NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

NAVY ADDITIVE MANUFACTURING AFLOAT, DATA SECURITY ANALYSIS

by

Edward C. Muncy

December 2023

Thesis Advisor:	Britta Hale
Co-Advisor:	Douglas L. Van Bossuyt
Second Reader:	Terry D. Norbraten

THIS PAGE INTENTIONALLY LEFT BLANK

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

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2023	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE NAVY ADDITIVE MANUFACTURING AFLOAT, DATA SECURITY ANALYSIS	**5. FUNDING NUMBERS**
6. AUTHOR(S) Edward C. Muncy	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

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

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

13. ABSTRACT (maximum 200 words)

The integrity of additive manufacturing (AM) schematics is currently an open question for AM systems installed onboard U.S. Navy ships. Additionally, there are several possible entry points that exist in the AM toolchain that provide hackers with numerous opportunities to corrupt valuable data. This research focuses on understanding how AM systems function, especially in schematic (aka 3D printer diagram) transfers to and from ships; identifies existing weak points in current AM security practices; and develops a smooth process for integrity protection of AM schematics. The recommended implementation spans both user and application system aspects to ensure comprehensive protection. To achieve these results, this thesis meticulously compiles and analyzes various additive manufacturing policies across the Department of Defense to scrutinize alternative architectures, from manpower based to blockchain, and conducts cross-comparisons against prevailing guidelines.

14. SUBJECT TERMS additive manufacturing, AM, 3D printing, integrity, authentication, security, vulnerabilities, toolchain, data, schematic, file, Navy, ships, USN, system	**15. NUMBER OF PAGES** 117
	16. PRICE CODE

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

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

NAVY ADDITIVE MANUFACTURING AFLOAT, DATA SECURITY ANALYSIS

Edward C. Muncy
Lieutenant, United States Navy
BS, United States Naval Academy, 2016

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
December 2023

Approved by: Britta Hale
Advisor

Douglas L. Van Bossuyt
Co-Advisor

Terry D. Norbraten
Second Reader

Gurminder Singh
Chair, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The integrity of additive manufacturing (AM) schematics is currently an open question for AM systems installed onboard U.S. Navy ships. Additionally, there are several possible entry points that exist in the AM toolchain that provide hackers with numerous opportunities to corrupt valuable data. This research focuses on understanding how AM systems function, especially in schematic (aka 3D printer diagram) transfers to and from ships; identifies existing weak points in current AM security practices; and develops a smooth process for integrity protection of AM schematics. The recommended implementation spans both user and application system aspects to ensure comprehensive protection. To achieve these results, this thesis meticulously compiles and analyzes various additive manufacturing policies across the Department of Defense to scrutinize alternative architectures, from manpower based to blockchain, and conducts cross-comparisons against prevailing guidelines.

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

List of Figures

List of Tables

THIS PAGE INTENTIONALLY LEFT BLANK

List of Acronyms and Abbreviations

ACAS	Assured Compliance Assessment Solution
AM	Additive Manufacturing
AMOC	Advanced Manufacturing Operations Cell
AN/SPY-1	Array, Navy/Search Protect, Yellow 1
C2	Command and Control
CAC	Common Access Card
CAD	Computer Aided Design
CANES	Consolidated Afloat Networks and Enterprise Services
CC	Cloud Computing
CD	Compact Disks
CG-LIMS	Coast Guard Logistics Information Management System
CHENG	Chief Engineer
CIA	Confidentiality, Integrity, and Availability
CNC	Computer Numerical Control
CLI	Command Line Interface
CM	Cloud Manufacturing
CO	Commanding Officer
CUI	Controlled Unclassified Information
DAME	Digital Advanced Manufacturing Ecosystem

DLR	Depot Level Repair
DME	Digital Manufacturing Environment/Ecosystem
DOD	Department of Defense
DODIN	Department of Defense (DOD) Information Network
EMCON	Emissions Control
ESD	Electronic Systems Support Detachment
FDM	Fused Deposition Modeling
FFF	Fit, Form, and Function
FTSC PAC	Fleet Technical Support Center, Pacific
GUI	Graphical User Interface
HBSS	Host-Based Security System
HLF	Hyperledger Fabric
IIoT	Industrial Internet of Things
IoT	Internet of Things
IRB	Institutional Review Board
IPT	Integrated Product Team
ISSA	In-Service Support Activity
JAMMEX	Joint Additive Manufacturing Model Exchange
JAMWG	Joint Additive Manufacturing Working Group
JTDI	Joint Technical Data Integration
MRG	Main Reduction Gear
NAVAIR	Naval Air Systems Command

NAVSEA	Naval Sea Systems Command
NIWC PAC	Naval Information Warfare Command Pacific
NIST	National Institute of Standards and Technology
NSWC	Naval Service Warfare Center
NUC	Next Unit of Computing
NPS	Naval Postgraduate School
PMA	Program Manager, Air
PKI	Public Key Infrastructure
PoW	Proof of Work
RDTE	Research, Development, Test, and Evaluation
RMF	Risk Management Framework
CSF	Cybersecurity Framework
SD	Secure Digital
SFLC	Surface Forces Logistics Center
SM	Subtractive Manufacturing
SSH	Secure Shell
STIG	Security Technical Implementation Guide
STL	Standard Tessellation Language
TDP	Technical Data Package
TIMB	Technical Information Management Branch
TWH	Technical Work Holder
TWP	Technical Work Package

TXID	Transaction ID
UAV	Unmanned Aerial Vehicle
UI	User Interface
USCG	United States Coast Guard
USN	United States (U.S.) Navy
USB	Universal Serial Bus
VPN	Virtual Private Network
XO	Executive Officer

Executive Summary

Securing files and data in the digital realm remains a growing concern across various sectors, including business and industry. One notable category is that of Additive Manufacturing (AM) schematics, otherwise known as 3D printing schematics. The military recognizes immense possibilities and expedience offered by AM, primarily focusing on leveraging its streamlined production processes and logistical advantages to enhance resource utilization and operational effectiveness; however, limited and/or vague information is available regarding the current state of security tools and policies employed for managing AM schematics across the Fleet. The aim of this work is to understand how the United States Navy (USN) is currently approaching management of AM schematics, especially shipboard, so as to identify appropriate security measures and to propose a security solution that integrates with current AM processes for a usable and practical outcome. We draw heavily from AM architecture and policy documents as well as practices and experiences of Department of Defense (DOD) personnel to build a comprehensive view of the state of the art. Additionally, the research surveys other work conducted on supply chain security using blockchain and assesses its efficacy in supporting security under current architectures and shipboard constraints.

Background exploration was conducted to understand the challenges for AM security. Information was gathered from various sources, including industry, academia, and DOD. While many sources emphasize the importance and potential of AM technology, solutions for existing security concerns – especially for schematic authenticity guarantees – are few. Prior research mainly acknowledges that there is a problem, but how it can be addressed is unique to the use case, with the USN shipboard uses being distinct from industrial system use. The literature review also hints at how AM security in the USN and DOD might be afflicted by existing schematic transfer methods, such as the use of external storage devices, encrypted email, and cloud-based storage methods. Existing proposals using blockchain are also explored through two projects: Project Hivemind and Blockchain Mergence. We delve into blockchain applications, benefits, and limitations – especially for shipboard use.

There are two primary branches in the Navy with notable existing AM policies: the surface forces (Naval Sea Systems Command (NAVSEA)) and air forces (Naval Air Systems

Command (NAVAIR)). Both seek to use AM to accommodate their specific mission sets. This research explains how AM data is currently handled in the USN. Additionally, ongoing projects are discussed to provide insight into the direction in which the USN is heading.

The United States Coast Guard (USCG) is another military branch seeking to unlock the full advantages that AM can provide. While the USN AM process is still undergoing refinement, the USCG aspires to eventual alignment. The USCG presently relies on informal guidance for the utilization and approval of AM parts within their force, but official guidance is still pending.

Following the exploration of current AM handling in the DOD, the research breaks down the current policies to better understand what is practical in the future. Understanding the intent and goals behind these processes helps refine our solution for easier incorporation with current and future practice. Existing instructions do not go into great detail regarding specific security practices, and there are several locations in the Navy's current data flow where vulnerabilities can fester. In the scope of this research, authentication is the primary pillar of security being analyzed. It must ensure that access to and generation of data, instructions, and ideas related to AM schematics are limited to authorized users such as the router and approving authorities such as a Chief Engineer (CHENG), sponsors, etc.

