing resilience (Sheffi & Rice Jr., 2005). Resilience, whether through tolerating or absorbing system impacts, can reduce the consequences associated with an incident or event and can also impact the likelihood that an incident or event happens at all (U.S. Department of Homeland Security, 2010). Building resilient capabilities into a system can effectively act as a deterrent, preventing the exploitation of existing vulnerabilities.

Within the research literature, there are two main interpretations of the concept of vulnerability (Johansson & Hassel, 2010). The first considers vulnerability in a similar vein as risk, namely as an overarching system property that manifests the extent of adverse effects resulting from the occurrence of a given hazardous event. Vulnerability is still differentiated from risk in this interpretation, as the identification of risk scenarios depends upon a specific hazardous event taking place. The second portrays vulnerability as characterizing a system component or an aspect of a system. A component can be viewed as a vulnerability of a system given that failure of the component yields significant negative consequences to the system. This component can be labeled as a critical component, and the associated perspective can be extended to describe vulnerabilities relevant in a critical geographic location. The co-location of components belonging to different infrastructure systems can lead to additional criticalities, as an event that occurs in the same location (i.e., inclement weather or an act of terrorism) can adversely impact multiple systems.

An important distinction is that between vulnerability and risk. While both vulnerability and risk assessments are critical tools for the proactive management of risk and crises, the meaning of the concepts and the relationship between them varies based on a given discipline (Johansson & Hassel, 2010). Pettit et al. (2010) define risk as a combination of the likelihood of an event and its potential severity. Risk involves uncertainty, specifically about the extent of the consequences of an activity (Aven, 2011). The National Institute for Standards and Technology (NIST) characterizes risk as a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence (U.S. Department of Commerce National Institute of Standards and Technology, 2012). Risk assessment is further defined as incorporating threat and vulnerability analyses while considering mitigations from implemented security controls (U.S. Department of Commerce National Institute of Standards and Technology, 2012). Therefore, this thesis considers vulnerability assessment to be one component of a comprehensive risk analysis and advocates that vulnerabilities be addressed in a broad manner encompassing the threats and hazards that may lead to exploitation (Aven, 2007; Johansson & Hassel, 2010).

3.2. Vulnerability Assessment

Vulnerability Assessment is the study of the characteristics of a system in order to discern vulnerabilities and can be used to evaluate and record vulnerabilities that may impede or degrade the performance or capabilities of a system. The primary purpose of a vulnerability assessment is to identify physical features or operational attributes that can render an entity, asset, system, network, or geographic area susceptible or exposed to hazards; ideally, a vulnerability assessment will yield estimates of vulnerabilities across a spectrum of hazards or assets, systems, or networks (U.S. Department of Homeland Security, 2008). The translation of hazard levels into information regarding vulnerability into risk levels is a crucial step in system risk assessment (Sterlacchini, 2011). In this thesis, a vulnerability assessment is assumed to be equivalent to a vulnerability analysis.

A vulnerability assessment can uncover weaknesses, or areas in which a critical function can be exploited with the intent of preventing or degrading the system's operation, in system design, development, production, components, operation, and supply chain (Popick & Reed, 2013). A vulnerability assessment should address who or what is vulnerable, along with how it is vulnerable (Schnaubelt et al., 2014). The two main outputs of a critical infrastructure vulnerability assessment are the identification of critical elements and the quantification of system vulnerability indicators (Kröger & Zio, 2011). The information provided by these outputs is complementary; while vulnerability indicators are parameters encompassing static and/or dynamic characteristics of an overarching system, the determination of critical elements comes from their rankings with respect to their individual connectivity efficiency and/or their impact on the propagation of failures, with their effects, through the network (Kröger & Zio, 2011).

Potential vulnerabilities can be identified through studying requirements and examining critical functions and system concepts for access paths (Popick & Reed, 2013). This can be accomplished through listing system vulnerabilities as specified in industry databases or leveraging Information Assurance (IA) and System Security Engineering (SSE) expertise and guidance. Failure modes, or sources of vulnerability, of particular interest for supply chain applications include disruption in supply, disruption in transportation, disruption at facilities, freight breaches, disruption in communications, and disruption in demand (Sheffi et al., 2003). Additional sources of

vulnerability include interoperability, information sharing, collaboration, design imperfections, and system limitations (Antón et al., 2004).

Qualitatively, a vulnerability assessment is considered to be one step of a general risk assessment (Moore, 2006; Kröger & Zio, 2011). The vulnerability assessment typically occurs after hazard and threat assessment but before risk assessment and involves the identification of potential vulnerabilities (Kröger & Zio, 2011). The amount of vulnerability is evaluated in one of two ways: (I) by the formulation of risk scenarios, or (II) on the basis of asset protections (Kröger & Zio, 2011). The higher the consequence and attractiveness ranking, the more likely a scenario-based vulnerability assessment approach, which assigns risk rankings to developed scenarios, is to be applied (Kröger & Zio, 2011). Alternatively, an asset-based vulnerability assessment approach can yield a target ranking value based on the consequences and attractiveness of an asset (Kröger & Zio, 2011).

A vulnerability assessment is often conducted in the following manner:

- Assets and capabilities are listed, along with the threats against them.
- Common criteria for assessing vulnerabilities are determined.
- The vulnerability of assets and capabilities is evaluated (Schnaubelt et al., 2014).

It is worthwhile to note that vulnerability evaluation criteria can include the degree to which an asset may be impacted or disrupted, the quantity available of an asset given that replacement is required due to loss, dispersion (geographic proximity), and key physical characteristics (Schnaubelt et al., 2014).

A comprehensive vulnerability assessment requires consideration of a broad spectrum of hazards and threats, including failures, in addition to interacting, spatially-distributed elements with non-linear behavior and feedback loops. Three main activities for a vulnerability analysis are proposed:

- System analysis including system properties.
- Quantification of system vulnerability indicators and identification of important elements.
- Application to technical or organizational system improvements (Kröger & Zio, 2011).

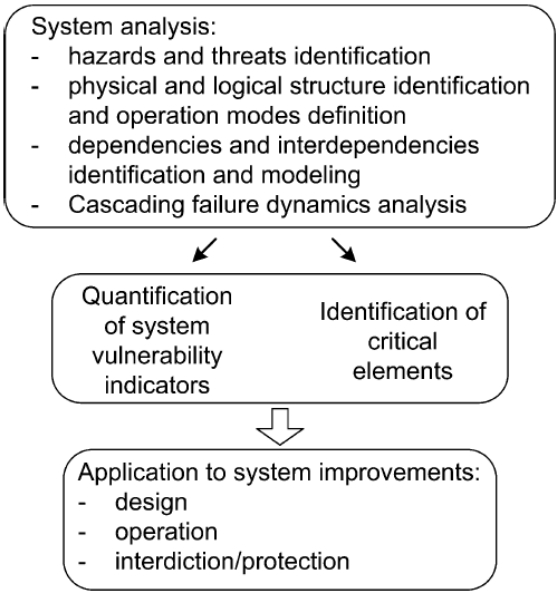


Figure 3-1. Critical Infrastructure Vulnerability Assessment (Kröger & Zio, 2011).

3.2.1. Ideal Criteria to be Evaluated by a Vulnerability Assessment

While a vulnerability assessment will reflect specific objectives of an organization or sponsoring party along with the amount of time, money, and data bestowed upon the work, a common set of criteria to be evaluated exists regardless of application or discipline (Hoddinott & Quisumbing, 2003). A vulnerability assessment should, at very least:

- Identify the correlates of vulnerability (namely the extent and who or what is vulnerable).
- Examine the sources of vulnerability by characterizing risks and shocks faced by the population (or system) as well as the distribution of those shocks.
- Determine the gaps between risks and risk management mechanisms (Hoddinott & Quisumbing, 2003).

A comprehensive vulnerability assessment of a critical infrastructure system should aspire to:

- Identify the set and sequences of events that can cause damages and losses given a system and an end state of interest.
- Identify the relevant set of "initiating events" and evaluate their cascading impact on a subset of elements or the system in its entirety.
- Identify the set of events or respective event sequences that can cause an undesired effect given a system and an end state of interest.

- Determine and elaborate on (inter)dependencies (within the system and among systems) and on coupling of different orders given the set of initiating events and observed outcomes (Kröger & Zio, 2011; Zio et al., 2011).

These outcomes can be translated into a battery of questions to be answered by an individual or organization about to carry out a vulnerability assessment on a complex infrastructure system:

- What are the end states of interest for the given system(s) and how should system boundaries be defined?
- What are threats and hazards of relevance to which the system(s) under consideration may be exposed?
- What is the resilience and sensitivity (susceptibility) of the system(s) experiencing the threats and hazards?
- What are resulting cascades and identifiable (inter)dependencies? What are the respective impacts and what are the high consequence scenarios?
- What uncertainties are involved?
- What are the obvious and non-obvious ("hidden") vulnerabilities? How can these vulnerabilities be better managed and/or reduced? (Kröger & Zio, 2011).

More simply, these questions can be boiled down to:

- What can go wrong?
- What is the likelihood of that happening?
- What are the consequences if it does happen? (Sheffi & Rice Jr., 2005).

A vulnerability assessment should aspire to identify obvious as well as covert vulnerabilities within an infrastructure system and enable a decision-maker to intervene to manage and/or mitigate these vulnerabilities (Kröger & Zio, 2011; Zio et al., 2011). This cannot occur without a full analysis of the system, its components, and their interactions. A vulnerability assessment must also take into consideration the environment in which a system operates and the objectives for which the system is designed to attain (Kröger & Zio, 2011; Zio et al., 2011).

Finally, a vulnerability assessment focused on assessing security risks en route to ensuring mission-critical system functionality should:

- Establish objective criteria that can be adapted by a domain and is repeatable with a focus on critical functions and components.
- Apply methods encouraging analysis to the system or subsystem at the level of design specificity available.
- Be performed before each engineering review in the phase to extend the assessment to the design level of the system under review.
- Employ a blend of techniques to identify vulnerabilities across the system life cycle, pulling from the strengths of each to ensure a comprehensive assessment.
- Utilize a sampling approach to estimate legacy vulnerabilities in the new system environment and to gain an understanding of inherited system security risks upon the adaptation of legacy elements.
- Heed feedback and update techniques based on results (Reed, 2014b; LeSaint et al., 2015).

3.2.2. Characteristics of a Strong Vulnerability Assessment

Vulnerability is often poorly assessed due to a lack of observational data related to hazardous events and the difficulty of collecting data pertaining to the inherent characteristics of the elements at risk (Sterlacchini, 2011). This is due to complexity, spatial and temporal exposure, and socio-technical factors. Existing vulnerability assessment techniques have been critiqued as being superficial or narrowly focused and lacking objective, comprehensive criteria allowing for the identification of vulnerabilities (Reed, 2014b; LeSaint et al., 2015). Vulnerability assessments must be performed early on in the system life cycle as well as at critical milestones and address the risks posed by legacy software and hardware components (Reed, 2014b; LeSaint et al., 2015). Finally, vulnerability assessment methodologies focusing on information systems have noted weaknesses in their ability to guide an individual through a determination of critical system vulnerabilities and to identify appropriate security mitigation techniques to mitigate these vulnerabilities (Antón et al., 2004).

For the purposes of this thesis, a successful vulnerability assessment method is one that:

- Holistically considers all facets of a system in order to uncover potential vulnerabilities.
- Takes into account “unknown unknowns” as best as possible.

- Highlights causal chains and cascading failures.
- Allows for the identification of intervention points.
- Takes the needs of potential end-users into consideration.

A vulnerability analysis should be performed when a system is about to be developed rather than after a system has already been developed or changes to a system have been put into place. The analysis should consider the system in a steady, or normal, state of operation in order to determine as many disparate areas of weakness as possible, as the continued stability, reliability, and availability of a system depend on how secure a system is from potential threats and vulnerabilities (Zafar, 2011).

The final results of a vulnerability assessment should be evaluated regarding their overall credibility, as these results drive potential system improvements to reduce and/or better manage system vulnerabilities (Kröger & Zio, 2011). In a situation where results are not credible, revisiting the vulnerability assessment and making appropriate modifications is recommended. Improvements to alleviate system vulnerability may include modifying structural and functional system design, adding in additional redundancy or separation, increasing safety margins and system investment, modifying operational conditions, and implementing new standards and procedures (Kröger & Zio, 2011). The final decision regarding system improvements is under the purview of the decision-maker or system owner, often after thoroughly investigating the effectiveness of proposed interventions and the potential to avoid negative feedback (Kröger & Zio, 2011).

3.3. Existing Frameworks

Vulnerability assessment is an emerging field in which new frameworks continue to be developed in order to better analyze and understand threats to operational systems. The main methods used to assess vulnerability are familiar mostly from risk management literature (Nowakowski et al., 2015). Traditional risk analysis techniques including Fault Tree Analysis (FTA) and Failure Mode and Effects Analysis (FMEA) can shed light on internal and external factors affecting a system but do not comprehensively analyze hazards and threats.

Vulnerability assessment frameworks have been developed within academia, and this thesis considers two in particular created by Dr. Yacov Haimes and Dr. Terje Aven. Haimes

emphasizes the importance of incorporating an element of time into the concept of resilience and states that the following must be completed in order to evaluate the risks to a vulnerable system (Francis & Bekera, 2014). He states that in order to evaluate the risks to a vulnerable system:

1. The likelihood of an attack must be assessed.
2. Responses of the interdependent state variables characterizing the system upon realization of a threat scenario must be modeled. This process "translates" an attack scenario into consequences.
3. The severity of consequences befalling the system or a subset of systems must be assessed (Haimes, 2006).

Aven is critical of Haimes's approach, arguing that it lacks precision and is too dependent on modeling, and articulates his own approach for performing risk and vulnerability analysis (Aven, 2011). He divides his analysis process into eight main steps:

1. Identify the relevant functions and subfunctions to be analyzed, and relevant performance measures (observable quantities).
2. Define the systems to meet these functions.
3. Identify relevant sources (threats, hazards, opportunities).
4. Perform an uncertainty analysis of the sources.
5. Perform a consequence analysis, addressing uncertainties.
6. Describe risks and vulnerabilities.
7. Evaluate risks and vulnerabilities.
8. Identify possible measures, and return to Step 3 as necessary (Aven, 2007).

Therefore, a vulnerability analysis can be thought of as a component of a more comprehensive risk analysis (Johansson & Hassel, 2010). While insights gleaned from these frameworks can lead to better understanding of a system and inform and advance the CEM analytic technique, utilization of these frameworks is not required to produce a comprehensive CEM diagram for a system. However, it can be said that existing frameworks for risk and vulnerability assessment have informed this research through their emphasis on defining security goals and developing relevant artifacts that can be used as CEM inputs.

Several formal analysis frameworks with a focus on systems vulnerability have been developed within government and industry and investigated for this thesis, including:

- Government-Developed Frameworks:
    - System Security Engineering (SSE) (Department of Defense).
    - Trusted Systems and Networks (TSN) Analysis (Department of Defense).
    - Mission, Symbolism, History, Accessibility, Recognizability, Population, and Proximity (MSHARPP) (Department of Defense).
    - Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognizability (CARVER) (Department of Defense).
- Information System-Centric Frameworks:
    - Vulnerability Assessment & Mitigation (VAM) Methodology (RAND).
    - Security Quality Requirements Engineering (SQUARE) method (Software Engineering Institute – Carnegie Mellon University).
    - OCTAVE Allegro (Software Engineering Institute – Carnegie Mellon University).
- Cybersecurity-Centric Frameworks:
    - Cyber Mission Assurance Engineering (MAE) Methodology (MITRE).
    - Threat Assessment and Remediation Analysis (TARA) (MITRE).
    - Resilient Architectures for Mission and Business Objectives (RAMBO) (MITRE).
    - Security Systems Engineering (SSE) System of Systems (SoS) (MITRE).
- Service-Oriented Architecture-Centric Frameworks:
    - ATLIST (Lowis & Accorsi).
- Operation and Theater-Centric Frameworks:
    - Vulnerability Assessment Method Pocket Guide (VAMPG) (RAND)

3.3.1. Government-Developed Frameworks

3.3.1.1. System Security Engineering

System Security Engineering (SSE) is an element of systems engineering that applies scientific and engineering principles to identify security vulnerabilities and minimize or contain risks associated with these vulnerabilities (U.S. Department of Defense, 2012). These risks can

originate from foreign collection, design vulnerability, supply chain exploit/insertion, and battlefield loss and can occur throughout the acquisition lifecycle (Rebovich et al., 2014). The Department of Defense (DoD) employs SSE for the protection of systems, mission-critical functions, and components; SSE can also be used to identify advanced cyber threats and assure cyber technologies (Rebovich et al., 2014). SSE addresses a range of critical security risks, provides a valuable taxonomy of threats, and is accomplished through Program Protection Planning (PPP).

A Program Protection Plan, in turn, determines candidate protection measures to address vulnerabilities including anti-tamper, cybersecurity, exportability features, hardware/software assurance, physical security, operations security, supply chain, system security, and trusted suppliers (Reed, 2014a; Reed, 2015). An SSE risk-based methodology allows for the identification of critical system functionality and components; assesses threats and vulnerabilities of these components in the operational, program, and development environments; and identifies and advocates for potential countermeasures for the system (Rebovich et al., 2014).

SSE is iterative in nature and can be implemented throughout a program or system's life cycle (Baldwin et al., 2012). Each iteration of the SSE Program Protection Process incorporates prior SSE analysis results, including design countermeasures, until an acceptable combination of risk, cost, and benefit (protection) is determined (Baldwin et al., 2012). Newer iterations may reveal new or changed threats and vulnerabilities as a result of evolving system design or external environmental factors (Baldwin et al., 2012). Key SSE activities and criteria have been developed for pre-Milestone A, pre-Milestone B, pre-Milestone C, and full-rate production and beyond; SSE process controls and design features should be exercised as soon as possible in developmental and operational test plans and procedures, as engineering and planning efforts can be diminished given undiscovered vulnerabilities (Baldwin et al., 2012).

3.3.1.2. Trusted Systems and Networks Analysis

DoD refers to its SSE risk-based analysis as Trusted Systems and Networks (TSN) analysis. TSN analysis is the DoD SSE methodology for protecting mission-critical functions and components. DoD Instruction (DoDI) 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks," implements the DoD's TSN strategy, which is intended to be applied in

an iterative fashion as system design matures (LeSaint et al., 2015; U.S. Department of Defense, 2012). TSN analysis activities are also included in draft NIST SP 800-160, "Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems" (LeSaint et al., 2015; Ross et al., 2014). TSN analysis includes requirements analysis, design, and implementation activities for system security as defined in ISO 15288, "Systems and Software Engineering – System Life Cycle Processes" and advocates for a balanced approach to countermeasures including those that prevent, detect, and respond to an adverse event (LeSaint et al., 2015; ISO/IEC/IEEE, 2015; Deputy Assistant Secretary of Defense for Systems Engineering & Department of Defense Chief Information Officer, 2014).

The objective of TSN analysis is to keep malicious content out by protecting key mission components (Reed, 2014b). As such, vulnerability assessment is an activity that is a key part of a TSN analysis, conducted to point out vulnerabilities in system design and COTS products (Deputy Assistant Secretary of Defense for Systems Engineering & Department of Defense Chief Information Officer, 2014). A vulnerability assessment conducted as a part of a full TSN analysis seeks to focus on identifying and quantifying potential vulnerabilities so that cost-effective "countermeasures" can be integrated into system requirements or the Statement of Work (SOW) prior to a Request For Proposal (RFP) being issued (Reed, 2012c).

An adversary that is able to gain access to, modify, or restrict the performance of a system is dangerous; it is imperative to assess vulnerabilities and weaknesses that could result in significant mission impact (Deputy Assistant Secretary of Defense for Systems Engineering & Department of Defense Chief Information Officer, 2014). Decisions about particular vulnerabilities to address and applicable mitigation strategies are governed by an understanding of threats, mission impact, and program priorities (Deputy Assistant Secretary of Defense for Systems Engineering & Department of Defense Chief Information Officer, 2014). Outputs from the vulnerability assessment, along with those from a separate threat assessment, allow for the determination of the likelihood of losing mission capability as shown in Figure 3-2 (LeSaint et al., 2015).

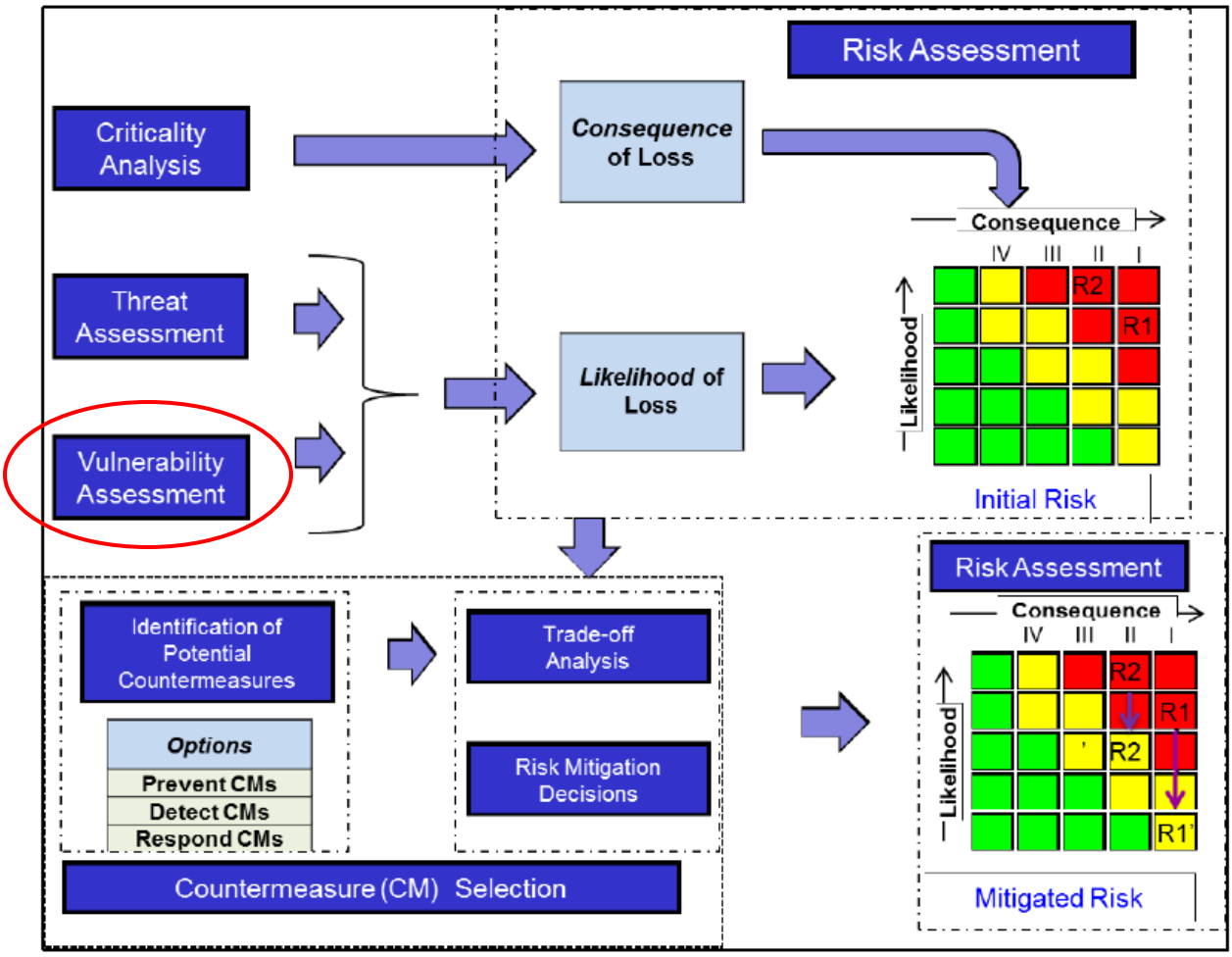


Figure 3-2. Trusted Systems and Networks (TSN) Analysis Overall Methodology (Deputy Assistant Secretary of Defense for Systems Engineering & Department of Defense Chief Information Officer, 2014).

Per TSN Analysis, the three principal vulnerabilities to watch for in systems engineering processes are:

- Access paths within the supply chain, development, and test environments and processes allowing adversaries to insert components (software, hardware, or firmware) that could at a later time cause the system to fail.
- Access paths allowing threats to trigger a component malfunction or failure at the adversary's discretion.
- Access paths within the design and architecture allowing threats to circumvent the integrity, confidentiality, and availability of the system or overall mission through

weaknesses in component design, architecture, or code (Deputy Assistant Secretary of Defense for Systems Engineering & Department of Defense Chief Information Officer, 2014).

The vulnerability assessment methodology followed by a TSN analysis is shown in Figure 3-3. The first step, Determine Access Path Opportunities, takes system concept of operations (CONOPS) into consideration along with the notional system architecture to determine design-attribute related attack surfaces (Reed, 2012c). Systems engineering, software, and supply chain processes pertaining to process-activity type weaknesses are also enumerated (Reed, 2012c). The second step, Select Attack Scenarios, investigates which types of attack scenarios may apply to the system under investigation by considering how supply chain and software weaknesses could potentially be exploited by an adverse actor (Reed, 2012c). The third step, Determine Exploitable Vulnerabilities, figures out whether or not an attack vector is successful when applied to a specific component; if successful, an exploitable vulnerability is said to be present (Reed, 2012c). Vulnerabilities are then listed for each critical component. Finally, the fourth step, Inform the Threat Assessment/Vulnerability Assessment Based Risk Likelihood Determination, transitions the analysis to the next step of determining the overall risk likelihood (Reed, 2012c).

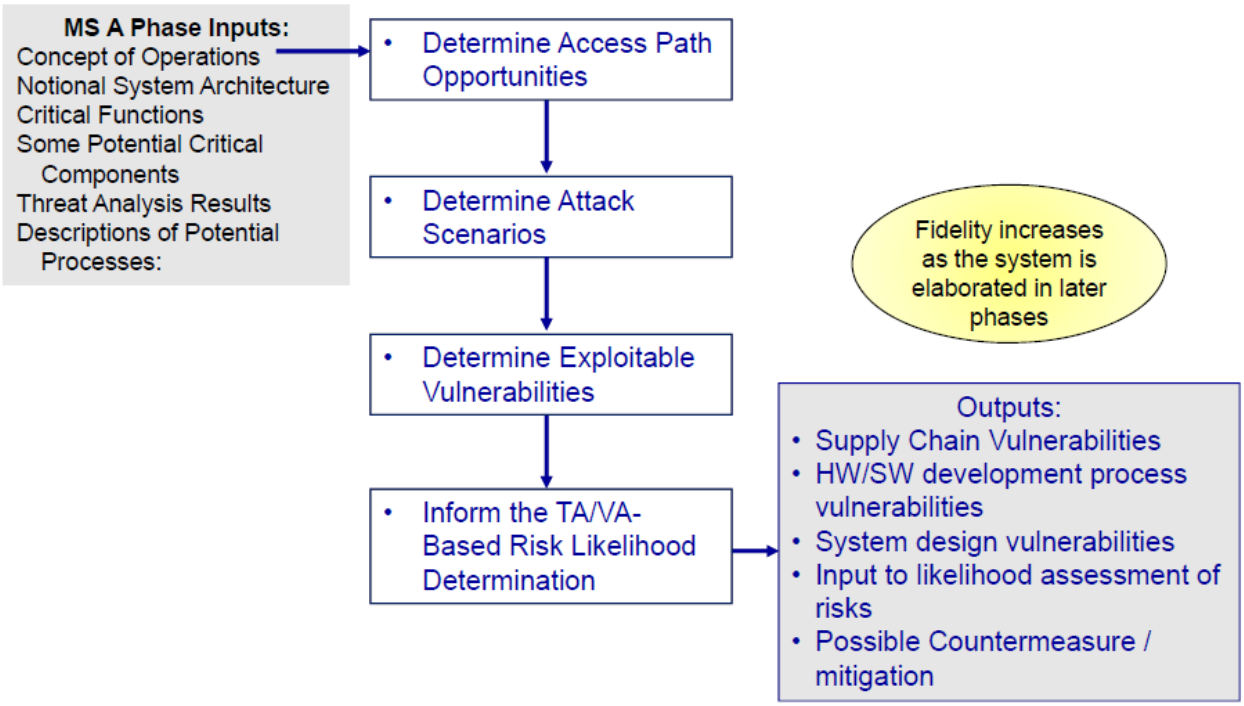


Figure 3-3. TSN Vulnerability Assessment Methodology (Reed, 2012a).

In assessing the vulnerability of critical components, a vulnerability assessment conducted as a part of a larger TSN analysis seeks to shed light on potential security-related concerns via the following questions:

- Where and under what conditions was the system designed?
- Where and under what conditions were critical components developed?
- How and where are components assembled and integrated into completed systems?
- Where and under what conditions was critical software or firmware developed?
- How are software updates distributed and loaded in the field?
- How are other system maintenance operations conducted? (Reed, 2012a).

TSN Analysis identifies six techniques capable of effectively identifying system vulnerabilities. A program or system may employ one or more of these techniques to adequately assess vulnerability throughout the entire system lifecycle:

- Milestone A Vulnerability Assessment Questionnaire.
- Vulnerability databases.
- Static analyzer tools and other detection techniques.

- Component Diversity Analysis.
- Fault Tree Analysis (FTA).
- Red Team Penetration Testing (Deputy Assistant Secretary of Defense for Systems Engineering & Department of Defense Chief Information Officer, 2014).

The Milestone A Vulnerability Assessment Questionnaire is a battery of yes or no questions that a program answers to identify vulnerabilities present in the Statement of Work (SOW) and System Requirements Document (SRD) prior to the release of a Request For Proposal (RFP) (Deputy Assistant Secretary of Defense for Systems Engineering & Department of Defense Chief Information Officer, 2014). The results of the questionnaire are applied to determine the system security risk likelihood (Deputy Assistant Secretary of Defense for Systems Engineering & Department of Defense Chief Information Officer, 2014).

Several publicly-available databases contain extensive information on attack patterns, weaknesses, and vulnerabilities including the Common Attack Pattern Enumeration and Classification (CAPEC), the Common Weakness Enumeration (CWE), and the Common Vulnerabilities and Exposures (CVE) databases (Deputy Assistant Secretary of Defense for Systems Engineering & Department of Defense Chief Information Officer, 2014). These databases amalgamate information on known, exploitable weaknesses in software capabilities, and the assignment of a CVE identifier can concatenate information and resources available globally regarding a particular software vulnerability (Deputy Assistant Secretary of Defense for Systems Engineering & Department of Defense Chief Information Officer, 2014). A Vulnerability Database Assessment Process utilizing the information stored in the CAPEC, CWE, and CVE databases to assess system vulnerabilities in a methodical way is proposed as a TSN Analysis technique capable of effectively identifying system vulnerabilities (Deputy Assistant Secretary of Defense for Systems Engineering & Department of Defense Chief Information Officer, 2014).

The CAPEC serves as a resource for identifying attack patterns that may be used by an adversary against a system (Deputy Assistant Secretary of Defense for Systems Engineering & Department of Defense Chief Information Officer, 2014). The CAPEC lists potential attacks on a system as well as on its supply chain and development environments; a user or program should select all applicable attacks that could lead to an adverse event (Deputy Assistant Secretary of Defense for

Systems Engineering & Department of Defense Chief Information Officer, 2014). The set of attack vectors is compared against weaknesses catalogued in the CWE and CVE databases and used to evaluate development, legacy, open source, and COTS software (Deputy Assistant Secretary of Defense for Systems Engineering & Department of Defense Chief Information Officer, 2014). The CWE database lists specific vulnerabilities or weaknesses that can occur in software processes, practices, design, and architecture, while the CVE database is a repository of publically-known vulnerabilities that need to be remediated (Deputy Assistant Secretary of Defense for Systems Engineering & Department of Defense Chief Information Officer, 2014). The program uses the vulnerabilities and weaknesses as mapped to the software life cycle and development stage to complete the vulnerability assessment, which in turn serves as the basis for further inspection (Deputy Assistant Secretary of Defense for Systems Engineering & Department of Defense Chief Information Officer, 2014).

The Vulnerability Database Assessment Process assumes that standards for secure design and coding have been established for custom developed or legacy software and proceeds as follows:

1. Determine the applicable attack vectors from CAPEC that will be used for the assessment.
2. Determine whether each critical component is a COTS product or a customer-developed product. For the former, use the CVE database to identify a set of vulnerabilities associated with each attack. For the latter, use the CWE database to identify potential weaknesses associated with each attack.
3. Determine the risk likelihood of the weakness or vulnerability.
4. Identify possible mitigations for each weakness or vulnerability.
5. Combine the likelihoods for each of the components.
6. Repeat the steps periodically to account for elaboration of designs and database updates.
7. Use the vulnerability assessment results to inform the risk assessment and the risk-based cost-benefit trade-off (Deputy Assistant Secretary of Defense for Systems Engineering & Department of Defense Chief Information Officer, 2014).

The above approach is illustrated in Figure 3-4:

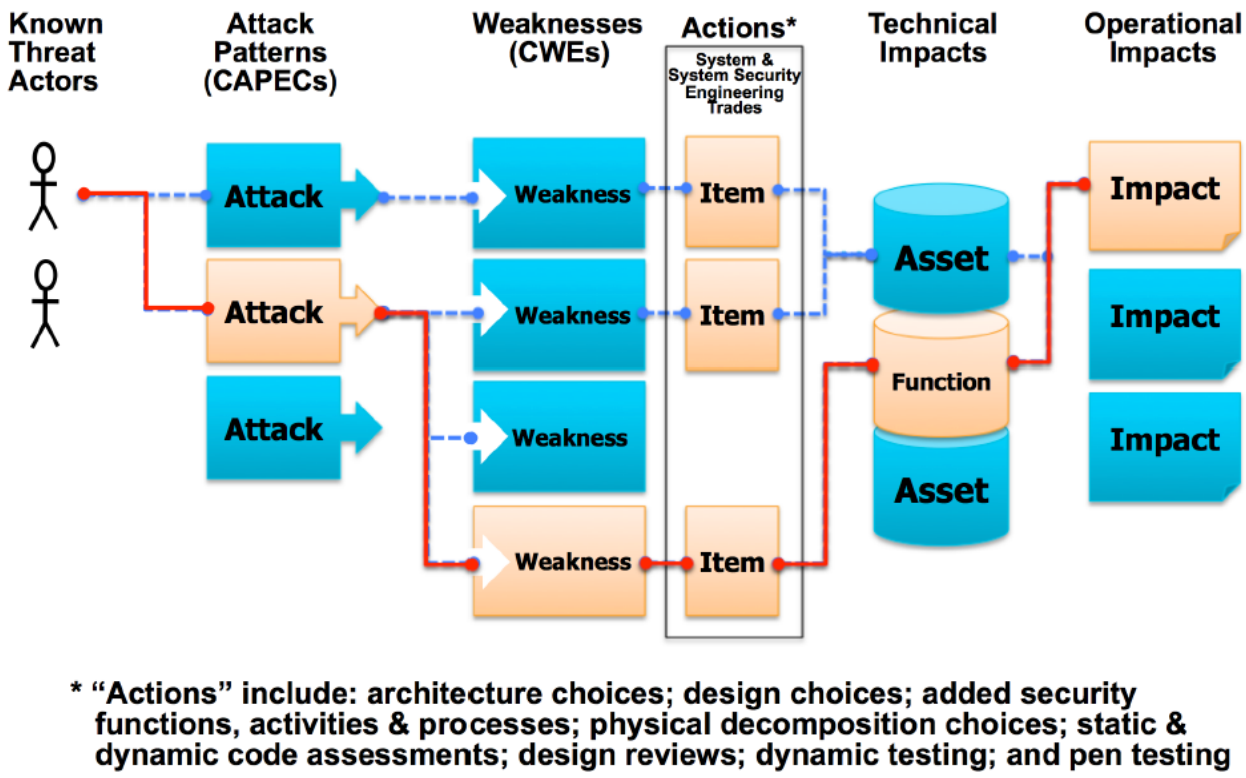


Figure 3-4. Evaluation of Custom Software for Vulnerability using Vulnerability Database Assessment Approach (Deputy Assistant Secretary of Defense for Systems Engineering & Department of Defense Chief Information Officer, 2014).

Static analysis, dynamic analysis, and other security analysis and testing tools can be used to identify vulnerabilities in software during the development phase as well as in legacy and open source software (Deputy Assistant Secretary of Defense for Systems Engineering & Department of Defense Chief Information Officer, 2014). These tools connect vulnerabilities to specific CWE weaknesses and CVE vulnerabilities (Deputy Assistant Secretary of Defense for Systems Engineering & Department of Defense Chief Information Officer, 2014). Different static and dynamic analyzers, especially those from different vendors, employ different testing techniques and internal criteria, allowing different weaknesses and vulnerabilities to be uncovered (Deputy Assistant Secretary of Defense for Systems Engineering & Department of Defense Chief Information Officer, 2014). This approach is particularly effective when combined with the Vulnerability Database Assessment described above (Deputy Assistant Secretary of Defense for Systems Engineering & Department of Defense Chief Information Officer, 2014).

Component Diversity Analysis can be used to gauge the potential impact of malicious insertion in a component used several times and in varying critical functions or subfunctions within a system (Deputy Assistant Secretary of Defense for Systems Engineering & Department of Defense Chief Information Officer, 2014). The analysis, which must balance the security benefits provided by diverse components with the operational and fiscal benefits provided by common components, can be performed at the subsystem, system, or system-of-systems levels and at various points in the system life cycle (Deputy Assistant Secretary of Defense for Systems Engineering & Department of Defense Chief Information Officer, 2014). This analysis can provide insight into the potential impact of a vulnerability on a system as a whole (Deputy Assistant Secretary of Defense for Systems Engineering & Department of Defense Chief Information Officer, 2014).

Commonality among components can be attractive for reasons including maintainability, reliability, and life cycle cost – the latter by allowing for economies of scale and/or smaller inventories of spare parts (Deputy Assistant Secretary of Defense for Systems Engineering & Department of Defense Chief Information Officer, 2014). However, common components can lead to increased security risk, as the vulnerabilities inherent to a common component are promulgated throughout the system (Deputy Assistant Secretary of Defense for Systems Engineering & Department of Defense Chief Information Officer, 2014). This can result in a component becoming a high-value target for the insertion of malicious logic, as a particular vulnerability can be exploited at multiple points in the system and have wide-reaching impacts (Deputy Assistant Secretary of Defense for Systems Engineering & Department of Defense Chief Information Officer, 2014).

Component diversity can make a system more secure by ensuring that a vulnerability or weakness will affect few, as opposed to several, critical system functions and providing a measure of redundancy (Deputy Assistant Secretary of Defense for Systems Engineering & Department of Defense Chief Information Officer, 2014). The probabilities in diversity are independent; therefore, the probability of two or more components failing is the product of each component failing, or having a vulnerability exploited, individually (LeSaint et al., 2015). This concept can be expanded to a system's supply chain, as using multiple suppliers for a component can spread the overall risk of the security of an individual suppliers' components being subverted

(Deputy Assistant Secretary of Defense for Systems Engineering & Department of Defense Chief Information Officer, 2014).

Discussed in Chapter 2 of this thesis, Fault Tree Analysis (FTA) is applicable to SSE given slight adjustments to account for intentional system faults introduced by malicious actors as opposed to random sources of failures (Deputy Assistant Secretary of Defense for Systems Engineering & Department of Defense Chief Information Officer, 2014). An FTA can be expanded to identify access and data transfer paths within a system, effectively tracing hypothetical security breaches, and to consider access paths and opportunities that can potentially be exploited by an adversary to discover vulnerabilities or to introduce new vulnerabilities (Deputy Assistant Secretary of Defense for Systems Engineering & Department of Defense Chief Information Officer, 2014). TSN Analysis advocates the following FTA approach:

- Establish the set of failure events for evaluation based on the list of critical functions.
- Decompose the fault tree to identify the logical dependencies among hypothetical component failures for each failure event.
- Identify "hot spots" that represent significant risks due to a role in multiple failure events (Deputy Assistant Secretary of Defense for Systems Engineering & Department of Defense Chief Information Officer, 2014).

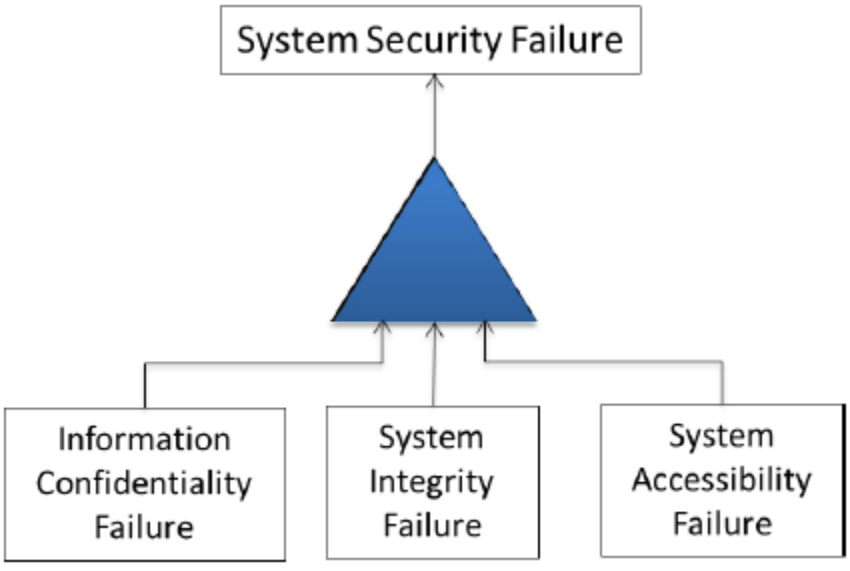


Figure 3-5. Example SSE Top-Level FTA Diagram (Deputy Assistant Secretary of Defense for Systems Engineering & Department of Defense Chief Information Officer, 2014).

Red Team Penetration Testing can be used to replicate the tactics of an actual threat and to contribute to extended knowledge of the security behavior of a system, supply chain, or development environment (Deputy Assistant Secretary of Defense for Systems Engineering & Department of Defense Chief Information Officer, 2014). For reference, penetration testing is the "simulation of an attack on a system, network, piece of equipment or other facility, with the objective of proving how vulnerable that system or "target" would be to a real attack" (Henry, 2012). The types of attacks to which the system is subjected are essentially a set of abuse or misuse cases (Deputy Assistant Secretary of Defense for Systems Engineering & Department of Defense Chief Information Officer, 2014).

Three major challenges exist with respect to conducting vulnerability analyses as part of a TSN analysis (LeSaint et al., 2015). First, the initial iterations of TSN analysis tend to occur early in a system's lifecycle, before the system is fully mature. While this is ideal for identifying weaknesses and implementing measures to enhance system effectiveness at the beginning of a system's life cycle, additional vulnerabilities can crop up as the system settles into a steady state. Components may require expensive retrofit measures later on, or the program manager may be put in a position where he or she will need to accept increased security risks (LeSaint et al., 2015). Second, the vulnerability assessment must reach beyond the system to consider risks present in the supply chain and development practices (LeSaint et al., 2015). Protection practices including secure design and coding standards can ensure that malicious insertion does not occur via the exploitation of weaknesses external to the system (LeSaint et al., 2015). Third, prevention efforts will never be completely effective, so placing detection and response mechanisms into the system, supply chain, and development practices is of utmost importance (LeSaint et al., 2015).

3.3.1.3. MSHARPP and CARVER

Mission, Symbolism, History, Accessibility, Recognizability, Population, and Proximity (MSHARPP) and Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognizability (CARVER) are two decision-support tools created by the DoD to perform criticality assessments and to inform the vulnerability assessment process (Antón et al., 2004). While MSHARPP focuses on assessing personnel vulnerabilities (inside looking out) and CARVER focuses on determining the hardness or softness of assets in criminal or terrorist actions (outside looking in), both tools employ a matrix-based approach (Haines, 2013). This

allows for the evaluation of assets and employment of metrics, yielding a quantitative measure of vulnerability.

MSHARPP is a numeric assessment in which each of the criteria are evaluated and combined to produce an overall score, which is typically applied to key assets in security risk management (U.S. Department of Homeland Security, 2008). MSHARPP is a targeting tool best suited toward assessing personnel vulnerabilities but can also be used to assess vulnerabilities pertaining to facilities, units, or other assets (Schnaubelt et al., 2014). A matrix is built as shown in Table 3-1, in which each asset is assigned a number (1 through 5) that corresponds to the relevant MSHARPP variable (Schnaubelt et al., 2014). The number 5 represents the greatest likelihood of attack or vulnerability, while the number 1 represents the lowest likelihood of attack or vulnerability. The numerical values are summed to yield a relative value as a target or the overall amount of vulnerability (Schnaubelt et al., 2014).

Table 3-1. Example MSHARPP Matrix (Schnaubelt et al., 2014).

Target	M	S	H	A	R	P	P	Total	Threat Weapon
Headquarters building	5	4	5	1	3	4	1	23	4,000-pound, vehicle-borne improvised explosive device
Troop barracks	2	4	5	4	4	4	2	25	220-pound, vehicle-borne improvised explosive device
Communications center	5	4	2	3	5	3	1	23	4,000-pound, vehicle-borne improvised explosive device
Emergency operations center	3	3	2	4	4	4	2	22	50-pound satchel charge
Fuel storage facility	4	3	1	5	5	1	3	22	Small-arms ammunition and mortars
Airfield	5	5	3	2	5	5	4	29	Mortars and rocket-propelled grenades
Ammunition supply point	5	5	1	1	5	3	1	21	Small-arms ammunition and mortars
Water purification facility	5	2	3	5	5	0	4	24	Chemical, biological, and radiological contamination

SOURCE: ATTP 3-39.20 (FM 3-19.50), p. 5-18.

