UNIVERSITY OF OKLAHOMA GRADUATE COLLEGE

ON DYNAMIC MANAGEMENT OF LEAD TIMES

A THESIS

SUBMITTED TO THE GRADUATE FACULTY

in partial fulfillment of the requirements for the
Degree of

MASTER OF SCIENCE

By

SAMANTHA CARPENTER

Norman, Oklahoma

2024

ON DYNAMIC MANAGEMENT OF LEAD TIMES

A THESIS APPROVED FOR THE
SCHOOL OF AEROSPACE AND MECHANICAL ENGINEERING

BY THE COMMITTEE CONSISTING OF

Dr. Farrokh Mistree, Chair

Dr. Janet K. Allen

Dr. John Klier

ACKNOWLEDGMENTS

I express my deepest gratitude to those who have supported and guided me on this journey.

To Professor Janet K. Allen and Professor Farrokh Mistree, I am profoundly thankful for the role you played in helping me secure a path in the thesis track, an opportunity that has been life changing in so many ways. Thank you for opening my eyes to new perspectives within academia, for welcoming me into the Systems Realization Laboratory community, and for your steadfast commitment to my success. Your support and belief in me have shaped my academic journey in ways I will never forget.

To Professor Farrokh Mistree, thank you for your dedication to my personal and professional growth in securing my thesis committee and providing me with a starting point for this thesis. Additionally, your guidance in AME 5303, *Designing for Open Innovation*, encouraged me to develop as both a student and an individual, and I am immensely grateful for the insights and wisdom you shared.

My heartfelt appreciation also goes to the Air Force Oklahoma City Air Logistics Complex (OC-ALC) for their sponsorship through the Long-Term Training Program. Their support has made it possible for me to pursue my Master's education and has been integral to my career journey.

To my thesis committee, Professor Farrokh Mistree, Professor Janet K. Allen, and Professor John Klier, I am deeply grateful for your dedication, insights, and expertise. Your guidance and feedback have strengthened my work and challenged me to grow as a researcher. This thesis is better because of your commitment and invaluable contributions.

I would like to extend my sincere gratitude to Dr. Ashlee Ford Versypt for introducing me to the world of research all those years ago and for being an incredible role model. Her mentorship taught me the standards of rigor, dedication, and integrity, and the experiences I shared with her have profoundly shaped my professional development. Thank you, Dr. Ford Versypt, for setting me on this path and inspiring me to pursue it with passion and purpose.

Finally, I would like to thank my leadership at the OC-ALC for their invaluable mentorship and perspective on my career. Your guidance has been instrumental to my development as an engineer, and your support has motivated me to grow and strive for excellence.

Each of you has played a key role in my journey, and I am forever grateful for your support, encouragement, and belief in my potential.

Thank you.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

Defense supply networks support the timely provision of resources in high-stakes and uniquely complex environments involving multiple stakeholders, including government entities, suppliers, and users. The unique complexity of defense supply networks stems from their role in maintaining national security, supporting military readiness, and ensuring that resources are reliably delivered under high-stakes, contested environments. These networks must also navigate conflicting goals, such as balancing cost efficiency, security, and mission readiness, while contending with unpredictable global environments. Due to these unique features, defense supply networks are typically designed to be resilient, lean, and efficient. However, resilience-based system design results in fragile networks that are vulnerable to disruptions potentially jeopardizing mission-critical operations. Since all defense supply networks operate within a landscape of both anticipated and unanticipated variations and disruptions, systems that go beyond resilience towards fail-safe must be developed. In this thesis, analyzing lead time management techniques as a feature of fail-safe system design presents a unique opportunity to identify gaps and a way forward for additional research. Identifying gaps in defense lead time management frameworks is a step towards determining principles for designing fail-safe defense supply networks.

In this context, defense supply networks designed for resilience are typically based on cyber-physical systems (CPS). CPS-based design often overlooks the social elements due to their qualitative nature. However, including social components in system design is hypothesized as more comprehensive perspective in cyber-physical-social systems (CPSS). These social components such as trust, leadership, and team cohesion are essential in modern defense contexts. In this thesis, CPSS principles are hypothesized to provide a robust perspective for

developing adaptable, fail-safe systems that incorporate both technological and social dimensions for enhanced decision-making and operational readiness.

In this thesis, a comprehensive literature review on current practices in both generalized and defense-specific supply network design is conducted with a focus on their responses to variations and disruptions. To identify constraints among stakeholders in a multi-stakeholder defense supply network, the Nested Function-Behavior-Structure Dilemma Triangle Method (F-B-S DTM) is used to develop a Requirements List based in Dilemma resolutions. Defense sustainment is further examined as a defense supply network using the Business Model Canvas to identify key network components. Next, defense sustainment as a defense supply network is analyzed using the Air Force Sustainment Center's *Art of the Possible* framework to reveal gaps in lead time management. These gaps are further explored using System Archetypes to contextualize patterns of Behavior and Structure, enabling a deeper understanding of constraints within defense supply networks.

The findings within this thesis include the hypothesis that fail-safe defense supply networks within contested logistics environments should include adaptability and robust decision-making strategies to counter disruptions. By integrating CPSS perspectives that include comprehensive human factors that include the worker and the stakeholders, defense supply networks can operate in and prepare for environments where social dynamics like trust and collaboration significantly impact operations. Designing fail-safe systems is hypothesized to require policies that shift from rigid resilience-based paradigms toward systems of flexibility, through an incorporation of real-time data, predictive analytics, and cross-functional collaboration. The way forward for policy recommendations include a design for dynamic system reconfiguration, decentralized governance, and adaptive feedback loops. These policies must include advocacy for networks that enable localized autonomy, foster public-private partnerships, and allow for effective cross-organizational collaboration among government, suppliers, and users. The way forward identified in this thesis culminated into potential research avenues for designing fail-safe systems based in satisficing decision frameworks, modular redundancy, and scalable dynamic reconfiguration strategies in a Ph.D. These research avenues include a prioritization of adaptability over strict efficiency and include supporting continuous improvement and proactive responses to complex, multidimensional threats.

GLOSSARY

E-CPSS: an adaptive network that integrates physical components, digital technologies, and human elements to respond dynamically to changing conditions (Allen, Nellippallil et al. 2023)

CPSS: cyber-physical-social system; systems of interactions between physical infrastructure, cyber capabilities (like data processing and analytics), and social factors (such as human behaviors, decisions, and cultural dynamics)

Fail-safe system: System that is agile, dynamic and capable of adapting operations to combat the impacts of variations and disruptions. Does not imply a binary of either fail-safe or non-fail-safe but rather a continuum.

Policy: A definite course or method of action selected from among alternatives and in light of given conditions to guide and determine present and future decisions (2024).

Variation: short-term changes in demand patterns or shortages. These variations can often be mitigated through adjustments or rearrangements of components within the network, ensuring continued functionality and adaptability (Cabrera, Santa et al. 2023)

Disruption: more significant impacts, often stemming from infrastructure damage or collapse (D'Souza 2017)

Fragile: a lean supply network is considered fragile because it is vulnerable to disruptions; even small disturbances, such as supply delays, demand fluctuations, or unexpected shutdowns, can lead to significant operational breakdowns due to the lack of buffers, redundancies, or alternative pathways (Rezapour, Khosrojerdi et al. 2018).

Adaptable: the ability of a system, organization, or individual to adjust effectively to new, changing, or unexpected conditions. In the context of systems and networks, adaptability implies having flexible structures, processes, or strategies that allow for rapid modification in response to variations and disruptions (Rezapour, Khosrojerdi et al. 2018).

Flexible: the capability of a system, organization, or individual to modify actions, processes, or structures easily to accommodate changing demands, requirements, or conditions. Flexibility emphasizes responsiveness and the ease with which adjustments can be made, often involving minimal resistance or structural changes (Rezapour, Khosrojerdi et al. 2018).

"The most important single ingredient

in the formula of success is

knowing how to get along with people."

- Theodore Roosevelt

26th President of the United States

CHAPTER 1: DEFENSE SUPPLY NETWORK MANAGEMENT WITHIN MULTI-STAKEHOLDER ENVIRONMENTS

Defense supply networks operate within multi-stakeholder environments that involve strategic coordination of resources, logistics, and information flows across diverse entities to meet defense readiness and national goals. Unlike traditional supply chains, defense supply networks are complex systems that must accommodate the needs and manage the constraints of various stakeholders, including government agencies, private contractors, international allies, and other public-sector entities (Rezapour, Khosrojerdi et al. 2018). These networks operate in a high-stakes context, requiring responsiveness to dynamic demands, security concerns, and evolving geopolitical factors. The interplay of different stakeholder priorities and perspectives creates unique challenges, necessitating advanced strategies that can exceed resilience to support fail-safe systems based in agility, collaboration, and responsiveness. In this thesis, the groundwork for successfully managing these networks through constraint management is proposed from a holistic approach that integrates cyber, physical, and social system components.

1.1 Background and Motivation for Incorporating Cyber-Physical-Social Systems into Supply Network Frameworks

In recent years, the integration of cyber-physical-social system (CPSS) principles into complex environments has emerged as a potential strategy for enhancing system performance and capturing accurate and authentic system dynamics in response to the complexities and uncertainties present in modern environments. Full integration of a comprehensive CPSS, cyber, physical, and social, represents a paradigm shift in supply chain and supply network management, that leverages advanced technologies to create interconnected systems that seamlessly blend and assign equal system value to digital, physical, and social elements.

Specifically, the integration of social components into traditionally cyber-physical supply network systems is proposed as strategy for increasing robustness and is a step towards fully integrated fail-safe systems (Rezapour, Khosrojerdi et al. 2018). The integration of CPSS principles into system design is driven by the growing potential benefits it offers across multiple sectors. For example, because the rapid development of new technologies increasingly changes the environment in which these systems must operate, systems must be able to adapt. System adaptation or evolution brought on by technological advancement can be charted throughout history, most notably the defined progression of manufacturing noted by Industry 1.0 through Industry 5.0 (Ivanov 2023). Industry 5.0, touted as the most recent stage of manufacturing practice, includes leveraging real-time data from interconnected sensors, devices, and human in the loop networks, and represents the first integration of a partial CPSS. This partial CPSS was incorporated to allow manufacturers to include a social aspect of the workers interacting with system components in traditional cyber-physical systems. However, while the inclusion of social components in Industry 5.0 is touted as the newest level of industry management, the social component of Industry 5.0 mainly refers to the interactions of the worker rather than a more comprehensive inclusion of the stakeholder (Wang, Yang et al. 2023). For the purposes of this work, Industry 5.0 will be considered a partial realization of a CPSS and an initial step towards fully realized CPSS in industry management systems. The gap between system and stakeholders remains.

1.1.1 Supply Network Design as a CPSS

The initial incorporation of CPSS principles into supply network design also stemmed from a need to alleviate the effects of several emerging challenges. Firstly, globalization and increased market volatility have increased the need for supply networks to be more agile and responsive to changes in customer demand, regulatory requirements, and geopolitical factors (Leffler 2022). Secondly, the proliferation of digital technologies, such as the Internet of Things (IoT), artificial intelligence (AI), and blockchain, have highlighted new opportunities to capture and analyze increasingly large amounts of data in real-time, enabling greater visibility and control over supply chain operations (Masip-Bruin, Marín-Tordera et al. 2021). Finally, the growing importance of social networks, stakeholder collaboration, and human factors has emphasized the need for supply networks to be more interconnected and collaborative, both internally and externally (Shi, Yuan et al. 2022). Defense supply networks also operate in highly dynamic and unpredictable networks, where rapid response times, mission-critical dependencies, and stringent security protocols are key. However, in the defense sector, where systems are tied to national security, strategic advancement in system performance and design is even more critical. The unique challenges and requirements present within modern defense logistics serve as a basis for this thesis which includes an analysis and critical review of the systems and frameworks used in current defense lead time management within the context of a complex multistakeholder defense supply network from the perspective of a CPSS.

By integrating CPSS principles into defense supply network design and management, it is hypothesized that defense organizations can enhance their ability to effectively manage and sustain complex logistics operations, ensuring the timely delivery of essential materiel and support services to users in the field. Additionally, the incorporation of CPSS principles is hypothesized to enable defense organizations to improve situational awareness, enhance collaboration with coalition partners and suppliers, and strengthen cybersecurity measures to safeguard sensitive information and critical infrastructure against emerging threats. This hypothesis ties into the further development of Industry 5.0 into contexts beyond manufacturing in a manner that includes both the worker and other stakeholders. As defense agencies continue to modernize their capabilities and adapt to evolving geopolitical dynamics, the incorporation of CPSS principles is hypothesized to play a pivotal role in maintaining operational readiness, robustness, and effectiveness in an increasingly interconnected and unpredictable world through the incorporation of strategic flexibility and dynamic frameworks. This infusion of flexibility into rigid and standardized systems is hypothesized to be the next step towards determining how historically rigid organizations can better respond to variation and disruption through dynamic system reconfiguration, identifying potential bottlenecks or disruptions, and proactively responding to changing market conditions or User preferences. Moreover, incorporating CPSS based design has the potential to facilitate greater collaboration and information sharing among supply network partners, potentially enabling more focused coordination of activities, faster decision-making, and improved risk management. Additionally, CPSS integration is hypothesized to allow supply networks to leverage more adaptable and robust system design in the face of disruptions. Through the use of predictive analytics, machine learning, and compromise or trade-off decision algorithms, initial CPSSs have already shown to be more able to anticipate and mitigate potential risks, strategies resource allocation, and dynamically manage supply lead times in response to changing conditions (Dong, Ranjan et al. 2015). Increased system adaptability is crucial for addressing the increasing frequency and severity of disruptions, such as natural disasters, geopolitical conflicts, or global pandemics, which can severely impact defense supply network performance and ultimate success.

Overall, the integration of CPSS principles into supply network frameworks represents a transformative approach to supply network management, offering organizations the opportunity to create more agile, dynamic, robust, and, in turn, fail-safe supply networks that can thrive in today's rapidly evolving landscape. However, realizing the full potential of CPSS requires a holistic approach that addresses not only technological challenges, but also organizational, cultural, and regulatory considerations found in complex multi-stakeholder environments. As defense organizations continue to embrace digital transformation and explore new ways to enhance their capabilities, the incorporation of CPSS design is likely to remain a key strategy for the realization of fail-safe systems.

1.1.2 Satisficing Solutions

In addition to adopting a cyber-physical-social system perspective, this thesis includes an emphasis and justification for utilizing satisficing as an approach to decision making over strict optimization to address the complexities of defense supply networks. Determining optimized solutions typically results in singular or limited solution spaces that leave little room for flexibility to respond to planned or unplanned disturbances. One approach to a particular problem solution selection is the negotiation of solutions to allow for decision flexibility without the requirement of performance maximization. These are called satisficing solutions (Brown and Sim 2009). These solutions represent a compromise among goals with an understanding that there are many solution spaces and trade-off situations that could produce a desired outcome. Pursuing a satisficing solution presents a possible avenue for making processes flexible enough to change while still establishing resilient and lean routines to maintain day-to-day efficiency (Lepori and Montauti 2020, Guo, Allen et al. 2024). Flexible but standardized decision-making is especially important in large organizations.

1.2 Defense Sustainment as a Defense Supply Network

In order to determine requirements for designing fail-safe defense supply networks, it is imperative to determine the major stakeholders within those supply networks and identify gaps in their current state of practice. One of the larger stakeholders operating within defense supply networks, made up of complex sets of systems and subsystems separate from purely logistic support organizations like the Defense Logistics Agency (DLA), is defense sustainment. While the unique features of a defense supply network are discussed in length in Section 2.3.3, framing defense sustainment as a defense supply network adds additional elements specificity. Defense sustainment at its core is the method by which an organization sustains its materiel and personnel for defense purposes (2024). The Department of Defense (DOD) specifically defines sustainment as the "provision of logistics and personnel services necessary to maintain and prolong operations through mission accomplishment and redeployment of the force" (Rowlett 2017). Defense sustainment can be separated into field-level and depot-level. For example, field-level defense sustainment often includes deployable levels of limited maintenance activities for direct organization support (2024). Field sustainment is heavily impacted by location and available resources and represents an environment with the largest potential for variability. Alternately, depot-level defense sustainment activities are often reliant on either organic facilities or private sector commercial firm infrastructures and include major maintenance, repair and overhaul (MRO) activities (2024). These organic facilities are often heavily impacted by their local environment and are responsible for the bulk, or approximately 55%, of military materiel MRO (2024). These types of MRO facilities often support large numbers of employees, many complex processes, and key infrastructure requirements based on maintenance technology and space needs. While each branch of the U.S. military requires and utilizes MRO services in both field-level and depot-level settings, depot-level U.S. Air Force sustainment as a defense supply network is the focus in this thesis. Air Force defense sustainment as a defense supply network includes the network used to maintain and support Air Force specific military equipment, infrastructure, and personnel readiness over time (AFSC 2024). More specifically, the Air Force Sustainment Centers (AFSC) includes systems of logistics, facilities, aircraft repair activities, supply chain management, and life-cycle maintenance to ensure that forces remain equipped and operational. This AFSC network is crucial to mission success and is done through a system of systems extending from facility upkeep to aircraft and equipment maintenance and logistical support across the globe. Due to the number of complex interconnected systems and the importance of ensuring timely support and defense readiness, the AFSC must manage lead times effectively. While lead time management techniques could be studied across the defense network studying the AFSC provides a unique opportunity to assess and improve defense supply network systems as its methods and frameworks are publicly available in their open-source lead-time management handbook, the *Art of the Possible* (AoP). This document includes detailed insights into AFSC belief systems and methods for managing operations through identifying and eliminating constraints. However, before gaps in the AoP can be identified the current state of practice and key definitions must be defined. The subsequent sections, Section 1.2.1 through Section 1.2.6, include detailed explanations of what the AoP is, why it is used in this thesis on dynamic management of lead times, and justification and connection to the way forward for designing fail-safe defense supply network systems.

1.2.1 Introducing Art of the Possible

Before gap identification can occur, the current state of practice and priorities within AFSC systems must be identified. In the AFSC, work control, lead time management, and constraints management within the system is currently dictated and organized using the AoP framework. The AoP is a framework developed by the AFSC as a fundamental basis and doctrine for sustainment performance and activities that includes principles to inspire innovation, a culture of driven leadership, creativity, and continuous process improvement (CPI) within primarily sustainment-based defense organizations (AFSC 2023). Unlike previous initiatives such as Total Quality Management, Lean, Theory of Constraints (ToC), and Six Sigma, which often brought challenges and resistance and ever-increasing changes with each change of command, AoP designers integrated the most valuable concepts from these initiatives into a standardized management system that would sustain despite changing commanders (AFSC 2023). AoP can trace its origins to the difficult task of establishing the Air Force Sustainment Centers in 2012 which involved combining various depots and supply chain functions. This complex merger presented Air Force leaders with an opportunity to standardize business practices under a new and universal and open-source framework. Before describing what the AoP is in the subsequent sections, it is important to clarify what it is not. AoP is not a temporary or passing process improvement initiative, nor is it intended to only apply to a specific office or team. Instead, the AoP was designed to be a universal and comprehensive set of best practice standards for Air Force sustainment to set consistent and common goals for constraint management (AFSC 2023).

1.2.2 Measures of Performance within Art of the Possible

Success, simply identified within the AoP framework, is measured by meeting targets. Targets are met by recognizing and managing constraints that are impeding positive progress towards that target. More specifically, constraint management within the AoP can be best described as techniques to manage a network of nested priorities with common goals for increasing throughput for combat capability (AFSC 2023). These goals are measured in terms of quality, speed, safety and cost effectiveness (Figure 1.1). Speed and associated throughput has direct links to safety, quality and cost effectiveness. Speed is not merely about simply working faster or cutting corners; rather, it involves swiftly identifying and resolving process flow issues through instilling a culture valuing constraint recognition and issue elimination. Urgency is highlighted as a key feature of speed in meeting critical timelines which are often linked with potential mission failures. The leadership principles of embracing a safety culture helps to reduce injuries and equipment damages alowing for an increase in speed while maintaining quality outputs. This attention to quick, safe, and high quality throughput leads to improved cost-effectiveness by reducing rework, resulting in better customer satisfaction, greater capacity, and stronger support for the mission. Each one of the core goals of the AoP has implications for leaders within the organization to take a direct and hands-on approach to creating a cuture of improvement.

Figure 1.1: Common Goals (AFSC 2023)

Those common goals are situated within the role of leadership within the context of People, Processes, and Resources. Within the AoP, leadership is the vehicle for success and is considered the key to bettering an organization and continuing to drive towards excellence. Leadership, in terms of the AoP, is described as the "tie that binds strategic planning with mission execution and makes it possible...to unite with the common goals that are needed for success" (AFSC 2023). These ties are represented in a Leadership Model shown in Figure 1.2 which includes "the essentials a successful leader must understand and execute to achieve true AoP performance" (AFSC 2023). The Leadership Model is visualized as multilayered components needed to increase throughput and warfighter readiness centered around common goals within a complex defense sustainment environment. The largest layer encircling the entire system is Leadership Culture which includes principles of teamwork, accountability, respect, transparency, credibility, and engagement (AFSC 2023).

Figure 1.2: The Leadership Model (AFSC 2023)

The AoP system is referred to as "The Machine" and is made up of three equally important and connected components: People, Processes and Resources (Figure 1.3). Processes, or "*the way we work",* are the backbone of defense sustainment operations. They can include both physical processes that include procedural steps to widespread system organization strategies. The basis for managing Processes, within the AoP framework, is rooted in continuous process improvement and standardization to eliminate waste and enhance efficiency. This involves visualizing current processes through techniques like mapping, establishing standardized procedures, and utilizing tools like Lean, Six Sigma, and Theory of Constraints (ToC) for problem-solving are discussed in more detail in Section 1.2.4. Efficient resource utilization is stressed, ensuring that resources are allocated effectively, capacities are balanced, and modern technology and infrastructure support those optimized processes. The next component in "The Machine" is Resources, or "*the 'stuff' needed to do the work"*, which includes both physical and digital assets from the smallest components to entire weapon systems. Lastly, People, or "*those doing the work"*, are another fundamental element in "The Machine" and can include components like prioritization of skilled training, leadership, and collaboration. Leadership, specifically, has a fundamental role in driving the AoP framework into practice. Leaders help by identifying requirements then coordinating People, Processes, and Resources for fully successful outcomes within their units. Leaders at all levels are responsible for maintaining and enforcing behaviors required for supporting, implementing, and sustaining AoP practices and doctrine, requiring a clear vision, consistent communication, and active engagement to manage adequate utilization of all process Machine components. Additionally, leadership is tasked with ensuring the empowerment and involvement of personnel, with a focus on providing necessary training, encouraging initiative and CPI-based decision-making, and fostering a collaborative environment for problem-solving.

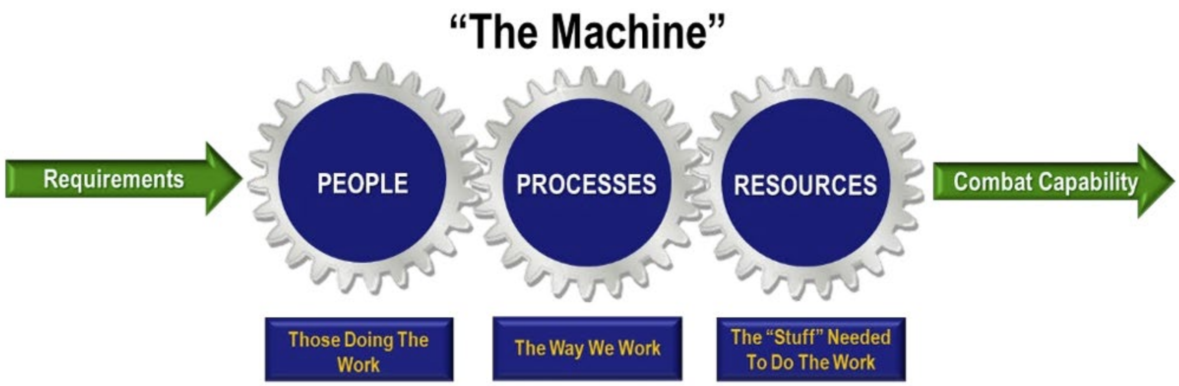

Figure 1.3: The AoP Machine (AFSC 2023)

1.2.3 Managing "The Machine"

While "The Machine" in Figure 1.3 is a representation of the entire sustainment system from initial requirements to resulting combat capability, the dynamics behind system management are based in the AoP Cycle. The AoP Cycle is a visual representation of the process of constraint management within the AoP framework. Constraint management begins in Step 1 establishing flow through the system. System flow is the movement of information, People, Processes, or Resources through the system aimed at achieving a specific objective. Once system flow and Work in Progress (WIP) have been identified the constraints management cycle can begin. The AoP-based constraint management framework is designed to operate on a repetitive cycle based on the Theory of Constraints (ToC) approach (Goldratt 1984, AFSC 2023). It begins by mapping the flow and location of the decreased throughput and increased WIP, identifying system constraints, and resolving the constraint (Figure 1.4). WIP control is further specified based on a modification of Little's Law which provides a mathematical foundation for identifying throughput and flowtime.

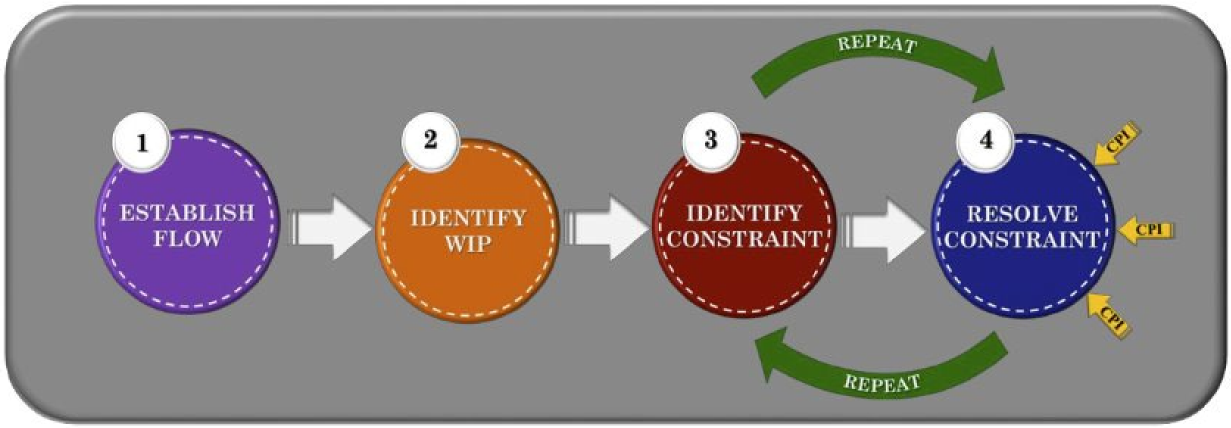

Figure 1.4: The AoP Cycle (AFSC 2023)

Little's Law is applied to distribute WIP and set target days throughout "The Machine" of a process from the input to the output and details the relationship between throughput, flowtime and WIP (AFSC 2023). Throughput or the required rate of a process "Machine" output in units of time and flowtime or the average time a single unit remains in a process Machine are both multiplied to calculate WIP (Eq. 1). This equation can be manipulated by the user to determine each component if two of the following variables are known for a particular process Machine (Eq. 2 and Eq. 3).

$WIP = Work\ in\ Progress$ $\qquad TP = Throughput$ $\qquad FT = Flowtime$

$$WIP = TP \times FT \qquad \text{(Eq. 1)}$$

$$TP = \frac{WIP}{FT} \qquad \text{(Eq. 2)}$$

$$FT = \frac{WIP}{TP} \qquad \text{(Eq. 3)}$$

The AoP modification of Little's Law involves the incorporation of takt time (Eq. 4). Takt time or the "heartbeat of the process Machine" is used as the basis for defining the frequency of a single unit produced by a particular process "Machine" based on available time and required output in that amount of time (AFSC 2023).

$$AT = Available\,Time \qquad\qquad RO = Required\,Output$$

$$Takt\,Time = \frac{AT}{RO} \qquad\qquad \text{(Eq. 4)}$$

Based on the ToC, constraints are identified by backups of excessive WIP in queue or the area or task with the lowest throughput rate. Once a constraint is identified the next step is to exploit the constraint by getting the maximum potential and throughput out of that task or area with the least amount of investment. For example, if a particular machine is limiting the number of parts available downstream, operating that machine for extended hours would be a way to exploit the constraint (AFSC 2023). Once the limiting constraint has been exploited, if it still represents a slowing to the system the other tasks preceding and proceeding that constraint must be subordinated, this is called Horizontal Integration. Lastly, if the constraint has not been resolved in the previous steps, escalation and elevation may be required. Based on the previous example, elevating the constraint would involve the purchase of an additional machine to increase output. Ultimately, the resolution of the constraint must be based in CPI within the AoP common goals.

1.2.4 Management System Integration

The AoP framework is grounded in several overarching core principles: constraint management and elimination, guiding throughput capacity to its fullest potential through engaged leadership, and committing to ongoing process improvement based on common goals. These principles each have associated detailed components that collectively represent a Requirements List for a process "Machine" to achieve success. These Requirements make up the Radiator Chart which includes a standardized set of operating principles for application in defense sustainment environments (Figure 1.5). The Radiator Chart is meant to serve as a roadmap for removing variability and setting expectations for "The Machine" for increased and consistent accountability (AFSC 2023).

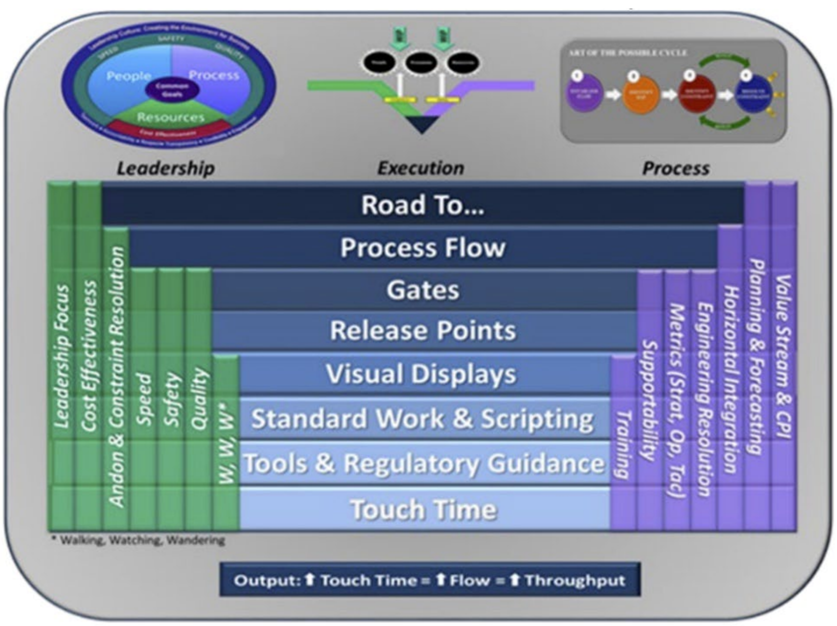

Figure 1.5: The Radiator Chart (AFSC 2023)

The overlapping design of the Radiator Chart, while complex, is designed to reflect the interdependence of each element where the length of each Horizontal Element, described in more detail in Figure 1.6, is used to indicate the scope of influence it has over the proceeding elements

(AFSC 2023). In addition to the length and layering of the elements, the Horizontal Elements are related to the execution or way to set up "The Machine" while the Vertical Elements are Leadership features or actions required for "The Machine" to achieve success.

Road to...

- Establishes the need for a future-state goal
- Process of communicating the goal throughout enterprise
- Must align directly with customer requirements

Process Flow

- Map of tasks required to achieve the Road to... Goal
- Defines the Critical Path or Critical Chain
- Basis for standardized work with repeatable, disciplined processes and predictable outcomes

Gates

- Involves breaking up long production flowtimes into discrete elements or increments to work along with tangible ending points

Release Points

- Production check to ensure work meets Road to...goals and quality standards before releasing to the next gate
- Requires business rules and checklists to create both culture and awareness at critical production processes

Visual Displays

- Located at execution points
- Provide information about the process or project
- Include measures of speed, safety, quality, cost, and critical path

Standard Work and Scripting

- Standard processes through gates to synchronize Resources
- Focused on creating repeatable processes

Tools/Tech Data

- Provides the process implementor with what is necessary to enact process

Touch Time

- Hands-on the project or product
- Gathering necessary materials and information in a central location (kitting)

Figure 1.6: The Center of the Radiator Chart (AFSC 2023)

The green vertical elements are related to the leadership components and are required for organizational success in managing the process "Machine". By adhering to these principles and methods, AoP Leaders can aim to create a culture of continuous improvement, leading to more efficient and effective operations across the organization. Each is described in more detail in Figure 1.7.

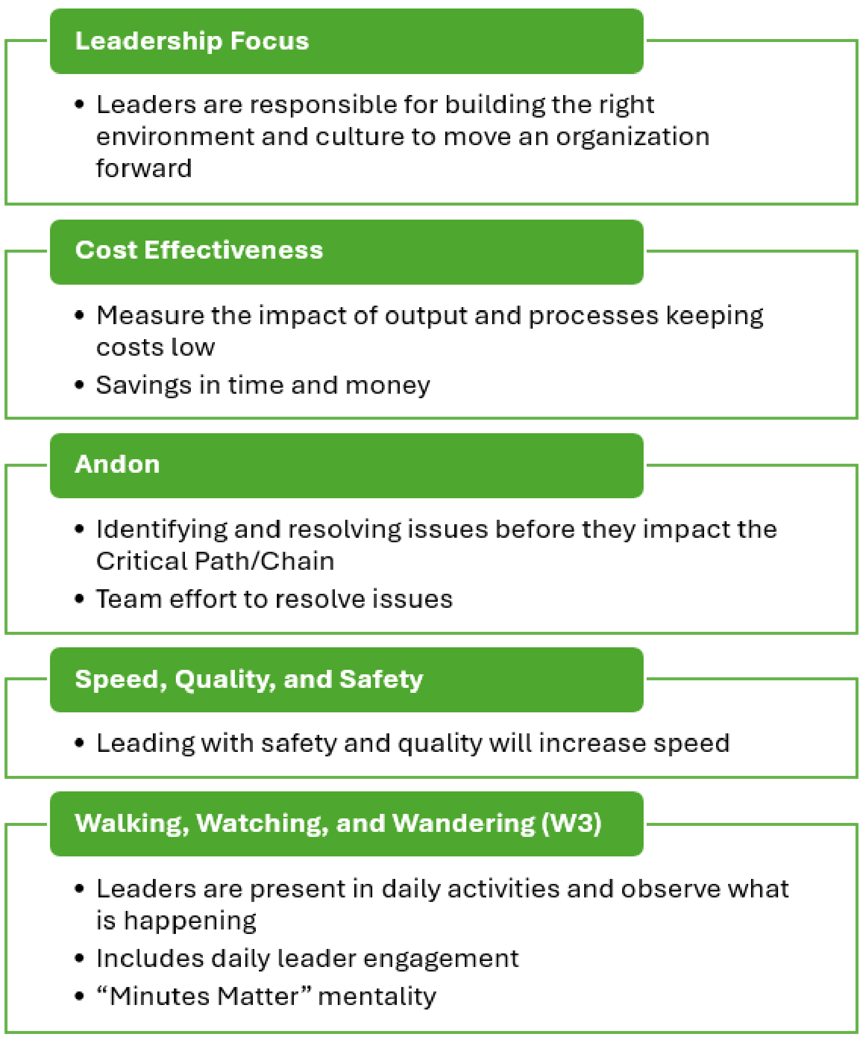

Figure 1.7: Radiator Chart Leadership Concepts and Tools (AFSC 2023)

The purple vertical elements center around the processes for success and act as a list of tools and techniques leadership can use to achieve an AoP mindset (Figure 1.8).

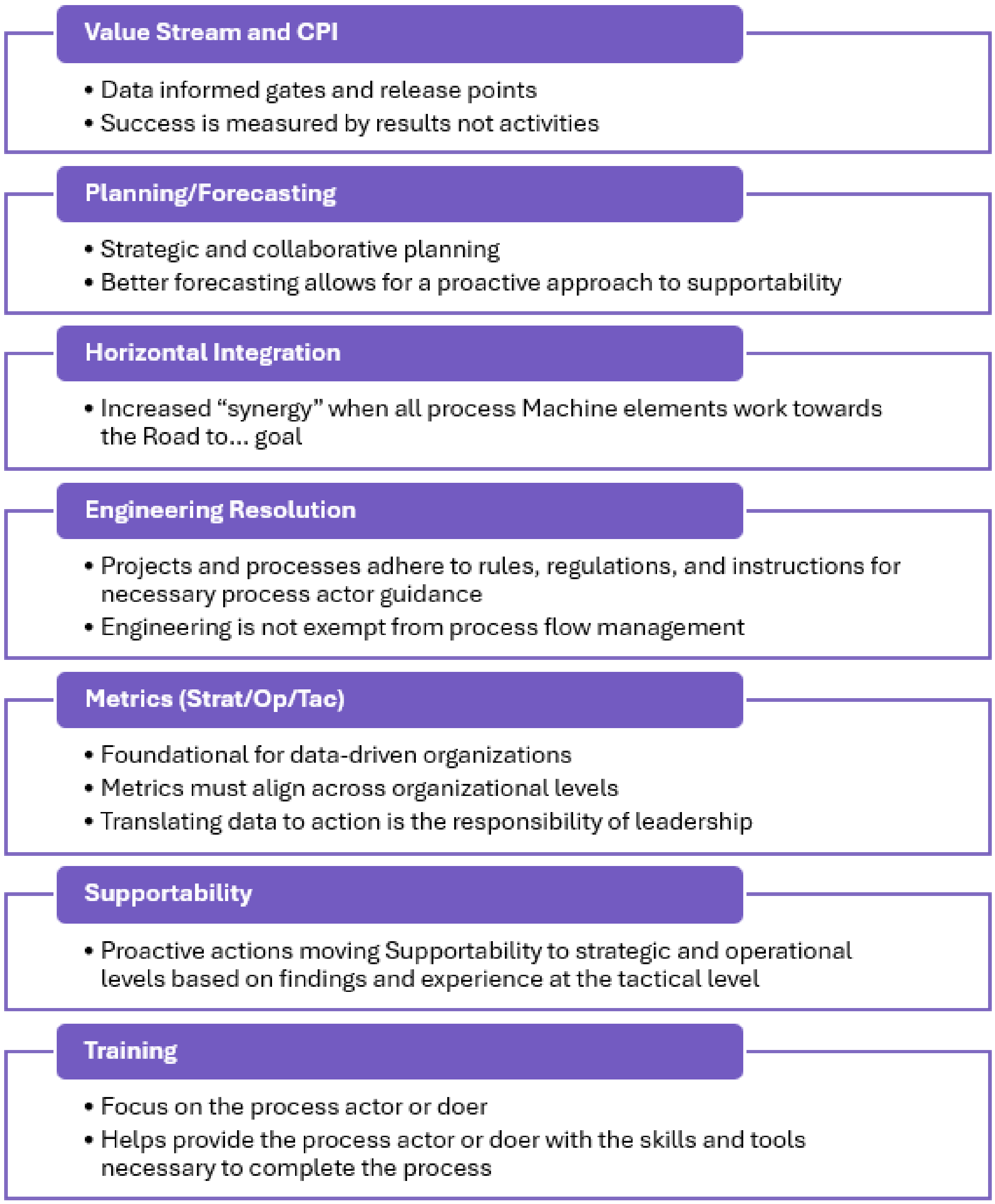

Figure 1.8: Radiator Chart Process Concepts and Tools (AFSC 2023)

Both the horizontal and vertical components of the Radiator Chart combine to represent the integration of the AoP system within principles of constraint management which are essential to manage "The Machine" of People, Processes and Resources. Additionally, each area of the Radiator Chart is based on data in some capacity whether through identifying process data to display visually, leaders tracking cost savings, or pure metrics gathering across organizations, accurate measurements and analyses are vital for CPI and timely and appropriate constraint identification and resolution. Comprehensive and accurate data analysis leads to informed decision-making and tracks progress. The implementation and sustained success of existing AoP components requires comprehensive planning, focused execution, and regular reviews to maintain CPI.

1.2.6 Art of the Possible Summary and Justification

In addition to its open availability in the public domain, the AoP is a framework for standardizing procedures and principles for the identification and management of constraints, measuring continuous improvement, and developing a socially inclusive leadership model centered on common goals. The main justification behind utilizing the AoP for this analysis, however, lies in its methods of identifying, prioritizing, and eliminating constraints within a system composed of People, Processes, and Resources. The AoP framework represents a key shift towards including comprehensive social components into traditional cyber-physical systems that exceed the inclusion of the worker's interactions like in the manufacturing-based Industry 5.0. Additionally, to validate the framework in action, the AoP handbook also includes a structured method for defining potential techniques for approaching complex challenges by providing detailed examples of situations of successful constraint management. These examples fall within Mission Essential Tasks (METs) and include real-world cases of standardization, strategic and measurable goal development, and visibility. Lastly, the handbook also includes extensive Lessons Learned of AoP in action which spurred the initial gap analysis. At its core, the framework is designed as a guide for leaders and teams to realize what could be achieved when constraint limitations are removed within the components of People, Processes, and Resources. By developing and encouraging a culture of improvement and new ideas, the AoP framework was designed as an empowerment tool for defense sustainment personnel to push boundaries, identify new opportunities, and develop new solutions that drive mission success and operational excellence.

1.3 The AoP as a Tool for Determining Requirements for a Fail-Safe Defense Supply Networks

Lead times are not static; instead, they can fluctuate based on factors such as demand variability, disruptions, and evolving mission requirements. The propensity for system impacts due to variation and disruption lead to the need to develop more dynamic methods of managing those lead times. Dynamic management of lead times in the context of defense supply networks involves the continuous assessment and adjustment of the time required to source, produce, and deliver materials and equipment in response to changing operational demands and conditions. While the detailed gap analysis of the AoP framework when applied to a defense supply network is contained within Chapter 4, an initial gap analysis for defense supply network dynamics in terms of lead time management through the lens of the AoP is contained within this section. These initially identified gaps serve as the basis for the development of questions for further investigation presented in Section 1.3.4.

1.3.1 Connecting the Art of the Possible

The AoP framework, with its basis in constraint identification and management, serves as a tool in this thesis for analyzing a more complex defense supply network. The AoP includes a list of requirements needed for detailed assessment of existing processes to pinpoint inefficiencies, bottlenecks, and lead-time challenges that slow down the system's responsiveness. This requirements list, presented in the Radiator Chart (Figure 1.5), is specific to defense sustainment but was developed through key principles that can be generalized for a defense supply network. This framework, when applied to defense supply networks, serves as a tool for a comprehensive examination of how various components of the supply network interact when framed as interactions between People, Processes, and Resources. By reframing this complexity in terms of "The Machine" a deeper grasp of dependencies, constraints, and opportunities for improvement can be revealed. As a result, AoP facilitates the development of a robust requirements list that reflects the nuanced needs of the defense supply network. This requirements list can guide strategic decision-making and investment, ensuring that resources are allocated effectively to enhance system responsiveness and overall mission effectiveness. Through the AoP lens, capabilities of the supply network can be aligned within stakeholders given the evolving demands of defense operations. Through an AoP-based leadership perspective, collaboration across stakeholders like government agencies, contractors, users, and suppliers can become more cohesive, providing a standardized approach to identifying constraints. This collaborative perspective is crucial for developing adaptive strategies that respond effectively to fluctuating demands and changing mission requirements. AoP also emphasizes data-driven decision-making, encouraging the use of advanced analytics and predictive tools to dynamically manage lead times, foresee disruptions, and strategize resource allocation. By applying AoP principles, defense supply networks can become more flexible and responsive, enhancing their ability to adapt to the complexities of modern defense needs and to provide timely, mission-critical support.

1.3.2 Initial Gap Identification

The initial gap analysis of the AoP framework revealed three main areas for further study: one, the use of trade-off or compromise-based decisions in practice where optimization is prioritized; two, clear quantification of social components of "The Machine" through the integration and inclusion of stakeholders; and three, defining requirements for variation and disruption response that go beyond resiliency.

For the first gap, a discussion of qualitative and quantitative measurements of successful AoP performance is referred to in the handbook as being "efficient and optimized," but in practice these situations are often resolved through tradeoffs or compromise-based decisions. A major area where the AoP framework states that efficiency and optimization as the goal but describes trade-off or satisficing solutions is in the development of Road to… Goals. These goals are developed by engaged leadership and involve a determination of common goals between the needs of the customer and the needs of the organization for each stakeholder (AFSC 2023). Realistically, multistakeholder relationships often include conflicting goals and priorities with each participant considering the best options for their organization while meeting the partnership obligations or objectives. These multistakeholder relationships are settled through contractual compromise and involve making tradeoff decisions for a satisficing result. Since constraints derived from multi-stakeholder interactions need to be resolved to truly dynamically manage lead times, an analysis of stakeholder constraints should be done.

For the second gap, while the AoP "Machine" can be considered largely one of the most successful integrations of social components into a traditionally cyber-physical systems, the AoP still places most of the social components in terms of the interactions of the worker within the supply chain in a cyber-physical system. The main advancement, however, is the integration of the role of leadership within the system as a key component for constraint identification and resolution. While successful leadership is often measured qualitatively, setting quantitative measures for leadership based in successful constraint management could assist in identifying key social requirements that can be applied in a generalization of the current AoP system. Integrating quantifiable human factors and social systems into traditional cyber-physical systems is widely considered the next step in a holistic, comprehensive, and more accurate contextualization of complex systems. In addition to the inclusion of the role of leadership, defense supply networks are more complex due to the interactions among multiple stakeholders. These stakeholders, each with their own leadership, expose the network to the potential for contradictory goals, global trade and communications complications, and are especially sensitive to both political and geographical disruptions.

For the third gap, the AoP framework is designed to provide guidance on responding to variation and disruption in terms of resilience. Variation is described through examples like finding more discrepancies during an inspection than expected, aging systems, funding short falls or unexpected time delays in generally consistent processes (AFSC 2023). These issues of variation are often exacerbated by a lack of information or low task proficiency levels. Variation in this context can be managed through variability management methods like: Critical Chain Project Management (CCPM), ToC, Drum-Buffer-Rope Method or intentional built-in time buffers and pipelining, Focus and Finish or bandwidth constraint identification (AFSC 2023). Each of these methods includes the goal of managing variability or managing or eliminating elements that limit flow and throughput. Disruption, while it is often used interchangeably with the term variation in the AoP handbook, is sequestered to a discussion on cascading failures in highly complex systems resulting in delays. What the AoP is missing is a robust framework for the management of constraints as a result of disruption that goes beyond resilience. For example, in the Radiator Chart the purple vertical elements, according to the AoP framework are "designed to improve performance and deliver sustained and enduring resiliency" (AFSC 2023). While this may be the goal, the steps and clear definition for enduring resiliency are vague and are mainly referred to in terms of success as a return to previous system stability. This return to status quo may not be sufficient in complex defense supply networks where success or failure has an increased chance of devastating and widespread impacts.

The initial gap analysis of the AoP framework identified three primary areas requiring further exploration. First, it highlighted the reliance on trade-off or compromise-based decisions in practice, particularly where optimization is emphasized, yet often results in satisficing solutions due to conflicting stakeholder goals. This necessitates a deeper analysis of stakeholder constraints to enable dynamic management of lead times effectively. Second, while the AoP framework includes a successful integration of social components into cyber-physical systems, it primarily focuses on worker interactions, with insufficient emphasis on quantifying leadership's role in constraint identification and resolution. This gap suggests that incorporating measurable social factors could enhance the AoP's applicability in more complex defense supply networks. Finally, the framework's guidance on managing variation and disruption primarily emphasizes resilience, lacking a comprehensive approach to constraint management that transcends merely returning to a previous state of stability. This gap is critical, as defense supply networks must contend with the complexities of multiple stakeholders, conflicting objectives, and potential disruptions that can have far-reaching consequences. In conclusion, addressing these gaps is essential for refining the AoP framework to better meet the demands of defense supply networks. By focusing on trade-off decision-making, quantifying social components, integrating stakeholders, and developing robust strategies for managing disruptions, the framework can be enhanced for increased operational readiness. The next sections include the objectives of this thesis and approaches used in subsequent chapters to analyze these identified gaps, ultimately contributing to the development of a Requirements List for dynamic lead time management within defense supply networks.

1.3.2 Objective for the Thesis

The work within this thesis centers around the belief that defense supply networks are critical to U.S. national security, continued materiel sustainment, and combat capabilities. Additionally, because defense supply networks are heavily integrated into civilian supply networks with national and international implications, these systems must be analyzed comprehensively to truly capture real world dynamics. The current methods of managing lead times and addressing supply network issues designed for optimization have resulted in lean but fragile supply networks based in cyber-physical system design that are not robust enough to handle both variation and disruption. By analyzing current DOD behavior and frameworks like the AoP for gaps, from the perspective of a cyber-physical-*social* system, the objective for this thesis is to develop requirements for a fail-safe supply network capable of dynamically responding to variation and disruption. The preliminary requirements and additional gaps discovered throughout this thesis will serve as avenues for developing Research Questions for further exploration and the opportunity to develop new knowledge in a Ph.D.

1.3.3 Questions for Investigation

The current state of defense supply network management systems is characterized by rigid structures and traditional processes that are not inherently adaptable to the dynamic and complex demands of modern defense operations. This pattern of rigidity shows itself in several identifiable problem areas like inconsistencies in lead time management, limited flexibility in response to disruptions, and a lack of real-time visibility across processes. While the AoP was developed to create standardized constraint management techniques to address variation, the framework reverts to a posture of resilience in the face of disruption. The AoP includes a close representation of a holistic system that includes cyber, physical, and social components in their "Machine" design reframed as People, Processes, and Resources. The People, in the AoP framework, consists mainly of the User of the material or the supply chain worker. "The Machine" management perspective was intended to leverage human expertise, continually optimize and improve operational processes, and efficiently utilize available resources for system resilience. This resilience is based on a return to a previous state and has resulted in the development of a lean but fragile system. To align the objective of the thesis with the questions for investigation, each question builds on the next to establish context and justification for the development of a Requirements List that goes beyond resilience towards fail-safe. This thesis will include an exploration of strategies and solutions for achieving fail-safe, focusing on dynamic lead time management as a measure of performance.

Three questions for investigation are addressed in this thesis:

Question 1 (Q1)
What are the current states and identifiable problem areas within current defense supply network management systems as it relates to Function, Behavior, and Structure?

Question 2 (Q2)

How are defense supply network responses designed to handle variation and disruption with respect to the AoP Machine: People, Processes, and Resources?

Question 3 (Q3)

How can an inherently structured, lean, but fragile environment like defense sustainment be dynamically integrated to become a flexible and fail-safe supply network?

Q1, "What are the current states and identifiable problem areas within current defense supply network management systems as it relates to Function, Behavior, and Structure?" was developed for several reasons. First, understanding the current state of defense supply networks provides a foundational baseline so improvements can be measured and understood in context. Secondly, by identifying specific problem areas in terms of Function, Behavior, and Structure, Tensions and potential Dilemmas that contribute to delays and disruptions in lead times can be identified within a complex inter-stakeholder environment. Gero and Kannengieser (2002) define Function as what the role is made for or the teleology, Behavior as what the role is expected to do and what the role actually does, and Structure as the organization of features. These are discussed in more detail in Section 3.1.1. Additionally, the defense sector operates under unique constraints and demands, making it imperative to tailor supply network management recommendations for this specific environment. By exploring how current defense supply network systems behave and are structured within a defined Function, systemic dilemmas can be identified and preliminarily resolved. To summarize, this question ensures that the research is bounded by current defense supply network performance to integrate real-world examples into practical recommendations.

For **Q2**, "How are defense supply network responses designed to handle variation and disruption with respect to the AoP Machine: People, Processes, and Resources?" was developed to fully investigate the current defense sector frameworks of constraint management to identify gaps and areas for development. The AoP Machine framework is based on managing "The Machine" which is made up of People, Processes, and Resources and can be considered a partial cyber-physical-social system from a defense sustainment perspective (AFSC 2023). Understanding how each of these components currently contributes to systems of variation and disruption management and how well those frameworks are functioning is essential for identifying gaps and opportunities for improvement. This approach is rooted in the belief that systems that are more in-tune to real-world dynamics are more fail-safe. The ability to design for fail-safe systems is particularly relevant in the defense sector, where the ability to quickly adapt to both variation and disruption can significantly impact operational readiness, national security, and mission success.

The last question, **Q3**, "How can an inherently structured, lean, but fragile environment like defense sustainment be dynamically integrated into a flexible and fail-safe supply network?" is essential for a thesis on dynamic management of lead times due to the unique challenges and critical importance of defense supply networks. Defense supply networks often operate within a highly structured, hierarchal, optimized, and lean systems, which, while efficient in terms of resource utilization, often lacks the flexibility and adaptability needed to respond to rapid changes and unanticipated disruptions. This question is crucial because it highlights the core challenge of transforming a resilience-based system into one that is fail-safe and can withstand

and quickly adapt to varying conditions. Defense supply networks must be capable of maintaining operational readiness and effectiveness in the face of uncertainties such as geopolitical disruptions and emergent threats. By exploring how to integrate dynamic lead time management practices into this environment, significant recommendations for defense system performance towards fail-safe supply networks can be made. By preliminarily answering this question, contributions towards the development of a robust framework that nests the strengths of lean operations with the adaptability of agile and dynamic system principles can be made. Ultimately, this research will be used to provide valuable insights for the development of additional Research Questions for designing a fail-safe defense supply network capable of supporting and adapting mission-critical activities in the face of variation and disruption.

1.3.4 Scientific and Engineering Relevance of the Thesis

A thesis on the dynamic management of lead times in a defense supply network environment is highly relevant to science and engineering due to its potential to significantly enhance system performance and adaptability for complex and defense related environments. From an engineering perspective, this research will lead to the development of a preliminary Requirements List for designing fail-safe systems based in constraint management to ensure that defense logistics are robust and dynamically responsive to changing demands. This is crucial in a defense sustainment environment where timely availability and deployment of people and resources can impact national security.

1.4 Organization of the Work

This section includes an overview of the strategy used in the thesis to address each question introduced in Section 1.3.3 and the overall roadmap for the verification and validation of the thesis.

1.4.1 Overview of Strategy

The strategy for this thesis is both systematic and organized (Figure 1.9). After developing key research questions (**Q1**, **Q2**, **Q3**), each of the questions are addressed and approached through the different methods (**M1**, **M2**, **M3**, **M4**) described in this section. There are four Methods utilized in this thesis to achieve the objective stated in Section 1.42. The first Method (**M1**) is a systematic and critical review of literature. **M1** which is introduced and deployed in Chapter 2, is used to frame the environment of focus within both generalized and defense specific supply network responses to variation and disruption. **Method 2** (**M2**) is a nested Function-Behavior-Structure (F-B-S) Dilemma Triangle developed for this Thesis to fully incorporate an F-B-S perspective into both Dilemma identification and resolution. **Method 3** (**M3**) includes the application of the Business Model Canvas (BMC) to develop a unique business value proposition for defense sustainment within a defense supply network. Lastly, **Method 4** (**M4**) includes the identification and specification of System Archetypes within defense supply network systems. Each of these methods will be used strategically in the Chapters they are best aligned with which will be described in more detail in Section 1.4.2.