In the next stage, this project takes a qualitative approach and analyzes the results of a survey questionnaire built to shed light on existing problems from the end-user perspective. More specifically, the survey seeks to understand how current AM schematic transfer is perceived from a functional and security viewpoint, including how this data is generated, authorized, stored, and transferred.

With the gathered information, this research develops a security solution proposal with a step-by-step process to help the surface warfare community and perhaps even the DOD. Authentication of AM schematics is a primary focus of this proposal, with design constraints for functionality and usability within current process and network architectures. A formal method must be set in place that confirms the data authenticity between the sender and recipient of AM information, especially from the authorizing authority of the approved diagrams and the end-user. This solution provides integrity assurance of the source of the AM schematic, its approval by the requisite authorities for use, as well as functional plans for when shipboard networking constraints (e.g., bandwidth limitations, Emissions

Control (EMCON), etc.) inhibit offship access. Moreover, under this proposal, once a schematic is approved for use the integrity of that schematic remains intact, attesting to authenticity from the time of approval. Being assured of exactly who has a hand in each step of the process, an assurance this solution provides, is vital in knowing that the AM schematic results in a 3D-printed part that is safe for use.

THIS PAGE INTENTIONALLY LEFT BLANK

Acknowledgments

I sincerely would like to convey my utmost thanks to my thesis advisory team, Dr. Britta Hale, Dr. Douglas Van Bossuyt, and Terry Norbraten, for helping me along this journey despite my elusiveness at times. I want to thank Dr. Hale, especially for her commitment to this project despite her one thousand other daily obligations. The patience, advice, and encouragement these professionals showed me throughout this process were all vital to the completion of this work.

I would also like to thank my classmates, who not only helped ensure that I succeeded in the classroom during my time here in Monterey, but also provided welcome companionship and laughter during these trying weeks.

Of course, I also wish to extend my gratitude again to my family and friends all over the country who pray for my success and well-being daily, especially my mother. Their unending support has pushed me through multiple life events, and this will be one more chapter to look back on and appreciate because of their boundless generosity.

And lastly, I wish to dedicate this thesis to remembering my honorable grandfather, Griffith Hopkins. He was a man who represented the embodiment of love, integrity, wisdom, and hard work; there will certainly never be one like him again. I'm so grateful for what you gave to our family, and I pray you're finally at peace. Love you, Pops.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 1:
Introduction

Securing files and data in the digital realm remains a steadily growing concern across various sectors, including business and industry. The use of the Confidentiality, Integrity, and Availability (CIA) triad has evolved into a widely accepted standard for safeguarding valuable data. Within this spectrum of data, one notable category is that of Additive Manufacturing (AM), otherwise known as 3D printing data. AM is a rapidly evolving technology across various industries and ensuring precise adherence to the CIA triad has become increasingly crucial for robust security in the AM context. Regrettably, AM technology still faces limitations in terms of how data is exchanged among multiple parties.

While certain features of this technology can be employed to guarantee the satisfaction of some aspects of the CIA triad, the Department of Defense (DOD) remains particularly concerned about the authentication security of 3D print schematics. Ensuring the confidentiality, integrity, and availability of data is crucial, but the specific challenges posed by the authentication of 3D print schematics continue to be a focal point for agencies like the DOD.

1.1 Motivation

The time needed to replace vital components within DOD assets frequently surpasses initial expectations. However, the military recognizes immense possibilities and expedience offered by AM and primarily focuses on leveraging AM's streamlined production processes and logistical advantages to enhance resource utilization and operational effectiveness. Gaining access to technology that can craft unique parts, mainly through the innovative process of AM, can significantly improve mission readiness and alleviate logistical stress. However, deploying these 3D-printed parts into valuable equipment requires ensuring the integrity of the 3D print schematics used, especially when our armed forces rely on this technology. Building a resilient cybersecurity infrastructure for AM data transfer within the DOD is crucial to instilling confidence in using these precisely crafted components.

AM data transfer refers to the secure transmission and exchange of information crucial to the AM process. This encompasses the transfer of digital data related to the design, specifications, and parameters of the 3D objects being produced through AM techniques, some of which will be covered in this thesis. The focus of AM data transfer security is on safeguarding this digital information's integrity, confidentiality, and authenticity throughout its journey from design to the actual fabrication of the object. Key aspects include protecting against unauthorized access or modifications, ensuring that the data reaches its destination accurately, and preventing any compromise that could impact the quality, reliability, or safety of the manufactured product. The goal is to establish a secure and trustworthy environment for the exchange of data specific to the additive manufacturing domain, acknowledging the unique properties and requirements associated with this intricate process. This thesis will primarily focus on the aspects of integrity/authenticity to help validate the legitimacy of AM data and its movement within the 3D printing process.

The issue of AM security provides an opportunity for diverse and nuanced strategies and solutions. The United States Navy (USN), in particular, has taken great interest in incorporating this technology into its ships and other assets, as the precise definition remains unknown in many of its policies. With so many 3D printers available, a solid security tool with a firm policy should be a top priority for this technology to help AM data move about safely within the DOD. This thesis centers on analyzing current and evolving needs and aspirations within the USN, aiming to pinpoint deficiencies in existing security methodologies and propose innovative solutions to advance the field. With the information provided in this report, decision-makers within the USN and DOD can better understand the challenges existing within AM security policies while suggesting possible methods to transfer this data safely.

One methodology that has been proposed to support the integrity of AM data across the surface fleet and its 3D printers is using blockchain technology. Blockchain acts as a distributed, immutable ledger that can record transactions and track assets on a network [1]. Using blockchain as an AM security practice could allow an established set of users to create, view, and edit data in a way that does not allow tampering from anyone not a member of the created network. Among other solutions, thesis investigates the potential application of blockchain as an element in developing a more efficient and secure AM network design for the Surface Navy and maybe even the DOD.

After providing an architectural analysis of how secure AM schematic transfer can be achieved within current operational approaches, this thesis looks at an authentication solution for AM schematics that introduces minimal change to the current operational processes end-users rely on. This involves offering a concept system architecture that captures current practices and outlines how and when authentication should be added.

Among other options analyzed for that solution are block-chain based options such as the Naval Postgraduate School (NPS) blockchain project, named Blockchain Mergence, and the Naval Sea Systems Command (NAVSEA)-sponsored Project Hivemind. Through cross-comparing existing initiatives, current practices, and necessary security guarantees, we explore alternative methods for cultivating an efficient AM security concept and ultimately proposes an architecture that might enhance the current state of AM security.

1.2 Problem Statement

Limited and/or vague information is available regarding the current state of security tools and policies employed for managing AM data across the Fleet. The lack of comprehensive insights into these aspects underscores the need for a thorough examination to identify potential gaps and formulate effective strategies for enhancing AM data security within the Fleet. While blockchain may be one of many solutions for ensuring integrity, it is first necessary to understand the Navy's definition of "secure AM." This will guide the way on how to achieve that security within current AM workflow processes. In this work, experiences and opinions of diverse DOD personnel actively engaged with this technology are gathered for comprehensive insights. Simultaneously, we'll leverage the research conducted on current DOD blockchain projects and assesses their alignment with current practices and experiences of DOD personnel andAM policy.

1.3 Research Questions

The ultimate goal of this work is to understand how the USN wishes to establish secure practices regarding AM data so that appropriate security measures can be applied accordingly. Additionally, the works of Project Hivemind and Blockchain Mergeance are dissected to discover how elements of each can be used and/or combined to improve the security features of blockchain in a new policy.

Research questions that will be answered include:

- What is the current state of AM security in the USN?
- What might represent a secure and usable AM workflow in the Fleet?
- Who should have approval authority for AM data and how should it be authenticated?
- How effective is a blockchain in addressing the needs of this workflow?

1.4 Thesis Organization

Chapter 2 furnishes background information and delves into the typical creation and transfer of AM data. It further elucidates existing threat vectors and the various transfer methods presently employed. Following that, we delve into an examination of pertinent literature and related research. Chapter 3 delves into the current application of AM data security within the USN, scrutinizing existing practices and protocols. Concurrently, Chapter 4 scrutinizes the United States Coast Guard (USCG)'s current approach to data security. Building on these insights, Chapter 5 covers a comprehensive examination of prevailing policies within the Fleet. The goal of this analysis is to uncover any inconsistencies and offer constructive suggestions for improvement. In Chapter 6, we explore existing workflow practices, delving into experiences and recommendations from DOD personnel.