CARVER is used to prioritize vulnerabilities and to characterize assets when applied to security risk management (Antón et al., 2004; U.S. Department of Homeland Security, 2008). The basic steps of an Integrated Vulnerability Assessment (IVA) in CARVER parallel those outlined in the VAM methodology:

1. Identify vulnerabilities.
2. Prioritize vulnerabilities.
3. Brainstorm countermeasures.
4. Assess risks (Antón et al., 2004).

A matrix is developed for each asset, and the assets are evaluated against a criteria list (which can be tailored based on mission or operational needs) and assigned a relative value ranking as shown in Table 3-2 (Schnaubelt et al., 2014). The values are then promulgated into the matrix shown in Table 3-3. However, it must be noted that the methodology's simple scoring scheme does not accurately preserve important distinctions among categories (Antón et al., 2004). This is further compounded when ratings from different parts of the assessment are combined to produce a metric describing overall vulnerability.

Table 3-2. Example CARVER Criteria (Schnaubelt et al., 2014).

Potential Targets	C	A	R	V	E	R	Totals
Commissary	5	7	10	8	8	10	48
Headquarters	1	4	10	8	6	6	35
Communications Center	10	10	6	8	3	4	41

SOURCE: ATTP 3-39.20 (FM 3-19.50), p. 5-20.

Table 3-3. Example CARVER Matrix (Schnaubelt et al., 2014).

Criteria	Relative Value Rating
Criticality	
Immediate output halt or 100 percent curtailment. Target cannot function without asset.	10
Halt less than 1 day or 75 percent curtailment in output, production, or service.	8
Halt less than 1 week or 50 percent curtailment in output, production, or service.	6
Halt in more than 1 week and less than 25 percent curtailment in output, production, or service	4
No significant effect.	1
Accessibility	
Standoff weapons can be deployed.	10
Inside perimeter fence, but outdoors.	8
Inside a building, but on a ground floor.	6
Inside a building, but on the second floor or in basement. Climbing or lowering is required.	4
Not accessible or only accessible with extreme difficulty.	1
Recuperability	
Replacement, repair, or substitution requires 1 month or more.	10
Replacement, repair, or substitution requires 1 week to 1 month.	8
Replacement, repair, or substitution requires 72 hours to 1 week.	6
Replacement, repair, or substitution requires 24 to 72 hours.	4
Same-day replacement, repair, or substitution.	1
Vulnerability	
Vulnerable to long-range target designation, small arms, or charges (weighing 5 pounds or less).	10
Vulnerable to light antiarmor weapons fire or charges (weighing 5 to 10 pounds).	8
Vulnerable to medium antiarmor weapons fire, bulk charges (weighing 10 to 30 pounds), or carefully placed smaller charges.	6
Vulnerable to heavy antiarmor weapons fire, bulk charges (weighing 30 to 50 pounds), or special weapons.	4
Invulnerable to all but the most extreme targeting measures.	1
Effect (on the population)	
Overwhelming positive effects, but no significant negative effects.	10
Moderately positive effects and a few significant negative effects.	8
No significant effects and remains neutral.	6
Moderate negative effects and few significant positive effects.	4
Overwhelming negative effects and no significant positive effects.	1
Recognizability	
Clearly recognizable under all conditions and from a distance and requires little or no personnel training for recognition.	10
Easily recognizable at small-arms range and requires little personnel training for recognition.	8
Difficult to recognize at night during inclement weather or might be confused with other targets or target components. Some personnel training required for recognition.	6
Difficult to recognize at night or in inclement weather (even in small-arms range). The target can easily be confused with other targets or components and requires extensive personnel training for recognition.	4
The target cannot be recognized under any conditions, except by experts.	1

SOURCE: ATTP 3-39.20 (FM 3-19.50), p. 5-19.

3.3.2. Information System-Centric Frameworks

3.3.2.1. Vulnerability Assessment & Mitigation

The Vulnerability Assessment & Mitigation (VAM) methodology provides insight into relationships within a system, facilitates the identification of vulnerabilities, and recommends applicable mitigation techniques (Antón et al., 2004). VAM addresses a gap in previous approaches by guiding a comprehensive review of vulnerabilities throughout all aspects of information systems (cyber, physical, human/social, and infrastructure objects) and mapping the vulnerabilities to specified security mitigations (Antón et al., 2004). This ensures that the system's Minimum Essential Information Infrastructure (MEII) is adequately understood and secured and allows the evaluator to think beyond known vulnerabilities (Antón et al., 2004). The VAM methodology utilizes a top-down approach and maps vulnerability attributes to a list of mitigation approaches (Antón et al., 2004). The breadth of mitigation approaches assists the evaluator to both discover vulnerabilities that have not yet been exploited or encountered during system operation and to develop a list of existing and potential concerns to deter surprise attacks (Antón et al., 2004).

The methodology has six steps that map security needs to critical organizational functions:

1. Identify your organization's essential information functions.
2. Identify essential information systems that implement these functions.
3. Identify vulnerabilities of these systems.
4. Identify pertinent security techniques to mitigate these vulnerabilities.
5. Select and apply techniques based on constraints, costs, and benefits.
6. Test for robustness and actual feasibilities under threat.
   (Repeat steps 3 – 6 as needed.) (Antón et al., 2004).

VAM breaks down system components or objects (parts of the system contributing to its function, execution, or management) into four categories: physical, cyber, human/social, and infrastructure (Antón et al., 2004). The methodology emphasizes that vulnerabilities arise from the fundamental properties of these objects and exploits this fact to provide a robust taxonomy for the user (Antón et al., 2004). The VAM vulnerability matrix shown in Table 3-4 utilizes these system components along with system properties to lead the user through a comprehensive

enumeration of obvious and non-obvious vulnerabilities (often in the socio-technical realm). The VAM vulnerability matrix compares system objects and vulnerability attributes, as vulnerabilities can arise from identifiable attributes of information system objects, and guides the user to recognize non-obvious vulnerabilities (Antón et al., 2004).

Table 3-4. RAND VAM Vulnerability Matrix (Antón et al., 2004).

RANDMR1601-tableS.1

		Object of Vulnerability			
		Physical	Cyber	Human/Social	Enabling Infrastructure
	Attributes	Hardware (data storage, input/output, clients, servers), network and communications, locality	Software, data, information, knowledge	Staff, command, management, policies, procedures, training, authentication	Ship, building, power, water, air, environment
Design/Architecture	Singularity				
	Uniqueness				
	Centrality				
	Homogeneity				
	Separability				
	Logic/ implementation errors; fallibility				
	Design sensitivity/ fragility/limits/ finiteness				
	Unrecoverability				
Behavior	Behavioral sensitivity/ fragility				
	Malevolence				
	Rigidity				
	Malleability				
	Gullibility/ deceivability/naiveté				
	Complacency				
	Corruptibility/ controllability				
General	Accessible/ detectable/ identifiable/ transparent/ interceptable				
	Hard to manage or control				
	Self unawareness and unpredictability				
	Predictability				

VAM identifies a thorough taxonomy of security techniques to prevent, detect, and mitigate compromises in information systems (Antón et al., 2004). These techniques are grouped into categories including resilience and robustness; intelligence, surveillance, and reconnaissance (ISR) and self-awareness; counterintelligence, denial of ISR, and target acquisition; and deterrence and punishment as shown in Figure 3-6:

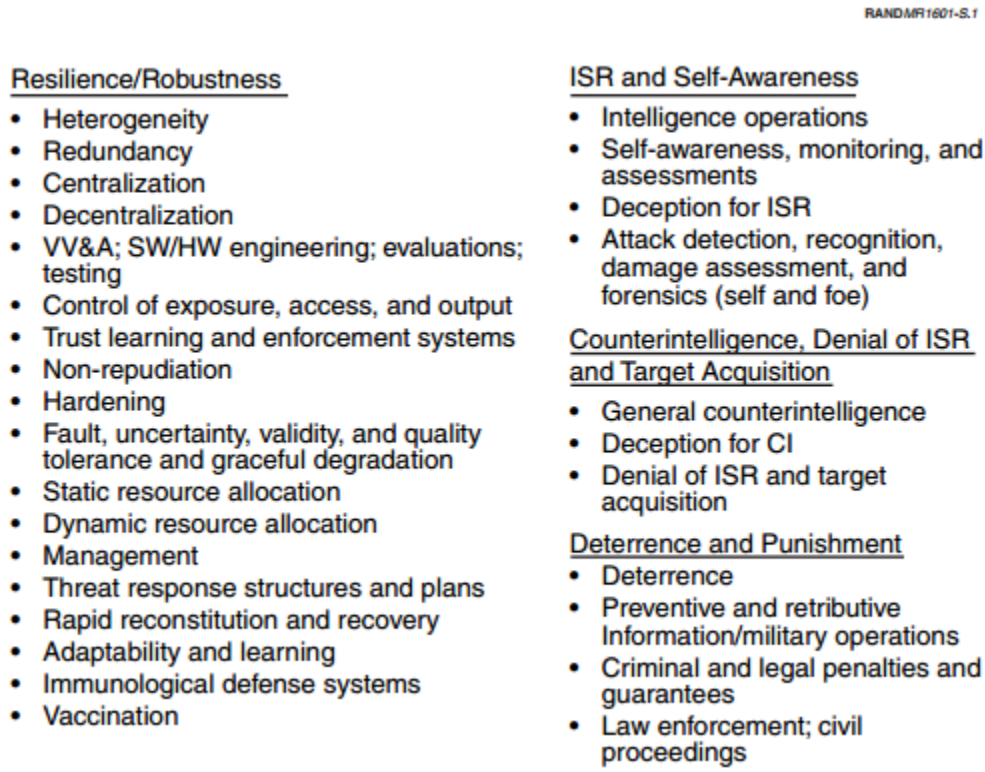


Figure 3-6. RAND VAM Security Mitigation Techniques (Antón et al., 2004).

The methodology uses several approaches to identify which security techniques should be considered to address the identified vulnerabilities (Antón et al., 2004). A second matrix connects each identified vulnerability to security techniques capable of mitigating the vulnerability. This is shown in conceptually in Figure 3-7 and practically in Figure 3-8:

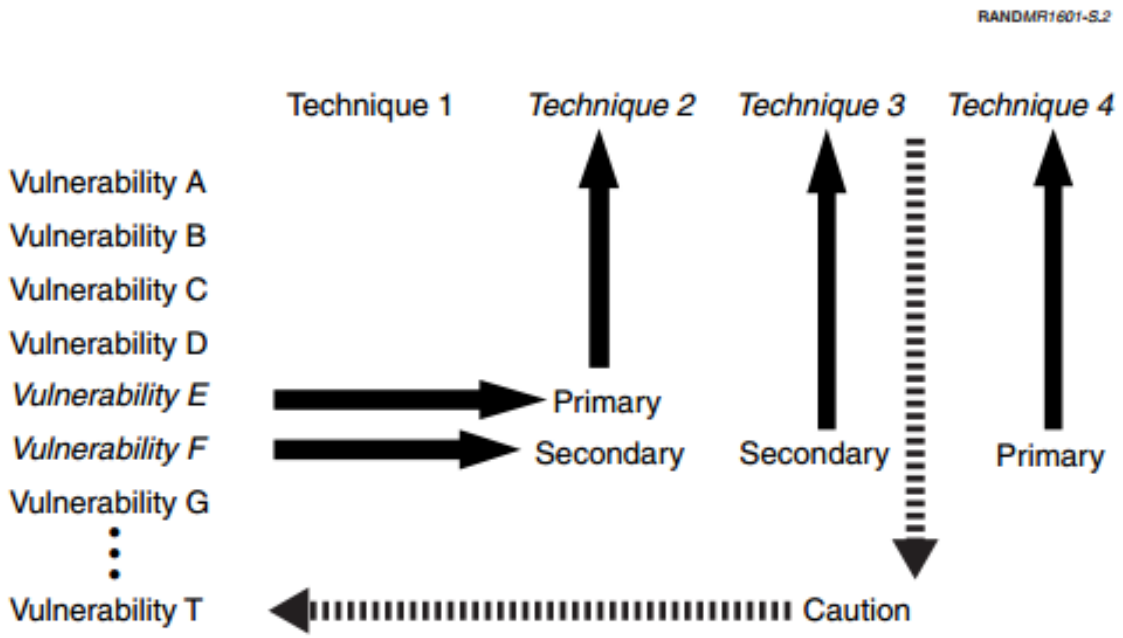


Figure 3-7. The RAND VAM Process of Mapping Vulnerabilities to Security Mitigation Techniques (Antón et al., 2004).

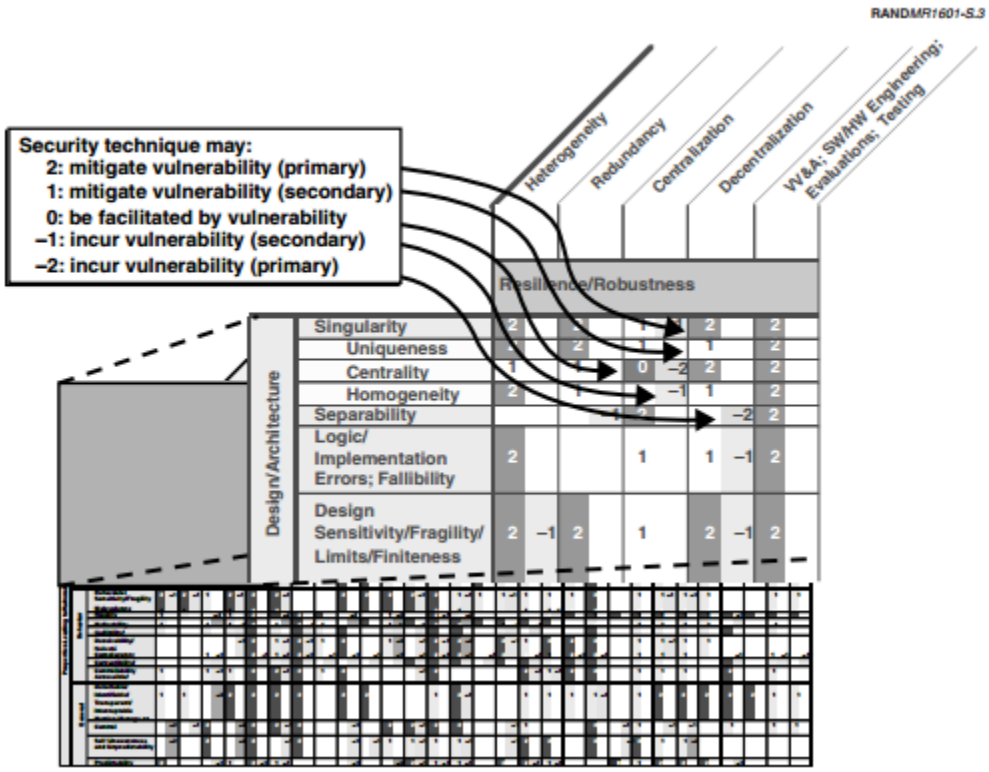


Figure 3-8. RAND VAM Values Relating Vulnerabilities to Security Techniques (Antón et al., 2004).

The output of a matrix resembling Figure 3-8 is the filtering of candidate security techniques; the partitioning of information system compromises into essential components of an attack or failure including knowledge, access, target vulnerability, non-retribution, and assessment; and the generation of recommendations with respect to system security (Antón et al., 2004). It is important to note that VAM fills a gap in existing methodologies by proffering explicit guidance on uncovering system vulnerabilities and suggesting appropriate mitigations as shown in Figure 3-9 (Antón et al., 2004). Filters tuned to vulnerabilities, evaluator type, and attack component are instrumental in improving the usability of the recommendations yielded by the methodology (Antón et al., 2004). The VAM methodology complements other approaches by providing an explicit mechanism to facilitate the understanding of the causes of vulnerabilities, knowledge regarding applicable security techniques, and knowledge of problems that may arise from the selected security techniques (Antón et al., 2004). In particular, VAM steps 3 and 4 can provide value upon integration into other vulnerability assessment methodologies (Antón et al., 2004).

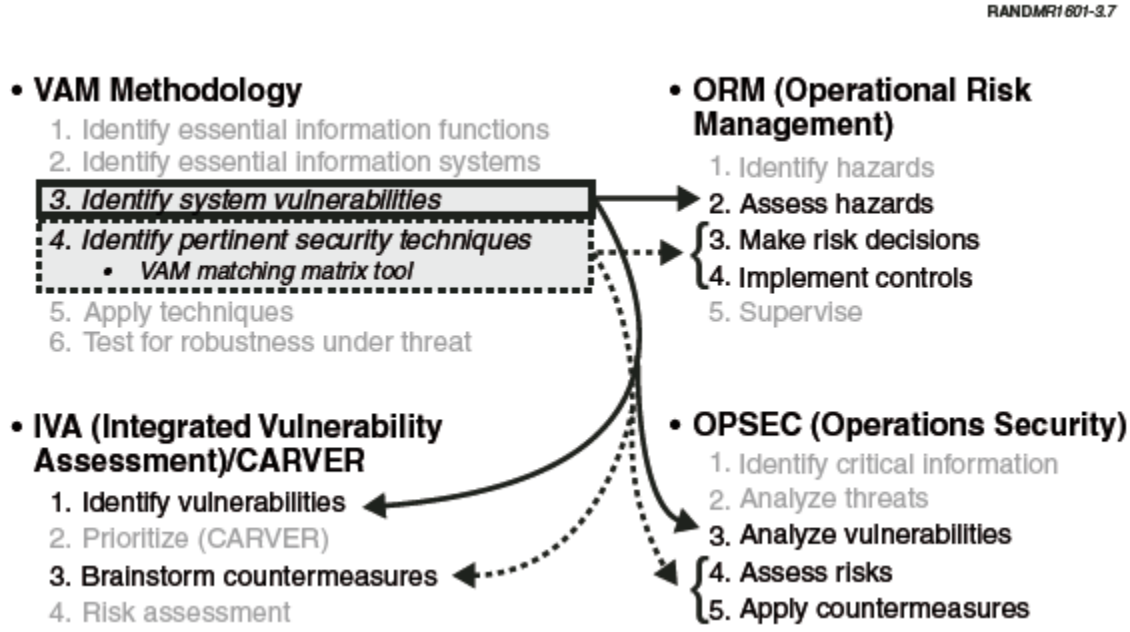


Figure 3-9. Greater Applicability of VAM Methodology (Antón et al., 2004).

3.3.2.2. SQUARE and OCTAVE Allegro

The Security Quality Requirements Engineering (SQUARE) methodology was developed by the Software Engineering Institute – Carnegie Mellon University to assist organizations with implementing security into the beginning stages of the production life cycle. SQUARE is

primarily designed for use with information technology systems but has been adapted to accommodate software acquisition. The methodology has nine steps that yield prioritized and categorized security requirements as a final deliverable:

1. Agree on definitions.
2. Identify security goals.
3. Develop artifacts.
4. Perform risk assessment.
5. Select elicitation technique.
6. Elicit security requirements.
7. Categorize requirements.
8. Prioritize requirements.
9. Requirements inspection (Mead et al., 2005).

SQUARE is easily applied to large-scale systems and provides a great amount of flexibility, allowing the user to select methods for artifacts development, risk assessment, and requirements elicitation. System artifacts can include use and misuse cases as well as architectural diagrams (attack trees) in order to concentrate understanding and facilitate system investigation (Zafar, 2011). The risk assessment step allows for the user to select an appropriate framework for the problem, and it should be noted that the National Institute for Standard and Technology's SP 800-30, "Guide for Conducting Risk Assessments" is a popular method. The NIST framework promotes detailed understanding of system threats and vulnerabilities and assists with the identification of risk impacts (Zafar, 2011).

Frequently-used requirements elicitation methods include Joint Application Development (JAD), Issue-Based Information Systems (IBIS), and Accelerated Requirements Method (ARM). These methods were three of several studied by students at Carnegie Mellon University (N. Mead, 2006).

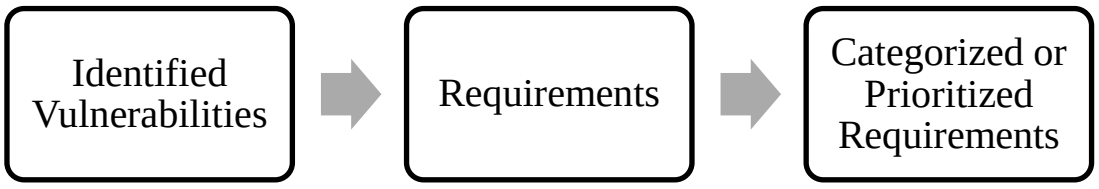


Figure 3-10. Partial SQUARE Process Flow.

The SQUARE process flow is highly dependent, with outputs of each step serving as input for the next respective step (Zafar, 2011). The quality of the artifacts developed early on dictates the quality of the threats and vulnerabilities identified in the subsequent risk assessment process (Zafar, 2011). Shortcomings do exist, particularly in the areas of repeatability and giving too much freedom to the researcher at various points in the process; SQUARE is better suited to a system about to be developed rather than an already-developed system due to the difficulties involved in bolstering an insecure system following deployment (Zafar, 2011). SQUARE also fails to guarantee a thorough set of artifacts, vulnerabilities, and requirements. While SQUARE is not perfect, the method is a valid, flexible framework capable of performing vulnerability analysis that potentially could be applied to a wide variety of case studies.

The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Allegro framework also was developed by the Software Engineering Institute – Carnegie Mellon University. OCTAVE Allegro is a tool for information system analysis, namely identifying and managing security risks, tailored for large organizations and sponsored by the Department of Defense (Antón et al., 2004). The third in a series of frameworks designed to streamline and optimize the process of information security risk assessment, OCTAVE Allegro encourages consideration of people, technology, and facilities in the context of their relationship to information and applicable business processes and services (Caralli et al., 2007). At its core, OCTAVE Allegro facilitates a lean risk assessment and assists with the evolution from security to organizational resilience through focusing on processes and services. The methodology does not provide guidance with respect to the selection of security controls.

OCTAVE Allegro has four main objectives: assisting with the development of criteria reflective of an organization's risk tolerances to qualitatively evaluate risks, identifying mission-essential organizational assets, identifying vulnerabilities and threats potentially impacting those assets, and determining and evaluating consequences to the organization given the realization of threats (Caralli et al., 2007). OCTAVE Allegro is ideally suited for use by individuals without extensive knowledge of risk assessment, as a battery of detailed worksheets is provided for stepping through the process.

The four main objectives are distilled into eight steps:

1. Establish risk measurement criteria.
2. Develop information asset profile.
3. Identify information asset containers.
4. Identify areas of concern.
5. Identify threat scenarios.
6. Identify risks.
7. Analyze risks.
8. Select mitigation approach (Caralli et al., 2007).

While developed in a similar vein as SQUARE, OCTAVE Allegro provides more structure and a robustly thought-out approach given the multiple worksheets that can prompt an organization or individual to think critically about information assets and resiliency while assessing risks. While OCTAVE Allegro asserts that identifying vulnerabilities is an important step preceding the identification of risks, the methodology eliminated a formal vulnerability testing component present in previous versions and currently focuses on risk more than vulnerability (Caralli et al., 2007). The methodology has overly streamlined some portions of analysis, an example of which is distilling all possible threats for threat tree construction into four broad categories.

3.3.3. Cybersecurity-Centric Frameworks

The MITRE Corporation has taken a risk-based, threat-informed Cyber Mission Assurance Engineering (MAE) approach to addressing challenges presented by advanced cyber threats (MITRE, 2013). Cyber resiliency engineering is a sub-discipline of MAE and focuses on (i) the ways in which an evolving set of resilience practices can be applied to improve cyber resiliency, and (ii) the trade-offs associated with different strategies for enacting those practices (Bodeau & Graubart, 2011). As shown in Figure 3-11, cyber resiliency engineering brings together key aspects of mission assurance engineering, resilience engineering, and cyber security (MITRE, 2013).

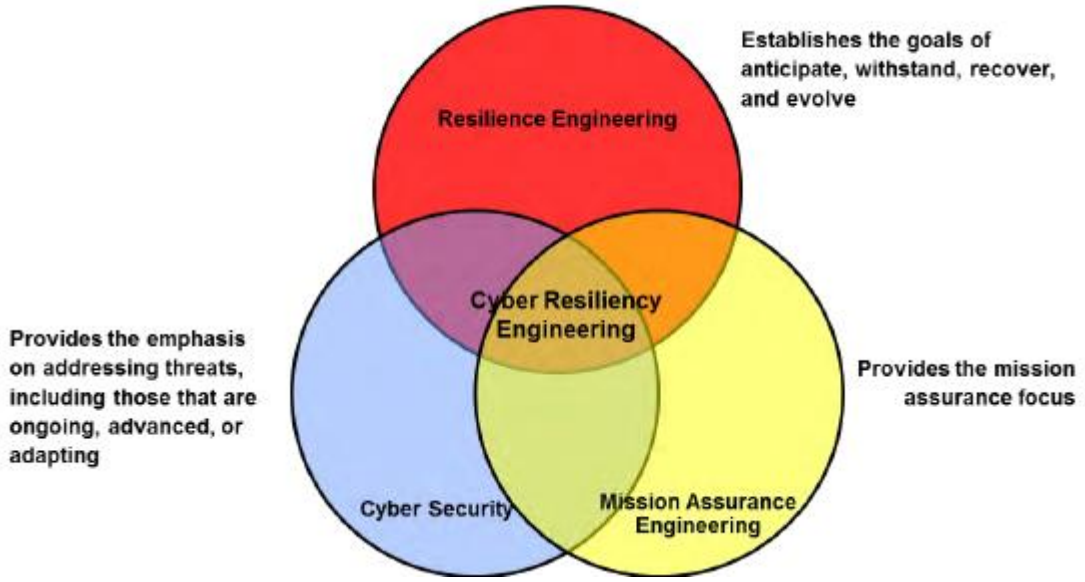


Figure 3-11. Cyber Resiliency Engineering (Bodeau & Graubart, 2011).

The primary objective of Cyber MAE is to enable organizations and missions that depend on cyberspace to reach their goals despite threats exploiting that dependence, in particular advanced threat actors (MITRE, 2013). Cyber MAE consists of processes, consistent with a conceptual and analytic framework, that can complement and extend existing processes to facilitate cost-effective risk management (MITRE, 2013). These Cyber MAE processes rely on capabilities including tools, knowledge bases, procedures, and worked examples to select appropriate mitigation techniques and to secure cyber systems (MITRE, 2013). Threat Assessment & Remediation Analysis (TARA), Resilient Architectures for Mission and Business Objectives (RAMBO), and System of Systems (SoS) Security Systems Engineering (SSE) are three Cyber Resiliency Engineering Frameworks (CREFs) developed to address cyber risks (Bodeau & Graubart, 2011; Rebovich et al., 2014).

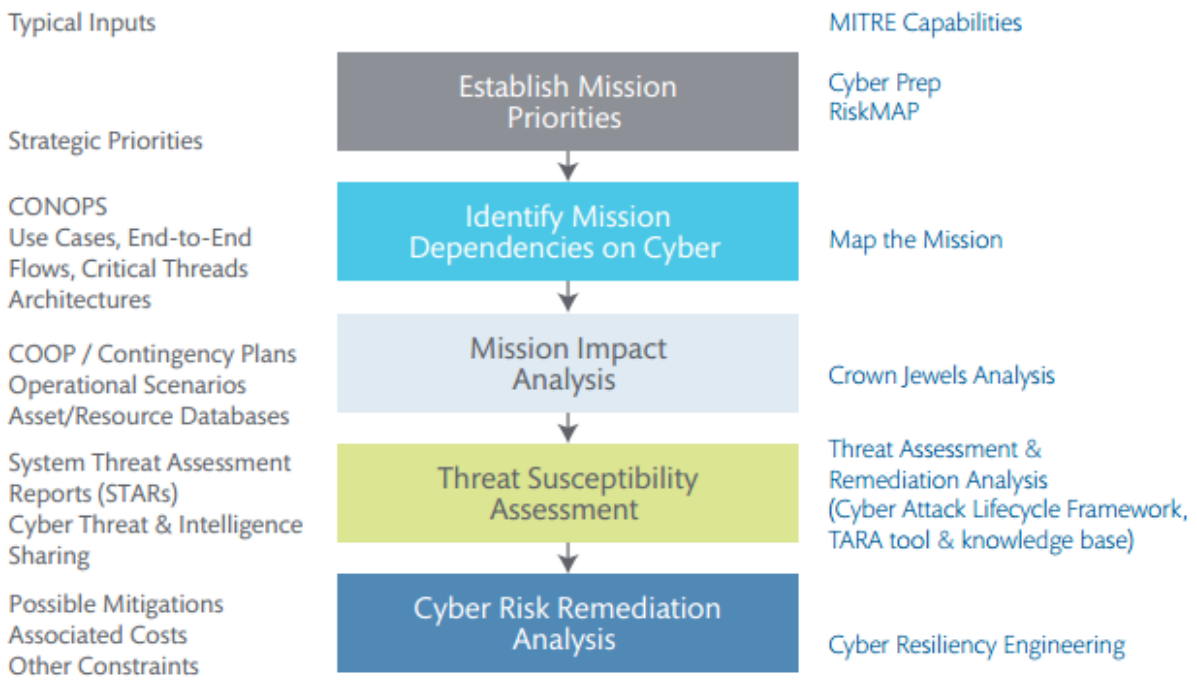


Figure 3-12. MITRE Cyber MAE Capabilities (MITRE, 2013).

Cyber Mission Assurance Engineering (MAE) is a risk-based, threat-informed approach to address advanced adversaries (MITRE, 2013). Cyber MAE focuses on advanced cyber threats that present a challenge to established engineering and strategic analysis processes; the methodology facilitates cost-effective risk management through complementing and extending established processes (MITRE, 2013). Cyber MAE is comprised of processes, consistent with a conceptual and analytic framework, realized through capabilities including tools, knowledge bases, procedures, and worked examples (MITRE, 2013).

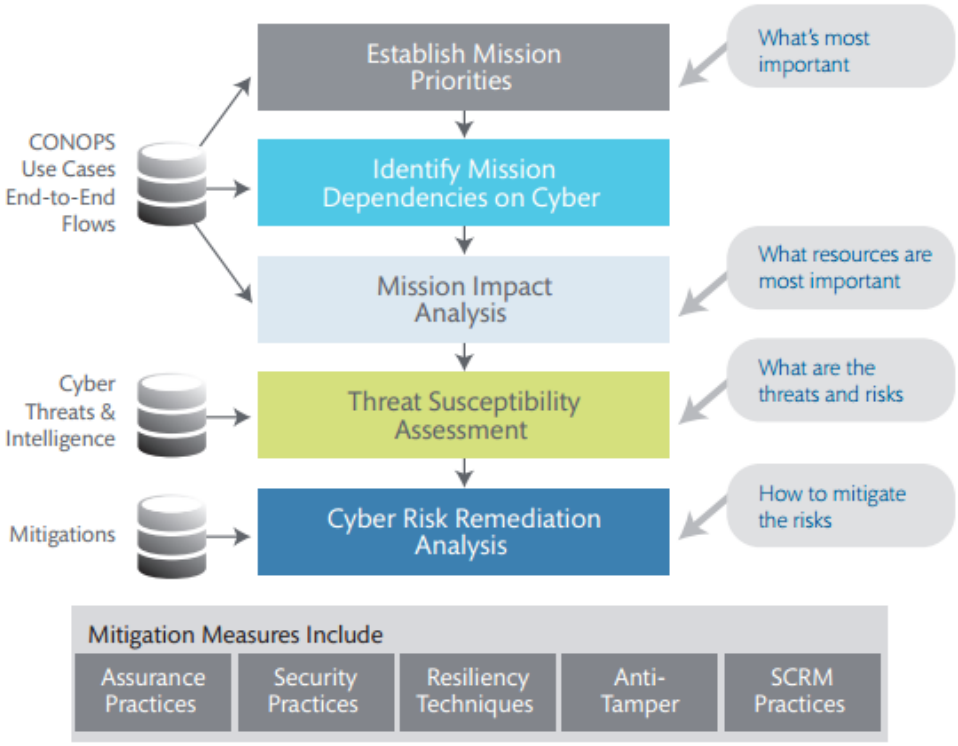


Figure 3-13. MITRE Cyber MAE Methodology (MITRE, 2013).

Threat Assessment & Remediation Analysis (TARA) is another methodology developed by The MITRE Corporation to identify and assess cyber threats and to select countermeasures capable of mitigating those threats (Wynn et al., 2011). TARA applies MAE to systems and acquisitions and is particularly effective when applied in conjunction with a Crown Jewels Analysis (CJA) assessing mission impact; the two in concert allow for the identification, assessment, and security enhancement of mission critical assets (Wynn et al., 2011).

The TARA methodology includes three distinct activities: Cyber Threat Susceptibility Analysis (CTSA), Cyber Risk Remediation Analysis (CRRA), and Data and Tools development (Wynn et al., 2011). These activities in turn support three workflows: TARA assessments, catalog development, and toolset development (Wynn et al., 2011). A TARA assessment is sponsor-directed and evaluates selected cyber assets using data about known adversarial Tactics, Techniques, and Procedures (TTPs) and countermeasures as documented in catalogs (Wynn et al., 2011). The assessment is a three-step process and ultimately delivers recommendations allowing program managers to make informed decisions on how to make a system less vulnerable and more resilient upon deployment (Wynn et al., 2011). A TARA assessment can

take place immediately following a Crown Jewels Analysis, in which mission-critical cyber assets are identified, and can be performed on and benefit deployed systems as well as systems still in the acquisition lifecycle (Wynn et al., 2011). Catalog and toolset development ensures that catalogs, mappings, and software tools are consistent and up-to-date (Wynn et al., 2011). It is important to note that the toolset contains tools that can be tailored to quantitatively assess TTP risk and the cost-effectiveness of selected countermeasures (Wynn et al., 2011).

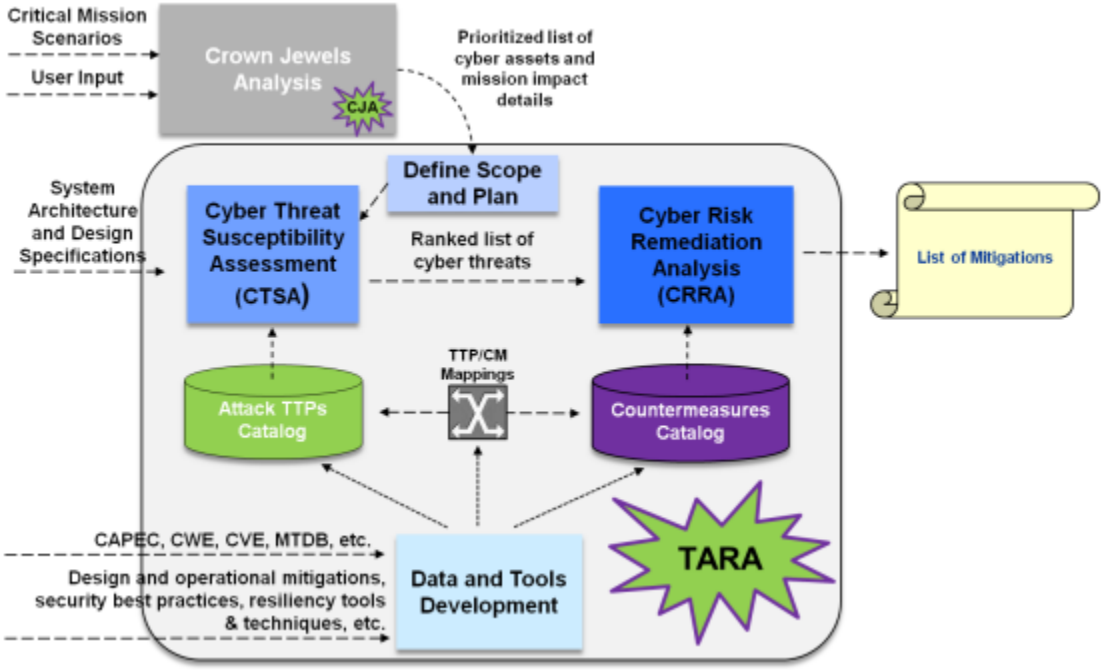


Figure 3-14. MITRE TARA Methodology (Wynn et al., 2011).

Resilient Architectures for Mission and Business Objectives (RAMBO) is another MITRE framework which describes an initial set of technical and cost metrics pertaining to cyber resiliency (Bodeau et al., 2012). RAMBO establishes an approach to identify, characterize, and define cyber resiliency metrics and prototypes a tool enabling the evaluator to identify cyber resiliency metrics from the representative set that are most relevant to their needs (Bodeau et al., 2012). These metrics can then be applied either across an entire enterprise or to a specific implementation of a RAMBO technology (Bodeau et al., 2012).

RAMBO assesses how government information-system architectures can remain resilient during certain types of cyber attacks and offers recommendations for how organizations should design, deploy, and operate critical systems to allow for system reconfiguration and data recovery given

compromised data, system components, or services (Lee, 2012). The methodology encourages organizations to protect and prepare, monitor and respond, constrain and isolate, maintain and recover, and continuously adapt en route to working towards resilient architectures (Lee, 2012).

System of Systems (SoS) Security Systems Engineering (SSE) is an actionable engineering framework developed by MITRE that provides a structured systems engineering approach to handling security for SoS supporting missions (Rebovich et al., 2014). For reference, SoS refers to a set or arrangement of systems that result when independent and useful systems are integrated into a larger system that delivers unique capabilities (Rebovich et al., 2014). The framework tackles the question of whether existing SSE risk-based methodology can be applied to SoS, in particular to focus on the mission impact of security threats to and vulnerabilities of supporting SoS, constituent systems, enabling infrastructure, and interdependencies (Rebovich et al., 2014). SoS SSE provides technical grounding for security-related investments in order to improve the likelihood of successful mission outcomes and is utilized by both organizations responsible for delivering technically robust mission capabilities and decision makers responsible for system investments (Rebovich et al., 2014).

The proposed SoS SSE framework allows for increased recognition of persistent threats and the impact of these threats on critical mission outcomes, considers operational system configurations and possible improvements to legacy systems to counter residual risk, and is cognizant of the complex environment and challenges associated with applying system-level approaches to SSE (Rebovich et al., 2014). As shown in Figure 3-15, the SoS SSE framework can be thought of as a bridge between acquisition/engineering and operations, as it is capable of implementing fixes to fielded and new systems in an effort to tackle current operational risks (Rebovich et al., 2014).

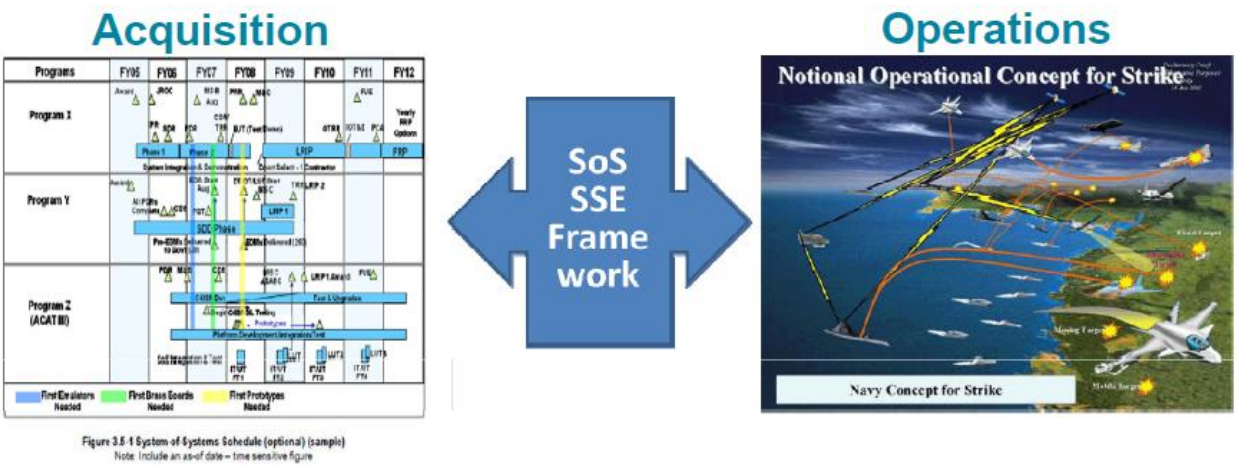


Figure 3-15. SoS SSE Framework Bridging Acquisition and Operations (Rebovich et al., 2014).

The SoS SSE framework puts SSE into an SE and SOS context and consists of the following five steps:

1. SoS Baselining – Establish structured understanding of the SoS as an end-to-end system.
2. SoS Criticality Analysis – Conduct analysis to identify key areas of SoS to be protected.
3. Focused Security Risk Analysis – Apply current threat, vulnerability, risk, and countermeasures approaches to critical elements of the SoS.
4. Risk Mitigation Identification & Evaluation – Apply current threat, vulnerability, risk, and countermeasures approaches to critical elements of the SoS. Risk Mitigation
5. Implementation & Feedback – Implement changes and refine as necessary as part of a current acquisition process (Rebovich et al., 2014).

3.3.4. Service-Oriented Architecture-Centric Frameworks

ATLIST, named for the "attentive listener," is a vulnerability assessment method developed during and for the analysis of service-oriented architecture (SOA) service orchestrations (Lowis & Accorsi, 2011). ATLIST is applicable to business processes comprised of services as well as to single services; the method facilitates the detection of known vulnerability types and allows for the derivation of vulnerability patterns for tool support (Lowis & Accorsi, 2011). The method consists of three steps:

1. Element instantiation.
2. Tree building and examination.
3. Refinement of vulnerability details (Lowis & Accorsi, 2011).

An ATLIST tree is developed by composing predefined analysis elements including point of view, attack effect, active component, involved standard, and triggering property (Lowis & Accorsi, 2011). The main analysis consists of creating one ATLIST tree for each attack effect as shown in Figure 3-16.

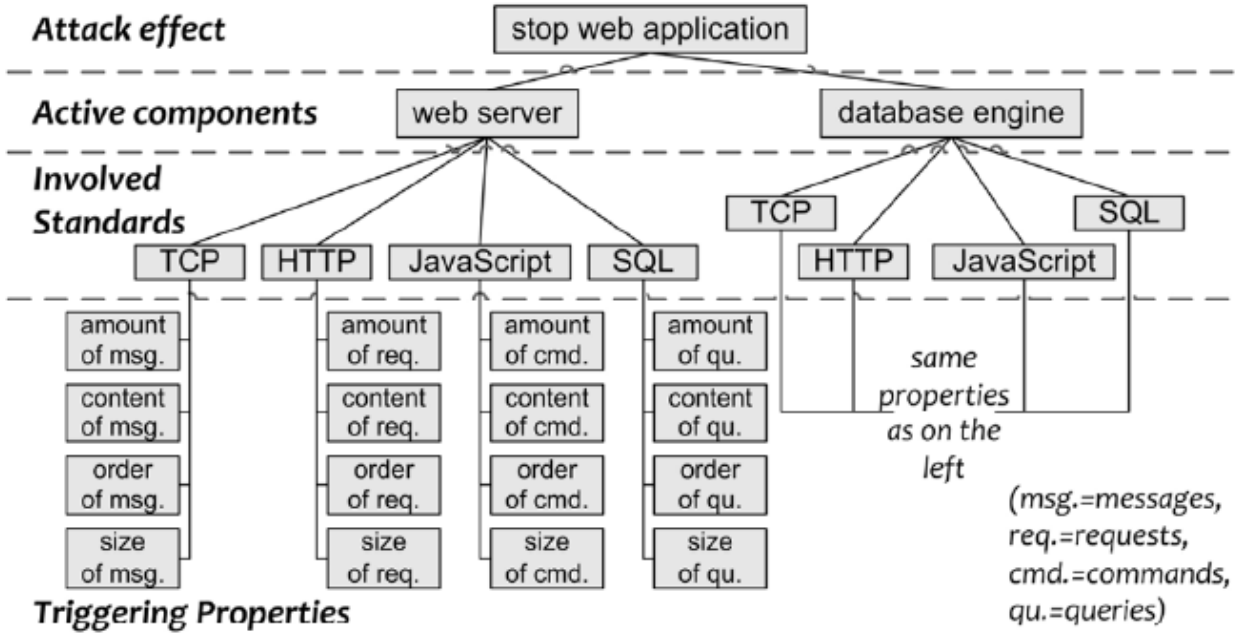


Figure 3-16. Example ATLIST Tree (Lowis & Accorsi, 2011).

ATLIST improves upon prior SOA-centric vulnerability assessment methods by offering better transferability through the use of established analysis elements (Lowis & Accorsi, 2011). It is interesting to note that ATLIST blends elements of the FTA and FMEA approaches while providing additional guidance regarding starting points and the focus of the analysis, preventing the vulnerability assessment from becoming circuitous (Lowis & Accorsi, 2011).

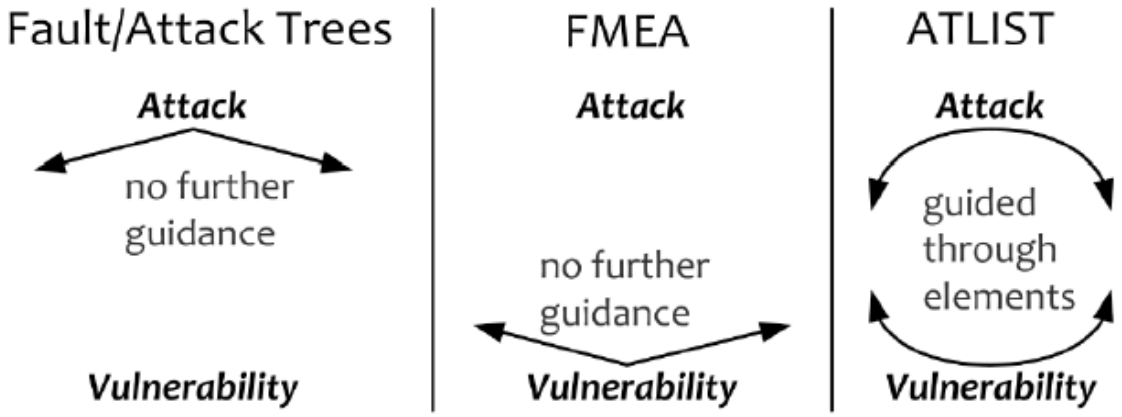


Figure 3-17. Comparison of Fault Trees, FMEA, and ATLIST (Lowis & Accorsi, 2011).