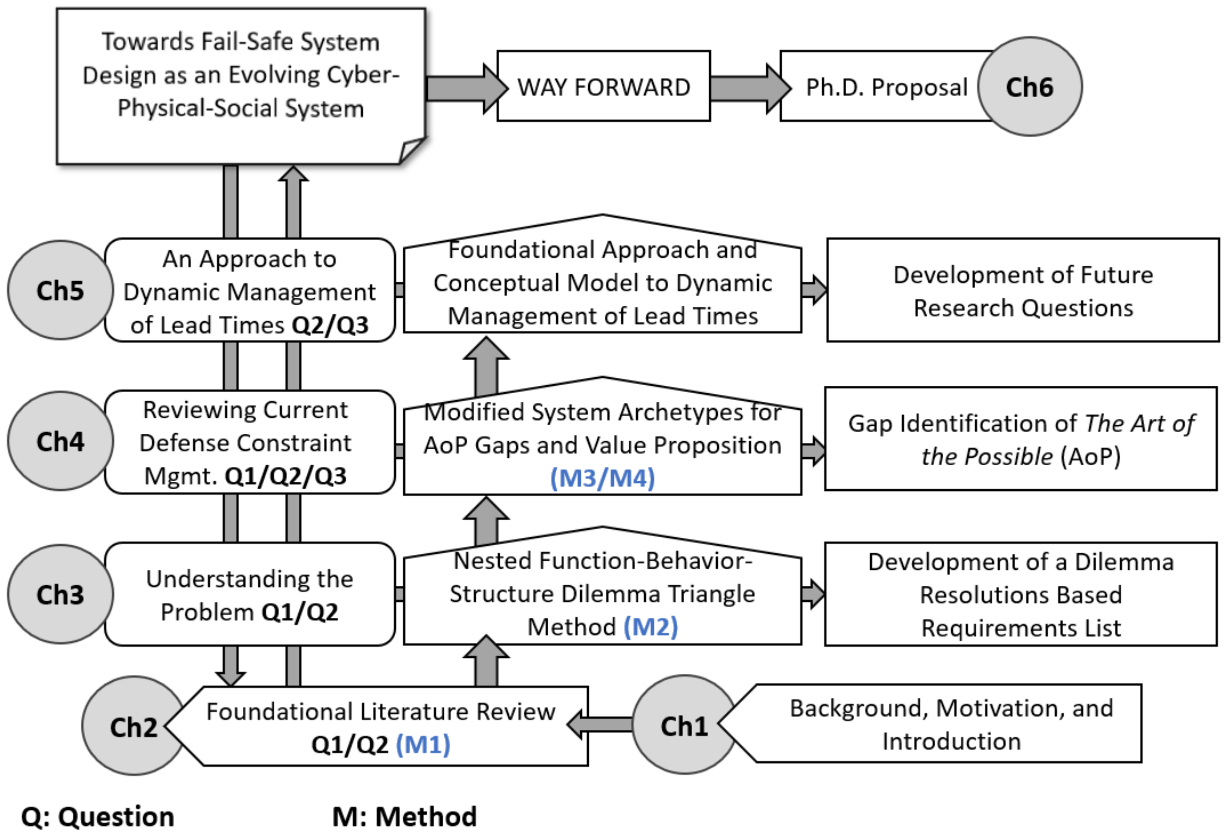

Figure 1.9: Strategy of the Thesis

1.4.2 Thesis Road Map

The work in this thesis is organized around the Validation Square quadrants outlined in Figure 1.10. This thesis begins with this Chapter, Chapter 1, which contains the frame of reference, background, justification, engineering and scientific relevance and road map of the Thesis.

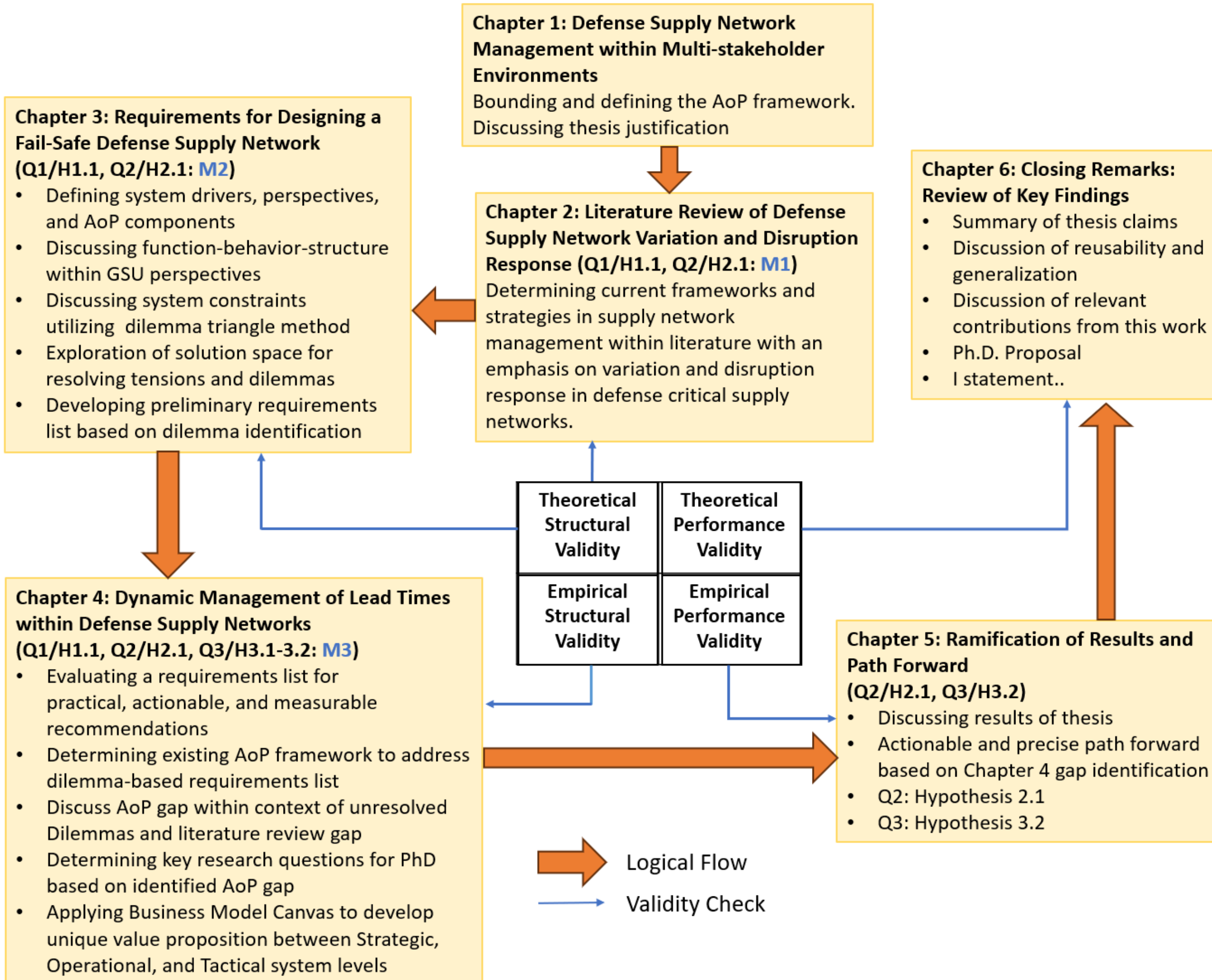

Figure 1.10: Thesis Road Map

In Chapter 2, **M2** is deployed by selecting numerous papers for review based on strict criteria described in detail in Section 2.2 to determine where potential gaps in supply network design exist based on identified current practice and research. The first Hypothesis (**H1**), which states that by determining and systematically evaluating the current state of practice and systemic problem areas within supply network management, research gaps can be identified, and solution spaces bounded by previous lessons learned is evaluated in Chapter 1. The gap identification warrants further study aligning the answers to **Q1** and **Q2**. Chapter 3 contains the application of a nested Dilemma Triangle Method to include the F-B-S construct in a multistakeholder defense supply network environment. This new method, **M2**, also answers **Q1** and **Q2** except from the perspectives of the stakeholders Government, Supplier, and User and is used to set up the justification for the modification and enhancement of the AoP method in Chapter 4. The Hypothesis associated with Chapter 3, **Hypothesis 2** (**H2**), is based on incorporating the domains and interactions of a cyber-physical-social system to address variation and disruption response in multistakeholder defense supply networks, whereby defense organization systems can move towards fail-safe. Chapter 4, includes the connections between dynamic management of lead times through the identification of gaps within the AoP framework to answer **Q1**, **Q2**, and **Q3** specifically related to defense sustainment for future extension. Chapter 4's Hypotheses, **H3.1** and **H3.2** are as follows. **H3.1** includes the hypothesis that by managing lead times at every stage and organizational level within a defense supply network can be more holistic and consistent with real world systems by analyzing existing practices from a cyber-physical-social perspective. **H3.2** includes the hypothesis that fail-safe supply network design is based on increasing system flexibility by focusing on satisficing solutions rather than optimization. Chapter 5 is centered on the ramification of results from Chapters 2 through 4 and includes the identification of the way forward. **H3.3**, is the focus of Chapter 5, and includes the hypothesis that systems based in resilience are not sufficient in modern logistic environments and that to reach fail-safe further work in the form of new knowledge must be done. Lastly, Chapter 6, which serves as the Ph.D. proposal, includes a summary of the claims made in the Thesis, a discussion of reusability, generalization, relevant contributions from this work, the proposed outline and plan for the Ph.D. dissertation, and a final "I statement" finishing the work.

CHAPTER 2: LITERATURE REVIEW OF DEFENSE SUPPLY NETWORK VARIATION AND DISRUPTION RESPONSE

2.1 Frame of Reference

Supply chains and supply networks are both discussed in emerging literature and research focuses. However, the distinction between the two lies in complexity. For example, supply chains are characterized by dyadic value creation, partnerships, and smaller loci of control whereas supply networks include interconnected relationships among supply chain members (Pilbeam, Alvarez et al. 2012, Braziotis, Bourlakis et al. 2013). Since supply networks function within multi-stakeholder environments the interconnected priorities and interests of the stakeholders this has been reframed for this thesis as interactions between Government, Suppliers, and Users comingle to form a complex ecosystem crucial for the flow of goods and services across and within each group. Government entities often oversee regulatory frameworks, security protocols, and infrastructure development, aiming to ensure stability and resilience in supply chains and networks. Resilience is defined as the ability for a supply network to return to acceptable pre-disruption performance (Rezapour, Srinivasan et al. 2018). Suppliers navigate production processes, sourcing materials, and meeting demand while contending with fluctuations in market dynamics and technological advancements. Users rely on the seamless functioning of supply chains to access essential goods and services, emphasizing the importance of reliable and accessible services.

As the global geopolitical landscape continues to evolve and technological advancements reshape warfare, the management of defense specific supply networks has become increasingly complex and critical for maintaining military readiness and operational effectiveness. **Q1**, stated below, was developed to guide the literature search to identify the current state of defense supply network management systems, examining their Function, Behavior, and Structure. As mentioned in Section 1.3.1, Function is defined as what the role is made for or the teleology, Behavior as what the role is expected to do and what the role actually does, and Structure as the organization of features (Gero and Kannengiesser 2002).

Question 1 (Q1)
What are the current states and identifiable problem areas within current defense supply network management systems as it relates to Function, Behavior, and Structure?

By analyzing the existing frameworks and current state, this question-based literature review will be used to identify problem areas and challenges that hinder the effectiveness and responsiveness of defense supply networks. Through this examination, the goal is to gain insights into the pressing issues facing defense logistics and explore potential strategies and areas for development to enhance the agility and effectiveness of military operations in an ever-changing security environment.

In the dynamic landscape of supply network management, the ability to effectively respond to variations and disruptions is paramount for ensuring operational continuity and mitigating potential impacts and risk. **Q2**, stated below, will be used to focus the analysis on the intricate mechanisms governing supply network responses, from the perspective of “The Machine” containing People, Processes, and Resources. How defense organizations manage constraints within the context of wider supply networks is examined to elucidate the strategies, practices, and challenges currently deployed in defense environments to manage variation and disruption responses.

Question 2 (Q2)
How are defense supply network responses designed to handle variation and disruption with respect to the AoP Machine: People, Processes, and Resources?

By examining the interplay among human factors, operational processes, and resource allocation, an analysis and examination of the current capacity for adaptability within defense supply network systems can be highlighted. The findings of this literature review will be used to pave the way to identify gaps in the current defense constraint management frameworks for addressing constraints within a larger defense supply network to ultimately provide recommendations for enhanced performance and preparedness in the face of uncertainty.

This chapter is organized as follows. Section 2.2 includes the explanation of the method used for the acquisition of literature. Section 2.3 a discussion of findings within the papers identified in the literature search to define and explain the terminology used throughout the rest of the chapter and a discussion on supply network response to variation and disruption from the perspective of a generalized supply network. Section 2.3 also includes a discussion on literature with an introduction to defense specific supply networks which will merge into a discussion on defense supply network response strategies for variations and disruptions. Section 2.4 includes a summary and conclusion to the chapter.

2.2 Literature Review Approach

A systematic literature review as conducted that is based in repeatable and transparent literature selection processes to reduce bias and encompassed the variety of research and discussions in this field (Bier, Lange et al. 2020). The steps used to search for and select the literature discussed in Section 2.3 are as follows:

Step 1 – Formulation of a Research Question: This literature review addresses the questions provided and discussed in Section 2.1 and Chapter 1.

Step 2 – Identify Potentially Relevant Works: To identify relevant works, scholarly databases were selected; SCOPUS, Web of Science, Directory of Open Access Journals (DOAJ), and via EBSCO, Academic Search Complete, Military and Government Collection were used. SCOPUS, Web of Science and DOAJ were selected for their breadth of information and interdisciplinary sources. The Military and Government Collection via EBSCO was selected to specifically integrate military and government publications. The topics of supply network and defense supply networks were well documented in these databases.

Step 3 – Selection of Relevant Works: A keyword-based search was conducted in the databases listed in Step 2. The keywords were either combined with the "OR" operator while the groups intended for combination were combined using the "AND" operator. Each group of key words is directly related to the questions posed in Section 1. The first group, the focus of this literature search, included the key words 'defense supply chain(s)' and 'defense supply network(s)'. The second group reflects the aspect of variation and disruption response and contains the terms 'resilience*', 'variation*', 'disruption*', and 'art of the possible*'. These words were carefully selected and based on a wide variety of utilizations within supply network research.

This search was further restricted by publication date to include sources published after 2010. The duration of time was chosen due to the nature of defense organizations being slow to change and this date range is classified, to governmental and military sources, as recent. Non-peer-reviewed journal articles were eliminated. Both criteria reduced the number to 370.

The list was further reduced to 120 journal articles by screening by preliminary relevance to the questions posed in Section 1 by reviewing their respective abstracts, introductions, and conclusions. The categories and topics excluded were articles based on fuzzy data analysis, the movement of people or migration, the humanitarian supply chain, specific articles related to litigation, and supply networks specific to agriculture or ecology. While the research in the excluded articles is valuable, this thesis is fundamental in nature and based in satisficing and defense specific supply network issues that were not captured in these articles. Based on the exclusion and inclusion criteria, the final list was reduced to 80 articles. A common theme of many of these included articles is variation and disruption response within a supply network with specific defense supply network implications.

2.3 Discussion of Findings

2.3.1 Defining Variation and Disruption

Variations within a supply network, as described by Cabrera et al. (2023), typically manifest as short-term changes in demand patterns or shortages. These variations can often be mitigated through adjustments or rearrangements of components within the network, ensuring continued functionality and adaptability. In contrast, disruption events, as noted by D'Souza (2017) and Majchrzak et al. (2021), are characterized by more significant impacts, often stemming from infrastructure damage or collapse. These disruptions may arise from spontaneous occurrences such as wildfires, earthquakes, diseases, and climate change, as highlighted by Ide (2023), or they may be the result of human intervention, including criminal activities and terrorist acts. Regardless of their origin, all disruptions pose potential implications for national security, global economies, and potentially human life and necessitate structural changes within the supply network to overcome (Son, Chae et al. 2021). A striking example of such a disruption is the COVID-19 pandemic, which spread rapidly across the globe, affecting virtually every aspect of the supply network. The unforeseen consequences of the virus underscored the interconnectedness and vulnerability of existing supply networks, prompting organizations to reassess their response mechanisms in the face of unprecedented challenges.

2.3.2 Variation and Disruption Response in a Generalized Supply Network

There are two types of responses used to resolve and alleviate the impacts of variation and disruption events in a supply network: proactive and reactive. Mathematical models and simulation techniques are often tools that can be used to proactively predict potential variations, disruptions, and response results for a given situation.

Variation responses are more readily facilitated within traditional cyber-physical systems and can provide opportunities for strategic digitalization and deployment of some Artificial Intelligence (AI) technologies. Leveraging AI technology within supply networks can help stakeholders forecast demand more accurately, continually monitor large inventories across multiple sites and streamline distribution channels by quickly analyzing large data sets (Turri, Smith et al. 2017, Gyenge, Kasza et al. 2021). AI can also enable real-time monitoring of supply network activities, facilitating the potential for proactive and early identification and mitigation of variations through machine learning and task performance metrics (Auletta, Kallen et al. 2023). For Nguyen et *al*. (2020) they found success in minimizing the maximum lead time and minimizing the time to recover from a major disruption through developing scheduling decision rules for a multi-echelon assembly supply network that is capable of managing variation. Fang et *al*. (2021) furthered this work in their study on a new scheduling method based on sequential time windows using a multi-objective stochastic programing model tool to proactively determine an appropriate and successful distribution schedule under demand uncertainty. In the article by Lee et *al*. (2016) various mathematical models applied to supply network management are discussed with the prevailing theme that quality, inventory, and logistics management is best supported by strategic alliances and holistic supply network design regardless of mathematical model utilized.

While some aspects of disruption events can be proactively accounted for, the impacts of disruptions are marked by reactive responses with reflection after the disaster has been mitigated. For example, the natural disaster disruption responses developed because of the COVID-19 pandemic initiated and catalyzed changes throughout many supply networks. As the impacts of COVID-19 prompted a reevaluation of disaster responses, other sectors within the supply network learned from these experiences, using them as a steppingstone to reassess and enhance their own disruption response strategies (Jacobsen 2020). For example, Mirza et *al*. (2023) reflected on the successful strategic distribution of critical oxygen supplies in India during an infection surge to develop a multi-stakeholder approach to identify real-time supply and predict high-use areas while simultaneously incorporating governmental support through a reduction of customs restrictions and transportation facilitation. In response to sudden changes in pharmaceutical operations, a health system successfully navigated their disaster response framework by approaching the system as a cyber-physical-social system and adapting their workforce and leadership team to prioritize teamwork and build timely and strategic flexibility in the study by Hannan et *al*. (2020). All of these examples utilized lessons learned through reactive disruption response brought on by COVID-19 to make their organization's supply networks more robust and proactive in the face of future disruptions.

Human initiated disruptions like acts of terror and crime have equally destructive impacts on a generalized supply network and associated digital environments and are difficult to proactively position for and predict. An example of a mix of proactive and reactive responses can be found within cybersecurity systems. As the world's population moves towards increasing digitalization and globalization, individuals become more dependent on technology. This dependency is also pervasive within supply networks as most activities have a digital component. With increased digitalization nearly every sector is vulnerable to cybercrimes increasing the critical need to maintain information security and data protections (Maglaras, Janicke et al. 2022). A potential option to increase proactivity and reactivity within cybersecurity is proposed by Jones and Horowitz (2012) by combating cyber-attacks through the use of System-Aware Cyber Security that includes the integration of dynamically interchangeable redundant subsystems, developing subsystems capable of dynamic surface changes, data consistency confirmation services, and forensic analysis for post-attack analysis. Masip-Bruin et *al*. (2021) similarly incorporates a comprehensive system of digital architecture analysis that includes the whole of supply network components to address security and privacy functionalities in an attempt to reduce vulnerabilities in the cyber network.

In conclusion, the management of variations and disruptions within generalized supply networks requires a balanced approach encompassing both proactive and reactive responses. Proactive measures, facilitated by mathematical models, simulation techniques, and AI technologies, enable stakeholders to predict and mitigate potential variations, enhancing the resilience and efficiency of supply chains within supply networks. However, the impacts of disruptions often necessitate reactive responses, prompting reflection and adaptation after the event has occurred. Lessons learned from reactive responses, such as those prompted by the COVID-19 pandemic, can inform strategies to enhance supply network robustness and preparedness for future disruptions. Additionally, addressing human-initiated disruptions, such as cybercrimes, requires a combination of proactive cybersecurity measures and reactive responses to mitigate vulnerabilities and protect digital environments. By integrating proactive and reactive approaches, flexibility can be built into supply networks, ensuring continuity and effectiveness in the face of evolving challenges and uncertainties that go beyond resilience.

2.3.3 The Defense Supply Chain as a Network

United States (U.S.) has maintained logistics support over the last century in a variety of peace and wartime conditions; however, over the last twenty years the field has been marked by a "Supply Chain Management Revolution" moving away from traditional combat support into a systems approach to align with complex integrated weapons systems and life cycle management with an emphasis on technology, lean processes, and strategic alliances (Russell 2011). With this revolution and reevaluation of traditional supply chain principles came the development of new operation models. The DOD has used a variety of supply chain operation models to modify, manage, and coordinate supply practices across the department and associated services. In response to this cultural shift to account for the increased complexity within the defense supply network the U.S. developed enterprise-wide program is referred to as Joint Supply Chain Architecture (JSCA) in conjunction with various Materiel Command Centers. Fletcher (2011) explains the six fundamental principles within the JSCA aimed at enhancing supply chain management within the DOD as the following. First, it seeks to integrate the Supply Chain

Operation's Reference (SCOR) Model across DOD operations through the implementation of JSCA. Secondly, the process aims to establish performance measures focused on outcomes and end-to-end efficiency. Third, decisions are approached to optimize the entire DOD budget while enhancing readiness levels. It emphasizes not sacrificing overall system effectiveness for the sake of individual functional outputs within the supply chain. Additionally, the process advocates for the creation of a governance framework capable of facilitating alignment and coordination across the joint supply chain. Lastly, policy design within the JSCA framework prioritizes accountability, responsibility, consistency, and adequate resource allocation to support informed decision-making throughout the end-to-end supply chain. Each of these processes are designed to enhance visibility, control, support, and efficiency throughout the warfighter supply network and DOD supply chain in response to variation and disruption (Taghizadeh, Venkatachalam et al. 2021). This revolution and development of the JSCA, while beneficial in bringing defense logistics more aligned with industry's characteristic agility cannot necessarily overcome the unique limitations found within a defense specific supply network connected to a wider governmental organization (Haraburda 2017). Additionally, the JSCA goals, while commendable, lack specificity in potential strategies or methods for achieving them leaving a gap between desired outcomes and actionable design.

Defense supply networks are marked by several specific characteristics that separate them from a generalized supply network. The defense supply network is incredibly complex, with multiple stakeholders, intricate networks, and diverse supply sources all under a relationship of enhancing and maintaining national security. The complexity within a defense supply network is also impacted by its external environment. The defense supply network does not operate in a vacuum of purely domestic supply; it must operate and participate in a multipolar supply network environment with the potential for competing priorities and influences. Multipolarity in supply networks refers to the presence of multiple stakeholders with diverse interests and power dynamics that influence the flow of goods and services (Blagden 2015). In a multipolar supply network, there are various actors within the stakeholders of Government, Supplier, and User such as manufacturers, distributors, retailers, and fabricators, each playing a role in shaping the network's structure and dynamics. These stakeholders often operate within a globalized context, where supply networks extend across different regions and countries, further complicating the network's multipolarity. This globalization of defense operations exposes supply networks to geopolitical tensions, trade conflicts, and regional instability, further exacerbating risks and uncertainties. One such example is the defense supply network's reliance on key materials with globalized supply sources like rare earth metals that require extensive industrial mining and refining facilities that may not be possible to support domestically. The ability to acquire these materials without domestic supply sources is increasing the U.S.'s reliance on foreign, potentially non-allied or adversarial sources (Zhou, Li et al. 2017, Lind and Press 2018). Sanders (2012) however, offers a different perspective on the perceived criticality of certain markets by highlighting that the indispensable role of the item or service in the defense supply network is more important than the size of the overall market or quantity demanded as in the case of rare earth metals.

Increased defense supply network globalization can also develop into symbiotic relationships like how the U.S. relies on allied relationships to maintain critical defense priorities and to either assist or receive assistance if necessary. However, these relationships are complex and not without difficulties. This complexity arises from factors such as differing regulations, cultural norms, market conditions, and geopolitical tensions, which can impact the interactions and relationships among allies in this next generation of warfare (Anagnostakis 2016). These relationships can also introduce a dependency on international research, technology, or materials reducing U.S. control and potentially opening the U.S. up to disagreements related to intellectual property laws (Tyson and Guile 2021). Increasing globalization of the defense supply network also underscores the need to develop more sustainable operations due to the global impact of such large carbon footprints (Alvarez, Zavala-Araiza et al. 2018, Belcher, Bigger et al. 2020).

Additionally, the defense sector's reliance on specialized equipment, materials, and technologies for combat success introduces dependencies on specific suppliers and perpetuates situations of sole source, increasing the risk of supply shortages and bottlenecks. Sole source relationships can open the system up to catastrophic disruptions if the supplier deems the item or service is obsolete in the event the defense sector demand is not large enough to sustain its production. The impact of obsolescence in the defense sector is profound. It poses significant challenges to military readiness, operational effectiveness, and national security. As technology advances and threats evolve, defense systems and equipment rapidly become outdated, rendering them less capable or even obsolete in the face of emerging challenges. Obsolescence not only undermines the performance and reliability of critical defense assets but also increases maintenance costs and limits interoperability with newer systems. Additionally combat environments can present supply networks with increasingly dynamic demand variability. To combat situations where managing parallel supply distribution lines need to respond to match different operating environments like those present in a multiple front conflict, Purivis et *al*. (2014) recommends focusing on flexible vendor and sourcing relationships which can have equally beneficial implications when faced with reducing sole source situations. Lastly, the stringent security requirements and classification of sensitive information within defense logistics pose challenges in terms of information sharing, collaboration, and transparency, all of which can hinder agility and responsiveness in times of crisis.

These inherent defense supply network characteristics underscore the importance of proactive risk management, redundancy, and contingency planning efforts within defense logistics systems to address vulnerabilities and ensure mission readiness. Effectively managing multipolarity in supply networks requires strategies for coordination, collaboration, and risk mitigation to ensure the smooth functioning of the network and to address challenges like variations, disruptions, conflicts of interest, and fluctuating demand.

2.3.4 Variation and Disruption Response in a Defense Supply Network

While a defense supply network is equally susceptible to disruptions stemming from national, international, and civilian events, its unique characteristics, such as a complex multipolar environment, stringent security requirements, long lead times for specialized equipment, and complex legacy supported bureaucratic processes, render it particularly vulnerable (Klibi and Martel 2012). This complexity can lead to inefficiencies, delays, and vulnerabilities, particularly when disruptions occur.

The defense supply network is equally responsive in both proactive and reactive ways. For example, simulations within the defense sector, or War Games, have been a critical tool used to pre-evaluate tactics, operations, and defense strategy to enhance a proactive stance in the past century most notably since the beginning of the Cold War (Reddie, Goldblum et al. 2018). These simulations while helpful, generally function without all the data needed causing large generalizations and assumptions that can fail to capture real-world dynamics and often reduce complexity by removing human factors limiting the ability to exercise and model ‘real-world’ decision making (Anderson 2015). For those reasons, these simulations cannot always prepare the perfect proactive responses for a user or a nation for a large unpredictable catastrophe or changing event causing widespread disruption in the supply network. Increasingly however in addition to War Games, the defense sector is studying large-scale disruption responses to gather critical insights into both proactive and reactive supply network management techniques, drawing from real-world examples such disasters that rely on the utilization of agile distribution strategies and dynamic inventory management during these crises (Kamalahmadi, Shekarian et al. 2022).

The defense supply networks have benefited from studying disaster disruption response. For example, Osgood et *al*. (2023) state that as a result of COVID-19 pandemic response lessons learned, the U.S. Army modified its pillars of readiness to incorporate a comprehensive infusion of flexibility, agility, and adaptability into the Army's operating framework. Tatham et al. (2012) discuss an adapted military planning framework based on a Resource Based View to analyze and discuss the success and preparedness of response strategies for two very different countries: Bangladesh and Australia. Their study concludes by stating that using disaster relief as a framework for disaster management is a great opportunity for cross-learning that is generalizable to a variety of sized disruptions and environments. To apply a more comprehensive approach to determining the success of disruption responses, Day (2014) shows how disaster relief organizations vary in quality of disaster response through their interactions with their environment. He notes that systems with strong information management, resource allocation, and feedback system status are best facilitated through a flexible distributed decision-making framework with strategic task specialization. This is a contrasting perspective to defense supply networks that are managed by top-down, rigid hierarchies. Continuing the discussion of flexibility but modifying instead to the flexibility of resources, the study by Handfield et *al*. (2020) considers a flexible structure of receiving and distributing materials and recommends developing a national material "control tower" for improved transparency and real-time access following the response to deficiencies seen in the COVID-19 pandemic personal protective equipment (PPE) shortages. Increased visibility for critical material status and location within a defense supply network would better position a defense organization for rapid equipment relocation to disrupted areas and help produce a more proactive stance on supply distribution and stock. This is equally important in managing inventory that is unique only to defense organizations and critical in response to mobilizations, national defense or other emergencies (Haraburda 2016). The lessons learned from disaster disruption responses underscore the importance of flexibility, agility, and adaptability in enabling defense supply networks to be more proactive and effective disruption response.

Cybersecurity is paramount in a defense supply network and requires ever vigilant digital architecture and technology development to combat cybercrime-related disruptions. House (2021) suggests a method to insulate the Government and associated defense organizations from potential vulnerabilities in cybersecurity through the development of the Cybersecurity Maturity Model Certification (CMMC) that requires a third-party audit based on multiple levels of certifications to examine defense contractors in the supply network. House goes on to say that while the CMMC does bolster cybersecurity culture, the requirements within the certification can put undue pressure on small businesses and potentially stifle or remove competition. Cybercrime is not the only area of vulnerability within a defense supply network. Increasingly damaging and devastatingly invasive are disruptions caused by counterfeit parts especially in the defense and aerospace sectors where enhanced capabilities usually follow additional parts and complex electrical components (Zhou 2014, Akhavantaheri, Sandborn et al. 2023). These counterfeits are hard to detect and may potentially go unnoticed if installed as a component within a larger system. For example, in September of 2011 Raytheon Company alerted U.S. Naval Supply Systems Command to the suspected use of counterfeit parts installed on their SH-60B forward-looking infrared systems resulting in a recall of those helicopters that could have had detrimental effects in an active combat environment (2012). While this was just one major case involving counterfeit parts, it is a situation that must be actively removed from the equation of combat. To assist in the identification of counterfeit risk Sullivan and Wilson (2017) utilized the open-source Department of Defense Product Counterfeiting Database (PCD) to provide insights into identifying key issues and opportunities for counterfeiting that may be remedied through policy and practice.

In the U.S. defense supply network, lead times are critical for warfighter readiness and combat success of the entire nation. Lead times within Air Force sustainment are currently managed with the framework outlined in the AoP handbook which contains the framework for a comprehensive tactical level approach to addressing lead times in terms of Work In Progress (WIP) within the intricate landscape of a production-based defense supply network (AFSC 2023). This framework provides Air Force defense sustainment organizations, at various levels of command, with a standardized method for evaluating, visualizing, and managing lead time dynamics to enhance operational efficiency and readiness in order to maximize throughput by distilling the complexities within defense sustainment network down to People, Processes, and Resources (AFSC 2023). At its core, the AoP framework was designed to emphasize an incorporation of a holistic understanding of defense system management requiring persistent leadership, deliberate personnel development, and system wide buy-in to drive efforts (Douglas, Overstreet et al. 2016). By systematically analyzing each component of sustainment People, Process, and Resource management, defense sustainment teams can identify bottlenecks, inefficiencies, and vulnerabilities that contribute to extended lead times. Additionally, the AoP framework was designed to promote a culture of data-driven decision-making and continuous improvement, empowering defense organizations to leverage performance metrics and feedback mechanisms to refine their lead time management strategies over time.

While literature provides valuable insights into the current systems within defense supply networks, several gaps and challenges exist. The unique complexities inherent in defense supply networks present significant vulnerabilities that have not been comprehensively and conjointly alleviated. Current proactive measures, such as simulated War Games, while beneficial, often fall short in capturing the full spectrum of real-world dynamics and human factors, limiting their proactive effectiveness in responding to disruptions. The lessons learned from disaster response efforts are significant, particularly during events like the COVID-19 pandemic, and underscore the importance of flexibility, agility, and adaptability within defense supply networks. However, there is a need for further research and development to address issues such as cybersecurity vulnerabilities, counterfeit parts, and lead time management within defense supply networks. Additionally, lead time management, as outlined in frameworks like the AoP is crucial for ensuring warfighter readiness and national defense, yet further refinement and implementation are necessary to optimize operational efficiency. Addressing these gaps and challenges will be essential for building more robust defense supply networks capable of effectively responding to variation and disruptions while simultaneously maintaining national security in a continuously changing landscape.

Stakeholder Integration within Defense Supply Networks

Several sources discuss the importance of stakeholder integration and cooperation in environments subjected to variation and disruption. Defense partnerships and system-wide stakeholder integration are also critical for continued defense success. These partnerships can be local, international, academic, industry, or governmental and are usually financially or contractually managed (Tyson and Guile 2021, Katsaliaki, Kumar et al. 2024). Tatham and Rietjens (2016) begin the discussion by comparing the similar demands within civilian and defense logistics highlighting that many of the activities of both parties overlap. Due to that overlap, stakeholder collaboration and integration can help to reduce disruption propagation and increase viability throughout a supply network (Shi, Yuan et al. 2022, Wang and Yao 2023). For example, through a defense and academia partnership, the Army Materiel Command was able to utilize data systems to generate metrics like customer wait time, a strategic performance metric, to measure bottom-up supply chain performance with tactical traceability (Tseng, Burns et al. 2017). Additionally, Acar and Atadenzi (2015) found that stakeholder integration benefits are higher as demand uncertainty increases eventually leading to higher levels of customer service and less reliance on physical inventory redundancy. In each of these cases, intricate and complex systems were modified to manage the impacts of disruption and were successful by deploying strategies that incorporated integrated system perspectives within a multi-stakeholder environment.

Successful and sustained stakeholder integration requires an infusion of consistent trust built among stakeholders in order to generate a productive partnership relationship (Sofitra, Takahashi et al. 2015, Giannoccaro and Iftikhar 2022). The Government has a unique position within the defense supply network, especially when it comes to consistency. Government functions as oversight to regulatory frameworks, provides strategic planning for national security priorities, and coordinates procurement activities to ensure the availability, reliability, and security of essential resources for military readiness and operational effectiveness. This oversight of regulatory frameworks can involve all three branches of government: executive, legislative, and judicial. Most commonly, interactions among Government agencies are regulated through legal and maintained through financial means to protect and insulate national interests and security. Government action and oversight affects the behavior of civilian Suppliers and Users through incentives and consequences both directly and indirectly (Hasik 2021). There are many instances of these interactions. For example, to directly reduce nuclear proliferation, the U.S. government fined businesses that participated in the trade of dual-use technologies to nuclear sanctioned countries (Weise and Hund 2016). Additionally, to combat the litany of fraud facilitated through Supplier shell companies that can have national security implications, the Government has imposed strict penalties for this behavior through the Corporate Transparency Act (Azrilyant 2021). While the Government has the authority to regulate Suppliers and Users within the legal framework, the Government often considers the burden on Suppliers when introducing new legislation. In the sphere of national security, the SAFETY Act balanced Government and Supplier behavior in screening cargo for illegal goods and potential acts of terror helped to share the liability concerns of Suppliers and resulted in additional compliance strengthening national security initiatives (Crowe 2011). Additionally, to combat the wide spread disruption brought on by the COVID-19 pandemic, the U.S. deployed the Defense Production Act to manage critical and scarce resources by granting authority to gather secure intellectual property from businesses, at-will relocate existing supplies, expand domestic production, and compel industry to support government manufacturing contracts (Raunig, Kesselheim et al.

2020). A more indirect approach can be seen in the Inflation Reduction Act which had widespread impacts by offering various tax credits to behavior modification within Supplier systems and the federal budget in an attempt to reduce inflation impacts on Users (Bistline, Blanford et al. 2023). Instances of collaborative legislation increase the opportunities to build trust among stakeholders. However, while each of these examples focuses on the impact of the Function of Government on the behavior of Suppliers and Users, the enactment of these legislative actions is not always seamless or clear. For example, the 2019 National Defense Authorization Act which was "intended to insulate U.S. supply chains from technologies developed by entities identified as posing a significant risk to national security" placed the onus on Suppliers to comply with legally ambiguous language (Kim 2022). Ultimately, each of these examples found in the literature emphasize that the Government's behavior and function within a defense supply network has behavioral and structural implications for Suppliers and Users.

There are several examples of stakeholder integrations that are unavoidable. The defense supply network heavily relies on civilian resources like public utilities, shipping routes, information systems, and natural resources. This reliance opens up potential avenues for additional disruptions that impact the flow of supplies. Managing relationships between private companies and defense organizations is critical for a more flexible response to potential disruptions (Waller 2011). Additionally, while many disruption events are likely out of the control of infrastructure Suppliers, occasionally the Supplier can be a source of disruption. Koenig (2019) discusses the potential for an adversarial relationship related to Government use of public utilities and points out that most utilities are managed by for-profit private companies organized as regulated monopiles and have the potential to charge Government customers higher operating costs in order to have a higher rate of return. Another stakeholder integration relationship is the continued outsourcing of many logistics services from the Government to third-party private sector companies. These relationships, governed by standardized contractual agreements, can leave both expectations unmet and incentives misleading. Lukassen and Wallenburg (2010) suggest that the in order to make third party logistics service outsourcing contracting more successful more customizable pricing frameworks need to be developed to create a more comprehensive and relational version of the established purchasing framework.

Obsolescence is increasingly becoming a major source of disruption within defense supply networks as the defense organizations rely heavily on legacy supported equipment with older technology. Chellin and Miller (2023) take a systems perspective to combating obsolescence, finding that to mitigate the impacts of obsolescence within an organization, teams and organizations need to fully understand the relationships between and within systems in their supply network and associated support structures. Petel’s (2014) research on mitigating counterfeit risk also highlights that to combat increasingly sophisticated and difficult to detect counterfeits there must be coordination between government and supplier stakeholders. Since the legacy supported defense equipment cannot be removed quickly from defense inventory and new acquisition relies on exceedingly more complex components with a potential for counterfeit infiltration, solutions to these two issues likely lies in leveraging the unique characteristics of each stakeholder within a systems response.

Robust and dynamic defense supply network operations are increasingly critical in the defense sector as the U.S. maneuvers to maintain global competitiveness and ensure a strategic advantage in an age of complex defense and national security concerns. To address these challenges effectively, it is imperative to mesh multi-stakeholder logistics seamlessly wherever possible.

The Cyber-Physical-Social Defense Supply Network

System management techniques that have largely dominated supply chain and supply network practices are traditionally designed as cyber-physical systems. These systems involve the organization and prioritization of the digital landscape and physical resources involved in producing and managing the flow of goods and services. While a cyber-physical system emphasis can increase efficiency it adds fragility into a supply network where variations and disruptions pose significant challenges, particularly in exceedingly complex global environments. Cyber-physical system based organizational frameworks introduce potentially exploitable vulnerabilities, as disruptions in digital infrastructure or physical components can cascade across the supply network, leading to delays, shortages, potential economic crises and security breaches (Krichene, Inoue et al. 2020, Mu, Yue et al. 2021). This leads to a discussion on the use of AI. AI technology, while introducing immense potential within supply network systems, is predominantly utilized in cyber-physical systems with a focus on optimizing technical processes and developing predictive analytics. Robinson (2018) describes the potential critical advantages of AI-driven supply network management which could provide for military maintenance by ensuring timely delivery of essential resources to military units, cross-tracking maintenance schedules for equipment, and enhancing logistical support in complex operational environments. With regard to national security, AI-powered analytics can enable defense agencies to anticipate emerging threats, assess vulnerabilities, and develop and test agile response strategies, thus bolstering national security and combat readiness through pattern recognition and big data analyses (Park 2020). However, the use of AI also raises concerns regarding data security and privacy, necessitating robust legal frameworks and risk management protocols to mitigate potential risks and leaks and ensure responsible AI deployment within both civilian and defense supply networks (Martin 2016). One emerging research topic found within the literature to combine more realistic metrics is to further the development of comprehensive AI algorithms to predict real-world variations and response successes, by incorporating human or social factors. In one such study, Charitoudi and Blyth (2014) propose that to achieve common objectives and predictive modeling of consequences in an organization an interdependence impact assessment approach should be used to incorporate the complexities involved in socio-technical interactions. Another example of the importance and criticality of human involvement within cyber-physical systems is highlighted in the study by Michelena et al. (2023). In their study, they discuss the development of a fault-detection system approach for optimizing warship equipment replacement parts. While this discussion initially seems to refer only to the cyber-physical components within warships, the researchers highlight that without the input from highly qualified and seasoned operators their model would fail to accurately reflect the real-life system. This is just one case of many where the importance of human social input into cyber-physical systems allowed researchers to model a more realistic and comprehensive approach.

According to description provided within the AoP handbook, the AoP framework sounds like a physical-social system. The missing piece is the integration of cyber-physical-social components within a defense-based supply network system. By incorporating the integration of advanced technologies, such as predictive analytics, automation, and real-time tracking systems, with physical and social systems, defense supply network operations can be strategically streamlined and reduce lead time variability. By adopting this comprehensive approach, defense supply networks can achieve greater agility and effectiveness in managing lead times, ensuring the timely and reliable delivery of critical resources to support mission-critical operations.

Social integration into existing cyber-physical systems has been preliminarily discussed in the literature regarding internal and external organizational communication teams and contracting. Furthering the research on other social system concepts with scalability can be considered the next step in designing and analyzing defense supply networks from a systems perspective. For example, successful variation and disruption responses are marked by clear and accurate communications of risk among stakeholders (Can Saglam, Sezen et al. 2020, Hannan, Lundholm et al. 2020). Communication can be furthered and quickened through digital networks, but communication also needs to be initiated through human interaction with the system to identify key risk areas and priorities within complex systems. Van den Adel et *al*. (2022) further specifies the discussion on communication exchange by emphasizing that higher cross-boundary information exchange, both internal and external, to that organization can help develop well-integrated mitigation strategies to avoid duplication and potential operational opposition. This communication also impacts the lower levels of an organization like small teams. Apte et *al*. (2011) found that the most effective team structures for defense contract management were made up of cross-functional teams to bridge the gap often present between contracting officers and acquisition teams. The value and continued success of teams is also heavily impacted by workforce retention and low turnover highlighting the need to incorporate a more attractive incentives and more flexible methodology within civilian service to bring and retain talent (Bryant, Darwin et al. 2011, Ahn and Menichini 2022). While communication can be quickly facilitated and generated through digital means, the strategic prioritization of key information and determining critical information streams is based on an organization or team and cannot necessarily be infused into more rigid algorithms as quickly as humans can adapt. This is emphasized in the study by Gerstein (2020) who reported that poor pandemic response in the early days of the disease's spread highlighted the importance of incorporating consistent strategic communication into existing defense systems. Effective communication within an organization can also significantly improve its ability to negotiate contracts and make more effective contract awards by facilitating the dissemination of prior contract performance data across departments. Performance-based and comprehensive evaluation of contracts can help a defense organization ensure its contracts both effectively communicate their requirements and negotiate better for better outcomes (Randall, Brady et al. 2012, Lin, Lin et al. 2016). Incorporating social integration into existing cyber-physical systems represents the next step in designing and analyzing defense supply networks from a holistic and comprehensive systems perspective.

2.4 Closing Remarks

In this chapter, a systematic literature review was used to explore and identify key contributions within defense supply network research specifically related to variation and disruption response techniques within supply networks based on the questions identified in Section 2.1. The chapter included a discussion of the dynamics of defense supply networks, operating within multi-stakeholder environments comprised of Government, Supplier, and User stakeholders. These research contributions have been organized as a review of defense supply network responses to variation and disruption, or uncertainty within systems.

Q1 was discussed as an inquiry into the current state and challenges found within defense supply networks by investigating the current supply network management techniques currently deployed. The discussion begins by identifying systems within generalized supply networks and moves into a specific discussion of the unique characteristics and challenges defense supply networks must contend with when presented with uncertainty. **Q2** involves investigation into defense supply network response strategies, particularly within defense supply networks and the

AoP Machine framework of People, Processes, and Resources. Two different types of uncertainty, variation and disruption, were compared and discussed. AI was proposed as a potential avenue for improving cyber-physical systems, with a section describing how cyber-physical systems are efficient and lean but fragile when exposed to disruption leading to the recommendation to integrate social systems into cyber-physical frameworks. Also, the literature included many examples of stakeholder integration and lessons learned within defense supply networks from studying disaster relief response.

The culmination of this literature review is clear. To incorporate resiliency in the face of both variation and disruption events the defense supply network needs to incorporate cyber-physical-social system principles. The evidence-based recommendation to incorporate cyber-physical-social system principles into existing defense systems is a gap within the literature and warrants additional study. Reevaluating and reexamining existing defense practices from a cyber-physical-social system perspective will allow an infusion of flexibility and agility with the result of dynamically managed lead times and in turn increased readiness and warfighter support.

CHAPTER 3: REQUIREMENTS FOR DESIGNING A FAIL-SAFE DEFENSE SUPPLY NETWORK

3.1 Frame of Reference

Designing and managing defense supply networks is a complex and ever evolving topic full of different recommendations, commentaries, and sometimes contradictory perspectives. This chapter will serve to build on the foundation laid in Chapter 2, where the distinctions between supply chains and supply networks were defined, the unique characteristics of defense supply networks were introduced and discussed, and supply network responses to variation and disruption through the lens of a cyber-physical-social system were explored. In that discussion, defense supply networks, unlike conventional supply chains, were defined as more complex networks composed of interdependent systems involving numerous stakeholders with diverse objectives and operational needs. Now, in this chapter which is based on the paper Designing Fail-Safe Defense Supply Networks presented at the 2024 International Design Engineering Technical Conferences and Computes Conference, the focus pivots to identifying and analyzing the Dilemmas, or zero-sum solutions, that arise from these extensive stakeholder interactions. By pinpointing the constraints that arise from conflicting priorities, resource dependencies, and decision-making dynamics, the aim is to understand how these constraints impact lead times and what is required to reach fail-safe. This analysis will be key for developing a Requirements List for a more responsive and adaptable defense supply network, aligning with the broader goals of dynamic lead-time management and continuous improvement.

The move towards fail-safe supply network design is rooted in current DOD strategic plans. More specifically related to defense sustainment, the DOD Regional Sustainment Framework (RSF) they specify goals for enhancing coordination through collaborative partnerships (2024). In this thesis, the original RSF partnerships, displayed on the left side of Figure 3.1, have been reframed as Government, Supplier, and User stakeholders which is shown on the right in Figure 3.1.

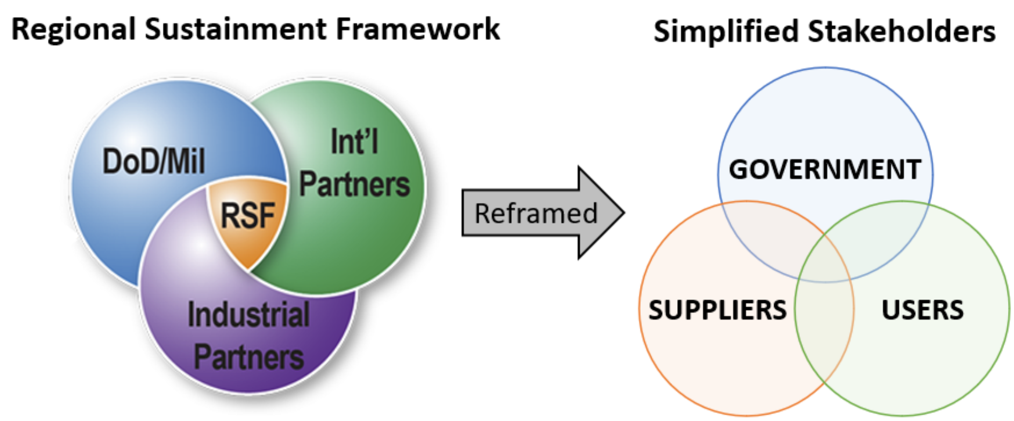

Figure 3.1: Future Goal State of the RSF Toward Multilateral, Multi-National Government Industry Cooperation (2024)

By simplifying the RSF stakeholders to Government, Suppliers, and Users (GSU) the task of determining their constraints is clearly defined based on a set, Function. In the RSF the lines can blur between Government, Supplier, and User in that each partner, either International or Industrial, could reasonably assume the role of any. However, in the reframed stakeholders the Function remains fixed for a single interaction. Function-Behavior-Structure is discussed in detail in Section 3.1.1. After defining clear stakeholders operating in a defense supply network, they are then analyzed to identify constraints in the context of the AFSC AoP "Machine" to determine where constraints or Tensions occur. The AoP is used as a tool to analyze the complex defense supply network through the lens of defense sustainment. It is hypothesized that by discovering the sources of constraints, or Tensions, Dilemmas caused by multi-stakeholder interactions within a defense supply network can be uncovered. The resulting list of requirements needed to resolve these Dilemmas culminates into the Requirements List for a fail-safe defense supply network. It is proposed that resolving Dilemmas amongst stakeholders in a defense supply network is critical for designing a fail-safe supply network. The proposed solutions to these Dilemmas in the form of a Requirements List is generated to produce a positive-sum resolution from the perspective of a cyber-physical-social system. Fail-safe defense supply network design is rooted in the resolution of these Tensions and Dilemmas resulting in a dynamic approach to managing lead times by addressing and eliminating stakeholder constraints.

3.1.1 Stakeholder Function-Behavior-Structure

Within a supply network there are multiple stakeholders as discussed in the previous section they have been simplified by Function as: Government, Suppliers, and Users (Figure 3.1). While these stakeholders are potentially interchangeable, for example, the Government may take on the role of User and a supplier may also be the Government, for the purposes of this discussion their role are sequestered based on a defined Function statement in a snapshot of time. Gero and Kannengieser (2002) define Function as what the role is made for or the teleology. The function of the Government is to maintain regulatory oversight and enforcement laws that have significant impacts in the User and Supplier roles. For example, the Government can impose tariffs on goods originating from certain countries. These tariffs are imposed on the Supplier and transferred to the User through increased fees. The function of the Supplier is to provide material inputs such as raw materials, equipment components, or complete products. Suppliers are the producers of goods with varying degrees of further intended use depending on the end goal. For example, Suppliers who sell raw materials, like copper ore, must maintain appropriate mining strategies to support User demand. The function of the User is to generate demand. Understandably, functions may overlap and vary throughout a supply network. However, even if the Functions change as the process evolves, for one single transaction of goods there are clearly defined and fixed Functions for the stakeholders of User, Supplier, and Government.

Now that the three main Functions of the stakeholders are defined, the next class of variables within the F-B-S construct is Behavior. Behavior variables are defined as both: behavior expected (Be) what the role is supposed or expected to do and behavior from structure (Bs) representing what the role actually does (Guo, Allen et al. 2024). The Be of the Government is related to the development of critical infrastructure, maintenance and enforcement of taxation laws, citizen entitlements, enforcement, and origination of environmental protection laws, and developing state, federal, and international policy. Government Bs from structure involves the origination, maintenance, and enforcement of policies that must be followed by both the User and the Supplier if these stakeholders are within its sphere of influence and establishing governance boundaries for the sustained health and functionality of the State. Changes in Government Behavior usually originate due to disturbances, like global disturbances, foreign allied or adversary actions, or domestic incidents. The changes reflect a protective stance for individuals and communities within the State while also ensuring the security of the State as a whole. For the Supplier the Be is that the Supplier requests fair market value for items that are needed, relevant, and necessary for continued User support. The Bs from structure of the Supplier is centered on supply and demand and ever-increasing goals for financial profit. Supplier Behavior changes are related to dynamic responses to User demand, lowering their internal costs through diversifying their portfolios, and adapting to changing Government policy to mitigate or eliminate risk of litigation or consequences for noncompliance. The User's Be is to generate consistent demand and drive invention through dynamic changes in requirements and needs. The Bs of Users from structure is more complex. Users, while they do generate demand, their inconsistency can lead to volatile market conditions and sometimes their demand can exceed the availability and abilities of the Supplier.

3.1.2 Stakeholder Response to Variation and Disruption

Disturbances in a supply network are divided into two groups based on the extent of duration and method of resolution. As described in detail in Chapter 2, variations are defined as "minor deviations from the plan that occur during execution" while disruptions are "rare and unanticipated events" that have a large enough impact to distort the supply network structure and make some components inoperable(Rezapour, Khosrojerdi et al. 2018). One recent example of Suppliers unable to meet User demand due to a disruption occurred with medical supplies and the subsequent supply network breakdown due to the unprecedented demand resulting from the spread of the Coronavirus Disease 2019 (COVID-19) pandemic. In this situation, due to a reliance on an international supplier as a main source of crucial medical supplies, the United States experienced a near collapse of critical supply as the Supplier began to limit international export in favor of domestic use and stock piling (Sutter, Schwarzenberg et al. 2020). The COVID-19 pandemic resulted in a compounding effect in a change of Behavior for all stakeholders. The Suppliers were unable to meet User demand, and the Government had to change its Structure and Behavior by bypassing potential administrative delays to circumvent supply network breakdowns and prevent network collapse. Additionally, the Government also began a program of tax incentives for domestic suppliers, often times previously unrelated to the medical supply industry, to diversify or change their material output bridging the gap left by an absence of international supply (Marples, Schwarzenberg et al. 2020, Parrott 2020). In this situation, the Government provided the policy and financial incentive to warrant an increase in Supplier motivation and flexibility to meet critical User demands. In this situation, the traditional cyber-physical supply network system was designed to deal with variations but were fragile and prone to collapse when met with the large disruption caused by the pandemic. For example, Structural changes are often slow to enact in cyber-physical system and require social or human intervention to bridge the gap between previous and current network needs. The cyber-physical system attempts to “return to normal” while the cyber-physical-social system can reroute systems to a “new normal” allowing for dynamic change management. By including the social domain, the supply network systems were more prepared and capable of handling both variation and disruption. To connect this situation to defense sustainment, the AoP framework contains clear and concise Behavioral steps on how to resolve variation-induced tactical level Tensions to return to high throughput operations. This system of managing variations has been successful and adopted by U.S. sustainment centers around the world and has proven effective at increasing system resilience. The AoP, however, does not necessarily include a discussion on the implications of disruptions that require a change in Structure. For this reason, the next step in fail-safe defense supply network design that includes dynamic lead time management is one that includes a capacity to change Structure throughout the organization. Determining the details and extent of the ability for a system to change in Structure is begun in the preliminary Requirements List developed through Dilemma resolution in this chapter. The preliminary Dilemma resolutions are related to the operational management level where it is proposed that effectiveness is evaluated and disseminated to the tactical teams. These Requirements are foundational to determining what is needed to design a fail-safe defense supply network for the changing environment of a future full of both variations and disruptions.