This thesis also contains a supplemental, CUI-classified chapter dedicated to extracting valuable insights from a diverse array of end-users proficient in AM technology and current processes in the Fleet. This supplemental chapter delves into an analysis of user perspectives, existing practices, and ongoing projects within the realm of securing AM.

Subsequently, in Chapter 7, we scrutinize the outcomes of the analyses and propose a novel AM architecture applicable to the USN Surface Fleet. Appendix B.3 explores some finer details behind Project Hivemind and assesses its overall security contribution. In Appendix C.2, we investigate a modification of the Blockchain Mergence project to see how it can be used in an AM environment.

CHAPTER 2:
Background/Related Work

This chapter provides a background on AM and explains various thought processes, active research, and methodology already explored in AM cybersecurity. Furthermore, the synthesis of information from various sources serves to underscore that the research undertaken for this thesis does not duplicate the efforts of others. The primary goal of this comprehensive background exploration is to comprehend challenges identified across multiple sources and potentially enhance techniques previously examined and employed within the USN and DOD. Information was compiled from diverse backgrounds, encompassing industry, academia, and the DOD.

2.1 Understanding Additive Manufacturing

AM refers to innovative technologies that construct physical objects from digital models layer by layer. Unlike traditional methods that subtract material from a larger piece, AM builds up objects from scratch, facilitating the creation of intricate and customized shapes. Businesses across various industries, including aerospace, automotive, medical, and consumer products, have increasingly adopted this technology for its convenience and transformative potential [2].

AM utilizes diverse materials, such as plastics, metals, ceramics, or biological substances, depending on the application and desired product properties. Techniques like direct metal laser melting, electron beam melting, and binder jetting are commonly employed in the additive manufacturing process [2]. Despite its numerous advantages, including waste reduction, time and cost savings, and enhanced innovation, additive manufacturing faces challenges, such as quality control, material limitations, and security. The remainder of this chapter will delve into the multifaceted security challenges encountered by AM technology.

2.2 The Additive Manufacturing Workflow

While plenty of sources emphasize the importance and potential of AM technology, the solutions for these existing security concerns are few. Prior research mainly only acknowledges that there seems to be a problem without actually addressing it. However, there is usually always a description and deep exploration of a printer's typical workflow and the existence of multiple network architectures to which it can be subjected. But how does one guarantee data integrity in the AM flow chain? The first step in building and improving upon the security of any system is to first get into the mindset and acknowledge the existence of residual threats. Once this is recognized, only then is it acceptable to transition onto the next step to assess further and categorize any discovered vulnerabilities in the processes and system [3].

Zeltmann et al. [4] dissect their interpretation of the entire AM workflow into a series of three phases to provide a more digestible image of the overall AM process chain and where things could go wrong. The first phase is design, which starts with the concept of the part schematic, the creation within the Computer Aided Design (CAD) software, and then the finite element analysis (or optimization). The second phase involves manufacturing, which handles a Standard Tessellation Language (STL) file and goes through to the G-code and printer. Finally, the testing phase involves mechanical or physical testing methods that may or may not use destructive techniques to follow quality assurance requirements. The testing methods of the final phase are subject to vary, but the point of this phase is to demonstrate that the part can withstand the expected demands.

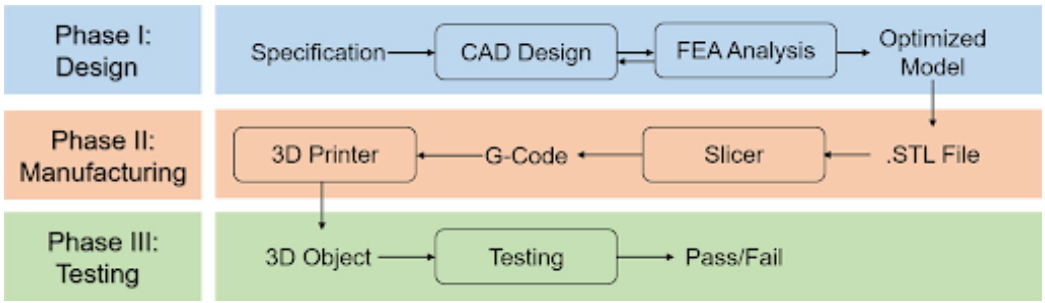

Figure 2.1. Additive Manufacturing Process Chain. Source: [4, figure 2].

This research only provides a general overview of the flow of AM data and does little to address any specific concerns for security within the entire process. Instead, the emphasis is placed on the multiple layers within these phases, demonstrating potential access points for attackers.

In related research, Graves et al. [3] elucidate that the characteristics of AM workflows can significantly differ based on the installation configurations of these 3D printers within our networks. Some possible factors that are mentioned in their paper that could affect the structure of these workflows consist of:

- The type and level of security required for the 3D printer, such as physical, network, or data security
- The type and complexity of the 3D printer, such as desktop, industrial, or bioprinter
- The type and availability of the input and output data, such as audio, video, or code
- The type and capability of the security tools and frameworks, such as National Institute of Standards and Technology (NIST) Risk Management Framework (RMF), NIST Cybersecurity Framework (CSF), or AM Security Taxonomy

Additionally, the architecture of any of these respective networks will dictate the size of these workflows, which only contributes to the risk factor. In Figure 2.2, the example of a workflow concerning a metal printer provided as a service can be broken down to emphasize all the factors that must come together to ensure the data can reach the printer [3].

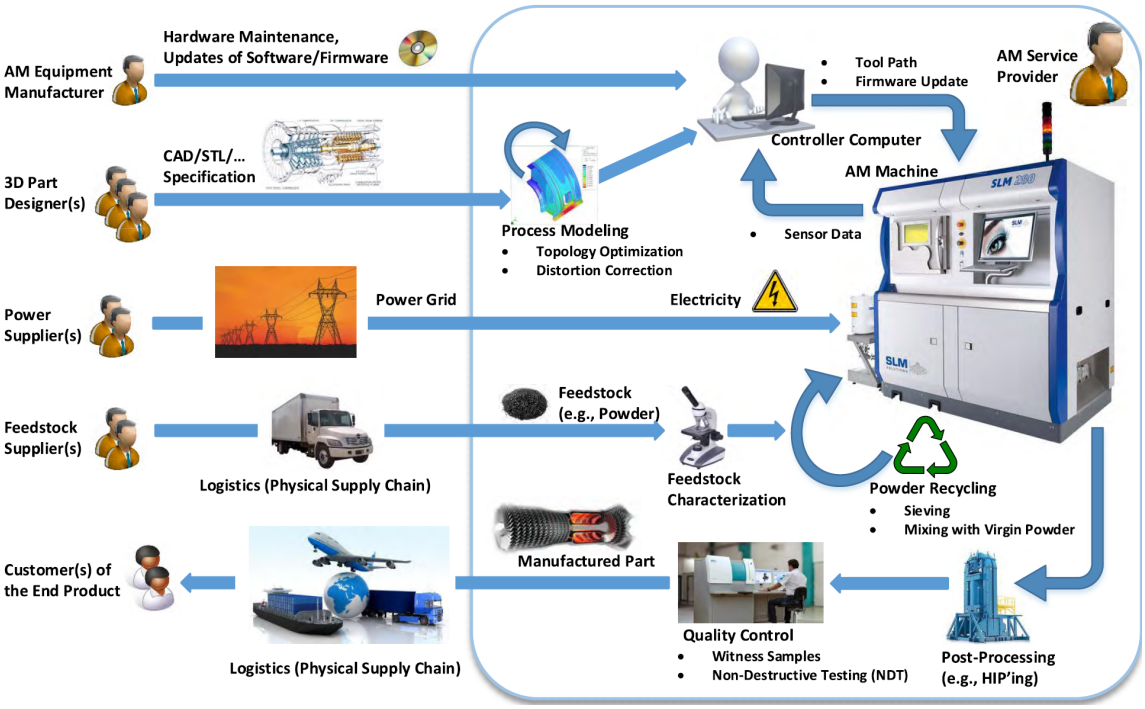

Figure 2.2. AM Workflow, from Design, Supply, to Production. Source: [3, figure 2].