3.3.5. Operation and Theater-Centric Frameworks

The RAND Vulnerability Assessment Method Pocket Guide (VAMPG) explains how the Vulnerability Assessment Method (VAM), which differs from the Vulnerability Assessment & Mitigation methodology described above, can be embedded into doctrinal planning processes and large-scale exercises (Schnaubelt et al., 2014). This method, specifically developed for use at the operational and tactical level, was spearheaded by the U.S. Army Asymmetric Warfare Group (Schnaubelt et al., 2014). VAM enumerates a process for identifying adversary, friendly, and other key stakeholder centers of gravity to support the construction of plans that can exploit an adversary's vulnerabilities while protecting friendly systems and components (Schnaubelt et al., 2014). This method can enable commanders, leaders, and planners to identify what is most important both in adversary and non-adversary systems and to prevent wasted resources generated from less productive courses of action (Schnaubelt et al., 2014).

The five steps of applying the VAMPG are as follows:

1. Receive mission; understand higher headquarters guidance and strategic direction.
2. Understand the operational environment.
3. Frame and define the problem.
    a. Identify the problem or problem set, then view it as an adversary system.
    b. Determine the adversary Center of Gravity (COG):
        i. Identify the organization's desired ends (what are the adversary's goals?).

ii. Identify “ways” or actions that can achieve the desired ends.
iii. Select the way(s) the organization is most likely to use. This identifies the critical capability(ies).
iv. List the organization’s means or resources available or needed to execute the critical capability.
v. Select the entity (tangible agent) from the list of means that inherently possess the critical capability. This is the COG. It is the doer of the action that achieves the ends.

c. Identify the adversary COG’s critical requirements, then its critical vulnerabilities:
    i. From the remaining means select those that are critical for execution of the critical capability. These are the critical requirements.
    ii. Complete the process by identifying the critical requirements that are vulnerable to adversary action. These are the critical vulnerabilities.

4. Develop the operational approach:
    a. Identify own COG and those of other key stakeholders (friends and allies, neutrals, others), critical requirements, and critical vulnerabilities (i.e., repeat 3.b and 3.c).
    b. Assess and prioritize vulnerabilities for attack or protection.
    c. Determine initial decisive points.
    d. Determine lines of operation (LOOs) or lines of effort (LOEs).
    e. Decide on and document the operational approach.
    f. Issue guidance and direction.
5. Assess performance and effectiveness:
    a. Monitor.
    b. Evaluate.
    c. Recommend or direct action (Schnaubelt et al., 2014).

A comparison of several frameworks as shown in Table 3-5 illustrates that most contain provisions for screening analysis along with some variety of in-depth or focused analysis and mitigation (Eusgeld et al., 2009). Chapter 4 expands the research investigation into the area of supply chain vulnerability and associated frameworks and queues up model development.

Table 3-5. Comparison of Vulnerability Assessment Techniques.

STEP	Haimes (2006)	Aven (2007)	CARVER (Antón et al., 2004)	VAM (Antón et al., 2004)	SQUARE (Mead et al., 2005)	OCTAVE Allegro (Caralli et al., 2007)	Cyber MAE (MITRE, 2013)	SoS SSE Framework (Rebovich et al., 2014)	VAMPG (Schnaubelt et al., 2014)
1	Assess attack likelihood	Identify functions to be analyzed and performance measures	Identify vulnerabilities	Identify essential information functions	Agree on definition	Establish risk measurement criteria	Establish mission priorities	Baselining	Receive mission
2	Model interdependent state variable responses	Define systems to meet functions	Prioritize vulnerabilities	Identify essential information systems	Identify security goals	Develop information asset profile	Identify mission dependencies on cyber	Criticality analysis	Understand operational environment
3	Assess consequence severity	Identify relevant sources	Brainstorm countermeasures	Identify vulnerabilities	Develop artifacts	Identify information asset containers	Mission impact analysis	Focused security risk analysis	Frame and define problem
4		Perform uncertainty analysis of sources	Assess risks	Identify security techniques to mitigate vulnerabilities	Perform risk assessment	Identify areas of concern	Threat susceptibility assessment	Risk mitigation identification and evaluation	Develop operational approach
5		Perform consequence analysis		Select and apply techniques	Select elicitation techniques	Identify threat scenarios	Cyber risk remediation analysis	Implementation and feedback	Assess performance and effectiveness
6		Describe risks and vulnerabilities		Test for robustness and actual feasibilities	Elicit security requirement	Identify risks			
7		Evaluate risks and vulnerabilities			Categorize requirements	Analyze risks			
8		Identify possible measures			Prioritize Requirements	Set mitigation approach			
9					Requirements inspection				

CHAPTER 4: EXPANSION TO SUPPLY CHAIN AND MODEL DEVELOPMENT

Supply chains are becoming increasingly complex, leading to increased interdependencies among companies or individuals, and can be disrupted in myriad ways in today's rapidly-changing global business environment (Hennet et al., 2008; Nowakowski et al., 2015). Achieving a better understanding of supply chain vulnerability and resilience has become imperative for many companies, as inevitable supply chain disruptions can result in detrimental performance and economic impacts (Murino et al., 2011; Nowakowski et al., 2015). A company needs to know the current level and drivers of vulnerability within a supply chain in order to proactively manage risk and ensure resiliency. The identification and evaluation of potential system vulnerabilities, often through the use of empirically-validated methods, can determine whether enhanced security requirements or constraints are necessary to protect the supply chain and the environment in which the system operates (Wagner & Neshat, 2012).

For the purposes of this thesis, the term "supply chain" includes any point in a system's design, engineering and manufacturing development, production, test and evaluation, configuration in the field, updates, and maintenance (Baldwin et al., 2012). This can be thought of as the network of organizations that are involved, through both upstream and downstream linkages, in the different processes and activities that produce value in the form of products and services in the hands of the ultimate consumer (Christopher, 1998; Peck, 2006). Furthermore, supply chains can be thought of as three different interdependent, interacting networks consisting of:

1. A physical logistics system for transporting goods.
2. A transaction-based system that procures and distributes goods and that is driven primarily by information flows.
3. An oversight system that implements and enforces rules of behavior within and among the subsystems through standards, fines, and duties (Van de Voort et al., 2007).

4.1. Supply Chain Vulnerability

The term "supply chain vulnerability" has been studied and defined in various ways, and several different interpretations are present in the research literature as illustrated in Table 4-1 (Nowakowski et al., 2015). Attacks to a supply chain seek to exploit weaknesses in the system's

defense or to decrease performance; therefore, all aspects of supply chain performance must be taken into consideration when assessing security measures (Van de Voort et al., 2007).

Table 4-1. Definitions of Vulnerability in Supply Chain Contexts (Wagner & Neshat, 2012).

Albino & Garavelli, 1995	"…aimed to estimate the system sensitivity to changes, in terms of damages to performance due to the intrinsic system incapacity of reaction to unexpected events."
Asbjørnslett, 2009	"…concept that may be used to characterize a supply chain system's lack of robustness or resilience with respect to various threats that originate both within and outside its system boundaries. The vulnerability of a supply chain system may be manifested both in its infrastructures – both nodal and modal, its processes, as well as the operation and management of the supply chain."
Bakshi & Kleindorfer, 2009	"…possibility of occurrence of a disruption. It is determined by a combination of the kind of infrastructure already in place for risk mitigation, as well as environmental factors such as political turmoil, proximity to a fault line/volcano, etc." "Mathematically, we capture the concept of vulnerability through the supplier's marginal probability of disruption as a function of investment."
Barnes & Oloruntoba, 2005	"…susceptibility or predisposition to change or loss because of existing organizational or functional practices or conditions."
Christopher & Peck, 2004	"An exposure to serious disturbance, arising from risks within the supply-chain as well as risks external to the supply-chain."
Jüttner et al., 2003	"The propensity of risk sources and risk drivers to outweigh risk mitigating strategies, thus causing adverse supply chain conditions."
Svensson, 2002	"…condition that is caused by time and relationship dependencies in a company's business activities in supply chains. The degree of vulnerability may be interpreted as proportional to the degree of time and relationship dependencies, and the negative consequence of

	these dependencies, in a company's business activities towards suppliers and customers."
Wagner & Bode, 2009	"…susceptibility of the supply chain to the harm of [a supply chain disruption] is of significant relevance. This leads to the concept of supply chain vulnerability. The basic premise is that supply chain characteristics are antecedents of supply chain vulnerability and impact both the probability of occurrence as well as the severity of supply chain disruptions."
Wagner & Neshat, 2012	"…a function of certain supply chain characteristics and that the loss a firm incurs is a result of its supply chain vulnerability to a given supply chain disruption."

The impact of decisions and other factors on supply chain vulnerability is shown in Figure 4-1:

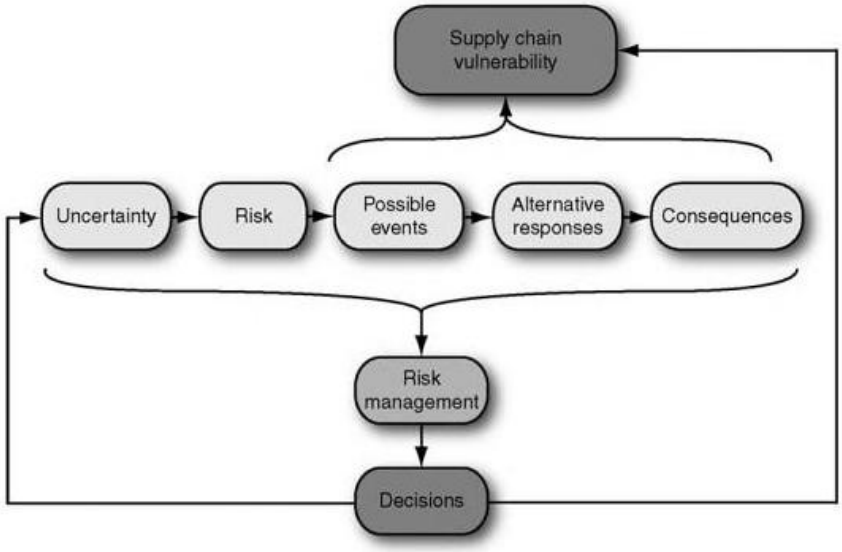


Figure 4-1. Vulnerability Within a Typical Supply Chain (Waters, 2011).

As discussed previously, vulnerability is closely related to resilience (Steen & Aven, 2011; Nowakowski et al., 2015). Key parameters of supply chain resilience include:

- Readiness – the probability of disruptions occurrence;
- Response – the level of consequences of those disruptions occurrence;

- Recovery – the time to recover to normal state from disruption state (Bora et al., 2014; Nowakowski et al., 2015).

Supply chain vulnerability and resiliency is broader in scope than supply chain management, business continuity planning, and commercial corporate management, as political and public policy dimensions exist and will be further explored in Chapter 6 (H. Peck, 2005). Supply chain management is a complex endeavor on its own, given continuous regulatory changes and the issues associated with managing across different legal, environmental, and cultural settings (H. Peck, 2005). Governments are looking to the private sector to reduce costs and improve efficiency in the delivery and management of infrastructure and services; the private sector in turn experiences commercial pressures to engage in lean manufacturing without having a full understanding of the impact on network resilience (H. Peck, 2005). Slack in a system, coupled with constant awareness and vigilance, is necessary if a supply chain is to become resilient and sustain a given level of resiliency (H. Peck, 2005).

The following four principles are asserted to promote supply chain resilience as shown in Figure 4-2:

1. Resilience can be built into a system prior to a disruption.
2. Risks can be managed and identified through a high level of collaboration.
3. Agility to react promptly to unforeseen events is essential.
4. A culture of risk management is a necessity (Christopher & Peck, 2004).

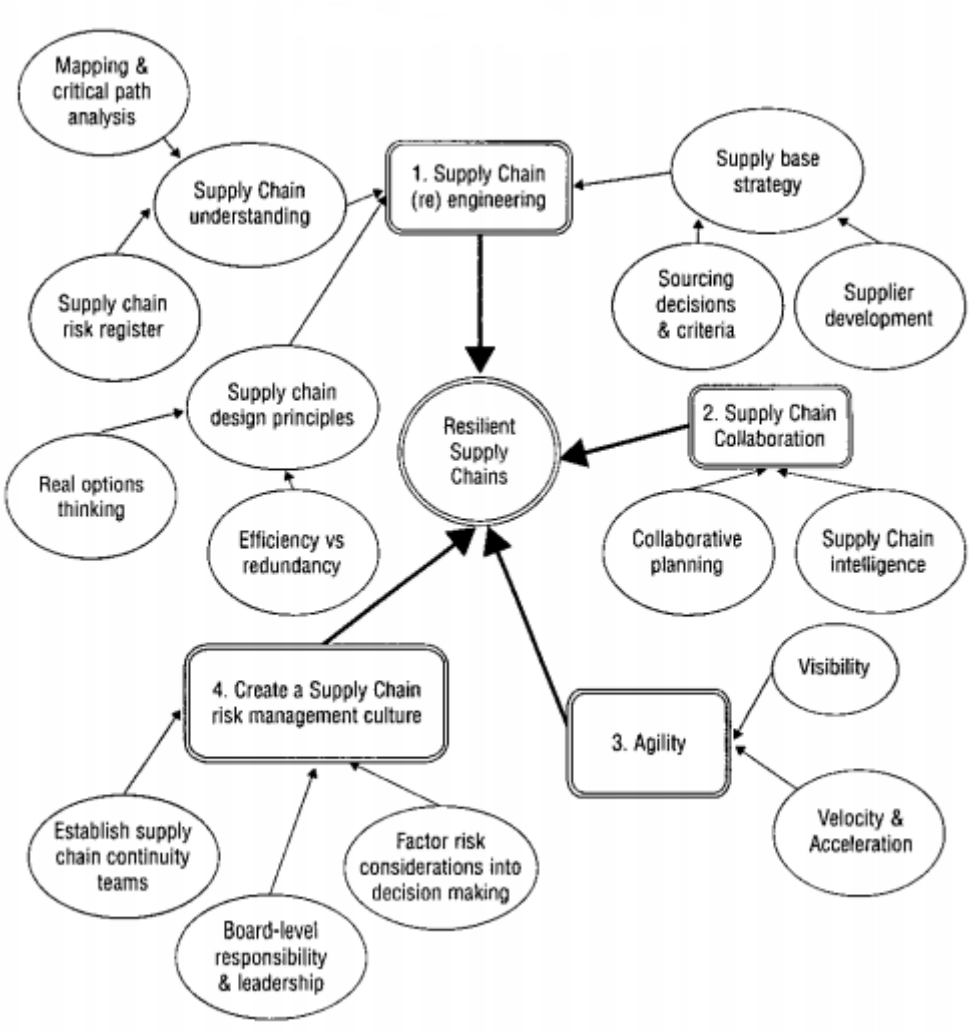


Figure 4-2. Factors for a Resilient Supply Chain (Christopher & Peck, 2004).

The dynamic and evolving nature of supply chain risk and vulnerability implies that a supply chain strategy is highly unlikely to ever be risk-free, and that a system, however well-fortified, is unlikely to ever be shielded from all vulnerabilities (H. Peck, 2005). There is often a disconnect between the functional goals of supply chain management and higher-level organizational structure and business strategy changes; the implications of strategic decisions on a supply chain frequently go unrecognized until problems occur (H. Peck, 2005). Both public and private sector organizations may choose to accept the risk as-is, concluding that the benefits of continuous improvement initiatives outweigh the costs of mitigating the impact of a potential disruption (H. Peck, 2005).

4.1.1. Sources of Supply Chain Disruption

As discussed earlier in Chapter 2, supply chain failure occurs when the product or service provided by the supply chain is unable to be delivered per specifications to the customer (Neureuther & Kenyon, 2009). This can occur due to disruption in supply, disruption in transportation, disruption at facilities, freight breaches, disruption in communications, and disruption in demand (Sheffi et al., 2003).

Five likely areas of supply chain disruption include supply failure, manufacturing operations failure, logistics failure, information and technology failure, and workforce unavailability (Plenert et al., 2012; Nowakowski et al., 2015). Sources of disruption for a specific company may depend on factors such as the industry, location, operating strategies, suppliers, customers, political situation, and government policies (Stecke & Kumar, 2009). Four identified "vulnerability causing factors" for a supply chain include increase in the number of exposure points, increase in distance/time, decrease in flexibility, and decrease in redundancy; Table 4-2 highlights the relationships between these vulnerability causing factors and current supply chain management practices (Stecke & Kumar, 2009). Additional factors contributing to supply chain disruptions may include globalized supply chains (and associated geo-political and economic dependencies), specialized factories, centralized distribution, increased outsourcing, reduction in supplier base, increased volatility of demand, and technological innovations (Cranfield University School of Management, 2002; Centre for Logistics and Supply Chain Management at the Cranfield School of Management, 2003; Pettit et al., 2010).

Table 4-2. Supply Chain Practices and Their Effect on Vulnerability Causing Factors (Stecke & Kumar, 2009).

	Vulnerability causing factors			
Supply chain management practices	Increase in the number of exposure points	Increase in distance/time	Decrease in flexibility	Decrease in redundancy
Globalization	X	X		
Decentralization	X	X		
Outsourcing	X	X		
Sole sourcing			X	
JIT			X	X
Product/process complexity	X			
Litigation	X			

4.1.2. Supply Chain Vulnerability and the DoD

Department of Defense (DoD) programs face major system security challenges (LeSaint et al., 2015). DoD systems have become increasingly reliant on commercially-available technology, which is frequently developed and manufactured outside of the U.S. (LeSaint et al., 2015). These components are readily available throughout the world to be studied, reverse engineered, and exploited (McGrath et al., 2002; LeSaint et al., 2015). Another issue is the complex nature of the supply chains necessary to sustain major acquisition programs; these tend to contain layer upon layer of prime contractors, subcontractors, suppliers, and sub-suppliers (LeSaint et al., 2015). This makes it difficult to be aware of each and every component in the system along with their respective origins and manufacturing history.

DoD systems have become increasingly networked and software-intensive and depend on a complicated global supply chain (LeSaint et al., 2015). This has increased both complexity and the importance of security as a systems design consideration, as systems engineers play a key role in making security-related accommodations during system specification, design, and implementation. The insertion of malicious logic is one way that a vulnerability within a supply chain can be exploited (Shanahan, 2014). Access points are present throughout the system lifecycle and across multiple supply chain entry points, from Government to prime and sub-contractors to vendors and commercial parts manufacturers to third party test and certification activities (Reed, 2014).

4.2. Supply Chain Vulnerability Assessment

Assessing the vulnerability of a supply chain can be a complex, challenging task (Vlajic et al., 2013; Nowakowski et al., 2015). Key issues to be considered include:

- The necessity to define variables driving vulnerability (such as supply chain complexity).
- The identification and categorization of potential disruptions according to probability of occurrence and consequences.
- The definition of the main interrelationships between the defined drivers and disruptions.
- The development of a multi-dimensional measure of supply chain vulnerability, employing both well-known and new methods (Asbjørnslett, 2009; Sheffi & Rice Jr., 2005; Wagner & Neshat, 2012; Nowakowski et al., 2015).

4.2.1. Supply Chain Vulnerability Assessment Frameworks

Several frameworks for assessing supply chain vulnerability currently exist in risk management and supply chain management literature (Nowakowski et al., 2015). These include:

- Supply Chain Event Management (SCEM).
- Supply Chain Risk Management (SCRM).
- Resilient and secure supply network, Business Continuity Planning (BCP).
- Supply Chain Vulnerability Workbook Flow.

4.2.1.1. Supply Chain Event Management

Supply Chain Event Management (SCEM) engages partners in a supply chain to collaborate and identify nodes and links critical to the flow of materials and information (Stiles, 2002; Christopher & Lee, 2004). SCEM effectively acts like a hospital intensive care monitor, which uses probes measuring different, discrete functions at strategic points on a patient's body (Stiles, 2002). Control limits are defined at the supply chain node and link level; if the level of activity reaches a level outside the control limit, an automatically-generated alert is issued and allows for corrective action (Christopher & Lee, 2004). SCEM is an umbrella application, encompassing the entirety of a supply chain; when used correctly, it can allow decision-makers to analyze each link in the supply chain, to detect anomalies earlier than normal, and to alter any processes that increase costs or place limitations upon the system (Stiles, 2002). This can ultimately increase operational efficiency and lead to SCEM becoming a source of competitive advantage (Stiles, 2002).

A successful SCEM application can be achieved by the following steps:

1. Analyze each function and system within the supply chain and decide what data SCEM should receive and what decisions SCEM should make.
2. Determine unique measurement points along the supply chain and install appropriate probes.
3. Program the SCEM application to monitor the plan-to-actual supply chain progress and establish upper and lower control limits.
4. Publish alerts or alarms if control limits are exceeded or anomalies occur so that corrective action can occur.

5. Utilize SCEM information and feedback to execute strategic, incremental continuous improvement, particularly in the areas of data compliance and quality, and to create enhanced plans, processes and procedures, ways-of-working, and metrics (Stiles, 2002).

4.2.1.2. Supply Chain Risk Management

The Supply Chain Risk Management (SCRM) approach outlined by Jüttner, Peck, and Christopher takes supply chain risk sources, risk consequences, risk drivers, and risk mitigating strategies into account as shown in Figure 4-3 (Jüttner et al., 2003). SCRM is particularly useful for evaluating potential parts for supply chain-related vulnerabilities early in the system life cycle while design changes and component substitutions are easily performed (Baldwin et al., 2012).

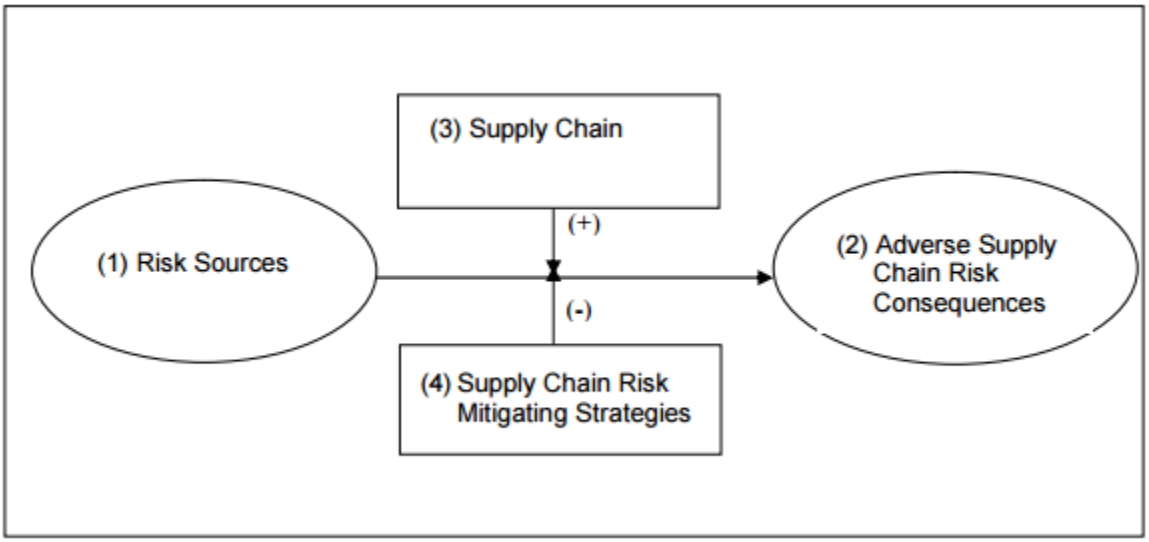


Figure 4-3. Supply Chain Risk Management Construct (Jüttner et al., 2003).

Implementing SCRM into the system development life cycle can be beneficial when designs are evaluated and alternative parts considered, and additional instruction can be found in the Supply Chain Risk Management Practices for Federal Information Systems and Organizations document (Baldwin et al., 2012; Boyens et al., 2015). A framework for directing future research in Supply Chain Risk Management is proposed consisting of the following steps:

1. Assessing the risk sources for the supply chain, in particular environmental, network, and organizational risk.
2. Defining the risk concept and adverse consequences.
3. Identifying the risk drivers of the supply chain strategy.

4. Mitigating risks in the supply chain (Jüttner et al., 2003).

4.2.1.3. Business Continuity Planning

Business Continuity Planning (BCP) focuses on minimizing the effects of unanticipated events on meeting customer requirements and involves developing plans for a system or supply chain to be resilient (Zsidisin et al., 2005; Rice Jr. & Caniato, 2003). This entails being in a position to respond to and restore operations following an unexpected, major disruption in a timely manner (Rice Jr. & Caniato, 2003). BCP can improve supply chain security through exposing weaknesses in the system and then focusing efforts to address identified weaknesses; BCP also assists a company or individual in making better decisions with respect to what level of resilience and security is desired (Rice Jr. & Caniato, 2003). Finally, BCP takes non-supply chain factors into consideration, including IT and leadership succession, as the integration of information and procedures can further contribute to system recovery following a disruption (Savage, 2002; Barnes, 2001).

The four steps to developing an effective BCP are:

1. Identify threats or risks.
2. Conduct a business impact analysis.
3. Adopt controls for prevention and mitigation.
4. Test, exercise, improve your plan routinely (Travelers, 2016).

4.2.1.4. Supply Chain Vulnerability Workbook Flow

The Supply Chain Vulnerability Workbook Flow was developed by LCP Consulting in conjunction with the Centre for Logistics and Supply Chain Management at the Cranfield School of Management. The Supply Chain Vulnerability Workbook Flow has four steps as shown in Figure 4-4 and enumerated below:

1. The company is guided to identify and describe supply chains in which it is a participant.
2. The company is encouraged to test each supply chain identified above utilizing the six dimensions of possible vulnerability (demand, supply, environment, control, process, contingency) to identify critical issues and areas of concern.
3. The exposure of the company to each of the four key risk characteristics (scale, duration, recovery, cost) is determined.

4. The company is encouraged to enact the provided framework to explore the potential to put mitigation and contingency actions in place (Centre for Logistics and Supply Chain Management at the Cranfield School of Management, 2003).

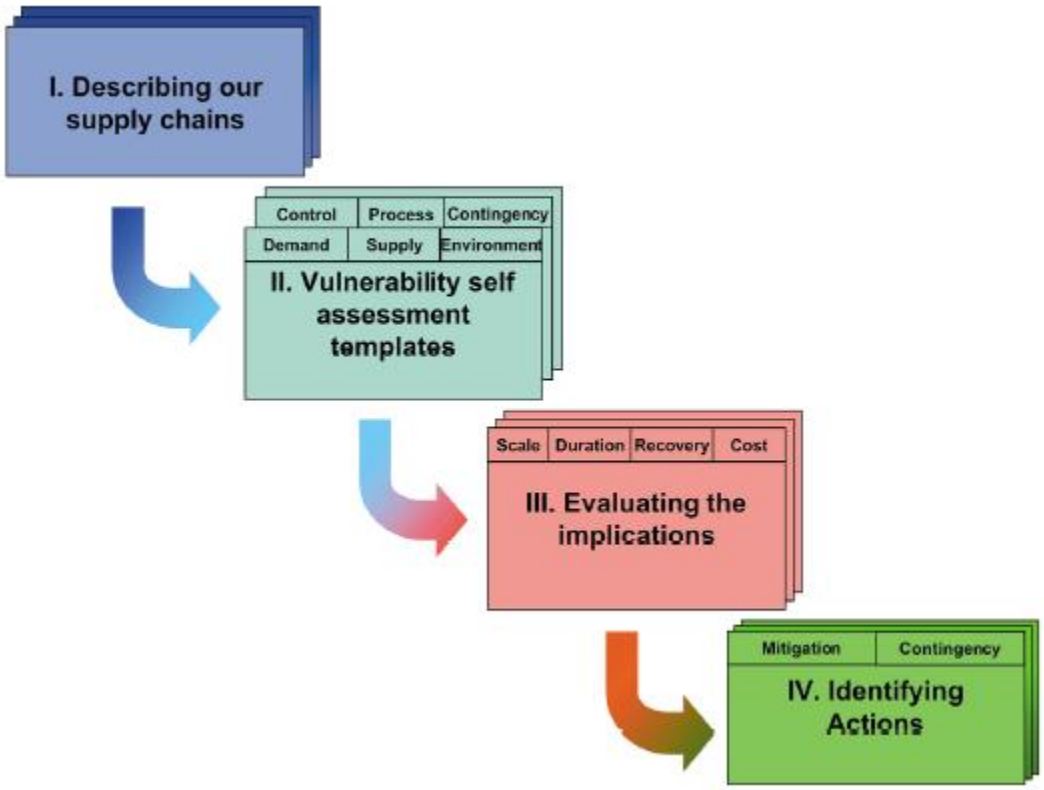


Figure 4-4. Supply Chain Vulnerability Workbook Flow (Understanding Supply Chain Risk, 2003).

As shown in Table 4-3, these four frameworks for supply chain vulnerability assessment again demonstrate the critical need for screening activities, such as identifying threats and risks, and an in-depth or focused analysis tailored to the characteristics of a given supply chain (Eusgeld et al., 2009). Business considerations and controls are also imperative for formulating mitigations and ensuring a resilient supply chain.

Table 4-3. Comparison of Supply Chain Vulnerability Assessment Techniques.

STEP	SCEM (Stiles, 2002)	SCRM (Jüttner et al., 2003)	BCP (Zsidisn et al., 2005)	Supply Chain Vulnerability Workbook Flow (Cranfield SOM, 2003)
1	Analyze functions and systems and decide what data SCEM should receive and what decisions SCEM should make	Assess risk sources	Identify threats or risks	Identify and describe supply chains
2	Determine measurement points and install probes	Define risk concept and adverse consequences	Conduct a business impact analysis	Test identified supply chains using six dimensions of possible vulnerability to identify critical issues and areas of concern
3	Program SCEM application to monitor progress and establish control limits	Identify risk drivers of supply chain strategy	Adopt controls for prevention or mitigation	Determine the exposure of the company to each of the four key risk characteristics
4	Publish alerts or alarms if control limits exceeded in order to begin corrective action	Mitigate risks in supply chain	Test, exercise, and improve plan	Enact provided framework to explore potential to put mitigation and contingency actions in place
5	Utilize SCEM information and feedback to execute continuous improvement			

4.3. Generic Model Development

Experts tacitly agree that a conceptual model for vulnerability assessment should take the form of a stepwise, problem-driven approach tailored to the needs of the evaluation or analysis (Kröger & Zio, 2011). None of the currently available models, methods, or frameworks alone is capable of addressing and tackling the myriad issues associated with supply chain vulnerability assessment,

including the impact of system (inter)dependencies (Kröger & Zio, 2011). A universal, all-encompassing "silver bullet" model or approach capable of comprehensively addressing all issues simply does not exist (Eusgeld et al., 2009; Johansson & Hassel, 2010; Kröger & Zio, 2011). This necessitates a conceptual model to amalgamate all aspects, attributes, and capabilities and to go beyond the pure analytical framework or architecture (Kröger & Zio, 2011).

The generic supply chain model is greater in scope and reveals more information than the CEM case application shown in Figure 5-1. The model was developed by studying historical information, engaging in discussions with SMEs, and analyzing and applying empirical data. Many frameworks were examined for similarities with respect to conducting system vulnerability assessments and analyzing supply chain risk, and facets of SSE and TSN along with leading indicators were incorporated into the model.

The primary purpose of the generic model is to enhance vulnerability assessments performed by systems engineers. The model may be valuable for system decision-makers and analysts in defense and industry, with possible differences in how it is used by novices and experts. The generic model studies and incorporates previous events in order to understand the behavior of critical infrastructures and the (inter)dependencies between systems and to identify patterns of interest (Kröger & Zio, 2011). Predictive approaches, such as the use of leading indicators, are employed to simulate the behavior of a single or a group of critical infrastructures in order to find potential high-consequence cases and non-obvious vulnerabilities (Kröger & Zio, 2011).

A certain degree of knowledge is required in order to align threats to vulnerabilities as part of a security analysis (Hibshi et al., 2015). However, the iterative nature and flexibility of the generic model can assist novices in developing greater Situation Awareness (SA) and moving from perception of vulnerabilities to comprehension and projection (Hibshi et al., 2015). The ability to select from different techniques and tools and the generic framework's clear notation, presentation, and guidance contribute to this transition and allow novices to engage in the process (Ledermüller & Clarke, 2011, Hibshi et al., 2015). This is especially relevant, as knowledge gaps in cyber risks and defense technologies frequently exist (Koh, 2015).

4.3.1. Vulnerability Assessment Goals

As discussed in Chapter 3, the goal of a vulnerability assessment on a complex infrastructure system is to answer a set of questions including the following:

- What are the end states of interest for the given system(s) and how should system boundaries be defined?
- What are threats and hazards of relevance to which the system(s) under consideration may be exposed?
- What is the resilience and sensitivity (susceptibility) of the system(s) experiencing the threats and hazards?
- What are resulting cascades and identifiable (inter)dependencies? What are the respective impacts and what are the high consequence scenarios?
- What uncertainties are involved?
- What are the obvious and non-obvious ("hidden") vulnerabilities? How can these vulnerabilities be better managed and/or reduced? (Kröger & Zio, 2011).

Further refinement of these questions is necessary when commencing a vulnerability assessment of a particular system or set of interconnected systems and must be conducted with input from all stakeholders, including the decision-maker (Kröger & Zio, 2011). The questions of what define vulnerability and risk and how these can be measured with respect to a given system and at what level of accuracy need to be answered in an accurate manner (Kröger & Zio, 2011). This drives and informs the model structure outlined below.

4.3.2. Generic Model Background

A generic model is defined by the Inter-Agency Network on Education Simulation Models (2008) as "a standard tool with some built-in elements, which can facilitate its adaptation to a particular…system." The generic model does not correspond to a specific system, and careful restructuring and adaptation is required if the generic model is desired to be used as a tool for designing policy or a detailed strategy (Inter-Agency Network on Education Simulation Models, 2008). A generic model can also refer to a prototypical model (Keselman & Dickinson, 2005). Furthermore, Penzenstadler & Femmer (2013) state that a "generic sustainability model can be

instantiated for development processes (companies) and for software systems (products)" as shown in Figure 4-5:

Figure 4-5. Example Instances of the Generic Sustainability Model (Penzenstadler & Femmer, 2013).

A generic model can exhibit qualities of both a generic process model and a reference model. A generic process model is a formal framework for process analysis that extends concepts from the ontology developed by Bunge (Process: Knowledge and Decisions Group, Department of Information Systems, University of Haifa, n.d.). Generic process models, as shown in Figure 4-6, are frequently used within software engineering and establish the foundation for a complete software process through pinpointing a small number of framework activities applicable to all software development efforts, regardless of size or complexity (Pressman, 2005). The process

framework also encompasses a set of umbrella activities, which assist with project communication, planning, modeling, construction, and deployment (Pressman, 2005).

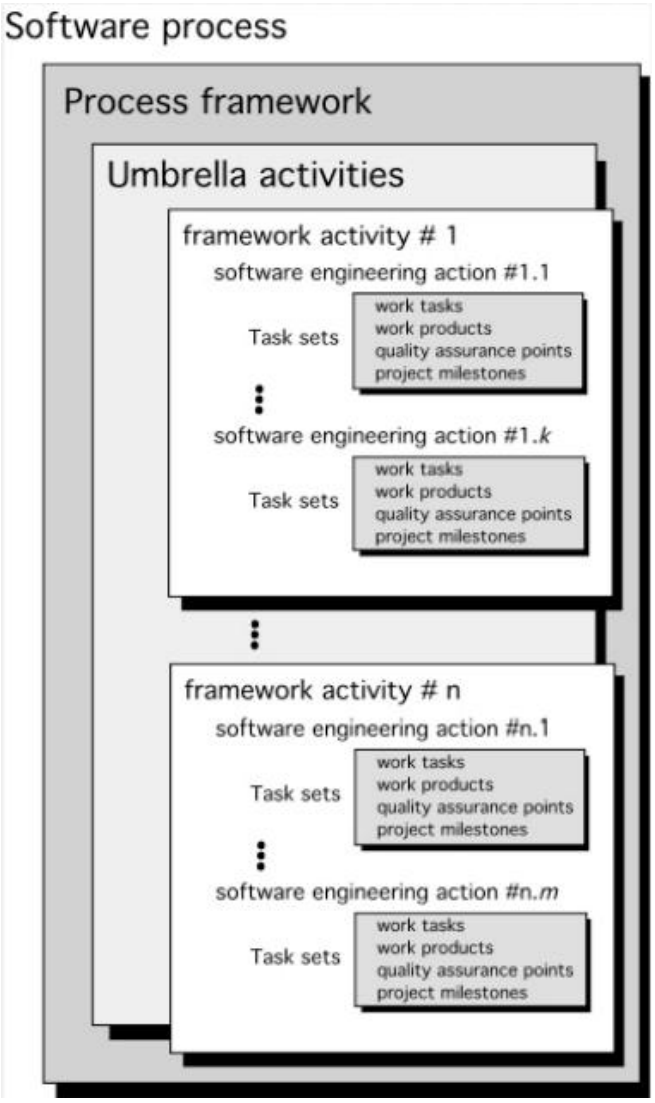


Figure 4-6. Software Engineering Generic Process Model (Pressman, 2009).

In systems, enterprise, and software engineering, a reference model is defined as an "abstract framework or domain-specific ontology consisting of an interlinked set of clearly defined concepts produced by an expert or body of experts in order to encourage clear communication" (Babers, 2015; MITRE, 2015). A reference model can "represent the component parts of any consistent idea, from business functions to system components, as long as it represents a complete set," and "this frame of reference can then be used to communicate ideas clearly among

members of the same community" (Babers, 2015; MITRE, 2015). Reference models are assembled to represent patterns in reality by pinpointing component parts and their interactions within the framework (G. Peck & Beam, 2005). Reference models can be used as a starting point for the development of specific conceptual models (Becker et al., 2009; Pajk et al., 2012). Reed (2012a) separates supply chain, software, and design-specific vulnerabilities; as such, this thesis proposes that the generic model can be instantiated in these three areas, respectively.

4.3.3. Generic Model Structure

The structure of the generic model was influenced by previous frameworks developed by Eusgeld et al. (2009) and Kröger & Zio (2011) to assess the vulnerability of critical infrastructures. These approaches follow a problem-driven, iterative approach and consist of main steps, decision points, and feedback loops (Eusgeld et al., 2009). The framework proposed by Eusgeld et al. (2009) and modified slightly by Kröger & Zio (2011) contains five steps as shown in Figure 4-7 and boils down to two successive stages: a screening analysis for pinpointing parts of the critical infrastructure pertaining the most to its vulnerability, and in-depth modeling of the operational dynamics of the identified parts for the purpose of gaining insights on the causes and mechanisms accountable for the vulnerability.

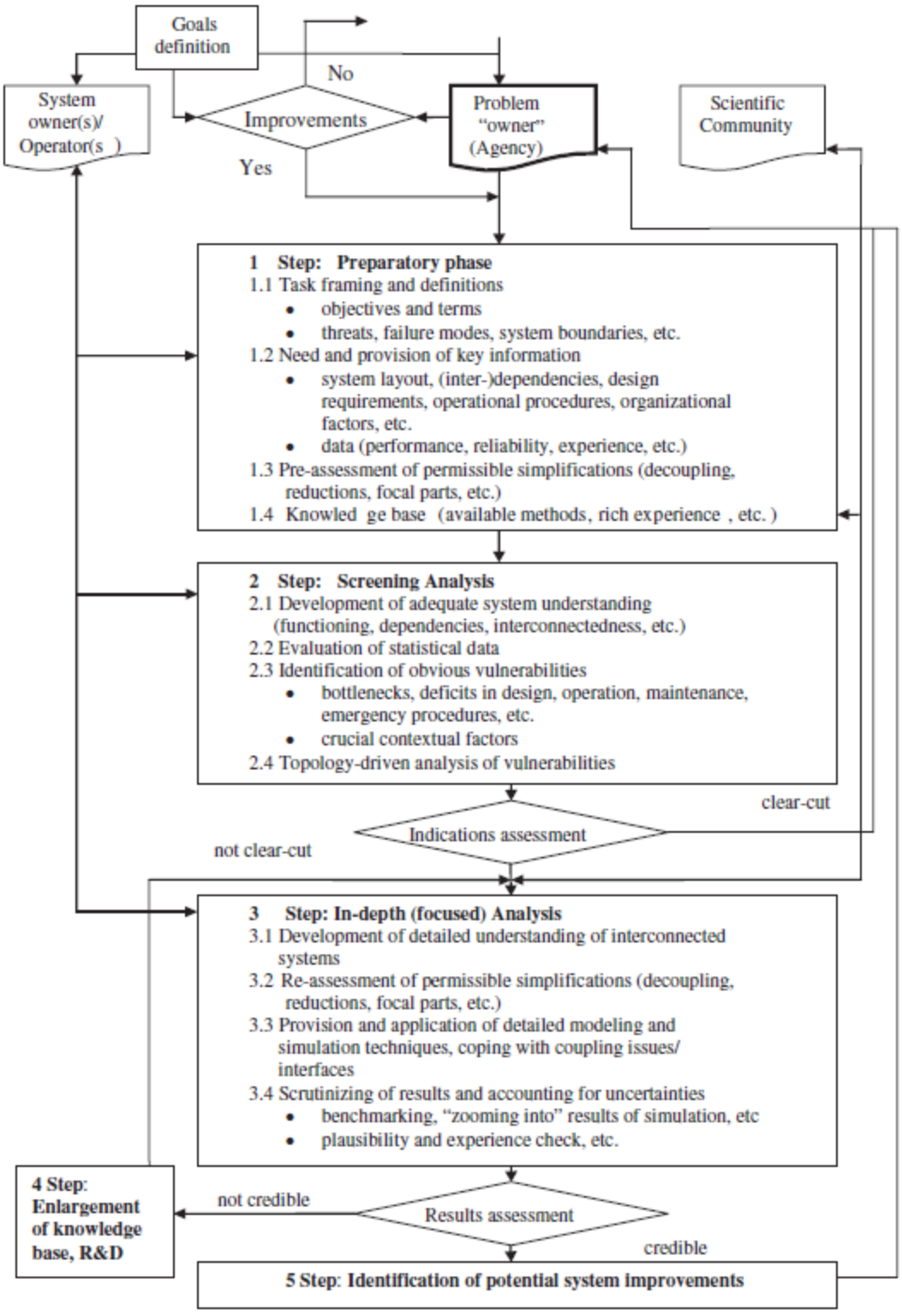


Figure 4-7. Framework for the Vulnerability Analysis of Interconnected Infrastructures (Eusgeld et al., 2009).

The Preparatory Phase focuses on clearly defining terms and developing a mutual understanding of the objectives between all stakeholders; this can facilitate distinguishing between vulnerabilities that are obvious as opposed to those that are hidden (Eusgeld et al., 2009). While obvious vulnerabilities are often recognized as a result of a screening analysis, hidden vulnerabilities require more detailed system exploration and modeling in order to come to the surface (Eusgeld et al., 2009). The Screening Analysis emphasizes the development of adequate system understanding and places importance on expert opinions, brainstorming, and other elicitation methods rather than on the application of detailed models (Eusgeld et al., 2009). The step concludes with a topology-driven analysis of vulnerabilities, which targets the identification of system connection patterns and shortest paths typically using techniques from network theory (Eusgeld et al., 2009).

The In-Depth (Focused) Analysis Phase follows given indications of major vulnerabilities yet to be identified (Eusgeld et al., 2009). More sophisticated tools are employed, utilizing additional information both about the system and its operating environment, in order to achieve a more accurate evaluation of vulnerability (Eusgeld et al., 2009). This step places greater weight on interdependencies within or among systems and reassesses earlier assumptions and simplifications; an object-oriented modeling approach could be applied (Bar-Yam, 1997; Eusgeld et al., 2009). Finally, benchmarking and like methods can be used to account for any remaining uncertainties (Eusgeld et al., 2009).

The Enlargement of Knowledge Base, R&D Phase can be triggered given the need to further develop modeling and simulation techniques in order to fully address system concerns (Eusgeld et al., 2009). Furthermore, the Identification of Potential System Improvements Phase can be useful for concluding the analysis and proposing mitigations to protect system vulnerabilities, whether through structural safety provisions or organization changes (Eusgeld et al., 2009). The decision-maker ultimately chooses whether or not to implement the proposed improvements, sometimes after iterating the vulnerability assessment to account for the effectiveness of proposed measures and to avoid negative feedback (Eusgeld et al., 2009).

4.3.4. Identification and Initial Analysis (CEM)

In the first step of the generic model, Identification and Initial Analysis (CEM), sufficient system understanding is developed to allow for the identification of spontaneous events, perturbations, and terminal events (Rovito & Rhodes, 2016). The user is guided to develop an initial set of vulnerabilities and to create a Cause-Effect Mapping diagram as detailed in Chapter 2 (Rovito & Rhodes, 2016). In addition to imparting improved understanding of system vulnerabilities, non-linear relationships, and causality, the Cause-Effect Mapping diagram can enable decision-makers to pinpoint where strategies can be implemented to prevent the occurrence of terminal events through the avoidance and mitigation of and recovery from root-cause perturbations (Rovito & Rhodes, 2016).

4.3.5. Application of SSE Principles (TSN Analysis)

In the second step of the generic model, Application of SSE Principles (TSN Analysis), scientific and engineering principles are applied to identify security vulnerabilities and to minimize associated risks (Rovito & Rhodes, 2016; Baldwin et al., 2012). This is done through taking into consideration the supply chain-specific System Security Engineering (SSE) risk categories of quality escape, reliability failure, fraudulent product, malicious insertion, anti-tamper, and information losses as shown in Figure 4-8 (Baldwin, 2014).