3.1.3 AoP Based Dilemma Resolution and Gap Identification

As mentioned in Section 3.1, the AoP includes a plethora of constraint management techniques related to a focus on maximizing throughput with high quality, safety, and cost effectiveness metrics. These techniques are especially helpful in regimenting a standardized management process for a large organization where its main goal is continued management and sustainment of military materiel as quickly as possible. Within the AoP framework, constraints are stated to be easily identifiable through a pattern of low throughput or extended lead times where the preference in all outcomes is shorter lead times and higher performance demonstrated through increased throughput rate. Constraints in this sense are referred to as Tensions which are potential Dilemmas. However, by only viewing constraints by the feedback metrics of increased lead times, work slowdown or longer work in progress (WIP) queues the AoP framework's definition of constraints should be more closely tied to the definition of Tensions, in this thesis. If the implementation or purchase of some service, system, or product can resolve the constraint then that constraint is really a Tension. For this reason, the AoP can be more closely considered a framework for a Tension-management system. In this chapter, the Dilemmas identified are Tensions that are unresolvable with current mitigation techniques and do not fit easily into the constraint management system outlined in the AoP. These Dilemmas highlight a need to develop new techniques for the design of dynamic satisficing-based approach to lead time management that is fail-safe.

Additionally, the Tensions in the AoP are identified at the lowest and largest level, the tactical management level whereas goals and process effectiveness are managed at the strategic and operational levels respectively. In this structure, the operational management level positioned between the strategic and tactical layers, is proposed as the ideal setting to incorporate dynamic lead-time management, as it has an opportunity to uniquely balance tactical flexibility with strategic goal alignment, allowing for agile adjustments that support overarching objectives while responding effectively to real-time demands (Figure 3.2).

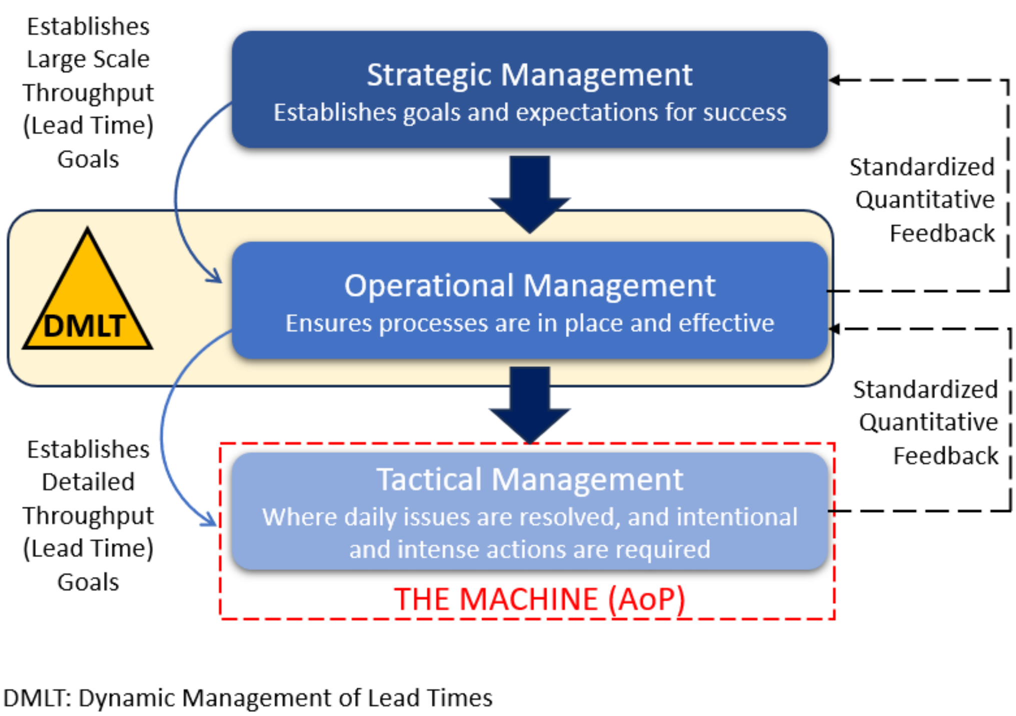

Figure 3.2: Managing the Machine through Dynamic Management of Lead Times (AFSC 2023)

3.1.4 DMLT Dilemma Triangle Focus Node

Within Figure 3.2 highlighting the operational level of management, the gold triangle node, Dynamic Management of Lead Times (DMLT) node, is representative of the balance between the resolution of all Tensions and Dilemmas among the People, Processes, and Resources components within the AoP framework for each stakeholder(AFSC 2023). The DMLT node will be different for each stakeholder based on that stakeholder's unique Function, Behavior, and Structure. The DMLT node also represents the balance between the cyber-physical-social domains within the supply network with necessary and justifiable tradeoffs identified.

3.2 The Dilemma Triangle Method

Before the DTM is used, the method's user should define a problem statement. For this application of the DTM, the problem statement is focused on lead time management for the design of a fail-safe supply network regardless of variations and disruptions. The statement is further specified for defense supply networks utilizing this Dilemma resolution technique.

***Problem statement**: What is required for a defense organization to secure a fail-safe supply network through resolving Dilemmas for each stakeholder in a defense supply network for increased national security and combat capabilities?*

The Dilemma Triangle Method (DTM) is the method used in this chapter to identify Dilemmas within the GSU stakeholders. The method is taken a step further to organize the stakeholder Dilemmas based on Function-Behavior-Structure. Through the resolution of the Dilemmas uncovered in this section, a foundational Requirements List for a fail-safe defense supply network is developed.

3.2.1 Method Overview

This section includes an overview of the steps of the DTM. The initial step in developing a Requirements List that is foundational to finding satisficing solutions for the Stakeholders involves executing the DTM; see (Yadav, Das et al. 2017). The goal in using the DTM's is to take situations with zero-sum outcomes and transform them into dynamically adaptable positive-sum outcomes through trade-offs and compromises (Yadav, Das et al. 2017). This method is outlined in Figure 3.3 as a three-part process with many sub-steps to provide a systematic and organized method to identify elements of the Requirements List for the dynamic management of lead times accounting for both variation and disruption response.

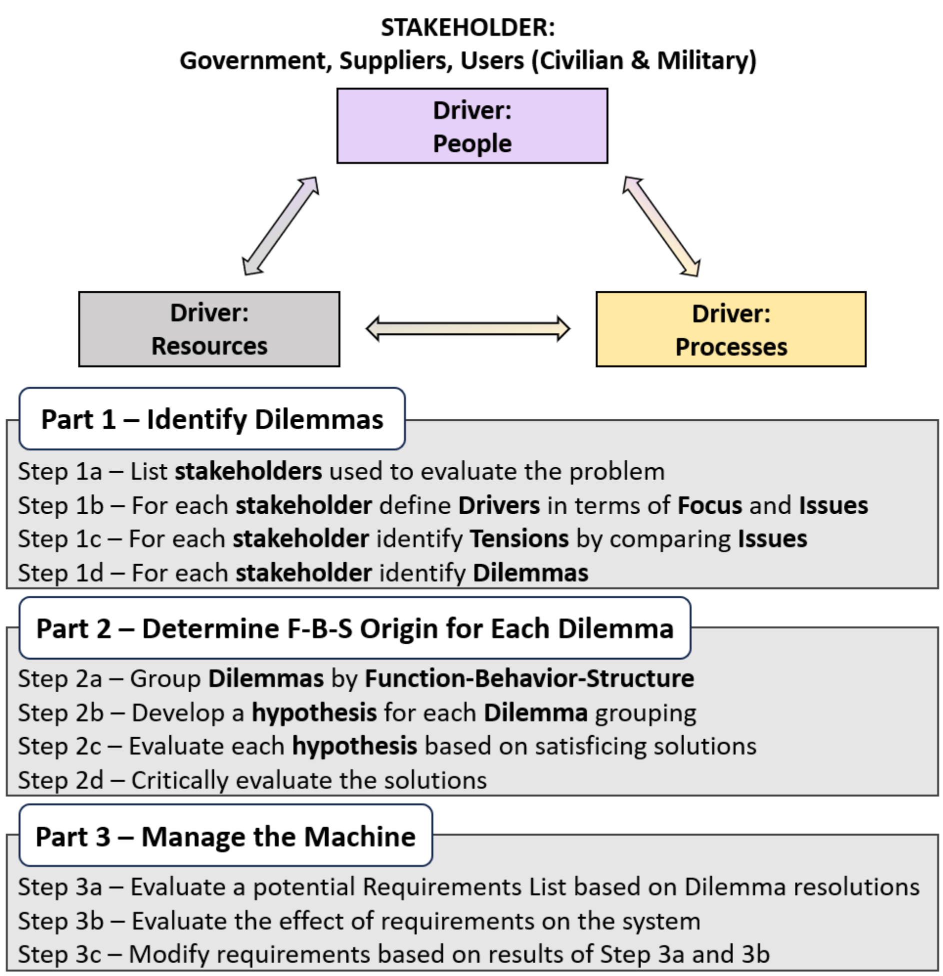

Figure 3.3: Steps of the DTM (Yadav, Das et al. 2017)

3.2.2 Part 1: Identifying Dilemmas

First to identify the Dilemmas for any application of this method, Drivers must be identified based on Stakeholder aspirations. The Stakeholders in this problem are Government, Supplier, and User. Additionally, the Drivers are tied to the components of the AoP Machine: People, Processes, and Resources.

Step 1a – List Stakeholders Perspectives used to evaluate the problem.

- This step helps to ensure that the problem is appropriately bounded. For example, if the Perspective is too narrow the full system will not be accurately evaluated. However, if the Perspective is too large the complexity of the system will preclude identifying a satisficing solution.

Step 1b – For each Stakeholder define Drivers in terms of Focus and Issues

- Drivers are the domains of interest that result in behavior within the Perspective of the problem.
- These Drivers are assigned a Focus based on characteristics exemplified in the Driver.
- Finally, Issues are typically verb/noun combinations that represent possible problems within that Driver based on its Focus.

Step 1c – For each Stakeholder identify Tensions by comparing Issues.

- This step includes identifying Tensions. Tensions are an interaction between two different Focus Issues that have the potential of becoming Dilemmas.
- Tension identification is done by choosing one Issue from one Driver and comparing it to the other Driver Issues one at a time in a matrix style layout for organization displayed in Figure 3.4.

➢ Tensions are not guaranteed between each Issue so careful consideration in this step is critical.

PERSPECTIVE		Driver 1			Driver 2		
		Issue 1	Issue 2	Issue 3	Issue 1	Issue 2	Issue 3
Driver 3	Issue 1						
	Issue 2						
	Issue 3						
Driver 2	Issue 1						
	Issue 2						
	Issue 3						

Figure 3.4: The Tension Matrix Layout

Step 1d – For each Stakeholder identify Dilemmas.

➢ Lastly, identification of Dilemmas from the list of Tensions is based on a mode of resolution for each Tension. If the Tension is easily resolved through implementing a new policy or a purchase, buying that Tension does not represent a Dilemma. Dilemmas are Tensions that represent a zero-sum solution and require a hypothesis to transform it into a positive-sum solution.

3.2.3 Part 2: Determine F-B-S Origin for Each Dilemma

Part 2 of the DTM involves determining value propositions by hypothesizing solutions for each discovered Dilemma. Satisficing solutions must be considered during the evaluation of hypothesized solutions because a reality check must be performed.

Step 2a – Group Dilemmas by Function-Behavior-Structure

- Based on the previously stated definitions of Function-Behavior-Structure, group the Dilemmas by type.

Step 2b – Develop a hypothesis for each Dilemma Grouping.

- The hypotheses developed to address each Dilemma should be based on either experience-based judgment or supported through literature and considered at face value in the idea generation stage. They will be evaluated for merit in the next step.

Step 2c – Evaluate each hypothesis based on satisficing solutions.

- Evaluation of the hypotheses is dependent on the problem statement or overall goal of addressing Dilemmas based on the Users particular application. Consider trade-off decisions and compromise solution spaces.

Step 2d – Critically evaluate the solutions.

- This step is considered as a reality check. Critical thinking techniques must be used to systematically evaluate the list of hypotheses to determine if they hold merit.
- Including situations where there must be an unlimited amount of a resource or item to resolve a Dilemma should be removed.

3.2.4 Part 3: Manage the Machine

Lastly, to manage the discovered Dilemmas an evaluation of their solutions related to long-term supply network sustainment and ultimate effect on the larger cyber-physical-social system within a multi-echelon network must be present to resolve the Dilemmas and reach towards fail-safe.

Part 3a – Evaluate the Requirements List based on Dilemma resolutions.

- Speculation is especially important for this step. It is important to see the hypothesized solution's immediate as well as sustained impact. Important questions related to the duration of success must be asked at this juncture.

Part 3b – Evaluate the effect of Requirements List on the system.

- Since the DTM is a valuable tool when used within systems by requiring a critical examination of interactions between different loci of interest, the hypotheses should be subjected to the same rigor of examination.
- This step focuses the user on how these hypothesized solutions impact the system both within and beyond the boundary defined in Part 1.

Part 3c – Modify requirements based on results of Step 3b.

- Modification after critical evaluation must be considered based on sound justification. Modification for the sake of change without evaluating the thought processes behind the change can potentially expose the Dilemma Triangle results to weak assumptions after such careful consideration was taken during the previous parts.

3.3 Implementation of the Dilemma Triangle Method

3.3.1 Driver Identification (Step 1a)

Identifying Drivers is critical to establishing the boundaries of a problem space. The Drivers in this analysis are directly tied to the AoP "Machine" components of People, Processes, and Resources. The AoP Drivers are then contextualized within the perspective of a CPSS. The AoP Processes component is linked with cyber, the Resources component is paired with physical, and the People component is tied to social finishing the representation of each component of the cyber-physical-social system within an AoP framework. Drivers will remain consistent throughout the analysis, however the process utilized in section will be a nested Dilemma Triangle Method beginning first with identifying the Dilemmas present within each stakeholder: Government, Suppliers, Users then examining the Tensions and Dilemmas in the context of stakeholder interactions terms of Function, Behavior, and Structure.

3.3.2 Focus and Issue Identification (Step 1b)

The Focuses and Issues of the Drivers all relate to a supply network or movement of goods and services based on the stakeholder. The basis for these identified Issues stems from both experience-based judgment and numerous outside sources.

Government Stakeholder

Driver: People

Focus: To protect the interests of the public through fair and equitable trade practices, contribute to a free market national and international supply network, and maintain public trust.

Issues:

1. History of social inequality – In the past, governmental actions and policies have resulted in the situations of inequality like the structural discrimination of "redlining" residential communities based on race (2019).
2. Income inequality – Disparity between level of skill and income in certain employment categories (Greenstein 2020).

3. Erosion of public trust – Pattern of decreasing public trust in governmental institutions (Stevenson and Wolfers 2011).
4. Resistance to change regional belief systems – Resistant regional belief systems that result in limiting policy dynamics (Henry, Lubell et al. 2011).
5. Extremism/Terrorism – Instances of extremism within governmental institutions can further erode public trust and willingness to participate; Acts of terror can devastate Government structure and feelings of security. May result in the loss of life and the destruction of property (Khan, Akhtar et al. 2018).
6. Corruption – Instances of mismanaged funds and improper allocation of information in exchange for personal gain (Tierney 2010).
7. Misinformation – Media and foreign influence can erode public trust in the supply systems and increase the proliferation of misinformation (Rogers 2023).

Driver: Resources

Focus: To enforce strategic and sustainable resource management to reduce negative environmental impacts due to supply network mismanagement.

Issues:

1. History of environmental issues – Instances of improper toxic waste disposal and environmental contamination frequent throughout history (U.S. House of Representatives, 1992).

2. Reliance on fossil fuels – Continued reliance on fossil fuels both disrupts the environment with the additional emissions of greenhouse gases but often ties governments to foreign Suppliers rather than supporting domestic supply (U.S. Department of State, 2024).
3. Resources difficult to acquire due to area conflicts – Conflict in various parts of the globe can and has disrupted foreign supply networks resulting in critically low national stock of essential items.
4. Difficulties in managing consumer demand – When experiencing critical or unprecedented events, consumer demand can exceed regularly supplied items resulting in governmental intervention that, due to urgency, may result in less sustainable means of acquisition to manage the unforeseen demand.
5. Outdated infrastructure and equipment – Inoperable, damaged, or antiquated infrastructure and equipment is often maintained rather than replaced favoring long term sustainment costs rather than possibly high initial acquisition costs to replace (Holman 2006, Nicastro 2023).

Driver: Processes

Focus: To maintain and generate regulatory authority processes that ensure oversight, legal compliance, accountability, and continued movement of capital within the supply network.

Issues:

1. Antiquated policies – Policy change procedures are complex resulting in the enactment and sustainment of processes that do not accurately manage a dynamic environment.
2. Slow to change – Policy change is slow resulting in less agile processes.

3. Security at the expense of efficiency – In order to maintain national security measures, new technologies are often difficult to acquire and utilize due to security concerns.
4. Cybersecurity – Threats from cyber criminals are increasingly common and potentially devastating and extremely costly when successful. The necessary security levels needed to maintain cybersecurity can slow down systems and cut off critical governmental systems from new technologies that cannot adhere to their strict security requirements.
5. Pre-authorized funds – Government allocated funds are often approved on a yearly basis, meaning that unpredictable problems that arise during the already allocated funds year results in an emergency allocation of financial support from another organization or previously planned project. This disruption affects both the financial response time to the unpredicted event and the previously planned project that is now unfunded or underfunded.

Supplier Stakeholder

Driver: People

Focus: To build strong consumer relationships, foster innovation, and collaboration in the development of new technology to meet current and future consumer needs.

Issues:

1. Stock market impacts – Business environments are more dynamic when tied to the stock market (Huang, Song et al. 2022).
2. Workforce diversity and inclusion – Companies that have a more diverse workforce perform better in turbulent markets (Sung and Choi 2021).

3. Skills gap – A high turnover rate can result in a decrease in key on-the-job training opportunities for new employees, possibly resulting in a lower quality product.
4. Profit focus – Suppliers are often tied to businesses that must retain a certain level of profit to continue growing and producing in a market.
5. Public trust – Suppliers can gain and lose customers due to their perception of trustworthiness.

<u>Driver</u>: Resources

<u>Focus</u>: To meet customer demands, maintain quality and strive for continual improvement by managing costs and optimizing sourcing strategies to increase company value.

<u>Issues</u>:

1. Fluctuating demand – Consumer demand can change rapidly and dynamically. Shifting demand can result in previously popular items losing consumer interest, leaving Suppliers with unsold items that can become waste.
2. Global market volatility – Global markets are ever shifting and difficult to predict.
3. Regulatory compliance – Suppliers must follow local, federal, and international law regardless of business impact or face consequences.
4. Transportation and Logistics Challenges – Suppliers must interact with a shipping system that is outside of their control presenting unpredictable challenges and logistical issues.
5. Safety and quality concerns – Suppliers have control over their own quality control, however, that reach does not necessarily extend to the raw materials or piece-part components they receive from other sources. Contamination is also a major issue in supply safety.

6. Need for sustainable practices – Suppliers may favor or be unable to achieve certain sustainable practices.

<u>Driver</u>: Processes

<u>Focus</u>: To develop and utilize sustainable practices for resource extraction and cost effective and energy efficient movement of desired goods and services.

<u>Issues</u>:

1. Dynamic goods and services acquisition – Since the buying power and investment potential of Suppliers is flexible, purchases or investments in untested products or processes can result in a loss of brand reputation if that product or process proves to be unsuccessful.
2. Inefficient and inflexible policies – Suppliers may favor antiquated policies that provide a sense of security rather than expose themselves to possible financial losses.
3. Cybersecurity – Supplier systems can be infiltrated by cyber criminals leaving the company open to ransomware attacks and potentially catastrophic financial losses.
4. Poor inventory management – Poor inventory management can result in damaged, expired, or lost materials resulting in a pattern of repurchasing the unusable equipment or materials again.
5. Ineffective quality control – Unorganized or ineffective quality control measures can result in returned merchandise from consumers.
6. Inadequate technology integration – Purchasing oftentimes expensive new technology without integrating it into existing systems and training relevant employees can both reduce

the effectiveness of the technology on the product sold and reduce potential benefits desired from its acquisition.

7. Capacity constraints – Unsold merchandise must be sold before new merchandise can be made if storage is a constraint. This potentially limits a Supplier's ability to fill large orders.
8. Speed constraints – New Suppliers may be unable to fulfill large orders when beginning their operations due to limited initial capital. They may lack the funds necessary to purchase their necessary materials before receiving revenue from their sales resulting in a slow to start operation.

User Stakeholder – Civilian & Military

The User stakeholder has been split into two categories: Civilian and Military because each category of users has unique characteristics that must be addressed and explained.

Driver: **People**

Focus: To promote innovation through User feedback and transparency in supply network relationships.

Issues (Civilian):

1. Lack of reviews and recommendations – Reliance on reviews and recommendations is common in society limiting the experience of Users that only rely on reviews to influence their purchasing decisions. Additionally, new technologies may not have any reviews or recommendations resulting in a limited understanding of the product before purchase.
2. Limited customization – Many products are no longer customizable limiting User selections and reducing personalization and tailoring of products to specific User needs.

3. Locality delays – Depending on the User's location, shipping services may take longer resulting in potentially significant and localized delays.
4. Technical barriers – Digital literacy is not entirely widespread. Users may have trouble navigating a Supplier site. The User may be unable to find a product due to selective search engines. Ordering interfaces are generally all digital with a decrease in physical retail stores over the last few years. If an internet connection is unavailable, ordering and product availability will be limited.
5. Inadequate customer or product support – Users may be satisfied with a product until it is damaged, or a particular component fails. Oftentimes, Users are unable to repair the product themselves and may be left with a difficult choice to either replace or attempt an uninformed repair. Users may also experience difficulties interacting with Supplier customer service when experiencing difficulties or questions with a particular product or service.
6. Poor communication networks – Users may be unable to communicate their needs adequately or accurately to Suppliers.

Issues (Military):

1. Security concerns – Supply network security is paramount in military operations where the location and nature of shipment is to remain confidential.
2. Rigid hierarchal processes – Military chain of command is critical for military success.
3. Disruptions with change of command – Frequent change of command, may result in a possible disruption as that new leader is brough up to speed or priorities change.
4. Limited flexibility – Military actions are heavily regulated by law and United States command.

5. Conflict area barriers – Military Users that are engaged in active conflict or currently within the boundaries of a conflict zone are subject to the security and safety measures put forth by the country's Military command. The influx and outflux of materials for User needs may be surveilled or impacted due to enemy interference.

Driver: Resources

Focus: To ensure availability, sustainability, and affordability through ethical sourcing at the consumer (User) level of resource allocation through purchasing behavior.

Issues (Civilian):

1. Unethical resource acquisition practices – Users may be either unaware or unconcerned with the source of their supply. Unethical practices can be masked or disguised by Suppliers unknowingly implicating participating Users.
2. Resource scarcity – A reliance on non-renewable resources or slow to replenish resources results in the depletion of that resource for future generations. Generally, this overuse is driven by User demand.
3. Improper storage – Of materials can result in unwanted environmental contamination or an accumulation of unnecessary waste if the improper storage technique resulted in damage or in operability.

Issues (Military):

1. Inaccurate resource forecasting – User needs are difficult to predict in conflict environments resulting in potential waste from unused items and unique needs due to conflict related damage. Additionally, when removing military personnel from active conflict sites, personnel the priority over potential materiel left behind.
2. Antiquated record management/software – Old software systems often require large server rooms to maintain old data in a secure environment. These server rooms are energy intensive and not especially cost effective for long term data storage.
3. Environmental Impact of Combat – Combat related munitions waste is inherent to active conflict areas or activities.

Driver: Processes

Focus: To create an efficient, convenient, and streamline process for utilization of purchased goods with point of use visibility and communication at each step of the supply network.

Issues (Civilian):

1. Data security concerns – Users have been victims of cybersecurity leaks of critical information.
2. Price volatility – Suppliers may increase the price of critical items during an unforeseen circumstance. Users may be victims of price-gouging to acquire critical items.
3. Unreliable supply – Supply can be unreliable depending on shipping or customs issues if the item is traveling internationally. Additionally, if the User requires items that are closely linked with a natural resource that resource supply is prone to change.

4. Complex ordering systems – Users may experience difficulty with ordering interfaces limiting their ability to acquire necessary items.
5. Inconsistent product quality – Product recalls and product contamination due to improper quality control is detrimental to critical User supplies.
6. Inaccurate product information – Users may be lied to by Suppliers and receive items that are not as they were either described or advertised.
7. Limited funds – User needs may exceed User funds.

Issues (Military):

1. Predetermined and inflexible budget allocations – Military budgets are determined well in advance of conflict or DOD actions. Due to financial predetermination, dynamic financial changes must be approved through complex and oftentimes lengthy processes.
2. Limited access to resources due to conflict – Depending on the conflict area, new materials may be difficult to source and require additional funds to procure after deployment.
3. Inflexibility in choosing Suppliers – Military Users must first determine if their needs can be met utilizing existing defense contracts. This can leaves military Users with limited Supplier options and higher costs from Suppliers with guaranteed use contracts.

3.3.3 Tension Identification (Step 1c)

A Tension is a conflict or exacerbating relationship between two Issues and can represent a possible Dilemma (Yadav, Das et al. 2017). The Tensions are best organized in a matrix to facilitate visualization with the Issues and respective Driver categories on the x and y axis as illustrated in Table 3.1 through 3.4. After the Tensions are identified, they are grouped, if possible, by topic and prioritized based on the impact to either Function, Behavior, or Structure.

Tensions – Government Stakeholder

The following include the Tensions related to the Government stakeholder based on the Driver of People, Processes, or Resources. The Tension number corresponds to the number within the associated Tension Matrix see Table 3.1.

Table 3.1: Government Stakeholder Tension Matrix

GOVERNMENT		People						Processes				
		Inequality	Low Public Trust	Resistance to Change	Extremism/ Terrorism	Corruption	Misinformation	Antiquated Policies	Slow to Change	Prioritizing Security	Cybersecurity	Prior Authorized Funds
Resources	Environmental Issues	1		2				3	4			5
	Fossil Fuel Reliance			6					7			
	Resource Conflicts									8		
	Excessive Consumer Demand						9					
	Outdated Infrastructure/ Equipment								10			
Processes	Antiquated Policies					11						
	Slow to Change		12									
	Prioritizing Security			13								
	Cybersecurity				14							
	Prior Authorized Funds											

<u>Tension 1 (G1)</u>: Between environmental concerns and generalized systemic inequality: The Government can exacerbate unequal treatment of the communities it serves in relation to environmental management and equality worsening localized environmental concerns.

<u>Tension 2 (G2)</u>: Between environmental concerns and cultural resistance to change: The Government is culturally slow to change and requires complex and systemic structure changes to

enact these changes. Concerns related to disruption are typically dynamic and require a variety of responses. Since the Government's culture has a tendency for rigidity it may not be able to meet these dynamic needs presented in environmental concerns.

<u>Tension 3 (G3)</u>: Between environmental concerns and antiquated policies: Similar to Tension 2, the structure and complex bureaucracy of enacting change in the Government is often difficult, old established policies are often left in place due to the legislative hurdle of required to get new policies approved.

<u>Tension 4 (G4)</u>: Between environmental concerns and slow to change: This Tension is also similar to Tensions 2 and 3, but this Tension represents the relationship between approved legislation and legislative action. Once a new law is introduced and approved, the time it takes to disseminate these new rules and policies into action within a potentially antiquated structure can place added time into responding to issues.

<u>Tension 5 (G5)</u>: Between environmental concerns and prior authorized funds: When met with an unexpectedly devastating or unexpected environmental disaster, governmental funds are already allocated for a certain severity of potential need at the beginning of the year. If the environmental issue is larger or smaller than expected these funds are either insufficient to remedy the situation or potentially stuck in their account assignment requiring further governmental steps to move these funds elsewhere.

Tension 6 (G6): Between fossil fuel reliance and cultural resistance to change: The United States has a long history of fossil fuel use, and it is often heavily engrained in the culture of the country. To move away from fossil fuels towards renewable energy would require a cultural shift.

Tension 7 (G7): Between fossil fuel reliance and slow to change: Since the Government is deeply engaged in the utilization and production of fossil fuels many of its processes today are dependent on these energy sources. The processes currently used by the Government are intertwined with fossil fuels.

Tension 8 (G8): Between environmentally related resource concerns and prioritizing security: Depending on the current global situation the Government may pivot resource sources to areas that are less dangerous for extraction but do not necessarily represent the most environmentally conscious method.

Tension 9 (G9): Between excessive consumer demand and misinformation: Consumer demand can be managed by the Government in the event of a crisis. However, the fear of sacristy or the proliferation of widespread misinformation regarding critical Government resources can cause excessive consumer demand resulting in unnecessary environmental waste. Misinformation can create a fear-based consumer environment affecting critical Government resources.

Tension 10 (G10): Between outdated infrastructure/equipment and slow to change: Processes in the Government are often slow to change when met with new types of technologies. This results in the potential accumulation of outdated equipment and infrastructure setups in governmental sites. The older infrastructure and equipment can also result in a more negative environmental impact as they are usually relics of a less environmentally conscious time and lack the necessary technology to reduce their impact (Office of the Under Secretary of Defense for Acquisition and Sustainment, 2019).

Tension 11 (G11): Between antiquated policies and corruption: Antiquated policies can open the Government up to potential loopholes for corruption activities.

Tension 12 (G12): Between slow to change and low public trust: Oftentimes depending on the person, they may have a low opinion of the Government and the institutions it represents. Whether from personal experience or political ideology, an individual's trust in the Government is heavily impacted by their beliefs and culture. Since the processes of the Government are slow to change, that slow pace may be a catalyst in furthering low public trust, while on the other hand a new policy if changing enough from the old process may be met with low trust due to the change itself.

Tension 13 (G13): Between prioritizing security and resistance to change: After the September 11th terrorist attacks, many of the Government's processes as it relates to security changed. Many of the Government's resources are now devoted to security to bolster national defense and security. This prioritization of security has produced a culture of security first that can produce a resistance to change. These changes have the potential to be seen as an affront to security efforts and a potential vulnerability. While this culture has maintained the Government's superiority in securing many different sectors of the country, its perpetuation of a culture of resistance to change can further rigidify governmental processes.

Tension 14 (G14): Between cybersecurity initiatives and extremism and terrorism: Cybersecurity is a huge portion of Government security efforts in all sectors. Unfortunately, as extremism and terrorism continue to increase, so must cybersecurity. However, to secure Government cyber systems, cybersecurity initiatives have made digital processes more complex and less able to dynamically respond to changes.

Tensions – Supplier Stakeholder

The following include the Tensions related to the Supplier stakeholder based on the Driver of People, Processes, or Resources. The Tension number corresponds to the number within the associated Tension Matrix see Table 3.2.

Table 3.2: Supplier Stakeholder Tension Matrix

SUPPLIERS		People					Processes						
		Stock Market Impacts	Workforce Diversity	Skills Gap	Profit Focus	Public Trust	Dynamic Acquisition	Inefficient/ Inflexible Policies	Cybersecurity	Inventory Management	Quality Control	Tech Integration	Capacity/ Speed Constraints
Resources	Fluctuating Demand						1			2			
	Global Market Volatility	3											
	Regulatory Compliance										4		
	Logistics Challenges							5	6				
	Safety and Quality				7								8
	Need for Sustainable Practices				9			10					
Processes	Inefficient or Inflexible Policies		11										
	Cybersecurity												
	Inventory Management												
	Quality Control					12							
	Tech Integration			13									
	Capacity/Speed Constraints												

<u>Tension 1 (S1)</u>: Between fluctuating demand and dynamic acquisition: Suppliers are often flexible and dynamic in their processes for the acquisition of new business ventures or products. This ability to make quick decisions can have either positive or negative impacts on the Supplier depending on the demand for that newly acquired item. That product may not remain in demand long after its acquisition presenting that Supplier with a potential business loss.

<u>Tension 2 (S2)</u>: Between fluctuating demand and poor inventory management: Depending on how the demand of products relates to the amount of product a Supplier has on hand the available product could exceed their current processes of managing that inventory. Additionally, if the Supplier is unable to appropriately manage inventory for potential demand surges, they could be presented with either damaged items, low stock, or missing inventory resulting in profit loss.

<u>Tension 3 (S3)</u>: Between global market volatility and stock market impacts: The stock market can be impacted by unexpected and anticipated global events. Suppliers that engage in an open

market or public stock exchange with their shareholders can experience business losses based on global events that may have little to do with their industry. These stock market impacts can devalue a business' performance in the larger economy and result in a potential weakening of monetary power. While the stock market is not the only or likely the primary determinate of supplier financial viability or investment the impacts can have wider implications depending on User and Government responses to changing stock market performance.

<u>Tension 4 (S4)</u>: Between unmet regulatory compliance and supplier set quality control: Every Supplier has internal measures of quality control. Generally, these internal standards align with wider regulatory control measures. However, a Tension presents itself when the regulatory body enacts quality measures that exceed the Suppliers established processes. These additional quality inspections can result in slower process throughput and pose a potential limitation on that product line until regulatory compliance is reestablished.

<u>Tension 5 (S5)</u>: Between logistics challenges and inefficient or inflexible policies: Logistics challenges are one of the main sources of unpredictability present in the supply network because it involves the interaction of many different variables. If a Supplier has inefficient or inflexible policies that cannot respond to or anticipate any potential logistics challenges either for supplies required in the Supplier processes or for the movement of product after production the resulting impact to a business can be catastrophic.

Tension 6 (S6): Between logistics challenges and cybersecurity: Visibility is often one method of overcoming and anticipating logistics challenges, however, given cybersecurity concerns visibility is not always possible. Cybersecurity can limit visibility in key industries due to security concerns over cyber networks and potential vulnerabilities that could be exposed with additional visibility.

Tension 7 (S7): Between safety and quality and profit focus: The Tension between safety and quality and profit focused culture has real implications that can even cost lives. If profit is the sole cultural focus of a Supplier safety and quality may suffer at the expense of a better bottom line.

Tension 8 (S8): Between safety and quality and compacity or speed constraints: As a Supplier ramps up production due to demand, their speed may exceed their quality and safety measures currently in place.

Tension 9 (S9): Between few sustainable practices and profit focused culture: Sustainability in business, when just beginning, does not necessarily result in the most profitable options for Suppliers. Oftentimes Suppliers forgo developing these more sustainable options because their viability is longer-term than what their quarterly projections need to reflect. If the culture of the Supplier is only focused on profitability, sustainability may not be a large priority.

Tension 10 (S10): Between few sustainable practices and inefficient or inflexible policies: If existing policies produce procedures that are inefficient or wasteful in their use of or disposal of unused resources not addressing these processes will result in both monetary and environmental issues.

Tension 11 (S11): Between inefficient or inflexible policies and low workforce diversity: When Suppliers limit their hiring practices, diversity of thought can be lower, and inefficiencies and inflexibility may go unnoticed. Additionally, the ability to acquire and retain a diverse workforce when status-quo policies are preferred over new ideas could result in these perspectives finding outside opportunities.

Tension 12 (S12): Between low public trust and poor quality control: Public trust may have an incongruous relationship with a Supplier's quality. For example, Suppliers may have experienced many years of quality production but recently are producing lower quality items and relying on high public trust to maintain demand. The opposite may also be true, that if a Supplier has a history of producing low quality items public perception may be unable to adapt when their production quality increases.

Tension 13 (S13): Between poor technology integration and workforce skills gap: As new technologies increase and continue to advance more cost effective and innovative processes, the skills gaps within established workforces may be a barrier to new technology integration into existing processes.

Tensions – Civilian User Stakeholder

The following include the Tensions related to the civilian User stakeholder based on the Driver of People, Processes, or Resources. The Tension number corresponds to the number within the associated Tension Matrix see Table 3.3.

Table 3.3: Civilian User Stakeholder Tension Matrix

USERS - CIVILIAN		People						Processes						
		Lack of Reviews	Limited Customization	Locality Delays	Technical Barriers	Inadequate Product Support	Poor Communication Networks	Data Security Concerns	Price Volatility	Unreliable Supply	Complex Ordering Systems	Inconsistent Quality	Inaccurate Product Information	Limited Funds
Resources	Unethical Resource Acquisition									1			2	3
	Resource Scarcity		4	5					6			7		
	Improper Storage						8							
Processes	Data Security Concerns													
	Price Volatility													
	Unreliable Supply			9										
	Complex Ordering Systems				10									
	Inconsistent Quality					11								
	Inaccurate Product Information	12												
	Limited Funds			13										

<u>Tension 1 (CU1)</u>: Unethical resource acquisition and unreliable supply: When supplies are infrequent or affected by limiting events like natural disasters or conflict, Users may reach out to less reputable sources for their needs.

Tension 2 (CU2): Between ethical resource acquisition and inaccurate product information: Users may be unable to differentiate between potential Suppliers due to limited regulation on information required to present to customers. For example, a product may say that it is “fair trade” or “ethically sourced” but if the User is unable to determine if these words are backed up with regulatory compliance, the User may be misled.

Tension 3 (CU3): Between unethical resource acquisition and limited funds: Depending on the User's priorities when seeking out supply or resources, they may favor a lower cost option versus a sustainable ethical alternative.

Tension 4 (CU4): Between resource scarcity and limited customization: Users may require certain resources that are either difficult to obtain, slow to replenish, or short in supply. These resources present potential constraints in the User’s goals. Additionally, the User’s ability to customize these products to their specific needs may be impossible resulting in more User modification after purchase.

Tension 5 (CU5): Between resource scarcity and locality delays: If a User is located in a difficult to reach area or is very far from their supply, locality may present unique Tensions in the acquisition of Supplier goods. Also, if the User location requires multiple modes of transportation to receive products, there is usually additional lead time affecting surge capacity.

Tension 6 (CU6): Between price volatility and resource scarcity: The rarer and more critical a resource is for User operations the more vulnerable that User is for price volatility from Suppliers. If the User must have that product the User is subjected to what that particular Supplier charges.

Tension 7 (CU7): Between inconsistent quality and resource scarcity: If a User is unable to choose from a variety of Supplier options and the resource is not well regulated, the product received may be of varying quality.

Tension 8 (CU8): Between improper storage and poor communication networks: It is critical that a User must maintain visibility and correct inventory of their products. If the communication network is not able to provide necessary information and staff is not properly trained and incentivized for its use, the storage of critical supplies may be at risk of damage or repeated unnecessary purchases.

Tension 9 (CU9): Between unreliable supply and locality delays: If a User is located in a difficult to reach area and that resource has a historically unreliable supply that User may be left without critical items due to these compounding delays.

Tension 10 (CU10): Between complex ordering systems and technical barriers: Users that must rely on digital ordering for supplies can have trouble ordering from Suppliers if their digital systems are unable to interface with a Supplier ordering site. For example, if the User has unreliable internet services or is untrained in utilizing digital systems, they will be unable to communicate needs and orders to a Supplier.

Tension 11 (CU11): Between inconsistent quality and inadequate product support: When User's experience quality issues with a supply they usually reach out to the Supplier for a replacement or other remedy. If the User cannot receive support with a replacement part or repair kit for modification of the received item, they experience a loss of capability and financial investment.

Tension 12 (CU12): Between limited product information and lack of reviews: Oftentimes Users rely on customer reviews to help guide their purchasing decisions. If the product is well reviewed the User may be falsely convinced of that product's quality or resourcefulness, or even if a product has few reviews may seem like an untrustworthy product choice leading the User to another Supplier. Additionally, reviews can be artificially inflated by Supplier interference to mislead Users.

Tension 13 (CU13): Between locality delays and limited funds: Users do not have unlimited funding sources. These funds are usually carefully allotted for certain purchases. If these purchases require shipping and the locality of the User results in a higher cost to purchase, the User may be unable to fund the acquisition of certain resources.

Tensions – Military User Stakeholder

The following include the Tensions related to the military User stakeholder based on the Driver of People, Processes, or Resources. The Tension number corresponds to the number within the associated Tension Matrix see Table 3.4.

Table 3.4: Military User Stakeholder Tension Matrix

USERS - MILITARY					Processes		
		Rigid Hierarchy	Changing of Command	Conflict Area Barriers	Inflexible Budget	Conflict Limited Resource Access	Inflexible Supplier Options
Resources	Inaccurate Resource Forecasting				1	2	
	Antiquated Record Management		3				
	Environmental Impact of Combat			4		5	
Processes	Inflexible Budget		6				
	Conflict Limited Resource Access						
	Inflexible Supplier Options	7					

<u>Tension 1 (MU1)</u>: Between inaccurate resource forecasting and inflexible budget: Since military Users are required to forecast their needs based on a preauthorization of funds every year, if these needs change the budget is unable to dynamically respond or adjust to compensate. Additionally, if these needs are overestimated the funds are generally bureaucratically locked in that particular use requiring additional time and effort to reallocate as needed.

Tension 2 (MU2): Between inaccurate resource forecasting and conflict limited resource access: Military Users may be actively engaged in combat activities. These combat activities can result in unpredictable resource damage. If forecasting is not accurately predicted and the military User is currently in an active combat zone, these Users will be unable to support their activities.

Tension 3 (MU3): Between outdated record management and frequent changing command: If changing of command is a frequent and met with outdated record management systems the result can be inaccurate resource forecasting, limited supply, duplicate orders, unnecessary and unutilized excess.

Tension 4 (MU4): Between environmental impact of conflict and conflict area barriers: Conflict can be inherently impactful to the environment whether due to direct troop movement, munitions waste, or destruction of infrastructure amongst other factors. However, as this relates to supply networks, conflict can reduce a military User's options for selecting an environmentally conscious supply choice.

Tension 5 (MU5): Between environmental impact of combat and conflict limited resource access: This Tension is similar to Tension 4. Depending on the conflict's location, the environmental effects of combat on an area can increase that location's negative environmental state and reduce overall supply out of that conflict area. This is especially impactful when these area conflicts occur in a location that produces a product that is in high demand or requires unique features only present in that location.

Tension 6 (MU6): Between inflexible budget and changing command: Military Users can be presented with frequent and wide sweeping command changes that have the potential to alter an organization's priorities. While the ultimate priority of sustained national security each person can be different in how they approach that task. Since military Users have strict budget allocations and limited flexibility, the new commander may be unable to enact their priorities because of an inflexible preauthorization of available funds based on a previous commander's choices.

Tension 7 (MU7): Between inflexible Supplier options and rigid hierarchy: As previously discussed, military Users have strict processes that limit their ability to receive and purchase from certain Suppliers. In addition to these strict processes, the culture of military Users is based on a strict adherence to the chain of command with the higher ranks having authority over the lower ranks each generally communicating with one rank above and one rank below to disseminate information. This hierarchal personnel structure requires a multilevel approval process for purchases and process approval, with the potential for slowing down the system and limiting the available options. To divert from previously authorized Suppliers, the higher ranks must be involved and approve of the new Supplier through a potentially complex and time-intensive approval process.

3.3.4 Dilemma Identification

Dilemma identification is discussed and recorded by stakeholder in their respective Tension matrices in Table 3.5 through 3.8. The Dilemmas identified are not exhaustive and currently encompass the analysis and perspectives put forth in this chapter. There are several other Tensions and Dilemmas that could be considered in the context of this analysis.

Tension Groupings, Prioritization and Dilemma Identification – Government

The following includes the grouped Tensions and highlights Government Dilemmas (GD) based on the Tensions identified in Section 3.3.3. The Dilemma number corresponds to the number within the associated Dilemma Matrix see Table 3.5.

Table 3.5: Dilemma Identification for Government

GOVERNMENT		People						Processes				
		Inequality	Low Public Trust	Resistance to Change	Extremism/ Terrorism	Corruption	Misinformation	Antiquated Policies	Slow to Change	Prioritizing Security	Cybersecurity	Prior Authorized Funds
Resources	Environmental Issues	1 (GD1)		2 (GD1)				3 (GD2)	4 (GD2)			5 (GD2)
	Fossil Fuel Reliance			6 (GD1)					7 (GD2)			
	Resource Conflicts									8 (GD3)		
	Excessive Consumer Demand						9					
	Outdated Infrastructure/ Equipment								10			
Processes	Antiquated Policies					11						
	Slow to Change		12									
	Prioritizing Security			13 (GD3)								
	Cybersecurity				14 (GD3)							
	Prior Authorized Funds											

<u>Government Dilemma 1 (GD1): Tension 1, Tension 2, and Tension 6</u> –These Tensions focus on the cultural barriers within the Government and their interactions with environmental issues. The complexity of these systems and historical culture that is resistant to change has benefited only some individuals within that system presents a Dilemma as that system relates to continuing environmental issues with increasing complexity and destruction requiring a cultural shift towards sustainability.

Government Dilemma 2 (GD2): Tension 3, Tension 4, Tension 5, and Tension 7 – These Tensions group to form a Dilemma between the Government's need to respond quickly to environmental issues that require a change in processes within structures that inherently require consistency and long-term solutions. Government systems are historically slow to change and require many bureaucratic checks-and-balances in order to enact change. These checks-and-balances are meant to ensure continued and long-lasting success of Government processes, but these same processes meant for longevity can result in slower response times and complexity that make dynamic responses difficult.

Government Dilemma 3 (GD3): Tension 8, Tension 13, Tension 14 – These Tensions are focused on how national security efforts can create issues in dynamic responses to different events that occur in the supply network. The Government relies on a secure environment within all sectors of influence and control. From border or physical security that can impede the distribution of goods at ports and borders due to necessary customs and immigration laws to cybersecurity efforts that limit changes to cyber networks and potentially eliminate new technology adoption due to limited security features. Even security initiatives within the social domain can limit international collaboration to reduce foreign influence. These Tensions result in a Dilemma between the Government's need for control and security that can acts as a limiting factor in the adoption of new technologies, international collaboration, or the smooth movement of goods.

Tension 9 – Tension 9 involves the impact of misinformation on unregulated consumer demand. This does not represent a Dilemma because this can be prevented by ensuring an organized and consistent response that is widely disseminated to the public in times of disruption. By maintaining a reliable stream of information from a reputable Government-controlled source the effect of misinformation while uncontrollable can be less severe.

Tension 10, Tension 11, and Tension 12 – These Tensions have a focus on how the public interacts with and has beliefs about the Government. Since governmental systems are slow to change and include many antiquated processes and structures, the public can take these features and attribute them to label the country as having an ineffective Government. Additionally, lone "bad actors" within the Government can cause the public to generalize all Government organizations and personnel as corrupt. This while similar to the Dilemma presented in the grouping of Tensions 3,4, 5 and 7, this particular grouping does not result in a Dilemma. By adding visibility into Government processes and following through on promises, the Government can continue its long-term processes with visibility and justification to the public. For example, if a new highway is needed in a community and the process is complex and slow to begin, timely and consistent updates to the public can help to redefine the Government's action and commitment to the community.

Tension Groupings, Prioritization and Dilemma Identification – Suppliers

The following includes the grouped Tensions and highlights Supplier Dilemmas (SD) based on the Tensions identified in Section 3.3.3. The Dilemma number corresponds to the number within the associated Dilemma Matrix see Table 3.6.

Table 3.6: Dilemma Identification for Suppliers

SUPPLIERS		People					Processes						
		Stock Market Impacts	Workforce Diversity	Skills Gap	Profit Focus	Public Trust	Dynamic Acquisition	Inefficient/ Inflexible Policies	Cybersecurity	Inventory Management	Quality Control	Tech Integration	Capacity/ Speed Constraints
Resources	Fluctuating Demand						1 (SD1)			2 (SD1)			
	Global Market Volatility	3 (SD1)											
	Regulatory Compliance										4 (SD2)		
	Logistics Challenges							5 (SD3)	6				
	Safety and Quality				7 (SD4)								8 (SD2)
	Need for Sustainable Practices				9 (SD4)			10 (SD3)					
Processes	Inefficient or Inflexible Policies		11										
	Cybersecurity												
	Inventory Management												
	Quality Control					12 (SD2)							
	Tech Integration			13									
	Capacity/Speed Constraints												

<u>Supplier Dilemma 1 (SD1): Tension 1, Tension 2, and Tension 3</u> – The focus of these Tensions is that Suppliers are subject to very dynamic relationships between their customers and their subsequent global performance as it relates to the stock market. While this Dilemma is not especially strong as inherent profitability drives reinvestment oftentimes as a precursor to stock performance, publicly traded Suppliers can experience devastating public impacts to their stock performance if consumer demand fluctuates. That stock price can result in layoffs, stakeholder changes, and even major interventions but not necessarily reflect poor business performance. These Tensions form a Dilemma because it is common that customer demand can fluctuate and participation in the stock market can open businesses up to larger resources and visibility but the impact of stock performance and customer buying power may be inconsistent with actual Supplier performance.

Supplier Dilemma 2 (SD2): Tension 4, Tension 8, and Tension 12 – These Tensions have a theme of quality in a high-speed high-quality production environment. Many Suppliers benefit from a fast production line to get their product to Users; however, that speed can result in lower quality items if not carefully and systematically monitored along the speed-up process. Users may value a quicker production speed but can be disappointed when these products are of low quality leading to a decrease in public trust in the Supplier. This Dilemma is further compounded with the quality measures that have regulatory compliance requirements. Failure to meet these regulatory requirements can result in the disqualification of a Supplier from producing that item for sale. Ultimately, this Dilemma theme focuses on the Tensions between speedy production and quality requirements.

Supplier Dilemma 3 (SD3): Tension 5 and Tension 10 – Many Suppliers have strict policies and procedures that may be many decades old depending on the age of the company. While these policies and procedures were effective in managing business activities in the past, they may lack the flexibility necessary to meet a dynamic environmental challenge or logistical challenge in the present. A Dilemma is formed when the Supplier relies on preexisting historical policies and procedures that have made them successful that do not represent the most sustainable option or the most flexible structure to meet a continually changing environment. Changing these historically successful policies will require a revaluation of Supplier priorities.

Tension 6 – Cybersecurity is critical to maintaining an organization's information from leaking to competitors or possibly being utilized for crime. These cybersecurity networks can potentially impede Supplier visibility in key portions of production by sequestering databases or compartmentalizing automated processes from each other. This Tension does not necessarily result in a Dilemma because through integrating different software or altering a cybersecurity system to allow for more visibility and control can mitigate this problem.

Supplier Dilemma 4 (SD4): Tensions 7 and Tension 9 – These Tensions include the theme of profit focused culture. Many Suppliers consider their financial portfolio bottom-line as their main priority and disregard many elements of sustainability or equality. A focus on pure profit can perpetuate systems of oppression and environmental mismanagement all for the sake of money. This culture puts profit above any other business priority and presents a Dilemma. The Dilemma is between a profit focus which is currently one of the main measurements of a Supplier's success with a desire for more ethically and sustainably acquired resource based on tradeoff decisions.

Tension 11 – Oftentimes antiquated policies that are inefficient or ineffective can be perpetuated by homogenous workforces with a low influx of new outside perspectives. While this can be a major roadblock to Supplier successes and reactions to change, it is not a Dilemma. By enacting an open chain of communication for new ideas that can be submitted anonymously to management and reevaluating the hiring criteria for new employees both dissenting ideas and new perspectives can be infused into the Supplier employee network. Incentivized process improvement programs can help encourage employees to reevaluate existing procedures and provide suggestions for more efficient and effective processes.

Tension 13 – New technology integration always has a learning curve as existing employees reorient themselves to a new process or system, but not having proper workforce training to address potential skills gaps can make the new technology less effective. While this presents a problem for Suppliers to integrate new technologies into existing systems, it is not a Dilemma. By introducing and enacting an employee cross training program to develop new skills for seasoned workers and on the job training opportunities for new employees the skills gap can be closed.

Tension Groupings, Prioritization and Dilemma Identification – Civilian Users

The following includes the grouped Tensions and highlights civilian User Dilemmas (CUD) based on the Tensions identified in Section 3.3.3. The Dilemma number corresponds to the number within the associated Dilemma Matrix see Table 3.7.

Table 3.7: Dilemma Identification for Civilian Users

USERS - CIVILIAN		People						Processes						
		Lack of Reviews	Limited Customization	Locality Delays	Technical Barriers	Inadequate Product Support	Poor Communication Networks	Data Security Concerns	Price Volatility	Unreliable Supply	Complex Ordering Systems	Inconsistent Quality	Inaccurate Product Information	Limited Funds
Resource	Unethical Resource Acquisition									1 (CUD1)			2 (CUD1)	3 (CUD1)
	Resource Scarcity		4 (CUD2)	5 (CUD3)					6 (CUD2)			7 (CUD4)		
	Improper Storage						8							
Processes	Data Security Concerns													
	Price Volatility													
	Unreliable Supply			9 (CUD3)										
	Complex Ordering Systems				10									
	Inconsistent Quality					11								
	Inaccurate Product Information	12												
	Limited Funds			13 (CUD3)										

<u>Civilian User Dilemma 1 (CUD1): Tension 1, Tension 2, and Tension 3</u> – The focus of these Tensions is a User's endorsement or engagement in unethical resource acquisition either through a desire to mitigate an unreliable supply, unknowing participation due to lack of information, or a lack of funds available limiting a User's choice of Supplier. The User is presented with a Dilemma when considering limited funds, but not necessarily unknowing participation because that could be remedied with additional research or diversifying their Supplier base for unreliable supply. The Dilemma is present for Users if their budget only allocates a certain amount of money for a purchase and the purchase of a more environmentally or ethically sourced product exceeds their budgetary allotment. If sustainability may not be "worth" the extra investment of funds the User will likely perpetuate a system that is not based in sustainability.

<u>Civilian User Dilemma 2 (CUD2): Tension 4 and Tension 6</u> – Resource scarcity is a major complication for Users in two major ways: limited customization and price volatility. In a resource scarce environment, the User must either accept the item as is and complete custom modification in house or with another Supplier or pay the price the Supplier sets due to limited options. If the item can be less scarce due to a diversification of Supplier this grouping would remain Tensions and not Dilemmas. However, in a sole source situation the User is unable to

reach out to other Suppliers for this item and may be only able to accept the conditions that a particular Supplier creates. The Dilemma is created when the User cannot afford the Supplier's set price, reach out to a different Supplier, or modify that item in-house to complete User tasks.

Civilian User Dilemma 3 (CUD3): Tension 5, Tension 9, and Tension 13 – The User's location determines much of what comes in and out of that User's operations. For this group of Tensions, the focus is on how User location can create Dilemmas within the supply network. Depending on the User's designated operations, whether dynamic and mobile or structured and stationary, their location can create a Dilemma. The Dilemma present for User locations that are structured and stationery is that Users must have their necessary supplies delivered to them in a potentially difficult to access or at a long-distance location. These items will likely also increase in price due to that added location complexity but in this situation the User cannot move to accommodate these issues. In the other case where the User's location is dynamic and mobile, recurring orders are difficult to maintain consistency or any level of automation when the User must manually enter location data for each shipment. Depending on a User's location, the locality delays may worsen resource scarcity and unreliable supplies while increasing User costs.

Civilian User Dilemma 4 (CUD4): Tension 7 – This Tension includes the interactions between resource scarcity and inconsistent quality. This Tension also presents a Dilemma for Users unable to acquire higher quality critical items due to limited Supplier options possibly impacting the User operations. If the User is unable to find a different Supplier due to resource scarcity, they must mitigate the low quality another way.

Tension 8 – The Tension present between communication networks and improper storage can be mitigated by introducing a storage tracking system with the capability to update any relevant parties within the User group and therefore is not a Dilemma.

Tension 10, Tension 11, and Tension 12 – While this Tension grouping has a theme of issues with communication between Users and Suppliers. Users are not able to control Supplier systems and only provide feedback for consideration. These Tensions do not represent a Dilemma because if a new Supplier is able to be found with an easier communication system the User should be able to divert their energies to that new Supplier. Additionally, Tensions related to User error or lack of understanding can be mitigated through digital literacy training and detailed instructions from Suppliers.

Tension Groupings, Prioritization and Dilemma Identification – Military Users

The following includes the grouped Tensions and highlights military User Dilemmas (MUD) based on the Tensions identified in Section 3.3.3. The Dilemma number corresponds to the number within the associated Dilemma Matrix see Table 3.8.