Such a complex design can be highly susceptible to numerous attacks, and the challenge is compounded when additional features are introduced. The fragility of this intricate network becomes even more pronounced as the failure of a single link in the chain jeopardizes the overall stability of the entire system, posing a significant risk. Figure 2.2 represents just one of the numerous examples detailed by Graves et al. [3], underscoring their focus on illuminating potential attack vectors that could be employed against additive manufacturing security systems. To summarize their analysis, an attack against an AM system falls into one of three categories: technical data theft, sabotage, and illegal part manufacturing [3].

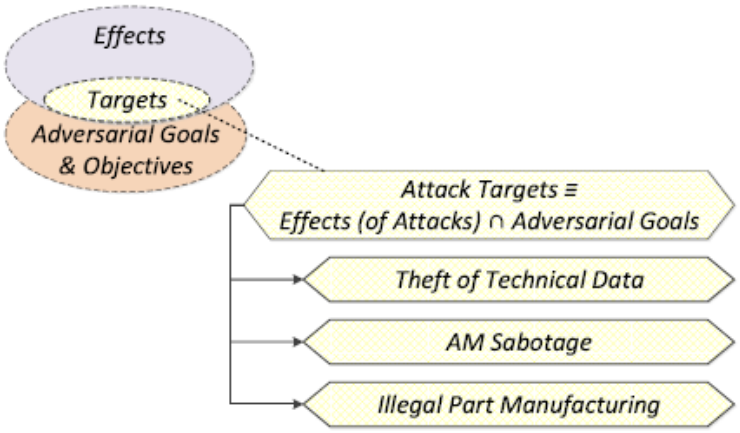

Figure 2.3. Attack Analysis Framework. Source: [3, figure 4].

While each threat vector might aim to achieve a different goal, the means of accessing them in the cyber domain are similar. Should an adversary exploit a user, acquire access somewhere in the network, infect the data, etc., any equipment existing on the chain can be compromised in addition to any AM data [5].

2.3 Additive Manufacturing Data Transfer Methods and Security Concerns

There are various methods and technologies for transferring AM data between different devices and systems, each with its own advantages and disadvantages. The choice of the method depends on the security, complexity, and availability of the AM data and the AM devices. For example, some of the existing practices include the use of external storage, encrypted email, cloud storage, or blockchain. However, as this chapter will show, no standard or uniform method for AM data transmission suits all scenarios and institutions. Different organizations may adopt different approaches according to their needs and preferences. Moreover, many transfer methods used in existing technology can be translated to the AM field, but they also come with complications that may not be tolerable by some.

2.3.1 External Storage

External storage devices, such as Universal Serial Bus (USB)s, Secure Digital (SD) cards, and Compact Disks (CD)s, can pose serious security, reliability, and compatibility issues for data transmission, as they can introduce malware, tamper with data, or leak sensitive information, and they are not usually regulated or standardized across different institutions and systems [6]. DOD Instruction 8170.01, Online Information Management and Electronic Messaging, discusses the security challenges and risks of using these external devices for data transmission within the DOD [7]. In higher-security settings, such devices are frequently prohibited due to the inherent ease with which malware can be distributed, posing a threat to system integrity. Additionally, these devices are highly susceptible to loss or theft. Nevertheless, despite these concerns, this method remains widely used across various sectors, including industry, the business world, and within the DOD [8].

AM data also suffers the same risk as any other form of data transferred through external storage devices. Different institutions may have their own policies and practices for AM data security, some of which may include the use of external devices. Therefore, external devices can pose severe threats to the quality and integrity of the AM products should they fall victim to their shortcomings. Unfortunately, the fact is that too many external storage devices do not run antivirus software, are not set up to scan USB drives, or are not set to disallow autorun when a USB or SD is in use. An infected flash drive plugged into an unprotected device could instantly infect the printer and spread a virus through any connected network [9]. The desired end state is to ban external storage in many security policies to help secure valuable AM data. Still, a more convenient/efficient practice has yet to be introduced to remove this process altogether [10].

2.3.2 Encrypted Email

In various environments, encrypted emails are a straightforward, user-friendly, and cost-effective approach for transmitting data via email. Incorporating encryption or password protection adds a layer of security, reinforcing the confidentiality and privacy of the transmitted data [11]. Unfortunately, there is still the matter of maintenance and assuring that whoever handles this information on each end is the person the information is intended for. While not an entirely terrible option, it still holds some risk and does not present the highest option of security desired by many industries.

One example of this is presented in a paper titled, *Protecting Additive Manufacturing Information When Encryption is Insufficient*, by J. Lubell, who dives into side-channel attacks and their specific impact on AM data [12]. In that research, the author discusses how side-channel attacks on a 3D printing workflow can bypass email encryption to acquire the contents of any data files. These attacks are leakages of non-digital information that consist of time measurement, power usage, or electromagnetic radiation. When applied to AM, an attacker can access the relevant printer's motors through the G-code and reverse engineer the parts(s) as desired. Though considered a more sophisticated method of attack, this emphasizes that relying solely on encrypted email should not be the cornerstone when aiming for secure AM data transfers [12].

2.3.3 Cloud-Based Systems

In terms of how the cloud relates to AM security, Haghnegahdar et al. [13] provides an overview of a standard cloud-based model and concept of Cloud Computing (CC), Cloud Manufacturing (CM), and the Internet of Things (IoT), along with their relations and influences in "the AM industry 4.0 era." AM technology that utilizes a cloud service certainly provides an incredibly convenient method of exchange, but unfortunately, convenience does not make up for higher security concerns. Cloud-based systems can achieve a flexible way of dealing with digital threads, which are the frameworks of communication that allow for a connected data flow throughout the product life cycle. By using cloud-based systems, this technology can be integrated into an Industrial Internet of Things (IIoT) design, which is the network of smart devices, machines (i.e, 3D printers), and systems that collect, analyze, and exchange data via the internet [12]. However, this integration is only limited to the scope of the industries willing to use cloud-based systems, as there may be some challenges and barriers to adopting this technology, such as scalability, performance, security, and cost.

The leading concerns about this practice centers around compliance and complexity. There is no globalized method for properly distributing AM data across the cloud, which can cause conflicts between organizations and regions with differing regulations and requirements.

For example, the size, format, and resolution of the data files used or generated in AM may not meet the security standards and expectations of all the parties involved. Additionally, updates and changes in any implemented AM software would require all parties involved to comply simultaneously. This becomes much less manageable the larger any cloud architecture becomes and causes strain on any existing security practices [13].

In terms of complexity, the research explains that the cloud is generally designed to support small to medium-sized chunks of data in transit. AM data can range in many sizes but also consists of multiple steps that ensure the information is sent in the correct order and is compatible with the respective technology. Increasing the number of steps needed to send any data in its desired form consequently increases the risks of a breach in the transfer. The diverse nature of this data and associated systems cause great difficulty in establishing any normalized security plan across industries [13].

Regarding utilizing the cloud for AM in a maritime context, there are notable advantages, such as enhanced efficiency, improved performance, cost-effectiveness, and increased convenience in data transmission, storage, and analysis [14]. However, incorporating cloud-based solutions also introduce unique challenges, primarily centered around susceptibility to malicious activity and connectivity issues. Cloud technologies can expose data to unauthorized access, potential modification, or theft by hackers, malware, or other malicious entities. Additionally, reliance on cloud-based technologies may lead to errors, corruption, or data loss due to network connectivity, bandwidth limitations, or storage constraints. These challenges compound the complexities highlighted by Haghnegahdar et al., underscoring that the cloud may not be the optimal choice for securing data in a maritime setting, let alone AM data [14].

2.3.4 Network Security Concerns

Implementing a 3D printer into a network can pose significant problems, in addition to the security concerns for AM data in transit. For convenience, making the printer an IoT device would be ideal to expedite the data transfer process. However, this also exposes the printer and the network to cyberattacks, such as malware, denial-of-service, or data theft. Moreover, the existing software architecture for these 3D printers is not standardized or compatible, which can increase the risk of errors, corruption, or data loss [15]. Research conducted by WatchGuard Technologies utilized a program called OctoPrint to serve as a network printing host for a small recreational printer. The open-source, Linux-based program was meant to run on a Raspberry Pi and allowed remote access to the 3D printer. All ranges of printers could use this software, but once that printer was connected to the network, any flaws existing within the equipment would also be exposed to the world [15].