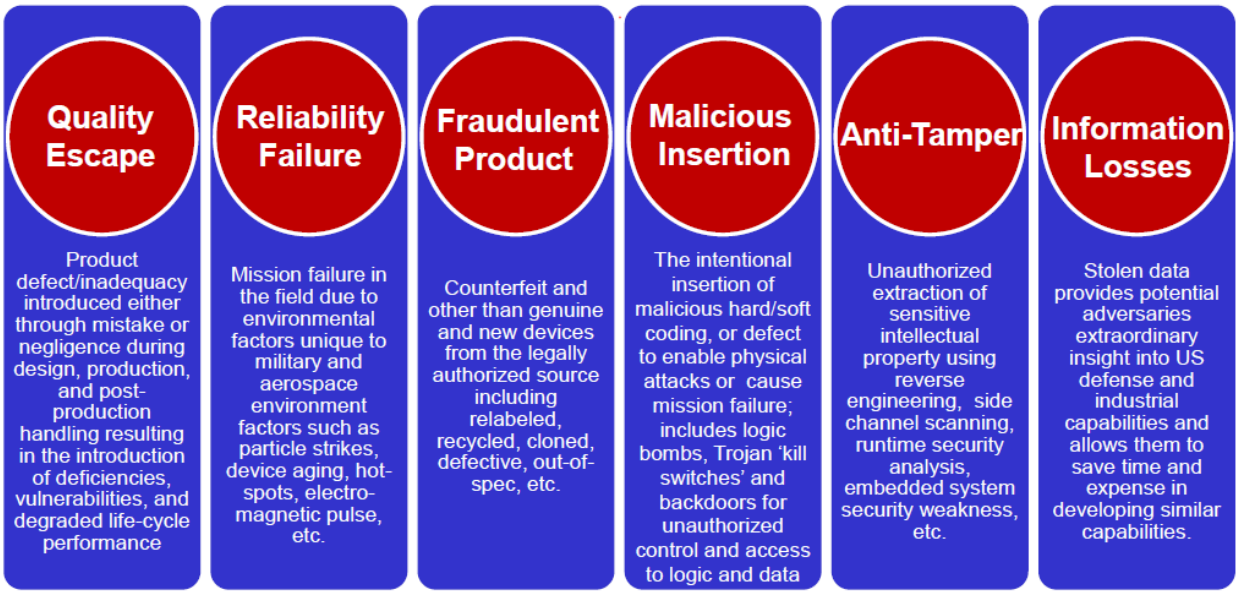


Figure 4-8. SSE Supply Chain Risks (Baldwin, 2014).

Trusted Systems and Networks (TSN) analysis is the risk-based SSE methodology for protecting mission-critical functions and components used by the United States Department of Defense (DoD). Vulnerability assessment is an activity that is part of a TSN analysis, conducted to point out vulnerabilities in system design and COTS products (Deputy Assistant Secretary of Defense for Systems Engineering & Department of Defense Chief Information Officer, 2014). Decisions about particular vulnerabilities to address and applicable mitigation strategies are governed by an understanding of threats, mission impact, and program priorities. Outputs from the vulnerability assessment, along with those from a separate threat assessment, allow for the determination of the "likelihood of loss," or risk likelihood (Deputy Assistant Secretary of Defense for Systems Engineering & Department of Defense Chief Information Officer, 2014).

As illustrated by Figure 4-9, the likelihood of loss is combined with the consequence of loss determined from a Criticality Analysis to yield the initial risk to the system under evaluation. The system's risk is reassessed upon identification, but prior to implementation, of selected security countermeasures. TSN analysis is iterative and should be repeated upon the discovery of new vulnerabilities or changes in the threat environment, as the latter can reveal new attack paths and areas of interest (Deputy Assistant Secretary of Defense for Systems Engineering & Department of Defense Chief Information Officer, 2014).

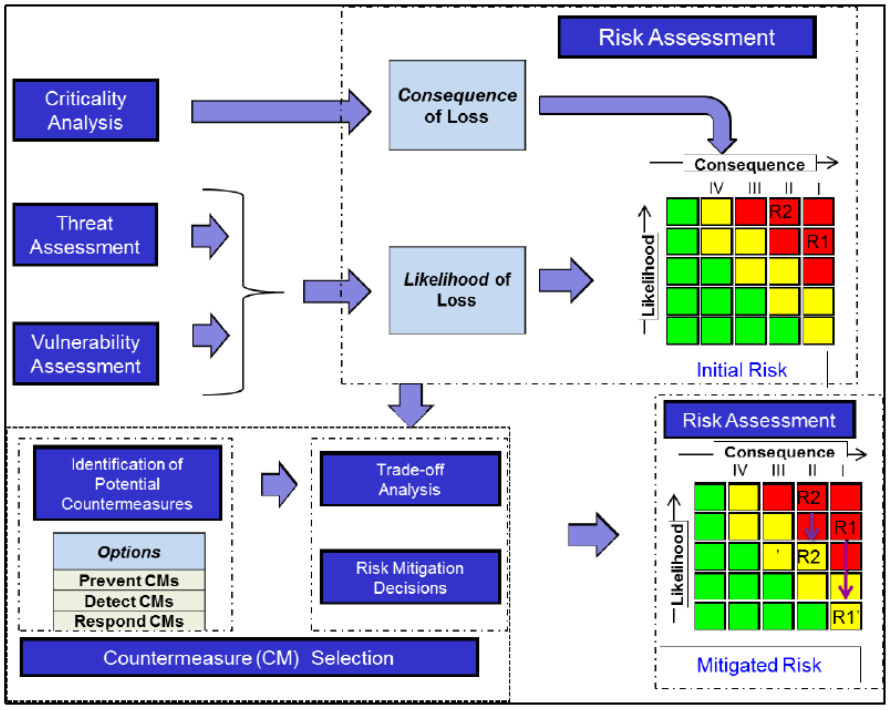


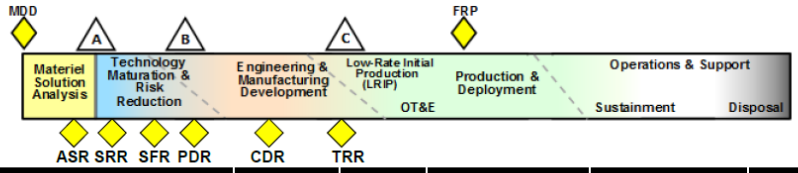
Figure 4-9. Trusted Systems and Networks (TSN) Analysis Methodology (Deputy Assistant Secretary of Defense for Systems Engineering & Department of Defense Chief Information Officer, 2014).

TSN analysis can utilize an attack-based approach or one of the six designated techniques and tools that have proven effective in identifying vulnerabilities in complex systems: a Milestone A Vulnerability Assessment Questionnaire, vulnerability databases, static analyzer tools and other detection techniques, Component Diversity Analysis, Fault Tree Analysis (FTA), and Red Team Penetration Testing (Deputy Assistant Secretary of Defense for Systems Engineering & Department of Defense Chief Information Officer, 2014). These are explored in detail in Chapter 3; each of these techniques possesses particular strengths and is capable of making a particular contribution to analyzing system vulnerability. From an ISO 15288 systems engineering process perspective, TSN analysis includes requirements analysis, design, and implementation activities essential for system security (LeSaint et al., 2015).

Vulnerability assessments conducted as a part of TSN analysis are completed to the system design level of detail throughout the system life cycle (LeSaint et al., 2015). This allows for the identification and implementation of cost-effective interventions (LeSaint et al., 2015). A specific vulnerability assessment technique can be selected based on a system's current phase in the

development life cycle; Table 4-4 shows the six techniques and tools and where they most effectively apply per IEEE 1220 (Reed, 2014b; LeSaint et al., 2015).

Table 4-4. Vulnerability Assessment Techniques Across the System Acquisition Life Cycle (Reed, 2014b).



	Techniques	Legacy	MSA	TMRR		EMD		P&D	O&S
				SRR	PDR	CDR	SVR		
1	VA Questionnaire		x	x					
2	Attack Pattern Path Analysis	x		x	x	x	x	x	x
3	Static Analysis & Other Detection Techniques	x			x	x	x	x	x
4	Component Diversity Analyzer	x	x	x	x	x			
5	Fault Tree Analysis/ Attack Tree Analysis	x			x	x	x	x	
6	Penetration Test	x				x	x	x	x

While a novice may select a technique with which she or he is most comfortable, an expert may select a technique capable of revealing the most additional insight into the system under investigation (Rovito & Rhodes, 2016). Regardless, each of these techniques and tools complements CEM and serves as a sanity-check on the set of already-defined system vulnerabilities and countermeasures (Rovito & Rhodes, 2016). Several of these techniques may be used in concert to provide a full life cycle approach to vulnerability assessment and to mitigate a range of possible vulnerability risks (Deputy Assistant Secretary of Defense for Systems Engineering & Department of Defense Chief Information Officer, 2014).

Table 4-5. TSN Vulnerability Assessment Techniques (LeSaint et al., 2015).

Analysis Technique	High-Level Description
Vulnerability Assessment Questionnaire	A set of questions a program answers to identify vulnerabilities that can be mitigated by Statement of Work and system requirements additions to the Request For Proposal
Vulnerability Assessment Database	Assessment using three databases of publically-available information that define attack patterns, vulnerabilities, and weaknesses (CAPEC, CVE, CWE)
Static Analyzer Tools and Other Detection Techniques	Static analysis, dynamic analysis, and other testing, tools, and techniques to identify vulnerabilities in software during development, in legacy software, and in open source
Component Diversity Analysis	Assessment of the potential impact of malicious insertion in a component that is used multiple times in one or more critical functions or sub-functions
Fault Tree Analysis (FTA)/ Attack Tree Analysis (ATA)	Analysis commonly used in system safety and reliability, adjusted for use in system security to account for malicious actors introducing intentional system faults, as opposed to random sources of failure
Red Team and Penetration Testing	Subjecting a system, supply chain, and/or the development environment to a series of attacks, simulating the tactics of an actual threat through the use of misuse cases

An investigation of vulnerabilities and access paths stemming from a TSN analysis may reveal the need to revisit previous determinations of system vulnerability (Deputy Assistant Secretary of Defense for Systems Engineering & Department of Defense Chief Information Officer, 2014). While it is unlikely that a program can prevent the exploitation of all system vulnerabilities, a balanced approach to countermeasures including prevention, detection (monitoring), and response can play a key role in keeping a system secure (Deputy Assistant Secretary of Defense for Systems Engineering & Department of Defense Chief Information Officer, 2014).

4.3.5.1. Vulnerability Assessment Questionnaire Development

One particular area of focus given the three instantiations of the generic model proposed in this thesis – supply chain, software, and design-specific – is that of the Vulnerability Assessment Questionnaire. Three different Vulnerability Assessment Questionnaires, one for each instantiation of the generic model, were derived out of the research literature and expert interviews (Reed, 2014b). While these questionnaires can be used at or before Milestone A in the system development process, the Vulnerability Assessment Questionnaires in Table 4-6, Table 4-7, and Table 4-8 below have been modified to be applicable later in the system life cycle.

The Vulnerability Assessment Questionnaire: Supply Chain Example shown in Table 4-6 focuses on questions pertinent to securing a defense microelectronics supply chain.

Table 4-6. Vulnerability Assessment Questionnaire: Supply Chain Example (Reed, 2014b; Reed, 2012a).

Yes/No	Question
	Does the Contractor have a process to establish secure suppliers?
	Does the Contractor require suppliers and sub-tier suppliers to have similar processes to establish secure suppliers?
	Has the prime contractor vetted suppliers of critical function components (HW/SW/Firmware) based upon the security of their processes?
	Does the Contractor obtain DoD-specific Application-Specific Integrated Circuits (ASICs) from a Defense Microelectronics Activity (DMEA)-approved supplier?
	Does the Contractor employ protections that manage risk in the supply chain for critical components or subcomponent products and services (e.g., integrated circuits, Field Programmable Gate Arrays (FPGAs), printed circuit boards) when they are identifiable (to the supplier) as having a DoD end-use?
	Does the Contractor require suppliers and sub-tier suppliers to have similar processes and protections in place to manage risk?
	Does the Contractor use secure shipping methods to ship critical components from one supplier to another and to their final destination?
	Does the receiving supplier or sub-tier supplier have processes to verify critical

	function components received from suppliers to ensure that components are free from malicious insertion (e.g., seals, inspection, secure shipping, testing, etc.)?
	Does the supplier or sub-tier supplier have controls in place to ensure technical manuals are printed by a trusted supplier who limits access to the technical material?
	Does the Contractor to have controls to limit access to critical components and associated information?
	Does the Contractor identify everyone that has access to critical components?
	Are Blind Buys used to contract for critical components?
	Are Life-of-Type Buys used to contract for critical components?
	Are specific security test requirements established for critical components?
	Does the developer require secure design and fabrication or manufacturing standards for critical components?
	Are the Contractor, suppliers, sub-tier suppliers, and developers required to report suspected counterfeits to the GIDEP database?

The Vulnerability Assessment Questionnaire: Software Example shown in Table 4-7 focuses on questions pertinent to a software development project or software-intensive defense system.

Table 4-7. Vulnerability Assessment Questionnaire: Software Example (Reed, 2014b; Reed, 2012a).

Yes/No	Question
	Does the developer have a design and code inspection process that requires specific secure design and coding standards (such as CWE and Software Engineering Institute (SEI) *Top 10* secure coding practices) as part of the inspection criteria?
	Have common software vulnerabilities been mitigated through the utilization of CWE, CVE, and CAPEC?
	Are static analysis tools used to identify violations of the secure design and coding standards?
	Are design and code inspections conducted to identify violations of secure design and coding standards?
	Does the software contain fault detection/fault isolation (FDFI) and tracking or logging of faults?
	Do the software interfaces contain input checking and validation?
	Is a separation kernel used to control communications between Level I critical functions and other critical functions?
	Is access to the development environment controlled with limited authorities, and does it enable tracing all code changes to specific individuals?
	Are specific code test-coverage metrics employed to ensure adequate testing?
	Are regression tests run routinely following changes to code?

Finally, a Vulnerability Assessment Questionnaire was created for a design-specific example as shown in Table 4-8. This questionnaire is the most flexible and can be tailored to address concerns specific to the nature of a given system.

Table 4-8. Vulnerability Assessment Questionnaire: Design-Specific Example (Reed, 2014b; Reed, 2012b).

Yes/No	Question
	Will the development tools undergo acceptance testing before installation in the development facility?
	Is red team penetration testing planned for each component in the supply chain as well as the development facility?
	Do critical components have zero memory if the system is not retrievable or ends up in the hands of an adverse actor?
	Do critical components possess anti-tamper measures to protect technology intellectual property?
	Do FPGAs utilize encryption for loading bit streams onto the component?
	Are custom-designed ASICs sourced from a trusted supplier?
	Have maintenance ports on the classification/sensor processor been disabled to prevent backdoor access?
	Does the Configuration Management system require two authenticated users to process a change?
	Is a code review performed on all open source software used by the component?

As a part of TSN Analysis, Vulnerability Assessment Questionnaires can be a useful, broadly applicable tool for guiding a user to ask critical questions regarding a system's procedures and for discerning areas of concern with respect to internal and external factors impacting a system.

4.3.6. Additional Insight (Leading Indicators)

The third step, Additional Insight (Leading Indicators) allows for the selection of leading indicators capable of providing qualitative insight as to how vulnerabilities can propagate within a system (Rovito & Rhodes, 2016). Leading indicators are measures that drive the performance of lag measures and can predict outcomes (International Customer Management Institute, n.d.). An effective leading indicator is essentially a means of filtering out valuable information from noise (Leveson, 2015). Leading indicators tend to be predictive in nature, allowing an organization to adjust or adapt based on results, and can be thought of as gauges of performance.

Leading indicators capable of revealing valuable information about system vulnerabilities and potential mitigations require careful thought to be defined in such a manner to provide benefit.

Leveson (2015) notes that the majority of large-scale accidents present precursors and cues, or "weak signals," that an adverse event is likely prior to the accident taking place. One explanation for this is the attribution of most major accidents to a relaxation of risk safeguards and controls over time due to complacency, tradeoffs, and conflicting goals (Rasmussen, 1997; Leveson, 2015). Additional indicators could take into account variation in supply or demand, fluctuating fuel prices, disruptions in related industries, geopolitical changes, and technological developments (Stecke & Kumar, 2009). The usefulness of leading indicators specifically tailored to the system under investigation as compared to more general, industry-wide indicators is also noted by Leveson (2015).

Leading indicators are especially applicable to the study of vulnerability within complex systems. A simple indicator can portray the direction in which vulnerabilities will propagate, and can in turn provide insight as to how system vulnerabilities may develop in the future (Zimmerman, 2004; Hofmann et al., 2012). For example, the inclusion of indicators assessing operational capability such as switching cost, operating profit margins, asset turnover ratio, quality capability, and technological capability may improve the assessment of supplier risk when taken into consideration with market and financial variables (Jung et al., 2011). Furthermore, Kröger & Zio (2011) find the quantification of system vulnerability indicators to be one of the two main outputs of a critical infrastructure vulnerability assessment given the information they provide with respect to the static and dynamic characteristics of a system.

A leading indicator approach is in contrast to existing supplier risk assessment practices, which estimate a weighted expected value of risk factors or categories (Jung et al., 2011). As demonstrated by the Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognizability (CARVER) decision support tool in Chapter 3, the use of metrics does not always yield a meaningful numeric representation of vulnerability (Antón et al., 2004). Sometimes simple numeric scoring schemes used to characterize system vulnerability can be flawed and obfuscate important distinctions among categories (Antón et al., 2004). The use of leading indicators and an empirical approach can be a preferred approach for holistically grasping system vulnerability.

Vulnerability indicators for supply chain systems can assess both susceptibility and coping capacity as shown in Figure 4-10 and Table 4-9. These indicators tend to cluster around variability, inventory, lead time, performance (time and magnitude), and cost (Nowakowski et al., 2015). Indicators can also be used to counter the bullwhip effect, or the phenomenon in which forecasts yield supply chain inefficiencies which ultimately bring about vulnerabilities (Sakli et al., 2014).

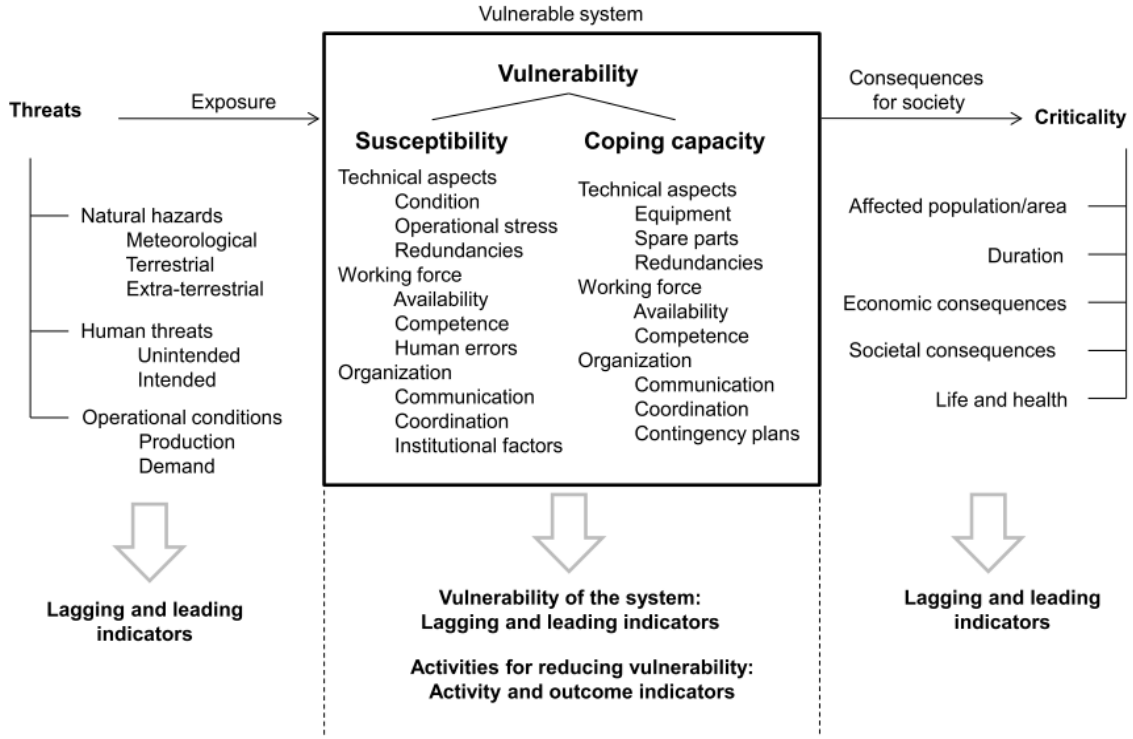


Figure 4-10. A Theoretical Framework for Supply Chain System Vulnerability Indicators (Hofmann et al., 2012).

Examples of indicators to monitor threats, susceptibility, coping capacity, and criticality in a power system are presented below in Table 4-9. The indicators for susceptibility encourage the individual evaluating the system to think at a higher level of abstraction and to consider factors impacting the indicators for threats.

Table 4-9. Examples of Threats and Corresponding Indicators for Monitoring Vulnerability (Hofmann et al., 2012).

	Indicator for threats	Indicator for susceptibility
Natural hazard: Storm	Wind prognosis Historical wind data	Localisation (exposure to wind) of critical power lines Technical condition of critical power lines Competence on condition evaluation of power lines Competence on system analyses and vulnerability evaluations
Human threat: Digging	Construction work near critical locations in the power system Historical data on cable joint failures	Number and localisation of junctions where infrastructures meet Technical condition of power cables including joints Competence on condition evaluation of power cables including joints Competence on system analyses and cross sector vulnerability evaluations
Operational conditions: Overload	Overload Stepwise increase in loading degree	Loading degree for critical systems and components Technical condition of critical systems and components Competence on condition evaluation of critical components Competence on system analyses and vulnerability evaluations

	Indicator for coping capacity	Indicator for criticality
All threats	System control centre competence (including cooperation and coordination between infrastructures) Competence on repair (of power lines, cables, other critical components) Available transport for repair (of power lines, cables, other critical components)	Localisation of critical loads including dependent infrastructures Interruption costs including dependent infrastructures Categories of end users affected Temperature

Once through Step 3, the model prompts the user to assess the credibility of results, namely the refined set of vulnerabilities and mitigations, before continuing on to Step 4. The iterative nature of the CEM and TSN analysis frameworks along with the generic model itself easily allows for corrections or the incorporation of new information (Rovito & Rhodes, 2016).

4.3.7. Identification of Potential Interventions

The fourth step, Identification of Potential Interventions, assumes a credible set of system vulnerabilities and allows the user to develop an evolving list of vulnerabilities and potential interventions (Rovito & Rhodes, 2016). These can serve as inputs into a formal risk assessment

and can inform countermeasure cost-risk-benefit tradeoff analysis (Deputy Assistant Secretary of Defense for Systems Engineering & Department of Defense Chief Information Officer, 2014). The vulnerabilities and interventions can also be incorporated into future policies or strategies.

4.3.7.1. Interventions and Countermeasures

Interventions can originate from multiple disciplines and be drawn from technology, verification, and policy (MITRE, 2013). A set of effective interventions addresses threats to the overarching mission and allows a system to avoid, mitigate, or recover from perturbations (MITRE, 2013). This comes about from the identification of reinforcing loops (non-linear relationships) within a system in order to prevent cascading failures; the prevention and mitigation of perturbations with multiple effects is critical. Intervention techniques vary greatly with respect to level of maturity; relevance to organizations, missions, and systems; and affordability, efficiency, and effectiveness (MITRE, 2013). Therefore, interventions can be prioritized based on different criteria selected by the decision-maker including benefit to system, effectiveness, ease of implementation, and cost. Other factors, such as constraints imposed by organizational culture, legal and contractual limitations, and commitments to technologies or standards, also must be taken into account when crafting strategies for intervention (MITRE, 2013).

A countermeasure is an action, measure, or device intended to reduce any component of an identified risk – threat, vulnerability, or consequence (U.S. Department of Homeland Security, 2010). This term is frequently used to describe interventions implemented by the Departments of Defense and Homeland Security. Two aspects of countermeasures selection are associated with vulnerability assessment results from a TSN analysis; these are how much should be invested in countermeasures (both the quantity of countermeasures and the total monetary commitment) and what types of countermeasures (acquisition process, system design) are needed (Reed, 2012a).

Countermeasures can prevent, detect, and respond to an adverse event or perturbation impacting a system (Reed, 2012a). Some countermeasures can reduce the exploitation of development, design, and supply chain vulnerabilities; others can monitor, alert, and capture data about an attack; and a final set of countermeasures can analyze an attack and subsequently alter a system or processes to mitigate an attack (Reed, 2012a). Countermeasures have also been grouped into

those focusing on assurance-focused design, those focusing on software assurance, and those focusing on supply chain risk management (Baldwin et al., 2012).

4.3.7.2. CEM Intervention Placement Experiment

An experiment was conducted to assess and understand where and why someone with limited familiarity of a supply chain would choose to intervene in the pilot application presented in Chapter 5. Twenty master's degree candidates in MIT's Technology and Policy Program were asked to analyze the Cause-Effect Mapping Diagram shown in Figure 5-1 and to distribute 100 "units" of intervention. This was determined to be a more straight-forward approach than attaching a monetary value to the amount of available funds.

The following heuristic questions were used to prompt the evaluator to share additional insights with respect to intervention placement:

- How did you determine the best places to intervene in the Cause-Effect Mapping Diagram? What led you to eliminate some places versus other places?
- Is/are the intervention(s) a sure thing, or do you see it/them as just reducing chances of system impact?
- Any other supply chain, vulnerability, or policy thoughts?

The locations found to be the most popular spots to intervene are shown below in Table 4-10. The total cumulative weighting sums to 2000 as expected (20 participants x 100 "units" of intervention = 2000 "units" of intervention).

Table 4-10. CEM Intervention Placement Experiment Results.

Location	Number of Evaluators Choosing to Intervene (Out of 20)	Cumulative Weighting (Out of 2000 Units Total)
After "Weak Security Controls" and before "Unauthorized Access"	8	383
After "Supplier Cost-Cutting" and "Raw Materials Unavailable" and before "Sub-par Material Substitution"	7	190
After "Economic Factors" and "Little or No Investment in Security Controls" and before "Weak Security Controls"	5	185
After "Economic Factors" and before "Little or No Investment in Security Controls"	6	175
After "Economic Factors" and before "Supplier Cost-Cutting"	5	170

A few main themes emerged among the twenty participants. Several debated the value of upstream (near the spontaneous events) versus downstream (near the terminal events) intervention, noting that mitigating a vulnerability upstream may require more of an upfront investment but could potentially keep the impact of an exploited vulnerability from impacting other areas of the supply chain. Some participants argued that funds were better spent downstream, as intervening later on in the supply chain could allow for more targeted interventions and "more bang for your buck." Another often referenced aspect was that of control and liability, with several participants choosing to focus on interventions to prevent "Compromised Components" since a supplier would ultimately be liable for several events resulting in "Components Not Available" or "Damaged Components." Several participants also noted the importance and availability of cyber-related interventions, which corroborates with the finding of after "Weak Security Controls" and before "Unauthorized Access" as the most popular location in the CEM Diagram for intervention. All participants viewed interventions as solely reducing the chances of system impact, not as a sure thing. Further data and discussion from the CEM Intervention Placement Experiment can be found in Appendix C.

With respect to security controls, which are defined as technical or administrative safeguards or countermeasures to avoid, counteract, or minimize loss or unavailability due to threats acting on their matching vulnerability, these can be implemented as preventative (e.g., a firewall), detective (e.g., an Intrusion Detection System (IDS)), and corrective (e.g., use of a "gold disk" to reload an operating system) controls throughout the life cycle of a system (Northcutt, 2009). Furthermore, compensating controls exist as alternate controls designed to accomplish the intent of the original controls given that these cannot be used due to environmental limitations (Northcutt, 2009). Potential controls for these four categories are enumerated in Table 4-11.

Table 4-11. Potential Security Controls (Northcutt, 2009).

Preventative	Detective	Corrective	Compensatory
Security Awareness Training	System Monitoring	Operating System Upgrade	Backup Generator
Firewall	Intrusion Detection System (IDS)	Restoration of Backup Data	Hot Site
Anti-virus	Anti-Virus	Anti-Virus	Server Isolation
Security Guard	Motion Detector	Vulnerability Mitigation	
Intrusion Prevention System (IPS)	Intrusion Prevention System (IPS)		

While the decision to investigate and strengthen security controls came about from the subjective CEM Intervention Placement Experiment, metrics can play an important role in determining where and to what extent to intervene in a complex system.

4.3.7.3. Intervention-Related Metrics

Lord Kelvin once stated "if you cannot measure it, you cannot improve it" (Ou & Singhal, 2012). Metrics for vulnerability measurement can assist decision-makers with the placement of interventions and provide a necessary link between strategy, execution, and value creation (Melnyk et al., 2004). Several fundamental tasks are fulfilled by metrics, namely measuring performance, educating stakeholders on value delivery, and directing resources to address potential problems (Melnyk et al., 2004). Metrics are seen as a means through which priorities are promulgated within a company and across a supply chain; metrics misalignment can be a source of inefficiency and disruption (Melnyk et al., 2004). Good metrics should be measured in a consistent manner, inexpensive to collect, expressed numerically, possess units of measure, and have specific context (Jaquith, 2007; Ou & Singhal, 2012).

The impact of potential interventions can be assessed by a decision-maker through the use of a metric or metric systems capable of quantifying information about individual or system vulnerabilities and interventions. The utilization of multiple vulnerability metrics allows for a more complete picture of network vulnerability, as individual metric systems may evaluate a specific aspect of a network and may not provide an overarching view of system vulnerability (Rocco et al., 2012). However, Melnyk et al. (2004) note that increasing the number of metrics used to evaluate a system could lead to greater conflict in the implied priorities along with greater equivocality with respect to future actions. Given the apparent trade-off between metrics set richness and complexity, a balance must be achieved regarding the number of metrics needed to adequately describe a system and to prevent the obfuscation and miscommunication of results (Melnyk et al., 2004).

There are varied approaches to the concept of vulnerability in the research literature as discussed in Chapters 3 and 4. With respect to metrics, one approach relates the vulnerability or robustness of a network with the network's connectivity (Criado et al., 2005). Other approaches relate vulnerability with the decrease in efficiency when one or more vertices or edges are under attack (Criado et al., 2005). Furthermore, there are two main approaches in existence to measure the vulnerability of a complex network: static vulnerability and dynamical vulnerability (Criado et al., 2007). Static vulnerability analyzes the topological behavior of a network, or the response of the structural properties of a network when nodes or links are removed (Criado et al., 2007);

Rocco et al., 2012). Dynamical vulnerability, meanwhile, assesses and measures the redistribution of flow in a network upon the occurrence of a failure or attack (Criado et al., 2007; Rocco et al., 2012).

This thesis focuses on three different types of metrics for static vulnerability assessment: basic connection and measurement metrics, spectral measurements, and statistical and probabilistic measurements (Rocco et al., 2012). While these categories of approaches have respective strengths and weaknesses, they all enable decision-makers and policy makers to target minimizing the vulnerability of a complex system to external events, such as a natural disaster or man-made actions, through the identification of vulnerable and weak points via specific metrics systems (Rocco et al., 2012).

4.3.7.3.1. Basic Connection and Measurement Approaches

Basic connection and measurement approaches include the Vulnerability Priority Number, the Common Vulnerability Scoring System, the Importance Approach, Basic Connectivity, Community Detection, and in-degree/out-degree. The Vulnerability Priority Number is based on the Risk Priority Number, a measure used when assessing risk to assist with the identification of critical failure modes that takes subjective estimates of severity, frequency of occurrence (likelihood), and detection (effectiveness) into account (FMEA - FMECA, 2006). The Vulnerability Priority Number seeks to incorporate and quantify the three key aspects of supply chain resilience discussed earlier in this chapter, namely readiness, response, and recovery (Nowakowski et al., 2015). Similar to the Risk Priority Number, the values for readiness, response, and recovery are determined subjectively by Subject Matter Experts (SMEs), who select a value from a parameter level definition table (Nowakowski et al., 2015). These values are then multiplied as shown in Figure 4-11 to yield the overall Vulnerability Priority Number for a complex system (Nowakowski et al., 2015).

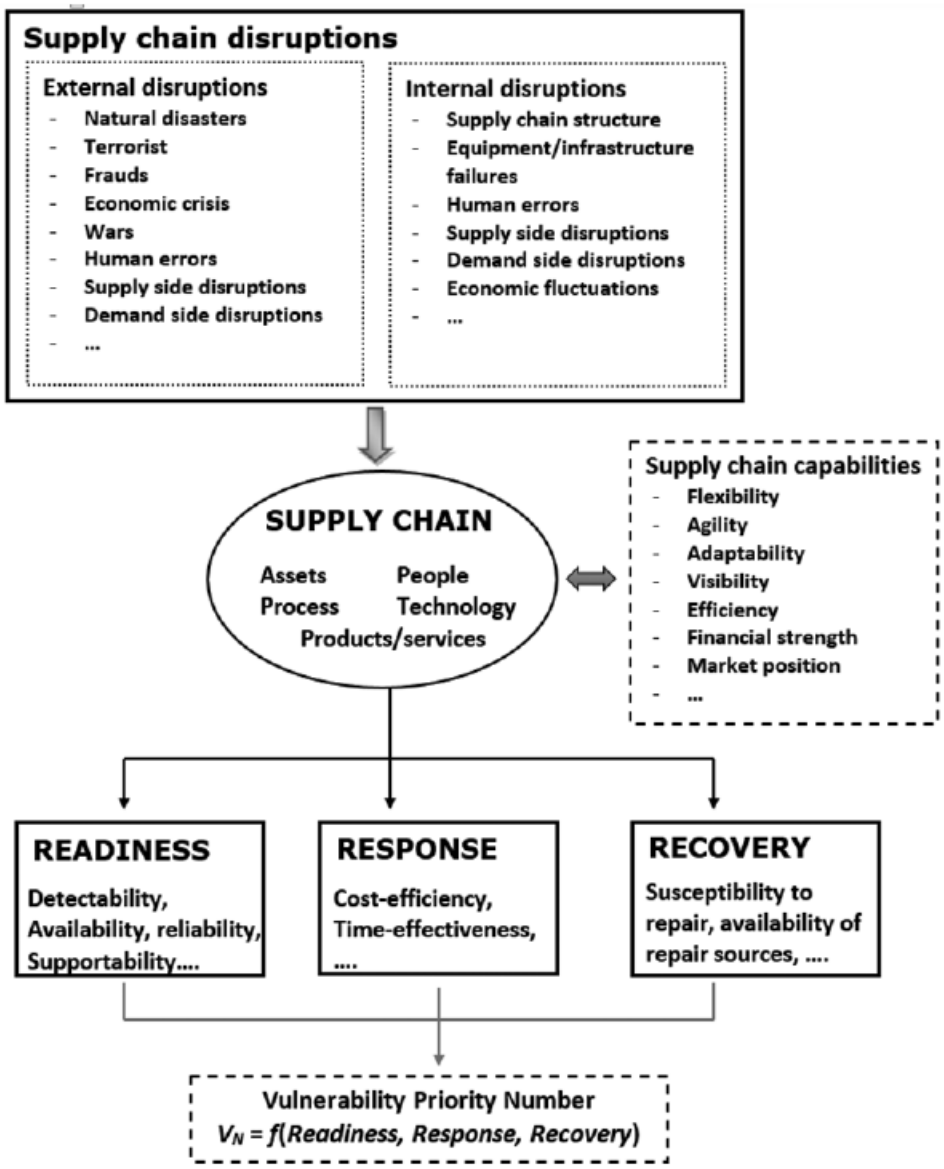


Figure 4-11. Vulnerability Priority Number (Nowakowski et al., 2015).

While the proposed Vulnerability Priority Number is well-intentioned, the subjective nature of expert opinions and lack of detailed system information leave room for a more comprehensive, quantitative vulnerability metric (Nowakowski et al., 2015). The Vulnerability Priority Number has yet to gain widespread exposure, unlike the Common Vulnerability Scoring System (CVSS).

The Common Vulnerability Scoring System (CVSS) is an open industry standard for communicating the characteristics and severity of computer system security vulnerabilities (Forum of Incident Response and Security Teams, 2015). CVSS sets out to assign severity scores

to vulnerabilities, representing the likelihood that a single attack step is successfully executed, enabling responders to prioritize responses and resources according to the present threat (Ou & Singhal, 2012). Scores are calculated using a formula that depends upon several metrics for approximating both the ease and impact of exploit and can range from 0 to 10, with 10 being the most severe (Forum of Incident Response and Security Teams, 2015). Temporal and Environmental scores also exist and can be factored in to address the availability of mitigations and how widespread vulnerable systems are within an organization, respectively (Forum of Incident Response and Security Teams, 2015). CVSS is best utilized for measuring individual vulnerabilities (Frigault & Wang, 2008). However, this framework can be misleading in situations in which individual vulnerability scores are low but the vulnerabilities taken as a whole can combine to compromise a critical component or resource (Frigault & Wang, 2008). Hamid & Al-Jumeily (2015) have proposed the Dynamic Vulnerability Scoring System (DVSS), capable of measuring a dynamic severity cost impact for each host, as a potential improvement.

Developed by Latora & Marchiori (2005), the Importance Approach lists the sets of events (links out) that effectively degrade the performance function of a network (Rocco et al., 2012). This information is useful for determining where new links should be placed within the network. The Importance Approach defines a performance function and a set of possible events D, such as the removal of a single link or node, or a group of links or nodes. The importance of each event d in the set of possible events D is calculated, and the performance of the network G including the event d in D is determined (Rocco et al., 2012). It is then possible to find the event d which maximizes the importance of the network G; this is said to be the most important event (Rocco et al., 2012). Furthermore, the vulnerability of the network, or the drop in the network efficiency caused by the deactivation of a node or nodes, can be calculated using the importance of the optimal event d (Criado et al., 2005); Rocco et al., 2012).

The Importance Approach has been widely used and is capable of incorporating different performance functions: some derived from complex network theory, others derived from a modeling of the physical system under evaluation (Rocco et al., 2012). The evaluation of the importance of components has been assessed as a single objective problem; for example, determining which network component should be reinforced in order to ensure that vulnerability

is minimized (or alternatively, which component should be damaged in order to ensure that vulnerability is maximized) (Rocco et al., 2012).

Basic Connectivity is another approach to vulnerability metrics proposed by Yazdani & Jeffrey (2010). This simple metric considers vertex connectivity, or the smallest number of vertices whose removal disconnects the network, and edge connectivity, or the smallest number of nodes whose removal disconnects the network (Rocco et al., 2012).

Another metric approach proposed by Rocco et al. (2012) is that of Community Detection, a group of vulnerability metrics for communities in a network proposed by Rocco & Ramirez-Marquez (2013). The approach is formulated on the determination of the set of communities, a set of nodes (or clusters) that are densely interconnected with one another but only sparsely connected with the rest of the network (Kumpula et al., 2007; Rocco et al., 2012). The proposed vulnerability metric gives a description or the "degree" relative to the connectivity of a community to both other communities and the network itself; lower values of this metric indicate that a community is less vulnerable (Rocco et al., 2012). Along with the Importance Approach, Community Detection allows for the quantitative assessment of the effects on the network vulnerability due to factors such as the addition of new links (Rocco et al., 2012).

One final basic approach is that of in-degree and out-degree, or very basic graph theory. In-degree is the number of arrows or paths going into a node or vertex, while out-degree is the number of arrows or paths going out of a node or vertex (Teknomo, 2015). A node or vertex without any arrows going in or out is known as an isolated vertex and has zero degree (Teknomo, 2015). In-degree is significant because it demonstrates the prominence or popularity of a node or vertex, since the node or vertex is the target of interest from another node or vertex (Hanneman & Riddle, 2005). Out-degree is significant, meanwhile, because it can assist with identifying nodes or vertices in a network that are particularly influential and impact a number of subsequent nodes or vertices (Hanneman & Riddle, 2005). The correlation between in-degree and out-degree can make a significant difference to the effective properties of the network, influencing the extent to which an exploited vulnerability promulgates (Nykamp, n.d.). This correlation determines the largest eigenvalue of the adjacency matrix, which in turn influences properties of dynamical systems that evolve on the network (Restrepo et al., 2007; Nykamp, n.d.). An example

of this is the synchronization of networked oscillators (Restrepo et al., 2006; Zhao et al., 2011). The in-degree and out-degree approach can be extended to a directed and weighted network and further analysis per Jin et al. (2015).

4.3.7.3.2. Spectral Measurement Approaches

Spectral measurement approaches, in particular Spectral Measurements and the Spectral Scaling Method, quantify vulnerability by relating the topology of a network through the analysis of the spectrum of the adjacency matrix (Rocco et al., 2012). The spectrum of a network is defined through the set of eigenvalues of the adjacency matrix associated to the network (Rocco et al., 2012). Two metrics are commonly used in this approach, the first of which is the Spectral Gap G, the difference between the first and second largest eigenvalue of the adjacency matrix (Rocco et al., 2012). A low Spectral Gap value indicates that the network has bridges, cut vertices, and network bottlenecks (Estrada, 2006). The second metric is the Algebraic Connectivity, the second-smallest eigenvalue of the Laplacian matrix of the network (Rocco et al., 2012). The magnitude of this metric can be considered as a proxy of the strength of connectivity within the graph (Rocco et al., 2012). A larger value can be interpreted as greater robustness within the network against efforts to decouple parts of the group (Yazdani & Jeffrey, 2010).

The Spectral Scaling Method is a recent approach developed by Estrada (2006). Two different types of networks are defined, Good Expansion Networks (GENs) and non-GENs (Rocco et al., 2012). A non-GEN is a graph possessing at minimum two parts that can be isolated from each other by disconnecting a “small” number of nodes or links (Rocco et al., 2012). These nodes or links that bridge the two parts are classified as bottlenecks; a GEN is a network that does not have any bottlenecks (Rocco et al., 2012). The analysis of GEN properties is an NP-hard computational problem and yields an indirect approach for its characterization (Rocco et al., 2012). A necessary condition for a network to be GEN is that its Spectral Gap G must be sufficiently large (Estrada, 2006; Rocco et al., 2012). Furthermore, a network is classified as a GEN or a non-GEN based on its values of the spectral scaling: correlation coefficient, slope, and expansion character (Estrada, 2006; Rocco et al., 2012).

Recent research has focused on examining quantitative measurements (Frigault & Wang, 2008). One research direction of note is that utilizing Attack Graphs (AGs) to model the security state of

a complex network (Frigault & Wang, 2008). AGs show the cumulative effect of attack steps and can illustrate how individual steps can potentially permit an attacker to gain privileges deep within a network (Ou & Singhal, 2012). AGs are capable of presenting logical causality relations among multiple privileges and configuration settings and reasoning about unknown vulnerabilities through the introduction of hypothetical vulnerabilities (Xie et al., 2010).

Tools for generating AGs include Topological Analysis of Network Attack Vulnerability (TVA), NETSPA (a network security planning architecture), and Multihost, Multistage, Vulnerability Analysis (MULVAL) (Singhal & Ou, 2011). Risk is computed using the probability of success of an attack path multiplied by the loss connected with the compromised target (Singhal & Ou, 2011). However, depending on the difficulty associated with an exploit, the difficulty of access, and the skills and resources possessed by an adverse actor, a vulnerability may or may not pose a high risk to a system (Singhal & Ou, 2011).

A probabilistic network security metric based on AGs has been created; this approach utilizes AG models to define the notion of a probabilistic network security metric (Frigault & Wang, 2008). Current research still arbitrarily combines scores, however, and cannot process situations in which the exploitation of a vulnerability affects the likelihood that another vulnerability will subsequently be exploited (Frigault & Wang, 2008). These approaches often assume likelihood scores that are independently distributed (Frigault & Wang, 2008).

4.3.7.3.3. Statistical and Probabilistic Measurement Approaches

Finally, statistical measurement approaches can be employed to provide quantification of a network through studying the most frequent patterns (Rocco et al., 2012). Relevant statistical measures can include node-degree distribution, clustering coefficient, average path-length, node betweenness, link density, and Markov modeling among other approaches (Boccaletti et al., 2006; Singhal & Ou, 2011; Rocco et al., 2012).

Liu & Man (2005) first broached the idea of using Bayesian Networks (BNs) to model network vulnerabilities and to formulate a quantitative measure representing the security of a network. Frigault & Wang (2008) later proposed modeling probability metrics based on AGs as a special BN to measure network security risk (Khaitan & Raheja, 2011). BNs can be employed to model the security states of a network and to encode the probabilistic properties of vulnerabilities

within a network under evaluation (Frigault & Wang, 2008). This approach, popular in recent years, utilizes conditional probabilities to address the general cases of interdependency between vulnerabilities and provides a sound theoretical foundation for developing probabilistic metrics (Khaitan & Raheja, 2011). A BN is inherently a graphical representation of cause-and-effect relationships within a given domain (Xie et al., 2010). Formally known as a Directed Acyclic Graph (DAG), a BN consists of nodes representing variables of interest and directed links representing the causal influence among the variables; the magnitude of an influence is represented by Conditional Probability Tables (CPTs) (Xie et al., 2010).