Table 3.8: Dilemma Identification for Military User

USERS - MILITARY					Processes		
		Rigid Hierarchy	Changing of Command	Conflict Area Barriers	Inflexible Budget	Conflict Limited Resource Access	Inflexible Supplier Options
Resources	Inaccurate Resource Forecasting				1 (MUD1)	2 (MUD2)	
	Antiquated Record Management		3				
	Environmental Impact of Combat			4 (MUD2)		5 (MUD2)	
Processes	Inflexible Budget		6 (MUD3)				
	Conflict Limited Resource Access						
	Inflexible Supplier Options	7 (MUD3)					

Military User Dilemma 1 (MUD1): Tension 1 – Military Users receive funding allocations from their sponsoring country or Government. For this reason, the funding is generally allocated at the beginning of the year based on forecasting provided by the leadership. While this funding system results in appropriate allocation to the military while considering the wider funding needs of the country, military Users are subjected to inflexible budget restrictions once funding has been awarded. This rigid budget structure limits military User flexibility to dynamically adapt funding depending on new technology introduction, combat activities, and changing military landscapes. This results in a Dilemma because the country cannot only fund the military within the Government's other funding needs impacting the flexibility military Users need.

Military User Dilemma 2 (MUD2): Tension 2, Tension 4, and Tension 5 – The impact of combat on areas where Users receive and rely on for supplies cannot be ignored. Combat can exacerbate environmental issues and further impede critical supply networks in these areas. This presents a Dilemma for the military User. It is the duty of the military User to engage in combat activities for the country they represent for a variety of reasons, however combat can have widespread and potentially negative impacts on supply lines that may be critical for the continuation and support of these compact activities.

Tension 3 – Record management is critical for any military User. While this Tension is critical, it does not represent a Dilemma. Enforcing a consistent and leadership-initiated records management system that is a requirement through military command can eliminate any difficulties presented by a change of command within an existing system.

Military User Dilemma 3: Tension 6 and Tension 7 – The social system within a military User is unique compared to more fluid civilian systems. The rigid chain of command and command hierarchy is a military directive and cannot be deviated from in a military User system. This social hierarchy coupled with the potential for an inflexible budget and inflexible Supplier option pool creates a rigid and standardized response to potentially dynamic disruptions. This structure creates a Dilemma between the necessary chain of command that ensures informed and direct military responses with a varied and unexpected environment full of variations and disruptions within a supply network.

3.4 Managing "The Machine"

The AoP handbook includes the framework for the AFSC's constraint management guidelines and refers to the interactions between People, Processes, and Resources as "The Machine" and the management of that "Machine" is outlined in the need to have visibility and understanding for continuous improvement at every step of a process (AFSC 2023). In Section 3.3, the Dilemma Triangle is used to determine the Dilemmas, or AoP constraints, within each Stakeholder Government, Supplier, and User both military and civilian. The AoP refers to Dilemmas as constraints but in this chapter the term constraints are synonymous with Tensions and Dilemmas are unresolvable Tensions. These Dilemmas will now be "managed" or resolved using the AoP framework as a tool to determine potential solutions or gaps in the existing framework.

3.4.1 The Nested F-B-S Dilemma Triangle

After discovering and defining the Dilemmas within each Stakeholder, potential overlaps and opportunities to tie these Dilemmas to the F-B-S construct are revealed. Discussing and analyzing how each Stakeholder performs or interacts with another as it relates to their F-B-S Dilemmas will help to define the problem space and develop the connection to a Requirements List for a fail-safe supply network.

3.4.2 Function Dilemmas

As mentioned in Section 3.1, for the purposes of this analysis, the Function of Government, Supplier, and User remain fixed, but as Stakeholders interact Tensions are created and in turn represent potential Dilemmas. The Dilemmas related to Function are GD3, SD1, SD2, UD1, UD2 and MUD2 displayed in Figure 3.5.

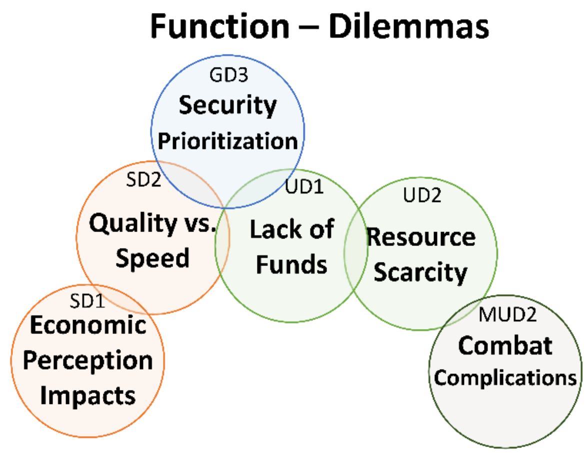

Figure 3.5: Dilemmas Related to Function

Their origins and original Tension Matrices are found in Tables 3.5 through 3.8. For Government, the Function is to provide stable national sustainment and security for its communities, citizens, and interests but that emphasis on security can result in a potential Dilemma as it can impact its ability to enact quick acquisition of critical infrastructure or products and potentially roadblock dynamic governmental responses in favor of more secure and lean systems. The Function of Suppliers is to provide material inputs whether services, raw materials, or components. In their quest to supply to meet demand, there are two potential Dilemmas related to quality while prioritizing speed and the potential impact of participating in a publicly tracked company. The Supplier must produce and provide enough product to remain economically viable but, in their quest to meet demand, quality standards can shift downward. Additionally, as a feature of the global economy the Supplier's performance is carefully monitored if publicly traded leading to potential shifts in supply unrelated to demand but simply guided by global performance measures. Lastly, the function of Users is to participate in purchasing and driving demand through product selection. The Function of the User is directly tied to the User's fund availability and the availability of the product. Limited funds can cause Users to purchase less or reach out to lower cost Suppliers. Additionally, resource scarcity coupled with limited funds creates a Dilemma when the User is unable to purchase the only availability supply due to increased cost. Lastly, the function of military Users is to often engage in activities related to national security, if necessary, in the event of a threat. Those activities can result in additional resource scarcity if these areas are a sole source for a particular industry. Each Dilemma arising from Function is closely linked to the defined role or purpose of the stakeholder and how these roles or functions interact within the system.

3.4.3 Behavior Dilemmas

Behavior addresses how the stakeholder or stakeholders behave in order to enact their respective Functions. The Dilemmas related to Behavior: GD1. SD4, UD4, and MUD1 and are displayed in Figure 3.6.

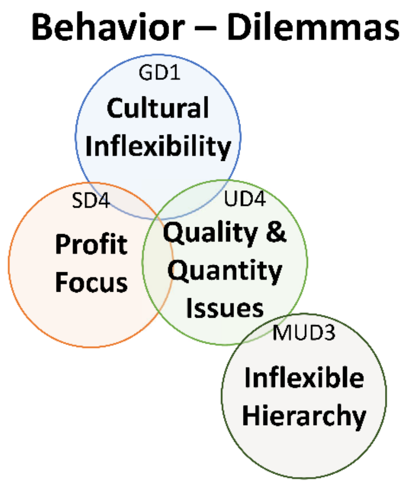

Figure 3.6: Dilemmas Related to Behavior

Their origins and original Tension Matrices are found in Tables 3.5 through 3.8. As previously stated, the Function of Government is to sustain and protect the national interests of its nation for as long as possible if not infinitely. With an infinite mindset, cultural norms within the Government may favor stability or previously successful behaviors. Additionally, Government is deeply connected to the history of a nation and relies on the experiences of older Government institutions and employees to continue the traditions to further national interests. This infusion of long-standing Behaviors presents in a Dilemma when the environment in which the Government operates does not behave in a predictable manner. This inflexibility while maintaining consistency within the governmental systems can result in inaction when the assumptions made to justify that maintenance of Behavior no longer hold true. For Suppliers, their Function as previously stated is to provide supply. This focus on production often leads to a focus on profitability for continued business success. Focusing on profit is essential when aiming for business viability, but only focusing on profit can predispose a Supplier's Behavior to cut corners, lower quality, or resort to questionable and ethically ambiguous business choices. For the User stakeholder, their demand may outweigh the available supply and cause a reduction in quality for the sake of quantity. These quality issues may go unnoticed until final use and may potentially result in system failures within critical User infrastructures. On the other hand, the reliance on a particularly high-quality Supplier may limit a User's access to available quantity, also limiting a User's ability to perform. Lastly, military User behaviors are often rigid and heavily procedurally controlled which is critical when maintaining chain of command and distribution of military critical information through a regimented hierarchy. This hierarchy, while critical to maintaining order can contribute to a reduction in adaptability when presented with unique or unexpected variations or disruptions. These could be a result of low quantity or quality received from Suppliers and can often mirror the inflexibility presented in governmental institutions.

3.4.4 Structure Dilemmas

Structure refers to the different aspects or components within a Stakeholder and their respective relationships with each other. For example, structure can include large regulatory bodies, hierarchies, departments, factories, relationships partners or shareholders, to smalls scale individual preferences. The Dilemmas related to structure: GD2, SD3, UD3, and MUD3 are displayed in Figure 3.7.

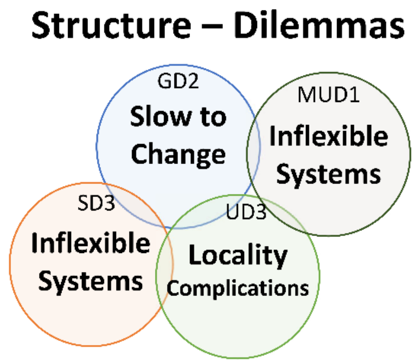

Figure 3.7: Dilemmas Related to Structure

Their origins and original Tension Matrices are found in Tables 3.5 through 3.8. Government is historically and categorically complex. Its systems are far-reaching and include everything in managing and maintaining a country from cross-country highways to public school lunches. Since Government is inherent complex, the systems and means of operation are slow to change and require many checks and balances to be changed. The nature of Government is to be stable and secure and results in a Structure that is slow to change. While effective in long term consistency, this complexity and rigidity leaves the Government without a dynamic system of change management. The Government's difficulty in responding quickly can also have cascading effects on other Stakeholders. For Suppliers, they are often involved or included in corporations that are many decades old and have had successes with a process or management system that has so far proven successful. A history of past business success may entice a Supplier to maintain antiquated or superfluous policies, procedures, or technologies rather than upset the status quo with developing new Structures. Often, too, the addition or change requires an influx of funds that may not be obtainable at that time. Additionally, Suppliers that have specialized in a certain market often have invested heavily in certain geographical regions and are unable to relocate without significant and detrimental impacts to their business. This Dilemma also ties into the

User locality issues. Users are located in a variety of areas depending on their purpose. These locations can add complexity to supply networks if the User is in an especially remote area. These Structure Dilemmas are further compounded by potentially inflexible military User systems. Since the military is a feature of a Government, their structures are often as old as the nation they protect. Antiquated systems are often supported by antiquated assumptions which can impact a military User's ability to reach new Suppliers or dynamically manage their supply networks when presented with new information.

3.4.5 Recommendations for Dilemma Resolutions

Now that the Dilemmas are identified and grouped by Function-Behavior-Structure in Section 3.4 the next step is identifying Requirements to address those zero-sum situations. These Requirements are based on the resolutions to previously uncovered Dilemmas with the goal of creating a fail-safe supply network. Since the Dilemmas are based in their respective Function, Behavior, and Structure, the Requirements also correlate to the F-B-S construct. The F-B-S construct is used as a sorting tool to determine similar Dilemmas between Stakeholders to develop a robust Requirements List that addresses multiple Dilemmas at a time. Those requirements are connected to Dilemma resolutions for each Stakeholder by Function, Behavior or Structure in the subsequent text.

Function Requirements (Summarized in Table 3.9)

For the Function of Government, the theme present in the requirements revolves around ensuring stable national sustainment and security, while also facilitating the rapid acquisition of critical infrastructure or products as needed. This could be done with a merging of defense acquisition and defense sustainment resources and personnel cross training. Flexibility is key to ensuring the development of responsive frameworks within existing systems and potential incentives to effectively balance security requirements with the dynamic nature of governmental responses. For Suppliers, they may need to balance providing consistent material input while upholding strict quality standards and ethical business practices through developing strategies that synergize profitability with the preservation of product quality and integrity. For Users, their ability to access essential products or services, especially for individuals with limited financial resources is crucial. These Users would likely benefit from an emphasis on promoting awareness regarding product selection and impacts of consumption decisions to reduce overconsumption and waste. Military Users face unique challenges, requiring them to maintain operational readiness amidst unforeseen and unpredictable obstacles and disruptions that have national and international implications. They may need to cultivate a culture of repeatable in-policy flexibility and agility within inherently rigid military institutions to effectively adapt to evolving scenarios.

Table 3.9: Summary of Requirements for Function

Government Function
• Ensure stable national sustainment and security while facilitating quick acquisition of critical infrastructure or products. • Develop flexible response mechanisms and potential incentives to balance security needs with dynamic governmental responses.
Supplier Function
• Provide material input while maintaining quality standards and ethical business practices. • Develop strategies to balance profitability with maintaining product quality and integrity.
User Function
Civilian • Ensure access to necessary products or services, particularly for Users with limited funds.

- Promote awareness of quality over quantity in product selection and consumption decisions.

Military

- Maintain operational readiness while adapting to unexpected challenges and disruptions.
- Foster a culture of repeatable and in-policy innovation and agility within military institutions.

Behavior Requirements (Summarized in Table 3.10)

For Government behavior, there needs to include an emphasis on cultivating adaptability and proactive thinking to appropriately respond to shifting environments. These behaviors should be able to respond to variation and disruption either through a modification of behavior, structure, or both. This requires a concerted effort to challenge and revise antiquated behaviors and traditions, to foster an environment conducive to open innovation. It is recommended that those decisions be better made through a behavior of adapting to satisficing rather than optimizing solutions (see discussion on satisficing in Section 1.1.2). Similarly, Supplier behavior should be guided by the promotion of ethical guidelines and standards, prioritizing quality over profit in decision-making processes. Furthermore, Suppliers need to establish enduring partnerships grounded in mutual respect and shared values. This is further supported through the sharing of defined requirements between both Government and Supplier parties and bolster shared goals through contractual agreements. User behavior requirements underscore the importance of transparent communication and visibility, which would require a collaborative approach between Users and Suppliers to collectively address quality concerns. Within military Users, their behavior requires a delicate balance between procedural control and rigid hierarchy, intermeshed with a culture that embraces adaptability and trade-off decisions. It is critical to provide comprehensive training and support systems for personnel to reinforce and sustain standardized problem-solving procedures while fostering adaptability in confronting complex challenges. Such complex dynamics emphasize the need to articulate and analyze the intricate interplay of behavior within governmental, Supplier, User, and military Stakeholders, when shaping organizational effectiveness and response efficacy in a complex defense supply network context.

Table 3.10: Summary of Requirements for Behavior

Government Behavior
• Foster adaptability and proactive-thinking to respond effectively to changing environments. • Challenge and update antiquated behaviors and traditions to encourage continuous process improvement.
Supplier Behavior
• Promote ethical guidelines and standards to guide decision-making and prioritize quality over profit. • Encourage long-term partnerships based on mutual respect and shared values.
User Behavior
Civilian • Communicate and provide need visibility. • Encourage collaboration between Users and Suppliers to address quality concerns. *Military* • Balance procedural control and hierarchy with adaptability and continuous improvement. • Provide training and support for personnel to develop standardized problem-solving skills and adaptability.

Structure Requirements (Summarized in Table 3.11)

For the requirements related to Government structure, there is a critical need to focus on streamlining processes and minimizing bureaucratic obstacles to enable faster, strategic, and more dynamic responses to both variations and disruptions. It is increasingly important to develop a dynamic system of change management capable of promptly adapting to evolving needs and circumstances. For Supplier structure there needs to be an investment and integration of modern technology adoption and process enhancement to boost overall efficiency and system visibility where possible. Additionally, providing robust structural support at each level of the organization will enable Suppliers to navigate shifting market dynamics with minimal impact to operational capabilities. User structure requirements should revolve around the development of fail-safe supply networks capable of accommodating Users situated in remote areas. This is achieved through exploring alternative models of consumption and demand forecasting to decrease reliance on centralized supply networks, promoting flexibility. For the military User Stakeholder, structure requirements must prioritize the modernization of systems and procedures to effectively counter contemporary threats and challenges marked by variations and disruptions. Establishing flexible supply networks enables agile responses to changing operational requirements, thereby enhancing overall readiness and adaptability. The emphasis on structured adaptability highlights the importance of influencing adaptability and strategic efficiency across governmental, Supplier, User, and military perspectives for navigating complex and dynamic environments.

Table 3.11: Summary of Requirements for Structure

Government Structure
• Streamline processes and reduce bureaucratic barriers to facilitate faster and more strategic responses. • Develop a dynamic system of change management to adapt to evolving needs.
Supplier Structure
• Encourage the adoption of modern technologies and processes to improve efficiency. • Provide support for Suppliers to adapt to changing market dynamics without significant disruption.
User Structure
Civilian • Develop fail-safe supply networks that can accommodate Users located in remote areas. • Explore alternative models of consumption and demand management to reduce reliance on centralized supply networks. *Military* • Modernize systems and procedures to adapt to contemporary threats and challenges in terms of variation and disruption. • Establish flexible supply networks to respond effectively to changing operational requirements.

3.5 Closing Remarks

This Chapter includes a discussion and identification of Dilemmas within the Stakeholders of Government, Supplier, and User as it relates to a defense supply network of People, Processes and Resources. The nested F-B-S DTM is introduced and implemented for each stakeholder with the goal of developing a Requirements List for a fail-safe multi-stakeholder defense supply network through the resolution of Dilemmas. Through the application of the DTM, Tensions revealed within each Stakeholder's "Machine" were grouped and analyzed as potential Dilemmas and related to their F-B-S. The Requirements List developed in Section 3.4 encompasses avenues for potential Dilemma resolutions. This Dilemma analysis is devised to serve as the first step in the realization of the boundaries and gaps within the AoP and lay the groundwork for areas of acknowledgement towards further work based on the assertion that resolving Dilemmas results in a closer realization of a fail-safe supply network system based in the perspective of a CPSS. The development of a fail-safe supply network is contingent upon the careful integration of Function, Behavior, and Structure across each Stakeholder, Government, Supplier, and User using trade-offs and compromise rather than optimization. The task of determining the resolutions of Dilemmas within each Stakeholder of a defense supply network as a cyber-physical-social system is complex and rooted in experience-based judgement but the DTM is generalizable to a variety of other cyber-physical-social systems that include multiple stakeholders. However, by augmenting the DTM to include the F-B-S construct a modified F-B-S DTM is developed which can be used as equally valuable tool for a variety of generalizable situations. By developing and utilizing a modified DTM nested within the F-B-S to discover Dilemmas within defense supply network Stakeholders, a systematic and repeatable method is demonstrated and deployed to support the development of a Requirements List based on Dilemma resolutions for the formation of a fail-safe supply network.

Grounded in the resolution of Dilemmas, the Requirements List in Section 3.4.5 includes a preliminary list of features necessary for designing a fail-safe supply network. The Requirements list is supported by resolving dilemmas with a consistent foundation of shared goals, robust communication and feedback networks, and an infusion of flexibility into structure and behavior within each Stakeholder. The development of the Requirements List for a fail-safe defense supply network also includes the proposition that dynamic responses in typically rigid and legacy supported systems to meet these complex and ever-changing environments is needed. Fostering an environment of common goals supported through contractual obligation and synergizing acquisition and sustainment stakeholders can inject resilience into traditionally inflexible cyber-physical defense supply network systems. This resilience, however, is not fail-safe and results in a return to the previous state of stability. Designing for fail-safe on the other hand will enable stakeholders to respond effectively to changing conditions and mitigate the simultaneous impact of variations and disruptions through a change in Behavior or Structure. To do this, both the methods and measurements of success will need to be adapted to fully support a fail-safe supply network, and the Requirements discussed in this chapter suggest potential avenues for investigation and investment. The discussion of the need to infuse flexibility, agility, and dynamic management of lead times in Section 3.4 highlights the need to incorporate an addition of strategic management and incorporation of social systems within inherently rigid traditionally designed cyber-physical systems. The approach is aligned with the principles of strategic social continuity in the development of fail-safe supply networks, by providing potential Requirements to increase the overall robustness and responsiveness of a defense supply network in the face of variation and disruption in increasingly unpredictable environments.

CHAPTER 4: REVIEWING CURRENT DEFENSE CONSTRAINT RESOLUTION FRAMEWORKS

4.1 Frame of Reference

Defense supply networks cannot and do not exist in a vacuum of total control. As discussed extensively in the literature review of Chapter 2, defense supply networks have various characteristics that make them unique when responding to variation and disruption impacts. With the ever-changing landscape of global and national security concerns, the ability to effectively manage and eliminate constraints impacting throughput, resulting in delays and long lead times, is critical. This chapter will include an exploration and evaluation of currently utilized defense-specific approaches and frameworks used to manage constraints. An analysis of their foundational assumptions, capability to adapt, workflow management techniques, and organizational structures is conducted. Additionally, gaps within existing practice related to specific system patterns are identified through a thorough comparison of a fail-safe CPSS compared to a resilient CPSS. These gaps are then addressed through a lens of practicality, level of fragility, flexibility, agility, and alignment with various levels of management control throughout defense organizations. Finally, a succinct definition of what is required to dynamically manage lead times through the further development of the Requirements List developed through Dilemma resolution in Chapter 3 for a defense specific supply network is outlined and reviewed. Through this comprehensive review of existing practice, steps towards closing the gaps are addressed, and way forward identified for designing fail-safe defense supply networks increasingly complex environments. By determining the requirements for dynamic lead time management, it is hypothesized that defense organizations can strengthen their logistics and supply network operations, ensuring that resources are delivered promptly and effectively to meet critical needs. This chapter also includes discussion and evaluation of the strategies and tools utilized to enhance lead time responsiveness, the role of real-time data and analytics in forecasting demand, and the importance of collaboration among stakeholders in achieving a more agile and responsive defense supply network. Through dynamic lead time management, it is possible for defense organizations to enhance their operational readiness, reduce waste, and improve overall mission success.

4.2 Dynamic Management of Lead Times in a Defense Supply Network

A discussion of currently deployed lead time management strategies will be conducted in the following sections. First, resilience-based lead time management strategies in defense supply network environments will be discussed in terms of advantages and disadvantages in Section 4.2.1. Then an analysis of currently deployed strategies for their potential ability to dynamically manage lead times, which is critical component for a fail-safe defense supply network are examined from the perspective of a fail-safe CPSS design. Additionally, the key differences between resilience-based system design and fail-safe system design are explained throughout.

4.2.1 Current Resilience-Based Strategies for Lead Time Management in Defense Supply Networks

While generalized supply networks and defense supply networks employ similar techniques to reduce lead times and enhance throughput, defense supply networks often need to incorporate specialized strategies tailored to their unique mission objectives. Those unique situations and characteristics are described in detail in Chapter 2 through a critical review of the literature. In Chapter 2, it was discussed that lead times within defense supply networks, while subject to unique situations due to their national and international security implications, are currently managed through numerous strategies each with their own advantages and disadvantages. While the list of lead time management strategies is exhaustive, three strategies: data-based forecasting, inter-stakeholder relationship management, and continuous process improvement (CPI) have the greatest potential for fail-safe design if further developed. Additionally, these strategies included the most potential for flexibility and closely align with the Requirements List developed in Chapter 3 and the framework used in the AoP. These three main techniques are discussed in detail in this section. Additionally, this section is foundational for refining the Requirements List developed in Chapter 3 to determine what is required for designing fail-safe defense supply network and determining gaps in current system design. These gaps will be used to illuminate a path forward towards additional research which is explained in more detail in Chapter 5.

One of the strategies used in defense lead time management and system design, discussed in Chapter 2, is data-based forecasting. Data-based forecasting is a technique used to address logistics challenges in environments of uncertainty through potentially automated decision-making tools and resource planning models (McConnell, Hodgson et al. 2021). In U.S. defense-based organizations like the Defense Logistics Agency, data-based forecasting is done through collaboration with Suppliers and Users through the Demand Data Exchange/Customer Collaboration (DDE/CC) web-based planning tool. The DDE/CC includes tools for customers, or Users, to track historical supply data and disclose future supply requirements for the goal of improving the forecast reliability and reduce shelf stock and wait time (DLA, 2024). Data-based forecasting has several potential advantages in defense environments and associated defense supply networks that can be useful in systems where inventory and transportation can be optimized (Summarized in Table 4.1). Firstly, it enables data-informed decision-making by enabling greater visibility into demand patterns, allowing military planners and supply chain managers to anticipate future requirements based on previous situations. This helps in managing inventory levels, production schedules, and procurement activities like transportation, thereby reducing the risk of stockouts and shortages during critical but predictable operations. Additionally, data-based forecasting can enable more appropriate and predictable resource allocation and logistics planning, enhancing overall operational readiness and effectiveness. However, there are also significant disadvantages to relying solely on data-based forecasting. Firstly, historical data, to be effective in prediction must be accurate. Historical data in military operations may not always be available due to poor technological integration or lack of capable methods of capturing emerging threats or sudden changes in operational requirements, leading to inaccuracies in forecasting (United States Government Accountability Office, 2024). Most notably, the complexity of military environments, characterized by dynamic and unpredictable factors such as shifting geopolitical landscapes or asymmetric warfare, can pose challenges for traditional optimization-based forecasting models rooted in resilience. Additionally, there is a risk of over-reliance on data-driven insights, which may overlook qualitative factors and situational context that could skew decision-making in critical or unique military and supply network operations. This over-reliance on technology and digital resources can also expose organizations to vulnerabilities due to cyberattacks and potential security leaks. Therefore, while data-based forecasting offers valuable advantages in systems based in resilience, it must be complemented with human judgment, qualitative analysis, and contingency planning with built-in trade-off decisions to mitigate its limitations effectively to reach fail-safe.

Table 4.1: Advantages and Disadvantages of Data-Based Forecasting

Strategy	Advantages	Disadvantages
Data-Based Forecasting	+ Proactive planning based on data-driven insights + Can track and provide anticipatory warning of demand fluctuations and lead time variability + Enhanced real-time visibility and monitoring of inventory movements + Early identification of potential issues	– Reliance on historical data may not capture sudden changes or disruptions – Complexity increases with the need for sophisticated modeling and analysis – Implementation costs associated with technology adoption and integration – Potential cybersecurity risks and data privacy concerns

The second technique, broadly referred to as managing inter-stakeholder relationships, is likely the least specific or defined strategy utilized to decrease lead times and enhance throughput. While potentially the most flexible of the supply network lead time management strategies, managing inter-stakeholder relationships has advantages and disadvantages that must be addressed (Summarized in Table 4.2). Managing inter-stakeholder relationships is complex and often requires a balance between stakeholders and can include an analysis of relational dynamics seen in studies of psychology (Choi and Wu 2009, Amici and Bietti 2015).

Furthermore, a long-term strategic approach to inter-stakeholder relationship management can facilitate the development of new technologies, as suppliers may offer valuable insights and advancements that contribute to defense capabilities. This strategy, however, is not without challenges and risks, especially in defense contexts. Dependence on a limited number of suppliers can create vulnerabilities, particularly if those suppliers are located in unstable regions. To counteract those potential vulnerabilities defense organizations must maintain an effective and ongoing investment in collaboration-building activities, where possible, which may diversify methods and means of acquiring People, Processes, or Resources in other critical defense areas.

Additionally, conflicts of interest, ethical concerns, and regulatory compliance issues may arise, necessitating careful selection policies and screening criteria to uphold transparency and integrity in procurement practices.

Table 4.2: Advantages and Disadvantages of Inter-Stakeholder Relationship Mgmt

Strategy	Advantages	Disadvantages
Inter-Stakeholder Relationship Management	+ Improved communication and collaboration with suppliers + Better visibility into supplier capabilities	– Dependency on disclosed supplier performance and reliability – Challenges in managing a large network of suppliers and subcontractors

The difference between resilience and fail-safe systems with regard to inter-stakeholder relationships lies in the difference between relationships based on cooperation or collaboration. Cooperation relationships are more transactional and based in assigned tasks whereas collaboration is more of a fluid relationship based in collective responsibility and autonomy (Table 4.3). Developing strong relationships with suppliers can result in numerous benefits, like enhanced communication, collaboration, and trust (Johnson and Klassen 2022). These relationships are often quantified in terms of benefits, duration, maturity and repeatability (Drewniak, Drewniak et al. 2020). Higher values in one or more quantifiable measures are correlated to an increase the supply network resilience or ability to resume operations after a change due to variation or disruption (Giannoccaro and Iftikhar 2022, Yang, Wang et al. 2022).

Table 4.3: Features of Cooperation and Collaboration (Taouil, Beau et al. 2010)

Cooperation	Collaboration
Skills • Mentoring/Supervision • Pyramidal Hierarchy • Control of top management	*Skills* • Maturity and Experience • Autonomy • Self-control
Modes of Participation • Division of tasks and sub-tasks • Mandatory and imposed	*Modes of Participation* • Individual and Collective • Voluntary and spontaneous
Realization of Tasks • Process of a specialization • Individual responsibility of the task or subtask assigned	*Realization of Tasks* • Explore, create, communicate • Global responsibility and support to peer
Cooperative Space • Learning skills • Knowledge and information dissemination	*Collaborative Space* • Network interaction • Synergy between cognitive and collective aspects

While in either resilience-based for fail-safe systems a balance of cooperation and collaboration is beneficial, fail-safe systems, to be truly fail-safe must include stronger collaboration between stakeholders (Nissen, Evald et al. 2014). By cultivating and maintaining mutually beneficial partnerships based on a strong balance of collaboration and cooperation, defense organizations can gain increased visibility into supplier capabilities, improve responsiveness to changing requirements, and mitigate risks associated with supply disruptions. Overall, while collaborative-based inter-stakeholder relationships in defense supply networks include significant opportunities to fortify defense supply network response to variation and disruption, it requires strategic management to mitigate associated risks and maximize its potential benefits to reach fail-safe.

The last strategy, continuous process improvement (CPI) is a relatively recent addition to supply network design and manufacturing operations. The specifics of this strategy generally depend on the organization's goals, but central themes are reducing cost, reducing time, increasing quality, and increasing throughput through continually monitoring and adjusting processes as necessary (Jaber, Bonney et al. 2010). CPI also has various advantages and disadvantages (Summarized in Table 4.4). CPI is rooted in ongoing process refinement, focusing organizations and teams to continually identify inefficiencies and optimize processes to enhance overall performance usually in the form of metrics. In defense organizations, CPI can lead to streamlined logistics operations, reduced waste, and the refinement of lean systems and processes, all of which contribute to organizational success when met with relatively predictable environments. Similarly, in defense supply networks, CPI prioritizes an optimizable inventory management system and increased supply chain visibility through continuous process monitoring. These improvements have led to the development of agile manufacturing practices through the continuous refinement of processes through CPI. Agile manufacturing practices, largely considered a by-product of CPI, with origins in the private automotive industry, resulted in the implementation of lean Just-in-Time production strategies has had significant impacts in the defense sector (Strategic Direction, 2022). Current agile manufacturing practices have an emphasis on low inventory, no stockpiling, and production-as-needed practices. CPI in resilience-based systems reverts the system back to a previous state and can result in unforeseen and potentially detrimental impacts down the line. Fail-safe CPI on the other hand includes a focus on vision and a willingness to change systems rather than return systems to previous Structures or Behaviors. Additionally, while CPI can help to reduce costs and potentially offer organizations more streamlined capabilities, the defense sector is subject to strict regulatory oversight and yearly allocated budgets making new procurement due to unforeseen circumstances even more difficult. CPI efforts also require significant time, resources, and commitment from personnel, which may pose challenges in environments characterized by stringent regulations, hierarchical structures, and competing priorities (Linnean III 2008). CPI can only be effective if the culture of an organization has complete buy-in from leadership and the majority of the workforce. Unfortunately, resilience-based CPI can only adjust for certain variations in production environments or goals. To mitigate major disruptions, CPI rooted in fail-safe principles must be utilized as a strategy for increasing process visibility and continued process refinement alongside the People and Resources ready and willing to support the process changes.

Table 4.4: Advantages and Disadvantages of Continuous Process Improvement

Strategy	Advantages	Disadvantages
Continuous Process Improvement	+ Systematic identification of inefficiencies and optimization opportunities + Culture of ongoing improvement	– Resource-intensive in terms of time and personnel – Resistance to change and rigid hierarchical personnel structures in implementing new initiatives

4.2.2 Dynamic Management of Lead Times in a Defense Supply Network

Section 4.1.1 included a discussion of strategies for managing lead times within supply networks with specific advantages and disadvantages noted for defense applications with respect to features of resilience-based and fail-safe system design. This section will continue the discussion of strategies for dynamic management of lead times (DMLT) to determine fail-safe principles, by examining those strategies from a CPSS perspective. Each strategy has been mapped on the cyber-physical-social domain in Figure 4.1 to indicate their respective relevance or features that fit into each system domain discussed in more detail in the following paragraphs.

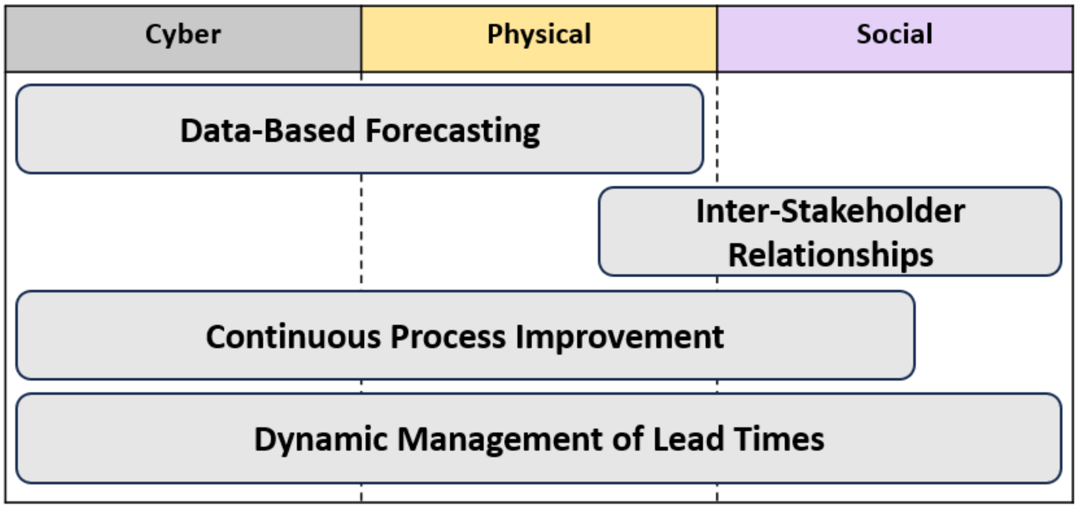

Figure 4.1: Lead Time Management Strategies from a CPSS Perspective

Data-based forecasting can be used as a potential strategy for better visibility within existing systems but because the forecasting systems are generally designed for optimization, changing goals and meeting expectations after disruptions leads to lean but fragile supply networks. From a CPSS perspective current data-based forecasting and associated optimization do not reflect 'real-world' environments in which decisions are made with uncertainty through their reliance on historical data and previous lessons learned. For these reasons, data-based forecasting as utilized today is largely based in resilience focused cyber-physical systems. To ensure data-based forecasting is fail-safe from the perspective of a CPSS, several critical requirements must be met to uphold stability and minimize risks across interconnected digital, physical, and human elements. One way to minimize system failure is redundant data sources ensuring multiple, reliable inputs to avoid single points of failure, while real-time error detection and anomaly alerts quickly flag issues before they cascade. Also, the data must have consistent quality controls to help maintain forecast accuracy, enhanced by high security and privacy standards to prevent unauthorized data access or manipulation. In systems with regularly accessed user interfaces, automated alerts could enable rapid responses to detected anomalies, while rigorous scenario testing and simulations could be used to prepare the system to manage diverse conditions by identifying weak points before they impact operations. While these features can guide a system design towards fail-safe, some features of resilience can be beneficial in fail-safe system design. For example, defined failover mechanisms, like backup forecasting models, can maintain functionality when primary systems fail, while human oversight and comprehensive training would allow personnel to respond effectively to complex disruptions. Together, the features of data-based forecasting as a CPSS can create potential avenues for designing fail-safe networks, enabling a network to function continuously while adapting to and proactively planning for potential disturbances holistically supporting a system of dynamically managed lead times.

Inter-stakeholder relationship management, discussed in Section 4.2.1, was described as the most fluid and least definable of the techniques used in lead time management. While it is notable that this strategy prioritizes a more holistic system perspective, by incorporating relational or social dynamics within cyber-physical systems, inter-stakeholder relationships cannot necessarily be monitored or standardized for a consistently deployable strategy. For example, managing relationships through means of cooperation is based in resilience in that the relationship, through its strength can help an organization return to a previous state of normalcy. Consistency is key for developing standardizable and predictable processes which increase an organization's resilience. Unfortunately, system design based on environmental or conditional predictability is often unable to manage complex disruptions leading to fragile system design that is unable to reach fail-safe. To design a fail-safe system, the system must be capable of changing. This change, with respect to inter-stakeholder relationships, may be realized through the initiation of new relationships based on collaboration that evolve as the system evolves. Fail-safe inter-stakeholder relationship management is based in CPSS design and requires a structured approach that addresses the complexities of communication, data integrity, and aligned objectives across digital, physical, and social domains. Alignment can be demonstrated through clear and secure communication channels to ensure that information flows consistently and accurately between stakeholders, minimizing misunderstandings and preventing data loss or misinterpretation. Establishing agreed-upon protocols and standardized data-sharing practices helps maintain data quality and coherence across different system components. This is especially critical for information sharing in a defense supply network where security must remain at the highest levels. Security can manifest in cyber, physical, and social domains. For cyber, high cybersecurity standards are crucial in protecting sensitive information from unauthorized access and ensuring data remains secure in transit and in storage. For social, to manage potential conflicts or misalignments in objectives it may be necessary to implement pre-determined decision-making frameworks that encourage transparency and allow for compromise without disrupting operational flow. For physical, real-time monitoring and automated alerts can identify discrepancies in interactions or process deviations early, allowing stakeholders to address issues proactively. Additionally, establishing clear escalation pathways and role-based permissions ensures that any required human intervention is managed by trained personnel, minimizing the chance of lead time delays. This structured, multi-faceted approach to CPSS based inter-stakeholder relationship management can be utilized to maintain a fail-safe system through dynamically managing lead times through the support of collaborative relationships, even amid complex and unpredictable disruptions.

Continuous process improvement (CPI) as a lead time management strategy is the closest strategy that incorporates all three aspects of a CPSS and implies the passage of time through process evolution. For the cyber component, CPI involves the integration of cyber resources like databases, data management systems, communication networks, and smart maintenance technologies into existing processes. The physical component of CPI is demonstrated through resource management, sustainable supplies, cost reduction, tool management, and physical maintenance operations. Lastly, the social component of CPI is that change-based process improvements are initiated by actors or humans within the system. Individuals and teams determine production goals that are then put into action through cyber and physical means. However, while the incorporation of widespread cultural buy-in for process improvement is a key addition towards a more holistic approach to lead time management, there are still areas of improvement to synthesize the strategic and operational organizational levels with the highly controlled and monitored tactical level. Similar to data-based forecasting, CPI can reach fail-safe through the incorporation of real-time data collection from all system layers for immediate detection of anomalies or lengthening lead times. The addition of real-time data into CPI can allow for the development of adaptive feedback loops, driven by predictive analytics and machine learning, that can assess evolving patterns and recommend targeted improvements, making sure processes remain relevant and responsive. To prevent errors, maintain high data integrity, and ensure that changes are based on reliable and correct information, data collection for CPI must follow standardized protocols for data validation and quality checks. Cybersecurity, also a major feature in data-based forecasting inter-stakeholder relationship management, is just as essential to safeguard the data and processes from unauthorized access or manipulation to eliminate the possibility of compromising improvement efforts. By aligning these elements, CPI from a CPSS perspective is the closest representation of a CPSS system in that it does address components from each domain. However, CPI is still often based on optimization and resilience focused system design.

Lastly, dynamic management of lead times incorporates the benefits of data-based forecasting, inter-stakeholder relationship management, and CPI strategies. Multi-strategy integration based in CPSS design may be the way forward for determining what is necessary for dynamic lead time management that enhances adaptability, accurately measures performance, and mitigates risks across a system's integrated components to reach fail-safe. From the CPSS perspective, dynamic management of lead times as a component of fail-safe system design can include key features of data-based forecasting, inter-stakeholder relationship management, and CPI to ensure timely, reliable, adaptive, and flexible operations. Data-based forecasting can play a central role, as real-time data collection and predictive analytics allow for accurate, up-to-the-moment lead-time estimates that can adjust to fluctuations in demand, supply disruptions, or operational delays. Forecasting based in fail-safe CPSS principles may be able to proactively prevent bottlenecks by predicting potential issues and suggesting adjustments in advance, thereby supporting a fail-safe approach by mitigating risks before they impact system performance. It is also beneficial to integrate the strategy of managing inter-stakeholder relationships, as lead times often depend on smooth interactions between diverse stakeholders, including Government, Suppliers, and Users. To design a fail-safe defense supply network as a CPSS, structured communication protocols, secure data-sharing channels, and alignment of objectives are necessary to prevent delays due to miscommunication or conflicting priorities. By maintaining transparent and flexible relationships, the system can quickly negotiate adjustments to lead times as conditions change, while also ensuring that critical information flows efficiently among all stakeholders. This alignment of stakeholders is also rooted in constraint identification and elimination which is explained and demonstrated in Chapter 3. Finally, continuous process improvement as a feature of CPSS-based fail-safe defense supply network design contributes to lead-time management by constantly reviewing processes based on real-time feedback. This involves adaptive feedback loops and iterative adjustments that identify constraints or delays early and adjust procedures to maintain smooth operations. While data is crucial for informed CPI, automation and human oversight must work in tandem to ensure that improvements are relevant and sustainable, reducing the likelihood of process failures that could disrupt lead times later in the production line. Together, these elements form the preliminary requirements for a fail-safe strategy for dynamically managing lead times in defense supply networks from the perspective of a CPSS Fail-safe design must enable the system to respond flexibly to evolving conditions while maintaining performance.

4.2.3 The Next Steps

In Section 4.2.1, current strategies for lead time management were discussed regarding their respective advantages and disadvantages within the context of a defense supply network. In Section 4.2.2, the analysis of potential lead time strategies exposed that a reliance on any singular strategy results in a residence-based system rooted in optimizing cyber-physical metrics. A prioritization for resilience results in a lean but fragile network when evaluated from the CPSS perspective. However, merging elements of each strategy from the perspective of a CPSS may result in a more dynamic and fail-safe network. Connecting the assertion in Section 4.2.2 that dynamic lead time management is a feature of fail-safe system design, failures in lead time management can help to identify system design gaps. To determine the gaps in defense sustainment supply networks frameworks, first the network will be introduced using the Business Model Canvas in Section 4.3, then potential failures in the AoP framework will be analyzed for gaps in Section 4.4. Lastly, the Requirements List for a fail-safe defense supply network from Chapter 3 will be refined for defense sustainment in Section 4.4.3.

4.3 The Defense Sustainment Supply Network

In this section, the Business Model Canvas will be used to define the elements of a defense sustainment network.

4.3.1 Introducing the Business Model Canvas

The Business Model Canvas (BMC) is a strategic management tool that is used as a comprehensive framework for developing, visualizing, and analyzing business models. It consists of nine key components: Customer Segments, Value Proposition, Channels, Customer Relationships, Revenue Streams, Key Resources, Key Activities, Key Partnerships, and Cost Structure (Table 4.5). These components, once applied, contribute to a holistic perspective of how an organization creates, delivers, and captures value (Jin, Ji et al. 2022). In the context of a multi-stakeholder defense supply network, the BMC can be instrumental in clarifying diverse interests, focusing supply chain operations within a wider supply network, and enhancing collaboration among military organizations, government agencies, defense contractors, and logistics providers. By mapping out each element of the network, stakeholders can identify opportunities for collaboration, clarify processes, and ensure that resources are effectively allocated to meet strategic defense objectives. This approach can encourage visibility into an organization and enhance the network's responsiveness to variation, disruption, and complex operational demands, ultimately contributing to national security and mission success.

Table 4.5: The Business Model Canvas Components Defined

<table>
<tr>
<td rowspan="2">Key Partnerships: The network of suppliers, partners, alliances, and other third parties that contribute to the business model's effectiveness and success.</td>
<td>Key Activities: The primary tasks, processes, or operations that a business must perform to deliver its value proposition effectively.</td>
<td rowspan="2">Value Propositions: The bundle of products and services that create value for a specific customer segment.</td>
<td>Customer Relationships: The types of relationships a business establishes and maintains with its different customer segments to acquire, retain, and grow its customer base.</td>
<td rowspan="2">Customer Segments: The different groups of people or organizations that a business aims to serve or target with its products or services.</td>
</tr>
<tr>
<td>Key Resources: The most important assets required to operate the business and deliver its value proposition.</td>
<td>Channels: The various ways through which a business reaches and interacts with its customer segments to deliver its value proposition.</td>
</tr>
<tr>
<td colspan="2">Cost Structure: The various costs incurred by the business in operating its model, including fixed and variable costs, economies of scale, and cost drivers.</td>
<td colspan="3">Revenue Streams: The sources of revenue generated by the business model, including pricing mechanisms and revenue models.</td>
</tr>
</table>

4.3.2 Applying the Business Model Canvas to Defense Sustainment

Applying the BMC to defense sustainment involves identifying the key components within defense sustainment from a business perspective with the goal of developing a value proposition cornerstone. Since defense sustainment exists within a multi-stakeholder defense supply network made up of increasingly private industry partners, it is even more critical to identify how a defense sustainment organization functions as a business. The BMC is used as a tool to structure and organize the complex operations within defense sustainment and clarify a clear value proposition to guide the recommendations for a fail-safe and resilient defense sustainment supply network.

4.3.3 Application of the Business Model Canvas

The application of the BMC for a defense sustainment organization within a defense supply network will follow the same outlined component content discussed in Section 4.3.1. Each component is explained and discussed with specifics then summarized in Figures 4.2, Figure 4.3, Figure 4.5, and Figure 4.6 according to each respective component grouping.

Key Partnerships (See Figure 4.2)

Key partnerships in defense sustainment within a defense supply network involve collaboration with defense contractors, technology providers, manufacturers, and government agencies. As discussed in more detail in Chapter 3, these stakeholders within partnerships can be described in overarching roles of Government, Supplier, and User. Defense contractors serving as Suppliers provide specialized maintenance, repair, and overhaul (MRO) services, essential for maintaining complex military systems. Partnerships with technology providers increase access to advanced diagnostic and maintenance tools, enhancing the capabilities of the sustainment network. Relationships with suppliers ensure a steady flow of spare parts and components, critical for timely repairs. Lastly, coordination with government agencies, such as defense logistics and acquisition organizations, facilitates the alignment of sustainment activities with broader defense strategies and objectives (Green and Stracener 2022).

Key Activities (See Figure 4.2)

The key activities for defense sustainment include maintenance and repairs, inventory management, quality assurance, training programs, and research and development. Conducting or coordinating routine and emergency maintenance to ensure that military equipment remains operational is the key activity of sustainment within a defense supply network. Effective inventory management guarantees the availability of spare parts and components, minimizing lead times for repairs. Quality assurance activities ensure that all modifications, activations, and repairs meet stringent military standards and regulations. Additionally, training programs develop and deliver essential knowledge and skills to military and civilian personnel. While ongoing research and development drive new ideas, new sustainment technologies and methods are introduced with the goal of improved efficiency and effectiveness.

Key Resources (See Figure 4.2)

Some of the key resources in defense sustainment include a skilled workforce, advanced technology, logistics infrastructure, and strategic partnership infrastructure. Technicians, engineers, and support staff with expertise in defense sustainment are crucial for delivering high-quality services. Advanced diagnostic tools such as predictive maintenance software and inventory management systems enhance operational efficiency and visibility. Logistics infrastructure, including warehouses, transportation fleets, and distribution centers, ensure that parts and equipment are available where and when they are needed. Lastly, strategic partnerships with suppliers, contractors, and technology providers further bolster the sustainment network, enabling comprehensive and coordinated service delivery.

Key Partnerships:

- Defense contractors and suppliers providing components, parts, technology, or systems
- Logistics and transportation providers
- Research institutions and technology partners for advancement and development
- Government agencies and international partners

Key Activities:

- Procurement and sourcing of People, Processes and Resources for defense purposes
- Production, assembly, acquisition, and sustainment of defense products and equipment
- Adherence to quality control and compliance with standards and regulations
- Distribution, warehousing, and logistics management

Key Resources:

- Inventory of materials, parts, munitions, and equipment
- Production facilities and manufacturing, sustainment, and repair capabilities
- Transportation and logistics infrastructure
- Skilled workforce

Figure 4.2: Summary of Key Partnerships, Activities and Resources

Customer Relationships (See Figure 4.3)

Building and maintaining strong customer relationships is critical for defense sustainment efforts within a defense supply network. Strategic relationships with military and defense agencies are essential for long-term collaboration and mutual success. These relationships include characteristics like responsive support and customer service, with increased availability to address inquiries and quickly resolve issues. Training and workshops offered through these relationships to military or civilian personnel can encourage cross training and cross-functional team structures increasing more robust workforce skill sets. Lastly, building strong relationships between Government, Supplier, and User can help establish contractual and noncontractual continuous feedback loops to capture customer needs, preferences, and outcomes, enabling continuous improvements, and ensuring that services align with dynamic requirements.

Channels (See Figure 4.3)

Defense sustainment services are delivered through multiple channels to ensure comprehensive coverage and accessibility. Direct contracts among military organizations, government agencies, and private-sector partners formalize sustainment services, establishing clear terms, expectations, and routes for financial and physical product exchanges. Digital platforms, including online procurement and sustainment management systems, facilitate efficient coordination and management of sustainment activities. While the potential for on-site support is provided through maintenance and repair facilities located at military bases, depots, and field sites ensure that services are available where they are needed most. Additionally, field service teams can offer mobile support, providing on-the-ground repairs and maintenance in various operational environments.

Customer Segments (See Figure 4.3)

Defense sustainment within a defense supply network includes multiple customer segments, including military organizations such as the Army, Navy, Air Force, Marines, Coast Guard, National Guard, and Space Force. These customers require reliable and efficient maintenance, repair, and overhaul (MRO) services to ensure their equipment and systems are always mission ready. Additionally, government agencies like the Department of Defense and the Defense Logistics Agency are key partners that oversee procurement and logistics activities for their diverse customer segments. Allied nations and international partners also rely on these services for their defense needs, often through cooperative agreements, partnerships, and alliances. Lastly, defense contractors involved in manufacturing and maintaining military equipment depend on sustainment services to support their products throughout their lifecycle.

Customer Relationships:

- Support for military customers
- Collaborative partnerships with suppliers and contractors
- Responsive end user communication channels to address inquiries and resolve issues
- Feedback mechanisms to capture end user requirements and preferences

Channels:

- Direct contracts with military organizations and government agencies
- Partnerships with defense contractors, suppliers, and logistics providers
- Online procurement platforms and supply chain management systems (e.g., DLA)
- Military bases, depots, warehouses, maintenance facilities, and distribution centers

Customer Segments:

- Military organizations (e.g., Army, Navy, Air Force, Marines)
- Government agencies involved in defense procurement
- Defense contractors and suppliers
- Allied nations and international partners

Figure 4.3: Summary of Channels, Customer Relationships and Segments

Revenue Streams (See Figure 4.5)

Revenue streams in defense sustainment within defense supply networks are diverse and complex, which reflects the range of services provided. The bulk of revenue for defense sustainment comes from the national budget and congressional approvals. These revenue streams are long standing and often require congressional appropriation buy-in to allocate revenue for changing services. For this reason, defense sustainment is largely a revenue out system. Funds are spent on a variety of goods, services, and infrastructure. For example, service contracts, which often involve recurring revenue, are a primary source of budgeting constraints with many, covering detailed maintenance and sustainment services. The procurement and maintenance of spare parts and components requires additional revenue that is essential for the upkeep of military equipment. Additionally, licensing fees for proprietary technology and software tools also require revenue, as these tools are critical for modern sustainment practices in a partnership setting. Lastly, depending on the location of the defense sustainment center, revenue must be allotted for the use of local infrastructure like utilities which can be unpredictable given the local environment and rising fuel costs. Changes in revenue streams may result in investments that go beyond less expensive options.

Cost Structure (See Figure 4.4 and 4.5)

The cost structure for defense includes labor costs, technology investments, logistics expenses, training and development, and research and development in addition to other categories for procurement displayed in Figure 4.4. Human capital includes salaries and benefits for skilled technicians and support staff. Facilities and construction procurement is the largest category for contract awards and currently has the longest administrative lead time leaving funds unawarded for longer. Investments in technology, such as diagnostic tools and maintenance software, are necessary for modern sustainment operations, but are often difficult to forecast. Logistics expenses cover warehousing, transportation, and distribution of parts and equipment.

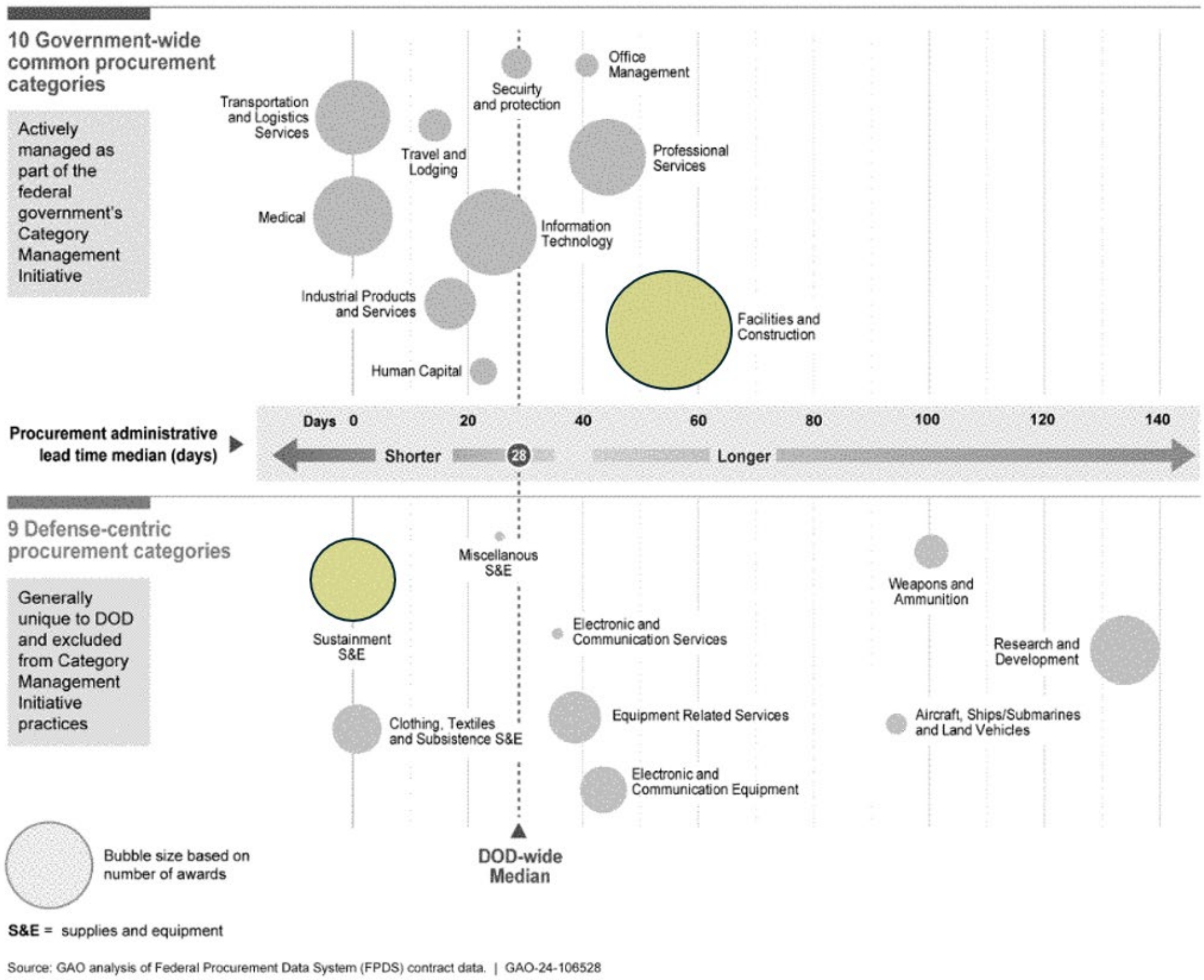

Figure 4.4: Federal Procurement Data System Contract Data (United States Government Accountability Office, 2024)

Training and development costs ensure that personnel are well-equipped with the necessary skills and knowledge and make highly skilled employee retention that much more crucial. Finally, research and development investments drive innovation, enabling the continuous improvement of sustainment practices and technologies.