The experiment examined what would happen if someone could access the OctoPrint setup. To validate this concept, an external actor was explicitly designated to employ a file exploit, initiating remote printing with a malicious file. This action exposed vulnerabilities in the printer, enabling the execution of the malicious code over the network. In summary, the experiment highlighted that the extent of its network access directly influences the printer's exposure. To address this issue, the solution involved implementing a Virtual Private Network (VPN) and/or utilizing additional authentication practices, especially if the priority was to enable printing over the internet. However, the ultimate recommendation was to avoid directly connecting any 3D printer to a network connected to the internet unless the user or company is confident in the equipment's ability to operate safely as an IoT device [15]. IoT devices can offer many benefits, such as convenience, efficiency, and automation, but they also pose many security challenges, such as data privacy, device integrity, and network resilience. Therefore, users and companies should carefully assess the risks and benefits of using IoT devices, like 3D printers, should they consider implementing them into their networks.

2.4 Blockchain

As briefly mentioned in Chapter 1, blockchain is a decentralized and distributed ledger technology that revolutionizes record-keeping by creating an integrity-protected and transparent transaction system. In a blockchain, data is organized into blocks, each containing a list of transactions, and these blocks are linked together to form a chain. The use of cryptographic hashing ensures the integrity of each block, making it resistant to tampering. Blockchain is based on the idea of decentralization, meaning that there are multiple copies of the same data stored on different nodes in a network. To ensure that the data is consistent and valid, the nodes use consensus mechanisms, such as Proof of Work (PoW), to agree on the state of the data and reject any fraudulent transactions [16]. The data is organized in blocks linked together in a chain, and each block is practically impossible to change once it is added to the chain, creating trust in the system. Some blockchains also have smart contracts, which are agreements that are written in code and executed automatically when certain conditions are met, adding functionality to the system. Blockchains can be public, meaning that anyone can join and participate, or private, meaning only a specific group can access and use them [1]. Figure 2.4 presents a visual synopsis of how blockchains work.

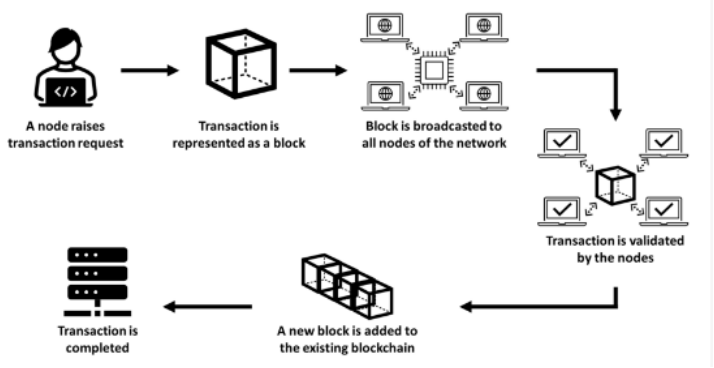

Figure 2.4. General Blockchain Flow. Source: [17, figure 1].

2.4.1 Moog and Supply Chains

Blockchain technology has the potential to offer many benefits for AM, such as enhancing the security, transparency, and traceability of AM data and products. However, there are few real-world examples of how blockchain is used with AM to help determine its feasibility in the professional sector. One company that has explored this possibility is Moog, an aircraft precision part manufacturer based in New York, NY.

In the research of [18], the authors aimed to create a blockchain platform their customers could use to exchange "value," which included metrics such as the number of IP exchanges and the number of downloaded AM schematics, among other features [18]. Additionally, they emphasized that establishing trust with their customers would be paramount for their vision to work. The problems they encountered are synonymous with a cloud-focused technique, ensuring the companies they chose to work with could maintain compatibility with multiple systems. The authors proposed a system reliant on real-time data exchange among multiple parties, a strategy susceptible to potential performance issues during large-scale disruptions in connectivity. Notably, their assumptions about the size of exchanged data imply an expectation of manageable bandwidth strain [18]. Moog is still in the early stages of developing its blockchain platform, but the company is excited about the potential of the technology to improve its supply chain and believes that the platform will help to reduce costs, improve efficiency, and enhance security.

Their proposal aims to leverage blockchain technology for tracking part provenance across the supply chain [18]. This approach ensures the authenticity of parts and guards against counterfeiting. The implementation of blockchain technology not only enhances visibility into the supply chain but also facilitates quicker identification and resolution of issues. While the analysis provides insights into how blockchain could securely manage AM data, it is essential to recognize that collaborating with multiple companies across the industry spectrum introduces additional complexities. The customers using this platform are pre-authenticated and, therefore, trusted parties on the platform. In a situation involving numerous peers, the transactions between Moog and its customers are meant to encompass signatures from each endorsing peer on the ledger. As CAD data and manufacturing information undergo updates within Moog, the smart contract seamlessly incorporates the most recent version of the data through the signatures distributed throughout the model [18].

2.4.2 Blockchain Mergence

Previous work with blockchain has shown that it is possible to share information across several parties who also possess the ability to update the contents, i.e. Blockchain Mergence [19]. As long as the respective personnel have a need-to-know authorization, it is possible to update an item's history throughout the transaction period.

The problem that Blockchain Mergence [19] aims to solve is how to manage and update item records within a supply chain using blockchain technology, particularly in scenarios where items undergo changes throughout their life cycle and offer a method of distributed decentralized trust. The concept of Blockchain Mergence comprises two key components: 1) the convergence of "internal" and "external" chains and 2) the distinction between local and global internal tracking chains, where the global constitutes a blockchain and the local chain is a more efficient signature chain [19]. The former emphasizes flexibility in adapting to potential variations in external supply chain tracking and accommodating diverse classification levels within the DOD. It advocates for the use of one or more internal blockchains to fulfill these needs, with operations such as device registration, repair, split, and combine authenticated through the Public Key Infrastructure (PKI) inherent in the Depot Level Repair (DLR) system. The discussion extends to multilevel security classification considerations, demonstrating how blockchain mergence supports activities across various security levels, with the term "chain" explicitly referring to a blockchain.

The latter concept revolves around the device chain, managing immediate time history and supporting operations like registration, repair, split, and combining to ensure precise device history and modifications [19]. Authentication relies on the DOD PKI, and this record uses digital signatures to authenticate device operations, ensuring documentation of authorized changes to components.

Multilevel security considerations enable the global blockchains to operate at different classification levels, fostering interoperability across security domains [19]. Collectively, these tracking chains significantly enhance accountability and flexibility in both the supply chain and device management processes.

To help demonstrate the second concept, the research team developed a DOD scenario where a ship required Unmanned Aerial Vehicle (UAV) assistance. It hinges on a ship deploying two UAVs, each possessing unique capabilities yet sharing fundamental functionalities. During a test flight, an unfortunate collision occurs between the two UAVs, leaving both vehicles with varying degrees of damage. The scenario illustrates a test flight where two UAVs, UAV1 and UAV2, experience a collision. The broken device would then have a device split operation in its item record, creating two new local chains: one for the component that will be reused and one for the remaining unusable assembly UAV1. *Combine* and *split* operations then allow integrating the component into UAV2. As such, the local item history of UAV1 is now linked to UAV2, which can then be logged globally on the blockchain. If there were relevant repairs to the reused component or if it comes to light that the reused component was compromised during manufacture and must be pulled from use, it will be immediately apparent from UAV2's record history that the part now resides within UAV2 instead of the UAV1 device carcass [19]. This vividly demonstrates the transformative potential of blockchain technology to revolutionize resupply and modification efforts within the fleet while safeguarding the integrity and security of sensitive information.

Every transaction between parties in this scenario must be authenticated. For this, Blockchain Mergence uses PKI already inherent in the DLR system. In the local chain, the operator responsible for the device signs the various operations, and the signature covers the current record for the device(s) being operated on and what type of operation is performed. Periodically, the authenticated transcript is then stored as part of the device record on the global blockchain. This is shown in Figure 2.5. The scenario introduces a key operational element termed a "device split operation," wherein two distinct UAVs, each with unique specifications, undergo operations recorded to their respective local chains. It is imperative to clarify that while the term "chain" is employed, the local chain deviates from a traditional blockchain, providing authentication through digital signatures using PKI vs through a distributed blockchain. In this difference, it is able to function as a flexible and efficient mechanism for tacking device-related operations in contexts where the consensus of device history is not needed until a later time (for which the global chain is used). Each operation performed on either UAV is meticulously synchronized with the corresponding local chain, effectively linking the item histories on a shared, immutable ledger. Any action undertaken on the component mandates the operator's signature and is subsequently stored as an in-

tegral part of the relevant local chain [19]. Figure 2.5 aptly illustrates the research team's envisioned process for this intricate procedure.