A BN is a powerful tool for conducting security analysis as long as a BN model can be constructed that reflects reality (Xie et al., 2010). Building a BN from an Attack Graph is not trivial, and difficulty exists in modeling the uncertainty inherent in security analysis (Xie et al., 2010). In addition, cyber security analysis does not easily lend itself to statistical analysis; CPT parameters come about from vague and subjective judgments and do not always reflect an adversary's adaptation (Xie et al., 2010). Xie et al. (2010) propose a BN modeling approach capable of overcoming these difficulties through modularization, namely keeping separate various types of uncertainty; the automatic computation of CPT parameters from realistic data sources; and a model programmed not to be too sensitive to perturbation on the CPT parameters. This highlights the extensive research and deliberate choices necessary to make the BN modeling approach applicable to real-world security analysis (Xie et al., 2010).

Fenz et al. (2011) propose a different Bayesian threat probability determination as part of the Automated Risk and Utility Management (AURUM) framework for information security risk management. The Bayesian threat probability determination employs a security ontology to gain knowledge regarding threats and their a priori probabilities, vulnerabilities, control implementations, adverse actor profiles, and organizational assets (Fenz et al., 2011). For each of the vulnerabilities, the security ontology facilitates mitigation controls and the vulnerability exploitation probability is calculated (Fenz et al., 2011). The Bayesian network approach is able to provide consistent probability values by taking stock of all vulnerabilities and existing control implementations; the approach is able to provide the risk manager with a structured, comprehensible way to determine the threat probability (Fenz et al., 2011).

Current research focuses on combining AGs, BNs, and CVSS (Frigault & Wang, 2008; Ou & Singhal, 2012). This aggregated approach is capable of analyzing all attack paths through a network and providing a probabilistic method of the overall system risk that is easily communicable (Ou & Singhal, 2012). Binding the model to the CVSS standard makes it more broadly applicable (Frigault & Wang, 2008). One potential difficulty in combining Bayesian theory and Attack Graphs lies in the cycles in attack graphs that significantly impact the probability computing of the nodes (Yin et al., 2013). Another difficulty, mentioned earlier, is the fact that an Attack Graph assumes that a vulnerability can always be exploited, while in reality, this is not always the case (Ou & Singhal, 2012). Research is continuing, utilizing Dynamic Bayesian Networks to add robustness to the Temporal domain measurements found within CVSS (Frigault & Wang, 2008).

4.4. Final Generic Model

The generic model consists of four steps as shown in Figure 4-12. As discussed earlier in Chapter 4, this thesis proposes three different instantiations of the generic model (supply chain, software, and design-specific). In the first step, Identification and Initial Analysis (CEM), sufficient system understanding is developed to allow for the identification of spontaneous events, perturbations, and terminal events. This guides the user to develop an initial set of vulnerabilities and to conduct CEM, which ultimately yields improved understanding of system vulnerabilities, non-linear relationships, and causality.

In the second step, Application of SSE Principles (TSN Analysis), supply chain-specific risk categories of quality escape, reliability failure, fraudulent product, malicious insertion, anti-tamper, and information losses are taken into consideration as part of TSN analysis (Baldwin, 2014). The user is able to choose from one or more of the six techniques and tools designated by TSN analysis as effective in identifying vulnerabilities in complex systems (Deputy Assistant Secretary of Defense for Systems Engineering & Department of Defense Chief Information Officer, 2014). While a novice may select a technique with which she or he is most comfortable, an expert may select a technique capable of revealing the most additional insight into the system under investigation. Regardless, each of these techniques and tools complements CEM and serves as a sanity-check on the set of already-defined system vulnerabilities and countermeasures

(Deputy Assistant Secretary of Defense for Systems Engineering & Department of Defense Chief Information Officer, 2014).

The third step, Additional Insight (Leading Indicators) allows for the selection of leading indicators capable of providing qualitative insight as to how vulnerabilities can propagate within a system. The application of the selected leading indicators can reveal additional information about system vulnerabilities and suggest further mitigations.

The model prompts the user to assess the credibility of results, namely the refined set of vulnerabilities and mitigations, and to return to an earlier step if necessary before continuing on to Step 4. The iterative nature of the CEM and TSN analysis frameworks along with the generic model itself easily allows for corrections or the incorporation of new information. The fourth step, Identification of Potential Interventions, assumes a credible set of system vulnerabilities and allows the user to develop an evolving list of vulnerabilities and possible mitigations. These can serve as inputs into a formal risk assessment and can inform countermeasure cost-risk-benefit tradeoff analysis (Deputy Assistant Secretary of Defense for Systems Engineering & Department of Defense Chief Information Officer, 2014). The vulnerabilities and interventions can also be incorporated into future policies or strategies.

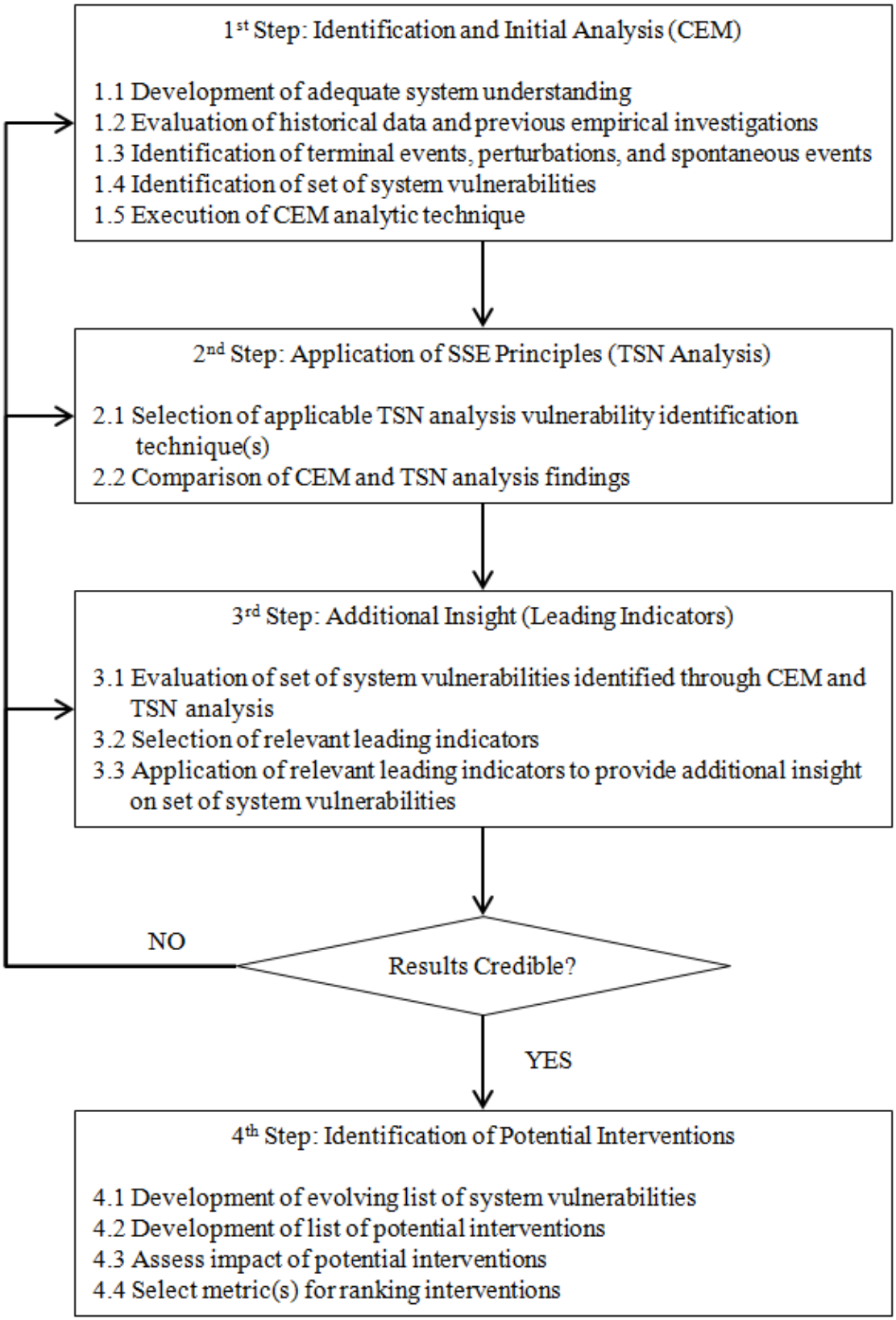


Figure 4-12. Final Generic Model.

4.5. Expert Evaluation of Generic Model

An expert evaluation of the generic model was conducted at a not-for-profit engineering corporation in March 2016. The objective of the evaluation was to assess and validate the usefulness of the proposed generic model based upon the following questions:

- What do you find to be positive about the process for vulnerability assessment?
- What do you find to be negative?
- What are the biggest barriers to implementation of the process in your organization?
- What changes can make the process even more useful for or valuable to your organization?
- What steps or elements within the process would you prioritize given a limited amount of resources?
- What feedback or comments do you have regarding the use of leading indicators?

The generic model was critiqued by twenty employees with the following backgrounds as shown in Table 4-12. These individuals were invited to participate based on recommendations from Subject Matter Experts (SMEs) and senior employees.

Table 4-12. Expert Evaluation Attendees.

Group Affiliation	Number of Employees
Cognitive & Behavioral Understanding	1
Guidance Production	1
High Performance Reliable Computing Systems	1
Inertial System Test Development	3
Modeling & Simulation	1
Product Integrity	2
Quality Design & Engineering or Quality Management	3
Strategic or GN&C Systems	2
System Assembly	1
Systems Analysis or Systems Engineering	3
Systems Science & Architecture	2
TOTAL	**20**

The generic model received largely positive feedback, with individuals stating that the generic model is "a potentially good approach for consistent evaluations," "a consistent way of looking across a variety of issues" impacting a system while learning where and when to probe in greater depth, and a tool capable of "pointing [an organization or individual, including those without supply chain expertise] in the right direction to focus resources." One staff member mentioned the particular need for a vulnerability assessment method that is more objective and quantitative than the "Red-Yellow-Green" risk assessment matrix promulgated in MIL-STD-882E, "Department of Defense Standard Practice System Safety."

Two main highlights of the generic model included its flexibility/tailorability and its ability to take socio-technical factors into account. The generic model, through different instantiations, can apply to systems and supply chains that are raw materials-centric, mechanical parts-centric, or sensor-centric (of particular interest, as detecting sensor-related issues early in the design process is critical to mission success). The ability to tailor "the process so that responsibilities for implementation at different levels of the organization are well understood" is another benefit. The generic model may be useful for dealing with obsolescence within a supply chain as well as supplier viability issues, and there is a desire to learn more about how the generic model can be employed to focus on parts integrity, fault-tolerant systems, and autonomous vehicles.

The ability of the generic model to consider the impact of socio-technical factors was not lost on those evaluating the model. One individual remarked that "this assessment looks at other issues besides the technical attributes of the part/component. I don't think we usually consider these other factors (or, only consider them when there is a problem)." Another individual found Cause-Effect Mapping (CEM) to be an influential approach for decision-making given its status as an analytical technique "applicable in the policy sphere due to the capability to deal with/process socio-technical elements" and capable of enhancing system understanding. The generic model allows for "improving decision-making as it applies to systems" and "thinking of systems in a more un-traditional sense."

CEM and Trusted Systems and Networks (TSN) Analysis were specifically called out as useful techniques within the generic model. One individual noted that CEM can "help greatly during early decision-making in large acquisition systems" and is particularly applicable to acquisition strategy development, as the dimensionality and complexity of acquisition strategies in general is not recognized and performance is not easily quantified. Existing systems prove where CEM, which contributes to the understanding of vulnerabilities and implementation of effective countermeasures early in the system life cycle, can be useful, since various strategies do not always mesh and different, more effective acquisition strategy-related decisions could be made. In addition, one individual noted that "TSN Analysis links familiar tools that programs currently use" including risk and criticality assessments.

With respect to prioritization, two individuals stated that they would prioritize Step 1 early in a development or production program as a tool to better prepare decision-makers. This is useful for tying upstream vulnerabilities to downstream consequences and can ensure that knowledge gained early in the program applies downstream. However, one major concern is that it is "hard to identify historical data" necessary to yield correct inputs and to produce a thorough Cause-Effect Mapping Diagram. Other implementation concerns include raising awareness of the generic model within an organization (potentially via the integration of the generic model into a larger inventory of Model-Based Systems Engineering (MBSE) tools); convincing staff of the generic model's implementation value without incurring excessive costs for the amount of research involved to satisfactorily execute, both in time and money; making the model less dependent upon SMEs given the limited number of experts capable of coordinating assessments and providing input; embarking upon the front-end challenge of getting into concept exploration; developing a vocabulary and tools to facilitate use of the generic model; and dealing with both a lack of coordination among internal departments (with respect to software development and internal systems) and a company culture that may be hesitant to adopt new methods.

Potential changes that could make the generic model even more useful include addressing knowledge transfer issues including the "Silver Tsunami," making the generic model more of a standard tool (e.g., reducing the barrier for entry and adopting plug-and-play capabilities), prioritizing steps for specific instantiations, providing pre-populated standards and attack vectors for consideration, and making the framework more accessible to systems architects and engineers within an organization by lessening dependence on SMEs for model execution or providing access to a core group of SMEs that are well-versed in the process and able to assist with implementation.

Evaluation of the generic model suggests that the integration of CEM into a sequence of tools for vulnerability assessment can be useful to different stakeholders for specific purposes. A systems engineer may be constructing a program-specific model using the generic model and generating metrics to support decisions. A systems architect may be using the generic model to work out strategies for designing interventions into the system. A program manager may use the model as a basis for discussion with customers. A pilot application applying the generic model to a generic electronics supply chain is presented in Chapter 5 and demonstrates the generic model's

usefulness to different stakeholders within an organization and potential to become a valuable knowledge asset.

CHAPTER 5: PILOT APPLICATION

The final generic model was applied to a case study focusing on electronics supply chain issues specific to the defense and aerospace industries. The pilot application gives emphasis to the use of CEM to identify causal chains and candidate intervention points in order to prevent undelivered, damaged, and compromised components. Special attention is paid to risks presented by quality escape, reliability failure, fraudulent and counterfeit products, malicious insertion of firmware, tampering, and information losses (Baldwin, 2014). All four steps of the generic model were implemented as part of the pilot application, yielding additional insights regarding vulnerabilities and socio-technical factors impacting such a system.

5.1. 1st Step: Identification and Initial Analysis (CEM)

Supply chain vulnerability is an active area of academic research and management practice, benefiting from increased interest in risk assessment and security along with commercial and public policy implications in the corporate governance, business continuity management, emergency planning and national security sectors (Peck, 2006). This thesis adopts Peck (2006)'s definition of a supply chain as a flow of materials, goods, and/or information that passes within and between organizations and is linked by tangible and intangible facilitators, including relationships processes, activities, and integrated (often information) systems. Supply chains are becoming increasingly complex; measures including outsourcing, supplier partnering, inventory reduction, globalization of production and sourcing networks, supply base reduction, and single sourcing are becoming the norm for companies seeking to overcome supply chain challenges and create competitive advantage (Wagner & Neshat, 2012). However, these initiatives have the potential to introduce vulnerabilities and new sources of risk (Svensson, 2002).

Supply chain failure occurs when the product or service provided by the supply chain is unable to be delivered per specifications to the customer (Neureuther & Kenyon, 2009). Failure modes of particular interest for supply chain applications include: disruption in supply, disruption in transportation, disruption at facilities, freight breaches, disruption in communications, and disruption in demand (Sheffi et al., 2003). Human resources is often a seventh area of concern (Rice Jr. & Caniato, 2003). Another way to characterize supply chain risk is through a System Security Engineering (SSE) lens, which offers the categories of quality escape, reliability failure,

fraudulent product, malicious insertion, anti-tamper, and information losses (Baldwin, 2014). This is discussed at length in Chapters 3 and 4.

One particular concern with respect to supply chain vulnerability is the threat posed by counterfeit parts, which along with poor quality parts have become increasingly prevalent in global supply chains in the aerospace and defense industries within the past ten years (Aerospace Industries Association of America, Inc., 2011). A Senate Armed Services Committee report found over 1,800 known cases of suspect counterfeit parts in the DoD supply chain as of 2012 (Committee on Armed Services, United States Senate, 2012). Counterfeit parts are commonly classified into two distinct categories: parts designed with malicious intent, and parts designed with intent to defraud (Rouse & Bodner, 2013). The stakes of counterfeiting are high, as components of sub-par quality, reliability, or integrity can compromise myriad interrelated systems and adversely impact the welfare of countless individuals.

The Defense Federal Acquisition Regulation Supplement (DFARS) Final Rule for the Detection and Avoidance of Counterfeit Electronic Parts, which will be discussed in-depth in Chapter 6, defines a counterfeit electronic part as an "unlawful or unauthorized reproduction, substitution, or alteration that has been knowingly mismarked, misidentified, or otherwise misrepresented to be an authentic, unmodified electronic part from the original manufacturer, or a source with the express written authority of the original manufacturer or current design activity, including an authorized aftermarket manufacturer" (Federal Register, 2014). This definition did not come into existence until May 2014 following years of contentious debate among government and industry stakeholders of what exactly characterizes a "counterfeit part." The definition has been limited in scope to solely cover "counterfeit electronic parts" for the DoD's initial policy response and takes care to address the element of intent involved in the deliberate production of counterfeit components. The DFARS Final Rule for the Detection and Avoidance of Counterfeit Electronic Parts ultimately applies to "counterfeit electronic parts," "suspect counterfeit electronic parts," and "obsolete electronic parts" (Covington & Burling LLP, 2014).

5.1.1. Background

While the art and practice of counterfeiting has been around since ancient times, the modus operandi has recently shifted from the "piecemeal production" of low-quality goods in tiny,

clandestine operations to the "coordinated and sophisticated production" of high-quality goods practically indistinguishable from the authentic part or product (Tehranipoor et al., 2015). This has particular implications for aerospace and defense, as electronic parts in the industry are critical to the function of every platform delivered to government and civilian customers. Unlike a knock-off designer bag still having the ability to be useful as a bag, a component that appears to be high-quality and to operate properly may covertly contain malicious firmware and software capable of not only compromising system functionality but also national security in an instant.

Counterfeit parts jeopardize the security and reliability of complex systems and networks, and pose a major threat to both government and industry. This can result in significant economic and security impacts. The cost of addressing counterfeit components in a supply chain is greater than merely replacing the counterfeit part. Possible ramifications for manufacturers and suppliers encompass lost revenue, theft and improper use of electronic data, and infringement upon intellectual property (such as through reverse engineering). In turn, this can lead to slower economic growth and innovation and lessened trade with countries taking a weak stance on the enforcement of intellectual property rights. The government is saddled with lost tax revenue, industry with lost sales, and citizens with low-quality goods (and associated replacement expenditures). While it is impossible to put an exact dollar figure on losses from counterfeiting, the Federal Bureau of Investigation (FBI) estimated in 2002 that U.S. businesses lose $200-$250 billion dollars annually on account of the practice (Government Accountability Office, 2010b).

Counterfeit electronic parts have the potential to "seriously disrupt" the DoD supply chain, delay missions, and adversely impact the integrity of weapon systems (Government Accountability Office, 2010a). The DoD procures parts from numerous global suppliers, and practically every single component – from complex electronics to simple fasteners – is at risk of being counterfeited. Unlike authentic parts which possess known performance histories and adhere to the manufacturers' quality control plans, counterfeit components are of unknown reliability and therefore undermine national security (Aerospace Industries Association of America, Inc., 2011). The DoD to date has uncovered numerous instances of counterfeit parts, ranging from GPS oscillators containing parts of questionable origin to fighter jet engine mounts comprised of substandard titanium to brake shoes manufactured with replacement materials including seaweed

(Government Accountability Office, 2010a). Maintaining the integrity of integral hardware and software is of utmost importance.

Increased incidences of counterfeiting are directly attributable to globalization. The dot-com boom and bust, outsourcing and offshoring, IT system interoperability, and the rise of global shipping companies set into motion fundamental changes that allowed counterfeiters to take advantage of exposed gaps in supply chains. China's entry to the World Trade Organization (WTO) on December 11, 2001 along with the U.S.'s non-ratification of the Basel Convention governing the export of hazardous e-waste to the developing world also serve as contributing factors (countries agreeing to the Basel Convention adhere to strict rules governing the disposal of old hardware components). The U.S. continues to send e-waste to China, where obsolete electronic parts are often washed with dirty river water, refurbished, and rebranded as new, authentic components. The counterfeiting problem itself does not come about from domestic contractors and distributors, but rather from actions undertaken by the counterfeiting parties as in this example. Counterfeiting is profitable, especially in countries with abundant resources, cheap labor, and reduced manufacturing costs.

5.1.2. Application of CEM-VA Process

CEM was applied to a generic electronics supply chain case using the process described in Chapter 2. The goal of applying this analytic technique is to investigate specific locations in the supply chain where an existing vulnerability can lead to mission failure, specifically the inability to deliver secure, reliable electronic components.

As designated in *Step 1: Knowledge Gathering and Investigation*, a thorough literature review was performed on electronics-related supply chain issues, and an interview was conducted with SME Kai Trepte (MIT Center for Transportation and Logistics (CTL)). This led to increased understanding of the electronics supply chain and the scope of the CEM as well as the identification of Components Not Delivered, Damaged Components, and Compromised Components as terminal events.

Step 2: Terminal Events to Spontaneous Events via Backwards Induction enabled the systems analysis to step backwards from the three unique terminal events to a series of perturbations and

ultimately seven spontaneous events (from three distinct, comprehensive categories) impacting the system.

Following the recognition of these events, *Step 3: CEM Development* was executed and resulted in the artifacts shown below in Figure 5-1 and further elaborated upon in Table B-1 provides additional information about each perturbation in the Supply Chain Pilot Application Cause-Effect Mapping Diagram:

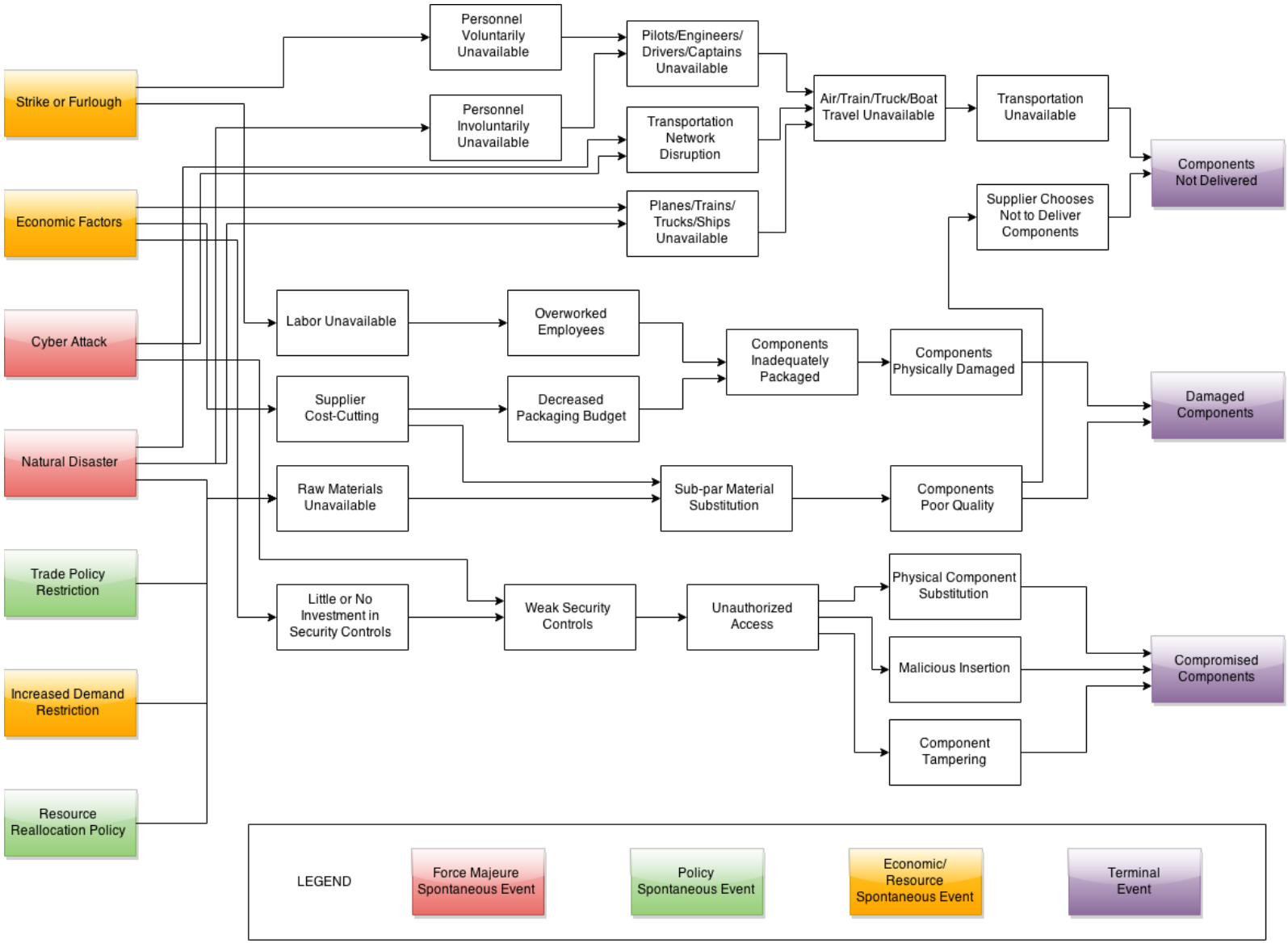


Figure 5-1. Cause-Effect Mapping Diagram of Supply Chain Case.

Of note is the fact that spontaneous events in this case can be classified into three categories: force majeure spontaneous events, policy spontaneous events, economic/resource spontaneous events. These broad categorizations add value in characterizing the nature of a spontaneous event and allowing for further exploration of socio-technical factors and interventions, particularly in the policy arena.

Figure 5-2. Spontaneous Event Categorization.

As the CEM is structured at present, the overarching terminal event – that components are unavailable for use in a system – is broken down into three categories: components not delivered, damaged components, and compromised components. This demonstrates multiple areas of concern with respect to logistics and product availability as well as product integrity. In addition, places in the supply chain are highlighted where System Security Engineering (SSE) risks including where quality escape, malicious insertion, tampering, and information losses can potentially occur (Baldwin, 2014).

Figure 5-3. Terminal Event Categorization.

Step 4: Continued CEM Analysis, provides insight into possible intervention points where strategies can be implemented to prevent terminal events from taking place. These strategies allow the system to avoid, mitigate, or recover from perturbations. The identification of reinforcing loops (non-linear relationships) is of particular interest, so that these can be broken in an effort to prevent cascading failures. Prevention and mitigation of perturbations with multiple effects is paramount in this process.

Six different points for intervention were explored. One way to overcome Air/Train/Truck/Boat Travel Unavailable could be to have 3-D printing capabilities for selected components. This would allow an organization to print a limited number of parts, potentially of lesser quality, to

use in an emergency situation. New policies could be put into place to prevent Overworked Employees, and strategic material reserves could be kept to mitigate Raw Materials Unavailable. Components Poor Quality can be addressed through the implementation of lean and quality-based initiatives. Finally, Weak Security Controls and Unauthorized Access can be assuaged through the implementation of better security measures, whether physical or virtual (some of which can be put into place at little cost to a supplier).

The six possible intervention points are identified in the Supply Chain CEM shown in Figure 5-4; a sampling of possible intervention strategies is characterized in Table B-2:

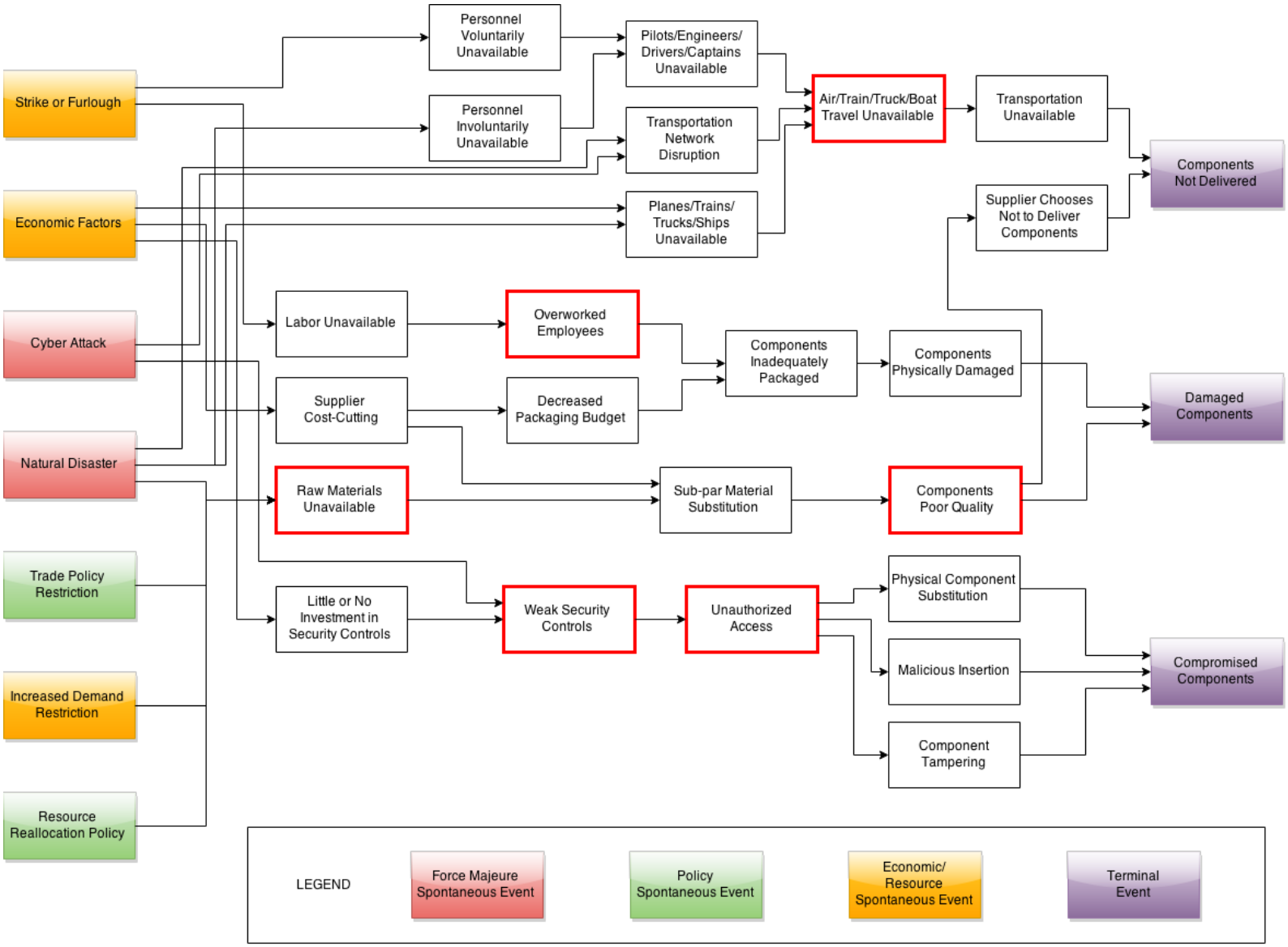


Figure 5-4. Cause-Effect Mapping Diagram of Supply Chain Case with Intervention Points.

The successful implementation of Cause-Effect Mapping has provided foundational system understanding as well as initial insights into where an electronics supply chain may be susceptible to exploitation. The system evaluation continues with the application of System Security Engineering (SSE) principles through Trusted Systems and Networks (TSN) Analysis.

5.2. 2nd Step: Application of SSE Principles (TSN Analysis)

As shown in Table 4-4, the six different vulnerability assessment techniques recommended by TSN apply at different points across the system acquisition life cycle and additionally vary in usefulness with respect to the type of system being evaluated (Reed, 2014b). For the purposes of this pilot application, a Vulnerability Questionnaire and Fault Tree Analysis (FTA)/Attack Tree Analysis (ATA) were conducted on the supply chain under evaluation. While not performed as part of this assessment, it is expected that further insight can be gleaned from performing Red Team Penetration Testing or a Component Diversity Analysis on the supply chain.

5.2.1. Vulnerability Questionnaire

As discussed in Chapter 4, three different Vulnerability Assessment Questionnaires, one for each instantiation of the generic model, were derived out of the research literature and expert interviews (Reed, 2014b). While these questionnaires can be used at or before Milestone A in the system development process, the Vulnerability Assessment Questionnaire: Supply Chain Example shown in Table 5-1 has been modified to be applicable later in the system life cycle. The questionnaire guides a user, whether a systems engineer or other stakeholder, through a battery of questions highlighting key supply chain security concerns.

Table 5-1. Vulnerability Assessment Questionnaire: Supply Chain Example (Reed, 2014b; Reed, 2012a).

Yes/No	Question
Yes	Does the Contractor have a process to establish secure suppliers?
Yes	Does the Contractor require suppliers and sub-tier suppliers to have similar processes to establish secure suppliers?
Yes	Has the prime contractor vetted suppliers of critical function components (HW/SW/Firmware) based upon the security of their processes?

Yes	Does the Contractor obtain DoD-specific Application-Specific Integrated Circuits (ASICs) from a Defense Microelectronics Activity (DMEA)-approved supplier?
Yes	Does the Contractor employ protections that manage risk in the supply chain for critical components or subcomponent products and services (e.g., integrated circuits, Field Programmable Gate Arrays (FPGAs), printed circuit boards) when they are identifiable (to the supplier) as having a DoD end-use?
Yes	Does the Contractor require suppliers and sub-tier suppliers to have similar processes and protections in place to manage risk?
Yes	Does the Contractor use secure shipping methods to ship critical components from one supplier to another and to their final destination?
Yes	Does the receiving supplier or sub-tier supplier have processes to verify critical function components received from suppliers to ensure that components are free from malicious insertion (e.g., seals, inspection, secure shipping, testing, etc.)?
No	Does the supplier or sub-tier supplier have controls in place to ensure technical manuals are printed by a trusted supplier who limits access to the technical material?
Yes	Does the Contractor to have controls to limit access to critical components and associated information?
No	Does the Contractor identify everyone that has access to critical components?
No	Are Blind Buys used to contract for critical components?
Yes	Are Life-of-Type Buys used to contract for critical components?
Yes	Are specific security test requirements established for critical components?
Yes	Does the developer require secure design and fabrication or manufacturing standards for critical components?
Yes	Are the Contractor, suppliers, sub-tier suppliers, and developers required to report suspected counterfeits to the GIDEP database?

The Vulnerability Assessment Questionnaire: Supply Chain Example should spur thought regarding both acquisition and development processes throughout the system life cycle. This can result in the identification of vulnerable areas and implementation of measures to prevent exploitation.

5.2.2. Fault Tree Analysis

A Fault Tree Analysis was performed as part of the pilot application as shown in Figure 5-5, Figure 5-6, and Figure 5-7. One key finding was of another root cause for “Components Poor Quality,” namely “Ineffective Quality Control Processes” resulting from a lack of formal or implemented standards as illustrated in Figure 5-5.

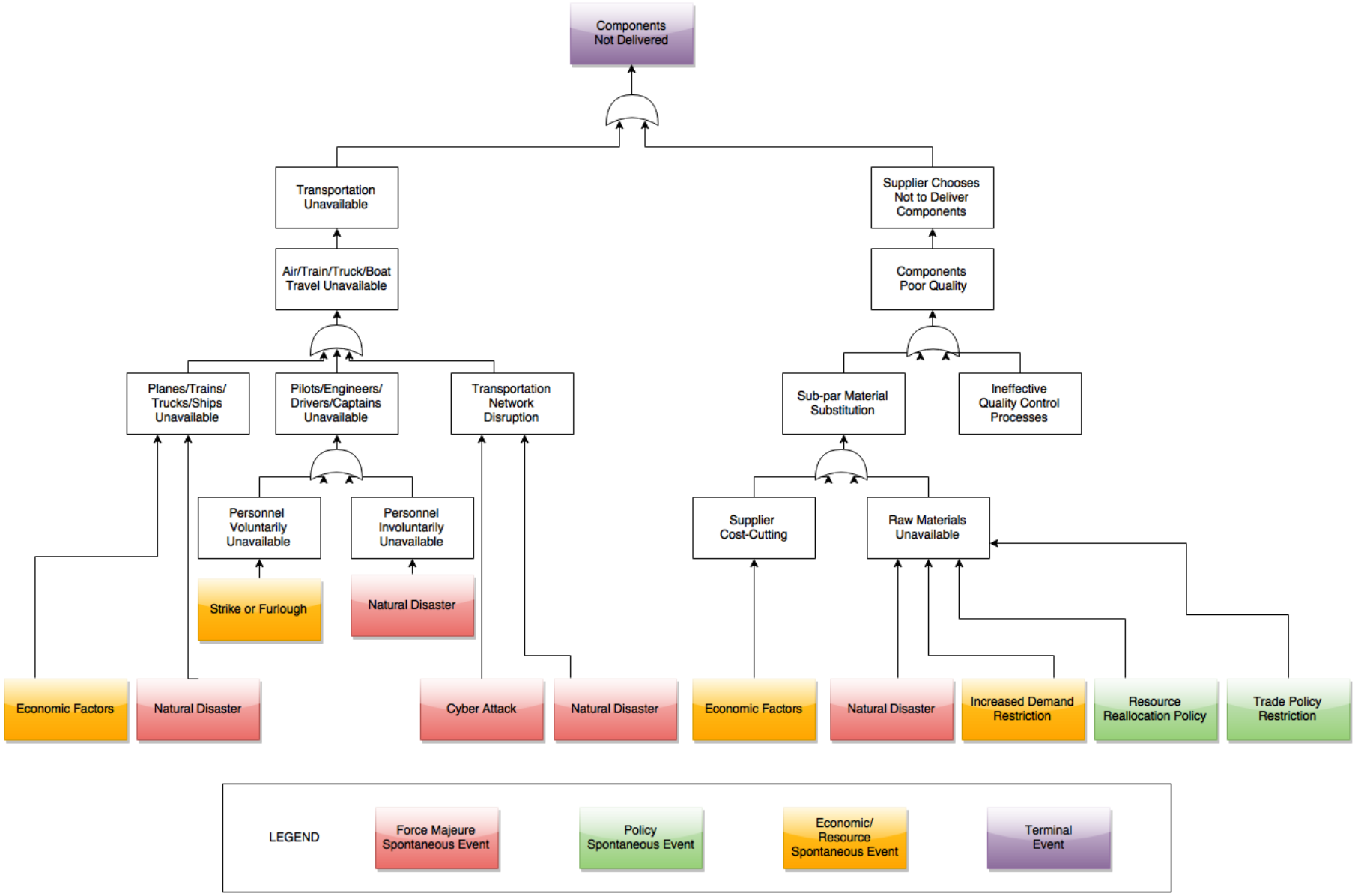


Figure 5-5. Fault Tree Analysis – Components Not Delivered.

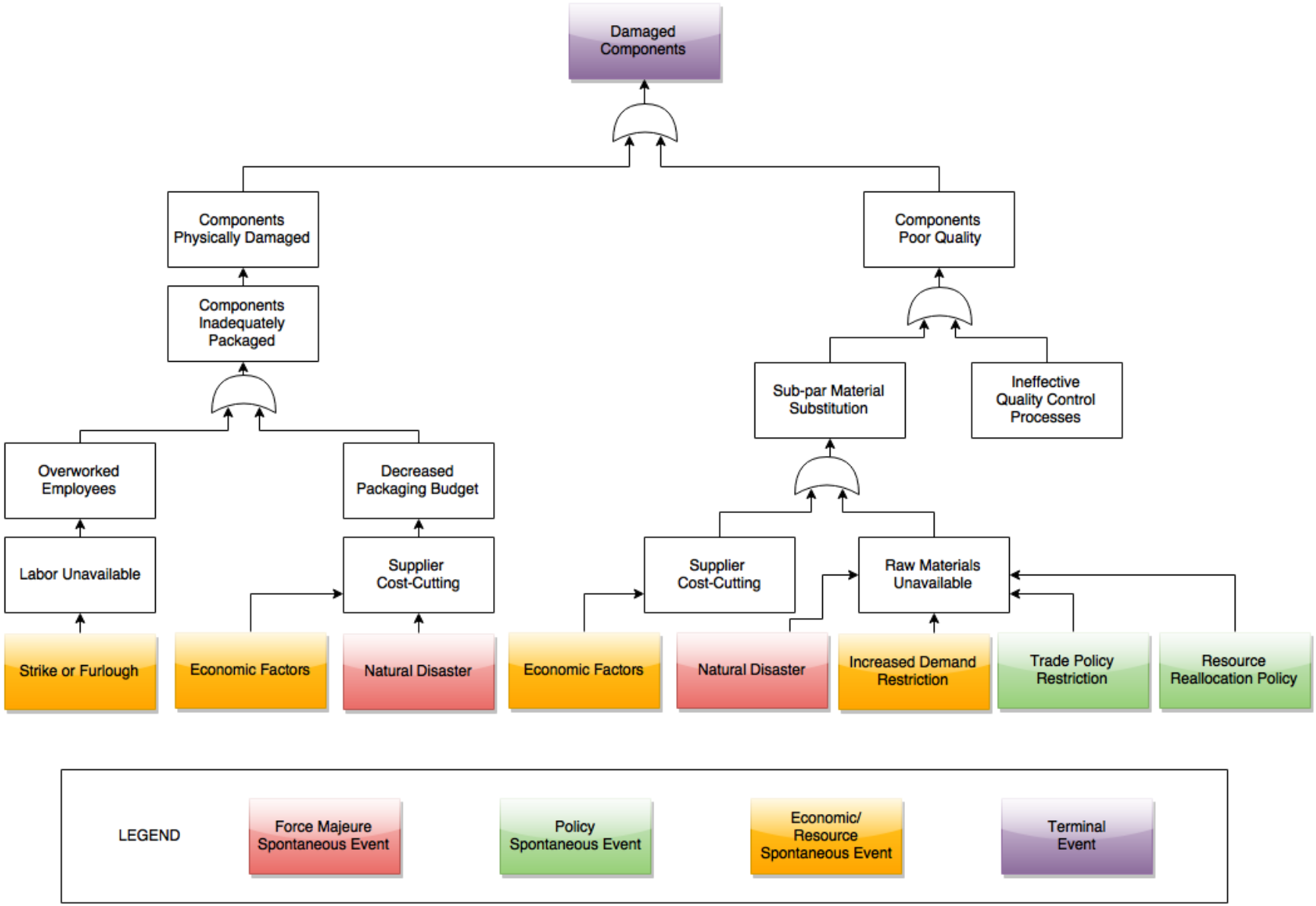


Figure 5-6. Fault Tree Analysis – Damaged Components.

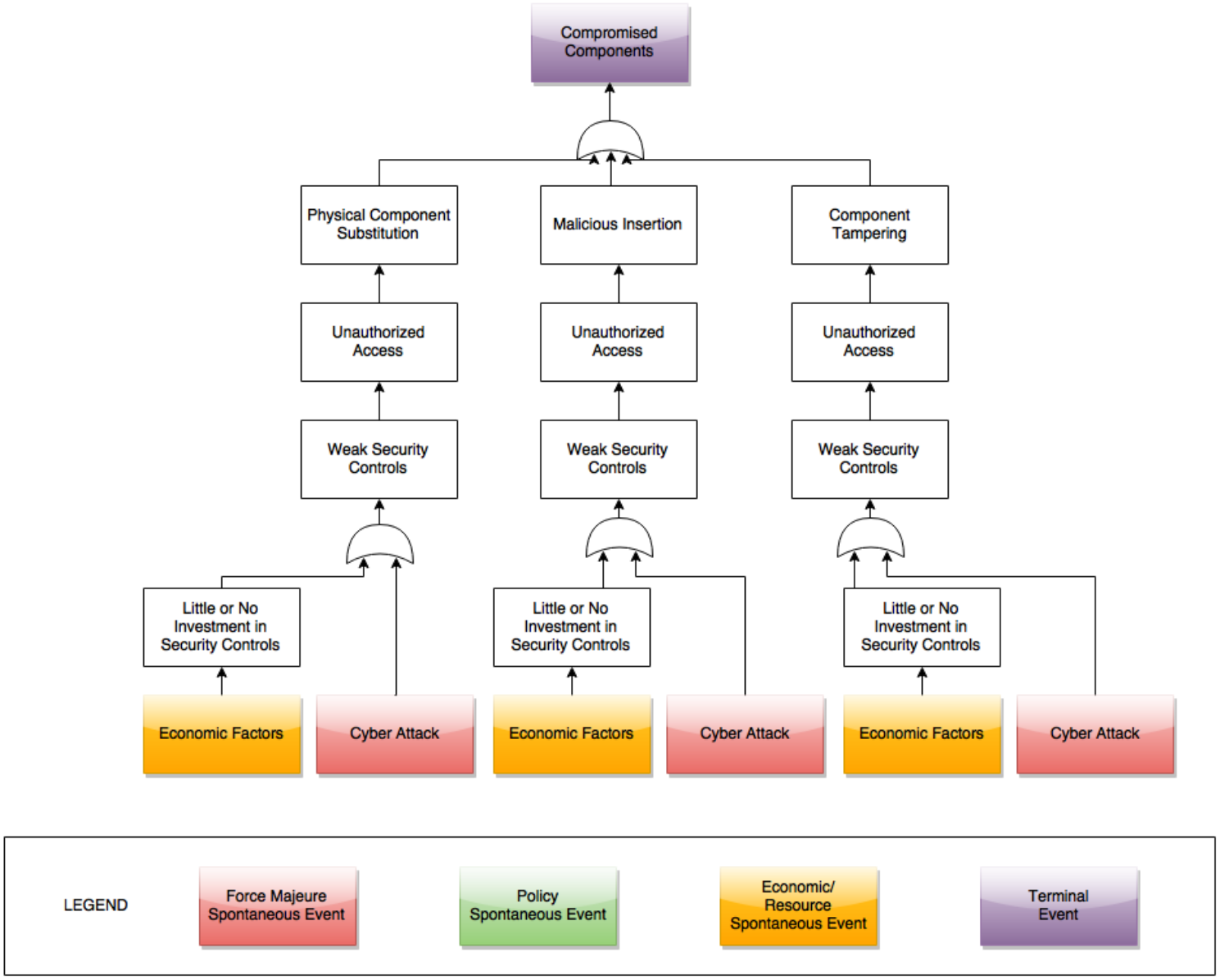


Figure 5-7. Fault Tree Analysis – Components Compromised.