Cost Structure:

- Procurement costs for materials, parts, and equipment
- Manufacturing and production expenses
- Logistics and transportation costs
- Research and development investments in innovation and technology
- Civilian service and military member salary and benefits

Revenue Streams:

- Sales revenue to local and national economies from contracts with military organizations and government agencies
- Subscription or usage fees for access to supply chain management platforms
- Licensing or royalties for proprietary technology or intellectual property
- Revenue-sharing arrangements with partners and suppliers

Figure 4.5: Summary of Cost Structure and Revenue Streams

Value Proposition (See Figure 4.6)

The value proposition for defense sustainment includes an emphasis on reliability, cost efficiency, dynamic response, and advanced capabilities. By ensuring that military equipment and systems are always operationally ready, sustainment services enhance the reliability and readiness of military forces. Cost-effective solutions extend the life cycle of defense assets and provide significant savings over time and resource conservation. Dynamic response capabilities minimize downtime by quickly addressing maintenance and repair needs, ensuring that critical equipment remains in service. Advanced capabilities, such as predictive maintenance and real-time diagnostics, leverage new and advanced technology to identify potential issues before they become critical, further enhancing the robustness and resilience of supply network operations within defense sustainment.

Value Proposition:

- On-time delivery of critical materials, parts, and equipment
- High-quality products meeting stringent military specifications
- Responsive and agile supply chain to support military operations
- Cost-effective solutions to meet budgetary constraints

Figure 4.6: Summary of Value Proposition

4.3.4 Analysis of Results

By applying the Business Model Canvas (BMC) to defense sustainment as a defense supply network several key areas critical to organizational success were highlighted (Table 4.6). The BMC application emphasizes how defense sustainment supply network complexity is increased within multi-stakeholder environments that include military organizations, government agencies, allied nations, and defense contractors. Each stakeholder discussed relies on a robust and agile sustainment network even though they each may have conflicting priorities and goals. The AoP framework outlines a discussion on determining common goals between each stakeholder as critical for continuity, but the discussion primarily focuses on intra-stakeholder goal setting (AFSC 2023). Inter-stakeholder common goals are often determined through contractually binding agreements where it is crucial for the acquiring party to understand their needs and clearly define their requirements. Conflicting goals may be addressed more comprehensively by intermeshing defense sustainment and defense acquisition teams when forming new relationships with outside partners (Green and Stracener 2022). Key resources and activities highlighted the need for skilled personnel, advanced technology, logistics infrastructure, and continuous improvement through research and development. The content developed as a result of applying the BMC key resources component is mirrored in both the AoP People Processes, and Resources Machine and the holistic cyber-physical-social system perspective. This further emphasizes that strategic partnerships with defense contractors, technology providers, suppliers, and government agencies are crucial for a well-coordinated and effective sustainment network. For the cost structure, that included labor, technology, logistics, training, and research and development expenses, there is an acknowledgement that significant investment is required to maintain and enhance sustainment capabilities. Revenue streams, while complex, highlight a potential constraint due to inflexible and lengthy funding policy requirements, reflecting the complexity of the defense sustainment market and the potential impact on various provided services.

Table 4.6: The Business Model Canvas Components for Defense Sustainment

Key Partnerships: • Defense contractors and suppliers providing components, parts, technology, or systems • Logistics and transportation providers • Research institutions and technology partners for advancement and development • Government agencies and international partners
Key Activities: • Procurement and sourcing of People, Processes and Resources for defense purposes • Production, assembly, acquisition, and sustainment of defense products and equipment • Adherence to quality control and compliance with standards and regulations • Distribution, warehousing, and logistics management
Key Resources: • Inventory of materials, parts, munitions, and equipment • Production facilities and manufacturing, sustainment, and repair capabilities • Transportation and logistics infrastructure • Skilled workforce
Value Propositions: • On-time delivery of critical materials, parts, and equipment • High-quality products meeting stringent military specifications • Responsive and agile supply chain to support military operations • Cost-effective solutions to meet budgetary constraints
Customer Relationships: • Support for military customers • Collaborative partnerships with suppliers and contractors • Responsive end user communication channels to address inquiries and resolve issues • Feedback mechanisms to capture end user requirements and preferences
Customer Segments: • Military organizations (e.g., Army, Navy, Air Force, Marines) • Government agencies involved in defense procurement

• Defense contractors and suppliers • Allied nations and international partners
Channels: • Direct contracts with military organizations and government agencies • Partnerships with defense contractors, suppliers, and logistics providers • Online procurement platforms and supply chain management systems (e.g., DLA) • Military bases, depots, warehouses, maintenance facilities, and distribution centers
Cost Structure: • Procurement costs for materials, parts, and equipment • Manufacturing and production expenses • Logistics and transportation costs • Research and development investments in innovation and technology • Civilian service and military member salary and benefits
Revenue Streams: • Sales revenue to local and national economies from contracts with military organizations and government agencies • Subscription or usage fees for access to supply chain management platforms • Licensing or royalties for proprietary technology or intellectual property • Revenue-sharing arrangements with partners and suppliers

The channels identified, such as direct contracts, digital platforms, on-site support, and field service teams, underscore the critical need to develop a dynamic approach to service delivery. Since these complexities are exacerbated by complex geopolitical tensions, as detailed in Section 2.3.3 and Section 3.3.2 Issue identification, defense organizations are impacted potentially more than others when global disturbances are present. These channels, while critical for developing and maintaining an agile supply network for defense sustainment, introduce vulnerabilities if maintained with only cyber-physical component incorporation. As discussed in more detail in Section 2.3.2, cyber threats continue to have an increasingly devastating impact on supply networks. For this reason, simply developing and utilizing open channels without robust and comprehensive cyber-security is a potential source of devastating disruption that far outweighs the potential benefits of open channel networks. The discussion of customer relationships focused on strategic partnerships, responsive support, training, and continuous feedback, and were framed as a vital component within a supply network for ensuring that sustainment services meet dynamic needs and standards. These are consistent with the AoP's focus on developing a full buy-in culture and agile labor utilization through cross-training (AFSC 2023). These relationships, however, are largely discussed in top-down hierarchal terms within the AoP and may not be representative of a different organizational framework utilized in non-defense organizations. An analysis of differing organizational structures with common goals would be valuable to determine how these differences can be either diminished or developed for all around benefit.

The value proposition component highlighted in the application of the BMC emphasizes the need for reliable, cost efficient, dynamic responses, and advanced capabilities, as essential for maintaining military readiness and operational success. These characteristics are also emphasized in the AoP discussion of common goals which highlights speed, safety, quality, and cost effectiveness as the "rallying point for everyone" within defense sustainment (AFSC 2023). The gap is highlighted in the need for integrated dynamic systems within defense sustainment to achieve those common goals.

4.4 Requirements for a Designing Fail-Safe Defense Sustainment Supply Network

Now that the network of a defense sustainment supply network have been defined in Section 4.3 the Requirements List developed for multi-stakeholder defense supply network in Section 3.4.5 can be refined for defense sustainment.

4.4.1 Connecting Defense Sustainment to the Requirements Developed for a Fail-Safe Defense Supply Network from Chapter 3

In Chapter 3, the preliminary Requirements List for establishing a fail-safe defense supply network was developed to address complex multi-stakeholder constraints among the stakeholders Government, Supplier, and User within defense supply networks in terms of Function, Behavior, and Structure. These constraints were evaluated in terms of Tensions among People, Processes, and Resources, or components of the AoP “Machine”. The list of unresolvable Tensions correlates to Dilemmas. Determining what is needed to resolve each Dilemma was used as the basis for the development of the Requirements List for fail-safe defense supply network design. However, these requirements now require a comprehensive review to assess if the Dilemmas can be resolved or addressed in the AoP framework. Dilemmas still left unresolved when approached from the AoP framework will be analyzed as potential gaps. By evaluating what is currently included in the AoP framework alongside the areas that remain unaddressed, a way forward for designing a fail-safe defense sustainment supply network can be charted.

4.4.2 Overview of Requirements Defined in Section 3.4.5

In Section 3.4.5, a preliminary Requirements List, summarized in Figure 4.7, was developed by resolving Dilemmas identified through the application of the Dilemma Triangle Method (DTM) nested within Function-Behavior-Structure (F-B-S) constructs for each stakeholder in a generalized defense supply network. While the focus within Chapter 3 is primarily the development and explanation of the method of a nested F-B-S DTM, the Requirements List developed as a result of using that method needs to be refined with respect to currently deployed lead time management techniques and practices within defense sustainment.

The refined Requirements List based on multi-stakeholder Dilemma resolutions in Chapter 3 is evaluated from the perspective of defense sustainment as a defense supply network through System Archetypes in Section 4.5.

Function

Government

- Ensure stable national sustainment and security while facilitating quick acquisition of critical infrastructure or products.
- Develop flexible response mechanisms and potential incentives to balance security needs with dynamic governmental responses.

Supplier

- Provide material input while maintaining quality standards and ethical business practices.
- Develop strategies to balance profitability with maintaining product quality and integrity.

User

Civilian

- Ensure access to necessary products or services, particularly for Users with limited funds.
- Promote awareness of quality over quantity in product selection and consumption decisions.

Military

- Maintain operational readiness while adapting to unexpected challenges and disruptions.
- Foster a culture of repeatable and in-policy innovation and agility within military institutions.

Behavior

Government

- Foster adaptability and proactive-thinking to respond effectively to changing environments.
- Challenge and update antiquated behaviors and traditions to encourage continual process improvement.

Supplier

- Promote ethical guidelines and standards to guide decision-making and prioritize quality over profit.
- Encourage long-term partnerships based on mutual respect and shared values.

User

Civilian

- Communicate and provide need visibility.
- Encourage collaboration between Users and Suppliers to address quality concerns.

Military

- Balance procedural control and hierarchy with adaptability and continuous improvement.
- Provide training and support for personnel to develop standardized problem-solving skills and adaptability.

Structure

Government

- Streamline processes and reduce bureaucratic barriers to facilitate faster and more strategic responses.
- Develop a dynamic system of change management to adapt to evolving needs.

Supplier

- Encourage the adoption of modern technologies and processes to improve efficiency.
- Provide support for Suppliers to adapt to changing market dynamics without significant disruption.

User

Civilian

- Develop resilient supply networks that can accommodate Users located in remote areas.
- Explore alternative models of consumption and demand management to reduce reliance on centralized supply networks.

Military

- Modernize systems and procedures to adapt to contemporary threats and challenges in terms of variation and disruption.
- Establish flexible supply networks to respond effectively to changing operational requirements.

Figure 4.7: Preliminary Requirements List for Designing a Fail-Safe Multi-Stakeholder Defense Supply Network

(See Section 3.4.5)

4.4.3 Refined Requirements List for Defense Sustainment

Before the preliminary Requirements List can be refined the stakeholders from Chapter 3 need to be specified for their Function, Behavior, and Structure for defense sustainment. For the stakeholder of Government, it primarily includes the DOD, DLA, and General Services Administration (GSA). The Function of these groups is to define and enforce sustainment policies, allocate funding, establish contracts, and manage the overarching supply chain strategies. They also ensure compliance with national security standards and regulatory guidelines and are responsible for setting long-term sustainment goals and overseeing procurement and logistics. For Behavior, Government maintains a proactive, regulatory role, continuously assessing requirements based on shifting defense needs, evolving technology, and emerging threats. This often involves adapting policies and budgets in response to real-time operational feedback and working to bridge gaps between supplier capabilities and military needs. The structure within the government stakeholder includes hierarchical top-down control agencies and departments organized by specific roles and missions, such as procurement (DLA), logistics (USTRANSCOM), and sustainment planning (various DOD branches). Each military branch has distinct offices for contracting, logistics, and compliance, with a clear chain of command guiding decisions across the sustainment lifecycle.

For Suppliers, or contractors, they Function as the responsible party for delivering materials, parts, and services necessary to maintain and repair military equipment. They provide specialized manufacturing, technology, and expertise needed for asset maintenance, and in many cases, perform modifications or upgrades to extend the lifecycle of defense assets. For Behavior, suppliers usually operate within strict contractual and regulatory guidelines, often working to meet rapid turnaround times, achieve high reliability, and adhere to military standards. They collaborate closely with government entities and end users to forecast demand and refine their parts and services to ensure readiness. Suppliers are more adaptive than the Government and tend to seek new technology or inventions to meet stringent requirements and competitive pressures within the defense market. The Supplier, or contractor, Structure typically consists of prime contractors, subcontractors, and a network of smaller suppliers, each handling distinct aspects of a project or supply chain. These organizations may have dedicated teams for compliance, quality assurance, and project management, often form contractually based partnerships with Government stakeholders to manage contract performance.

The Users in defense sustainment, which include military personnel and command units, Function as the stakeholder responsible for operating, monitoring, and maintaining the equipment provided by the sustainment network. They are crucial for identifying maintenance needs, reporting performance issues, and offering feedback on equipment reliability in the field. Their insights also help to shape sustainment priorities and operational requirements. Military User Behavior is dictated by established protocols and procedures to ensure equipment readiness and safety. These Behaviors include regular inspections, routine maintenance, and establishing feedback loops to flag issues that could impact operational performance and mission success. Their Behavior reflects a frontline, field-level, mission-focused approach, prioritizing readiness, functionality, and reliability in equipment use. The Structure of Users is mission driven. They are typically organized by units and command chains specific to each military branch. Each unit has assigned maintenance personnel, technicians, and operational leaders who oversee equipment readiness and report needs through command structures to Government or Supplier stakeholders. This chain of command ensures that equipment issues are communicated which can impact the broader sustainment network.

Now that the Stakeholders introduced in Chapter 3 have been specified for defense sustainment, the preliminary Requirements List can be refined. To ensure that defense sustainment is fail-safe, the stakeholders of Government, Supplier, and User groups must engage in targeted actions that include changes in Function, Behavior, and Structure. Government stakeholders should establish clear policies and standards that promote not just a resilient supply chain but a fail-safe supply chain through developing comprehensive procurement strategies that prioritize timely acquisition of critical resources while ensuring quality and compliance. They must foster a culture of collaboration and transparency, continuously assessing and adapting to changing operational needs. Suppliers and contractors need to continue to provide high-quality materials and services that meet military requirements while also engaging in research and development to create new technologies and improve product durability and capability. They should also maintain proactive communication with government stakeholders which can help partnerships remain agile and able to adjust production and supply strategies as necessary. End users, including military personnel and command units, should actively monitor and report on equipment performance, continue to participate in training to enhance readiness, and further embrace a mindset of accountability regarding maintenance. Additionally, by establishing clear communication lines within units and among organizing maintenance teams with defined responsibilities, it will increase visibility into processes and ensure timely reporting of issues before system failure can occur. By focusing on these areas, all stakeholders can collaborate effectively to dynamically manage lead times and create a fail-safe defense sustainment system that ensures operational readiness when faced with any challenge. The preliminary Requirements List developed through applying the nested F-B-S DTM in Chapter 3 refined for defense sustainment as a defense supply network is summarized in Figure 4.8.

Function	Behavior	Structure
Defense Sustainment Government • Establish clear policies and standards. • Develop rigorous performance and accountability metrics. • Develop comprehensive procurement strategies. • Establish key partnerships with Suppliers and Users.	**Defense Sustainment Government** • Foster a culture of collaboration and transparency. • Encourage open communication • Continuously assess and adapt to changing operational needs. • Systems capable of rapid adjustments to procurement and sustainment plans.	**Defense Sustainment Government** • Maintain a flexible organizational structure. • Enable quick decision-making and resource allocation during crises or unforeseen events. • Create integrated inter-departmental teams.
Defense Sustainment Supplier • Provide high-quality materials and services that meet the military's operational requirements and sustainment standards. • Engage in research and development improve the durability, reliability, and functionality of defense products.	**Defense Sustainment Supplier** • Develop proactive communication networks with all stakeholders • Reinforce reliability and trust in partnerships. • Remain agile and responsive to changes in government. requirements and operational conditions. • Address government inquiries and feedback efficiently.	**Defense Sustainment Supplier** • Implement a robust supply chain management framework that allows for real-time tracking of materials and performance. • Organize teams that specialize in compliance, quality assurance, and customer support. • Adjust production and supply strategies as needed.
Defense Sustainment User **Military** • Provide timely feedback that informs sustainment strategies. • Participate in training and drills to ensure effective use of equipment and systems under various scenarios.	**Defense Sustainment User** **Military** • Embrace a mindset of accountability and ownership regarding equipment maintenance and operational readiness. • Collaborate with Government and Supplier stakeholders to communicate needs and challenges. • Actively monitor and report on equipment performance and maintenance needs.	**Defense Sustainment User** **Military** • Establish clear lines of communication within units. • Facilitate the strategic flow of information regarding equipment status and operational challenges. • Organize maintenance teams with defined roles and responsibilities.

Figure 4.8: *Refined* Requirements List for Designing a Fail-Safe Multi-Stakeholder Defense *Sustainment* Supply Network

4.5 Identifying the Gap

The AoP handbook contains valuable tactical level insights and practical guidance for continuous process improvement (CPI) through constraint identification and management with respect to People, Processes and Resources. The framework presented in the AoP handbook includes a focus on collaborative and time-based constraint resolution by gating long complex processes into manageable and goal specific segments called gates. The AoP handbook also contains central assumptions as a basis for the framework. Two main assumptions are that each person and group in an organization has the capacity to change and that senior leadership is fully committed to AoP practices and beliefs. The handbook also includes the assumption that resources including funding, personnel, and technology are readily available. The AoP handbook, while outlining critical and well-developed frameworks and techniques for constraint management in defense environments, focuses on tactical operations as the source of both successes and constraints for defense organizations which potentially leaves out key operational and strategic perspectives. To better understand the potential gaps within the complex systems of defense supply networks through an AoP perspective, Systems Archetypes will be utilized to abstract common structures and dynamics within the various levels of organization and clearly identify AoP-based solutions deployed to determine the framework's potential gaps. Systems Archetypes, developed by Peter M. Senge (2006) and colleagues, are intended to be used as tools to identify recognizable patterns and insights into common interconnected elements and potential unintended consequences within systems. Systems Archetypes were developed in response to addressing the nonlinear and complex interdependent relationships within real-world systems and are helpful to determine and diagnose the underlying dynamics within those systems. The following sections examine the AoP goals, strategies, structures, and behaviors from the perspectives of Peter M. Senge's Systems Archetypes contained within his book The Fifth Disciple to better understand gaps within the AoP framework.

4.5.1 Fixes that Fail

The AoP handbook was developed to accelerate defense operations within the USAF and from the systems perspective to prevent or reduce the "Fixes that Fail" archetype. The "Fixes that Fail" archetype includes the description of an organization that responds to recurring problems by implementing short-term fixes to address symptoms rather than identifying and addressing root causes (Figure 4.9). These short-term fixes often have unintended consequences that can exacerbate the problem symptoms and result in the development and implementation of another fix that only addresses the symptoms. This pattern of system behavior results in a cycle of addressing symptoms without identifying the real or root cause of the constraint and can result in superfluous, unsuccessful, and potentially costly fixes.

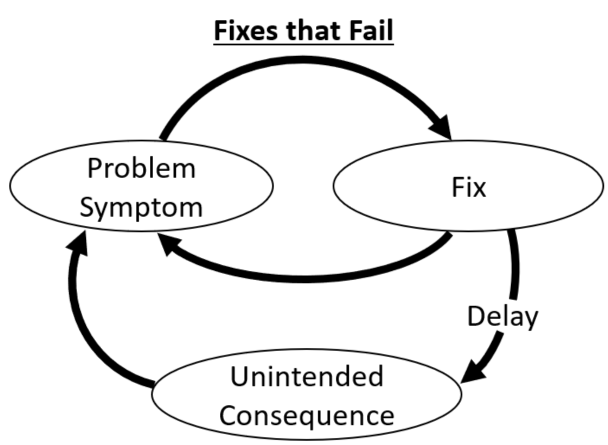

Figure 4.9: "Fixes that Fail" System Archetype (Senge 2006)

Since short-term reactive fixes to systemic issues eventually erode organizational effectiveness and supply network Resources, the AoP was designed to prevent this erosion through the development of a culture of continuous process improvement and standardized constraint identification and elimination frameworks. To address the potential system archetype of “Fixes that Fail”, the AoP structures defense organizations based on constraint identification by recognizing an increase in Work in Progress (WIP) and a decrease in throughput. The AoP framework was intended to directly reduce or eliminate the constraint and remove the potential for delay by continually monitoring production processes (Figure 4.10). This culture of continuous monitoring and CPI is only furthered through system understanding and increased visibility for constraint identification. High levels of visibility are encouraged, emphasized, and outlined in the current AoP framework in the form of visual displays, Walk the Wall meetings, and an emphasis on managing systems from all angles but these metrics may not capture the true constraint especially if it is qualitative in nature.

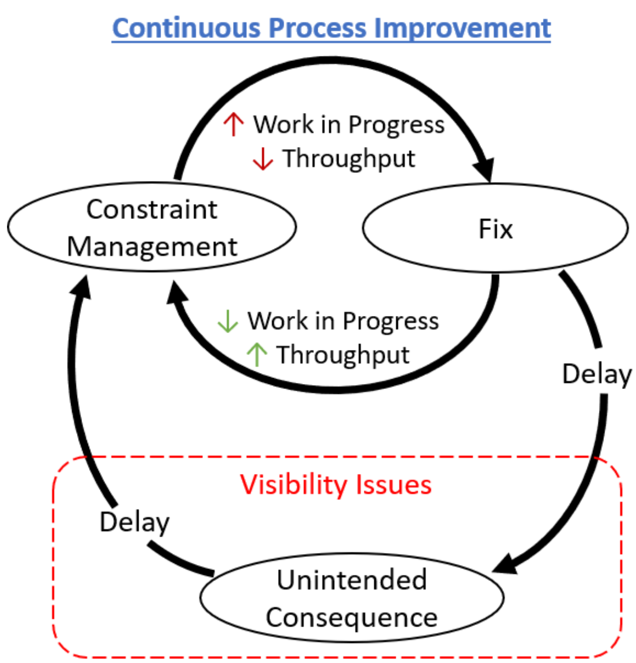

Figure 4.10: Fixes that Fix Through AoP Continuous Process Improvement

By standardizing constraint identification, management, and elimination as a cycle of constraint management signaled by high WIP and low throughput, the AoP framework may leave out more dynamic metrics to identify success in areas unrelated to time. While the AoP includes a discussion and emphasis on urgency and timeliness as it relates to all areas of the Radiator Chart the metrics for success and implementation of AoP principles unrelated to WIP and throughput for those areas are potentially vague. For standardized gated processes that have defined deliverables and completion metrics, AoP constraints management is incredibly effective at reducing WIP and identifying constraints based on rising completion times. However, for more fluid projects like those often found in engineering or logistics groups, standardized gating may not be easily or effectively accomplished under such standardized approaches. These difficult to standardize workloads and processes, critical to many defense operations, may lead to improperly visualized systems that rely on time as the only metric for identifying a constraint because, according to the AoP, if a constraint cannot be visualized it cannot be eliminated (AFSC 2023). Applying a standard framework for constraint identification and elimination through decreasing WIP and increasing throughput in these more specialized or less quantifiable areas may result in unintended consequences that may not be visible until the delay is eliminated. For example, to increase throughput and decrease WIP, a logistics team may initiate a contract with a different and quicker supplier with a potential unintended consequence of quick but low-quality product purchases. For the AoP-based observer, the constraint was effectively eliminated by sourcing a new faster supplier, however the delay is potentially offloaded to another customer or next receiving user as they struggle to identify within their own processes where their eventual constraint originated to eliminate the delay missed by the first group. These unintended consequences, that are not necessarily visible in the current AoP framework design, can propagate fragility throughout critical defense supply networks and erode inter-stakeholder relationships through the unintended redistribution of a constraint. For these reasons, identifying quantitative and qualitative visibility metrics unrelated to time may be crucial to dynamically managing lead times for a fail-safe defense supply network.

4.5.2 Drifting Goals

The difficulties in developing and achieving goals in all organizational levels within defense sustainment supply network systems can be described through the "Drifting Goals" Systems Archetype. This archetype is described through gap identification between the goal and reality. Once the gap is identified there are two courses of action, taking corrective action which takes time and effort to resolve the gap and lowering the goal to meet the current gap status (Figure 4.11). This archetype behavior is intensified when there is inconsistency, lack of communication, or misalignment between overarching goals and actual performance.

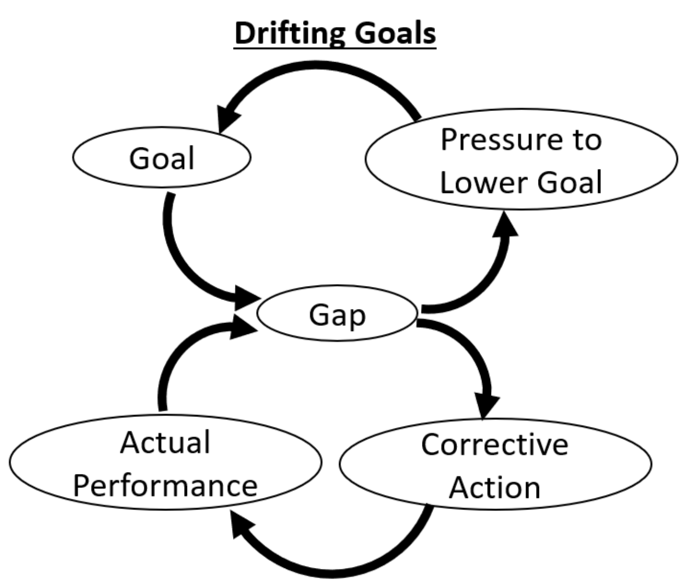

Figure 4.11: "Drifting Goals" System Archetype (Senge 2006)

From the AoP perspective, “Drifting Goals” behavior develops when overarching strategic objectives of defense organizations and the actual operational and day-to-day tactical behaviors are misaligned. While the AoP framework is one of the most successful large scale tactical frameworks deployed, the proactive approach to problem-solving and emphasis on identifying and addressing root causes of constraints is not solely seen in the tactical levels of an organization. From the AoP perspective, there are three defined and structured organizational levels within defense systems, strategic, operational, and tactical that each have their specific goals, behaviors, and structures. These organizational levels are all structured as highly hierarchical and generally follow chain of command lines for communication and directive dissemination and can operate individually when met with variation. While a strict and structured hierarchy is not necessarily unique to defense organizations, reliance on this structure has the potential to complicate goal identification between levels within a defense sustainment supply network when disruptions occur. To address the strategic and operational organizational levels, the AoP framework includes steps and necessary characteristics within leaders and leadership groups to reduce or eliminate potential conflicting priorities and goals. The AoP framework defines culture as evolving and requiring constant engagement in order to sustain, maintain and especially improve behaviors, systems and attitudes (AFSC 2023). The discussion and framework for AoP-based leadership is the closest integration of stakeholders into cyber-physical systems that goes beyond Industry 5.0. However, the focus on engaging leadership in the further development of standardized work may not be sufficient as efficiency and effectiveness have the potential to counteract each other. For example, efficient processes are lean processes, however when met with disruption events, lean processes may prove fragile. This fragility impacts effectiveness. In a highly disruptive environment effectiveness may need to be prioritized over efficiency.

The System Archetype of "Drifting Goals," when applied to the three-tiered structure of the AoP-based organization, presents itself through nested behavior loops between each level of the organization. For example, at the strategic level, the overarching goal of the defense sustainment supply network may be to ensure the timely availability of critical resources to support military operations while prioritizing certain desired efficiencies, cost-effectiveness measures, and sustainability. However, due to shifting geopolitical dynamics, changes in operational priorities and command personnel, and evolving threats may lead to a need to incorporate dynamic changes in strategic goals. These dynamic changes can present themselves as a new administration's defense strategies or budgetary constraints that may necessitate a realignment of priorities, leading to potential ambiguity or conflicting objectives within the existing network systems. Strategic level groups and personnel are structured at the top of a hierarchy and determine organizational priorities to align with large-scale efforts. The operational level contains teams or personnel focused on translating the strategic objectives into actionable plans and processes necessary to execute day-to-day operations within a defense supply network. However, if strategic goals are not clearly communicated or if there is ambiguity regarding priorities due to increasingly dynamic environments, operational managers may struggle to effectively prioritize Processes and allocate appropriate Resources. This can result in a drift in operational goals, with managers making decisions based on short-term expediency rather than alignment with broader strategic objectives. For instance, in the absence of clear guidance, operational managers may have to prioritize meeting immediate demands or cost constraints over long-term sustainability or more accurate project objective parameters. The tactical level, which makes up the largest number of personnel that are predominantly frontline and includes hands-on operators, is responsible for executing specific tasks and activities to support the operational objectives of the defense sustainment organization. Without clear direction and alignment with strategic and operational goals, tactical teams may experience confusion or disconnection from the overarching mission. This can result in a drift in tactical goals, with individual teams or units pursuing objectives that may not contribute effectively to the overall success of the defense supply network. For example, in the absence of clear communication regarding strategic priorities, tactical teams may focus on optimizing local processes or maximizing throughput of certain items without considering broader implications or trade-offs. Misaligned tactical communication can result in potentially large amounts of unnecessary rework, costs, and time wasted resulting in still unmet objectives that further dissatisfaction among the levels of an organization.

The AoP was designed to reduce this misalignment by managing the tactical level with the higher degree of oversight and control measures. This focus is also reinforced at the smallest level by reducing or eliminating individual multitasking. Preventing multitasking for focused task personnel such as a machine operator or a maintenance technician can increase task productivity and reduce errors. However, for personnel with more fluid requirements, there are often competing priorities between "firefighting" and long term or proactive projects. Standardizing work practices with departments or personnel with less standardized metrics and work schedules makes applying the AoP framework to all organizations and levels difficult. This situation was highlighted in the AoP Cases Studies, where the AFSC Logistics Directorate's Performance Management Division (LZZ) developed metrics for their largely administrative or project tracking tasks to monitor their special projects (AFSC 2023). While their team was exceptionally successful in their application of AoP principles in this fluid work environment, this task would prove all the more challenging when applied to a larger more complex defense supply network with potentially adversarial or competing priorities and goals among stakeholders. Additionally, while the AoP framework is effective in relatively stable environments with predictable and standardized goals among all three organizational levels, if presented with a disruption, “Drifting Goals” can manifest in even the most organized organizations. Disruption management can manifest in two ways within a “Drifting Goals” archetype. For a defense sustainment organization, made up of the three defined organizational management levels, goal dissemination can result in two patterns to address goals impacted by disruptions. Depicted in Figure 4.12 are the two potential paths possible when meeting goals using the “Drifting Goals” System Archetype. The red dotted line, the Goal Drifting path, is drawn to indicate how goal lowering can trickle down in an organization if corrective action and associated delay is not permitted or possible while the green line, Goal Directing path, depicts how corrective action also disseminates to all organizational levels with the potential for compounding delays. While the AoP is an exceptional tool for tactical constraints management, it could be even more effective if designed to analyze, determine, or link all organizational levels when identifying the root cause of some constraints. This assertion is reinforced through the national defense funding policy that is usually handled and developed by strategic levels of an sustainment organization for tactical operations. Improper tactical level budgeting can result in unnecessary spending and budget shortfalls often leaving goals unmet and leaders and Users dissatisfied. Either path, Goal Drifting or Goal Directing may meet mission needs but either option, when chosen, centers on adopting tradeoff decisions and a potential change in expectations to achieve desired results. The dynamic nature of responding to variation and disruption within a "Drifting Goals" archetype can produce cascading misalignment and potentially disastrous effects throughout defense supply networks if goals are not clearly communicated and lean resilience is favored over fail-safe.

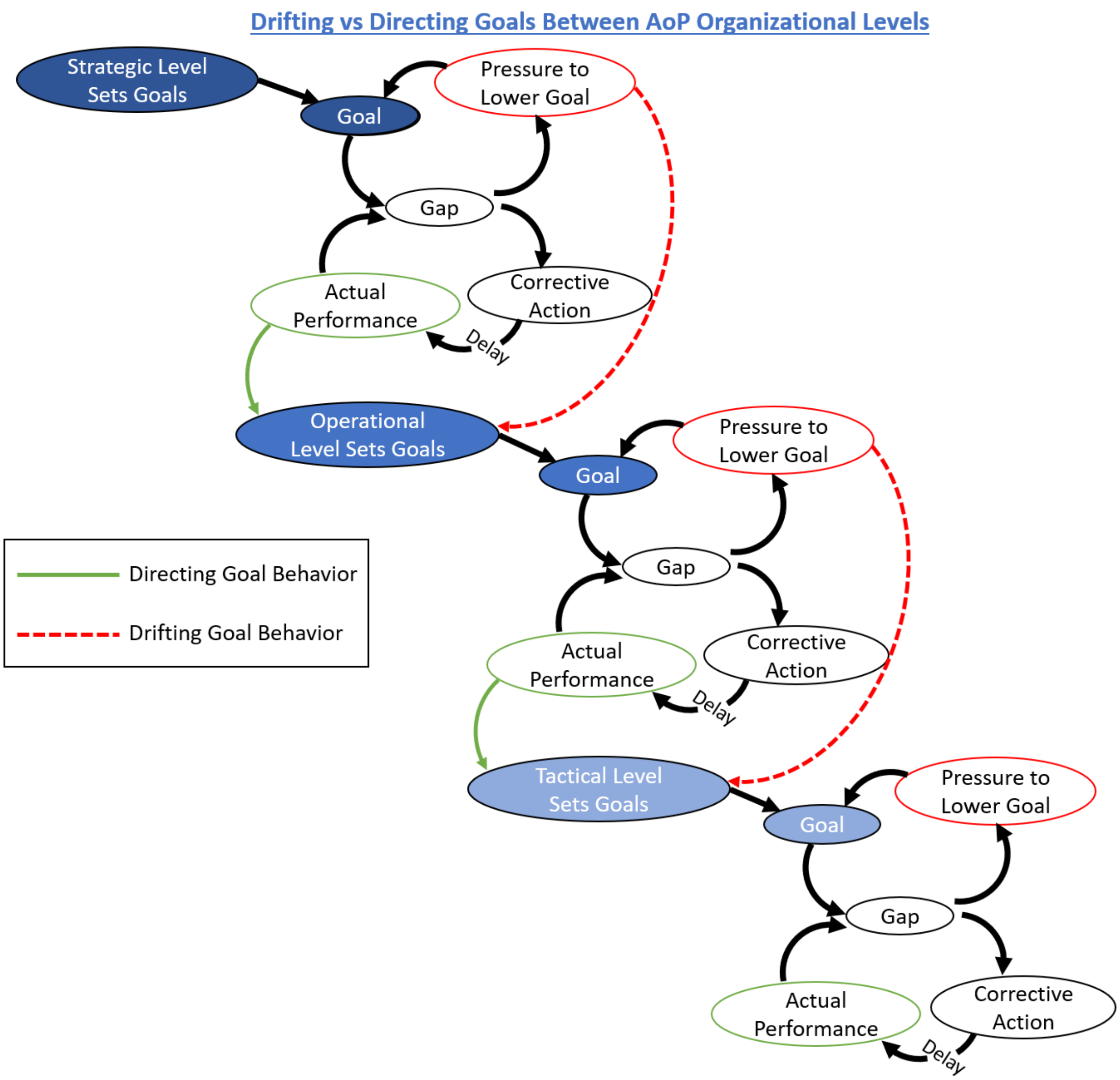

Figure 4.12: Drifting vs Directing Goals

4.5.3 Dynamic Management of Lead Times in Practice

While System Archetypes are a valuable tool for analyzing complex systems for patterns of behavior, an analysis of actual systems and direct practice of constraints management is necessary. The AoP handbook includes extensive examples on AoP in practice with different teams and goals within the AFSC network. Those examples will be examined to determine how well an AoP-based system addresses the Requirements List for constraints management in a fail-safe defense supply network. Generally, the AoP framework includes leveraging predictive maintenance metrics and time-based constraint identification to anticipate issues and long wait times to schedule proactive repairs and reduce unexpected downtime. This emphasis on time-based constraint identification has resulted in a multitude of system changes within defense sustainment and logistics, like continuous process improvement, just-in-time delivery, agile acquisition processes, and strategic partnerships with suppliers, all with the goal of minimizing delays and enhancing responsiveness (United States Government Accountability Office, 2024). These measures have ensured that the defense sustainment within a defense supply network remains resilient for meeting the demands of defense operations while maintaining operational readiness and mission success. While successful, what is often missing in the discussion of AoP in practice is the difference between resilience and fail-safe design.

The AoP contains consistent and strategic methods of organizing systems to ensure efficiency and effectiveness within defense sustainment in terms of resilience. This approach includes several key features. These features include identifying process flow, which involves mapping out the sequence of processes to optimize the movement of materials and track task completion. Secondly, setting clear, achievable goals to align multistakeholder efforts towards common and measurable objectives. Process gating, another key component of AoP applications, involves establishing checkpoints or stages where progress is evaluated before moving to the next phase, ensuring quality and adherence to standards. It is also noted that documentation standards need to be meticulously maintained to provide clear, accessible records of procedures, decisions, and changes. Identifying work in progress (WIP) entails tracking ongoing tasks to prevent bottlenecks and manage workload effectively, ensuring that resources are not over-committed. Lastly, constraint identification in the AoP focuses on pinpointing the lowest throughput points in the system, allowing targeted improvements to enhance overall efficiency. By integrating these methods, the AoP framework, as written, was designed as a cyber-physical system to ensure and maintain a streamlined, consistent, and resilient defense sustainment.

4.6 Steps Towards Variation and Disruption Response in Defense Supply Networks

In the complex environment of defense supply networks, defense sustainment organizations that can effectively and dynamically manage variation and disruption response is critical for maintaining national security and operational readiness.

Due to the unique attributes of defense environments like shifting geopolitical tensions, increasing technological demands coupled with legacy supported systems, unpredictable events and governmental or bureaucratic oversight, robust systems are difficult to control or design. It is proposed through this research that a holistic approach to system design that combines cyber, physical, and social components can increase resilience and reliability within these defense supply networks as these systems better represent real world conditions. This aligns with the resolution of many dilemmas in this multi-stakeholder environment discussed in Chapter 3 by encouraging the development of transdisciplinary teams and comprehensive strategies. These recommendations can be taken a step further by incorporating holistic approaches to traditional systems by integrating engineering, public policy, and business. While more complex, the environments in which defense supply networks operate include facets of all three sectors and designing in tandem will help develop robust systems capable of anticipating, mitigating, and rapidly recovering from disruptions. The answer may lie in educating a new generation in transdisciplinary studies that incorporate more than just one or two disciplines effectively proactively cross training the next generation of employees and leaders. This cross-training may also contribute to higher levels of autonomy within tactical level teams allowing variation and disruption to be managed across organizational levels rather than solely top-down. While fully integrating engineering, public policy, and business in multi-stakeholder defense supply networks has not been fully achieved, approaching this challenge from a cyber-physical-social perspective may bring defense sustainment closer to fail-safe.

While flexibility and adaptability in dynamic environments has been a central theme in the recommendations for fail-safe supply networks both in resolving dilemmas in Chapter 3 and current literature reviewed in Chapter 2, the recommendation and system design requirements to achieve fail safe have not been determined. Chapter 2 includes in-depth discussions related to disaster relief lessons learned that have wider applicability in defense environments. Chapter 3 includes a discussion on how the Function, Behavior, and Structure of an organization in a multi-stakeholder environment can be used to uncover and resolve constraints. While each Chapter contains foundational research and method application in resolving constraints, they each are aligned with the current defense sustainment constraint management system, AoP.

To design systems that are enduringly resilient there must be additional development of the central goals of the AoP framework: speed, quality, safety, and cost effectiveness. While these goals have been a vector for system performance and defense sustainment since the development of the AoP framework, the AoP process Machine is based on an assumption of standardization and successful variability management techniques. These methods have been designed for efficient and lean processes throughout defense organizations. But this efficiency has been at the cost of fragility. AoP-based systems are reliant on relatively stable environments and are not equipped to manage large, unexpected disruptions. These disruptions can cause issues with reliability and maintainability but have wider consequences for system effectiveness when goals are directed by variability-based constraint management techniques and methods.

4.7 Closing Remarks

Defense supply networks operate within dynamic, interconnected, and multistakeholder environments, requiring dynamic and strategic management to navigate constraints resulting from variation and disruption effectively. While Chapter 2 includes an exploration and discussion of the unique characteristics of defense supply networks and evaluate existing approaches for managing variation and disruption, Chapter 4 is meant to take the discussion further towards the more specified sphere of defense sustainment. Defense sustainment operations are based in, organized by and mandated by the AoP framework and currently utilize various lead time management techniques discussed in detail in Section 4.1.1 and Section 1.2. These techniques, while helpful, often require large amounts of data and usually do not track data related to human judgment or social factors. If social factors are included, they are either based entirely on qualitative measures or are included with the intention to exclude based on perceived potential negative impacts. These methods by themselves reinforce lean cyber-physical systems but increase system fragility due to the omission of social factors present in real-world systems. Based on this research, the future of managing lead times within complex supply networks may be based on the merging of data-based forecasting, inter-stakeholder relationship management, and continuous process improvement, emphasizing a holistic approach that considers cyber, physical, and social aspects. For example, data-based forecasting relies heavily on historical data, while relationship management prioritizes social systems but lacks standardization. Continuous process improvement integrates cyber, physical, and social components but requires further synthesis for true dynamic lead time management that can handle both variation and disruption. Additionally, the incorporation of continuous process improvement based in cyber-physical-social systems in defense sustainment will be a vital strategy in generalized supply networks and manufacturing sectors, allowing a multi-faceted focus on reducing costs, time, and increasing quality and throughput based in an enhancement of AoP framework. Further study into a cyber-physical-social framework for consistent and dynamic management of lead times is essential to incorporate proactive and reactive responses within defense organizations to ensure operational readiness and resource allocation in dynamic environments.

Since continuous process improvement is so heavily supported in the current defense sustainment constraint management framework, AoP, identifying both the current state and desired state disconnections can highlight the necessary improvements needed in the framework for increasing system resilience. The widespread utilization of AoP in the diverse areas of defense sustainment has led to the collection of opportunities to study AoP in practice. These AoP in practice situations, or case studies, allow a comparison to be made between AoP framework doctrine and AoP in action. These comparisons have helped to facilitate a gap analysis of the AoP framework by identifying its strengths, areas of improvement, and potential ambiguities or inconsistencies in practice. For instance, the AoP framework is based on constraint identification but does not necessarily include a holistic approach towards visibility through a reliance on time-based cyber-physical metrics. Additionally, discussions surrounding AoP in practice often overlook the time-intensive process of developing and organizing system data to identify constraints effectively. The AoP framework is based on data driven constrain identification, but if the data is not quantifiable the framework does not work.

The preceding sections have discussed and compared current strategies for lead time management within defense supply networks, highlighting the balance between lean but fragile cyber-physical approaches and more dynamic and resilient strategies that include cyber-physical-social system components. This Chapter also includes a refinement of the requirements list developed in Chapter 3 for a multi-stakeholder defense supply network based on the resolution of Dilemmas. The requirements list has been modified for defense sustainment within a defense supply network to include the complexities inherent in depot-based defense sustainment where the AoP framework is based. The defense sustainment application of the AoP includes valuable tactical insights for CPI by focusing on constraint identification and management within the process Machine of People, Processes, and Resources. However, while effective at addressing immediate tactical challenges and flowtime issues, the AoP framework may overlook broader operational and strategic perspectives within defense supply networks. By utilizing Systems Archetypes, derived from Peter M. Senge's work, system patterns are both identified and specified for AoP framework system patterns to identify potential gaps within the AoP framework and understand potential avenues for future development. For example, the "Fixes that Fail" archetype, where short-term fixes exacerbate underlying problems, underscores the importance of holistic and systemic approaches to developing visibility metrics used in constraint management. This is also evident in the measurements of performance. For example, the AoP framework while including quality, safety, and cost effectiveness, ties performance metrics almost exclusively to time or speed by reducing WIP and increasing throughput, overlooking more dynamic metrics for success, particularly in specialized areas like engineering and logistics where processes are not so easily gated. This over-reliance on time-based metrics may lead to unintended consequences, such as sacrificing quality for speed, which can propagate fragility within defense supply networks. Thus, there is a need to incorporate more diverse visibility metrics beyond time to dynamically manage lead times and address a variety of previously unidentified constraints effectively. The second System Archetype utilized in this Chapter is the "Drifting Goals" archetype. This archetype is used to highlight a significant challenge within defense sustainment and supply network systems, the gap between strategic objectives and day-to-day tactical behaviors. This potential for misalignment or reliance on higher levels for decision-making can lead to ambiguity, conflicting priorities, and inefficiencies across organizational levels. These archetypes serve as tools to derive a modification of AoP-based framework for constraints management by identifying areas for further improvement within the AoP framework patterns.

While the AoP framework addresses tactical constraints management effectively, it may fall short in analyzing and linking all organizational levels when identifying root causes of constraints. Disruptions in this line of communication between strategic and tactical can exacerbate goal drifting, leading to compounding delays or misguided corrective actions. The dynamic nature of variation and disruption underscores the need for an equally dynamic framework of constraint management that includes clear communication, alignment of goals, and effective leadership across all levels of defense organizations to prevent cascading failures and ensure mission success within defense supply networks.

In Section 4.4 the Business Model Canvas is applied to defense sustainment within a defense supply network to reveal critical areas vital to organizational success. Business Model Canvas is used to organize the complexity of supply networks within multi-stakeholder environments that include military organizations, government agencies, allied nations, and defense contractors. While each stakeholder interaction may involve conflicting priorities, a robust and agile defense supply network should be based on a set of common goals that are consistent across the stakeholders. The AoP framework addresses this need for common goals by underscoring the importance of determining common goals among defense sustainment stakeholders for continuity. This continuity is often reinforced and upheld with contractually binding agreements, requiring a clear understanding and a defined requirements list. Increasing the efficacy of the developed requirements list can be facilitated by integrating defense sustainment and acquisition teams when forming new partnerships. For key resources and activities, the need for skilled personnel, advanced technology, logistics infrastructure, and continuous improvement through research and development is emphasized. Lastly leveraging strategic partnerships with defense contractors, technology developers and researchers, suppliers, and government agencies is imperative for a comprehensive and effective defense supply network. Arguably, the most important component of the BMC is the value proposition. The value proposition for defense sustainment is based in reliable, cost-efficient, dynamic responses, and advanced capabilities crucial for maintaining military readiness and operational success in the face of variation and disruption. However, the gap between the identified value proposition and current practice is in the need for holistically integrated dynamic systems within defense sustainment to effectively achieve common goals.

In the complex environments of defense supply networks, the ability to manage variation and disruption effectively is crucial for national security and operational readiness. Given the unique challenges of defense environments, such as geopolitical shifts, technological demands, and bureaucratic oversight, developing robust systems becomes inherently necessary and increasingly complex. By identifying where the AoP framework can be improved, like a holistic approach to system design, integrating cyber, physical, and social components the network can enhance resilience and reliability with the goal of designing a fail-safe network. By focusing on transdisciplinary teams and comprehensive strategies, dilemmas in addition to constraints can be identified in multi-stakeholder environments and can be addressed more effectively. Furthermore, the recommendation for the integration of engineering, public policy, and business in system design can lead to the creation of more adaptable and fail-safe defense supply network systems that mirror the real-world. Educating future generations in transdisciplinary studies and promoting cross-training among employees and leaders can further enhance adaptability and autonomy within tactical level teams reducing the potential for communication misalignment. While the AoP framework has been instrumental in standardizing constraint management within defense sustainment organizations, there is a need to evolve its central goals of speed, quality, safety, and cost-effectiveness. While efficient and focused, the reliance on standardization and variability reduction techniques has led to fragility, especially in the face of unexpected disruptions. To ensure enduring resilience, the development of strategies that can effectively address large-scale disruptions while maintaining system effectiveness and reliability is crucial.

CHAPTER 5: RAMIFICATIONS OF RESULTS AND PATH FORWARD

5.1 Summary of Work

5.1.1 Connecting the Chapters

Beginning in Chapter 1, the background and motivation for analyzing defense supply networks through the perspective of a CPSS is highlighted as the next step towards realizing fail-safe system design based in dynamic lead time management. Dynamic lead time management is further specified for defense sustainment with a specialization in Air Force Sustainment and their approach and framework for lead time management: AoP. The justification for analyzing the AoP framework is based in its wide reach and high level of standardization within these large and complex defense specific environments. The AoP is also open source and therefore available to anyone for added process transparency. Also included in Chapter 1 is the explanation and discussion of the key questions addressed in the subsequent Chapters of this Thesis including a road map of the thesis. The development of the key questions addressed in this thesis focuses on the foundation and justification of the CPSS perspective as a way to analyze and conceptualize the AoP for gaps.

Moving through to Chapter 2, this chapter includes the analysis of the environment the AoP operates through the use of a detailed literature review. The literature review is three-tiered. Firstly, the explanation of different perspectives on the terms variation and disruption are discussed with respect to the language used to conduct the literature search. Secondly, the examination of variation and disruption response in a generalized supply network is highlighted and explained through the literature. Thirdly, the specific characteristics within a defense environment are outlined and tied to the literature from the perspective of a defense specific supply network. This chapter is foundational for examining the environment in which the AoP is currently deployed and explains the key differences between a generalized supply network and a defense supply network using specific literature examples.

Now that the research questions have been identified, the AoP framework for examination has been outlined and justified, and the environment the framework operates in has been explored and analyzed through literature, Chapter 3 begins with a direct examination of that AoP framework deployed within a defense supply network environment using a nested Function-Behavior-Structure Dilemma Triangle Method (F-B-S DTM). The justification of using the nested F-B-S DTM is based in the necessary step of determining constraints or Tensions within each stakeholder operating within a defense supply network: Government, Supplier, and User. These constraints are potential Dilemmas that present opportunities for the development of a requirements list based in Dilemma resolution.

The Requirements List generated in Chapter 3 is then evaluated in Chapter 4 with a perspective that rejects optimization for more realistic decision selections that are based on trade-off or satisficing solutions. Chapter 4 also includes an analysis of the system dynamics within the AoP framework in terms of System Archetypes. Then the defense supply network from a sustainment perspective is analyzed as a business using the Business Model Canvas to merge theory with practical application by breaking down key sustainment components to map each element for the development of a value proposition. The value proposition is explained as the aligning of strategic goals with operational readiness and focused tactical delivery of mission-critical support to sustain military operations.

Chapters 1 and 2 can be considered the justification and foundation of this Thesis, while Chapter 3 and 4 include further specification towards defense sustainment as a defense supply network with the goal of defining gaps in current methods of variation and disruption response to determine what is required for designing a fail-safe defense supply network.

5.1.2 Revisiting Purpose

The justification of this thesis is based on the identification of a way forward for further research by analyzing gaps within the AoP framework when modeling the system as a CPSS capable of addressing both variation and disruption. The analysis of the defense supply network is specified to apply to the complex environment of maintenance, repair and overhaul (MRO) operations for defense sustainment. While the AoP framework includes the assertion that through its use systems and users can maximize efficiency, innovation, and continuous improvement in complex systems, its practical implementation in an increasingly unstable and complex environment reveals areas where gaps may exist, and further enhancements and modifications may be needed. The purpose of this work is rooted in the systematic evaluation of the defense supply network environment from the AoP framework perspective while analyzing its limitations when modeled as a CPSS. This gap identification will serve as a foundation for further work in a Ph.D. towards the development of fail-safe systems that are more capable of supporting both strategic objectives and dynamic lead time management for increased operational readiness.

5.2 Answers to the Questions

The work produced in this Thesis is based in the justification, exploration, and eventual answers to the following three research questions:

Questions

Question 1 (Q1): What are the current states and identifiable problem areas within current defense supply network management systems as it relates to Function, Behavior, and Structure?

Question 2 (Q2): How are defense supply network responses designed to handle variation and disruption with respect to the AoP Machine: People, Processes, and Resources?

Question 3 (Q3): How can an inherently structured, lean, but fragile environment like defense sustainment be dynamically integrated into a flexible and fail-safe supply network?

Q1 serves as the basis for investigating the functional performance, operational behaviors, and system structures within defense supply network management systems. By focusing on these three components: Function, Behavior, and Structure (F-B-S) the goal is to identify inefficiencies, bottlenecks, or vulnerabilities i.e., Tensions and Dilemmas. Since defense supply networks are critical for national security, and any failure in these areas could compromise mission success a systematic evaluation of current practices is necessary to uncover the problem areas that increase fragility and lower resilience. The hypothesis associated with **Q1** is Hypothesis 1.1 (**H1.1**). **H1.1** is based in the belief that a comprehensive assessment of current practice will highlight the key challenges and key successes in the system, allowing for the identification of potential solutions.

The second question, **Q2**, was designed to further specify the analysis of lead time management in variation and disruption response by analyzing how the components of People, Processes, and Resources within the AoP Machine framework contribute to resilience. In an increasingly volatile and complex global environment, supply network disruptions ranging from cyber threats to local logistical challenges are becoming more common. This question includes an examination on how the AoP Machine performs when reframed from a cyber-physical-social systems perspective. The hypothesis associated with **Q2** is Hypothesis 2.1 (H2.1)**. H2.1** hypothesizes that integrating these systems can strengthen the defense industry ability to compete in contested logistics environments, where rapid, flexible, and adaptive responses are crucial. Understanding how to synchronize People, Processes, and Resources will offer insight into designing a fail-safe supply network.

The third question, **Q3**, was designed to guide the exploration into the transformation of defense sustainment systems, which are traditionally structured and lean and based in cyber-physical systems, into more adaptive and flexible frameworks capable of withstanding both variation and disruption. While lean systems are efficient, they can be fragile under stress due to their inherent lack of flexibility. This question serves to address how lead-time management, modeled as a cyber-physical-social system, can be used to bridge the gap between structure and agility. This question has two hypotheses Hypothesis 3.1 (**H3.1**) and Hypothesis 3.2 (**H3.2**). **H3.1** includes the proposition that by evaluating lead-time management techniques and frameworks within existing defense systems, gaps in existing frameworks can be identified. The second hypothesis, **H3.2**, is based in the assumption that rather than aiming for optimization, focusing on satisficing solutions through strategic trade-offs can create a balance between lean efficiency and dynamic resilience. This dual focus will lay the foundation to enable defense supply networks to adapt dynamically to the changing demands of modern warfare logistics through gap identification and strategic trade-off-based decisions.