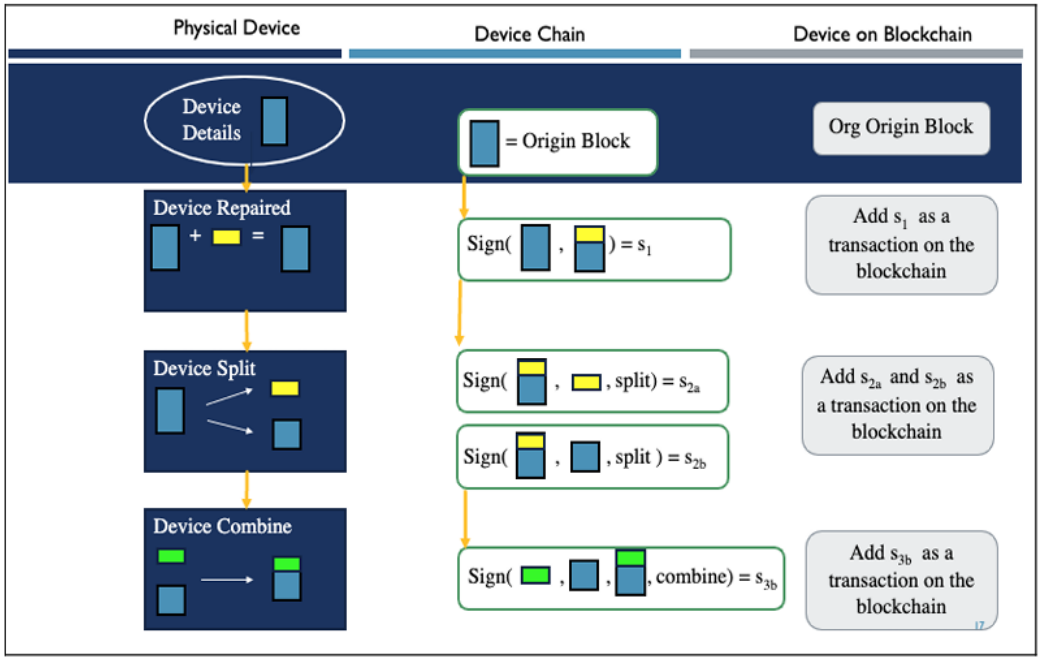

Figure 2.5. Sequencing Operations for Blockchain Mergence, local component (*Device Chain*) and global component (*Device on Blockchain*). Source: [19, figure 3].

While the presented research offers valuable insight into integrating parts and modifications onto a unified blockchain, its applicability remains confined to existing systems [19]. The outlined future work emphasizes incorporating Common Access Card (CAC) infrastructure into this process, an avenue that this thesis will delve into.

2.4.3 Project Hivemind

Other work with blockchain that is specifically linked to AM can be referenced to a project called Project Hivemind [20]. This solution utilizes a distributed ledger to establish and manage the AM Technical Work Package (TWP) repository. This repository serves as a comprehensive storehouse for part geometry, AM system settings, and approval information, encompassing the entirety of AM data in transit. Implementing a distributed ledger ensures the repository's tamper-proof nature and restricts access to authorized users [20].

Furthermore, the project introduces off-chain storage to optimize the handling of extensive data on the blockchain. Rather than storing the complete part data on the blockchain, this approach involves off-chain storage with reference pointers to pertinent data. This strategic choice enables the blockchain to validate data received through alternative means and allows for the referencing of smaller, separate blockchains, downloaded as needed and when bandwidth is available [20]. Further exploration of this research will be discussed later in Chapter B.3.

2.4.4 Summary of Varied Blockchain Approaches

The three aforementioned blockchain projects embrace the decentralized and distributed ledger technology inherent in blockchain, deploying it in unique ways aligned with their own distinct objectives. To encapsulate, Moog directs its attention toward overarching improvements in supply chain operations and the meticulous tracking of part provenance in a real-time setting. Meanwhile, Blockchain Mergence prioritizes security and effective management onboard ships even when a blockchain is unreachable, allowing for real-time authentication item records. In contrast, Project Hivemind takes on the task of fortifying AM settings and data security by employing a distributed ledger accompanied by innovative off-chain storage solutions. Each of these projects unfolds as a testament to its individualized strategies, meticulously crafted to address specific goals and challenges in the integration of blockchain technology with AM and supply chain processes.

2.5 Network Connectivity

Implementing a 3D printer into a network can pose significant problems, in addition to the security concerns for AM data in transit. For convenience, making the printer an IoT device would be ideal to expedite the data transfer process. However, this also exposes the printer and the network to cyberattacks, such as malware, denial-of-service, or data theft. Moreover, the existing software architecture for these 3D printers is not standardized or compatible, which can increase the risk of errors, corruption, or data loss [15]. Research conducted by WatchGuard Technologies utilized a program called OctoPrint to serve as a network printing host for a small recreational printer. The open-source, Linux-based program was meant to run on a Raspberry Pi and allowed remote access to the 3D printer. All ranges of printers could use this software, but once that printer was connected to the network, any flaws existing within the equipment would also be exposed to the world [15].

The experiment examined what would happen if someone could access the OctoPrint setup. To validate this concept, an external actor was explicitly designated to employ a file exploit, initiating remote printing with a malicious file. This action exposed vulnerabilities in the printer, enabling the execution of the malicious code over the network. In summary, the experiment highlighted that the extent of its network access directly influences the printer's exposure. To address this issue, the solution involved implementing a VPN and/or utilizing additional authentication practices, especially if the priority was to enable printing over the internet. However, the ultimate recommendation was to avoid directly connecting any 3D printer to a network connected to the internet unless the user or company is confident in the equipment's ability to operate safely as an IoT device [15]. IoT devices can offer many benefits, such as convenience, efficiency, and automation, but they also pose many security challenges, such as data privacy, device integrity, and network resilience. Therefore, users and companies should carefully assess the risks and benefits of using IoT devices, like 3D printers, should they consider implementing them into their networks.

2.6 Related Security Experiments

The following information in this section will indicate a scarcity of documented experiments concerning AM security. Nevertheless, the ensuing two experiments meticulously outline the thought process, implementation, and results, providing a deeper understanding of the options available to an attacker seeking to compromise this data.

2.6.1 The Fill Experiment

Among some existing studies, Straub [21] has endeavored to illustrate that while conventional security measures like encryption and firewalls maintain their value in AM security, the security of the 3D-printed schematic remains vulnerable in transit to its destination. The number of checkpoints that AM data must go through promotes too many opportunities to introduce defects that are difficult to prevent by normal means. To prove this, an experiment was conducted to sabotage 3D-printed objects by manipulating the fill level while the part data was in transit. The fill level refers to the amount of material used to fill the interior of the printed object, determining its structural integrity. Manipulating the fill level during transit in the experiment suggests an attempt to introduce defects or compromise the internal structure of the 3D-printed objects. To the naked eye, a slight change in the fill level presented no apparent discrepancies, but a minor alteration to the fill level settings proved sufficient to induce a malfunction in the 3D-printed object [21]. Unfortunately, the cybersecurity implications of the Fill Experiment were the focus of that work in comparison to the emphasis placed on quality assurance techniques. Straub suggested that the data of a 3D schematic should be verified in transit, meaning that it should be checked for any tampering or modification while it is being transferred from the computer to the 3D printer. This would prevent the attacker from modifying the data after it has been verified, and that is where the fill level defect could be detected and prevented [21]. The research did not specify how the verification data would be transmitted or stored or how it would be paired with the original data. It also did not test this idea in experimentation and left it for future work. Therefore, his proposal of verification in transit, referenced in Figure 2.6, remains a theoretical concept that needs further exploration and validation.

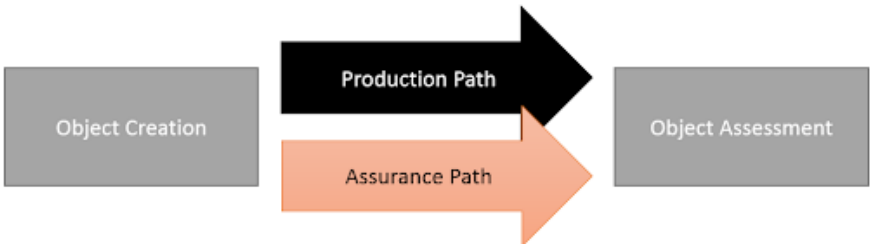

Figure 2.6. Dual Path Concept. Source: [21, figure 3].