5.3. 3rd Step: Additional Insight (Leading Indicators)

A preliminary set of leading indicators was derived out of the research literature and expert interviews to characterize potential sources of vulnerability within an electronics supply chain as shown in Table 5-2. Indicators for susceptibility depend to a significant extent on the threat being encountered; different threats have different corresponding indicators for monitoring vulnerability (Hofmann et al., 2012).

Table 5-2. Derived Leading Indicators of Vulnerability (Rovito & Rhodes, 2016).

Spontaneous Event	Indicator for Threats	Indicator for Susceptibility
Strike/ Furlough	Labor relations Contract status Historical strike/furlough data	Union issues/demands Upcoming contract expiration/renewal
Economic	Commodity prices Industry trends Historical economic data	Geopolitical factors Decrease in supply Stock Market Index (Inter-American Development Bank, n.d.) Exchange rates (Inter-American Development Bank, n.d.)
Cyber Attack	Formal monitoring software CWE/CVE/etc. Historical cyber attack data	Percentage of failure rates Volume of data passing through network traffic (Koh, 2015) Settings and strength of failure testing cycles, filter rules for data packets (Koh, 2015) Targeting of industrial control systems (Assante, 2014)

Natural Disaster	Weather prognosis Historical weather data	Localization (exposure to elements) of critical resource infrastructure (e.g. power lines) Technical condition of critical resource infrastructure Competence on condition evaluation of critical resource infrastructure Competence on system analyses and vulnerability evaluations
Trade Policy Restriction	Diplomatic relations Historical trade policy data	Geopolitical factors Pending legislation
Increased Demand	Industry trends Historical demand data	Geopolitical factors Shortage of substitute products Changes to manufacturing processes
Resource Reallocation	Industry trends Historical resource data	Adoption of new technologies Pending legislation

These leading indicators can be strategically implemented throughout the electronics supply chain system to serve as predictive measures of vulnerability (specifically, the direction in which it may propagate through the supply chain) and as early warning signs of a potential problem or intrusion by an adverse actor.

5.4. 4th Step: Identification of Potential Interventions

The three prior steps in the generic model yield the set of vulnerabilities shown in Table 5-3. While not collectively exhaustive on account of "unknown unknowns" in the supply chain, this list can be said to encompass the majority of known system vulnerabilities.

Table 5-3. Identified Electronics Supply Chain Vulnerabilities.

Strike or Furlough	Suppler Cost-Cutting	Pilots/Engineers/Drivers/ Captains Unavailable
Economic Factors	Raw Materials Unavailable	Transportation Network Disruption
Cyber Attack	Little or No Investment in Security Controls	Planes/Trains/Trucks/Ships Unavailable
Natural Disaster	Personnel Voluntarily Unavailable	Sub-par Material Substitution
Trade Policy Restriction	Personnel Involuntarily Unavailable	Unauthorized Access
Increased Demand Restriction	Overworked Employees	Components Inadequately Packaged
Resource Reallocation Policy	Decreased Packaging Budget	Air/Train/Truck/Boat Travel Unavailable
Labor Unavailable	Weak Security Controls	Transportation Unavailable
Supplier Chooses Not to Deliver Components	Components Poor Quality	Malicious Insertion
Components Physically Damaged	Physical Component Substitution	Component Tampering
Components Not Delivered	Damaged Components	Compromised Components
	Ineffective Quality Control Processes	

Potential intervention strategies were developed for the locations in the system flagged as worthwhile intervention points during the Cause-Effect Mapping early in the generic model. These are shown in Table 5-4.

Table 5-4. Description of Potential Intervention Strategies in Cause-Effect Mapping of Supply Chain Case.

Perturbation	Description	Strategy
Air/Train/Truck/Boat Travel Unavailable	Travel is unavailable regardless of mode of transportation	Strategic Reserves of components and potential for 3-D printing of temporary replacement parts
Overworked Employees	Employees are overworked due to labor shortages	Policies to prevent employees from becoming overworked, potential automation of tasks
Raw Materials Unavailable	Raw materials are unavailable due to various force majeure, policy, and economic/resource reasons	Strategic reserves and studies on potential replacement materials
Components Poor Quality	Components are of inferior quality and prone to failure	Use of lean initiatives to catch quality problems earlier in the design and manufacturing process, improved quality controls
Weak Security Controls	No or few security controls are in place to prevent physical or virtual security compromises	Implementation of more robust security controls (physical or virtual, in the areas of avoidance, transference, migration, and acceptance), ideally at low cost (Carbone & Tippett, 2004)
Unauthorized Access	No or few security controls are in place to prevent unwanted physical or virtual access to assets	Implementation of more robust access protection (physical or virtual, e.g. pop-up barriers and firewalls), special attention to administrative privileges (e.g. who has access and level of authentication)

As discussed in Chapter 4, interventions can be prioritized based on different criteria selected by the decision-maker including benefit to system, effectiveness, ease of implementation, and cost.

The depth of the supply chain case application does not allow for a full investigation of more quantitative approaches; the two approaches presented are illustrative of approaches that could possibly be applied to a larger-scale complex system.

A matrix-based approach was utilized as shown in Figure 5-8 to further analyze data and to explore intervention points for the supply chain case application in order to see what strategies would have the greatest impact on metrics. The spontaneous and terminal events are categorized by color, respectively, as discussed earlier in Chapter 5. In particular, this matrix highlights the vulnerability of the supply chain to Natural Disaster (a spontaneous event); Unauthorized Access, Raw Materials Unavailable, Air/Train/Truck/Boat Travel Unavailable (perturbations); and Compromised Components (a terminal event) and allows for the identification, implementation, and refinement of system intervention strategies.

	Strike or Furlough	Economic Factors	Cyber Attack	Natural Disaster	Trade Policy Restriction	Increased Demand Restriction	Resource Reallocation Policy	Personnel Voluntarily Unavailable	Personnel Involuntarily Unavailable	Labor Unavailable	Supplier Cost-Cutting	Raw Materials Unavailable	Little or No Investment in Security Controls	Pilots/Eng/Drivers/Captains Unavailable	Transportation Network Disruption	Planes/Trains/Trucks/Ships Unavailable	Overworked Employees	Decreased Packaging Budget	Weak Security Controls	Air/Train/Truck/Boat Travel Unavailable	Components Inadequately Packaged	Sub-par Material Substitution	Unauthorized Access	Transportation Unavailable	Supplier Chooses Not to Deliver Components	Components Physically Damaged	Components Poor Quality	Physical Component Substitution	Malicious Insertion	Component Tampering	Components Not Delivered	Damaged Components	Compromised Components	TOTAL
Strike or Furlough	--	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2
Economic Factors	0	--	0	0	0	0	0	0	0	1	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3
Cyber Attack	0	0	--	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	2
Natural Disaster	0	0	0	--	0	0	0	0	1	0	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4
Trade Policy Restriction	0	0	0	0	--	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Increased Demand Restriction	0	0	0	0	0	--	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Resource Reallocation Policy	0	0	0	0	0	0	--	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Personnel Voluntarily Unavailable	0	0	0	0	0	0	0	--	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Personnel Involuntarily Unavailable	0	0	0	0	0	0	0	0	--	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Labor Unavailable	0	0	0	0	0	0	0	0	0	--	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Supplier Cost-Cutting	0	0	0	0	0	0	0	0	0	0	--	0	0	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	2
Raw Materials Unavailable	0	0	0	0	0	0	0	0	0	0	0	--	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1
Little or No Investment in Security Controls	0	0	0	0	0	0	0	0	0	0	0	0	--	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Pilots/Eng/Drivers/Captains Unavailable	0	0	0	0	0	0	0	0	0	0	0	0	0	--	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1
Transportation Network Disruption	0	0	0	0	0	0	0	0	0	0	0	0	0	0	--	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1
Planes/Trains/Trucks/Ships Unavailable	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	--	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1
Overworked Employees	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	--	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1
Decreased Packaging Budget	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	--	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1
Weak Security Controls	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	--	0	0	0	1	0	0	0	0	0	0	0	0	0	1
Air/Train/Truck/Boat Travel Unavailable	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	--	0	0	0	1	0	0	0	0	0	0	0	0	1
Components Inadequately Packaged	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	--	0	0	0	0	1	0	0	0	0	0	0	1
Sub-par Material Substitution	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	--	0	0	0	0	1	0	0	0	0	0	1
Unauthorized Access	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	--	0	0	0	0	1	1	1	0	0	3
Transportation Unavailable	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	--	0	0	0	0	0	0	1	0	1
Supplier Chooses Not to Deliver Components	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	--	0	0	0	0	0	1	0	1
Components Physically Damaged	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	--	0	0	0	0	0	1	1
Components Poor Quality	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	--	0	0	0	0	1	1
Physical Component Substitution	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	--	0	0	0	0	1
Malicious Insertion	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	--	0	0	0	1
Component Tampering	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	--	0	0	1
Components Not Delivered	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	--	0	0
Damaged Components	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	--	0
Compromised Components	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	--	0
TOTAL	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**1**	**2**	**1**	**4**	**0**	**2**	**2**	**2**	**1**	**1**	**2**	**3**	**2**	**2**	**1**	**1**	**0**	**1**	**1**	**1**	**1**	**1**	**2**	**2**	**3**	

Figure 5-8. Supply Chain Pilot Application Matrix.

A simple in-degree/out-degree assessment of the Cause-Effect Mapping perturbations (nodes) was also conducted to reveal further insights about the electronics supply chain pilot application, particularly with regard to the propagation of risk. Table 5-5 shows the in-degree and out-degree of each perturbation in the Cause-Effect Mapping Diagram. While several permutations have an in-degree of 2, Air/Train/Truck/Boat Travel Unavailable and Compromised Components have the highest in-degree in the network at 3. As for out-degree, Economic Factors, Natural Disaster, and Unauthorized Access share the highest out-degree in the network at 3.

Table 5-5. Supply Chain Pilot Application In-Degree/Out-Degree Data.

	In-Degree	Out-Degree
Strike or Furlough	0	2
Economic Factors	0	3
Cyber Attack	0	2
Natural Disaster	0	3
Trade Policy Restriction	0	1
Increased Demand Restriction	0	1
Resource Reallocation Policy	0	1
Personnel Voluntarily Unavailable	1	1
Personnel Involuntarily Unavailable	1	1
Labor Unavailable	1	1
Supplier Cost-Cutting	1	2
Raw Materials Unavailable	1	1
Little or No Investment in Security Controls	1	1
Pilots/Eng/Drivers/Captains Unavailable	2	1
Transportation Network Disruption	2	1
Planes/Trains/Trucks/Ships Unavailable	2	1
Overworked Employees	1	1
Decreased Packaging Budget	1	1
Weak Security Controls	2	1
Air/Train/Truck/Boat Travel Unavailable	3	1
Components Inadequately Packaged	2	1
Sub-par Material Substitution	2	1
Unauthorized Access	1	3
Transportation Unavailable	1	1
Supplier Chooses Not to Deliver Components	1	1
Components Physically Damaged	1	1
Components Poor Quality	1	2
Physical Component Substitution	1	1
Malicious Insertion	1	1
Component Tampering	1	1
Components Not Delivered	2	0
Damaged Components	2	0
Compromised Components	3	0

The implementation of Bayesian Network and Attack Graph approaches as discussed in Chapter 4 is under consideration for quantifying information gleaned from the generic model and for providing further value with respect to increasing the resiliency of a complex system. Having the ability to employ these techniques as part of the generic model can allow for experimentation and the identification – through metrics – of the best intervention points and strategies to ensure system resiliency.

The pilot application of the generic model underscores the impact that policy can have on a system. This is evident through the policy and economic/resource spontaneous events as well as perturbations elsewhere in the system impacted by acquisition or development policy. Chapter 6 explores vulnerability and security-based policies, including formal legislation and regulation, and asserts the need for Government and industry stakeholders to work together in order to address the critical issue of counterfeit parts in the defense and aerospace supply chain.

CHAPTER 6: POLICY

Public policies developed to mitigate the impacts of adverse events can differ depending on whether they focus on reducing risk or on reducing vulnerability (Sarewitz et al., 2003). Vulnerability management, or the "cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities," is worthy of discussion separate from risk management, since combining the concepts can lead to a loss of focus on vulnerability as a unique contributor to unwanted outcomes (Foreman, 2009; Sarewitz et al., 2003). While vulnerability assessment is not in conflict with the strategies utilized by overarching risk assessments, decision makers tend to gloss over vulnerability and haphazardly apply risk assessment in myriad contexts (Sarewitz et al., 2003). This can lead to negative outcomes and stalled or ineffective policies, as effective planning for and responding to hazards and adverse events demands that the vulnerability associated with socio-technical and decision processes be comprehended in parallel with understandings of processes and probabilities of risk (Sarewitz et al., 2003). This allows judgments to be formulated regarding the suitable balance between risk and vulnerability-based management approaches (Sarewitz et al., 2003).

Focusing on vulnerability management necessitates a clear view of the limits of predictive science for leading the way to an uncertain future and contributing to the creation of robust decision processes (Sarewitz et al., 2003). These processes would enhance resiliency through being flexible and reflexive in order to adapt, being capable of improving with experience, and allowing for continued assessment of alternative approaches for the management of system vulnerabilities (Sarewitz et al., 2003). Six specific assertions are proposed that can assist in exploring the value of vulnerability-based policies:

1. Risk-based approaches to covering the costs of extreme events do not depend on the reduction of vulnerability for their success.
2. Risk-based approaches to preparing for extreme events are focused on acquiring accurate probabilistic information about the events themselves.
3. Understanding and reducing vulnerability does not demand accurate predictions of the incidence of extreme events.
4. Extreme events are created by context.
5. It is politically difficult to justify vulnerability reduction on economic grounds.

6. Vulnerability reduction is a human rights issue; risk reduction is not (Sarewitz et al., 2003).

Vulnerability-based policies are capable of addressing threats, vulnerabilities, and consequences and adding value in disciplines ranging from food security to critical infrastructure security (Van de Voort et al., 2007). While the acquirer and supplier share responsibility for system security in DoD programs, sharing or transferring the requirement for vulnerability assessment from an acquirer to a supplier may improve the effectiveness of an evaluation (LeSaint et al., 2015). This is since a supplier may possess expert knowledge regarding the susceptibility of a supplied capability to various attacks; adopting such an approach can further contribute to the development of resilient systems (LeSaint et al., 2015).

6.1. Federal Security Policy Development

While the U.S. Government does not have overarching legislation or regulation in place to oversee supply chain risk and vulnerability assessment, the National Infrastructure Protection Plan (NIPP) has followed shifts in security policy development in advocating for a comprehensive approach to risk assessment across sectors affecting the U.S. economy (Van de Voort et al., 2007). The NIPP asserts the usefulness of best practices outlined in National Research Council foundational reports, including *Risk Assessment in the Federal Government* (1983) and *Science and Judgment in Risk Assessment* (1994) which require risk assessments to be:

1. Analytic, addressing threat, vulnerability, and consequence, preferably in a quantitative and repeatable way.
2. Deliberative, as a way to incorporate values and risk perception, and make a tradeoff between financial and personal harm.
3. Practical, meaning the assumptions should be tenable and not be overly reliant on a single perspective (Willis, 2006; Van de Voort et al., 2007).

The Department of Homeland Security (DHS) is an interesting case study on this front, as both the NIPP and the Homeland Security Act of 2002 charge DHS to perform and integrate critical infrastructure vulnerability assessments in order to pinpoint priorities. DHS, however, has had difficulty executing to the intent of the policies due to diversity in the areas requiring

vulnerability assessment and the lack of established guidance on areas to be included in a vulnerability assessment (Government Accountability Office, 2014). Furthermore, several measures implemented by DHS in the aftermath of September 11, 2001, including the Customs-Trade Partnership Against Terrorism (C-TPAT), Container Security Initiative, and the 24-hour manifest, have the potential to delay materials or components at the border and in turn impact supply chains (Stecke & Kumar, 2009). Further study is needed to determine the impact of such policies on defense and industry supply chains (Stecke & Kumar, 2009).

Progress has been made within the past fifteen years with respect to maturing the analysis driving security policy (Van de Voort et al., 2007). The approach has transitioned from one of consequence assessment to one of vulnerability reduction, and even more recently to one of comprehensive risk-based decision-making as shown in Figure 6-1 (Van de Voort et al., 2007). However, policy makers have yet to give event response and recovery measures enough attention and have struggled with including the cost effectiveness of potential interventions (Van de Voort et al., 2007). This is on account of the inherent complexity of vulnerability and risk assessment along with a lack of associated data (Van de Voort et al., 2007).

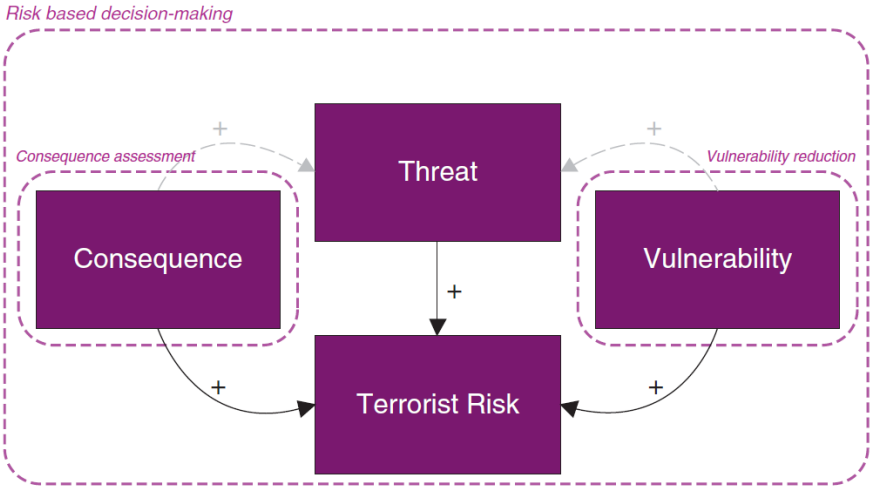


Figure 6-1. Maturing Security Policy Development (Van de Voort et al., 2007).

6.2. Policy Enterprise Modeling

The issue of counterfeit parts in the DoD supply chain can be considered as an enterprise problem with technical and socio components due to current multi-organizational system

acquisition and sustainment practices (Rouse & Bodner, 2013). Technical facets of the problem include systems engineering design in acquisition, sustainment networks and part flows, inventories, inspection regimens, and trusted supplier designation based on objective criteria, while socio facets include trust and collaboration, communication, information-sharing, and reaction to incentives (Rouse & Bodner, 2013). Decisions, actions, and outcomes are formulated and enacted in different areas of the enterprise as shown in Figure 6-2:

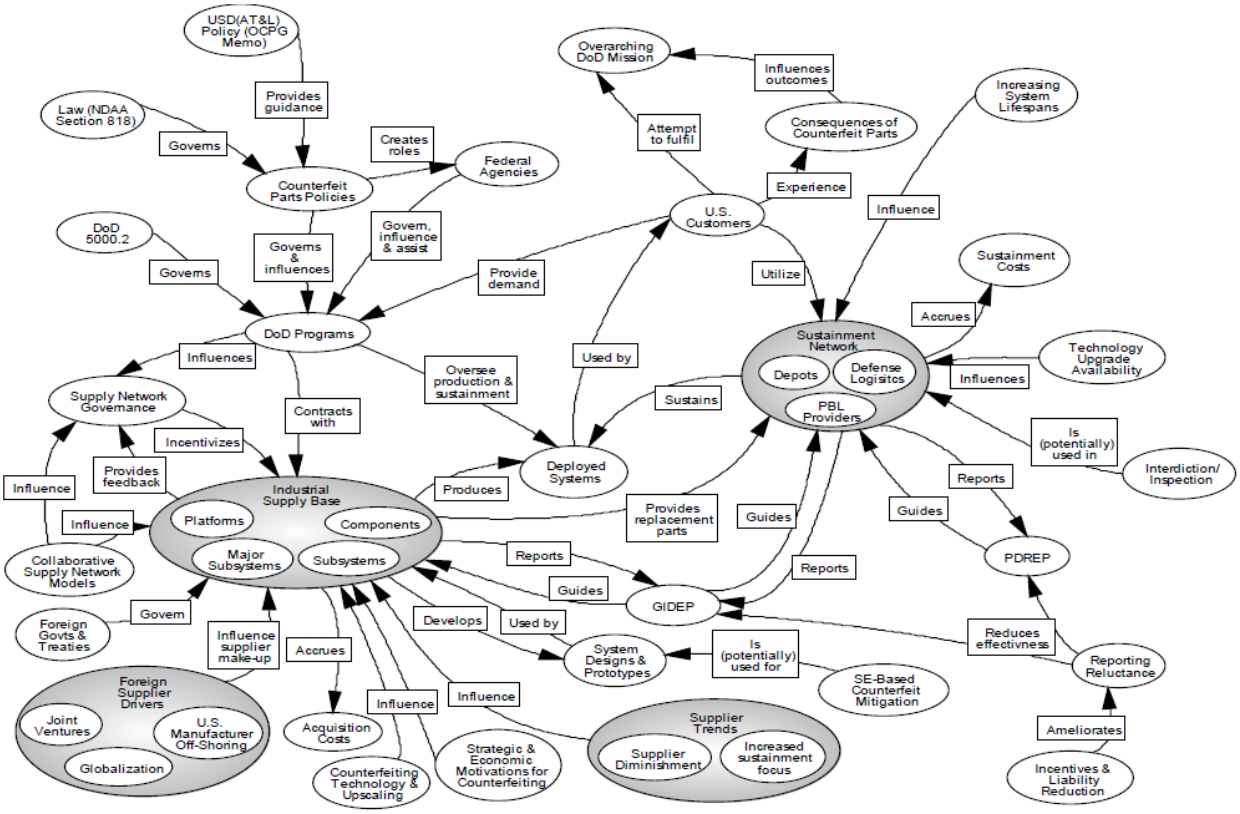


Figure 6-2. Counterfeit Parts Domain Ecosystem (Rouse & Bodner, 2013).

Much like a Cause-Effect Mapping Diagram, Figure 6-2 highlights relationships between different components within the ecosystem and allows for further exploration of a specific area (Rouse & Bodner, 2013). The ecosystem may be subject to trends including globalization, joint ventures, and new business models and consequentially exposed to counterfeiting risks from sources with either strategic or economic motivations (Rouse & Bodner, 2013). The ecosystem also may experience different trends such as increased system life spans and technological advancement as it transitions from acquisition to sustainment; thus, the ecosystem as a whole

encounters aggregate outcomes resulting from counterfeiting with respect to the impact on the overall mission (Rouse & Bodner, 2013).

Enterprise modeling can be performed as a way to test different policies for effectiveness in a multi-stakeholder environment and to capture the socio-technical nature of the counterfeit parts problem (Bodner, 2015; Bodner, 2014). This approach consists of five interacting elements, namely the exogenous environment, policy, enterprise actors, supply chain flows, and system/constituent behavior and performance, and can be used to identify strategies to tackle problems as well as to characterize unintended or secondary policy effects (McDermott et al., 2013; Park et al., 2012; Bodner, 2015; Bodner, 2014). The DoD has several different policy levers that it can apply in an enterprise simulation, some involving external government agencies including DHS, Customs and Border Patrol (CBP), and the Department of Justice (DOJ) (Federal Register, 2014; Livingston, 2007; McFadden & Arnold, 2010; Bodner, 2015).

6.3. Federal Legislation and Regulation

Congress and Government agencies are concerned with crafting and implementing legislation and policies to reduce or eliminate the risk associated with counterfeit parts through testing and interdiction or the use of trusted suppliers (Rouse & Bodner, 2013). A number of factors must be considered when developing new policies, such as the safety and expected performance of a system versus the cost and availability of spare parts (Rouse & Bodner, 2013). Ultimately, certain parties will be incentivized to behave in certain ways on account of policies and practices employed to address the counterfeit parts problem in the DoD supply chain, some expected and some unexpected (Rouse & Bodner, 2013).

This thesis focuses on two particular pieces of legislation, the Sarbanes-Oxley Act of 2002 and the Final Defense Federal Acquisition Regulation Supplement (DFARS) Rule for the Detection and Avoidance of Counterfeit Electronic Parts of 2014. The impact of subsequent National Defense Authorization Act (NDAA) provisions is explored, and potential policy-related solutions to the counterfeit parts problem are proposed.

6.3.1. Sarbanes-Oxley Act of 2002

The Sarbanes-Oxley Act of 2002, passed by Congress primarily to protect investors from the possibility of fraudulent accounting activities by corporations, mandates that top management is directly accountable for policing internal process controls and documenting procedures for "risk assessment and risk response" (United States Code, 2002). Sections 401, "Disclosures in Periodic Reports" and 404, "Management Assessment of Internal Controls," of the Act extend the scope of regulation into strategic procurement and address issues including inter-organizational risk sharing and risk transfer (Peck, 2006). Moreover, Sarbanes-Oxley requires that companies providing outsourced services be able to demonstrate the existence of internal process controls and give consideration to potential disruptions external to a company or system (Peck, 2006).

6.3.2. Final DFARS Rule of 2014

Gradual measures have been employed by the DoD and industry partners to enact policy change focusing on the prevention of counterfeit electronic parts. These efforts have culminated in the release of the Final Defense Federal Acquisition Regulation Supplement (DFARS) Rule for the Detection and Avoidance of Counterfeit Electronic Parts (Federal Register, 2014). The battle against counterfeiting in aerospace and defense is an effective example of government and industry stakeholders being involved from the outset and embarking upon parallel strategies to create policy through formal channels, including Congress, where there previously was a void.

Corresponding streams of concern have shaped and brought about the policy process addressing the damaging practice to date, with government and industry taking separate, incremental steps sometimes leveraging off of one another in order to move upward in the slow climb to conquer counterfeiting. Government agencies involved in this process include the DoD, the National Aeronautics and Space Administration (NASA), the Federal Aviation Administration (FAA), the Department of Commerce, the Department of Justice, the FBI, the Department of Homeland Security (DHS), the Government Accountability Office (GAO), and the Customs and Border Patrol Protection (CBP) agency among others. Two industry groups entrenched in this process include SAE International (formerly known as the Society of Automotive Engineers, the group has a strong aerospace focus and is a well-known publisher of aerospace standards) and the

Aerospace Industries Association (AIA), which represents almost 150 aerospace and defense manufacturers as well as a significant portion of the supplier base.

One of the earliest efforts in the battle to rein in counterfeit parts was the Organisation for Economic Co-Operation and Development's (OECD's) 1998 report on the economic effects of counterfeiting. This report was followed up with a more comprehensive report addressing the "magnitude and scope" of the counterfeiting problem in 2005 (Aerospace Industries Association of America, Inc., 2011). Meanwhile, the U.S. Chamber of Commerce established the Coalition Against Counterfeiting and Piracy (CACP) in 2004 to tackle the mounting threat of counterfeiting and piracy to the economy, jobs, and consumer health and safety (Aerospace Industries Association of America, Inc., 2011).

Another early effort in response to the increasing counterfeit parts threat was the summit conducted by the AIA for its member organizations in August 2007. Government and industry stakeholders came together to discuss challenges posed by counterfeit components to the aerospace and defense industries, in particular risks associated with cost, schedule, safety, and mission success. As a result, the AIA Counterfeit Parts-Integrated Project Team (CP-IPT) was established in December 2007. (The SAE G-19 Counterfeit Electronic Components Committee was also chartered in November 2007.) The CP-IPT produced tailored recommendations for use by government and industry, several of which have been incorporated into or have influenced later standards and policy addressing counterfeit parts.

Technical standard SAE AS5553, "Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition" was issued by SAE International on April 2, 2009. The standard, motivated by economic and security interests, was created to address a significant and growing volume of counterfeit electronic parts entering the aerospace supply chain and posing risks in the areas of performance, reliability, and safety (SAE International, 2009). The standard additionally specified uniform requirements, practices, and methods pertaining to counterfeit electronic parts with the goal of mitigating system risk. This document was widely promulgated and adopted by DoD and NASA shortly after release. (SAE AS5553 was adopted by DoD on August 31, 2009 and incorporated into the NASA Parts Policy dated November 3, 2008.) SAE AS5553 and its

subsequent implementation is an important example of industry influencing government in the effort to address counterfeit electronic parts.

The "Defense Industrial Base Assessment: Counterfeit Electronics" report was released by the U.S. Department of Commerce's Bureau of Industry and Security (BIS) in January 2010. The U.S. Navy's Naval Air Systems Command (NAVAIR) requested the report almost three years prior in response to suspicions that an increasing number of counterfeit electronic components were permeating the DoD supply chain and negatively impacting the reliability of certain weapon systems. The BIS report quantifies the growth of counterfeiting within aerospace and defense supply chains, examines government and industry practices and procedures that may contribute to counterfeiting, and puts forward recommendations and best practices for preventing and mitigating the effects of counterfeit electronic components. This was accomplished through surveying five segments of the defense supply chain: Original Component Manufacturers (OCMs), brokers and distributors, companies involved with circuit board assembly, prime contractors and subcontractors, and DoD agencies.

The BIS report found that the number of electronics counterfeiting incidents (some of which involved DoD-qualified components) rose from 3,369 in 2005 to 8,644 in 2008 (U.S. Department of Commerce, 2010). The BIS attributes this increase to several factors, including a growth in the number of counterfeit parts, more effective methods of detection, and better tracking of counterfeiting incidents (U.S. Department of Commerce, 2010). The report additionally details adverse effects on government (national security impacts, enforcement costs, lost tax revenue), industry (risk mitigation and replacement costs, lost sales), and consumers (replacement costs, safety concerns) and exposes that the DoD had yet to adopt regulations for the authentication of parts or reporting of counterfeiting incidents. The BIS report explicitly recommends clarifying criteria in the Federal Acquisition Regulations (FAR), including DFAR, to promote the ability to award electronic parts contracts on the basis of "best value" rather than on the criteria of "lowest price" or "low bid" in an effort to ensure component quality and limit opportunities for counterfeit parts to gain entry into the aerospace and defense supply chain (U.S. Department of Commerce, 2010).

A major issue in countering the proliferation of counterfeit parts in the aerospace and defense supply chain is the hesitance of organizations to report problems. While the reporting of counterfeits is critical, as it allows government and industry partners to search inventory and intercept potential problems, companies may not report potentially compromised parts for myriad reasons. The BIS report found that 88 percent of OCMs were not reporting suspected counterfeit parts to the Government Industry Data Exchange Program (GIDEP), which was selected as the primary counterfeit reporting organization by the AIA CP-IPT (U.S. Department of Commerce, 2010). Membership to the GIDEP is free of charge, and participating organizations include the U.S. Army, Navy, Air Force, Defense Logistics Agency (DLA), NASA, Department of Energy, Department of Labor, Department of Commerce, General Services Administration (GSA), Federal Aviation Administration (FAA), U.S. Postal Service (USPS), National Institute of Standards and Technology (NIST), National Security Agency (NSA), and the Canadian Department of National Defense (Aerospace Industries Association of America, Inc., 2011).

Frequent reasons for not reporting include being unaware of GIDEP or its function of tracking counterfeiting, assuming too few incidents to justify reporting, attempting independently to resolve the issue with the supplier or part manufacturer, or using an alternate system to report counterfeit components. Organizations also cite potential legal and liability issues and a lack of support or process to promulgate such findings external to the organization for choosing not to report. Notably, GIDEP issued an interim policy change on the topic of "Reporting Suspect Counterfeit Parts and Materials" in September 2010 with the goal of facilitating and encouraging "the reporting of suspect counterfeits until such time as federal policy and an appropriate supporting procedure can be determined and implemented" (Aerospace Industries Association of America, Inc., 2011). The policy change sought to encourage organizations to report counterfeit components by requiring the category of the component supplier in question rather than mandating the manufacturer or supplier name.

Two closely-following U.S. Government Accountability Office (GAO) reports, "Defense Supplier Base: DOD Should Leverage Ongoing Initiatives in Developing Its Program to Mitigate Risk of Counterfeit Parts" (March 2010), and "Intellectual Property: Observations on Efforts to Quantify the Economic Effects of Counterfeit and Pirated Goods" (April 2010), further raised

governmental awareness of the presence of counterfeit parts in aerospace and defense supply chains. GAO's Defense Supplier Base report, written in response to a congressional request from Senators Sherrod Brown and Evan Bayh in 2009, presents an alarming assessment of counterfeit parts in the DoD supply chain and notes the lack of a dedicated policy or process for detecting and preventing counterfeit electronic components. The report reveals the DoD's lagging response to the issue, being in the "early stages of gathering information on the counterfeit parts problem," and the lack of a universal definition of "counterfeit parts" (Government Accountability Office, 2010a). Furthermore, GAO's Observation on Efforts was written in response to a directive seeking additional information on the impacts of counterfeit goods in the Prioritizing Resources and Organization for Intellectual Property Act of 2008 (PRO-IP Act), passed by Congress in October 2008. The report studied existing research on the impacts of counterfeiting and piracy on government, industry, and consumers and provided insights from efforts to quantitatively express the effects of counterfeiting and piracy on the U.S. economy.

Awareness of the counterfeit parts issue spread rapidly. The AIA's "Counterfeit Parts: Increasing Awareness and Developing Countermeasures" special report, released in March 2011, utilized causal stories invoking economic and security concerns to convey the severity and urgency of the counterfeit electronic parts problem, summarized government and industry efforts to date, and provided recommendations from the CP-IPT (specifically the deployment of a risk mitigation process as stated in SAE AS5553 and strengthening of the GIDEP). Meanwhile, the Senate Armed Services Committee (SASC) became aware of the BIS report; a subsequent SASC investigation and hearing in November 2011 confirmed the Department of Commerce's findings of counterfeit parts permeating defense, aerospace, and commercial supply chains and provided a basis for further investigation into counterfeiting. Almost immediately after the SASC conclusion on November 29, 2011, Chairman of the SASC Senator Carl Levin introduced an amendment to the National Defense Authorization Act (NDAA) for Fiscal Year 2012 seeking to establish federal guidelines for the detection and reporting of counterfeit components. This amendment passed and became law with President Obama's signature on December 31, 2011.

The National Defense Authorization Act (NDAA) for both Fiscal Years 2012 and 2013 contained special provisions (Section 818 and Section 833, respectively) for addressing the issue of counterfeit parts. Section 818, "Detection and Avoidance of Counterfeit Electronic Parts,"

requires the Secretary of Defense to "assess DoD's acquisition policies and systems for the detection and avoidance of counterfeit parts," while Section 833, "Contractor Responsibilities in Regulations Relating to Detection and Avoidance of Counterfeit Electronic Parts," amends Section 811, "Additional Contractor Responsibilities in Regulations Relating to Detection and Avoidance of Counterfeit Electronic Parts," of the 2012 act in an effort to confront "allowability requirements for the costs of counterfeit electronic parts" and associated corrective actions (Covington & Burling LLP, 2014). The DoD issued a proposed rule on counterfeit electronic parts in an effort to implement these requirements on May 16, 2013. Meanwhile, the House considered a provision for additional contractor responsibilities in regulations pertaining to the detection and avoidance of counterfeit electronic parts in the NDAA for Fiscal Year 2014; Section 811, which would have amended Section 818 of the 2012 NDAA, was not adopted in the final legislation (U.S. Congress, 2013). During this time period, SAE International released AS6081, "Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition – Distributors" (November 7, 2012) as well as an update to AS5553, AS5553A (January 21, 2013). Following a comments period of nearly a year, the Final DFARS Rule for the Detection and Avoidance of Counterfeit Electronic Parts (DFARS Case 2012-D055), was finally issued on May 6, 2014.

The Defense Federal Acquisition Regulation (DFAR) governs the "basic legal guidelines and rules by which defense procurement takes place," and the DFARS Final Rule for the Detection and Avoidance of Counterfeit Electronic Parts layers on top of acquisition rules already in existence (U.S. Department of Commerce, 2010). Even as an addition to the existing DFAR, the Final Rule is positioned to bring about substantial change. The Final Rule addresses how organizations must treat electronic parts in their respective supply chains when contracting with the government, establishes an agreed-upon definition for counterfeit electronic parts, mandates government contractors to develop and maintain a counterfeit electronic part detection and avoidance system addressing a minimum of twelve enumerated areas, and requires reporting of suspected incidents of counterfeiting to the GIDEP. The Final Rule applies to "counterfeit electronic parts," "suspect electronic parts," and "obsolete electronic parts."

6.3.3. Subsequent NDAA Provisions

Subsequent NDAAs also include content relating to counterfeit parts; the DoD can propose to amend the DFARS in order to implement a newly-mandated NDAA requirement. The Senate considered a provision that would clarify sourcing requirements essential to avoiding counterfeit electronic parts in Section 824, "Matters Relating to Reverse Auctions," of the NDAA for Fiscal Year 2015; while not considered by the House, Section 817, "Sourcing Requirements Related to Avoiding Counterfeit Electronic Parts," of the agreement includes the Senate provision along with a clarifying amendment and amends Section 818 of the 2012 NDAA (U.S. Congress, 2014).

The NDAA for Fiscal Year 2016 addresses counterfeit parts in two separate sections. Section 238, "Study of Field Failures Involving Counterfeit Electronic Parts," requires DoD to perform hardware assurance studies to assess the impact of counterfeit electronic parts that have passed through the supply chain and into fielded systems upon DoD operations (U.S. Congress, 2015). Furthermore, Section 885, "Amendments Concerning Detection and Avoidance of Counterfeit Electronic Parts," expands the criteria for contractors to include counterfeit parts-related costs for rework and corrective actions as allowable expenses under DoD contracts and permits the DoD to approve trusted suppliers selected by industry (U.S. Congress, 2015).

6.4. Potential Policy Solutions

Congress and Government agencies, in particular the DoD and DHS, must continue to address the threat of counterfeit parts in the supply chain; however, the solutions must strike an appropriate and acceptable balance between risks and costs given continued budgetary constraints (Gansler et al., 2014). Three recommendations to continue to address the threat of counterfeit parts and to explore necessary trade-offs within the within the supply chain include:

- Strengthening standards.
- Implementing stronger preventative measures.
- Developing a long-term strategy (Gansler et al., 2014).

6.4.1. Strengthening Standards

The DoD has implemented industry standards (including AS5553 as noted above) and continues to be a member of government and industry working groups responsible for developing

international standards for the aerospace and automotive industry (Government Accountability Office, 2016a). As the acquirer and supplier share responsibility for system security, the DoD should require contractors to rely on recognized standards when devising counterfeit detection and mitigation procedures as well as clarify the criteria upon which DoD will assess contractor systems (LeSaint et al., 2015; Gansler et al., 2014; Government Accountability Office, 2016a). DoD program managers should perform further outreach to contractors, partnering with individual companies to craft individualized, risk-based approaches to counterfeit mitigation that adheres to established, applicable standards (Gansler et al., 2014). The DoD should impose stringent quality assurance standards, given that non-conforming parts threaten the integrity of mission-critical systems and can lead to costly remediation measures (Gansler et al., 2014).

Finally, the DoD should embark on a series of measures to provide increased compliance with the GIDEP reporting requirement among the defense supplier-base (Government Accountability Office, 2016a). The DoD should establish mechanisms for department-wide oversight of GIDEP reporting requirement compliance by defense agencies; develop a standardized process, along the lines of a tiered reporting structure, for figuring out the amount of evidence needed to report a part as a suspect counterfeit in GIDEP; and create guidance regarding access to GIDEP reports for government versus industry users (Government Accountability Office, 2016a). It should be noted that the DoD is expected to release a new instruction in 2017 covering the use of GIDEP and including guidance as to when GIDEP reports should be released to industry versus restricted to government only (Government Accountability Office, 2016a). The DoD should consider expanding GIDEP reporting of suspect counterfeits to foreign companies along with potential penalties for non-compliance (Gansler et al., 2014).

6.4.2. Implementing Stronger Preventative Measures

Given the potential for system and mission impact, the DoD should advocate for the implementation of stronger preventative measures with the ability to keep counterfeit parts out of defense systems. The DoD should encourage the use of existing deterrent measures, including tamper-proof packaging and non-destructive evaluation methods such as x-ray inspection, and invest in the development of new anti-counterfeiting technologies (Gansler et al., 2014). One example of such investment is the Defense Advanced Research Project Agency's (DARPA's) Supply Chain Hardware Integrity for Electronics Defense (SHIELD) Program, which seeks to

eliminate counterfeit integrated circuits through the development of a "dielet," or 100 micrometer by 100 micrometer chip incorporating passive, unpowered sensors, capable of being inserted into the packaging of an integrated circuit and having its provenance verified via the use of an external probe facilitating a secure link (Defense Advanced Research Projects Agency, n.d.). Expected to cost less than a penny each, the dielet is designed to be "robust in operation, yet fragile in the face of tampering" and to offer "an on-demand authentication method never before available to the supply chain" (McDuffee, 2014). The DoD should also consider debarring suppliers who consistently furnish components containing counterfeit parts (Gansler et al., 2014).

6.4.3. Developing a Long-Term Strategy

The Defense Science Board Task Force on High Performance Microchip Supply concluded a decade ago that DoD had "no overall vision of its future microelectronics components needs and how to deal with them" and that technology and supply problems were being addressed reactively rather than proactively (Department of Defense, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, 2005; Government Accountability Office, 2015c). Furthermore, the report stated that "an overall vision would enable the Department to develop approaches to meeting its needs before each individual supply source becomes an emergency" (Department of Defense, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, 2005; Government Accountability Office, 2015c). The overarching DoD Counterfeit Prevention Policy and Trusted Defense Systems Strategy are in need of strategy-related updates, and strategic considerations should also be included in future NDAAs.

Current strategies developed by the DoD, in conjunction with industry, to tackle the counterfeit parts problem include:

- Acquisition regulations addressing supplier qualification, suspect counterfeit reporting, supplier penalties for counterfeits and pass-throughs (Federal Register, 2014).
- Use of a secure trusted foundry network of suppliers to reverse engineer and produce obsolete parts.
- Testing regimens to detect counterfeits at points where they enter the supply chain (McFadden & Arnold, 2010).

- Traceability of components throughout traversal of the supply chain (similar to the DARPA SHIELD Program) (Livingston, 2007).
- Criticality analysis under Program Protection Plans to focus on parts/sub-systems deemed mission critical.
- Industry standards for supplier qualification (SAE International, n.d.).
- Obsolescence management and re-engineering obsolete sub-systems.
- Law enforcement to identify and remove counterfeiters (Bodner, 2014).

The critical question is determining what set of the above strategies is best for addressing the problem of counterfeits, taking cost, effectiveness, and the adaptive behavior exhibited by suppliers and counterfeiters into consideration (Bodner, 2014). Each countermeasure has an associated cost, which may be shouldered by one or many stakeholders and may include research and development investment costs, operational costs, monitoring and inspection costs, and increased part costs (along with decreased part availability) on account of trusted suppliers producing a limited supply of a particular component (Rouse & Bodner, 2013). In this circumstance, the DoD should focus on best value, instead of lowest cost, in its acquisition of critical technologies to combat counterfeit parts (Gansler et al., 2014).

Furthermore, the DoD should seek to minimize the impact of obsolescence by using parts and components for which multiple suppliers exist when possible (Gansler et al., 2014). Use of the Trusted Foundry and Defense Microelectronics Activity (DMEA)-accredited trusted suppliers can further assure the integrity of microcircuits and other components (Department of Defense, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, 2014). In situations with a sole or high-risk supplier, the DoD should develop a robust obsolescence management strategy utilizing comprehensive testing and inspection measures (Gansler et al., 2014; Meshel, 2014). In addition, the DoD should enhance part availability throughout a product's life cycle though practices such as identifying acceptable substitute products and engaging in system redesign (Meshel, 2014). The United States should position itself to retain domestic design capabilities for critical technologies if at all possible, through the implementation of effective policy and coordination between stakeholders on issues such as trusted foundries (Gansler et al., 2014).

Developing a long-term strategy to address counterfeit parts in the DoD supply chain and to assure access to secure and reliable microelectronics is imperative to maintain national security and military superiority, as the threat of counterfeit parts is real and will continue to escalate in the coming years (Government Accountability Office, 2015c; Gansler et al., 2014). The DoD and its industry partners will need to work together in order to formulate, enact, and promulgate regulatory vehicles, particularly focusing on acquisition, capable of keeping up with technological capabilities and addressing critical system vulnerabilities. This will involve assessing vulnerabilities with respect to exposure and exploitability and mitigating risk to acceptable levels at a reasonable cost in order to diminish critical threats (Baldwin et al., 2012; Gansler et al., 2014). Policy is capable of impacting all parts of a system or supply chain – from spontaneous events to terminal events; therefore, careful consideration must be afforded to the alignment of applicable incentives, penalties, and rewards (Gansler et al., 2014). This will ensure that the expected behavior of stakeholders results in the desired outcome and does not create further uncertainties or vulnerabilities within a complex system.

CHAPTER 7: CONCLUSION

A study conducted by MIT over ten years ago discovered that "most companies are still not thinking systematically about managing supply chain risks and vulnerabilities" (Sheffi, 2007). This thesis explores the concept of vulnerability, in particular the lack of a holistic understanding of how the concept applies to complex systems and the paucity of support tools for identifying and accounting for vulnerability in supply chains (Centre for Logistics and Supply Chain Management at the Cranfield School of Management, 2003). Supply chains are essential to the safe, secure, and timely movement of goods and information; however, these complex systems are vulnerable to internal and external disruptions and subject to exploitation. This can result in adverse impacts to the system and inhibit value delivery.