The core methods utilized in this Thesis address and progress towards answers for multiple questions and hypotheses. But, for the purposes of answering the previously listed questions they can be categorized and labeled as follows:

Methods
Method 1 (M1): Comprehensive Literature Review
Method 2 (M2): Nested Function-Behavior-Structure Dilemma Triangle Method
Method 3 (M3): Business Model Canvas for Value Proposition Development
Method 4 (M4): Modification of System Archetypes for Gap Identification

After covering the background, motivation, and introduction to the thesis in Chapter 1, Chapter 2 is based in the development and use of **M1**, the comprehensive literature review. The aim of completing this literature review is mainly rooted in the answer to **Q1 H1.1** and **Q2 H2.1**. For **Q1 H1.1** the comprehensive literature review was used to document and assess the current state of supply network management, clarify differences between generalized supply networks and defense supply networks, and organize a review of current methods of variation and disruption response from a CPSS perspective. By reviewing existing research, reports, and case studies, the literature review was used as a tool to identify and clarify constraints related to

Function, Behavior, and Structure for stakeholders within the environment of defense specific supply networks. For **Q2 H2.1** the literature review included the exploration and identification of how defense supply networks have responded to disruptions and variations in the past, particularly regarding the AoP Machine framework (People, Processes, and Resources). By reviewing past strategies and case studies, **M1** was able to serve as a basis for understanding the limitations and strengths of current approaches in managing disruptions in addition to allowing for the review of research by other fields like disaster response as potential avenues for fail-safe system disruption response.

M2, or the development and use of a Nested Function-Behavior-Structure Dilemma Triangle Method (NFSB DTM), is also similarly tied to **Q1 H1.1** and **Q2 H2.1**. However, in this examination of **Q1 H1.1** and **Q2 H2.1**, located within Chapter 3, the method is applied to the situation of multi-stakeholder interactions within a defense specific supply network environment from the perspective of the AoP Machine. While **M1** includes the gathering and review of other systems of constraint identification and management, **M2** is the direct development and application of a new method of examining this situation's constraints. This method includes the break down the defense supply network into its key stakeholders: Government, Supplier, and User to analyze how these elements interact and the resulting Tensions that arise through their conflicting goals. By mapping out these relationships, **M2** was used as a tool to provide insights into how these Tensions can result in Dilemmas which contribute to ineffective systems that fail to meet mission goals. These Dilemmas were further examined from their impact to Function, Behavior, or Structure to identify a preliminary requirements list based in their resolution or alleviation of problem areas in the current system.

M3, the deployment of the Business Model Canvas (BMC) also in Chapter 4, is based in the perspective that defense supply networks and defense sustainment operate in environments made up of businesses and while the defense organizations are not operating as businesses the principle of addressing and developing a value proposition from a business perspective is valuable. For **Q3 H3.2**, **M3** is applied to propose a potential solution for integrating lean, structured environments into more adaptable and flexible networks by mapping out the core activities, resources, and partners within the defense supply network specified for sustainment. By taking a business approach, this method allowed for a focus on satisficing solutions rather than strict optimization which favors situations of high uncertainty. This approach facilitated the development of a value proposition that can align with strategic trade-offs for designing a fail-safe supply network.

M4 which is focused in the gap identification of Chapter 4, bases its analysis in the identification and explanation of System Archetypes within the frameworks design is tied to both **Q2 H2.1** and **Q3 H3.1**. For **Q2 H2.1**, **M4** is used to both explain how existing System Archetypes are seen within the defense supply networks and system behavior and to specify modified System Archetypes that are specific to the AoP frameworks approach to managing variation. The concept of disruption response is related to identifying potential constraints within variation response as a building block towards managing more impactful disruptions. For **Q3 H3.1**, **M4** is applied to specifically evaluate the workflow and lead-time management frameworks in defense sustainment systems in detail. While **Q2 H2.1** includes applying the AoP Machine to the defense supply network system, **Q3 H3.1** focuses on the AoP framework directly from the perspective of defense sustainment. By modifying system archetypes within the framework of the AoP, **M4** is used as a tool to allow the identification of gaps in systems that are designed lean but fragile. By using the System Archetypes perspective in **M4** gaps are highlighted in current sustainment systems, helping to evaluate how they could be adapted for greater dynamic resilience.

Each of these methods act as tools that help to facilitate a strategic and organized approach to answering the questions developed in this Thesis. The progression of research questions and methods with deliverables is visualized in Figure 5.1.

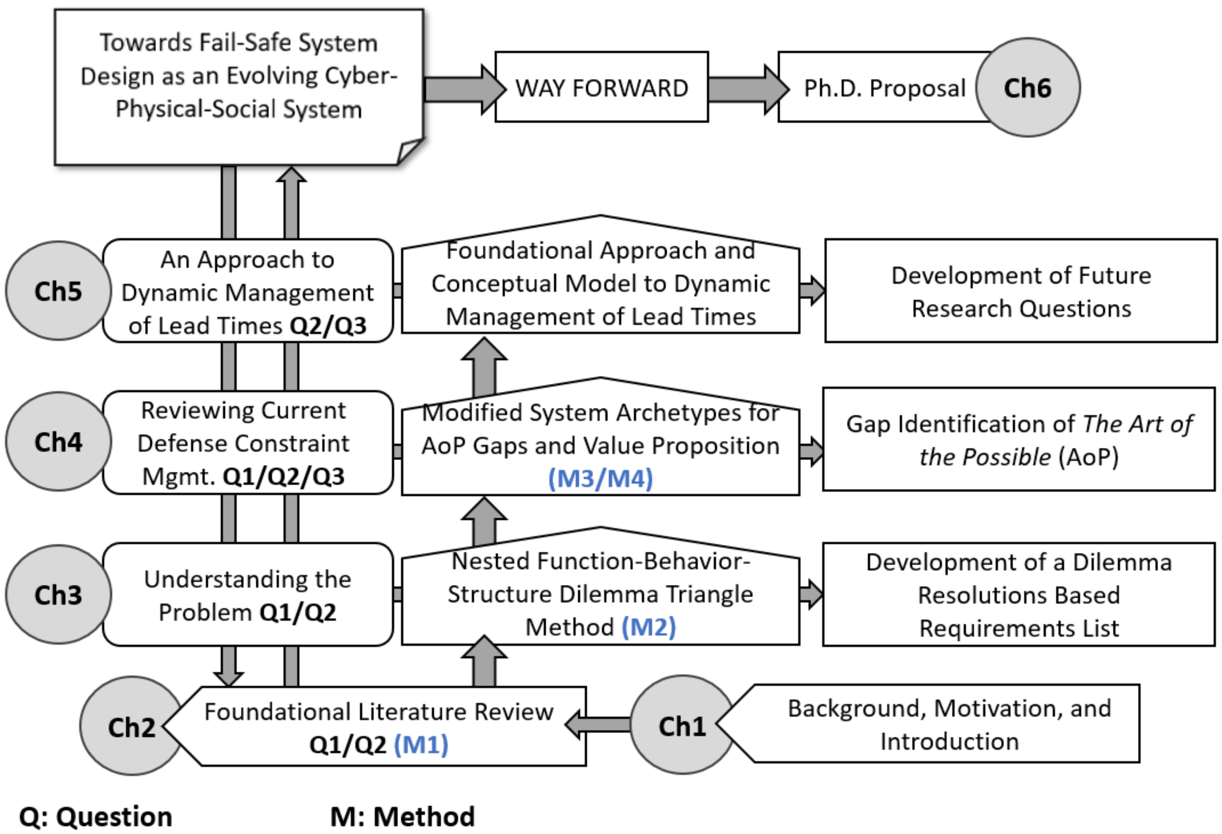

Figure 5.1: Chapter Progression and Connections between Questions and Methods

5.2.1 Revisiting Question Justification and Development

This thesis includes defining and exploring the evolving challenges and opportunities within defense supply network management, focusing on ways to design fail-safe systems capable of adaptability in the face of disruptions through the test case of defense sustainment. The key questions guiding this research were designed to strategically guide the examination of the current state of defense supply networks in how they respond to variation and disruption, and how they can be dynamically transformed to meet the demands of an increasingly unpredictable environment. By analyzing the Function, Behavior, and Structure of these supply networks, assessing their current responses, and exploring pathways to greater agility and robustness through the detailed review of the AoP framework, this is foundational in providing a comprehensive requirements list for improving defense sustainment operations through a dynamic perspective of lead time management in this thesis.

5.2.2 Connections Between Questions

The questions developed and selected for this thesis are strategic and connected in that each proceeding question serves as another foundational step for the next question. The thesis begins with the analysis of the current states and identifiable problem areas within current defense supply network management. This analysis exposes the key differences between a generalized supply network response to variation and disruption and a defense specific supply network by asking Question 1 which is foundational for Questions 2 and 3. These differences are highlighted and explained through a comprehensive literature review contained in Chapter 2. Then the defense supply network is reframed as an overlapping system of three stakeholders: Government, Supplier, and User in Chapter 3. These stakeholders are analyzed particularly as it relates to their Function, Behavior, and Structure (F-B-S) for internal Tensions, and which represent potential Dilemmas. This method functions as a critical diagnostic tool for how the supply network operates in practice (Function), how it performs and reacts under both normal and disruptive conditions (Behavior), and the organizational framework within which these processes occur (Structure). By focusing on Dilemma resolutions based in these three components, F-B-S, Chapter 3 ends with the development of a preliminary requirements list highlighting potential for improvement in the existing system and revealing areas where inefficiencies or vulnerabilities threaten overall supply network effectiveness. This foundational understanding is essential for building any strategy aimed at improving network adaptability and flexibility to reach fail-safe.

After outlining the current issues in lead time management within the context of a supply network, the focus shifts to evaluating how defense supply networks handle disruptions and variations, with specific reference to the AoP framework. The AoP framework was justified and selected based on its strategic, standardized, and widespread application in defense sustainment, arguably the largest arm of defense supply network activities. This portion of the thesis primarily focuses on Question 2. This question was designed to aid in the focused examination of network responses through the lens of People, Processes, and Resources the three core components that make up the AoP "Machine" (AFSC 2023). Chapter 4 includes the critical review of the AoP framework through examining the roles and capabilities of personnel in managing variation and disruption, the effectiveness of established processes, and the adequacy of resources and technologies to mitigate disruption impacts from the perspective of lead time management. By assessing these components of the "Machine", the analysis includes highlighting existing strengths and weaknesses in how the system responds to real-world challenges. This evaluation sets the stage for exploring improvements by pinpointing where response mechanisms succeed and where they fail to meet expectations of performance which is critical in gap identification.

Building on the insights developed from the evaluation of current responses, the final phase of the thesis serves to address the proposed transformation of defense sustainment lead time management into more agile, flexible, and fail-safe. The inherently structured and often fragile nature of defense operations presents challenges in adapting to an increasingly dynamic and complex environment. By framing the defense supply network as a cyber-physical-social system the limitations of lean and fragile cyber-physical systems are addressed through the addition of the social components into system design. The previous Chapters of the thesis serve as a foundation for proposing strategies for integrating lean but rigid systems into a more adaptable and flexible framework based in CPSS design. The focus is on developing greater agility to rapidly respond to emerging challenges, increasing flexibility in processes to accommodate variations and disruptions, and designing a fail-safe supply network system that maintains operational continuity despite disruptions. The goal is to create a supply network based in dynamic management of lead times that not only survives but thrives in the face of uncertainty.

5.2.3 Answering the Questions

Question 1
What are the current states and identifiable problem areas within current defense supply network management systems as it relates to Function, Behavior, and Structure?

Beginning with **Q1**, this question is designed to highlight the problem areas within defense supply network management in terms of Function, Behavior, and Structure therefore the answer should follow the same strategy. In terms of Function, defense supply networks Function as framework used to ensure the timely and secure delivery of critical materials, equipment, and services to defense operations. However, they often lack real-time visibility, limiting decision-makers' ability to track assets and respond quickly to changes in demand or disruptions. This results in delays and inefficiencies, as decision-making is based on outdated information. Additionally, many systems remain rigid, relying on fixed funding allocations and static or antiquated inventory management, which struggles to adapt to rapidly changing operational needs. This rigidity is further compounded by manual processes that persist despite advancements in automation and data-driven solutions, slowing down response times and increasing the risk of human error. Additionally, the issue of an over-reliance on single source vendors, potentially due to lengthy supplier approval processes, strict overly specific acceptance criteria, or niche customer needs, expose defense supply networks to vulnerabilities caused by variations or disruptions when suppliers face challenges, particularly in the context of geopolitical instability.

From the Behavior component, defense supply networks tend to react slowly to disruptions either due to the inherent unpredictability of disruptions, the level of impact is underestimated, or geopolitical events exacerbate already tenuous situations. Whether caused by natural disasters, contested environments, or logistical issues, the response tends to be reactive rather than proactive. This is largely due to the absence of predictive analytics and dynamic decision-support systems, which could forecast and mitigate risks before they escalate. Another behavioral challenge is the siloed nature of operations across different branches of the military and defense contractors. Poor coordination and communication between these entities can lead to inefficiencies, redundancies, and gaps in resupply, especially in time-sensitive situations.

Moreover, many defense supply networks fail to capitalize on the wealth of available data for demand forecasting and system optimization, often relying on outdated methods to predict needs due to stringent cyber-security infrastructure. The balance between just-in-time (JIT) and just-in-case (JIC) inventory strategies is also problematic. While JIT systems reduce excess inventory, they leave the supply network vulnerable to delays, whereas JIC stockpiling leads to excessive storage costs and the risk of obsolescence.

In terms of Structure, defense supply networks are highly fragmented, made up of multiple layers of contractors, subcontractors, and service providers operating independently. This decentralized structure complicates coordination, making it difficult to manage disruptions or track materials across the entire system. Additionally, the globalized nature of defense supply chains poses significant risks but is inherent to the system's purpose. This globalization results in critical components and materials being sourced internationally, making a particular supply chain vulnerable to geopolitical tensions, trade barriers, and supply security issues. The globalization of critical corporations that operate internationally but act as sole suppliers to defense organizations and specialized weapons systems also pose a challenge. This exposure to global risks is further complicated by cybersecurity vulnerabilities, as increasing digitization in defense networks also opens the door to cyberattacks. The duality of increased flexibility and visibility must be met with increased security that in its nature must remain secure is a challenge throughout the defense system network. The structural complexity means that weaknesses in one part of the supply chain can expose the entire system, jeopardizing operational security and continuity. Finally, the traditional contracting and procurement structures in defense are often inflexible to meet the equally structured fiscal policy of governmental and military institutions. Long-term contracts may lack the adaptability needed for defense organizations to shift suppliers or reallocate resources in response to changing operational conditions, contributing to slower procurement cycles and delayed response times.

So, to summarize the answer to **Q1**, defense supply networks face significant challenges in each component of their Function, Behavior, and Structure. Limited real-time visibility, rigid processes, and vendor dependencies hamper operational flexibility. Patterns of reactive behavior, siloed operations, poor use of data, antiquated systems, and difficulties in inventory management further weaken supply network responsiveness. Structurally, the complex, global, and often fragmented nature of defense supply chains, along with cybersecurity vulnerabilities and inflexible contracts, compound to reduce supply network system adaptability to modern defense requirements specifically as it relates to contested logistics. Addressing these challenges requires leveraging advanced technologies like real-time data integration, predictive analytics, and dynamic response capabilities, as well as fostering cross-functional collaboration and introducing flexible contracting mechanisms. By examining the current state of generalized supply networks with a focus on defense supply network management systems, these problem areas pertaining to Function, Behavior, and Structure are revealed. These methods and revelations are outlined in depth in the critical review of the literature in Chapter 2.

Question 2
How are defense supply network responses designed to handle variation and disruption with respect to the AoP Machine: People, Processes, and Resources?

Q2 is rooted in the analysis of defense sustainment operations, one of the large stakeholders within defense supply networks that interacts with defense logistics, defense contractors, software, research and development, with significant military and civilian interactions. Defense sustainment has been further specified to Air Force sustainment operations due to their open-source framework, the *AoP*. This framework is hinged on the interaction between leadership and the sustainment or production Machine made up of three central components: People, Processes, and Resources. By evaluating variation and disruption response techniques in terms of the AoP Machine gaps can be identified in currently deployed frameworks and serve as a guide towards further improvements or applications in other systems. **Q2** is also based in the reframing of the AoP Machine as a cyber-physical-social system (CPSS). For this reason, the answer to **Q2** lies in the review and comparison of the AoP Machine when modeled as a cyber-physical-social system.

For the purposes of this thesis the AoP Machine has been analyzed from the perspective of a CPSS. In both a CPSS and the AoP Machine the human element in defense supply networks plays a critical role in encouraging adaptability and resilience. For example, skilled personnel are essential for making real-time decisions, assessing risks, and implementing contingency plans when disruptions occur. To retain and develop skilled personnel, training programs need to include the development strategic cross-functional teams that are capable of responding swiftly to changing conditions and collaborate effectively across various defense organizations and among defense supplier relationships. Additionally, cultivating a culture of strategic and experience-based autonomy within the workforce can empower individuals to take initiative and leverage their expertise in continuous process improvement and problem-solving. Workforce empowerment is also a core tenant of the AoP Leadership Model but is often subjective and allocated to structured leadership hierarchies rather than more horizontal or bottom-up organizations. However, regardless of hierarchical organization by enhancing communication and collaboration among personnel, defense organizations can better manage both variation and disruption within the context of supply network impacts. The CPSS perspective takes the element of people or social to the next step. This evolution involves integrating a CPSS approach that holds the user and the worker in the position of a stakeholder rather than a component of the AoP "Machine" ensures that the defense supply network can respond dynamically to emerging challenges, adapting strategies to meet complex needs.

The Processes employed in defense supply networks are intended to be flexible and responsive, allowing for quick adjustments when responding to variation but can fall short in the face of disruption. These modern supply network management techniques, focused on optimized, standardized, and agile systems, promote iterative planning and continuous improvement, with the goal of organizations to be able to continually optimize their operations. This optimization does result in lean supply networks, but this leanness results in fragility. For instance, adopting just-in-time (JIT) inventory strategies helps to minimize waste and reduce lead times, but these strategies are often complemented by just-in-case (JIC) practices that ensure essential supplies are available during unexpected disruptions. While beneficial when situations are predictable and responses can be standardized, these procedures do not account for emerging properties and needs due to their reliance on historical data. Rather than focusing on the individual parts that may need to be managed through inventory, the methods and structures that support the quick allocation of any product need to be the focus. This will rely on the integration of advanced technologies, such as predictive analytics and artificial intelligence. These advancements, when used strategically, can enhance forecasting capabilities and enable more dynamic risk assessment. By coupling historical data and processes that generate valuable real-time information, defense supply networks can anticipate potential disruptions and implement proactive measures, thereby mitigating their impact.

For the third component of the AoP Machine, effective management of Resources is vital for enabling defense supply networks to manage variations and disruptions. This includes not only tangible assets like materials, equipment, and transportation but also intangible resources such as technology and information systems. Defense organizations are increasingly investing in robust information and communication technologies that provide real-time visibility and facilitate collaboration across the supply chain. These systems can enable tracking of inventory levels, shipment statuses, and supplier performance, allowing for rapid identification of potential issues when coupled with the cyber framework capable of recognizing potential problem areas. Additionally, diversifying supplier bases and logistics partners can reduce dependence on single sources, thereby enhancing resilience. By maintaining alternative supply routes and backup suppliers, defense networks can better navigate disruptions and ensure continuity of operations.

To answer **Q2**, the ability of defense supply networks to handle variation and disruption is fundamentally rooted in the smaller scale AoP Machine, which relies on the effective integration of People, Processes, and Resources. This integration is based in the belief that more collaboration and communication will result in a more positive outcome when systems experience variation and disruption. The emphasis on collaboration must however be practical. This practically is rooted in satisficing solutions rather than optimization of the human element in terms of stakeholders. The satisficing solution is based in compromise decision selection and resolutions of Dilemmas among the defense supply network stakeholders: Government, Supplier, and User. Based in Tension identification, the preliminary Dilemma resolutions, which serve as the foundation for the development of the Requirements List can be found in Chapter 3. However, the analysis is taken a step further in Chapter 4 where the AoP is specifically analyzed from the CPSS perspective, to identify framework gaps. Both Chapter 3 and Chapter 4 are instrumental in the development of the answer **Q2**. To summarize, empowering skilled personnel, developing and adopting flexible processes and resource management, defense organizations, when modeled as CPSS, can enhance system adaptability and responsiveness in an increasingly complex and unpredictable operational environment. The CPSS approach ensures that defense supply networks are well-equipped to navigate challenges while maintaining mission readiness as cyber-physical-social systems.

Question 3
How can an inherently structured, lean, but fragile environment like defense sustainment be dynamically integrated into a flexible and fail-safe supply network?

Q3, or how can integrating an inherently structured, lean, but fragile environment like defense sustainment into an agile, flexible, and fail-safe supply network, requires a comprehensive approach that balances existing operational frameworks with the need for flexibility and adaptability. The first step involves assessing and redefining the current systems and frameworks to identify areas where lean principles can coexist with flexibility. Defense sustainment systems often prioritize efficiency, focusing on minimizing waste and reducing costs which as recipients of tax dollars fiscal responsibility is paramount. However, this focus on leanness can lead to fragility when these systems experience unexpected disruptions. By shifting to a system perspective that embraces components of flexibility alongside lean practices, defense organizations can create a fail-safe framework that allows for rapid response to changes in mission requirements or supply network dynamics.

One strategy for answering **Q3** aimed at achieving this integration is through the implementation of advanced technologies that enhance visibility and data-sharing across the supply network. Real-time tracking systems, predictive analytics, and decision-support tools can provide valuable insights into inventory levels, demand fluctuations, and potential disruptions. By leveraging these technologies, defense sustainment operations can shift from reactive to proactive management, enabling timely adjustments to resource allocation and supply chain strategies when met with variation. For instance, the use of data analytics can help identify trends and forecast demand, allowing for better planning and more informed decision-making. This dynamic integration of technology fosters a culture of agility, enabling the defense supply network to respond swiftly to evolving challenges while maintaining lean operational efficiencies. This technology, however, must remain secure which reduces its ability to move freely through non-defense systems like those of Suppliers. Additionally, many cyber-physical systems within defense organizations are still antiquated, when compared to current technological advancements, due to these stringent security requirements leaving the system vulnerable to disruption. Therefore, the cyber-physical system design is not sufficient to meet the response needs in the case of variation and disruption.

An additional layer to further develop the cyber-physical system is the inclusion of social to form a CPSS. The social component can manifest in a variety of ways whether at the smallest unit of the individual to the social hierarchy of an entire government. At the individual or team level, establishing cross-functional training to facilitate shared terms of communication and intra-organizational collaboration, ensuring that all parties are aligned in their goals and strategies. This collaborative approach can improve operational effectiveness and build trust and shared accountability, enabling faster responses to disruptions and more effective resource management based on expertise. The addition of social at the macro level involves the integration of stakeholder priorities based in satisficing decisions, or compromise. Collaboration, or the vehicle of compromise, is presented as the essential element in merging structured defense sustainment operations with features of supply networks more capable of flexibility. Collaboration-based relationships can widen a defense organization's access to additional or different People, Processes, and Resources found in other organizations. In the defense sector, collaboration is better known as partnership. So, for defense specific environments, fostering strong partnerships among various stakeholders like military branches, allies, contractors, suppliers, and logistics providers, defense organizations can enhance information sharing within collective problem-solving environments often bounded by contractual or diplomatic boundaries.

Finally, promoting a culture of continuous improvement is critical for sustaining this integration over the long term. Continuous process improvement is heralded as the gold standard in the AoP and is an attempt at addressing the evolution of a system throughout the life cycle in basic terms. System evolution is not expressly defined however, and much is left to interpretation within the bounds of the AoP framework. Ultimately, defense organizations are governed by larger governmental bodies and are subject to their authority. Flexibility cannot simply be added to a defense supply network design without considering security and cost constraints. Given the constraints inherent in defense environments, satisficing based decisions are likely the best compromise for infusing flexibility into inherently rigid systems without sacrificing the integrity of system security and prioritizing cost effectiveness while meeting mission goals.

In summary, the dynamic integration of a structured, lean, but fragile defense sustainment environment into a flexible and adaptable supply network requires a multifaceted approach that prioritizes compromise. By first identifying constraints among stakeholders in the defense supply network environment using the open-source constraint management framework, AoP, requirements were developed to preliminary identify what is needed to move the network towards fail-safe. The work is particularized for gap identification within defense sustainment operations within defense supply networks in Chapter 4 for the development of requirements for designing dynamically managed lead times based in CPSS design. The preliminary requirements include leveraging advanced technologies for visibility and data sharing, emphasizing collaboration among stakeholders, and cultivating a culture of continuous improvement by integrating social components into traditionally cyber-physical systems. By addressing defense supply network variation and disruption response from the perspective of a collaborative CPSS, defense organizations can potentially integrate of principles of strategic flexibility into systems for increased operational resilience.

5.2.4 Defining Dynamic Management of Lead Times (DMLT)

Dynamic management of lead times in supply networks, when based on satisficing solutions, refers to managing the timing and coordination of supply chain activities to achieve "good enough" outcomes rather than ideal or optimized ones. In the context of defense specific operations, where constraints such as heightened security, inflexible budget, and geopolitical challenges are significant, dynamic management of lead times can be achieved through timely adjustments in procurement, production, and delivery processes without overburdening the system or exceeding its capacities. The focus is on achieving functional, acceptable outcomes that ensure the continuous flow of critical materials and equipment in support of defense missions, rather than striving for complete efficiency, which may not be practical or realistic in environments of significant uncertainty.

As described in more detail in Section 2.3.2, mitigating negative impacts from variation and disruption includes an incorporation of both proactive and reactive responses. When defining dynamic management of lead times (DMLT), the definition must include both proactive and agile reactive coordination of people, processes, and resources to ensure timely delivery necessary to support defense operations. DMLT includes continually adjusting lead times throughout supply chains that make up the supply network from procurement and acquisition to distribution and deployment. The goal of dynamically managing lead times within a defense supply network is rooted in maintaining operational readiness, supporting mission-critical activities, and ensuring appropriate resource allocation in an environment of evolving uncertainties and potential threats.

Satisficing decision selection plays a key role in the work presented in this thesis. Defense supply networks are often constrained by rigid structures, budgetary restrictions, and long approval cycles. Thus, instead of aiming for perfectly optimized lead times, which can be difficult due to changing operational needs and unpredictable disruptions, satisficing emphasizes the need for feasible, adaptable solutions that meet minimum operational requirements. This means defense planners and logisticians prioritize meeting the most critical needs of the supply chain, accepting that some inefficiencies may occur but ensuring that mission objectives are still met. For example, instead of waiting for the least expensive supplier to deliver a part, the supply network might use a more expensive, but reliable, local supplier to ensure timely delivery during a high-priority mission. The choice to move to the more expensive supplier represents a compromise between speed, cost, and quality.

In practice, satisficing solutions in dynamic lead time management rely on flexibility, real-time data, and collaboration. Defense organizations must establish adaptable processes that allow for rapid adjustments to lead times in response to new information, such as a sudden change in demand or a disruption in the supply chain. This could involve temporarily switching and approving a move to alternate suppliers, expediting or altering transportation routes, or reallocating resources to where they are most urgently needed. The use of real-time data and advanced decision-support systems can ensure that these decisions are informed by up-to-date insights into supply chain conditions, while collaboration across different users, governmental entities, contractors, and suppliers ensures that all stakeholders can work together to address disruptions swiftly.

In summary, dynamic management of lead times based in satisficing solutions includes the recognition that defense supply networks must balance flexibility with the realities of their operational environment. The goal is not perfection but rather to maintain a functional and fail-safe supply chain that can adapt to challenges while meeting mission-critical needs. These recommendations represent the environment in which dynamic management of lead times can be achieved (Figure 5.2). By accepting the trade-offs inherent in satisficing decisions, defense organizations can better manage the complexities of lead times in an uncertain, resource-constrained environment.

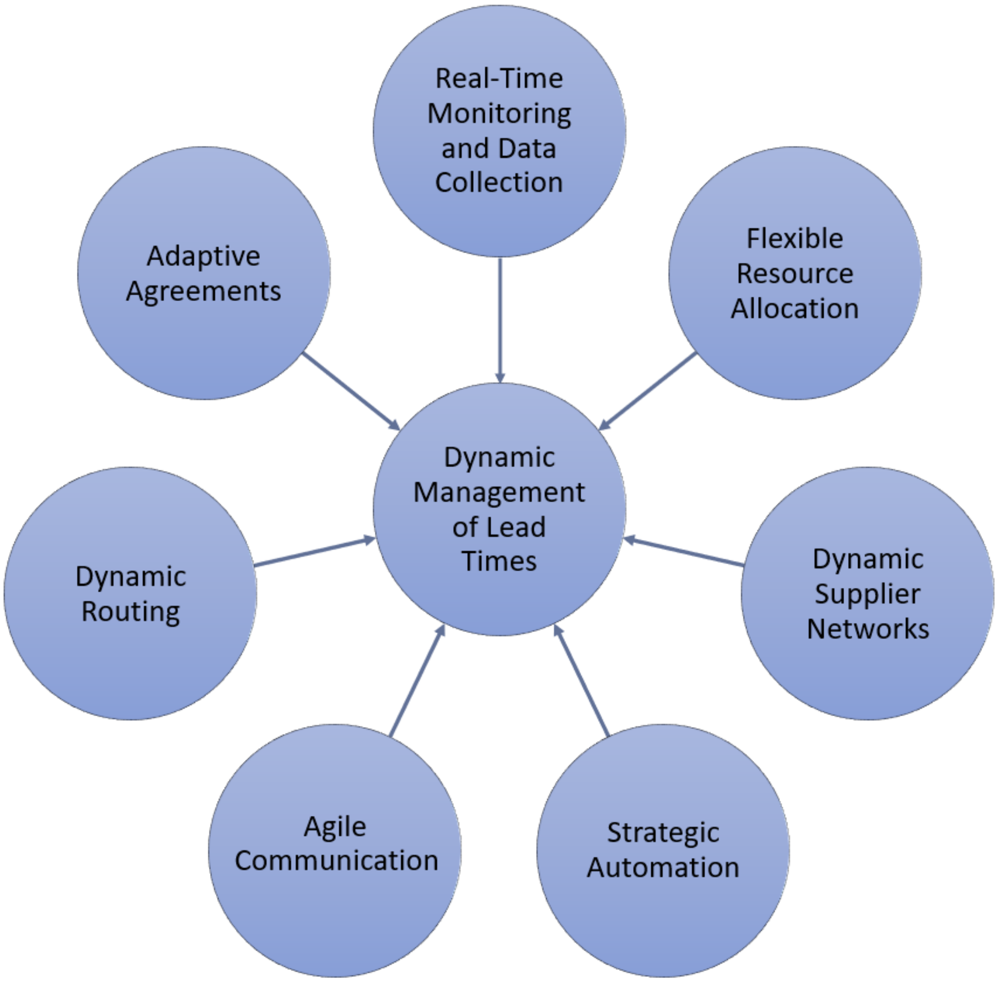

Figure 5.2: The Ingredients for Dynamic Management of Lead Times

5.3 Verification and Validation

This thesis is based on the Validation Square to ensure that the recommendations developed in this work are supported with high confidence. The Validation Square is a framework used to evaluate the robustness of a design method by examining its theoretical and empirical validity across structural and performance dimensions (Seepersad, Pedersen et al. 2006). It ensures that the method is internally consistent and logically sound, referred to as Theoretical Structural Validity, where the constructs of the method are coherent both individually and together. The framework also assesses Empirical Structural Validity to determine whether the chosen example problems are appropriate for testing the elements of the method. In terms of performance, Empirical Performance Validity includes an evaluation of the method's ability to generate useful and practical results when applied to real-world, comprehensive problems. Finally, Theoretical Performance Validity includes the evaluation of the overall ability of the method to address complex problems, which may require a "leap of faith" but is supported by the confidence built through the earlier validation processes. Together, these aspects ensure that the method is both theoretically sound and practically useful.

The work in this thesis is guided by a roadmap that relates to the Validation Square that serves as an outline for the structure, content, and flow of research focusing on dynamic lead time management within multi-stakeholder defense supply network environments. The map displayed in Thesis Roadmap Figure 5.3 includes all six chapters of the Thesis, and how each includes key components related to the gap analysis in defense supply networks lead time management techniques in a way that relates to the process of verification and validation.

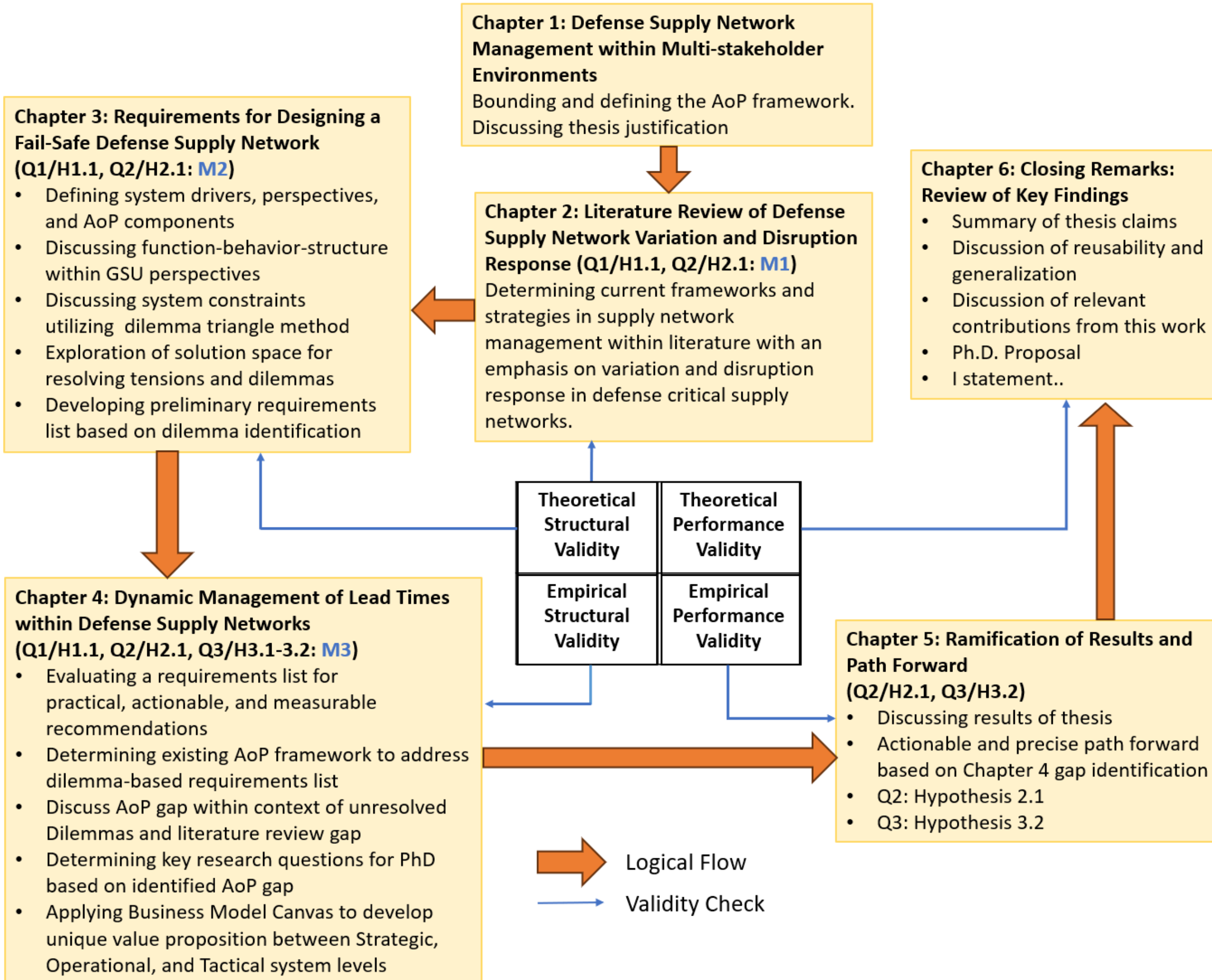

Figure 5.3: Thesis Road Map

5.3.1 Theoretical Structural Validity

Theoretical Structural Validity refers to the internal consistency of a method, ensuring that the framework or model in question is logically sound and coherent within its structure (Seepersad, Pedersen et al. 2006). In the context of verification and validation, theoretical structural validity involves assessing whether the components of a method or framework align logically and whether they function as intended within the given system. This quadrant, quadrant 1 in the Thesis Roadmap Figure 5.3, and step in the Verification and Validation process is critical for verifying that a framework is not only theoretically sound but also applicable in real-world scenarios. In examining the existing DOD Air Force sustainment center framework, known as the AoP, it is essential to identify both consistencies and inconsistencies within the framework itself and its application in current practices. These inconsistencies can be a step towards gap identification. This involves a thorough analysis to determine if the framework maintains its internal logic when applied to real-world defense sustainment operations. Furthermore, identifying gaps within the AoP framework is crucial, particularly those that leave supply networks vulnerable to disturbances. These gaps must be examined from the perspective of a cyber-physical-social system to assess whether the framework is robust enough to handle variations while still maintaining its adherence to simplicity and standardization. This analysis of theoretical structural validity extends into a broader discussion of cyber-physical-social systems within the context of the AoP and defense supply networks in Chapter 2 and Chapter 3. By examining the current state of these systems and identifying areas for improvement by developing a requirements list based on constraint identification and resolution, the aim is to reach a desired state of fail-safe operations, where the framework is not only theoretically valid but also practically flexible in the face of potential disruptions.

5.3.2 Empirical Structural Validity

Empirical Structural Validity deals with the appropriateness and relevance of the example problems or case studies used in modeling a method (Seepersad, Pedersen et al. 2006). This quadrant of the Validation Square involves assessing whether the scenarios or problems selected for analysis accurately represent the conditions under which the method will be applied, ensuring that the model's outcomes are valid and applicable to real-world situations. In the context of this thesis, empirical structural validity, Quadrant 2 in the Thesis Roadmap, Figure 5.3, includes the focus of systematically validating the solution space and evaluating the methods discussed and demonstrated in Chapter 4. This involves a thorough examination of whether the AoP framework from a cyber-physical-social system chosen for modeling a defense supply network accurately reflects the complexities and challenges faced by defense sustainment centers. The evaluation will include a justification and clarification of the satisficing solutions or solutions that meet several acceptable criteria rather than a single optimized solution, applied to the identified constraints or dilemmas. Additionally, by simulating a defense sustainment center from a business perspective using the Business Model Canvas, a value proposition is established, and key components of the system are outlined. The goal is to ensure that the hypothetical simulations are not only theoretically valid but also practically applicable, providing insights that can be effectively translated into real-world defense sustainment practices and stakeholders.

5.3.3 Empirical Performance Validity

Empirical performance validity refers to the degree to which the application of a method to sample problems yields practical and useful results (Seepersad, Pedersen et al. 2006). In the context of verification and validation, it ensures that the method, when applied to real-world or simulated scenarios, produces outcomes that are not only theoretically sound but also actionable and effective in addressing the given challenges. In this thesis, empirical performance validity is based on determining whether the solutions or methods developed in this thesis generate practical, real-world applications when applied to comprehensive or additionally complex problems. This section, corresponding to Quadrant 3 in the Thesis Road Map shown in Figure 5.3, includes the emphasis on the ability of the simulated defense sustainment center within the context of a defense supply network, developed in the earlier phases, to test solutions for the research questions and hypotheses previously established. Specifically, the assessment centers around whether the outcomes derived from applying the method to the sample problems provide meaningful and actionable insights for Questions 2 and 3. This quadrant includes significant emphasis on the development of validated recommendations, ensuring that the recommendations developed in the thesis not only function within a theoretical framework but also perform effectively when confronted with real-world defense sustainment challenges. The practical applicability of the findings is key, as it determines whether the solutions proposed can be implemented in actual defense environments to improve operations, enhance resilience, and address systemic issues.

5.3.4 Theoretical Performance Validity

Theoretical Performance Validity refers to the extent to which the application of a method to various problems produces both practical and generalizable results (Seepersad, Pedersen et al. 2006). In the context of verification and validation, this involves evaluating whether the method, when applied to different scenarios beyond the initial problem set, continues to yield meaningful and applicable outcomes. This ensures the robustness and adaptability of the method across diverse contexts. In this thesis, theoretical performance validity, Quadrant 4 in the Thesis Roadmap Figure 5.3, includes the culmination of the efforts made in the previous quadrants, synthesizing all prior findings and testing the method's applicability to a broader range of problems. This quadrant serves as the final sections of this thesis, including a comprehensive discussion of all claims made throughout the research. It also includes an evaluation of the reusability and generalization of the methods, ensuring that the approach is not only valid for the initial problem set but also applicable to other defense-related challenges. Additionally, this section includes a proposition for future research focuses through identifying gaps in current knowledge and methods discovered while producing this thesis. This thesis will culminate as a PhD proposal that outlines potential areas for further investigation, aimed at expanding the scope of the method and advancing the development of new knowledge in the field of systems engineering. In addressing theoretical performance validity, the proposed method of dynamically managed lead times relevance is demonstrated contributing to utility in a variety of defense or industry operations and sustainment practices.

5.4 Ramification of the Results

5.4.1 Multidisciplinary to Transdisciplinary Value

Multidisciplinary research in engineering involves collaboration between experts from different fields, each bringing their specialized knowledge to solve a problem. However, in this approach, each discipline typically works within its own boundaries, contributing insights that are later combined to address the issue. In engineering education, multidisciplinary studies have been the forefront of new academic techniques for the next generation of engineers. This approach can expose students to fields like mechanical, electrical, and computer engineering, allowing them to see how each discipline independently contributes to solving complex problems outside of their major focus. The emphasis remains on the distinct roles and perspectives of each discipline, making this approach ideal for projects that benefit from a segmented but collaborative approach. Transdisciplinary research, in contrast, takes the collaboration a step further and rather than simply integrating expertise from multiple subsections of a particular field, it involves merging disciplines both within and outside of the original field. In engineering, this approach can encourage the development of new methods or frameworks that transcend traditional disciplinary limits, allowing for more holistic and comprehensive problem-solving. While multidisciplinary research may offer depth in specialized areas, transdisciplinary research is better suited for addressing complex, interconnected problems that require evolving or comprehensive solutions, making it ideal for industries tackling global challenges like sustainability, smart infrastructure, or systems engineering. A case for which is better can be based in the goal of the researchers and the problem being addressed. For the purposes of this thesis, multidisciplinary research is effective for well-defined problems based often in cyber-physical systems requiring multiple perspectives, while transdisciplinary research is more diverse and flexible for addressing broad, systemic issues found within cyber-physical-social systems.

5.4.2 Revisiting Resilience

This work begins with a focus on the development of a list of requirements in order to design a fail-safe defense supply network capable of dynamically managing lead times in the face of both variation and disruption. The goal of developing a fail-safe system of defense supply networks within the context of a master's thesis is a lofty goal therefore for the purposes of this thesis the goal of fail-safe must be addressed in terms of level of uncertainty and autonomy within the AoP system and a system designed as a comprehensive CPSS (Figure 5.4).

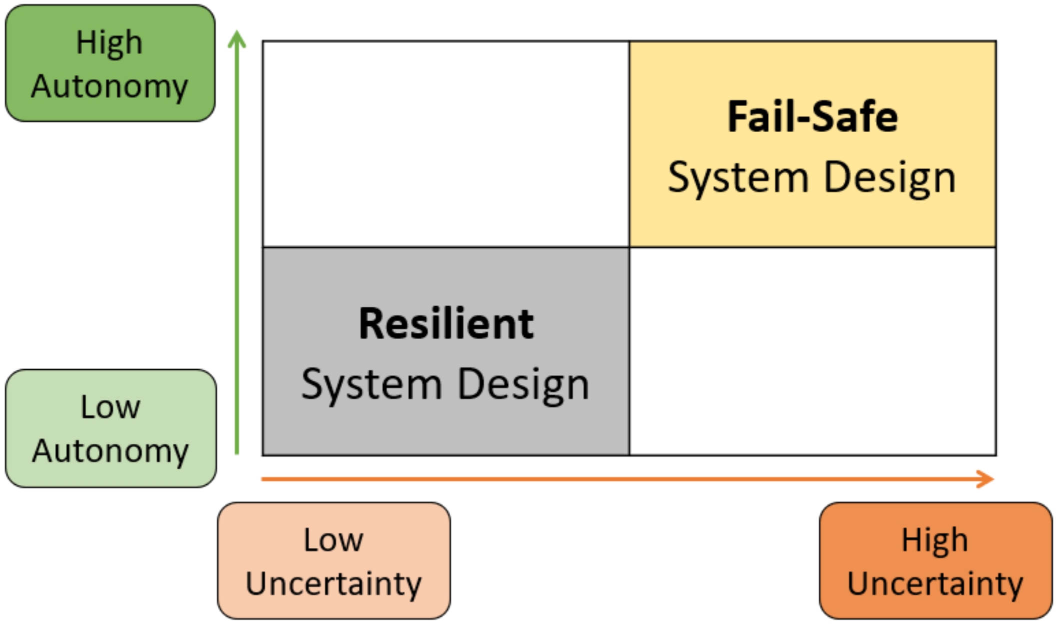

Figure 5.4: Fail-Safe System Design within the Context of Uncertainty and Autonomy

Shifting this thesis from the goal of resilient system design to fail-safe system design in the context of defense environments reflects a significant evolution in how defense supply network systems can be conceptualized and managed. Resilient system design focuses on preventing failure with respect to variation by either anticipating all potential points of system constraints or designing mechanisms to ensure that, in the event of a disruption, the system defaults to its original state. This is vital in defense systems like weaponry, aircraft, or missile defense, where safety in failure scenarios is paramount. However, resilient systems under the currently available frameworks tend to be rigid, designed around pre-identified failure modes, and often assume a relatively static set of threats or operational conditions and thus operate in conditions of low uncertainty and low autonomy. The relationship between resilient system design and the AoP is that the AoP was designed to provide prescriptive and standardized methods of variation response within complex defense sustainment environments. Given this perspective, the AoP mainly serves as a guide to manage systems of low uncertainty and low autonomy. However, the addition of the Leadership Model and an emphasis on leaderships role to address systems of high uncertainty the AoP serves as a guide and toolbox of potential techniques leaders can take to move a system towards fail-safe. The initial merging of both cyber-physical and social systems is one way the AoP framework takes a step towards fail-safe system design.

5.4.5 The Way Forward

This thesis, through exploring the requirements for fail-safe system design and dynamic management of lead times, primarily serves as the foundation for the development of research questions for further study. By studying the limitations and rigidities of resilient systems, particularly in an AoP-based defense supply network, it is clear that these systems may struggle to adapt to both variation and disruption. The requirements developed for dynamic management of lead times, framed through the lens of satisficing solutions, reveal the need for more flexible, adaptive approaches in handling supply network uncertainties that include an incorporation of CPSS principles. These insights lay the groundwork for moving toward fail-safe system design, which focuses not only on preventing failures but also on maintaining operational continuity in the face of disruption in a system that has the ability to change its function, behavior, or structure to meet evolving situations (Figure 5.5). This thesis, therefore, positions fail-safe system design as the way forward, building on the lessons learned from resilient approaches and emphasizing the importance of adaptability, agility, and collaboration within complex systems.

Fail-safe system design, as proposed, includes an emphasis on adaptability, recovery, and continued functionality under a wide array of unforeseen variations and disruptions to the system. In the defense sector, the move towards fail-safe is crucial as modern military systems face increasingly complex and dynamic threats, including cyberattacks, modern warfare, contested logistics, and unpredictable geopolitical environments. Fail-safe systems are designed to react gracefully, maintain critical functions, and recover quickly through change after disruptions. This paradigm shift acknowledges that it is impossible to foresee every potential failure mode in today's defense landscape. Thus, the focus moves from preventing failure entirely to building systems that can withstand, adapt to, and recover from unexpected disruptions, maintaining operational capabilities in difficult situations. This makes fail-safe system design potentially more suited to modern, asymmetrical warfare and the rapidly evolving defense landscape.

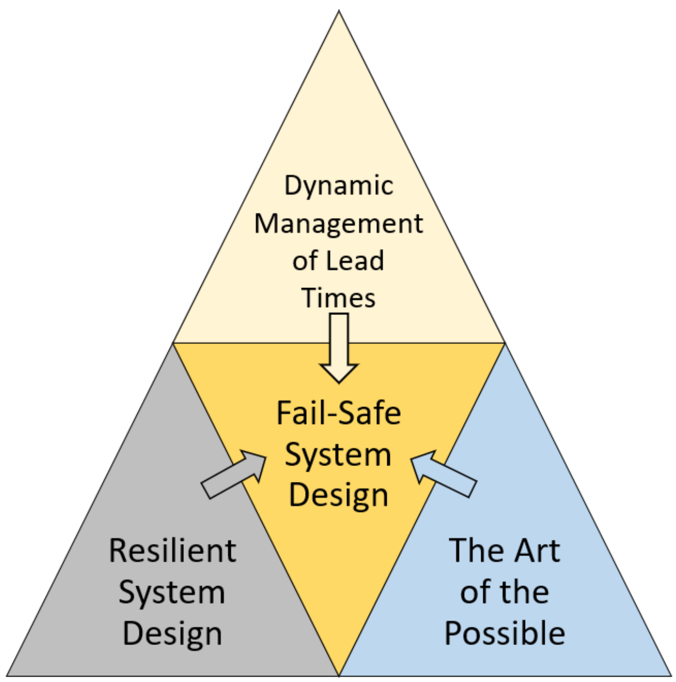

Figure 5.5: The Way Forward

5.5 Closing Remarks

In conclusion, this thesis includes a definition and analysis of the complexities and challenges inherent in defense supply network management, particularly through the lens of fail-safe system design and the dynamic management of lead times. By examining the current limitations of rigid, lean, and often fragile systems, it has become clear that such approaches, while useful in predictable and stable environments, may not be sufficient to meet the evolving demands of modern defense logistics. These systems tend to lack the flexibility and adaptability required to respond effectively to the uncertainties posed by geopolitical instability, supply chain disruptions, and shifting operational needs. The dynamic management of lead times, rooted in satisficing solutions, has been identified as a key mechanism for addressing these challenges by enabling real-time adjustments and prioritizing mission-critical outcomes over idealized efficiency.

Building on these insights, this research serves as the groundwork for a broader shift towards fail-safe system design, which emphasizes the ability of systems to not only prevent failure but to adapt, recover, and thrive in the face of disruptions. The lessons learned from studying resilience-based systems and lead time management provide critical pathways for developing fail-safe defense supply networks. By offering that, the integration of advanced technologies, fostering cross-functional collaboration, and adopting flexible strategies that account for cyber, physical, and social factors, defense organizations can better navigate the uncertainties of the future. This thesis, therefore, represents a foundational step toward a new era of supply network management: one that prioritizes adaptability, flexibility, and continuous improvement in the face of unpredictable constraints to ensure mission readiness in even the most challenging environments. Ultimately, the findings and frameworks outlined in this thesis serve as a first step in understanding the need to evolve from rigid resiliency-based designs to dynamic and fail-safe systems. As defense supply chains become increasingly complex and interconnected, the ability to dynamically manage lead times and embrace fail-safe principles will be critical for maintaining operational continuity. Future research in the form of a Ph.D. dissertation on fail-safe system design, outlined within Chapter 6, will continue to build on these concepts, exploring new ways to integrate fail-safe principles into the fabric of defense logistics, ensuring that the supply networks of today are better equipped to handle the variations and disruptions of a rapidly changing world tomorrow.

CHAPTER 6: CLOSING REMARKS: REVIEW OF KEY FINDINGS, CONTRIBUTIONS, and Ph.D. PROPOSAL

6.1 Critical Review of the Thesis

To critically review this thesis, the work will be evaluated based on the following categories, the initial problem definition, the literature review, the methods used to evaluate gaps, and the results of the thesis. Primarily, this thesis includes an exploration and evaluation of dynamic lead time management within the context of defense supply networks and defense sustainment using the AoP framework to identify gaps in defense system design when modeled as a cyber-physical-social system (CPSS). The work is centered around three questions that build on each other in an attempt to first evaluate the stakeholder environment defense supply networks operate in, the validity of defense specific methods and frameworks for lead time management, and gap identification towards the development of a requirement list for fail-safe systems.

While the topic is highly relevant to defense logistics and supply chain management, the framing of the questions could be clearer, particularly in terms of how the AoP framework and CPSS modeling intersect. The difficulty lies in that the AoP framework includes standardized procedures for physical and social components but refers to cyber in the abstract through the context of Processes. The importance however is that the social aspect is often overlooked or may only include social as the inclusion of the workers through leadership influence rather than stakeholder integration. The importance of incorporating social components in terms of stakeholders into lean cyber-physical systems is well justified, but the rationale for choosing AoP as the guiding framework is based in the widespread impact of the AoP framework and the open availability of the document. Additionally, the justification for analyzing the AoP lies in the author's unique experiences. As this work was produced in adherence to academic guidelines much of the personalization was left until the "I statement" at the end of this chapter which pulls the work together through a personal lens.

6.2 Towards Dynamic Management of Lead Times

The objectives in this thesis are threefold: first, to develop a requirement list within the context of defense supply networks through identification and propositions for the elimination of stakeholder dilemmas; second, to identify gaps in current lead time management frameworks using the test case of defense sustainment and the AoP, and thirdly, to identify and prioritize key research gaps that can be explored to develop new knowledge in a Ph.D. based in fail-safe system design. By analyzing the system dynamics within defense supply network logistics and assessing gaps in lead time management within these complex systems, the key areas where existing frameworks fall short, particularly in integrating social components and trade-off decision-making components is highlighted. These gaps serve as a foundational basis for further research and are instrumental in the development of a Ph.D. proposal, focused on addressing the gaps identified in this master's thesis through the lens of evolving cyber-physical-social system principles in policy development.

The literature review, in Chapter 2, includes a broad overview of cyber-physical systems, the AoP framework, and dynamic lead time management in generalized and defense-specific logistics and serves as a foundation for the subsequent chapters. However, while the review touches on key concepts, it lacks depth in certain areas, particularly in critically engaging with existing research on specifically designed and deployed CPSS. The integration of social components into cyber-physical systems is a crucial aspect of the thesis, yet the discussion of social component modeling is underdeveloped which mirrors the current research gaps needing further work and exploration. However, the thesis includes a focused exploration of the existing challenges and limitations in current lead time management approaches, particularly within defense sustainment, using real data provided within the AoP document to better frame the research gap. In this case, real-time data would have been beneficial, but for the purposes of evaluating the AoP framework the data contained within the open-source document was sufficient. Overall, the literature review covers relevant areas and fully situates the thesis within the broader academic conversation and identifies clear gaps and cornerstone research areas in need of further development.

The methods used in this thesis are centered around modeling lead time management as CPSS to identify constraints and develop a requirement list for dilemma resolution as a dynamic process within a defense-based system. The basis and justification for combining cyber-physical components with social components as CPSS is appropriate but still lacks quantification due to the fluid nature of social components. The social components are explained at a macro level in Chapter 3 through the examination of stakeholder interactions in terms of constraints within Functions, Behaviors, and Structures. And in Chapter 4, System Archetypes are utilized to visualize system patterns as it relates to large social components of defense organizational hierarchies contained within the AoP. Developing methods quantifying and integrating social components into existing systems remains a major research gap and is foundational to the work proposed for a Ph.D. in later sections of this chapter. Additionally, the use of the AoP framework over other potential frameworks for dynamic system management is justified on the basis that defense sustainment operates as one of the larger defense systems within the defense supply network that is not solely based in logistics support.