While this redundancy method offers a possible approach for data verification, it also poses specific challenges. Firstly, the reliability and accuracy of verification data may not be consistent enough to identify subtle or intricate defects in AM data, such as geometric deviations. Redundancy pathways also do not guarantee data authenticity. Additionally, incorporating AM data into the verification process could introduce latency or bandwidth constraints, potentially diverting attention away from the core concepts of the Fill Experiment [22].

2.6.2 The dr0wned Experiment

In Section 2.2, Graves et al. provided valuable insights into the primary threat vectors that pose challenges to AM security [3]. However, despite these insights, very few experiments cover an entire AM workflow to identify how attacks can be inserted into the process. One such sabotage experiment, named dr0wned [5], was conducted, forming a case study that details how something as seemingly simple as a home user on their laptop with a personal 3D printer could be at risk.

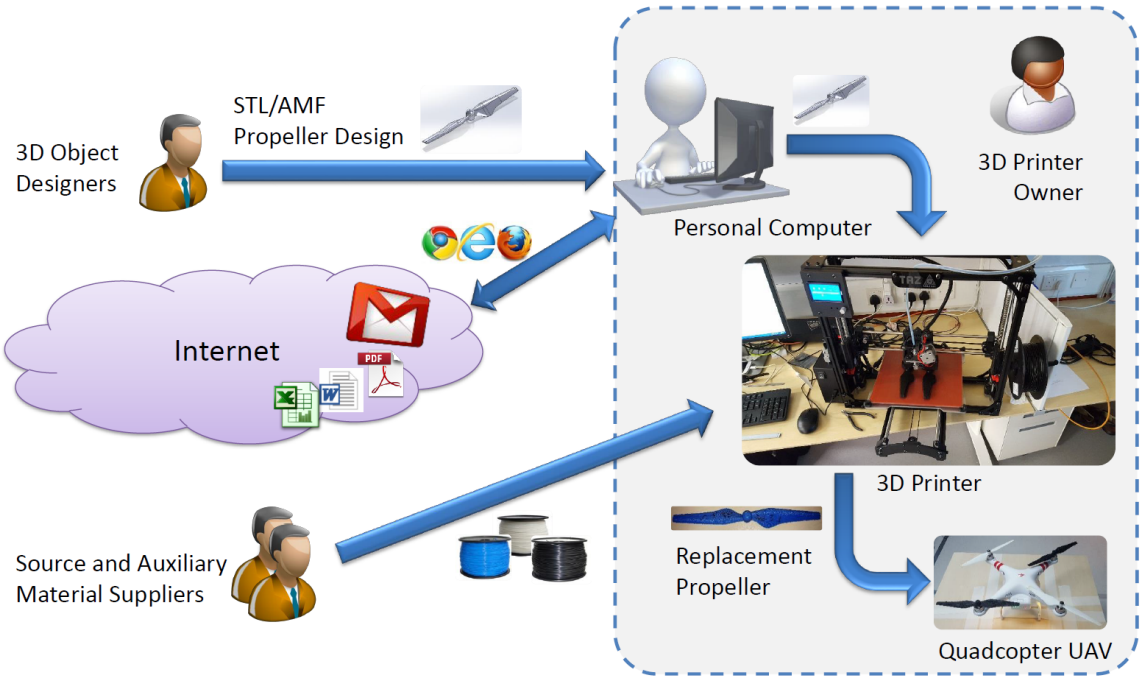

Figure 2.7. UAV Experiment Scenario. Source: [5, figure 7].

As seen in Figure 2.7, the sabotaged mechanism of choice was a recreational UAV. The group took the approach first from the attacker's point of view to alter the propeller of the UAV in such a way that would not be noticeable until the equipment had to rely on it in stressful situations. This assumed that the hacker had basic to slightly higher-than-average hacking skills. The attack of choice in this experiment was a phishing email that enticed the user into opening the attached file. Once this was done, the attacker could open a reverse shell, take control of the user's workstation, and manipulate the AM data as desired.

Field trials compared the performance of the UAV before and after the attack under identical conditions and indicated a successful attack. Though this is just one experiment conducted at a more superficial level, the critical takeaway is seeing how an attacker looks at the entire AM workflow to plan and decide which attack vector to act upon in more complex systems [5].

2.7 Summary

Overall, the point of exploring this background is to demonstrate the expansive and complex nature of AM workflows, how every design can be susceptible to different attack vectors, the need for solid security, and the possible tools available. It also hints at how AM security in the USN and DOD might be afflicted by the many existing complications, which will be explored in the following chapters. The experiments explored in this chapter build the foundation for this thesis that leverages and expands upon any existing ideas or unfinished thoughts from these prior works.

CHAPTER 3:
USN Application

The U.S. Navy has made significant efforts to integrate AM systems into a wide array of assets, including ships, aircraft, and support equipment, to fully embrace and capitalize on the innovative capabilities of 3D printing. This includes installing maker spaces onboard ships throughout the fleet. The first ship to receive such an upgrade was the USS Essex (LHD-2) in 2014 [23]. Over ten ships have since been outfitted to support AM capabilities [23]. While many printers have come and gone in this ongoing integration attempt, some of the most notable printer models that are currently installed on some of these ships consist of the XEROX ElemX, Markforged X7, Phillips Hybrid, and Stratasys F900 [24]. Each printer is outfitted with USB and network capability, and managing both features ultimately falls back on the Navy to ensure that proper security practices are in place to protect their AM data and equipment. Frequently, these printers are either hard-wired into the ship's network or act as a standalone system in which the data is brought directly to the source. While the current processes of transferring AM data have sufficed, multiple concerns must be addressed to achieve the desired level of security in these systems.

There are two primary branches in the Navy with notable existing AM policies. The surface forces, NAVSEA, and air forces, Naval Air Systems Command (NAVAIR), both seek to use AM to accommodate their specific mission set. Despite their distinct focuses, striking similarities exist in the current security implementations, allowing for seamless cross-referencing between the two. This chapter elucidates the current protocols governing the handling of AM data in the USN, shedding light on ongoing projects that aim to propel advancements in addressing associated challenges.

3.1 The NAVSEA Process

As it stands, there is no fully established uniformity across the Fleet regarding what the primary AM policy should be. In the case of NAVSEA, any applications to be used in a ship's AM workflow are to be electronically submitted by the ship's crew to a separate AM team off-ship via email for approved use. Any activity is logged for future analysis if this cannot be accomplished at sea. At this point, a submitter would begin developing the part information and building what is known as a Technical Data Package (TDP), shown in Figure 3.1.