This thesis proposes a generic model applicable to supply chains that can guide a user through existing vulnerability assessment techniques and reveal information regarding system vulnerabilities as well as opportunities for decision-makers to intervene. The model, adaptable to a diversity of systems and capable of recognizing non-obvious sources of vulnerability, can be used by systems engineers to impart system understanding and to provide a holistic view of a complex supply chain. Furthermore, the generic model assists the user with formulating a list of vulnerabilities and associated interventions and with communicating information regarding supply chain vulnerabilities to decision-makers and other stakeholders.

7.1. Research Questions

The following research questions were proposed in Chapter 1 in order to better understand where and how complex systems are vulnerable and to assist decision-makers in selecting potential interventions:

1. How can vulnerability assessment be defined within a complex engineering systems context?

2. What strategies can system architects use to identify "intervention points," or places within the system where causal chains can be disrupted to reduce or prevent vulnerabilities?

3. How can a comprehensive framework for vulnerability assessment facilitate better decisions with respect to uncertainty, resource constraints, and policy implications?

Within a complex engineering systems context, vulnerability assessment is defined as the study of the characteristics of a system in order to discern vulnerabilities and can be used to evaluate and record vulnerabilities that may impede or degrade the performance or capabilities of a system. Vulnerability assessment is an essential step for uncovering weaknesses, or areas in which a critical function can be accessed and exploited, in a system's design, development, production, components, operation, or supply chain (Popick & Reed, 2013). A comprehensive evaluation of a complex engineering system requires consideration of a broad spectrum of hazards and threats, including failures, in addition to (inter)dependent elements with non-linear behavior and feedback loops. A vulnerability assessment should consider the environment in which a system operates and the objectives which a system is designed to attain, strive to identify obvious as well as covert vulnerabilities within a system, and enable a decision-maker to intervene to manage and/or mitigate these vulnerabilities (Kröger & Zio, 2011; Zio et al., 2011). Finally, a vulnerability assessment is an iterative process that should be repeated at multiple points in the system life cycle to address emerging and persistent threats.

System architects can select from different strategies to identify "intervention points," or places within the system where causal chains can be disrupted to reduce or prevent vulnerabilities. A Cause-Effect Mapping Diagram illustrates relationships between different causes and effects and allows a user to identify perturbations with the greatest number of causes and effects, respectively. Before and after these nodes are ideal places to implement measures to allow a system to avoid, mitigate, or recover from a perturbation. The effective implementation of countermeasures can also play a role in preventing, detecting, and responding to an adverse event or perturbation impacting a system (Reed, 2012a). Some countermeasures can reduce the exploitation of development, design, and supply chain vulnerabilities; others can monitor, alert, and capture data about an attack; and a final set of countermeasures can analyze an attack and subsequently alter a system or processes to mitigate an attack (Reed, 2012a).

In addition, System Security Engineering (SSE), Trusted Systems and Networks (TSN) Analysis, and the definition and implementation of leading indicators can each inform further understanding of a system's vulnerabilities. SSE, as implemented through TSN analysis, applies scientific and engineering principles to identify security vulnerabilities and to minimize associated risks; evaluates vulnerabilities with respect to exposure, exploitability, and the

prevalence of attack paths; and asserts six different tools and techniques as useful methods for assessing the vulnerability of complex systems (Baldwin et al., 2012). Leading indicators provide a valuable predictive measure of how the vulnerability of a system will develop and portray the direction of vulnerabilities (Hofmann et al., 2012; Zimmerman, 2004).

A comprehensive framework for vulnerability assessment as illustrated by the generic model can facilitate better decisions with respect to uncertainty, resource constraints, and policy implications by developing comprehensive system understanding, allowing for better use of existing vulnerability assessment techniques, and providing a better, holistic grasp of the vulnerability space. The process involved with creating a Cause-Effect Mapping Diagram guides the user through identifying terminal events and tracing perturbations until spontaneous, or root-cause events, are reached. The generic model is capable of imparting holistic, system-level understanding of a complex system, taking diverse socio-technical factors into account, and formulating a list of vulnerabilities and associated interventions enabling informed decisions.

Furthermore, vulnerability metrics provide an essential link between strategy, execution, and value creation (Melnyk et al., 2004). Metrics for static vulnerability assessment can take the form of basic connection and measurement metrics, spectral measurements, and statistical and probabilistic measurements (Rocco et al., 2012). While these categories of approaches have respective strengths and weaknesses, they all enable decision-makers and policy makers to target minimizing the vulnerability of a complex system to external events, such as a natural disaster or man-made actions, through the identification of vulnerable and weak points via specific metrics systems (Rocco et al., 2012). Better information, provided through a comprehensive metrics approach, can lead to the communication of system information and empower decision-makers to make better choices.

7.2. Research Contribution

The research contribution of this thesis is the in-depth exploration of vulnerability and vulnerability assessment as pertaining to complex systems and the development of a generic model capable of imparting system-level understanding of vulnerabilities specific to a supply chain and taking socio-technical factors into account.

The research conducted for the purposes of this thesis yields three findings concerning the vulnerability assessment of complex systems:

1. Cause-Effect Mapping is a useful analytic technique for assessing vulnerability and exploring relationships between the causes and effects of perturbations and non-linear relationships within a system.

Cause-Effect Mapping can guide a user in identifying an appropriate scope of a system for analysis, identifying spontaneous through terminal events, and developing a comprehensive Cause-Effect Mapping Diagram for further evaluation. Cause-Effect Mapping provides a more compact and robust representation of a system than Fault Tree Analysis (FTA), and the technique can be particularly useful for future system acquisition decisions.

2. The vulnerability assessment of complex critical infrastructure and supply chain systems is a broad field encompassing a number of disciplines, including risk, management, logistics, and the humanities.

The research investigation conducted for the purposes of this thesis has gathered a wide body of literature that can serve as the foundation for future research on socio-technical factors impacting systems vulnerability.

3. Placing different existing vulnerability assessment techniques into a structured process can allow a user to conduct a thorough evaluation of vulnerabilities impacting a system and to uncover non-obvious vulnerabilities.

The different vulnerability assessment techniques presented in this thesis have different strengths and weaknesses, based on when a technique is best implemented with respect to the system life cycle and the specific characteristics of the system under evaluation (whether the system or supply chain primarily consists of hardware, software, or firmware among other factors). Vulnerability assessment techniques can work in concert across the system life cycle, and the outcomes of one technique can be compared and contrasted with those of another technique (LeSaint et al., 2015; Rovito & Rhodes, 2016).

The generic model brings together three different vulnerability assessment techniques in a sequential process that allows for a robust evaluation of vulnerabilities affecting a system. Cause-Effect Mapping, the usefulness of which is noted above, provides an initial foundation of knowledge with respect to the relationships between different causes and effects and intermediate perturbations. SSE and TSN analysis present six different vulnerability techniques, one or more of which can be selected to further investigate access paths for possible exploitation within a system. Finally, leading indicators are an effective predictive measure that can be enacted within a system to detect potential problems before they occur. The usefulness of this approach was reinforced during the expert evaluation of the generic model conducted at a not-for-profit engineering corporation.

7.3. Future Work and Limitations

Several research areas merit further investigation with respect to future work. One area of interest is the integration of the TSN vulnerability assessment into the larger TSN risk assessment picture. A more complete understanding of the system can be gained by conducting criticality and threat analyses in concert with the vulnerability assessment and combining the results as show in Figure 7-1 below.

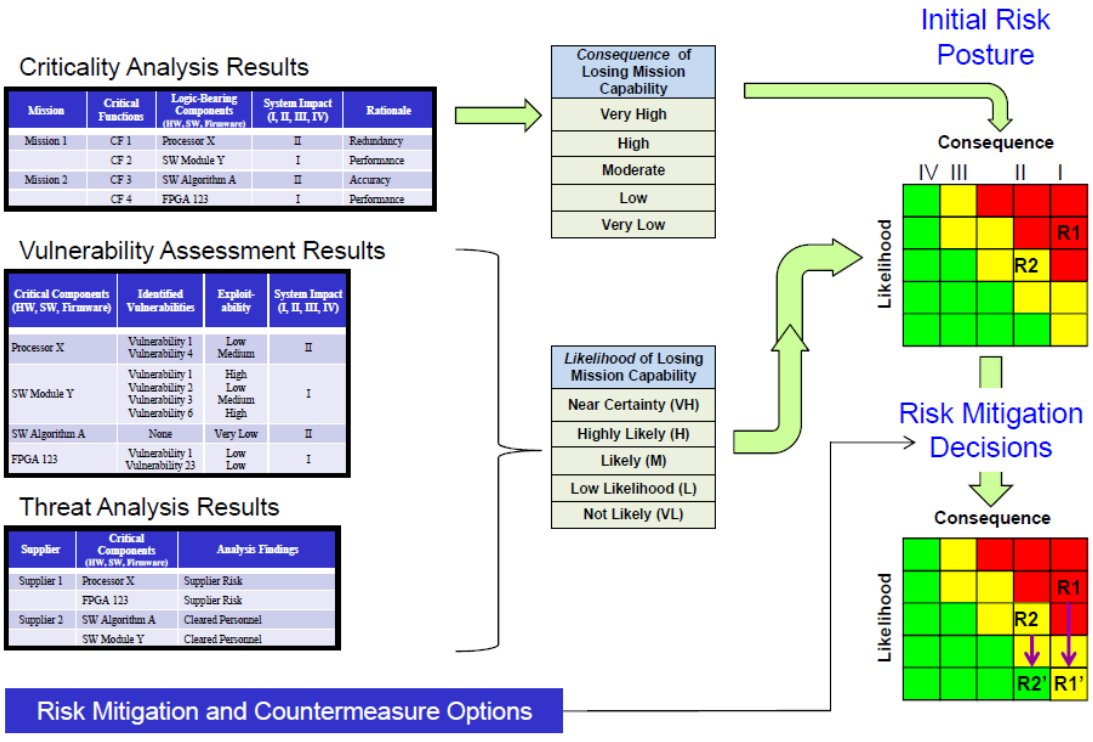


Figure 7-1. Full Trusted Systems and Networks (TSN) Analysis Methodology.

Developing and incorporating a go-to quantitative metric or metrics as part of the generic model is another area of future work. Wang et al. (2008) acknowledge that there is a gap between existing security metrics, which tend to focus on individual vulnerabilities, and qualitative models of vulnerabilities, which are usually constrained to binary views of security. There is a demonstrated need for metrics to measure the combined effects of vulnerabilities within a system, since the exploitation of one vulnerability often makes subsequent vulnerabilities easier to exploit. While the aggregated approach proposed by Frigault & Wang (2008) does make some headway, further research is necessary in order to employ Dynamic Bayesian Networks to add robustness to the Temporal domain measurements found within CVSS. Research on change, risk, and vulnerability propagation throughout a system could be an additional area of focus.

Portfolio analysis, namely selecting which portfolio of countermeasures should receive investments to mitigate the problem impacting a system, merits further investigation as a method for evaluating strategies for success (Rouse & Bodner, 2013). This is specifically called out as an underdeveloped area in the supply chain management field per Knemeyer et al. (2009). The Analytic Hierarchy Process (AHP), a pair-wise comparison method used by Government agencies for prioritizing interventions and capabilities, should also be explored in greater detail.

The supply chain pilot application should consider personnel issues beyond strike or furlough, as talent management considerations including knowledge transfer and the "Silver Tsunami" are becoming more of an issue in the high-tech and manufacturing workplace. Supply chain best practices and synergies should also be sought out beyond aerospace and defense, particularly in the automotive industry.

In addition to technical limitations impacting future research, close attention must be paid to Government and industry policies and standards. These continue to change given evolving threats and require flexibility and adaptability. Fiscal limitations will always be present as well, as both Government and industry seek to trim expenses while increasing profit.

Predicting and mitigating system vulnerabilities and designing appropriate interventions can lead to the development of more resilient systems, capable of delivering a sustained level of value. However, ensuring secure and resilient systems is an art of balancing risk and cost (Singhal & Ou, 2011). The generic model proposed in this thesis is a small step towards making use of

existing assessment tolls and providing a better, holistic grasp of the vulnerability space, enabling decision-makers to make informed choices with respect to vulnerable complex systems.

APPENDIX A: SPIDERS CASE STUDY

This appendix contains additional detailed information pertaining to the SPIDERS Case Application found in Chapter 2 and the Supply Chain Case Application found in Chapter 5.

Table A-1 provides additional information about each perturbation found in the SPIDERS Phase 2 Cause-Effect Mapping Diagram.

Table A-1. Description of Perturbations in SPIDERS Phase 2 Cause-Effect Mapping Diagram.

Perturbation	Type	Description	Causes	Effects
Electric Grid Failure	Terminal Event	Both Commercial Grid and Microgrid Unavailable	Commercial Grid Unavailable	Unable to execute mission (provide electricity)
Commercial Grid Unavailable	---	Commercial Grid is unavailable to provide electricity when the microgrid is unavailable	Lack of Service Level Agreement, Connection Equipment Failure	Electric Grid Failure
Connection Equipment Failure	---	Equipment allowing the unavailable microgrid to connect to the commercial grid fails	Microgrid Unavailable	Commercial Grid Unavailable
Lack of Service Level Agreement	---	Policies do not exist permitting the infrastructure of the unavailable microgrid to connect to the commercial grid	Microgrid Unavailable	Commercial Grid Unavailable
Microgrid Unavailable	---	Microgrid is offline and incapable of delivering electricity	Control Systems Unavailable	Lack of Service Level Agreement or Connection Equipment Failure

Control Systems Unavailable	---	Control Systems malfunctions lead control system to no longer function	Control Systems Malfunction, Natural Disaster, Lack of Redundancy	Microgrid Unavailable
Control Systems Malfunction	---	Changes are made to control systems so that they no longer function properly or function maliciously	Internal Comms Disruption, Data or Software Tampering	Control Systems Unavailable
Network Resources Taxed	---	Increased network traffic requires full network resources in order to function	Uncontrolled Network Traffic	Microgrid Unavailable
Uncontrolled Network Traffic	---	Attackers make changes that flood the network with traffic	Unauthorized Access, Data or Software Tampering	Network Resources Taxed
Data or Software Tampering	---	Attackers make changes to existing data or software	Unauthorized Access	Control Systems Malfunction or Microgrid Unavailable
Unauthorized Access	---	Attackers gain access to parts of system requiring administrative privileges (also includes access to passwords and critical data)	Cyber Attack	Data or Software Tampering or Uncontrolled Network Traffic
Internal Comms Disruption	---	Internal communications systems cease to function properly	Cyber Attack	Control Systems Malfunction
Task Failure	---	A necessary or required task is not performed or completed	Operator Overworked or Unavailable	Microgrid Unavailable
Insufficient Backup Plans/Capabilities	---	Plans or redundant systems are not	Cherry Pick Loads, Natural Disaster	Lack of Redundancy

		in place to backup major system functions		
Lack of Redundancy	---	No or not enough redundant systems are in place to effectively mitigate operational risk	Insufficient Backup Plans/Capabilities	Control Systems Unavailable or Microgrid Unavailable
Staffing Needs Unmet	---	No or not enough staff is in place to effectively operate the system	Strike or Furlough	Operator Overworked or Operator Unavailable
Operator Overworked	---	Operator is overworked and not at peak performance (errors occur)	Staffing Needs Unmet	Task Failure
Operator Unavailable	---	No operator is present to perform an essential function	Staffing Needs Unmet	Task Failure
Strike or Furlough	Spontaneous Event	Workers strike or are furloughed and are unavailable	Political Factors	Staffing Needs Unmet
Cherry Pick Loads	Spontaneous Event	Certain specified loads are able to be handled by the system while others are not	Inability of grid to handle all loads (capacity)	Insufficient Backup Plans/Capabilities
Natural Disaster	Spontaneous Event	Blizzard, hurricane, tornado, earthquake among others	Environmental Factors	Control Systems Unavailable or Insufficient Backup Plans/Capabilities
Cyber Attack	Spontaneous Event	Hostile entity penetrates network and executes cyber attack	Inability to meet Information Assurance requirements, “unknown	Internal Comms Disruption or Unauthorized Access

			unknowns," system compromised	

Table A-2 provides additional information about each potential intervention strategy in the SPIDERS Phase 2 Cause-Effect Mapping Diagram.

Table A-2. Description of Potential Intervention Strategies in SPIDERS Phase 2 Cause-Effect Mapping Diagram.

Perturbation	Description	Strategy
Insufficient Backup Plans/ Capabilities	Plans or redundant systems are not in place to backup major system functions	Put appropriate, effective backup plans and capabilities (redundant software, components) in place
Control Systems Malfunction	Changes are made to control systems so that they no longer function properly or function maliciously	Ensure the robustness of essential control systems software and components
Internal Comms Disruption	Internal communications systems cease to function properly	Ensure that a secure protocol is being used to handle internal communications
Unauthorized Access	Attackers gain access to parts of system requiring administrative privileges (also includes access to passwords and critical data)	Put strong encryption infrastructure in place and ensure that administrative functions are protected using strong passwords
Data or Software	Attackers make changes	Put strong encryption

Tampering	to existing data or software	infrastructure in place and ensure that administrative functions are protected using strong passwords
Uncontrolled Network Traffic	Attackers make changes that flood the network with traffic	Put measures in place to troubleshoot or shut down the system given a steep increase in network traffic
Lack of Service Level Agreement	Policies do not exist permitting the infrastructure of the unavailable microgrid to connect to the commercial grid	Put appropriate policies in place governing the specifics of connecting the microgrid to the commercial grid in times of need

APPENDIX B: SUPPLY CHAIN PILOT APPLICATION

Table B-1 provides additional information about each perturbation in the Supply Chain Pilot Application Cause-Effect Mapping Diagram.

Table B-1. Description of Perturbations in Supply Chain Pilot Application Cause-Effect Mapping Diagram.

Perturbation	Type	Description	Causes	Effects
Components Not Delivered	Terminal Event	Supply Chain is unable to ensure the delivery of components	Transportation Not Available, Supplier Chooses Not to Deliver Components	Unable to execute mission (provide secure, reliable components)
Damaged Components	Terminal Event	Supply Chain is unable to ensure the delivery of intact components	Components Physically Damaged, Components Poor Quality	Unable to execute mission (provide secure, reliable components)
Compromised Components	Terminal Event	Supply Chain is unable to ensure the delivery of components with integrity	Physical Component Substitution, Malicious Insertion, Component Tampering	Unable to execute mission (provide secure, reliable components)
Transportation Unavailable	---	Transportation is unavailable to move parts and materials from one location to another	Air/Train/Truck/ Boat Travel Unavailable	Components Not Delivered
Supplier Chooses Not to Deliver Components	---	A supplier chooses not to deliver poor quality components	Components Poor Quality	Components Not Delivered
Components Physically Damaged	---	Components are damaged during shipping	Components Inadequately Packaged	Damaged Components
Components Poor Quality	---	Components are of low quality and fail more quickly/often	Sub-par Material Substitution	Damaged Components

Physical Component Substitution	---	Original components are replaced with other components of unknown origin and quality	Unauthorized Access	Compromised Components
Component Tampering	---	Attackers make changes to existing data or software	Unauthorized Access	Compromised Components
Air/Train/Truck/ Boat Travel Unavailable	---	Method of travel is unavailable	Pilots/Engineers/ Drivers/Captains Unavailable, Transportation Network Disruption, Planes/Trains/ Trucks/Ships Unavailable	Transportation Unavailable
Components Inadequately Packaged	---	Components are not packaged for shipping as securely as possible	Overworked Employees, Decreased Packaging Budget	Components Physically Damaged
Sub-par Material Substitution	---	Original materials are unknowingly replaced with alternate materials of lesser quality	Supplier Cost-Cutting, Raw Materials Unavailable	Components Poor Quality
Unauthorized Access	---	Attackers gain access to parts of system (physical or virtual) requiring administrative privileges (also includes access to passwords and critical data)	Weak Security Controls	Physical Component Substitution, Component Tampering
Pilots/Engineers/ Drivers/Captains Unavailable	---	Personnel unavailable to operate various modes of	Personnel Voluntarily Unavailable, Personnel	Air/Train/Truck/ Boat Travel Unavailable

		transportation	Involuntarily Unavailable	
Transportation Network Disruption	---	Transportation is disrupted due to external factors, such as an Air Traffic Control outage or a bridge being washed away during a storm	Natural Disaster, Cyber Attack	Air/Train/Truck/ Boat Travel Unavailable
Planes/Trains/ Trucks/Ships Unavailable	---	Physical vehicles for transportation unavailable	Natural Disaster, Economic Factors	Air/Train/Truck/ Boat Travel Unavailable
Overworked Employees	---	Employees are overworked and not at peak performance	Labor Unavailable	Components Inadequately Packaged
Decreased Packaging Budget	---	Packaging budget is cut leading to the use of less or lower quality shipping materials	Supplier Cost-Cutting	Components Inadequately Packaged
Weak Security Controls	---	Physical and virtual security controls are easily able to be overcome or compromised	Little or No Investment in Security Controls, Cyber Attack	Unauthorized Access
Personnel Voluntarily Unavailable	---	Workers choose not to work	Strike or Furlough	Pilots/Engineers/ Drivers/Captains Unavailable
Personnel Involuntarily Unavailable	---	Workers cannot get to work	Natural Disaster	Pilots/Engineers Drivers/Captains Unavailable
Labor Unavailable	---	Not enough employees to fulfill tasking (also works unable to be replaced by next shift)	Strike or Furlough	Overworked Employees
Supplier Cost-Cutting	---	Supplier cuts costs in order to	Economic Factors	Decreased Packaging

		stay competitive		Budget, Sub-par Material Substitution
Raw Materials Unavailable	---	Raw materials necessary for part production are unavailable	Natural Disaster, Trade Policy Restriction, Increased Demand Restriction, Resource Reallocation Policy	Sub-par Material Substitution
Little or No Investment in Security Controls	---	Lack of investment in physical or virtual security measures, from security guards and locks to proper encryption	Economic Factors	Weak Security Controls
Strike or Furlough	---	Workers strike or are furloughed and are unavailable	Political Factors	Personnel Voluntarily Unavailable, Labor Unavailable
Economic Factors	Spontaneous Event	Market factors affect a company's economic circumstances or profitability	Market Factors, Inflation, Increased Prices	Planes/Trains/ Trucks/Ships Unavailable, Supplier Cost-Cutting, Little or No Investment in Security Controls
Cyber Attack	Spontaneous Event	Hostile entity penetrates network and executes cyber attack	Inability to meet Information Assurance requirements, "unknown unknowns," system compromised	Transportation Network Disruption, Weak Security Controls
Natural Disaster	Spontaneous Event	Blizzard, hurricane, tornado, earthquake	Environmental Factors	Transportation Network Disruption, Personnel

		among others		Involuntarily Unavailable, Planes/Trains/ Trucks/Ships Unavailable, Raw Materials Unavailable
Trade Policy Restriction	Spontaneous Event	Trade-related policy changes impact the system	Political Factors	Raw Materials Unavailable
Increased Demand Restriction	Spontaneous Event	Increased demand of a material or product impacts price, other factors	Political Factors	Raw Materials Unavailable
Resource Reallocation Policy	Spontaneous Event	New policy regulates the amount of a material able to be mined or produced	Environmental Factors, Political Factors	Raw Materials Unavailable

Table B-2 provides additional information about potential intervention strategies in the Supply Chain Pilot Application Cause-Effect Mapping Diagram.

Table B-2. Description of Potential Intervention Strategies in Supply Chain Pilot Application Cause-Effect Mapping Diagram.

Perturbation	Description	Strategy
Air/Train/Truck/Boat Travel Unavailable	Travel is unavailable regardless of mode of transportation	Strategic reserves of components and potential for 3-D printing of temporary replacement parts
Overworked Employees	Employees are overworked due to labor shortages	Policies to prevent employees from becoming overworked, potential automation of tasks
Raw Materials Unavailable	Raw materials are unavailable due to various force majeure, policy, and	Strategic reserves and studies on potential replacement materials

	economic/resource reasons	
Components Poor Quality	Components are of inferior quality and prone to failure	Use of lean initiatives to catch quality problems earlier in the design and manufacturing process
Weak Security Controls	No or few security controls are in place to prevent physical or virtual security compromises	Implementation of more robust security controls (physical or virtual, in the areas of avoidance, transference, migration, and acceptance), ideally at low cost
Unauthorized Access	No or few security controls are in place to prevent unwanted physical or virtual access to assets	Implementation of more robust access protection (physical or virtual, e.g., pop-up barriers and firewalls), special attention to administrative privileges (e.g., who has access and level of authentication)

APPENDIX C: CEM INTERVENTION PLACEMENT EXPERIMENT MATERIALS

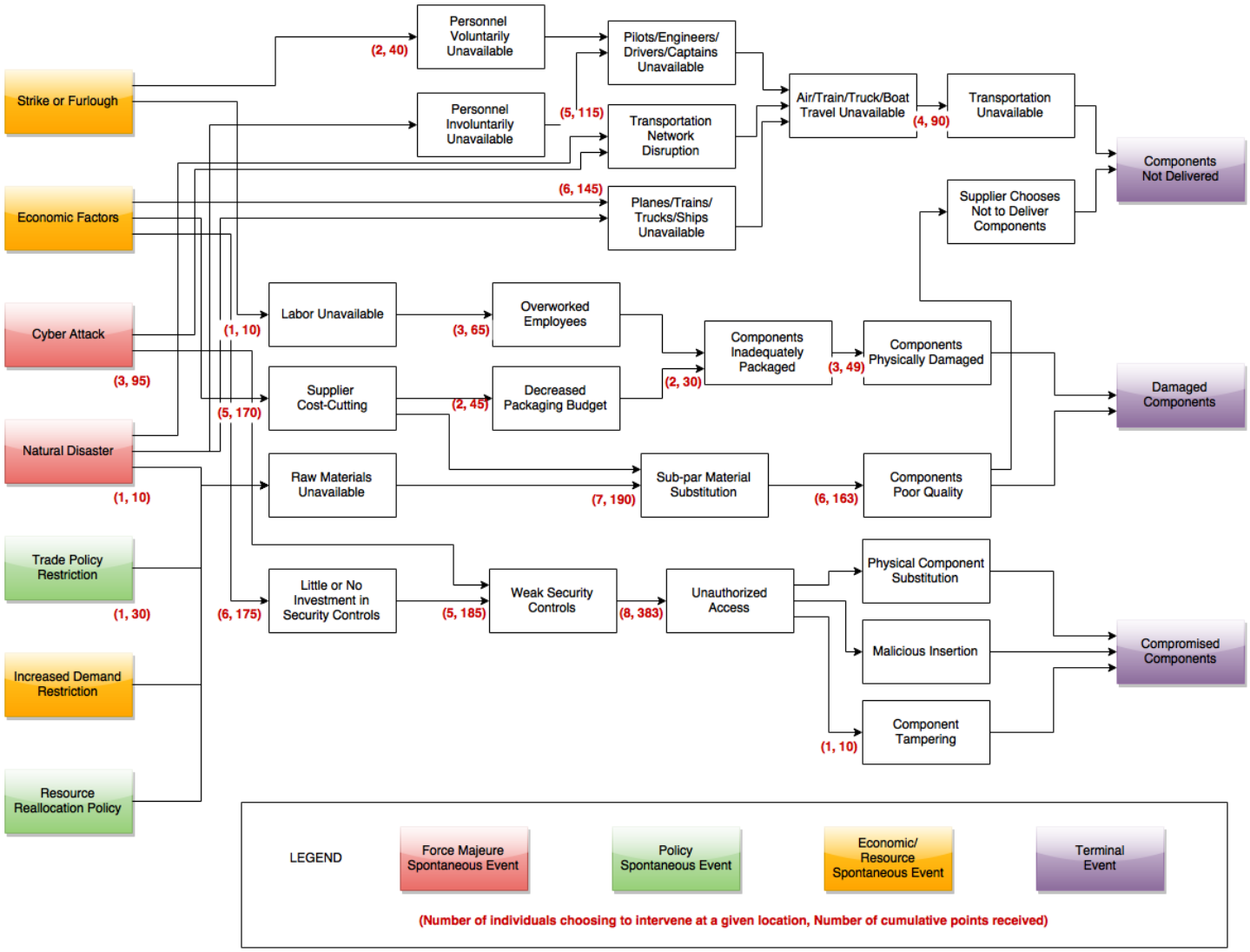


Figure C-1. Cause-Effect Mapping Diagram with Cumulative Intervention Placement Experiment Data.

Table C-1. CEM Intervention Placement Experiment Responses.

Name	Response
R.C.	What can you actually influence versus what you can't? Tackled the low-hanging fruit. Higher upstream would cost a lot more investment. Unauthorized access – swipe access. If this costs this much more units than this intervention, what can we do right now to lessen the impacts of some of these things? Unauthorized access, can beef up security systems, doesn't completely eliminate threat but reduces it more or less immediately. In terms of damaged components, can't do anything about the labor or raw materials, but can switch suppliers. What can you control and how easy is it to do? Interventions never a sure thing, but reduces chances.
S.M.	Had a mix of strategies already mentioned. Looked at three end results – tradeoff between what I can control and what I really cannot control. Thinking of myself as an industry person, thinking about components not delivered, I can put money in it but it is not so much in my control when things go wrong. Did not focus on this branch. Focused on other two branches. Looked more upstream because if something goes wrong upstream, will percolate downstream. Good quality product but doesn't reach on time – can still satisfy consumer (customer?) somehow versus giving them something damaged or broken or with a security threat. Harder to justify and have to spend more money cleaning this up later. So I put my money more on investing in security controls, making sure the quality was of good product, so you put enough money in the materials, and making sure employees are happy because then they won't make a bad product. Undamaged (damaged?) components and compromised components were a bigger problem for me, more in my control/justifiable to a customer. Based on my values, I feel product quality is most important, so what can we do early on so does not percolate downstream.
A.C.	Long-term problems; worth it to invest in security for good, or don't want to deteriorate supplier/personnel relationship. What an industry official can actually act on. Not much we can do about transportation network disruption. Seeing this diagram, I would still be unsure that the root causes have been accurately identified. I feel you can always find a cause you can influence if you go back up the causal chain. Interventions – nothing is sure: just reducing!
A.R.	Cyber policy is essentially where you can easily intervene. Places where you cannot intervene – people going on strike. Depends on what you feel you can prevent and what you feel you can't prevent. Damaged components – packaging – have time to fix this. Transparency – why aren't controls in place in the first place? Could lead to a lot of finger pointing.
P.V.	Similar potential investments upstream that would prevent multiple links from occurring, such as preventing impacts from cyber attack. A single investment downstream that prevented failure from multiple initial sources, such as subpar material substitution impact. I didn't really do much for natural disasters. Looking for malicious agents (defense – cyber attack) in system because pose a more direct threat. We can make investments upstream – two links coming out of that – similar investments allow us to prevent multiple downstream failures in all three areas, specifically cyber threat,

	transportation network disruption. Downstream on other end – where can I make investments near the end that could potentially stop a failure from potential multiple starting points – components poor quality. Focused more on components compromised or damaged versus not delivered – if I wasn't considering implementability of solution, would focus on four links stopping everything going from the left to the right (can isolate along four links). Could cut with four links and prevent everything.
H.G.	I tended to want to intervene earlier in the process in the hopes that preventing problems early on would eliminate later issues, although maybe that reasoning is false because you might not be able to prevent things higher up. I also thought there needed to be interventions in each of the three branches because these are three distinct problems and this is necessary to have the best possible system. Can't do anything about labor. Interventions are just reducing, can't ensure anything.
B.K.	The first thing that I did was look at what is the worst possible thing that could happen. In my mind, components not delivered, not a huge issue, the liability is on my supplier. Damaged components are a pain, again, not a huge issue because the liability is on my supplier. Compromised components, a lot of liability is immediately put on me. So that is the worst thing that can possibly happen. So I went to the critical node in the whole supply chain and figured if I can take out that one node, then I can take out that entire issue. So I put 60% of my units on solving the critical node in that chain, and hopefully that will solve that issue. I didn't want to commit my entire resources to that one issue, since there are other issues. Then I looked at what is the next worst thing that can happen. Damaged components are a pain, but assuming I am working on contract with my supplier, the liability of the cost is on them. Components not delivered, that is more of a pain to me. So I wanted to try to find a critical node in that supply chain. It seemed that the issues that were most prevalent were strike or furlough, economic, or natural disaster. There's not really much you can do to prevent against a natural disaster, so I want to look primarily at economic factors and strike or furlough. So I split the rest of my resources evenly between those two to solve that problem with components not delivered. It still was not clear that solving things upstream would keep any of the downstream things from happening, so I'm not sure that I would actually break the connections or attack the actual boxes. I'm not necessarily convinced that solving one of the upstream boxes would correct for one of the downstream boxes, so I assumed that it would based on the structure of it, but I don't think that it actually would for a lot of these issues. Just looking at the cyber issues, since that is my domain, I can do these things even having these things solved.
E.G.	Initially, I would want to try to target things earlier on, just because the sooner you can fix things the less cost it will be. But, with this limited amount of resources I wanted to get the most bang for my buck, and by targeting the places with only one arrow, I could make a cut in the causal chain just at that one place. Where, if I did things earlier on, I would have been fixing one tiny piece, but I still would have been very liable to problems in different chains. So, I chose to make the cuts further on even though it would be more expensive probably, but I saw that as being the most efficient use of those resources. My general strategy was to mitigate the occurrence of all three negative events. Wanted to allocate the biggest portion of my resources to stopping compromised components failure. If components not delivered or components damaged, I know what

	my problem is and then I can go forward and fix it from there. If my components are compromised and I don't know it, then I won't be fixing the problem once it has occurred. I wanted to target this specific place right before unauthorized access because that ensures that it cuts off the rest of the chain to compromised components. Then, my next highest allocation of resource was right before the components of poor quality, and I put more towards that because cutting off that link, components of poor quality feeds into both damaged components and components not delivered, so by focusing on that, I felt like I was able to impact more. The next two were components physically damaged and transportation unavailable, they both feed into only one problem so didn't want to put as much emphasis on those but still both a place where I could make one single cut and still have a pretty big impact.
R.S.	Attack all the problems given lack of data. Decided to spread money across three different end goals. Planes, trucks, trains unavailable seems like a very capital-intensive problem. I was thinking if we could find something to do with transportation network disruption – if we can somehow improve the efficiency of the network through cheaper means instead of investing money on trucks or ships – invest money on transportation network disruption. Second thing – human resources, overworked employees. Land, labor, capital – the three things for a production function. I thought labor is quite important, so I gave it 25 units. Decreased packaging – if a product is already made and just because of packaging or something else it is getting damaged, it is an easy problem to solve, but even though it looks small, it could have a bigger effect. So I will spend some money on that. Sub-par material substitution – chose this because materials are important. Spent a little money on security, no tampering of components. Preventing wrongdoing from taking place. I didn't really have a lot of thorough investigation to do this, this is just my first impression. I have been working on transportation, I was somewhat neutral about other things. Personnel available or unavailable, things like that, I didn't really feel like intervening there.
G.G.	I wasn't sure of the context specifically, may have been more civilian supply chain, but I saw this from a military perspective. That puts a sway on things, since you won't have a strike or a furlough really in the military. When I saw the left side things, I started to eliminate the ones I had little control over. Strike and furlough I didn't think would be too much of an effect, thinking military or difficult to control if you had the opportunity (civilian side). Natural disasters, I decided that there is little control over. Good to consider, but in terms of allotting resources somewhere, I wouldn't really highlight that as a high ROI spot. The same can be said for trade policy, increased demand restriction, and resource reallocation policy, any large policies like this, that are larger than your specific supply chain, I didn't really feel like in the position I was imagining myself, I wouldn't have much control over. So, what is there of concern: one, is definitely the cyber attack stuff. This is an issue that has been brought up in cyber cases, specifically again with the military stuff. When we are sourcing a lot of our components from overseas, there is a concern that we are going to buy things – say we have closed circuit TVs for security and they all come from China – maybe we can test them, but maybe they are also programmed when flashed with a certain pattern of lasers, to stop working. That's bad, and I don't think there's very much thought at all put into that sort of thing, but it is an area that I think we can target, could use more funding, and could become a large problem. Natural disasters are a known problem, but the cyber attack stuff is very

	unknown and in my mind a problem. Even just at the beginning here, the first leg of that, I crossed it out and said that malicious insertion and component tampering being the largest potential negative aspects. The last thing, economic factors and supplier cost cutting, this is constrained a lot and so then you see people with sub-par materials and then sub-par equipment, it's the lowest bidder thing, and that's frustrating for people in that line of work.
K.M.	I looked at the terminal events first and decided to focus on compromised components, since further down the line these may cause the most problems and you may not know they are compromised. Then, I went as far up the chain as I could and chose between little or no investment in security controls and weak security controls because I think there are policies that you can implement there to prevent that chain from happening. I would put 100% of my interventions there.
J.M.	I chose all of them based on the weighted amount that is going into it. So I assumed that every single line was equal, and every single accident was equal. So I sketched it out, roughly 33% went to the component compromises, these were shared, so I broke them out to 16, 16, 33, 35. I don't believe that this will do anything, though, to prevent the hazards.
C.R.	I liked downstream approach but I didn't do that. I thought upstream is better because will have more effect downstream and you will get more bang for your buck. I was trying to focus on what you can actually control, what is not as subjective. So I thought that strikes – you can't tell people to go on strike, natural disasters similarly. So I thought cyber attack and trade policy – maybe you can do some effective lobbying – maybe there and a lot of wheeling and dealing to keep your trade alive. Cyber attacks there is a lot of technical stuff you can do, so I thought those were more objective. Focus on what is preventable (less related to humans, more in control). This is hard! A lot seems unpredictable, and there is a lot you can't actually prevent or do much about. Interventions reduce (lobbying, cyber technology prevention).
S.L.	I was looking for where the chains bottlenecked so that I could disrupt the greatest number of causal chains at each spot. I tried to allocate the amount of effort that we had evenly between the three impacts at the end of the chain. It's a complex picture, if you can reduce the complexity, essentially reduce the number of possible air (?) chains, it will be easier to make the decisions as to where you allocate resources to prevent errors. Reducing complexity would improve intervention options. Interventions reduce chance of system impact.
C.W.	Chose the arrow after weak security controls, sub-par material substitution, and air/train/truck/boat travel unavailable to focus my energy on solely for the reason that the unit after each of these has more linkages coming out of it or going into it. So I thought that was a pretty critical path due to the number of linkages. So I gave the ones with three 40 points, and I gave the ones with two 20 points. I took a look at the diagram and went with my gut. Interventions reduce chances.
P.L.	The metrics I used were the places where the problem could be easily solved by

	throwing money at it, and also places where it seemed like it would cause a lot of issues. So I focused first on the compromised components, because that seemed like probably the worst outcome, because you might not necessarily know they are compromised, who knows what's in there, this seemed like the worst outcome. Little or no investment in security controls seemed like, well if you invest in security controls, you could have a really large impact on this bad outcome. Then, I looked at the stuff that would lead to transportation being unavailable or the components being physically damaged, and it looked like it would be super easy to have some long-term contracts for planes, trucks, etc., so throwing a little bit of money at that would be an easy way to solve the problem, hopefully. And then for the materials substitution and inadequate packaging, those seem like things you could specify in a contract you will provide this standard of packaging, this standard of checking that the materials are not substituted, willing to pay a premium for that. This should be an easy way to make your money to actually have an impact. Where stuff like overworked employees or personnel being involuntarily unavailable is much fuzzier with respect to the relationship between your money and the impact.
N.N.	I chose four different areas to split the 100 points, into 20, 10, 50, and 20. They were at the very beginning, cyber attack and natural disasters, mostly. I put 20% at the very beginning of cyber attacks, 10% at natural disasters and those links, 50% at supplier cost-cutting, since I know that these lengths go to/link to every type of component failure, like it not being delivered, or a damaged component, or a compromised component. A lot of the supplier cost-cutting can come from something like cyber attack, economic factors, and can lead to disruptions in the network or substituting sub-par materials and other things. I put 20% for little or no investment in security controls, and that's because I know cyber issues are a really big thing today in all fields of study. There is a lot of research going on in how do you make the security for this better? What kind of systems do you need in place in order to do that? I think that there is always innovation that can happen with security controls for different scenarios of attacks, and so I think, even though that mostly leads to compromised components, I think that's still a huge factor. I also am not exactly sure what the breakdown the DoD has seen with components not delivered versus damaged components versus compromised components, but I think these four areas cover the supply chain of all three. The one thing I didn't take into account is what are the costs. I know the costs might be smaller potentially if you investigate something towards the end of the supply chain, something that most directly impacts something not being delivered or damaged or compromised, where there could be a lot more research going into the very beginning and throughout the whole supply chain, saying where would the failure be in this whole supply chain. I think, fundamentally, looking at these sort of root causes, would be more beneficial than saying this was something very close to the end of the supply chain.
A.T.	I didn't want to go for one place but distributed, and went across the whole system. But when I started reading about it, I focused in the central part of it. For instance, transportation network disruption – probably because I spent the whole last week reading about different disasters – Haiti for a homework and then Ecuador and what happened in Japan – right now, this seems important. Same with the planes and trains and ships unavailable – seems like the supply chain, part of it, just physically moving different parts, should play about a third. I joked about it, but labor unavailable – that could be a big reason. I'm not sure if it would just be due to strike, or if it would be

	another one of those disasters. Cyber attack has been coming up in the news recently, just the concerns with the digitalization of everything, it may be something to look at. Labor unavailable, and supply cost-cutting, I had seen those cases back in Russia – you start delivering a product, and halfway through, you buy the product and it's great, but only as soon as this product appears, due to corruption or whatever is happening behind, people just start cutting the cost and that is very, very probable and similar to the sub-par materials substitution, to which I allocated 40 points. I also wanted to not leave out this whole chain of compromised components. I think the investment there should be done upfront, mainly because when it comes to matters of security and IT, it is something that can actually be created without mistakes, it's not like you're digging a metro line where there is something or some artifact that you could have not predicted. You could conceive a system such that there are few errors if you do it well enough in advance. For me, the best places are to intervene up front.
M.N.	I put 50% of resources with cyber attack linking to weak security controls because it is something you can directly work on and eliminate. You have full control on it, at least if you dedicate the resources. You could completely eliminate it, as compared to something like a policy solution, where a lot of other factors are involved, or a natural disaster, where you can't even control. The next 40% is with the economic factors, with planes/trains/ships not being available. Again, a higher level of control, and if you are able to put in the resources, you are able to get all of the transportation network in place, and you want to make sure you always have your components. The remaining 10% is for natural disaster, for example, if you have something that needs to be there, you need to assess the risk of a disaster happening and dedicate a bit of resources for those one-time scenarios, those one-off like a flood, and make sure you have an alternate method of transportation available to get to the place that you want, at the time that you want. I don’t think interventions are a sure thing, I think depending on the factors, some are more sure than the others. But, I would view them all as reducing chances. Even with cyber, which I thought was the most sure you could fix, you never know who could come up with a new or different protocol and make the system tough again. You have to continuously be on the hook for new changes that are happening in the system.
S.B.	I've never looked at a system like this, and I'm sure these wouldn't be my final choices. But not having seen something like this before, I looked at which boxes had the most links coming out of them, since I knew that money could be spread to remediate different effects, not just one arrow in, one arrow out, since some links have two arrows in, two arrows out. I chose the few boxes I saw that had a couple of links going out, the poor component quality, unauthorized access, and supplier cost-cutting, and I weighted the supplier cost-cutting a little higher. I did 40, 30, 30. So I did supplier cost-cutting as 40, since it is earlier in the chain, and then the two 30s because they were later in the chain. I think if I spent more time learning about these factors, I probably would have weighted differently and maybe distributed a little more, but this is my first thought, to maximize the money we use in places that it will be directed to more than one place. I wanted to know how effective, the chance of the money being effective is, how to quantify some of this stuff. It looks like components poor quality, what are the chances of being successful if I invest, what is my ROI, and I think it will vary and sometimes you can't even know. Having more numbers to decide where the trade-off should be

	would be helpful. But again, I've never seen something like this, so this is what my first impressions of making this choice was.

REFERENCES

Adger, W. N. (2006). Vulnerability. *Global Environmental Change*, *16*, 268–281.

Aerospace Industries Association of America, Inc. (2011). *Counterfeit Parts: Increasing Awareness and Developing Countermeasures*. Arlington, VA. Retrieved from http://www.aia-aerospace.org/assets/counterfeit-web11.pdf

Albino, V., & Garavelli, A. C. (1995). A methodology for the vulnerability analysis of just-in-time production systems. *International Journal of Production Economics*, *41*(1–3), 71–80. http://doi.org/10.1016/0925-5273(95)00014-3

Antón, P. S., Anderson, R. H., Mesic, R., & Scheiern, M. (2004). *Finding and Fixing Vulnerabilities in Information Systems: The Vulnerability Assessment and Mitigation Methodology*. Retrieved from http://www.jstor.org/stable/10.7249/mr1601darpa

Asbjørnslett, B. E. (2009). Assessing the Vulnerability of Supply Chains. In G. A. Zsidisin & B. Ritchie (Eds.), *Supply Chain Risk* (pp. 15–33). Springer US. Retrieved from http://link.springer.com/chapter/10.1007/978-0-387-79934-6_2

Assante, M. (2014, November 11). America's Critical Infrastructure Is Vulnerable To Cyber Attacks. Retrieved from http://www.forbes.com/sites/realspin/2014/11/11/americas-critical-infrastructure-is-vulnerable-to-cyber-attacks/

Aven, T. (2007). A unified framework for risk and vulnerability analysis covering both safety and security. *Reliability Engineering & System Safety*, *92*(6), 745–754. http://doi.org/10.1016/j.ress.2006.03.008

Aven, T. (2011). On Some Recent Definitions and Analysis Frameworks for Risk, Vulnerability, and Resilience, *31*(4). http://doi.org/10.1111/j.1539-6924.2010.01528.x

Babers, C. (2015). *The Enterprise Architecture Sourcebook, Volume 1, Second Edition*. Lulu.com.