The results of the thesis are presented in a structured manner, showing how the incorporation of social components could impact lead time management when modeled as a CPSS in addition to identifying gaps for further research. The results include the development of a requirements list based on inter-stakeholder dilemma resolutions, key gap identification within current literature and the defense sustainment-based lead time management framework, the AoP, development of a value proposition for defense sustainment from a business perspective and identifying research gaps for the development of a Ph.D. proposal and dissertation plan. The thesis could include a more thorough analysis of the specific trade-offs involved in balancing cyber, physical, and social components, but as these trade-offs are highly specific for certain stakeholders and a more generalized approach is taken in this work. The types of trade-off decisions are identified instead. For example, there are specific cases where the inclusion of social components complicates system efficiency, and the strategic deployment of advanced automation is a better choice like in systems of cybersecurity. While the results are linked to the theoretical framework, the implications of these findings for real-world defense logistics can be explored in further depth in work beyond the pages of this thesis and serve as the basis for a Ph.D. explained in Section 6.3.

6.3 Relevant Contributions from this Work

6.3.1 Foundational Review of the Literature

Contained within Chapter 2, this thesis includes a comprehensive and foundational review of literature surrounding lead time management response to variation and disruptions, explanation of current defense and generalized supply network frameworks, and key identification of the unique challenges in defense-specific environments. Most notably, the inclusion and evaluation of disaster or pandemic related research that included dynamic supply conditions in environments of high uncertainty and low predictability offered a key avenue for developing test cases for further work.

6.3.2 An Approach for Framing Multi-stakeholder Supply Networks by Evidentiary and Interpretive Analysis

Chapter 3 includes the development of a new method to identify dilemma resolutions related to multistakeholder interactions in terms of Function, Behavior, and Structure (F-B-S). The environment of defense supply networks was reframed as interactions among three key stakeholder groups: Government, Supplier, and User. These interactions were then distilled into Tensions and Dilemmas according to the Dilemma Triangle Method (DTM). Once Dilemmas were identified, they were grouped based on Function, Behavior, or Structure and preliminarily resolved which served as the basis for the development of a Requirements List. Both the Nested F-B-S DTM and the Requirements List were supported by both evidence and interpretive analysis based on experience.

6.3.3 Gap Identification of Resilient System Design within the AoP

In Chapter 4, AoP is examined for gaps through an interpretation of System Archetypes and the use of the Business Model Canvas (BMC). The gap identification is primarily based in CPSS principles that include a comprehensive and holistic system integration of cyber, physical, and social components. The system framework contained and designed within the AoP is essentially a lean resilient system that prioritizes lean optimization but ultimately results in fragility in the face of disruption. Using the BMC on defense sustainment operations within the context of greater defense supply networks provides a structured and comprehensive way to analyze and identify various key components of these complex systems. The BMC includes a breakdown of the key aspects of defense sustainment from a business perspective allowing for a better understanding of how these elements may interact. In defense sustainment, where operations are mission-critical and involve high levels of coordination, understanding how each part of the supply network functions is vital for identifying the gap between design perfection and system failure.

6.3.4 Establishing Foundational Requirements for DMLT

Chapter 5, which includes the establishment of foundational requirements for the dynamic management of lead times in defense supply networks by addressing the gaps in traditional system designs, highlights the limitations of rigid, lean approaches, which may perform well in stable environments but struggle to adapt to the unpredictable nature of modern defense logistics. By examining resilient system design, the basis for the development of the AoP, and the need for more flexibility it is proposed that dynamic lead time management, driven by satisficing solutions, is essential for real-time adjustments that prioritize mission-critical outcomes over rigid efficiency. Chapter 5 includes the groundwork for a shift toward fail-safe system design, emphasizing adaptability, recovery, and responsiveness to variations and disruptions. It is proposed that integrating advanced technologies, fostering collaboration, and incorporating cyber, physical, and social factors into system design are critical and foundational requirements for achieving system resilience. Finally, the findings of the previous chapters are summarized and contextualized to pave the way for further exploration into fail-safe systems, setting the stage for future research in fail-safe system design in the development of a Ph.D. proposal.

6.3.5 Foundation for Future Research

The work in this thesis serves as the foundation and initial exploration into addressing critical challenges in defense supply networks, such as responding to variation and disruption, designing for cross-organizational autonomy, and managing multi-stakeholder environments with conflicting goals, creates a platform for further research into fail-safe system design and the development of new knowledge. This work not only exposes the limitations of traditional fail-safe and lean system designs but also illuminates the need for systems that can adapt, recover, and evolve in complex, uncertain environments. By framing these challenges through the lens of proactive and reactive system dynamics, cross-organizational autonomy, and satisficing tradeoff decisions, the thesis sets the stage for a Ph.D. that deeply explores fail-safe system design as an evolving cyber-physical-social system (E-CPSS). The Function, Behavior, and Structure of the E-CPSS design can be divided into four main research areas based on the gaps identified in this thesis:

1. **Responding to Variation and Disruption through System Dynamics:**

   This research area is focused on a system's ability to manage both anticipated and unforeseen disruptions which lies at the heart of resilience. By addressing how systems can respond proactively, through strategic predictive analytics and dynamic systemic planning, and reactively, by adapting in real-time, this thesis includes the beginning groundwork for researching how cyber-physical systems (CPS) can integrate social elements to enhance flexibility. A Ph.D. on fail-safe system design will focus on developing models for dynamic risk assessment, using real-time data to improve system recovery and sustain operations in defense and other critical industries. The evolution from static fail-safe designs to systems that not only withstand but also adapt to change forms a central pillar of fail-safe CPSS research.

2. **Designing for Cross-Organizational Autonomy:**

   Defense and other complex global multi-stakeholder environments require a high degree of organizational autonomy while maintaining coordination across diverse entities. This autonomy is essential for resilience, as it can allow individual components of a network to make decisions independently, ensuring localized adaptability. Research through a Ph.D. dissertation may expand on how cyber-physical-social systems can enable strategic distributed decision-making, allowing each organizational unit, whether military branches, contractors, or suppliers, to act autonomously while remaining aligned to a shared mission. By leveraging decentralized control within a CPSS framework, systems can be designed to maintain operational coherence even when central coordination is disrupted.

3. **Operating in Complex Multi-Stakeholder Environments with Conflicting Goals:**

   In environments focused on defense, where stakeholders often have multiple competing priorities (e.g., cost vs. readiness, security vs. agility), this thesis includes the introduction to the concept of satisficing, making tradeoffs that meet minimum acceptable outcomes rather than striving for perfect solutions, as a basis for CPSS design and resilience. Further research in a Ph.D. may delve into how satisficing-based decision frameworks can be embedded in fail-safe system design, ensuring that conflicting goals are balanced dynamically without compromising system integrity. The CPSS framework offers a way to model these complex interactions, incorporating the social aspects, human decisions, partnerships, and collaborations, alongside physical and cyber systems to better manage competing demands.

4. **Evolving Satisficing Tradeoff Decisions vs. Optimization:** Traditional optimization methods often fall short in complex, unpredictable environments where the optimal solution today may not hold tomorrow. By focusing on satisficing tradeoff decisions in environments of high uncertainty, this thesis serves as a case for an alternative approach where resilience is not about perfection but about adaptability. A Ph.D. may include an exploration on the mathematical basis for incorporating satisficing decision support principles to the design of fail-safe E-CPSS, investigating how tradeoff-based decision models can improve system survivability, adaptability, and long-term evolution. Rather than focusing on minimizing costs or maximizing efficiency, the research would emphasize how systems can continue to function effectively under changing conditions, even if all variables are not ideal.

In summary, this thesis is a foundation for advancing research into fail-safe system design, specifically as an evolving cyber-physical-social system. By addressing dynamic response mechanisms, cross-organizational autonomy, multi-stakeholder collaboration, and satisficing tradeoff decisions that evolve with system changes, it includes the groundwork for a Ph.D. on determining the principles for creating systems that evolve and adapt in real time for increased resilience. These systems would integrate not only physical infrastructure and digital technologies but also human factors, social dynamics, and organizational structures all key elements for building fail-safe systems capable of thriving in the complex, unpredictable landscapes of defense and beyond.

6.3.6 A Way Forward Specified

While several research avenues have been discovered as a result of the work done in this thesis, the central question of "How?" has not yet been addressed. For the purposes of determining a way forward, the focus will be on policy development for fail-safe system design as an E-CPSS. This will require a multi-layered approach that integrates flexibility, autonomy, and collaboration within defense and other critical supply networks. Policies must evolve to accommodate new technological advancements, changing geopolitical landscapes, and the growing complexity of multi-stakeholder environments.

To manage variation and disruption effectively, policies may need to adapt beyond rigid, fail-safe paradigms and embed dynamic decision-making capabilities. Defense supply networks should be designed to be supported by policies that promote real-time data integration, predictive analytics, and dynamic resource management within the environment of enhanced security. These policies may benefit from encouraged investment in technologies that enable proactive, predictive, and reactive approaches to disruptions, including tools for real-time monitoring and adaptive planning. This policy shift may create the necessary foundation for rapid system recalibration in response to changing operational conditions.

Defense policy frameworks currently emphasize strict hierarchies and centralized control, but fail-safe systems are believed to thrive on distributed decision-making and localized autonomy. To develop cross-organizational autonomy, policies may need to promote decentralized governance models that allow individual units to make decisions independently while maintaining alignment with broader strategic goals and units of command. This could involve redefining reporting structures in civilian settings, incentivizing collaboration across sectors, and ensuring that some decision-making authority is devolved to the lowest effective level, all while safeguarding against security risks.

Policies must evolve to support cross-functional, cross-organizational collaboration that bridges Government, Supplier, and User stakeholders. Defense environments, by nature, involve conflicting goals, such as cost, readiness, and security. Policy may need to emphasize partnership and communication across the entire defense ecosystem, creating frameworks for satisficing decisions that address tradeoffs in real time. This may include the development of new contractual and procurement policies and frameworks that allow more flexibility in shifting suppliers, adjusting priorities, or reallocating resources based on evolving mission requirements. Furthermore, policies may need to streamline communication channels, enhance data-sharing protocols, and foster public-private partnerships to better integrate civilian suppliers into defense networks without compromising security.

While each of these ways forward for developing fail-safe system design in policy as an E-CPSS, the central themes are incorporating satisficing-based decisions and integrating CPSS into evolving policy design for ensuring long-term continuous improvement. This could translate into policy frameworks that prioritize resilience over efficiency by allowing for more redundancy in supply chains, encouraging the diversification of supplier bases, and building in contingencies that help systems cope with disruptions. All of which will require tradeoff decisions based on the priorities of cost effectiveness, quality, and speed. Policies may benefit from moving away from rigid cost-cutting measures that prioritize efficiency at the expense of flexibility, allowing for a more balanced approach that sustains operational readiness even when disruptions occur. For integrating CPSS into policy design, this involves establishing policies that likely encourage the use of advanced cybersecurity protocols, while also ensuring that human factors, such as workforce training, organizational culture, and stakeholder engagement, are fully integrated into system design and management. Policies may incentivize the adoption of CPSS frameworks that view system resilience as a holistic challenge, encompassing not only technology and infrastructure but also the social and organizational structures that make them function effectively.

In conclusion, policy development in an evolving system must include direct advancements in flexibility and resilience in defense supply networks. Policies should also emphasize continuous improvement as a fundamental component of fail-safe system design. This means requiring regular system reviews, audits, and updates that integrate lessons learned from variations and disruptions. Such policies could include mandated adaptive feedback loops that allow for constant system refinement and adjustment, supported by strategic investments in new technologies through research and development. This could be further supported by flexible funding models that allow for flexible responses to changing conditions and evolving threats. By designing cross-functional autonomy, collaboration, and proactive adaptation, policies may be able to transform defense systems from being fragile and rigid into fail-safe and adaptable networks capable of handling modern-day disruptions. The development of E-CPSS framework-based policies, rooted in satisficing tradeoff decisions, could serve as a powerful model for evolving system resilience and provide a clear path for creating defense policies that support dynamic, responsive, and future-proof supply networks.

6.3.7 Towards Generalizability

While the work in this thesis is primarily centered on defense supply networks and the specific test case of defense sustainment constraint management frameworks, the issues present within defense supply networks do not only impact defense organizations. While defense supply networks primarily function as a means of national defense and are characterized by high levels of regulation, higher security concerns, and are particularly sensitive to geopolitical conflict as it relates to national security, industry partners are operating in many of the same environments and can equally benefit from fail-safe system design through policy. Specifically, the concepts of proactive and reactive system dynamics, satisficing trade-off decisions, and integrating E-CPSS design are relevant across various industries. For example, in commercial logistics and smaller industry specific supply chains, face similar disruptions due to natural disasters, geopolitical conflicts, or unexpected market fluctuations. The ability to dynamically manage lead times, establish a framework for diversifying suppliers, and adopt flexible but strategic organizational structures is crucial in any environment that values resilience. The research presented in this thesis can serve as a preliminary list of requirements that include enhancing cross-functional collaboration, utilizing real-time data, and balancing just-in-time (JIT) with just-in-case (JIC) strategies as a means of dynamically managing lead times and can be applied to industries like healthcare, aerospace, manufacturing, and even global humanitarian aid or disaster relief, where flexibility and rapid adaptation are equally important.

For the proposed way forward, the strategic integration of advanced technologies like predictive analytics, AI-driven decision support that utilizes satisficing based decisions, and real-time tracking systems has broad applicability. These tools are increasingly essential in industries such as retail, pharmaceuticals, and automotive manufacturing, where supply networks are global, and disruptions can severely impact operations. By generalizing the principles of cross-organizational autonomy, and collaboration within multi-stakeholder environments, and designing policy as E-CPSS, this proposed avenue towards new knowledge may serve as a valuable step for improving resilience in complex systems across a range of industries. While this thesis may include the groundwork for establishing dynamic management of lead times and gap identification in current system design, a way forward can include applying fail-safe system design beyond defense. The benefit of strategic flexibility and cyber-physical-social integration throughout system evolution to enhance the resilience, can have benefits for any supply network operating in a dynamic and unpredictable world.

6.3.8 Scholarship Achieved Through the Thesis

The academic scholarship achieved through this thesis is summarized in Table 6.1.

Table 6.1: Scholarship Achieved Through the Thesis

Academic Scholarship	Contributions in MS Thesis	Related Research Gap
Requirements for Designing a Fail-Safe Defense Supply Network Conference Paper – IDETC **Status:** Accepted	A Framework and an Approach to identifying and resolving Dilemmas within a multi-stakeholder defense supply network. Introducing new method of a nested F-B-S DTM.	RG1, RG2
DARPA Proposal: Securing Tomorrow **Status:** Rejected	An approach that anchors in foundational and fundamental model to design public policies by establishing the utility of interaction between E-CPSS and Collective Adaptive Systems.	RG3
Fail-safe System Design as an Evolving Cyber-Physical-Social System Funding source: Unknown **Status:** Section 6.3	Ph.D. Proposal	

6.4 Ph.D. Proposal

While this thesis includes the systematic identification and preliminary addressing of key research gaps in the context of defense supply networks as CPSS, this work has included the foundation for the identification of further research gaps with a potential to develop new knowledge. Through an in-depth exploration of existing literature and current defense constraint management frameworks using tools like the Function-Behavior-Structure construct, the Dilemma Triangle Method, the Business Model Canvas, and System Archetypes, the aim was to highlight areas where current research gaps exist or where emerging trends demand new approaches. By identifying these gaps, this work has included contributions to a broader understanding of the challenges and opportunities in designing fail-safe systems through the integration of physical, cyber, and social elements. The outcome of this gap analysis forms the foundation for proposing new research which will focus on a framework to design more responsive, fail-safe, and socially cognizant systems. This effort is further specified to focus on the development of E-CPSS in the context of policy design, social quantification and integration, and autonomous decision-making structures.

6.4.1 Gap Identification

To advance the field of cyber-physical-social systems (CPSS), several critical research gaps have emerged throughout the work in this thesis that warrant further exploration to enable more robust, adaptive, and socially integrated solutions for designing systems. While three major areas of focus have emerged, they must be prioritized for what is possible to address in a Ph.D. dissertation. They are prioritized here. First, *Designing Evolving Systems as Policy* is based in the need for policies that can adapt and evolve in response to dynamic technological and societal changes, moving beyond static regulatory frameworks. Second, there is a gap in understanding the role of *Social Components within Traditionally Cyber-Physical Systems*, particularly how human behaviors, social interactions, and collective decision-making can be more seamlessly integrated into systems that have traditionally focused on the interaction between physical and cyber elements alone. Finally, the rise of autonomous systems presents new complexities, particularly in relation to *Autonomy with Satisficing-Based Decision Support Systems*, where systems need to make "good enough" decisions in uncertain and dynamic environments, balancing optimality with practicality in a way that also integrates human decisions and human factors. Identifying and addressing these gaps is essential to building the next generation of CPSS that are fail-safe, adaptive, and socially inclusive.

Designing Evolving Systems as Policy

An evolving system, in the context of cyber-physical-social systems (CPSS), refers to an interconnected network where digital, physical, and human elements continuously interact and adapt over time (Figure 6.1).

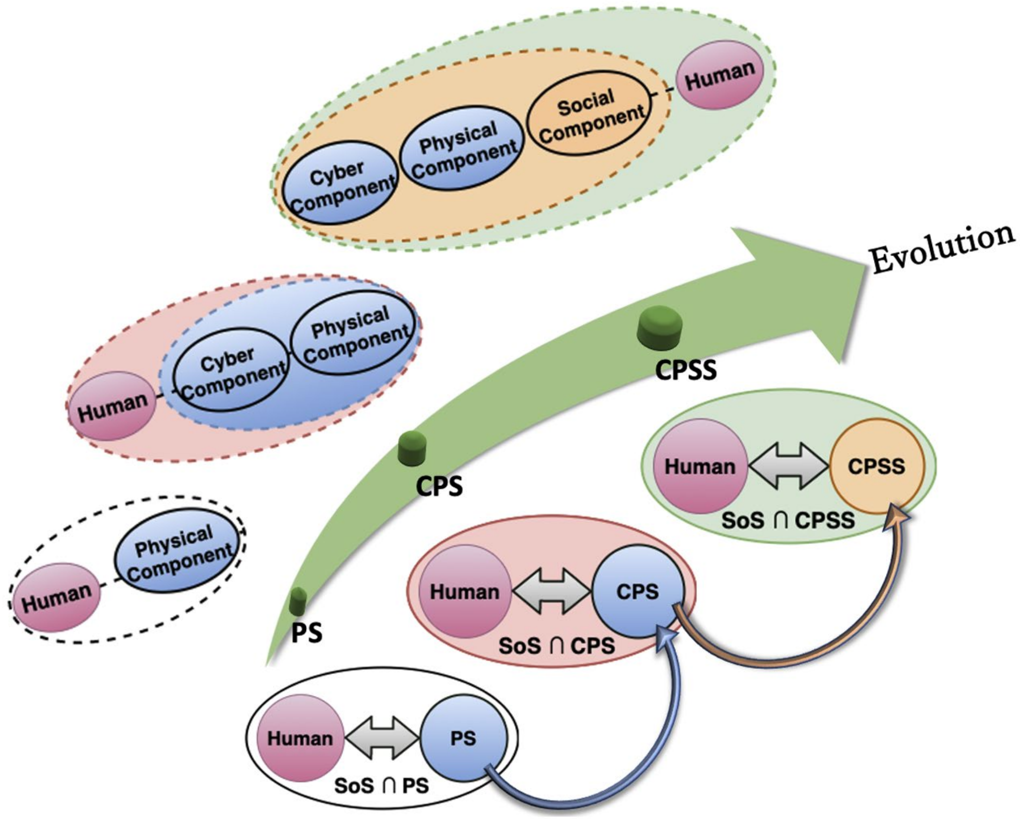

Figure 6.1: The Evolving Cyber-Physical-Social System (Yilma, Panetto et al. 2021)

These systems are dynamic, meaning they are not static or fixed; instead, they evolve as new information, technologies, and societal inputs emerge. In such systems, data from the physical world like sensors and machines interacts with cyber elements (e.g., software, algorithms) and is influenced by social behaviors, preferences, and policies. Designing evolving systems as policy will likely involve creating adaptive frameworks that can change over time to respond to shifting social, technological, and environmental conditions. The key research gap in this area lies in understanding how to effectively structure such systems to balance stability with flexibility within policy frameworks. This may also help to address ever-present policy issues. Current policies often struggle to keep pace with modern technology and societal changes, largely because they are static and designed with fixed rules and assumptions. This mismatch between the environment of policy development and the environment in which the policy attempts to address leads to both unit and systemic failures when policies become outdated. To address this gap, it is hypothesized that integrating or augmenting system archetypes to include mechanisms that allow systems to evolve, potentially incorporating feedback loops, predictive models, and stakeholder inputs may help to ensure policies remain relevant throughout time. However, policy relevance is not the only focus. Systemic issues in policy design like the lack of implementation practicality, transition challenges within existing systems, security concerns, scalability, mechanisms of system maintenance, regulation and enforcement must be included. Further study is also needed on the governance and ethical implications of evolving systems, particularly how to avoid unintended consequences and ensure equitable outcomes as policies change dynamically over time.

Social Components within Traditionally Cyber-Physical Systems

In traditionally designed cyber-physical systems (CPS), the social component refers to the human and societal factors that influence, and are influenced by, the system's operation. This includes human behaviors, interactions, preferences, and collective decision-making processes, which are essential in shaping how systems function within real-world environments. However, these social components are often excluded in the design of CPS, as the focus tends to be on optimizing the interaction between physical and cyber elements (Figure 6.2). This exclusion occurs largely because social dynamics are complex, unpredictable, and difficult to quantify, posing a challenge for system modeling and integration.

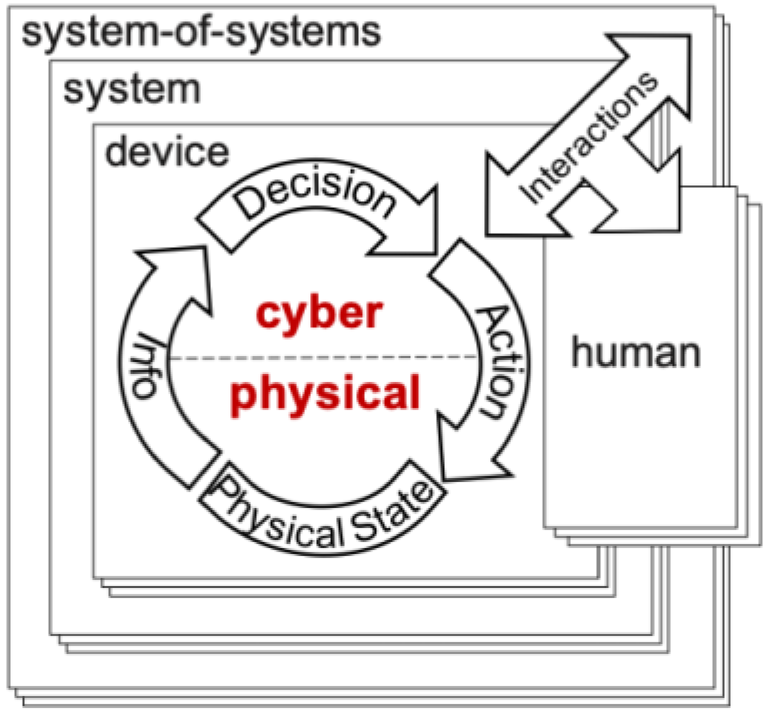

Figure 6.2: The Relationship of Humans and CPS (Burns, Manganelli et al. 2018)

The research gap lies in developing strategic and generalizable methods to quantify these social components and incorporate them meaningfully into system design. Current approaches lack the tools to measure and model human behaviors and societal impacts in a way that is as precise as the physical and cyber elements. This gap highlights the potential need for trans-disciplinary research that bridges social science, data analytics, and systems engineering. Quantifying social components is hypothesized to be crucial for enhancing the adaptability, resilience, and inclusivity of CPSS, ensuring that these systems can operate effectively in diverse social contexts and respond to both worker and stakeholder needs and preferences.

Autonomy with Satisficing-Based Decision Support Systems

Autonomy in systems refers to the capability of a system or in the context of social organization, teams, departments, or organization branches to operate independently, making decisions without intervention. The concept of system autonomy is currently a major research field in traditional CPS like those found in robotics, artificial intelligence design, automation, and manufacturing where systems must act in complex, unpredictable environments and address variation autonomously for seamless system activities. Autonomy is important because it enables systems to respond quickly to changing conditions and reduce the need for constant human oversight. In this research gap however, the meaning of autonomy is rooted in human autonomy within the system. Incorporating autonomy into system design presents significant challenges, particularly when balancing flexibility and rigidity. In flexible systems, system actors must adapt to varying inputs and contexts, while in more rigid systems, autonomy can operate within clearly defined parameters or be organized in a structured hierarchy. Designing for flexible autonomy is much more complex, as it will require system actors to make decisions in uncertain and dynamic conditions. Autonomy in team settings has been studied as a component of teams that perform at a high or exceptional level (Figure 6.3). Even in a team setting the role of autonomy is considered to be the foundation for the resulting positive progress.

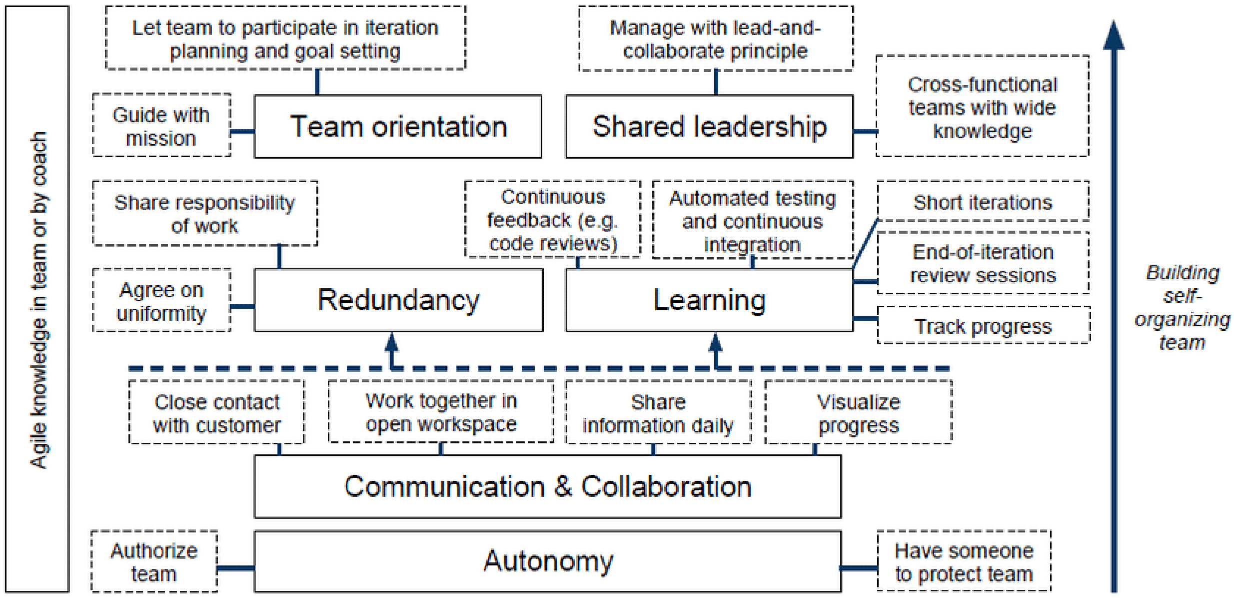

Figure 6.3: High-Performing Team with Agile and Lean Practices (Oza, Kettunen et al. 2013)

The research gap, for this area lies in determining appropriate levels of autonomy within systems that make good enough decisions, balancing optimality with practicality. Most current research focuses on fully autonomous or strictly human-controlled systems, but little is known about how to implement satisficing autonomy that adapts to changing conditions and imperfect information. It is hypothesized that by developing a new framework that can determine the right level of autonomy, systems can make reasonable decisions without overextending computational resources or making errors under uncertainty in a manner that is generalizable and adaptable. Further exploration is needed to define how satisficing decision-based design can be balanced with autonomy, ensuring systems can act efficiently while remaining responsive to real-world variability.

6.4.2 Proposed Approaches

To address the identified research gaps in *Designing Evolving Systems as Policy*, *Social Components within Traditionally Cyber-Physical Systems*, and *Autonomy with Satisficing-Based Decision Support Systems*, several approaches and methods can be proposed. These approaches are centered around the development of a system framework for designing adaptive and fail-safe systems that integrate the dynamic, unpredictable nature of social behaviors, policy frameworks, and satisficing-based decision-making processes. For evolving systems, methods that incorporate real-time feedback loops and predictive analytics could help create more adaptive policies that remain responsive to changing conditions. This could be advanced through the advancement of research in *dynamic system reconfiguration*. In terms of quantifying social components, new interdisciplinary models are needed that leverage social science insights and data-driven techniques to better understand and integrate human behaviors into system design. A proposed technique could be the development of *modular based redundancy* within CPSS that can evolve with changing system needs. This method would benefit the most from transdisciplinary research that includes social sciences, business, government, and engineering. Finally, for balancing or determining levels of autonomy with *satisficing-based systems*, a hybrid framework that dynamically adjusts the level of autonomy based on environmental complexity and decision quality thresholds can help systems operate more efficiently and effectively in uncertain conditions. These proposed approaches will not only address existing research gaps but also serve as vehicles for the development of new knowledge.

6.4.3 Test Problems for Verification of Efficacy of Proposed Framework

To verify the efficacy of the proposed methods to address the research gaps in dynamic system reconfiguration, satisficing-based design, and modular redundancy, several test problems can be designed. These test problems can be used as tools to evaluate the system's adaptability, decision-making capabilities, and fault tolerance. Some potential test scenarios are as follows:

Smart Grid Energy Management

This test case could review the ability of a dynamic system to respond to evolving and fluctuating energy demands and supply, such as integrating renewable energy sources (e.g., solar and wind) with unpredictable output. The evolving system should adapt real-time energy distribution policies based on environmental data, consumption patterns, and grid stability. This would be coupled with policy development for the use and deployment of energy.

Satisficing-Based Supply Chain Design

A satisficing-based approach can be tested in an evolving supply chain management scenario where the system must make decisions about supplier selection, inventory levels, and logistics that leverages Just in Time and Just in Case methods. The system should achieve practical solutions under changing conditions, such as demand fluctuations, supplier delays, and resource shortages, without aiming for perfect optimization.

Redundant Emergency Communication and Resource Allocation System

During a natural disaster, simulate failure in a city's emergency response communication system, which integrates social components like real-time reports from citizens and on-ground responders. The test should measure the ability of redundant modules to reconfigure and maintain coordination among first responders, volunteers, and affected citizens. Social data like evacuation behaviors, crowd movement, and information on social factors could be quantified and integrated into the backup system, ensuring accurate resource allocation and communication despite system failures. This would include the development of evolving policy systems that can meet emerging needs.

6.4.4 Research Plan and Tasks

In this section, the proposed research plan for a Ph.D. is introduced. This research plan is based on a five-stage structured strategy, displayed in Table 6.2 through 6.6, aimed at addressing key gaps in the fields of evolving cyber-physical-social systems (E-CPSS), social component quantification and integration in cyber-physical systems (CPS) all based on satisficing-based decisions. For each table, which corresponds to work proposed during a single stage, includes preliminarily outlined tasks and any connection to this MS thesis in addition to the proposed Ph.D. dissertation chapter. The plan begins, in Stage 1, with an in-depth literature review and problem definition, followed by the development of conceptual frameworks and early strategy explanations. Over the course of the five stages, these frameworks and strategies will be refined, expanded, and validated through simulations and real-world examples. The primary goal is to create systems that can dynamically adapt to changing conditions, integrate human behavior, and make practical decisions under uncertainty all with the result of increased system resilience. By the end of the fifth stage, the research will include validated systems, contributing significant advancements to the understanding and application of evolving CPS, social quantification, and the role of autonomy in satisficing decision-making.

For the first stage, a thorough literature review that includes portions of the literature review contained within this MS thesis, Chapter 2, is used to identify and refine the key gaps in evolving systems design, social component quantification and integration in CPS, and satisficing-based decision support (Table 6.2). Additionally, research objectives are defined, and initial data collection is either initiated or simulated to build foundational models. Another major focus within Stage 1 is establishing collaborative partnerships with either industry or governmental institutions to establish an avenue for real-world testing and validation.

Table 6.2: Stage 1 – Literature Review and Problem Definition

<table>
<tr><th colspan="3">STAGE 1</th></tr>
<tr><td></td><td>MS Thesis Connection</td><td>Ph.D. Chapter</td></tr>
<tr><td>1. Problem Definition and Research Objectives</td><td>Chapter 1, 2</td><td>Chapter 1</td></tr>
<tr><td colspan="3">Tasks
Clearly define the research questions and hypotheses related to the three key areas:
1.1: How to design evolving policies for dynamic systems?
1.2: How to quantify social components and integrate them into traditional CPS?
1.3: How to balance autonomy and satisficing-based decision-making?</td></tr>
<tr><td>2. Enhance and Augment Literature Review</td><td>Chapter 2, 3</td><td>Chapter 2</td></tr>
<tr><td colspan="3">Tasks
Conduct an in-depth review of existing work in dynamic systems, satisficing-based decision-making, and cyber-physical-social systems. Identify current methods, frameworks, and gaps that are still unresolved.</td></tr>
<tr><td>3. Structure and Strategy</td><td>Chapter 5, 6</td><td>Chapter 3</td></tr>
<tr><td colspan="3">Task
Determine strategy and structure for the design of system architectures that incorporate elements of modular redundancy, social quantification, and satisficing.</td></tr>
<tr><td colspan="3">4. Set Up Collaborative Partnerships</td></tr>
<tr><td colspan="3">Task
Partner with industry or academic institutions to gain access to real-world test environments (e.g., smart cities, health systems, autonomous systems) for data collection and future validation.</td></tr>
</table>

In the second stage, conceptual frameworks for evolving systems, social quantification, and satisficing-based decision support are developed (Table 6.3). The development of early system models are designed, and model-based validation is conducted through simulations to determine if the models or frameworks work for the defined problems. Data collection from experimental environments begins to provide insights and additional context for refining these models.

Table 6.3: Stage 2 – Conceptual Framework Development and Early Modeling

STAGE 2		
	MS Thesis Connection	Ph.D. Chapter
1. Development of Conceptual Frameworks	**Chapter 5, 6**	**Chapter 3**
Tasks Develop preliminary models for evolving systems policy, social quantification methods, and satisficing-based decision support systems. Formulate initial hypotheses for integrating social behaviors into traditionally cyber-physical systems and how satisficing-based systems will perform.		
2. Simulated System Design	**New**	**Chapter 4**
Tasks Begin gathering or simulating initial data for modeling dynamic systems (e.g., social behavior data, decision-making datasets). Build simulated systems with limited functionality to test theoretical frameworks: 2.1: A policy-evolving system that adapts in response to real-world input. 2.2: A prototype for social quantification in ECPSS. 2.3: A basic decision support system that implements satisficing autonomy in ECPSS.		
3. Initial Validation (Model-based)	**New**	**Chapter 5**
Tasks		

Begin model-based validation to check for consistency with theoretical expectations. Use simulations to validate whether the models behave as expected in ideal, controlled environments. Recording system responses to different variables or environments.

Stage 3 includes the steps to refining initial models based on collected data and extending frameworks and models into full systems (Table 6.4). These frameworks and models are then tested in more complex simulated environments, and interim data analysis is conducted to ensure models are consistent with theoretical expectations. Additionally, the social component quantification is enhanced, and satisficing-based decision-making is further defined and explored.

Table 6.4: Stage 3 – Refinement and Full System Development and Design

STAGE 3		
	MS Thesis Connection	Ph.D. Chapter
1. Model/Framework Refinement	**New**	**Chapter 5**
Tasks Use data collected from framework testing and simulations to refine the models and frameworks. Adjust assumptions, data inputs, and parameters for social quantification and satisficing decision-making within ECPSS.		
2. Full System Design and Expansion	**New**	**Chapter 5**
Tasks Expand simulations into more comprehensive systems with enhanced functionality for evolving policies and modular redundancy. Integrate and quantify full-scale social components (e.g., human feedback, interaction patterns) into the system.		
3. Validation with Simulations	**New**	**Chapter 6**

Tasks
Tasks Run extensive simulations to test the refined models and systems, validating their functionality across a broader range of conditions. Begin testing decision-making autonomy in more dynamic and uncertain environments, focusing on how satisficing works under different constraints.

In the fourth stage, the systems are deployed in real-world environments to validate their performance (Table 6.5). By testing the integration of social behaviors in CPS and verifying the effectiveness of satisficing-based decision support, frameworks can be validated and supported. Depending on partnership organization, extensive data can be collected from real-world deployments to assess system adaptability and decision-making efficacy.

Table 6.5: Stage 4 – Validation in Real-World Environments

STAGE 4		
	MS Thesis Connection	Ph.D. Chapter
1. Real-World System Deployment	**New**	**Chapter 6**
Tasks Deploy systems in real-world environments (e.g., smart city traffic management, autonomous vehicle fleets, hospital systems) to validate their performance. Ensure that evolving policies and decision-making systems are stress-tested in varying levels of dynamic, unpredictable conditions.		
2. Validation of Social Component Quantification	**New**	**Chapter 7**
Tasks Validate the effectiveness of social component quantification in real-world CPS, ensuring that systems can adapt based on human behavior, preferences, and feedback.		
3. Testing of Satisficing-Based Decision Support	**New**	**Chapter 7**
Tasks		

Test the satisficing-based decision support systems in real-world scenarios, where perfect optimization is not possible, and practical decisions must be made (e.g., in autonomous navigation or supply chain management).		
4. Data Collection for Validation	**New**	**Chapter 7**
Tasks Collect extensive real-world data from system performance, user interactions, and environmental responses. Gather user feedback to measure satisfaction and system efficacy related to evolving policies and decision support systems.		

The final stage involves testing the systems based on real-world performance data (Table 6.6). This stage includes robust testing to ensure the frameworks can adapt and evolve to meet various scenarios and conditions. Final validation and data analysis are conducted in this year to complete the Ph.D. dissertation. Finally, the recommendations for future research, based on the results of the Ph.D. are collected and explained in terms of a career proposal.

Table 6.6: Stage 5 – Evaluation and Final Analysis

STAGE 5		
	MS Thesis Connection	Ph.D. Chapter
1. System Refinement	**New**	**Chapter 8**
Tasks Refine evolving system policies to better respond to diverse conditions. Improve social quantification models to more accurately reflect human behaviors. Enhance satisficing decision support algorithms to strike better balances between decision quality and speed.		
2. Final Validation and Generalization	**New**	**Chapter 8**
Tasks Perform final rounds of validation, testing system robustness across different scenarios and conditions, including stress tests to assess system failures and redundancy. Ensure that systems maintain performance under varied social behaviors and decision-making challenges.		

3. Final Data Analyses and Hypothesis Evaluation	**New**	**Chapter 8**
Task Conduct a final analysis of all collected data to evaluate the success of the proposed approaches/frameworks.		
4. Evaluation of Results	**New**	**Chapter 8**
Tasks Evaluate claims made in dissertation and discuss generalization, efficacy, and areas of improvement.		
5. Recommendations for Future Research	**New**	**Career Proposal (Chapter 9)**
Tasks Based on the findings, outline key areas where further research is needed, such as improvements in social behavior modeling or decision-making under extreme uncertainty. Propose potential applications of the developed systems in new domains, such as defense, healthcare, transportation, or autonomous manufacturing.		

6.4.5 Project Management and Timeline

In order to successfully complete the Ph.D. dissertation, effective project management and a well-structured timeline is critical. While there are significant steps, like contributing organization or partnerships, that can alter the trajectory of the dissertation the timeline is represented in terms of the major milestones. This section includes an outline of the approach to managing the project's scope and necessary resources through task milestones. In Figure 6.4, key checkpoints for initial publications, validation, verification, and data analyses are preliminarily placed to maintain alignment with the dissertation objectives, allowing for adjustments as necessary. This structured approach to project management will ensure that the work remains on track, on time, and within scope.

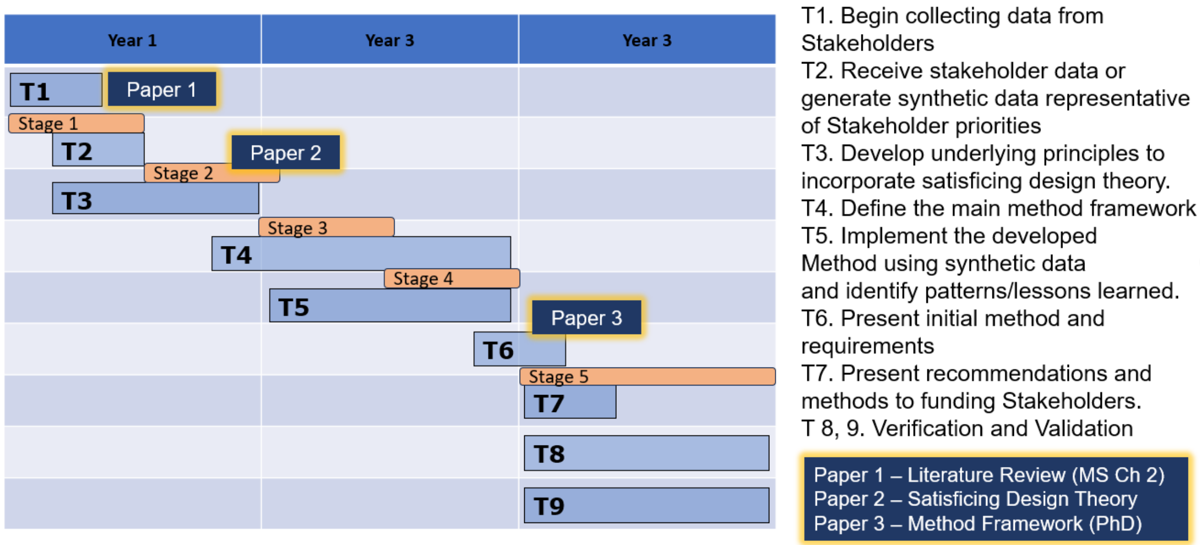

Figure 6.4: Preliminary Dissertation Timeline and Proposed Papers

6.5 I statement…

This thesis was born out of two things: the love for my country, and the love for my defense sustainment community. Serving this nation in any capacity is a privilege, but being part of the defense sustainment team is something I hold close to my heart. We are bound by a shared purpose and driven by a desire to contribute to something greater than ourselves. It’s not just a job, but a calling, one that demands excellence, integrity, and unwavering support for one another. Together, we build the backbone of our nation's defense, and there is no greater source of pride than knowing we play a part in protecting the freedoms and values that make this country great. Processes, no matter how well-designed or meticulously planned, are only as strong as the people who carry them out. The most advanced systems, the best technologies, and the most thorough frameworks mean little without the dedication, skill, and commitment of the individuals responsible for their execution. It's the people, those who rise to challenges, solve problems in real-time, and push through adversity, who ultimately determine the success of any mission. In our work, where the stakes are high, and every decision can impact the safety and readiness of our nation, this truth has never been more evident. I have always believed that the strength of our processes lies not in the procedures themselves, but in the heart, intelligence, and commitment of those who make them happen. The people in our defense sustainment family are not just cogs in a machine; they are the very lifeblood of everything we do. Every task, every decision, no matter how small, contributes to a much larger goal: protecting our country and ensuring that those who defend it have what they need to succeed. It's an honor to work alongside individuals who understand that responsibility and rise to meet it with professionalism and passion every day.

I believe in us, and I believe in the power of people to overcome any obstacle. No process or framework can replace the human spirit, and I have faith that there is no challenge we cannot meet. Together, as a defense sustainment family, we will continue to adapt, grow, and succeed in the mission we all hold dear.

"Aim High… Fly-Fight-Win"

- U.S. Air Force Mission

REFERENCES

U.S. Congress (1992). The Long Island Solid Waste Crisis and Toxic Chemical Exposure-Induced Breast Cancer: Hearing before the Subcommittee On Environment of the Committee On Science, Space, And Technology, U.S. House of Representatives. 102nd Congress, Second Session, Washington : U.S. G.P.O.

S. Rpt. 112-167 (2012). Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain: Hearing before the Committee On Armed Services, U.S. Senate, 112th Congress, Second Session, Washington : U.S. G.P.O.

(2019). The Community Reinvestment Act: Assessing the Law's Impact on Discrimination and Redlining: Hearing before the Subcommittee on Consumer Protection and Financial Institutions of the Committee on Financial Services, 116th Congress, First Session, Washington : U.S. G.P.O.

(2019). "Report on the Effects of a Changing Climate to the Department of Defense." from https://media.defense.gov/2019/jan/29/2002084200/-1/-1/1/climate-change-report-2019.pdf.

(2022). "The Toyota Way: Adopting Lean and Agile Manufacturing Processes from the Toyota Production System." Strategic Direction **38**(12): 33-34.

(2024). "Assistant Secretary of Defense (Sustainment) - About Us." Retrieved October 3, 2024, from https://www.acq.osd.mil/asds/about-asds.html.

(2024). "The Climate Crisis: Working Together for Future Generations." Retrieved September 15, 2024, from https://www.state.gov/policy-issues/climate-crisis/.

(2024). DDE/CC - Data Demand Exchange/Customer Collaboration. https://www.dla.mil/Working-With-DLA/Applications/Details/Article/2953489/ddecc-data-demand-exchangecustomer-collaboration/.

(2024). Defense Contracts: Better Monitoring Could Improve DOD's Management of Award Lead Times, Washington, DC : United States Government Accountability Office.

(2024). "Maintenance Levels ALCL 077." Retrieved October 8, 2024, from https://www.dau.edu/acquipedia-article/maintenance-levels.

(2024). "Policy." Retrieved October 20, 2024, from https://www.merriam-webster.com/dictionary/policy.

(2024). "Regional Sustainment Framework." from https://www.acq.osd.mil/asds/docs/RSF-9MAY24.pdf.

Acar, Y. and S. N. Atadeniz (2015). "Comparison of Integrated and Local Planning Approaches for the Supply Network of a Globally-Dispersed Enterprise." International Journal of Production Economics **167**: 204-219.

AFSC. (2023). "Art of the Possible Handbook 60-101." from https://static.e-publishing.af.mil/production/1/af_sustainment_ctr/publication/afsch60-101/afsch60-101.pdf.

AFSC. (2024). "Air Force Sustainment Center Strategic Plan." from https://www.afsc.af.mil/About-Us/Strategic-Plan/.

Ahn, T. and A. A. Menichini (2022). "Optimal Talent Management of the Acquisition Workforce in Response to COVID-19: Dynamic Programming Approach." Defense AR journal **29**(1): 50-77.

Akhavantaheri, H., P. Sandborn and D. Das (2023). "An Enterprise Network Model for Understanding and Disrupting Illicit Counterfeit Electronic Part Supply Chains." IIE Transactions **56**(3): 257-268.

Allen, J. K., A. B. Nellippallil, Z. Ming, J. Milisavljevic-Syed and F. Mistree (2023). "Designing Evolving Cyber-Physical-Social Systems: Computational Research Opportunities." Journal of Computing and Information Science in Engineering **23**(6).

Alvarez, R. A., D. Zavala-Araiza, D. R. Lyon, D. T. Allen, Z. R. Barkley, A. R. Brandt, K. J. Davis, S. C. Herndon, D. J. Jacob, A. Karion, E. A. Kort, B. K. Lamb, T. Lauvaux, J. D. Maasakkers, A. J. Marchese, M. Omara, S. W. Pacala, J. Peischl, A. L. Robinson, P. B. Shepson, C. Sweeney, A. Townsend-Small, S. C. Wofsy and S. P. Hamburg (2018). "Assessment of Methane Emissions from the U.S. Oil and Gas Supply Chain." Science (American Association for the Advancement of Science) **361**(6398): 186-188.

Amici, F. and L. M. Bietti (2015). "Coordination, Collaboration and Cooperation: Interdisciplinary Perspectives." Interaction Studies **16**(3): vii-xii.

Anagnostakis, D. (2016). "Securing the Transatlantic Maritime Supply Chains from Counterterrorism: EU-U.S. Cooperation and the Emergence of a Transatlantic Customs Security Regime." Studies in Conflict and Terrorism **39**(5): 451-471.

Anderson, J. (2015). Risk Unbound: Threat, Catastrophe, and the End of Homeland Security. Homeland Security Affairs. Monterey, Monterey: Naval Postgraduate School, Center for Homeland Defense and Security.

Apte, A., U. M. Apte and R. G. Rendon (2011). "Services Supply Chain in the United States Navy: an Empirical Study of Current Management Practices." Journal of Public Procurement **11**(4): 538-562.

Auletta, F., R. W. Kallen, M. di Bernardo and M. J. Richardson (2023). "Predicting and Understanding Human Action Decisions During Skillful Joint-action Using Supervised Machine Learning and Explainable-AI." Scientific Reports **13**(1): 4992-4992.

Azrilyant, J. (2021). "Shell Game: How the Corporate Transparency Act Aims to End the Illicit use of Shell Companies, Where it Fails, and What to do About it." Public Contract Law Journal **51**(1): 1-27.

Belcher, O., P. Bigger, B. Neimark and C. Kennelly (2020). "Hidden Carbon Costs of the “Everywhere War”: Logistics, Geopolitical Ecology, and the Carbon Boot-print of the US military." Transactions - Institute of British Geographers (1965) **45**(1): 65-80.

Bier, T., A. Lange and C. H. Glock (2020). "Methods for Mitigating Disruptions in Complex Supply Chain Structures: a Systematic Literature Review." International Journal of Production Research **58**(6): 1835-1856.

Bistline, J., G. Blanford, M. Brown, D. Burtraw, M. Domeshek, J. Farbes, A. Fawcett, A. Hamilton, J. Jenkins, R. Jones, B. King, H. Kolus, J. Larsen, A. Levin, M. Mahajan, C. Marcy, E. Mayfield, J. McFarland, H. McJeon, R. Orvis, N. Patankar, K. Rennert, C. Roney, N. Roy, G. Schivley, D. Steinberg, N. Victor, S. Wenzel, J. Weyant, R. Wiser, M. Yuan and A. Zhao (2023). "Emissions and Energy Impacts of the Inflation Reduction Act." Science (American Association for the Advancement of Science) **380**(6652): 1324-1327.

Blagden, D. (2015). "Global Multipolarity, European Security and Implications for UK Grand Strategy: Back to the Future, Once Again." International Affairs (London) **91**(2): 333-350.

Braziotis, C., M. Bourlakis, H. Rogers and J. Tannock (2013). "Supply Chains and Supply Networks: Distinctions and Overlaps." Supply Chain Management **18**(6): 644-652.

Brown, D. B. and M. Sim (2009). "Satisficing Measures for Analysis of Risky Positions." Management Science **55**(1): 71-84.

Bryant, J., J. Darwin and C. Booth (2011). "Strategy Making with the Whole Organisation: OR and The Art of the Possible: OR's Contribution to Supporting Strategy." The Journal of the Operational Research Society **62**(5): 840-854.

Burns, M., J. Manganelli, D. Wollman, R. Laurids Boring, S. Gilbert, E. Griffor, Y.-C. Lee, D. Nathan-Roberts and T. Smith-Jackson (2018). "Elaborating the Human Aspect of the NIST Framework for Cyber-Physical Systems." Proceedings of the Human Factors and Ergonomics Society Annual Meeting **62**(1): 450-454.

Cabrera, B., R. Santa, T. Tegethoff, D. Morante and M. Ferrer (2023). "Supply Chain Resilience in the Colombian Defense Sector Before and During the COVID-19 Pandemic: A Comparative Study." PloS One **18**(3): e0282793-e0282793.

Can Saglam, Y., B. Sezen and S. Y. Çankaya (2020). "The Inhibitors of Risk Information Sharing in the Supply Chain: A Multiple Case Study in Turkey." Journal of Contingencies and Crisis Management **28**(1): 19-29.

Charitoudi, K. and A. J. C. Blyth (2014). "An Agent-Based Socio-Technical Approach to Impact Assessment for Cyber Defense." Information Security Journal: A Global Perspective **23**(4-6): 125-136.

Chellin, M. D. and E. E. Miller (2023). "Frustrated with Obsolescence — Try Changing Your Mental Model." Defense AR Journal **30**(3): 228.

Choi, T. Y. and Z. Wu (2009). "Triads in Supply Networks: Theorizing Buyer-Supplier-Supplier Relationships." The Journal of Supply Chain Management **45**(1): 8-25.

Crowe, A. (2011). "SAFETY Act Liability Protections for Air Cargo Screeners." The Air and Space Lawyer **23**(4): 4.

D'Souza, R. M. (2017). "Curtailing Cascading Failures." Science (American Association for the Advancement of Science) **358**(6365): 860-861.

Day, J. M. (2014). "Fostering Emergent Resilience: The Complex Adaptive Supply Network of Disaster Relief." International Journal of Production Research **52**(7): 1970-1988.

Dong, M., R. Ranjan, A. Y. Zomaya and M. Lin (2015). "Guest Editorial on Advances in Tools and Techniques for Enabling Cyber-Physical-Social Systems-Part I." IEEE Transactions on Computational Social Systems **2**(3): 38-40.

Douglas, M. A., R. E. Overstreet and B. T. Hazen (2016). "Art of The Possible or Fool's Errand? Diffusion of Large-Scale Management Innovation." Business Horizons **59**(4): 379-389.

Drewniak, Z., R. Drewniak and R. Karaszewski (2020). "The Assessment of the Features of Inter-organisational Relationships: Benefits, Duration, Repeatability and Maturity of the Relationship with the Company's Stakeholders." European Research Studies **23**: 443-461.

Fang, J., H. Hou, C. Lu, H. Pang, Q. Deng, Y. Ye and L. Pan (2021). "A New Scheduling Method Based on Sequential Time Windows Developed to Distribute First-Aid Medicine for Emergency Logistics Following an Earthquake." PloS One **16**(2): e0247566-e0247566.

Fletcher, M. P. (2011). "Joint Supply Chain Architecture: the Department of Defense has used the Supply Chain Operations Model to Develop a Method for Coordinating and Managing Supply Chain Practices Across the Department and the Services." Army Sustainment **43**(2): 20.

Gero, J. S. and U. Kannengiesser (2002). The Situated Function — Behaviour — Structure Framework. Dordrecht, Dordrecht: Springer Netherlands.

Gerstein, D. M. (2020). "Assessing the US Government Response to the Coronavirus." Bulletin of the Atomic Scientists **76**(4): 166-174.

Giannoccaro, I. and A. Iftikhar (2022). "Mitigating Ripple Effect in Supply Networks: The Effect of Trust and Topology on Resilience." International Journal of Production Research **60**(4): 1178-1195.

Goldratt, E. M. (1984). What is this thing called THEORY OF CONSTRAINTS and how should it be implemented?, Croton-on-Hudson, N.Y. : North River Press.

Green, J. and J. Stracener (2022). "Investigating the Role of System Effectiveness in the Acquisition and Sustainment of U.S. Defense Systems: 1958 to 2022." Systems **10**(5): 169.

Greenstein, J. (2020). "The Precariat Class Structure and Income Inequality Among US Workers: 1980–2018." The Review of Radical Political Economics **52**(3): 447-469.

Guo, L., J. K. Allen and F. Mistree (2024). "Optimize or Satisfice in Engineering Design?" Research in Engineering Design **35**(3): 1-29.

Gyenge, B., L. Kasza and L. Vasa (2021). "Introducing the EPP house (topological space) Method to Solve MRP problems." PloS One **16**(6): e0253330-e0253330.

Handfield, R., D. J. Finkenstadt, E. S. Schneller, A. B. Godfrey and P. Guinto (2020). "A Commons for a Supply Chain in the Post-COVID-19 Era: The Case for a Reformed Strategic National Stockpile." The Milbank Quarterly **98**(4): 1058-1090.

Hannan, R. J., M. K. Lundholm, D. Brierton and N. R. M. Chapman (2020). "Responding to Unforeseen Disasters in a Large Health System." American Journal of Health-System Pharmacy **78**(8): 726-731.

Haraburda, S. S. (2016). "Transforming Military Support Processes from Logistics to Supply Chain Management." Army Sustainment **48**(2): 12.

Haraburda, S. S. (2017). "Supply Chain Management Maturity Level Assessment." Defense AR Journal **24**(4): 656-681.

Hasik, J. (2021). "How to Bail Out a Defense Contractor: Cases on Securing a Supply Chain in extremis." Defense Acquisition Research Journal **28**(96): 166-189.

Henry, A. D., M. Lubell and M. McCoy (2011). "Belief Systems and Social Capital as Drivers of Policy Network Structure: The Case of California Regional Planning." Journal of Public Administration Research and Theory **21**(3): 419-444.

Holman, B. W. (2006). DOD's Overseas Infrastructure Master Plans Continue to Evolve, Washington, DC : U.S. Government Accountability Office.

House, A. (2021). "The Price of a Cybersecurity Culture: How the CMMC Should Secure the Department of Defense's Supply Chain without Harming Small Businesses and Competition." Public Contract Law Journal **50**(3): 449-470.

Huang, F., J. Song and N. J. Taylor (2022). "The impact of Business Conditions and Commodity Market on US Stock Returns: An Asset Pricing Modelling Experiment." Quantitative Finance and Economics **6**(3): 433-458.

Ide, T. (2023). "Climate Change and Australia's National Security." Australian Journal of International Affairs **77**(1): 26-44.

Ivanov, D. (2023). "The Industry 5.0 Framework: Viability-based Integration of the Resilience, Sustainability, and Human-centricity Perspectives." International Journal of Production Research **61**(5): 1683-1695.

Jaber, M. Y., M. Bonney and A. L. Guiffrida (2010). "Coordinating a Three-level Supply Chain with Learning-based Continuous Improvement." International Journal of Production Economics **127**(1): 27-38.

Jacobsen, K. H. (2020). "Will COVID-19 generate global preparedness?" The Lancet (British edition) **395**(10229): 1013-1014.

Jin, Y., S. Ji, L. Liu and W. Wang (2022). "Business Model Innovation Canvas: a Visual Business Model Innovation Model." European Journal of Innovation Management **25**(5): 1469-1493.

Johnson, P. F. and R. D. Klassen (2022). New Directions for Research in Green Public Procurement: The Challenge of Inter-stakeholder Tensions. Cleaner Logistics and Supply Chain, Elsevier BV. **3**.

Jones, R. A. and B. Horowitz (2012). "A System-Aware Cyber Security Architecture." Systems Engineering **15**(2): 225-240.

Kamalahmadi, M., M. Shekarian and M. Mellat Parast (2022). "The Impact of Flexibility and Redundancy on Improving Supply Chain Resilience to Disruptions." International Journal of Production Research **60**(6): 1992-2020.

Katsaliaki, K., S. Kumar and V. Loulos (2024). "Supply Chain Coopetition: A Review of Structures, Mechanisms and Dynamics." International Journal of Production Economics **267**: 109057.

Khan, M. N., P. Akhtar and Y. Merali (2018). "Strategies and Effective Decision-Making Against Terrorism Affecting Supply Chain Risk Management and Security: A Novel Combination of Triangulated Methods." Industrial Management & Data Systems **118**(7): 1528-1546.

Kim, S. (2022). "Mind your Due Diligence: Section 889 and an Emerging Minefeild of FCA Violations." Public Contract Law Journal **51**(3): 413-438.

Klibi, W. and A. Martel (2012). "Modeling Approaches for the Design of Resilient Supply Networks Under Disruptions." International journal of production economics **135**(2): 882-898.

Koenig, P. C. (2019). "Defense Procurement and Public Utility Regulation: A 21st-Century Re-examination." Defense AR Journal **26**(4): 337-347.

Krichene, H., H. Inoue, T. Isogai and A. Chakraborty (2020). "A Model of the Indirect Losses from Negative Shocks in Production and Finance." PloS One **15**(9): e0239293-e0239293.

Lee, Y. H., P. Golinska-Dawson and J.-Z. Wu (2016). "Mathematical Models for Supply Chain Management." Mathematical Problems in Engineering **2016**: 1-4.

Leffler, L. L. (2022). "Improving the US Supply Chain to Sustain National Security." Defense Transportation Journal **78**(4): 15-30.

Lepori, B. and M. Montauti (2020). "Bringing the Organization Back In: Flexing Structural Responses to Competing Logics in Budgeting." Accounting, Organizations and Society **80**: 101075.

Lin, Y.-K., J.-J. Lin and R.-H. Yeh (2016). "Coordinating a Service Supply Chain under Arms Offset Program's Intervention by Performance-Based Contracting." Mathematical Problems in Engineering **2016**: 1-10.

Lind, J. and D. G. Press (2018). "Markets or Mercantilism? How China Secures Its Energy Supplies." International Security **42**(4): 170-204.

Linnean III, H. W. (2008). Air Force Smart Operations for the Twenty-first Century: Identifying Potential Failure Points in Sustaining Continuous Process Improvement across the Air Force, Air University Press.

Lukassen, P. J. H. and C. M. Wallenburg (2010). "Pricing Third-Party Logistics Services: Integrating Insights from the Logistics and Industrial Services Literature." Transportation Journal **49**(2): 24-43.

Maglaras, L., H. Janicke and M. A. Ferrag (2022). "Cybersecurity of Critical Infrastructures: Challenges and Solutions." Sensors (Basel, Switzerland) **22**(14): 5105.

Majchrzak, D., K. Michalski and J. Reginia-Zacharski (2021). "Readiness of the Polish Crisis Management System to Respond to Long-Term, Large-Scale Power Shortages and Failures (Blackouts)." Energies (Basel) **14**(24): 8286.

Marples, D. J., A. B. Schwarzenberg and M. D. Sutherland. (2020). "COVID-19: Tax Policy Options to Address Medical Supply Chain Concerns." COVID-19, from https://www.everycrsreport.com/reports/IN11536.html.

Martin, K. (2016). "Data Aggregators, Consumer Data, and Responsibility Online: Who is tracking consumers online and should they stop?" The Information Society **32**(1): 51-63.

Masip-Bruin, X., E. Marín-Tordera, J. Ruiz, A. Jukan, P. Trakadas, A. Cernivec, A. Lioy, D. López, H. Santos, A. Gonos, A. Silva, J. Soriano and G. Kalogiannis (2021). "Cybersecurity in ICT Supply Chains: Key Challenges and a Relevant Architecture." Sensors (Basel, Switzerland) **21**(18): 6057.

McConnell, B. M., T. J. Hodgson, M. G. Kay, R. E. King, Y. Liu, G. H. Parlier, K. Thoney-Barletta and J. R. Wilson (2021). "Assessing Uncertainty and Risk in an Expeditionary Military Logistics Network." Journal of Defense Modeling and Simulation **18**(2): 135-156.

Michelena, Á., V. López, F. L. López, E. Arce, J. Mendoza García, A. Suárez-García, G. García Espinosa, J.-L. Calvo-Rolle and H. Quintián (2023). "A Fault-Detection System Approach for the Optimization of Warship Equipment Replacement Parts Based on Operation Parameters." Sensors (Basel, Switzerland) **23**(7): 3389.

Mirza, M., M. Verma, S. Sahoo, S. Roy, R. Kakkar and D. Singh (2023). "India's Multi-Sectoral Response to Oxygen Surge Demand During COVID-19 Pandemic: A Scoping Review." Indian Journal of Community Medicine **48**(1): 31-40.

Mu, D., X. Yue and H. Ren (2021). "Robustness of Cyber-Physical Supply Networks in Cascading Failures." Entropy (Basel, Switzerland) **23**(6): 769.

Nguyen, H., T. C. Sharkey, J. E. Mitchell and W. A. Wallace (2020). "Optimizing the Recovery of Disrupted Single-sourced Multi-echelon Assembly Supply Chain Networks." IIE Transactions **52**(7): 703-720.

Nicastro, L. A. (2023). U.S. Defense Infrastructure in the Indo-Pacific : Background and Issues for Congress U.S. Defense Infrastructure in the Indo-Pacific: Background and Issues for Congress, Washington, D.C. : Congressional Research Service.

Nissen, H. A., M. R. Evald and A. H. Clarke (2014). "Knowledge Sharing in Heterogeneous Teams Through Collaboration and Cooperation: Exemplified Through Public–Private-Innovation Partnerships." Industrial Marketing Management **43**(3): 473-482.

Osgood, J. M., J. W. Froude, S. P. Daye, O. A. Cabrera, M. R. Scherer, V. F. Capaldi, N. L. Michael, J. E. Moon, E. D. Lombardini, S. A. Peel, K. P. Peterson, D. S. Teyhen, C. K. Murray and R. J. O'Connell (2023). "Cross-Cutting Lessons Learned During the COVID-19 Pandemic-the Walter Reed Army Institute of Research Experience." Military Medicine **188**(1-2): 158-165.

Oza, V., P. Kettunen, P. Abrahamsson and J. Münch (2013). Attaining High-performing Software Teams with Agile and Lean Practices: An Empirical Case Study. International Software Technology Exchange Workshop 2011, Cornell University.

Park, J. H. (2020). "Symmetry-Adapted Machine Learning for Information Security." Symmetry (Basel) **12**(6): 1044.

Parrott, J. (2020). Liquor Makers in Indiana, Michigan Pivot to Making Hand Sanitizer in Wake of Coronavirus. TCA Regional News. Chicago, Chicago: Tribune Content Agency LLC.

Petel, G. (2014). "Mitigating Counterfeit Electronic Parts Risk: What EPA's Buy American Checklist Can Teach DOD." Public Contract Law Journal **43**(3): 507-525.

Pilbeam, C., G. Alvarez and H. Wilson (2012). "The Governance of Supply Networks: A Systematic Literature Review." Supply Chain Management **17**(4): 358-376.

Purvis, L., J. Gosling and M. M. Naim (2014). "The Development of a Lean, Agile and Leagile Supply Network Taxonomy Based on Differing Types of Flexibility." International Journal of Production Economics **151**: 100-111.

Randall, W. S., S. P. Brady and D. R. Nowicki (2012). "Business Case Analysis and the Confounds of Innovation Driven by Performance-Based Postproduction Support Strategies." Transportation Journal **51**(1): 33-58.

Raunig, B. L., A. S. Kesselheim and J. J. Darrow (2020). "Drug Shortages and the Defense Production Act." American Journal of Public Health (1971) **110**(10): 1504-1505.

Reddie, A. W., B. L. Goldblum, K. Lakkaraju, J. Reinhardt, M. Nacht and L. Epifanovskaya (2018). "Next-generation Wargames." Science (American Association for the Advancement of Science) **362**(6421): 1362-1364.

Rezapour, S., A. Khosrojerdi, G. Rasoulifar, J. K. Allen, J. H. Panchal, R. S. Srinivasan, J. D. Tew and F. Mistree (2018). Architecting Fail-Safe Supply Networks. Boca Raton, FL, CRC Press.

Rezapour, S., R. Srinivasan, J. Tew, J. K. Allen and F. Mistree (2018). "Correlation Between Strategic and Operational Risk Mitigation Strategies in Supply Networks." International Journal of Production Economics **201**: 225-248.

Robinson, D. (2018). "Machines Don't Have to Break: Defense Innovation Unit Experimental is Helping the Department of Defense Achieve the Financial and Readiness Improvements Available Through Artificial Intelligence." Army Sustainment **50**(5): 36.

Rogers, R. (2023). “Serious queries” and “editorial epistemologies”: How social media are contending with misinformation. The Propagation of Misinformation in Social Media A Cross-platform Analysis. Amsterdam, Amsterdam Amsterdam University Press**:** 9-32.

Rowlett, R. (2017). "Joint Publication 3-0, Joint Operations." Joint Force Quarterly(86): 122.

Russell, S. H. (2011). "Supply Chain Management: More than Integrated Logistics." Air Force Journal of Logistics **35**(3-4): 88.

Sanders, N. (2012). "A Response to Ryan P. Carpenters's "The Bottom of the Smart Weapon Production Chain: Securing the Supply of Rare Earth Elements for the U.S. Military"." Public Contract Law Journal **41**(4): 957-965.

Seepersad, C. C., K. Pedersen, J. Emblesvåg, R. R. Bailey, J. K. Allen and F. Mistree (2006). Validation of Design Methods. The Validation Square: How Does One Validate Design Methods? A. Press. New York, NY, ASME Press**:** 305-326.

Senge, P. M. (2006). The Fifth Discipline. New York, Doubleday/Currency.

Senge, P. M. (2006). "The Fifth Discipline."

Shi, X.-q., X.-j. Yuan and D.-s. Deng (2022). "Research on Supply Network Resilience Considering the Ripple Effect with Collaboration." International Journal of Production Research **60**(18): 5553-5570.

Sofitra, M., K. Takahashi and K. Morikawa (2015). "The Coevolution of Interconnected Relationship Strategies in Supply Networks." International Journal of Production Research **53**(22): 6919-6936.

Son, B.-G., S. Chae and C. Kocabasoglu-Hillmer (2021). "Catastrophic Supply Chain Disruptions and Supply Network Changes: A Study of the 2011 Japanese Earthquake." International Journal of Operations and Production Management **41**(6): 781-804.

Stevenson, B. and J. Wolfers (2011). "Trust in Public Institutions over the Business Cycle." The American Economic Review **101**(3): 281-287.

Sullivan, B. A. and J. M. Wilson (2017). "An Empirical Examination of Product Counterfeiting Crime Impacting the U.S. Military." Trends in Organized Crime **20**(3-4): 316-337.

Sung, S. Y. and J. N. Choi (2021). "Contingent Effects of Workforce Diversity On Firm Innovation: High-Tech Industry and Market Turbulence as Critical Environmental Contingencies." International Journal of Human Resource Management **32**(9): 1986-2012.

Sutter, K. M., A. B. Schwarzenberg and M. D. Sutherland (2020). COVID-19: China Medical Supply Chains and Broader Trade Issues. COVID-19. C. R. Service. Washington, D.C, Washington, D.C.

Taghizadeh, E., S. Venkatachalam and R. B. Chinnam (2021). "Impact of Deep-tier Visibility on Effective Resilience Assessment of Supply Networks." International Journal of Production Economics **241**: 108254.

Taouil, F. Z., S. Beau and P. Hassanaly. (2010). "Collaborate to Co-elaborate Knowledge: Between Necessity and Opportunity." International Conference on Information Systems and Economic Intelligence, from https://archivesic.ccsd.cnrs.fr/sic_00451018v1.

Tatham, P., R. Oloruntoba and K. Spens (2012). "Cyclone Preparedness and Response: an Analysis of Lessons Identified Using an Adapted Military Planning Framework." Disasters **36**(1): 54-82.

Tatham, P. and S. Rietjens (2016). "Integrated Disaster Relief Logistics: a Stepping Stone Towards Viable Civil-Military Networks?" Disasters **40**(1): 7-25.

Tierney, J. F. (2010). "Warlord, Inc: Extortion and Corruption Along the U.S. Supply Chain in Afghanistan." from https://www.cbsnews.com/htdocs/pdf/HNT_Report.pdf.

Tseng, F. T., L. Burns, J. T. Simpson and D. Berkowitz (2017). "Increasing Army Supply Chain Performance Using an Integrated End-to-End Metrics System." Defense Acquisition Research Journal **24**: 66-100.

Turri, A. M., R. J. Smith and S. W. Kopp (2017). "Privacy and RFID Technology: A Review of Regulatory Efforts: Privacy and RFID Technology." The Journal of Consumer Affairs **51**: 329-354.

Tyson, L. D. and B. Guile (2021). "Innovation-Based Economic Security." Issues in Science and Technology **37**(4): 44-47.

van den Adel, M. J., T. A. de Vries and D. P. van Donk (2022). "Resilience in Interorganizational Networks: Dealing with Day-to-day Disruptions in Critical Infrastructures." Supply Chain Management **27**(7): 64-78.

Waller, J. C. (2011). "From Manufacturer to Forward Operating Base." Army Sustainment **43**(4): 50.

Wang, M. and J. Yao (2023). "Intertwined Supply Design Under Facility and Transportation Disruption from the Viability Perspective." International Journal of Production Research **61**(8): 2513-2543.

Wang, X., J. Yang, Y. Wang, Q. Miao, F.-Y. Wang, A. Zhao, J.-L. Deng, L. Li, X. Na and L. Vlacic (2023). "Steps Toward Industry 5.0: Building "6S" Parallel Industries With Cyber-Physical-Social Intelligence." IEEE/CAA Journal of Automatica Sinica **10**(8): 1692-1703.

Weise, R. A. and G. E. Hund (2016). "Financial Incentives for Reducing Proliferation Risks." Bulletin of the Atomic Scientists **72**(5): 332-338.

Yadav, A., A. K. Das, R. B. Roy, A. Chatterjee, J. K. Allen and F. Mistree (2017). Identifying and Managing Dilemmas for Sustainable Development of Rural India. International Design Engineering Technical Conferences & Computers and Information in Engineering Conference, Cleveland, Ohio, USA, American Society of Mechanical Engineers.

Yang, X., L. Wang, F. Zhu and R. Müller (2022). "Prior and governed stakeholder relationships: The key to resilience of inter-organizational projects." International Journal of Project Management **40**(1): 64-75.

Yilma, B. A., H. Panetto and Y. Naudet (2021). "Systemic Formalisation of Cyber-Physical-Social System (CPSS): A Systematic Literature Review." Computers in Industry **129:103458**.

Zhou, B., Z. Li and C. Chen (2017). "Global Potential of Rare Earth Resources and Rare Earth Demand from Clean Technologies." Minerals (Basel) **7**(11): 203.

Zhou, Y. (2014). "Electronic Waste Export Regulations: How the Responsible Electronics Recyling Act Can Protect The Defense Supply Chain From Counterfeit Electronic Parts." Public Contract Law Journal **43**(3): 527-546.

APPENDIX A

On Designing Fail-Safe Systems as an Evolving Cyber-Physical-Social System
Ph.D. Dissertation Summary and Outline

A.1 Introduction

This appendix includes a comprehensive overview of the foundational elements that shaped the direction of this dissertation. Starting with the problem statement for the dissertation, outlining the overarching goals, scope, and approaches with potential to be used as tools to determine fail-safe and adaptable defense supply networks through policy. Details of the research gaps uncovered in the thesis from Chapters 5 and 6 are explained more fully. These gaps center around the limitations of existing resilience frameworks, specifically in their capacity to respond to dynamic disruptions and the lack of integration of social elements within cyber-physical systems. Identifying these gaps informed the development of hypotheses centered on enhancing fail-safe design through new approaches to lead time management, decentralized decision-making, and integration of evolving cyber-physical-social system (E-CPSS) principles. Finally, this appendix includes an explanation of the potential of new knowledge of this research. By addressing identified gaps and testing these hypotheses using the listed test cases, this dissertation will help to advance current understanding of how defense supply networks can be restructured to become fail-safe systems. The integration of E-CPSS principles is expected to yield valuable insights not only for defense logistics but also for other critical infrastructure sectors. This research will culminate into a new frameworks and practical guidelines, like an AoP Handbook 2.0, for policy development, offering a robust foundation for designing adaptable, fail-safe systems in complex and contested environments.

A.2 Dissertation Outline

Problem Statement
Success in a contested logistics environment is crucial to ensuring that defense organizations can operate effectively and meet mission goals under conditions where adversaries are actively attempting to disrupt supply chains, communications, and operations. In these environments, systems designers must address both variation and disruption response. For that reason, adaptability and critical decision-making strategies are essential to maintain the flow of resources and ensure the mission's success in the face of such unpredictability. Historically, engineered systems, including those based in the defense industry, mainly include a focus on cyber-physical systems. These systems include the integration of physical assets with digital capabilities like those seen in automation-based manufacturing, communication networks, and sensor systems but they often overlook the critical social element that underpins human interactions and impacts. Incorporating cyber-physical-social system (CPSS) principles is an essential next step in designing modern defense systems capable of reaching fail-safe. Since contemporary threats are multidimensional, affecting not only technology and infrastructure but also human behavior and decision-making, the social component must be accounted for and integrated. The social dimension is an indispensable component in contested environments where adversaries can engage in disinformation campaigns, psychological operations, or use socially based tactics to disrupt decision-making, sow confusion, and erode trust. Additionally, complex operations often require multi-national collaboration, which involves understanding diverse cultural and operational approaches. Incorporating CPSS principles into organizations operating with the goal of enhancing their ability to coordinate, adapt, and respond collectively under instances of variation and disruption can be done through evolving policy development. The integration of evolving social factors into system designs can ultimately lead to more successful outcomes in contested logistics and defense operations. By incorporating social dynamics, such as human trust, leadership influence, team cohesion, and levels of autonomy, defense organizations can more effectively predict and counter variation and disruption to design fail-safe systems through policy. To manage variation and disruption effectively, policies may need to be designed to adapt beyond rigid, resilience-based paradigms and embed dynamic decision-making capabilities. Defense supply networks should be designed to be supported by policies that promote real-time data integration, predictive analytics, and dynamic resource management within the environment of enhanced security. These policies may benefit from encouraged investment in technologies that enable both proactive, predictive, and reactive approaches to disruptions, including tools for real-time monitoring and adaptive planning. This policy shift may create the necessary foundation for rapid system recalibration in response to changing operational conditions. Currently, defense policy frameworks include an emphasis on strict hierarchies and centralized control, but to design fail-safe systems these systems must be capable of thriving on distributed decision-making and localized autonomy. To develop cross-organizational

autonomy, policies may need to promote decentralized governance models that allow individual units to make decisions independently while maintaining alignment with broader strategic goals and units of command. This could involve redefining reporting structures in civilian settings, incentivizing collaboration across sectors, and ensuring that decision-making authority is devolved to the lowest effective level, all while safeguarding against security risks. These policies must evolve to support cross-functional, cross-organizational collaboration that bridges Government, Supplier, and User stakeholders. Defense environments, by nature, involve conflicting goals, such as cost, readiness, and security. Policy may need to emphasize partnership and communication across the entire defense ecosystem, creating frameworks for satisficing decisions that address tradeoffs in real time. This may include the development of new contractual and procurement policies and frameworks that allow more flexibility in shifting suppliers, adjusting priorities, or reallocating resources based on evolving mission requirements. Furthermore, policies may need to streamline communication channels, enhance data-sharing protocols, and foster public-private partnerships to better integrate civilian suppliers into defense networks without compromising security.

Each of these potential ways forward for developing fail-safe systems is rooted in developing policies that incorporate evolving principles that are based in CPSS design. To add specificity, further research avenues to achieve fail-safe system design are based in determining how to incorporate satisficing-based decisions into exiting frameworks, developing a mathematically supported framework for modular redundancy in specific environments, and uncovering the principles of dynamic system reconfiguration that is scalable and supportable under generalized conditions. Each of these avenues translate into potential policy frameworks that prioritize fail-safe over efficiency by allowing for more redundancy in supply chains, encouraging the diversification of supplier bases, and building in contingencies that help systems cope with disruptions. All of which will require tradeoff decisions based on the priorities of cost effectiveness, quality, and speed. Policies may benefit from moving away from rigid cost-cutting measures that prioritize efficiency at the expense of flexibility, allowing for a more balanced approach that sustains operational readiness even when disruptions occur. For integrating CPSS into policy design, this will involve establishing policies that are likely to encourage the use of advanced security protocols, while also ensuring that human factors, such as workforce training, organizational culture, and stakeholder engagement, are fully integrated into system design and management. With these methods, policies are incentivized to adopt CPSS frameworks that view fail-safe system design as a holistic challenge, encompassing not only technology and infrastructure but also the social and organizational structures that make them function effectively.

In conclusion, policy development in an evolving system must include direct advancements in flexibility and adaptability in defense networks. Policies should also emphasize continuous improvement as a fundamental component of fail-safe system design. This means requiring regular system reviews, audits, and updates that integrate lessons learned from variations and disruptions. Such policies could include mandated adaptive feedback loops that allow for constant system refinement and adjustment, supported by strategic investments in new technologies through research and development. This could be further supported by flexible funding models that allow for responsive actions in the face of changing conditions and evolving threats. By designing cross-functional autonomy, collaboration, and proactive adaptation, policies may be able to transform defense systems from being fragile and rigid into fail-safe and adaptable networks capable of handling modern-day disruptions. The outcomes of applying these potential research avenues into designing fail-safe systems can be demonstrated through the test problems TP1, TP2, and TP3. In TP1: Smart Grid Energy Management, policies rooted in flexibility and adaptability would ensure that defense energy infrastructures are fail-safe against both cyber and physical attacks, while also allowing for dynamic allocation of power resources based on real-time demand and threats. Adaptive feedback loops would help modulate energy consumption and distribution, enhancing both system efficacy and the ability to withstand disruptions. For TP2: Supply Chain Design, the policy framework would enable the creation or modification of supply chains that are not only effective under normal conditions but also highly adaptable during contested environments. Policies supporting dynamic system reconfiguration within systems of distributed autonomy would foster adaptive supply routes, decentralized resource hubs, and more responsive logistics that can reconfigure in real-time, ensuring that resources reach the frontlines even when primary routes are compromised. In TP3: Redundant Emergency Communication and Resource Allocation Systems, these policies would ensure that emergency communication systems can rapidly adapt to disruptions, maintaining continuity of operations under both natural disasters and adversarial attacks. The integration of adaptive feedback mechanisms and continuous review processes would ensure that redundant systems are constantly updated and improved, securing reliable communication channels and effective resource allocation during crises. The development of E-CPSS framework-based policies, rooted in satisficing tradeoff decisions, could serve as a powerful model for designing fail-safe systems. By integrating lessons learned from TP1, TP2, and TP3, defense policies can support the creation of dynamic, responsive, and fail-safe networks, capable of handling the complexities of modern variations and disruptions.

Key Words: Evolving CPSS, CPSS, policy, dynamic, fail-safe, flexibility, variation, disruption, response

Glossary

E-CPSS: an adaptive network that integrates physical components, digital technologies, and human elements to respond dynamically to changing conditions (Allen, Nellippallil et al. 2023)

CPSS: cyber-physical-social system; systems of interactions between physical infrastructure, cyber capabilities (like data processing and analytics), and social factors (such as human behaviors, decisions, and cultural dynamics)

Fail-safe system: System that is agile, dynamic and capable of adapting operations to combat the impacts of variations and disruptions. Does not imply a binary of either fail-safe or non-fail-safe but rather a continuum.

Policy: A definite course or method of action selected from among alternatives and in light of given conditions to guide and determine present and future decisions [1]. Ref: https://www.merriam-webster.com/dictionary/policy **Variation**: short-term changes in demand patterns or shortages. These variations can often be mitigated through adjustments or rearrangements of components within the network, ensuring continued functionality and adaptability (Cabrera, Santa et al. 2023) **Disruption**: more significant impacts, often stemming from infrastructure damage or collapse (D'Souza 2017)
Questions and Gaps
Main Question – How can systems be designed as fail-safe in the face of variation and disruption using policy as an evolving cyber-physical-social system (E-CPSS)?
Hypotheses – Designing policy as an evolving cyber-physical-social system, system designers can: i. Accurately capture evolving and emergent properties in the system space ii. Design system interaction comprehensively and includes the stakeholders iii. Determine the appropriate levels of localized autonomy and support that design through policy iv. Uncover and resolve constraints between stakeholders v. Determine how to address variation and disruption through making changes in system function, behavior, or structure
Gap 1 – How do systems respond to variation and disruption from the cyber-physical-social perspective?
Gap 2 – How can policy incorporate evolving principles when policy is traditionally inflexible?
Gap 3 – What is the level of autonomy that provides necessary system flexibility without compromising mission priorities and success?
Gap 4 – What models and frameworks exist that incorporate quantified social components into traditionally cyber-physical system spaces?
Gap 5 – Can evolving policy be generalized for different industry or governmental sectors?

Research Gaps and Research Hypotheses
Research Gap 1 What are the principles of dynamic system reconfiguration needed for systems to successfully respond to variations and disruptions?
Research Hypothesis 1 By addressing how systems can respond proactively, through strategic predictive analytics and dynamic systemic planning, and reactively, by adapting in real-time, cyber-physical systems (CPS) can integrate social elements to enhance flexibility.
Research Gap 2 What is the supporting mathematical basis for determining the appropriate level of cross-organizational autonomy for modular based redundancy?
Research Hypothesis 2 Autonomy is essential for fail-safe system design, as it can allow individual components of a network to make decisions independently, ensuring localized adaptability. A framework for strategic distributed decision-making using modular based redundancy, allowing each

organizational unit, whether military branches, contractors, or suppliers, to act autonomously while remaining aligned to a shared mission may leverage decentralized control within a E-CPSS allowing systems to be designed to maintain operational coherence even when central coordination is disrupted.
Research Gap 3 What are the principles of E-CPSS policy design needed to operate in complex multi-stakeholder environments with numerous conflicting goals?
Research Hypothesis 3 Satisficing-based decision frameworks embedded in fail-safe system design may ensure that conflicting goals are balanced dynamically without compromising system integrity. The E-CPSS perspective may offer a way to model these complex interactions, incorporating the social aspects, human decisions, partnerships, and collaborations, alongside physical and cyber systems to better manage competing demands.
Research Gap 4 What is the mathematically supported method for incorporating satisficing trade-off decisions into policy?
Research Hypothesis 4 Using satisficing decision support principles to design fail-safe networks as E-CPSS, may improve system survivability, adaptability, and long-term evolution. Rather than focusing on minimizing costs or maximizing efficiency, evolving systems may be able to continue to function effectively under changing conditions, even if all variables are not ideal.

Table 1: Test Problems (Validation Square)			
Details of test problems discussed on pages 7 – 8			
Validation	TP1 Smart Grid Energy Management	TP2 Supply Chain Design	TP3 Redundant Emergency Communication and Resource Allocation Systems
Research Gap 1	X	X	X
Research Gap 2			X
Research Gap 3		X	X
Research Gap 4	X	X	X

Research Gap 1 (RG1) What are the principles of dynamic system reconfiguration needed for systems to successfully respond to variations and disruptions?
Research Hypothesis (RH1) By addressing how systems can respond proactively, through strategic predictive analytics and dynamic systemic planning, and reactively, by adapting in real-time, cyber-physical systems (CPS) can integrate social elements to enhance flexibility.
Expected New Knowledge – *System dynamics models* to include mechanisms that allow systems to evolve in the face of variation and disruption, potentially incorporating feedback loops, predictive models, and stakeholder inputs with *dynamic system reconfiguration*.

Proposed Test Problem: TP1 Smart Grid Energy Management
Tasks **Task 1.1:** Review relevant literature on system responses to variation and disruption in energy grids. **Task 1.2:** Explore the possibility/scope of augmenting system archetypes to include a system throughout time (evolving). Explore how this is related to the differences between variation and disruption response. **Task 1.3:** Identify the test problem within the scope of energy grids. **Task 1.4:** Identify knowledge base/s that can be used in system dynamic modelling. **Task 1.5:** Create visualizations of dynamic system reconfiguration that include variation and disruption responses. **Task 1.6:** Construct an approach for evaluating system dynamic models.
Validation Approach (RG1; RH1)
What: Validation of Research Hypothesis 1 (RH1) by using TP1 from Table 1. To validate the proposed system dynamics modelling approach, I will start by using TP1 Smart Energy Grid Management (refer Table 1) as the test problem. First, I will define the key stakeholders involved in this domain, including customers (users), energy suppliers, and regulatory bodies (government). With these stakeholders clearly identified and defined, I will then apply system dynamics and system archetypes to analyze historical system data with respect to variation and disruption response. Next, I will evaluate the insights generated by the system dynamic models to ensure they accurately reflect the perspectives and interactions of these stakeholders. This step will involve comparing the system dynamic and system archetype models with known stakeholder activities and interactions to assess their accuracy. Lastly, I will simulate various decision scenarios within the TP1 to test how well the system dynamic model adapts to different contexts and manages variation and disruption simultaneously. These scenarios will be designed to challenge the model and reveal its strengths and limitations.
Technology Used: System Dynamic Modelling Software
Key words: system dynamics, energy grid, system archetypes, variation, disruption, stakeholders, evolving systems

Research Gap 2 (RG2) What is the supporting mathematical basis for determining the appropriate level of cross-organizational autonomy within modular based redundancy?
Research Hypothesis 2 (RH2) Autonomy is essential for fail-safe system design, as it can allow individual components of a network to make decisions independently, ensuring localized adaptability. A framework for strategic distributed decision-making using modular based redundancy, allowing each organizational unit, whether military branches, contractors, or suppliers, to act autonomously while remaining aligned to a shared mission may leverage decentralized control within a CPSS framework allowing systems to be designed to maintain operational coherence even when central coordination is disrupted.

Expected New Knowledge – Information on mathematical formulation to determine the level of *modular based redundancy* necessary for different disaster situations through trade-off decisions. These determinations would be incorporated into policy recommendations.

Test Problem: TP3 Redundant Emergency Communication and Resource Allocation Systems

Tasks

> **Task 2.1** Develop a framework to determine the level of redundancy is appropriate by leveraging Just-In-Time and Just-In-Case inventory management techniques.
>
> **Task 2.2** Develop a method for prioritizing inventory redundancy and incorporate methods for early detection of emergent properties.
>
> **Task 2.3** Create Multi Level Redundancy Matrix
>
> **Task 2.4** Develop mathematical model for demonstrating robust coupled decision using DSP's.
>
> **Task 2.5** Analyze different scenarios and run simulations.

Validation Approach (RG2; RH2)

What: Validation of Research Hypothesis 2 (RH2) by using TP3 from Table 1.
I will validate the proposed model using the test problem of Redundant Emergency Communication and Resource Allocation Systems. The complex logistics network, involving processes like rapid new acquisition, rapid contracting supply negotiations, fluid supply demands, and emergency situations, will be modelled as coupled Decision Support Processes (DSPs). I will create and test various scenarios to assess how the model handles uncertainty, decision interactions, and multiple decision levels. After validation, I will generalize the method to apply across other fluid logistics networks, ensuring its broader applicability in policy design for complex systems. I will look at the problem from the perspective of various levels of autonomy and organizational structures by partitioning the problem. Through TP3, I will provide information on mathematical formulation to determine the appropriate redundancy levels in fluid supply environments which can be used to influence the development of evolving policy.

Technology Used – DSP's, cDSP, DSIDES

Key Words: Organizational structure, fluid supply demands, inter-stakeholder interactions, rapid acquisition, modular redundancy, emergent properties

Research Gap 3 (RG3)
What are the principles of E-CPSS policy needed to operate in complex multi-stakeholder environments with numerous conflicting goals?

Research Hypothesis 3 (RH3)
Satisficing-based decision frameworks embedded in fail-safe system design may ensure that conflicting goals are balanced dynamically without compromising system integrity. The CPSS framework may offer a way to model these complex interactions, incorporating the social aspects, human decisions, partnerships, and collaborations, alongside physical and cyber systems to better manage competing demands.

Expected New Knowledge – (i) Insights to design future state of multi-stakeholder systems, (ii) Information to incorporate evolutionary aspects of designing policies based in satisficing-based decisions.

Test Problem: TP2 Supply Chain Design

Tasks

Task 3.1 Review predictive analytics methods for multi-stakeholder systems. **Task 3.2** Prepare data for the test problems. **Task 3.3** Develop forecasting models **Task 3.4** Integrate forecasting with policy design **Task 3.5** Apply final models to test problems **Task 3.6** Interpret the results. Identify variable importance. **Task 3.7** Identify variables and the impact at various time steps. Analyze and recommend policy development. **Task 3.8** Refine forecasting and policy design approach **Task 3.9** Policy recommendations **Task 3.10** Develop method or framework for incorporating satisficing-based decisions as evolving policy based on Tasks 3.1 to 3.9
Validation Approach
What: Validation of Research Hypothesis 3 (RH3) by using TP2 from Table 1. To validate RG3 and RH3, data from TP2 - Supply Chain Design will be used. First, I will apply predictive analytics (with policy considerations), including time series analysis, to forecast the future state of a particularized industry. Using these forecasts, I will design adaptive policies tailored to the predicted evolution of the system. Next, these policies will be tested under different scenarios to assess their flexibility and effectiveness in responding to potential future developments. Finally, the model's accuracy and the adaptability of the policies will be evaluated against real-world trends and historical data-based insights. The test problem is exceptionally broad and will be narrowed and focused depending on sponsoring organization.
Technology Used – Satisficing-based design, Deep Learning, Interpretable Machine Learning
Key Words: Satisficing, flexibility, supply chain, evolving

Research Gap 4 (RG) What is the mathematically supported method for incorporating satisficing trade-off decisions into policy?
Research Hypothesis 4 (RH4) Using satisficing decision support principles to design fail-safe networks as E-CPSS, may improve system survivability, adaptability, and long-term evolution. Rather than focusing on minimizing costs or maximizing efficiency, evolving systems may be able to continue to function effectively under changing conditions, even if all variables are not ideal.
Expected New Knowledge – (i) Principles to establish an Information model for designing evolving policies, (ii) Information model for designing evolving policy.
Test Problem: All problems (TP1, TP2, and TP3)
Tasks **Task 4.1** Map the outcomes obtained from Research Gaps 1, 2, 3, and 4. **Task 4.2** Analyze and evaluate the outcomes to develop an information model. *I am not outlining any specific tasks right now. The progress of this depends on the tasks and outcomes associated with other research gaps.*
Validation Approach
What: Validation of Research Hypothesis 4 (RH4) by using TP1-TP3 from Table 1.

I will validate the proposed method by applying it to all test problems, simulating systems under uncertainty and conflicting stakeholder interests. The model will be used to generate scenarios, predict future system behavior, and provide robust policy recommendations. I will then evaluate the effectiveness of these policies in managing variation and disruption and conflicting interests, documenting results and assessing the model's overall usefulness and practicality for designing fail-safe systems.
Key Words: Information Model

Details of Test Problems
TP1 Smart Grid Energy Management This test case could review the ability of a dynamic system to respond to evolving and fluctuating energy demands and supply, such as integrating renewable energy sources (e.g., solar and wind) with unpredictable output. The evolving system should adapt real-time energy distribution policies based on environmental data, consumption patterns, and grid stability. This would be coupled with policy development for the use and deployment of energy. This problem will be used in validating Research Hypotheses 1.
TP2 Supply Chain Design A satisficing-based approach can be tested in an evolving supply chain management scenario where the system must make decisions about supplier selection, inventory levels, and logistics that leverages Just in Time and Just in Case methods. The system should achieve practical solutions under changing conditions, such as demand fluctuations, supplier delays, and resource shortages, without aiming for perfect optimization. This problem will be used in validating Research Hypotheses 3.
TP3 Redundant Emergency Communication and Resource Allocation Systems During a natural disaster, simulate failure in a city's emergency response communication system, which integrates social components like real-time reports from citizens and on-ground responders. The test should measure the ability of redundant modules to reconfigure and maintain coordination among first responders, volunteers, and affected citizens. Social data like evacuation behaviors, crowd movement, and information on social factors could be quantified and integrated into the backup system, ensuring accurate resource allocation and communication despite system failures. This would include the development of evolving policy systems that can meet emerging needs. This problem will be used in validating Research Hypotheses 2.

Validation Square

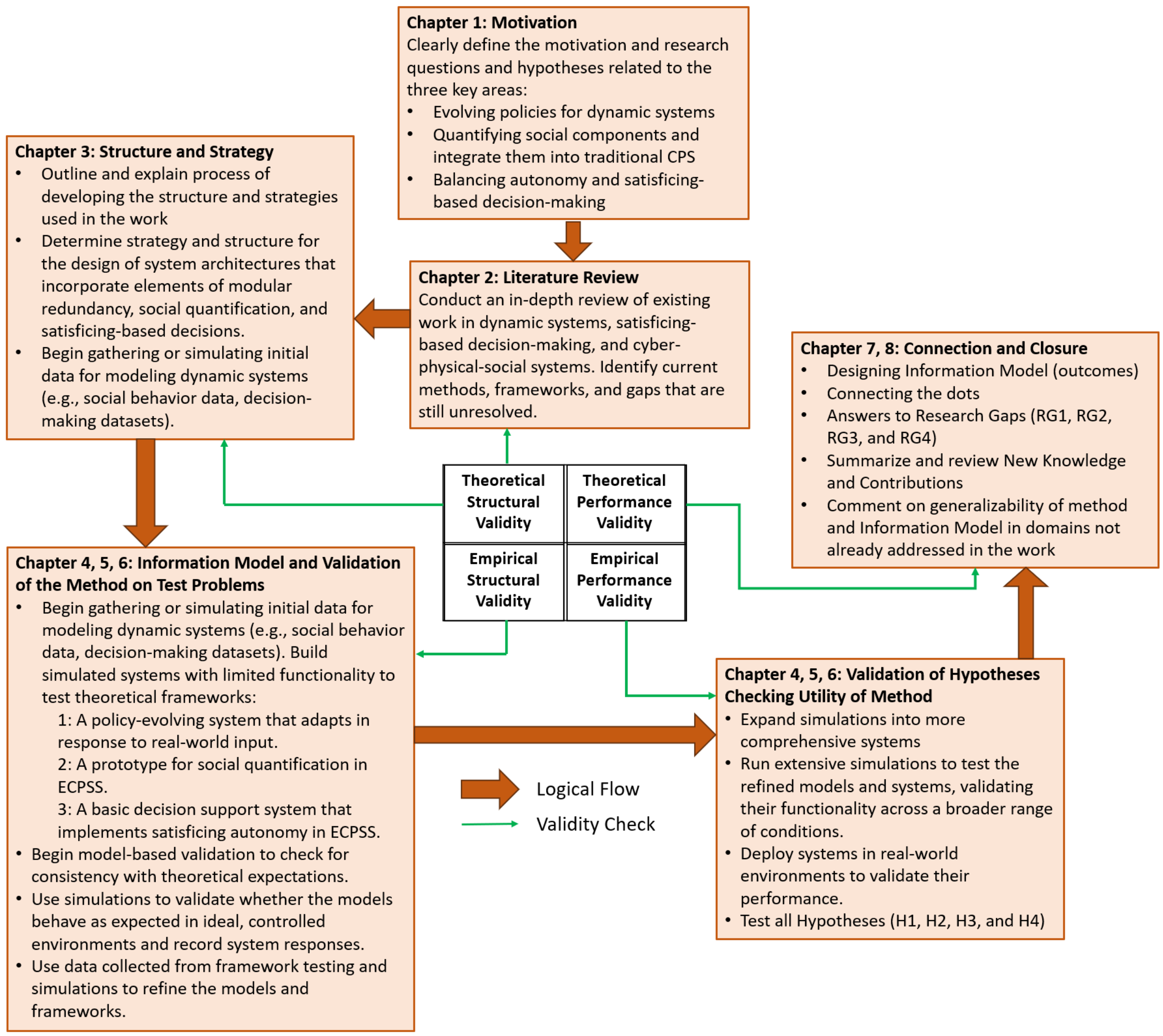

Figure 1: Verification and Validation Square

Theoretical Structural Validation

Is the design method internally consistent?

- Ensure that the constructs of the proposed method/s and processes followed are logically sound.
- The literature review and discussion of the State of the Art involves verifying that the components of CPSS, policy design, predictive analytics, policy design for fail-safe systems, and decision support techniques for designing policies interact and align with each other.
- Consistency of simulations followed and its theoretical appropriateness in designing policies.
- Develop clear definitions of the constructs of predictive analytics, E-CPSS, satisficing, resilient, variation and disruption, evolving policy and decision support. Include any other theory, principles, and technology used.

▪ Discuss on theoretical correctness and appropriateness of the selected method and illustrate how the constructs work together within the policy design framework.
Empirical Structural Validity *Are the example problem(s) intended to test elements of the method appropriate?*
▪ Document the appropriateness of policy design for the test problems to validate the method/s. These test problems include Smart Grid Energy Management (TP1), Supply Chain Design (TP2), and Redundant Emergency Communication and Resource Allocation Systems (TP3) ▪ Discuss on appropriateness on following five aspects: 1. Evolving Cyber Physical Social Systems 2. Policy Design 3. Modular Redundancy 4. Inter-organizational Autonomy 5. Dynamic System Reconfiguration ▪ <u>Process and Sub-Process Relevance:</u> Document to demonstrate the relevance that the scenarios/processes/sub-processes created accurately reflect real-world (or required) conditions and challenges. o Document that the data and problem structure associated with different test problems can support to draw conclusions for: RH1, RH2, and RH3 ▪ Document the relation and appropriateness of validating Hypothesis 1, 2, 3, in validating Hypothesis 4.
Empirical Performance Validity *Does the application of the method for the test problems produce useful results?*
▪ Build confidence and document of the useful and appropriateness of the method/s and the results obtained. ▪ Comment on the logical appropriateness of the result obtained and its relevance in decision making for designing policies. ▪ Document the utility of the test problems in producing useful results for the stated results. ▪ Discuss on the generalizability and extension of the proposed method/s for different application of E-CPSS and designing policy for fail-safe systems. ▪ Discuss on the utility of information model in designing appropriate policies and obtain useful results.
Theoretical Performance Validity *Does the application of proposed method to other comprehensive test problems yield useful and appropriate results?*
▪ Build confidence and demonstrate the potential of the policy design method to address broad and complex problems beyond the test scenarios. ▪ Use the confidence built from theoretical and empirical validations to support the method's general applicability. ▪ Extract the general characteristics of the test problem, tie it to different problems and argue the generalizability (and the ability to produce practical results for various test problems) of the method.

Project Stages (1 through 5)		
Stage 1 - Literature Review and Problem Definition		
	MS Thesis Connection	Ph.D. Chapter
1. Problem Definition and Research Objectives	**Chapter 1, 2**	**Chapter 1**
Tasks Clearly define the research questions and hypotheses related to the three key areas: 1.1: How to design evolving policies for dynamic systems? 1.2: How to quantify social components and integrate them into traditional CPS? 1.3: How to balance autonomy and satisficing-based decision-making?		
2. Enhance and Augment Literature Review	**Chapter 2, 3**	**Chapter 2**
Tasks Conduct an in-depth review of existing work in dynamic systems, satisficing-based decision-making, and cyber-physical-social systems. Identify current methods, frameworks, and gaps that are still unresolved.		
3. Structure and Strategy	**Chapter 5, 6**	**Chapter 3**
Task Determine strategy and structure for the design of system architectures that incorporate elements of modular redundancy, social quantification, and satisficing.		
4. Set Up Collaborative Partnerships		
Task Partner with industry or academic institutions to gain access to real-world test environments (e.g., smart cities, health systems, autonomous systems) for data collection and future validation.		

Stage 2 – Conceptual Framework Development and Early Modeling

	MS Thesis Connection	Ph.D. Chapter
1. Development of Conceptual Frameworks	**Chapter 5, 6**	**Chapter 3**
Tasks Develop preliminary models for evolving systems policy, social quantification methods, and satisficing-based decision support systems. Formulate initial hypotheses for integrating social behaviors into traditionally cyber-physical systems and how satisficing-based systems will perform.		
2. Simulated System Design	**New**	**Chapter 4**
Tasks Begin gathering or simulating initial data for modeling dynamic systems (e.g., social behavior data, decision-making datasets). Build simulated systems with limited functionality to test theoretical frameworks: 2.1: A policy-evolving system that adapts in response to real-world input. 2.2: A prototype for social quantification in ECPSS. 2.3: A basic decision support system that implements satisficing autonomy in ECPSS.		
3. Initial Validation (Model-based)	**New**	**Chapter 5**
Tasks Begin model-based validation to check for consistency with theoretical expectations. Use simulations to validate whether the models behave as expected in ideal, controlled environments. Recording system responses to different variables or environments.		

Stage 3 – Refinement and Full System Development

	MS Thesis Connection	Ph.D. Chapter
1. Model/Framework Refinement	**New**	**Chapter 5**
Tasks Use data collected from framework testing and simulations to refine the models and frameworks. Adjust assumptions, data inputs, and parameters for social quantification and satisficing decision-making within ECPSS.		
2. Full System Design and Expansion	**New**	**Chapter 5**
Tasks Expand simulations into more comprehensive systems with enhanced functionality for evolving policies and modular redundancy. Integrate and quantify full-scale social components (e.g., human feedback, interaction patterns) into the system.		
3. Validation with Simulations	**New**	**Chapter 6**
Tasks Run extensive simulations to test the refined models and systems, validating their functionality across a broader range of conditions. Begin testing decision-making autonomy in more dynamic and uncertain environments, focusing on how satisficing works under different constraints.		

Stage 4 – Validation in Real-World Environments

	MS Thesis Connection	Ph.D. Chapter
1. Real-World System Deployment	**New**	**Chapter 6**
Tasks Deploy systems in real-world environments (e.g., smart city traffic management, autonomous vehicle fleets, hospital systems) to validate their performance. Ensure that evolving policies and decision-making systems are stress-tested in varying levels of dynamic, unpredictable conditions.		
2. Validation of Social Component Quantification	**New**	**Chapter 7**
Tasks Validate the effectiveness of social component quantification in real-world CPS, ensuring that systems can adapt based on human behavior, preferences, and feedback.		
3. Testing of Satisficing-Based Decision Support	**New**	**Chapter 7**
Tasks Test the satisficing-based decision support systems in real-world scenarios, where perfect optimization is not possible, and practical decisions must be made (e.g., in autonomous navigation or supply chain management).		
4. Data Collection for Validation	**New**	**Chapter 7**
Tasks Collect extensive real-world data from system performance, user interactions, and environmental responses. Gather user feedback to measure satisfaction and system efficacy related to evolving policies and decision support systems.		

Stage 5 – Evaluation and Final Analysis

	MS Thesis Connection	Ph.D. Chapter
1. System Refinement	**New**	**Chapter 8**
Tasks Refine evolving system policies to better respond to diverse conditions. Improve social quantification models to more accurately reflect human behaviors. Enhance satisficing decision support algorithms to strike better balances between decision quality and speed.		
2. Final Validation and Generalization	**New**	**Chapter 8**
Tasks Perform final rounds of validation, testing system robustness across different scenarios and conditions, including stress tests to assess system failures and redundancy. Ensure that systems maintain performance under varied social behaviors and decision-making challenges.		
3. Final Data Analyses and Hypothesis Evaluation	**New**	**Chapter 8**
Task Conduct a final analysis of all collected data to evaluate the success of the proposed approaches/frameworks.		
4. Evaluation of Results	**New**	**Chapter 8**
Tasks Evaluate claims made in dissertation and discuss generalization, efficacy, and areas of improvement.		
5. Recommendations for Future Research	**New**	**Career Proposal (Chapter 9)**
Tasks Based on the findings, outline key areas where further research is needed, such as improvements in social behavior modeling or decision-making under extreme uncertainty. Propose potential applications of the developed systems in new domains, such as defense, healthcare, transportation, or autonomous manufacturing.		

Dissertation Outline (*very preliminary stages)*

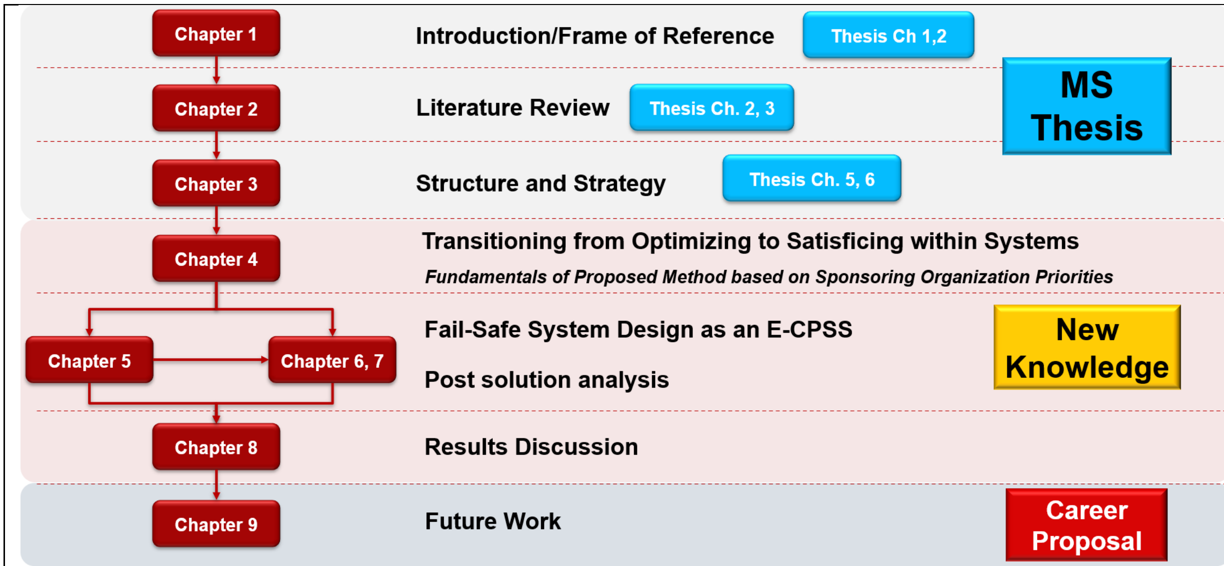

Figure 2: Dissertation Outline

Dissertation Schedule

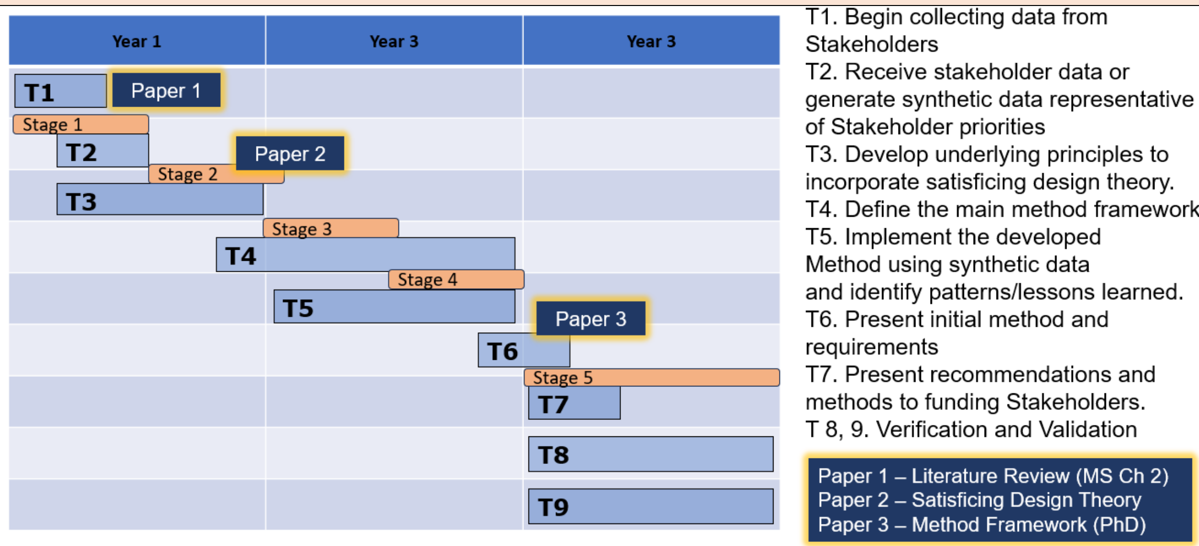

Figure 3: Optimistic Dissertation Schedule and Proposed Papers *(high level)*

Proposed Papers

Paper 1 – Comprehensive Literature Review on System Variation and Disruption Response
Paper 2 – Satisficing Design Theory in the Context of E-CPSS
Paper 3 – Fail-Safe System Design through Policy as an E-CPSS