Bakshi, N., & Kleindorfer, P. (2009). Co-opetition and Investment for Supply-Chain Resilience. *Production and Operations Management*, *18*(6), 583–603. http://doi.org/10.3401

Baldwin, K. J. (2014, August). *Complexity: Driver of Systems Engineering Reflecting on Defense Strategic Guidance*. Presented at the NDIA SE Division Meeting. Retrieved from http://www.acq.osd.mil/se/briefs/2014_08_20_Baldwin-NDIA-SED-Complex-Sys-Final-2.pdf

Baldwin, K., Popick, P. R., Miller, J. F., & Goodnight, J. (2012). The United States Department of Defense revitalization of system security engineering through program protection. In *2012 IEEE International Systems Conference SysCon 2012* (pp. 1–7). http://doi.org/10.1109/SysCon.2012.6189463

Barnes, J. C. (2001). *A Guide to Business Continuity Planning*. Chichester: Wiley. Retrieved from http://pqm-online.com/assets/files/lib/books/barnes.pdf

Barnes, P., & Oloruntoba, R. (2005). Assurance of security in maritime supply chains: Conceptual issues of vulnerability and crisis management. *Journal of International Management*, *11*(4), 519–540. http://doi.org/10.1016/j.intman.2005.09.008

Bar-Yam, Y. (1997). *Dynamics of Complex Systems*. Westview Press.

Becker, J., Beverungen, D. F., & Knackstedt, R. (2009). The challenge of conceptual modeling for product–service systems: status-quo and perspectives for reference models and modeling languages. *Information Systems and E-Business Management*, *8*(1), 33–66. http://doi.org/10.1007/s10257-008-0108-y

Blackhurst, J., Craighead, C., Elkins, D., & Handfield, R. (2005). An empirically derived agenda of critical research issues for managing supply-chain disruptions. *INTERNATIONAL JOURNAL OF PRODUCTION RESEARCH*, *43*(19), 4067–4081.

Boccaletti, S., Latora, V., Moreno, Y., Chavez, M., & Hwang, D.-U. (2006). Complex Networks: Structure and Dynamics. *Physics Reports*, *424*, 175–308.

Bodeau, D. J., & Graubart, R. (2011). *Cyber Resiliency Engineering Framework* (No. MTR110237). Bedford, MA: MITRE. Retrieved from https://www.mitre.org/sites/default/files/pdf/11_4436.pdf

Bodeau, D. J., Graubart, R., LaPadula, L., Kertzner, P., Rosenthal, A., & Brennan, J. (2012). *Cyber Resiliency Metrics, Version 1.0, Rev. 1* (No. MP120053, Rev. 1). Bedford, MA: MITRE. Retrieved from https://register.mitre.org/sr/12_2226.pdf

Bodner, D. A. (2014). Enterprise Modeling Framework for Counterfeit Parts in Defense Systems. *Procedia Computer Science*, *36*, 425–431.

Bodner, D. A. (2015). Mitigating Counterfeit Part Intrusions with Enterprise Simulation. *Procedia Computer Science*, *61*, 233–239.

Bora, S., Lim, G. J., Biobaku, T. O., Cho, J., & Parsaei, H. R. (2014). Assessing the Resiliency and Importance of a Supply Chain Network. In *CIE44 & IMSS'14 Proceedings* (pp. 1530–1540). Istanbul, Turkey. Retrieved from http://e2map.egr.uh.edu/sites/e2map/files/files/publications/imss14-cie44-400-fullpapers.pdf

Boyens, J., Paulsen, C., Moorthy, R., & Bartol, N. (2015). *Supply Chain Risk Management Practices for Federal Information Systems and Organizations. NIST Special Publication 800-161*. Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf

Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). *Introducing OCTAVE Allegro : Improving the Information Security Risk Assessment Process* (No. CMU/SEI-2007-TR-012).

Carbone, T. A., & Tippett, D. D. (2004). Project Risk Management Using the Project Risk FMEA. *Engineering Management Journal*, *16*(4), 28–35. http://doi.org/10.1080/10429247.2004.11415263

Centre for Logistics and Supply Chain Management at the Cranfield School of Management. (2003). *Understanding Supply Chain Risk: A Self-Assessment Workbook* (pp. 1–54). Cranfield, Bedford, UK: Cranfield University. Retrieved from http://hdl.handle.net/1826/4373

Christopher, M. (1998). *Logistics and Supply Chain Management: Strategies for Reducing Cost and Improving Service*. Financial Times/Pitman.

Christopher, M., & Lee, H. (2004). Mitigating supply chain risk through improved confidence. *International Journal of Physical Distribution & Logistics Management*, *34*(5), 388–396. http://doi.org/10.1108/09600030410545436

Christopher, M., & Peck, H. (2004). Building the Resilient Supply Chain. *The International Journal of Logistics Management*, *15*(2), 1–14.

Committee on Armed Services, United States Senate. (2012). *Inquiry Into Counterfeit Electronic Parts in the Department of Defense Supply Chain* (No. 112–167). Retrieved from http://www.armed-services.senate.gov/imo/media/doc/Counterfeit-Electronic-Parts.pdf

Committee on Risk Assessment of Hazardous Air Pollutants, Board on Environmental Studies and Toxicology, Commission on Life Sciences, National Research Council. (1994).

Science and Judgment in Risk Assessment. Washington, D.C.: National Academies Press. Retrieved from http://www.nap.edu/catalog/2125

Committee on the Institutional Means for Assessment of Risks to Public Health, Commission on Life Sciences, National Research Council. (1983). *Risk Assessment in the Federal Government: Managing the Process*. Washington, D.C.: National Academies Press. Retrieved from http://www.nap.edu/catalog/366

Covington & Burling LLP. (2014, May 9). DoD Releases Final DFARS Rule for the Detection and Avoidance of Counterfeit Electronic Parts. Retrieved March 19, 2016, from https://www.cov.com/-/media/files/corporate/publications/2014/05/dod_releases_final_dfars_rule_for_the_detection_and_avoidance_of_counterfeit_electronic_parts.pdf

Cranfield University School of Management. (2002). *Supply Chain Vulnerability: Executive Report*. Cranfield, Bedford, UK: Cranfield University. Retrieved from http://www.som.cranfield.ac.uk/som/dinamic-content/research/lscm/downloads/Vulnerability_report.pdf

Criado, R., Flores, J., Hernández-Bermejo, B., Pello, J., & Romance, M. (2005). Effective measurement of network vulnerability under random and intentional attacks. *Journal of Mathematical Modelling and Algorithms*, *4*(3), 307–316. http://doi.org/10.1007/s10852-005-9006-1

Criado, R., Pello, J., Romance, M., & Vela-Pérez, M. (2007). Structural analysis and optimality of vulnerability and efficiency in artificial networks. *New Trends and Tools in Complex Networks*, 31.

Defense Advanced Research Projects Agency. (n.d.). Supply Chain Hardware Integrity for Electronics Defense (SHIELD). Retrieved April 24, 2016, from http://www.darpa.mil/program/supply-chain-hardware-integrity-for-electronics-defense

Department of Defense, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics. (2005). *Report of the Defense Science Board Task Force on High Performance Microchip Supply*. Retrieved from http://www.acq.osd.mil/dsb/reports/ADA435563.pdf

Department of Defense, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics. (2014). *Department of Defense Assured Microelectronics Policy* (No. Senate Report 113-85). Retrieved from http://www.acq.osd.mil/se/docs/DoD-Assured-Microelectronics-Policy-RTC-July2014.pdf

Deputy Assistant Secretary of Defense for Systems Engineering, & Department of Defense Chief Information Officer. (2014). *Trusted Systems and Networks (TSN) Analysis*. Washington, D.C.: U.S. Department of Defense. Retrieved from http://www.acq.osd.mil/se/docs/Trusted-Systems-and-Networks-TSN-Analysis.pdf

Ericson, C. (1999). Fault Tree Analysis – A History Clifton A. Ericson II The Boeing Company; Seattle, Washington, 1–9.

Estrada, E. (2006). Network Robustness to Targeted Attacks: The Interplay of Expansibility and Degree Distribution. *The European Physical Journal B*, *52*, 563–574.

Eusgeld, I., Kröger, W., Sansavini, G., Schläpfer, M., & Zio, E. (2009). The role of network theory and object-oriented modeling within a framework for the vulnerability analysis of critical infrastructures. *Reliability Engineering & System Safety*, *94*(5), 954–963. http://doi.org/10.1016/j.ress.2008.10.011

Farahani, R. Z., Asgari, N., & Davarzani, H. (2009). *Supply Chain and Logistics in National, International and Governmental Environment: Concepts and Models*. Springer Science & Business Media.

Federal Aviation Administration. (2000). *FAA System Safety Handbook, Chapter 9: Analysis Techniques*. Retrieved from https://www.faa.gov/regulations_policies/handbooks_manuals/aviation/risk_management/ss_handbook/media/Chap9_1200.pdf

Federal Aviation Administration. (2004, October). Research and Development Accomplishments FY 2004. Retrieved March 21, 2016, from https://www.faa.gov/about/office_org/headquarters_offices/ast/about/media/032504.pdf

Federal Register. (2014, May 6). Defense Federal Acquisition Regulation Supplement: Detection and Avoidance of Counterfeit Electronic Parts (DFARS Case 2012-D055). Retrieved March 19, 2016, from https://www.federalregister.gov/articles/2014/05/06/2014-10326/defense-federal-acquisition-regulation-supplement-detection-and-avoidance-of-counterfeit-electronic

Fenelon, P., McDermid, J. A., Nicholson, M., & Pumfrey, D. J. (1994). *Towards Integrated Safety Analysis and Design*. High Integrity Systems Engineering Group, Department of Computer Science: University of York.

Fenz, S., Ekelhart, A., & Neubauer, T. (2011). Information Security Risk Management: In Which Security Solutions Is It Worth Investing? *Communications of the Association for Information Systems*, *28*(1). Retrieved from http://aisel.aisnet.org/cais/vol28/iss1/22

FMEA - FMECA. (2006). RPN - FMEA Risk Priority Number. Retrieved May 8, 2016, from http://www.fmea-fmeca.com/fmea-rpn.html

Foreman, P. (2009). *Vulnerability Management*. CRC Press.

Forum of Incident Response and Security Teams. (2015, June 10). Common Vulnerability Scoring System (CVSS-SIG). Retrieved May 7, 2016, from https://www.first.org/cvss

Francis, R., & Bekera, B. (2014). A metric and frameworks for resilience analysis of engineered and infrastructure systems. *Reliability Engineering and System Safety*, *121*, 90–103. http://doi.org/10.1016/j.ress.2013.07.004

Frigault, M., & Wang, L. (2008). Measuring network security using bayesian network-based attack graphs. *Proceedings - International Computer Software and Applications Conference*, 698–703. http://doi.org/10.1109/COMPSAC.2008.88

Gansler, J. S., Lucyshyn, W., & Rigilano, J. (2014). *Addressing Counterfeit Parts In The DoD Supply Chain* (No. UMD-LM-14-012). Center for Public Policy and Private Enterprise, School of Public Policy: University of Maryland. Retrieved from http://www.cpppe.umd.edu/publications/addressing-counterfeit-parts-dod-supply-chain

Glade, T. (2003). Vulnerability Assessment in Landslide Risk Analysis. *DIE ERDE*, *134*(2), 123–146.

Government Accountability Office. (2010a). *Defense Supplier Base: DOD Should Leverage Ongoing Initiatives in Developing Its Program to Mitigate Risk of Counterfeit Parts* (No. GAO-10-389). Retrieved from http://www.gao.gov/products/GAO-10-389

Government Accountability Office. (2010b). *Intellectual Property: Observations on Efforts to Quantify the Economic Effects of Counterfeit and Pirated Goods* (No. GAO-10-423). Retrieved from http://www.gao.gov/products/GAO-10-423

Government Accountability Office. (2014). *Critical Infrastructure Protection: DHS Action Needed to Enhance Integration and Coordination of Vulnerability Assessment Efforts* (No. GAO-14-507).

Government Accountability Office. (2015). *Defense Infrastructure: Improvements in DOD Reporting and Cybersecurity Implementation Needed to Enhance Utility Resilience Planning* (No. GAO-15-749). Retrieved from http://www.gao.gov/products/GAO-15-749

Government Accountability Office. (2015). *High-Risk Series: An Update* (No. GAO-15-290). Retrieved from http://www.gao.gov/assets/670/668415.pdf

Government Accountability Office. (2015). *Trusted Defense Microelectronics: Future Access and Capabilities are Uncertain* (No. GAO-16-185T). Retrieved from http://www.gao.gov/assets/680/673401.pdf

Government Accountability Office. (2016a). *Counterfeit Parts: DOD Needs to Improve Reporting and Oversight to Reduce Supply Chain Risk* (No. GAO-16-236). Retrieved from http://www.gao.gov/assets/680/675227.pdf

Government Accountability Office. (2016b). *Defense Infrastructure: Energy Conservation Investment Program Needs Improved Reporting, Measurement, and Guidance* (No. GAO-16-162). Retrieved from http://www.gao.gov/products/GAO-16-162

Haimes, Y. Y. (2006). On the Definition of Vulnerabilities in Measuring Risks to Infrastructures, *26*(2), 293–296. http://doi.org/10.1111/j.1539-6924.2006.00755.x

Haines, D. (2013, April). *SM05: Risk Analysis: A Comparison in Quantifying Asset Values, Threats, Vulnerabilities and Risk.* Retrieved from http://www.iscwest.com/rna/rna_iscwest_v2/docs/2013/conference-materials/sm05_risk_analysis.pdf?v=635018173433178174

Hamid, T., & Al-Jumeily, D. (2015). A dynamic cost-centric risk impact metrics development. In *2015 International Conference on Systems, Signals and Image Processing (IWSSIP)* (pp. 277–281). http://doi.org/10.1109/IWSSIP.2015.7314230

Hampl, V. (2010). *FMEA and FTA.* Retrieved from http://lrss.fri.uni-lj.si/sl/teaching/rzd/tutorials/hampl2010_FMEA-FTA.pdf

Hanneman, R. A., & Riddle, M. (2005). *Introduction to Social Network Methods*. Retrieved from http://faculty.ucr.edu/~hanneman/nettext/

Heise, D. R. (1975). *Causal analysis*. Wiley.

Hennet, J.-C., Mercantini, J.-M., & Demongodin, I. (2008). Toward an Integration of Risk Analysis in Supply Chain Assessment (pp. 255–260). Presented at the Proceedings of I3M-EMSS. Retrieved from http://www.lsis.org/hennetjc/PUBLIS/EMSS_08.pdf

Hibshi, H., Breaux, T., Riaz, M., & Williams, L. (2015). *Discovering Decision-Making Patterns for Security Novices and Experts* (No. CMU-ISR-15-101). Institute for Software Research, School of Computer Science: Carnegie Mellon University. Retrieved from http://www.cs.cmu.edu/~hhibshi/pdf/HBR15.pdf

Hoddinott, J., & Quisumbing, A. (2003). Methods for Microeconometric Risk and Vulnerability Assessments. *Food Policy*, (324), 134–134. http://doi.org/10.2139/ssrn.1281055

Hofmann, M., Kjølle, G. H., & Gjerde, O. (2012). Development of Indicators to Monitor Vulnerabilities in Power Systems. Presented at the PSAM 11 and ESREL 2012 Conference on Probabilistic Safey Assessment.

Inter-Agency Network on Education Simulation Models. (2008, September 7). What is a generic model? Retrieved May 2, 2016, from http://inesm.education.unesco.org/en/faq/what-a-generic-model

Inter-American Development Bank. (n.d.). The Prevalent Vulnerability Index (PVI). Retrieved April 15, 2016, from http://www.iadb.org/exr/disaster/idea_pvi.pdf

International Customer Management Institute. (n.d.). Leading & Lagging Indicators. Retrieved March 23, 2016, from http://www.icmi.com/files/ICMILeading_LaggingIndicatorsExplained.pdf

ISO/IEC/IEEE. (2015, May 15). ISO/IEC/IEEE 15288:2015 - Systems and software engineering -- System life cycle processes. Retrieved April 5, 2016, from http://www.iso.org/iso/catalogue_detail?csnumber=63711

Jaquith, A. (2007). *Security Metrics: Replacing Fear, Uncertainty, and Doubt*. Pearson Education.

Jin, W.-X., Song, P., Liu, G.-Z., & Stanley, H. E. (2015). The cascading vulnerability of the directed and weighted network. *Physica A: Statistical Mechanics and Its Applications*, *427*, 302–325. http://doi.org/10.1016/j.physa.2015.02.035

Johansson, J., & Hassel, H. (2010). An approach for modelling interdependent infrastructures in the context of vulnerability analysis. *Reliability Engineering and System Safety*, *95*(12), 1335–1344. http://doi.org/10.1016/j.ress.2010.06.010

Johansson, J., & Hassel, H. (2012). Comparison of vulnerability and reliability analysis of technical infrastructures. *Advances in Safety, Reliability and Risk Management - Proceedings of the European Safety and Reliability Conference, ESREL 2011*, 2465–2473.

Jung, K., Lim, Y., & Oh, J. (2011). A Model for Measuring Supplier Risk: Do Operational Capability Indicators Enhance the Prediction Accuracy of Supplier Risk? *British Journal of Management*, *22*(4), 609–627. http://doi.org/10.1111/j.1467-8551.2010.00697.x

Jüttner, U., Peck, H., & Christopher, M. (2003). Supply Chain Risk Management: Outlining an Agenda for Future Research. *International Journal of Logistics: Research & Applications*, *6*(4), 197–210.

Keselman, Y., & Dickinson, S. (2005). Generic Model Abstraction from Examples. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *27*(7). Retrieved from http://www.cs.toronto.edu/~sven/Papers/pami-abstraction.pdf

Khaitan, S., & Raheja, S. (2011). Finding Optimal Attack Path Using Attack Graphs: A Survey. *International Journal of Soft Computing and Engineering (IJSCE)*, *1*(3), 33–36.

Knemeyer, a. M., Zinn, W., & Eroglu, C. (2009). Proactive planning for catastrophic events in supply chains. *Journal of Operations Management*, *27*(2), 141–153. http://doi.org/10.1016/j.jom.2008.06.002

Koh, A. (2015). *Defending Against Cyber Security Threats to the Payment and Banking Systems*. Presented at the NYU Leonard N. Stern School of Business Master of Science Risk Management Risk Management Symposium. Retrieved from http://www.stern.nyu.edu/sites/default/files/assets/documents/Andrew%20Koh%20Presentation_New%20York_V1.2%20(1)(1).pdf

Koonce, A. M., Apostolakis, G. E., & Cook, B. K. (2008). Bulk power risk analysis: Ranking infrastructure elements according to their risk significance. *Electrical Power and Energy Systems*, *30*, 169–183.

Kröger, W., & Zio, E. (2011). *Vulnerable Systems*. London: Springer London. Retrieved from http://link.springer.com/10.1007/978-0-85729-655-9

Kumpula, J. M., Saramaki, J., Kaski, K., & Kertesz, J. (2007). Limited resolution and multiresolution methods in complex network community detection. *arXiv:0706.2230 [Physics]*, 660116-660116–8. http://doi.org/10.1117/12.725560

Langford, J. W. (1995). *Logistics: Principles and Applications*. McGraw-Hill.

Latora, V., & Marchiori, M. (2005). Vulnerability and protection of infrastructure networks. *Physical Review E - Statistical, Nonlinear, and Soft Matter Physics*, *71*(1), 1–4. http://doi.org/10.1103/PhysRevE.71.015103

Ledermüller, T., & Clarke, N. L. (2011). Risk Assessment for Mobile Devices. In *Proceedings of the 8th International Conference on Trust, Privacy and Security in Digital Business* (pp. 210–221). Berlin, Heidelberg: Springer-Verlag. Retrieved from http://dl.acm.org/citation.cfm?id=2035420.2035445

Lee, M. S. (2012). Resilient Cyber Architectures Keep Government IT Operations Mission-Ready. *The MITRE Corporation*. Retrieved from http://www.mitre.org/publications/project-stories/resilient-cyber-architectures-keep-government-it-operations-missionready

LeSaint, J., Popick, P., & Reed, M. (2015). System Security Engineering Vulnerability Assessments for Mission-Critical Systems and Functions (pp. 608–613). Presented at the Systems Conference (SysCon), 2015 9th Annual IEEE International, Vancouver, BC.

Leveson, N. (2011). *Engineering a Safer World: Systems Thinking Applied to Safety*. MIT Press.

Leveson, N. (2015). A systems approach to risk management through leading safety indicators. *Reliability Engineering & System Safety*, *136*, 17–34. http://doi.org/10.1016/j.ress.2014.10.008

Leveson, N. G. (2013). *An STPA Primer* (No. Version 1). Cambridge, Massachusetts: Massachusetts Institute of Technology. Retrieved from http://sunnyday.mit.edu/STPA-Primer-v0.pdf

Liu, Y., & Man, H. (2005). Network vulnerability assessment using Bayesian networks (Vol. 5812, pp. 61–71). http://doi.org/10.1117/12.604240

Livingston, H. (2007). Avoiding Counterfeit Electronic Components. *Components and Packaging Technologies, IEEE Transactions on*, *30*(1), 187–189. http://doi.org/10.1109/TCAPT.2007.893682

Lowis, L., & Accorsi, R. (2011). Vulnerability Analysis in SOA-Based Business Processes. *IEEE Transactions on Services Computing*, *4*(3), 230–242. http://doi.org/10.1109/TSC.2010.37

McDermott, T., Rouse, W., Goodman, S., & Loper, M. (2013). Multi-level Modeling of Complex Socio-Technical Systems. *Procedia Computer Science*, *16*, 1132–1141. http://doi.org/10.1016/j.procs.2013.01.119

McDuffee, A. (2014, February 26). DARPA Developing Tech to Detect Counterfeit Microchips in Military Gear. Retrieved April 24, 2016, from http://www.wired.com/2014/02/darpa-counterfeit-shield/

McFadden, F. E., & Arnold, R. D. (2010). Supply chain risk mitigation for IT electronics. In *2010 IEEE International Conference on Technologies for Homeland Security (HST)* (pp. 49–55). http://doi.org/10.1109/THS.2010.5655094

McGrath, M. F., LaBerge, W. B., Bement, Jr., A. L., DeMayo, R. P., Denman, G. L., Heim, J. A., … Yudken, J. S. (2002). *Equipping Tomorrow's Military Force: Integration of Commercial and Military Manufacturing in 2010 and Beyond*. Washington, D.C.: Board

on Manufacturing and Engineering Design, National Research Council, National Academies Press.

Mead, N. (2006). *Requirements Elicitation Case Studies Using IBIS , JAD , and ARM*. Software Engineering Institute: Carnegie Mellon University. Retrieved from https://resources.sei.cmu.edu/asset_files/WhitePaper/2013_019_001_297234.pdf

Mead, N. R., Hough, E. D., & Stehney II, T. R. (2005). *Security Quality Requirements Engineering (SQUARE) Methodology* (No. CMU/SEI-2005-TR-009). Pittsburgh, Pennsylvania: Carnegie Mellon University - Software Engineering Institute. Retrieved from http://www.sei.cmu.edu/reports/05tr009.pdf

Mekdeci, B. (2013, February 1). *Managing the Impact of Change Through Survivability and Pliability to Achieve Viable Systems of Systems*. Massachusetts Institute of Technology.

Mekdeci, B., Ross, A. M., Rhodes, D. H., & Hastings, D. E. (2012). A taxonomy of perturbations: Determining the ways that systems lose value. In *Systems Conference (SysCon), 2012 6th Annual IEEE International* (pp. 1–6). http://doi.org/10.1109/SysCon.2012.6189487

Melnyk, S. A., Stewart, D. M., & Swink, M. (2004). Metrics and performance measurement in operations management: dealing with the metrics maze. *Journal of Operations Management*, *22*(3), 209–218. http://doi.org/10.1016/j.jom.2004.01.004

Meshel, D. C. (2014, May). *Counterfeit Parts Prevention Strategy Guide Product Overview*. Retrieved from http://www.aerospace.org/wp-content/uploads/2015/04/TOR-2014-02161-Counterfeit-Parts-Prevention-Strategy-Guide-Product-Overview.pdf

Misra, V., Harmon, D., & Bar-yam, Y. (2010). Vulnerability Analysis of High Dimensional Complex Systems, 560–572.

MITRE. (2013). *Cyber Mission Assurance Engineering: A Risk-Based, Threat-Informed Approach to Address Advanced Adversaries*. Retrieved from https://www.mitre.org/sites/default/files/publications/cyber-mae.pdf

MITRE. (2015). EABOK | Knowledge Areas | Developing an EA. Retrieved May 2, 2016, from http://www.eabok.org/developing_an_ea/index.html

Moore, D. A. (2006). Application of the API/NPRA SVA methodology to transportation security issues. *Journal of Hazardous Materials*, *130*(1–2), 107–121. http://doi.org/10.1016/j.jhazmat.2005.07.042

Murino, T., Romano, E., & Santillo, L. C. (2011). Supply Chain Performance Sustainability Through Resilience Function. In *Proceedings of the Winter Simulation Conference* (pp. 1605–1616). Phoenix, Arizona: Winter Simulation Conference. Retrieved from http://dl.acm.org/citation.cfm?id=2431518.2431707

Neureuther, B. D., & Kenyon, G. (2009). Mitigating Supply Chain Vulnerability. *Journal of Marketing Channels*, *16*(3), 245–263. http://doi.org/10.1080/10466690902934532

Northcutt, S. (2009, September 1). Security Controls. Retrieved May 8, 2016, from http://www.sans.edu/research/security-laboratory/article/security-controls

Nowakowski, T., & Werbińska-Wojciechowska, S. (2014). Problems of Logistic Systems Vulnerability and Resilience Assessment. In P. Golinska (Ed.), *Logistics Operations, Supply Chain Management and Sustainability* (pp. 171–186). Springer International Publishing. Retrieved from http://link.springer.com/chapter/10.1007/978-3-319-07287-6_12

Nowakowski, T., Werbińska-Wojciechowska, S., & Chlebus, M. (2015). Supply chain vulnerability assessment methods—possibilities and limitations. Presented at the

European Safety and Reliability Conference ESREL, Zurich, Switzerland. http://doi.org/10.1201/b19094-217

Nykamp, D. Q. (n.d.). The Degree Distribution of a Network. Retrieved May 9, 2016, from http://mathinsight.org/degree_distribution

Ou, X., & Singhal, A. (2012). *Quantitative Security Risk Assessment of Enterprise Networks*. New York: Springer. Retrieved from http://download.springer.com/static/pdf/172/bok%253A978-1-4614-1860-3.pdf?originUrl=http%3A%2F%2Flink.springer.com%2Fbook%2F10.1007%2F978-1-4614-1860-3&token2=exp=1462659943~acl=%2Fstatic%2Fpdf%2F172%2Fbok%25253A978-1-4614-1860-3.pdf%3ForiginUrl%3Dhttp%253A%252F%252Flink.springer.com%252Fbook%252F10.1007%252F978-1-4614-1860-3*~hmac=60cd63d49386494459493928a85b5644b0d71640fba1862b05ed61cc07c8e138

Pajk, D., Indihar-Štemberger, M., & Kovačič, A. (2012). Reference model design: An approach and its application. In *Proceedings of the ITI 2012 34th International Conference on Information Technology Interfaces (ITI)* (pp. 455–460). http://doi.org/10.2498/iti.2012.0419

Park, H., Clear, T., Rouse, W. B., Basole, R. C., Braunstein, M. L., Brigham, K. L., & Cunningham, L. (2012). Multilevel Simulations of Health Delivery Systems: A Prospective Tool for Policy, Strategy, Planning, and Management. *Serv. Sci.*, *4*(3), 253–268. http://doi.org/10.1287/serv.1120.0022

Parlier, G. (2011). *Transforming US Army Supply Chains: Strategies for Management Innovation*. Business Expert Press.

Peck, G., & Beam, R. (2005). A Closer Look at Frameworks and Reference Models. *BPTrends*. Retrieved from http://www.bptrends.com/publicationfiles/07-05%20ART%20Closer%20Look%20at%20Frameworks%20-%20Peck%20-%20Beam1.pdf

Peck, H. (2005). Drivers of supply chain vulnerability: an integrated framework. *International Journal of Physical Distribution & Logistics Management*, *35*(4), 210–232. http://doi.org/10.1108/09600030510599904

Peck, H. (2006). Reconciling supply chain vulnerability, risk and supply chain management. *International Journal of Logistics: Research & Applications*, *9*(2), 127.

Penzenstadler, B., & Femmer, H. (2013). A Generic Model for Sustainability with Process- and Product-specific Instances. In *Proceedings of the 2013 Workshop on Green in/by Software Engineering* (pp. 3–8). New York, NY, USA: ACM. http://doi.org/10.1145/2451605.2451609

Pettit, T. J., Fiksel, J., & Croxton, K. L. (2010). Ensuring Supply Chain Resilience: Development of a Conceptual Framework. *Journal of Business Logistics*, *31*(1), 1–21. http://doi.org/10.1002/j.2158-1592.2010.tb00125.x

Plenert, G., Makharia, M., & Sambukumar, R. (2012). *Supply Chain Vulnerability in Times of Disaster*. WIPRO Consulting Services. Retrieved from http://www.wipro.com/documents/resource-center/Supply_Chain_Vulnerability_in_Times_of_Disaster.pdf

Popick, P. R., & Reed, M. (2013). Requirements Challenges in Addressing Malicious Supply Chain Threats. *What's Inside*, *16*(2), 223–223.

Pressman, R. S. (2005). *Software Engineering: A Practitioner's Approach*. Palgrave Macmillan.

Pressman, R. S. (2009). *Chapter 2: Process Models*. Retrieved from http://www.biology.emory.edu/research/Prinz/Cengiz/cs540-485-FA12/slides/ch02.pdf

Process: Knowledge and Decisions Group, Department of Information Systems, University of Haifa. (n.d.). Generic Process Model (GPM). Retrieved May 2, 2016, from http://mis.hevra.haifa.ac.il/~morpeleg/PKD/GPM.html

Rasmussen, J. (1997). Risk management in a dynamic society: a modelling problem. *Safety Science*, *27*(2–3), 183–213. http://doi.org/10.1016/S0925-7535(97)00052-0

Rebovich, G., Dahmann, J., & Turner, G. (2014). *An Actionable Framework for System of Systems and Mission Area Security Engineering*. Presented at the Systems Conference (SysCon), 2014 8th Annual IEEE International. Retrieved from http://www.dtic.mil/ndia/2013system/W16077_Rebovich.pdf

Reed, M. (2012, October). *System Security Engineering and Program Protection Case Study for the Materiel Solution Analysis Phase Tutorial*. Presented at the 15th Annual NDIA Systems Engineering Conference, San Diego, CA. Retrieved from http://www.acq.osd.mil/se/briefs/14762-2012_10_22-NDIA-SEC-Reed-PP-Tutorial.pdf

Reed, M. (2012, October). *System Security Engineering and Program Protection Case Study for the Materiel Solution Analysis Phase Tutorial: Exercise Exemplars*. Presented at the 15th Annual NDIA Systems Engineering Conference, San Diego, CA. Retrieved from http://www.acq.osd.mil/se/briefs/14762-2012_10_22-NDIA-SEC-Reed-PP-Tutorial-Exercise-Exemplars.pdf

Reed, M. (2012, October). *System Security Engineering and Program Protection Case Study for the Materiel Solution Analysis Phase Tutorial: Exercises*. Presented at the 15th Annual NDIA Systems Engineering Conference, San Diego, CA. Retrieved from http://www.acq.osd.mil/se/briefs/14762-2012_10_22-NDIA-SEC-Reed-PP-Tutorial-Exercise-hdouts-Approved.pdf

Reed, M. (2014a, October). *System Security Engineering and Program Protection Integration into SE Ensuring Confidence in Defense Systems*. Presented at the 17th Annual NDIA Systems Engineering Conference, Springfield, VA. Retrieved from http://www.acq.osd.mil/se/briefs/16994-2014_10_29-NDIA-SEC-Reed-SSE-PP-vF.pdf

Reed, M. (2014b, October). *Vulnerability Analysis Techniques to Support Trusted Systems and Networks (TSN) Analysis Office of the Deputy Assistant Secretary of Defense What Are We Protecting?* Presented at the 17th Annual NDIA Systems Engineering Conference, Springfield, VA. Retrieved from http://www.acq.osd.mil/se/briefs/16997-2014_10_29-NDIA-SEC_Reed-VulnerabilityAnalysis-vF.pdf

Reed, M. (2015, October). *System Security Engineering for Program Protection and Cybersecurity Ensuring Confidence in Defense Systems*. Presented at the 18th Annual NDIA Systems Engineering Conference, Springfield, VA. Retrieved from http://www.acq.osd.mil/se/briefs/2015_10_27_NDIA18-SSE-PP-Reed.pdf

Restrepo, J. G., Ott, E., & Hunt, B. R. (2006). Emergence of coherence in complex networks of heterogeneous dynamical systems. *Physical Review Letters*, *96*(25), 254103.

Restrepo, J. G., Ott, E., & Hunt, B. R. (2007). Approximating the largest eigenvalue of network adjacency matrices. *Physical Review E*, *76*(5), 56119. http://doi.org/10.1103/PhysRevE.76.056119

Rice Jr, J. B., & Caniato, F. (2003). Building a secure and resilient supply network. *Supply Chain Management Review*, *7*(5), 22–30.

Richards, M. G. (2009, June). *Multi-Attribute Tradespace Exploration for Survivability*. Massachusetts Institute of Technology.

Rocco, C. M., & Ramirez-Marquez, J. E. (2013). Identification of top contributors to system vulnerability via an ordinal optimization based method. *Reliability Engineering and System Safety*, *114*, 92–98. http://doi.org/10.1016/j.ress.2013.01.003

Rocco, S. C. M., Ramirez-Marquez, J. E., & Salazar, A. D. E. (2012). Some metrics for assessing the vulnerability of complex networks: An application to an electric power system. *Advances in Safety, Reliability and Risk Management - Proceedings of the European Safety and Reliability Conference, ESREL 2011*, 2556–2561.

Ross, R., Oren, J. C., & McEvilley, M. (2014). *Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems* (No. DRAFT SP 800-160). National Institute of Standards and Technology. Retrieved from http://csrc.nist.gov/publications/drafts/800-160/sp800_160_draft.pdf

Rouse, W. B., & Bodner, D. A. (2013). *Multi-Level Modeling of Complex Socio-Technical Systems – Phase 1* (No. SERC-2013-TR-020-2). Systems Engineering Research Center. Retrieved from www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA608173

Rovito, S. M., & Rhodes, D. H. (2016). Enabling Better Supply Chain Decisions Through a Generic Model Utilizing Cause-Effect Mapping (pp. 1–7). Presented at the Systems Conference (SysCon), 2016 10th Annual IEEE International.

SAE International. (2009, April 2). Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition, SAE AS5553. Retrieved March 19, 2016, from http://standards.sae.org/as5553/

SAE International. (n.d.). AS6301 (WIP) Compliance Verification Criterion Standard for SAE AS6081, Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition – Distributors - SAE International. Retrieved April 23, 2016, from http://standards.sae.org/wip/as6301/

Sakli, L., Hennet, J.-C., & Mercantini, J.-M. (2014). An Analysis of Risk and Vulnerabilities in Supply Networks. *Preprints of the 19th World Congress, The International Federation of Automatic Control*. Retrieved from http://www.nt.ntnu.no/users/skoge/prost/proceedings/ifac2014/media/files/2045.pdf

Samaras, C., & Willis, H. H. (2013). Capabilities-Based Planning for Energy Security at Department of Defense Installations [Product Page]. Retrieved March 21, 2016, from http://www.rand.org/pubs/research_reports/RR162.html

Sandia National Laboratories. (2015, May 11). SPIDERS. Retrieved from http://energy.sandia.gov/energy/ssrei/gridmod/resilient-electric-infrastructures/military/spiders-2/

Sarewitz, D., Pielke, R., & Keykhah, M. (2003). Vulnerability and risk: some thoughts from a public policy perspective. *Risk Analysis*, *23*(4), 805–810.

Savage, M. (2002). Business continuity planning. *Work Study*, *51*(5), 254–261. http://doi.org/10.1108/00438020210437277

Schnaubelt, C. M., Larson, E. V., & Boyer, M. E. (2014). *Vulnerability Assessment Method Pocket Guide: A Tool for Center of Gravity Analysis*. Santa Monica, CA: RAND Corporation. Retrieved from http://www.rand.org/content/dam/rand/pubs/tools/TL100/TL129/RAND_TL129.pdf

Shanahan, R. (2014, October). *Trusted Microelectronics*. Presented at the 17th Annual NDIA Systems Engineering Conference, Springfield, VA. Retrieved from http://www.acq.osd.mil/se/briefs/16990-2014_10_29-NDIA-SEC-Shanahan-vF.pdf

Sheffi, Y. (2007). *The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage*. MIT Press.

Sheffi, Y., Rice, J. B., Fleck, J. M., & Caniato, F. (2003). Supply Chain Response to Global Terrorism : A Situation Scan The context of the research Research background, 1–6.

Sheffi, Y., & Rice Jr., J. B. (2005). A Supply Chain View of the Resilient Enterprise. *MIT Sloan Management Review*, *47*(1), 41–48.

Singhal, A., & Ou, X. (2011). *Security Risk Analysis of Enterprise Networks Using Probabilistic Attack Graphs* (No. NIST Interagency Report 7788). Gaithersburg, MD: National Institute of Standards and Technology. Retrieved from http://csrc.nist.gov/publications/nistir/ir7788/NISTIR-7788.pdf

Stecke, K. E., & Kumar, S. (2009). Sources of Supply Chain Disruptions, Factors That Breed Vulnerability, and Mitigating Strategies. *Journal of Marketing Channels*, *16*(3), 193–226. http://doi.org/10.1080/10466690902932551

Steen, R., & Aven, T. (2011). A risk perspective suitable for resilience engineering. *Safety Science*, *49*(2), 292–297.

Sterlacchini, S. (2011). Vulnerability Assessment : concepts , definitions and methods.

Stiles, P. M. (2002, May 15). Demystifying Supply Chain Management. Retrieved from http://mthink.com/article/demystifying-supply-chain-management/

Svensson, G. (2002). A conceptual framework of vulnerability in firms' inbound and outbound logistics flows. *International Journal of Physical Distribution & Logistics Management*, *32*(2), 110–134. http://doi.org/10.1108/09600030210421723

Tehranipoor, M. (Mohammad), Guin, U., & Forte, D. (2015). *Counterfeit Integrated Circuits*. Switzerland: Springer International Publishing.

Teknomo, K. (2015). Graph Theory Tutorial: Degree. Retrieved May 9, 2016, from http://people.revoledu.com/kardi/tutorial/GraphTheory/Degree.html

Travelers. (2016). Business Continuity Planning in 4 Steps. Retrieved April 13, 2016, from https://www.travelers.com/resources/business-continuity/business-continuity-planning-in-4-steps.aspx

Trend Micro. (2015, March 18). The importance of vulnerability research: Recent findings. Retrieved April 7, 2016, from http://blog.trendmicro.com/the-importance-of-vulnerability-research-recent-findings/

United States Code. Sarbanes-Oxley Act of 2002, Codified in Sections 11, 15, 18, 28, and 29 USC 116 Stat 745 (2002). Retrieved from https://www.gpo.gov/fdsys/pkg/PLAW-107publ204/pdf/PLAW-107publ204.pdf

United States Committee on Armed Services. (2012, May 21). Senate Armed Services Committee Releases Report on Counterfeit Electronic Parts | United States Commitee on Armed Services. Retrieved April 6, 2016, from http://www.armed-services.senate.gov/press-releases/senate-armed-services-committee-releases-report-on-counterfeit-electronic-parts

U.S. Congress. (2013, December). National Defense Authorization Act for Fiscal Year 2014: Legislative Text and Joint Explanatory Statement to Accompany H.R. 3304, Public Law 113-66. Retrieved March 19, 2016, from https://www.gpo.gov/fdsys/pkg/CPRT-113HPRT86280/pdf/CPRT-113HPRT86280.pdf

U.S. Congress. Carl Levin and Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. Public Law 113-291 (2014). Retrieved from https://www.gpo.gov/fdsys/pkg/CPRT-113HPRT92738/pdf/CPRT-113HPRT92738.pdf

U.S. Congress. National Defense Authorization Act for Fiscal Year 2016, Pub. L. No. Public Law 114-92 (2015). Retrieved from https://www.congress.gov/114/plaws/publ92/PLAW-114publ92.pdf

U.S. Department of Commerce. (2010, January). Defense Industrial Base Assessment: Counterfeit Electronics. Retrieved March 19, 2016, from https://www.bis.doc.gov/index.php/forms-documents/doc_view/37-defense-industrial-base-assessment-of-counterfeit-electronics-2010

U.S. Department of Commerce National Institute of Standards and Technology. (2012). *Guide for Conducting Risk Assessments* (No. SP 800-30). Computer Security Division, Information Technology Laboratory: National Institute of Standards and Technology. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

U.S. Department of Defense. (2012). *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)* (Instruction No. DoDI 5200.44). Retrieved from http://www.dtic.mil/whs/directives/corres/pdf/520044p.pdf

U.S. Department of Homeland Security. (2008). *DHS Risk Lexicon*. Retrieved from https://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf

U.S. Department of Homeland Security. (2010). *DHS Risk Lexicon*. Retrieved from https://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf

Van de Voort, M., Willis, H., Ortiz, D., & Martonosi, S. (2007). Applying Risk Assessment To Secure The Containerized Supply Chain. In I. Linkov, R. J. Wenning, & G. A. Kiker (Eds.), *Managing Critical Infrastructure Risks* (pp. 79–95). Springer Netherlands. Retrieved from http://link.springer.com/chapter/10.1007/978-1-4020-6385-5_5

Vlajic, J. V., van Lokven, S. W. M., Haijema, R., & van der Vorst, J. G. A. J. (2013). Using vulnerability performance indicators to attain food supply chain robustness. *Production Planning & Control*, *24*(8–9), 785–799. http://doi.org/10.1080/09537287.2012.666869

Wagner, S. M., & Bode, C. (2009). Dominant Risks and Risk Management Practices in Supply Chains. In G. A. Zsidisin & B. Ritchie (Eds.), *Supply Chain Risk* (pp. 271–290). Springer US. Retrieved from http://link.springer.com/chapter/10.1007/978-0-387-79934-6_17

Wagner, S. M., & Neshat, N. (2012). A comparison of supply chain vulnerability indices for different categories of firms. *International Journal of Production Research*, *50*(11), 2877–2891. http://doi.org/10.1080/00207543.2011.561540

Wang, L., Islam, T., Long, T., Singhal, A., & Jajodia, S. (2008). An Attack Graph-Based Probabilistic Security Metric. In V. Atluri (Ed.), *Data and Applications Security XXII* (pp. 283–296). Springer Berlin Heidelberg. Retrieved from http://link.springer.com/chapter/10.1007/978-3-540-70567-3_22

Waters, D. (2011). *Supply Chain Risk Management: Vulnerability and Resilience in Logistics*. Kogan Page Publishers.

Westrum, R. (2006). A Typology of Resilience Situations. In *Resilience Engineering: Concepts and Precepts*.

Willis, H. H. (2006). *Analyzing Terrorism Risk* (No. CT-265). RAND Corporation. Retrieved from http://www.rand.org/content/dam/rand/pubs/testimonies/2006/RAND_CT265.pdf

Wynn, J., Whitmore, J., Upton, G., Spriggs, L., McKinnon, D., McInnes, R., … Clausen, L. (2011). *Threat Assessment & Remediation Analysis (TARA)* (No. MTR110176). Bedford, MA: MITRE. Retrieved from https://www.mitre.org/sites/default/files/pdf/11_4982.pdf

Xie, P., Li, J. H., Ou, X., Liu, P., & Levy, R. (2010). Using Bayesian networks for cyber security analysis. In *2010 IEEE/IFIP International Conference on Dependable Systems Networks (DSN)* (pp. 211–220). http://doi.org/10.1109/DSN.2010.5544924

Yazdani, A., & Jeffrey, P. (2010). A note on measurement of network vulnerability under random and intentional attacks. *arXiv:1006.2791 [Cond-Mat, Physics:physics]*. Retrieved from http://arxiv.org/abs/1006.2791

Yin, X., Fang, Y., & Liu, Y. (2013). Real-Time Risk Assessment of Network Security Based on Attack Graphs. Atlantis Press. http://doi.org/10.2991/isca-13.2013.13

Yu, S. (2011). A Comparison of FMEA , AFMEA and FTA, 954–960.

Zafar, N. (2011). Security Quality Requirements Engineering (SQUARE) Method Evaluation : A Case Study Using Smart Grid Customer Domain By.

Zhao, L., Beverlin, B., Netoff, T., & Nykamp, D. Q. (2011). Synchronization from second order network connectivity statistics. *Frontiers in Computational Neuroscience*, *5*(28), 1–16.

Zimmerman, R. (2004). Decision-making and the vulnerability of interdependent critical infrastructure. *IEEE International Conference on Systems, Man and Cybernetics, 2004*, *5*, 4059–4063. http://doi.org/10.1109/ICSMC.2004.1401166

Zio, E., Piccinelli, R., & Sansavini, G. (2011). An all-hazard approach for the vulnerability analysis of critical infrastructures. *Proceedings of the …*, 2451–2458.

Zsidisin, G. A., Melnyk, S. A., & Ragatz, G. L. (2005). An institutional theory perspective of business continuity planning for purchasing and supply management. *International Journal of Production Research*, *43*(16), 3401–3420. http://doi.org/10.1080/00207540500095613