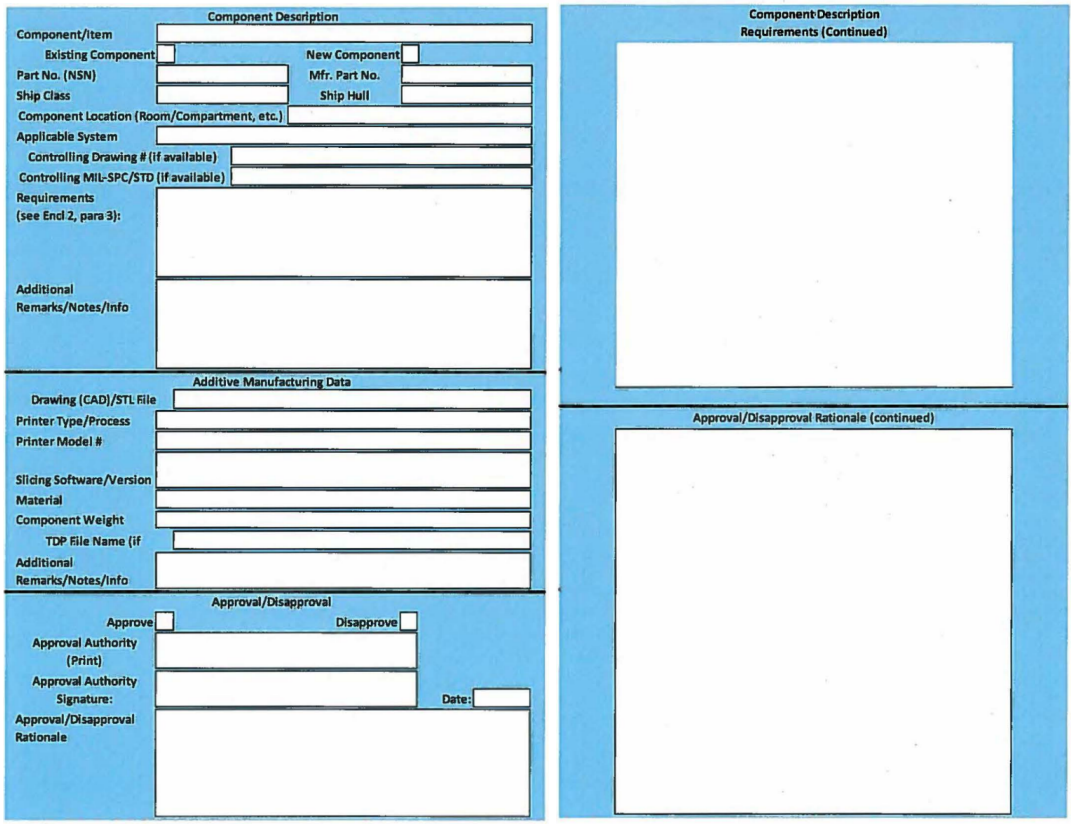

Figure 3.1. NAVSEA AM Technical Data Package. Source: [25, Figures E-3 and E-4]. TDPs are meant to contain critical information such as national stock numbers, STL files, printer settings, severity, etc. They are broken up into 5 blocks covering Component Description, AM Data, Approval/Disapproval, Component Description Requirements, and Approval/Disapproval Rationale.

These TDPs are meant to contain critical information such as national stock numbers, STL files, printer settings, severity, etc. They are broken up into 5 blocks to ensure the submitter includes all of the required information:

- Block 1: Component Description
  - Includes stock number, ship class, hull number, location of 3D printer, part requirements, etc.
- Block 2: AM Data
  - Includes STL file name, 3D printer model details, software version, etc.
- Block 3: Approval/Disapproval
  - Includes details on approval authority, their signature, date, and rational
- Block 4: Component Description Requirements
- Block 5: Approval/Disapproval Rationale

The severity level is perhaps the most crucial feature of the TDP. The submitter must assess the severity of the requested part based on a scale of 1 to 7 [25]. An adaptation of these severity levels can be seen in Table 3.1.

Table 3.1. NAVSEA AM Severity Levels. Adapted from [25, Table 5]

Severity Level	Severity Description
1-3	CVN Loss, Ship Loss, and Catastrophic
4	Critical
5-6	Significant and Marginal. Applications may include temporary installation of an AM component with monitoring required.
7 and N/A	Negligible severity. This may include the temporary installation of an AM component with monitoring required.

For all jobs labeled with a severity of 7 or N/A, a TDP is not required and only needs the approval of the ship's authority. For all levels below 7, it is required that the ship's submitter and approving officer collaborate with the owner/sponsor of the component in question to ensure that specifications are correct before submission. This collaboration might also

entail talks of making improvements to the parts in question via other printing methods. The last step before send-off requires one last round of risk assessment from all parties; at this point, the TDP is sent to the approving officer. However, in addition to shipboard approval, TDPs with a significant or greater severity level also require off-ship approval at NAVSEA AM Command and Control (C2) from a Technical Work Holder (TWH) or Chief Engineer (CHENG). Once approved onboard, the TDP is sent to a separate NAVSEA AM team for final approval before printing begins. This entire exchange of forms and data is conducted entirely through email. Certainly, this brings up a cause for concern regarding ensuring the security of the information being used. Figure 3.2 illustrates how this process is meant to be handled [25].

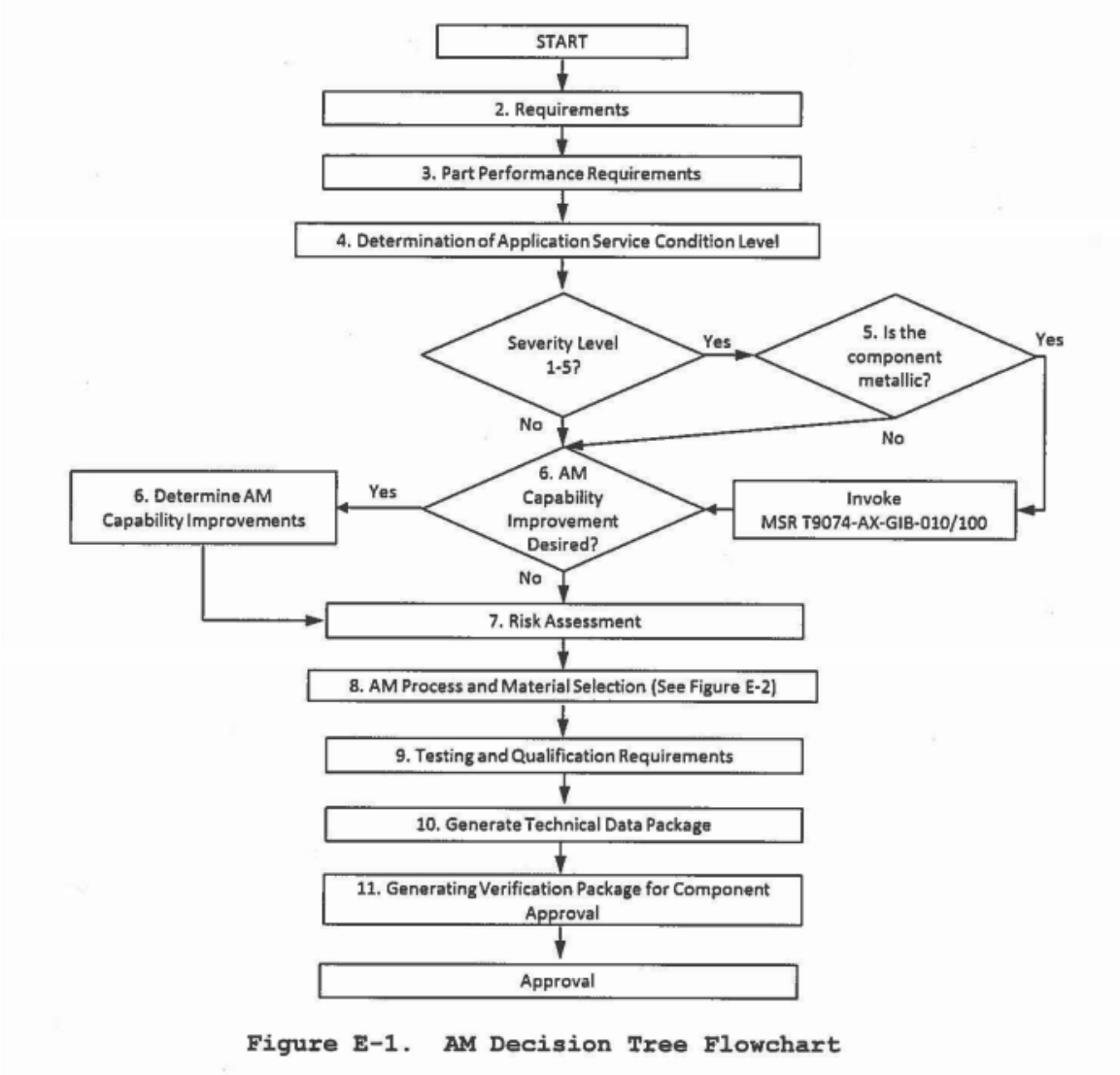

Figure 3.2. NAVSEA AM Decision Tree Flowchart. Source: [25, figure E-1].

Security measures for the utilization of AM components must be clearly outlined and recorded within the TDP [25]. In this context, the submitter or designated technical expert is responsible for identifying and documenting any pertinent security restrictions associated with the AM part. This encompasses considerations such as Controlled Unclassified Information (CUI) or adherence to export control regulations. The TDP, being the primary repository of information for manufacturing and inspecting these AM parts, must comprehensively capture these identified security restrictions.

Moreover, the submitter or designated technical expert ensures that the AM process and subsequent post-processing procedures are free from potential security vulnerabilities [25]. This necessitates taking precautionary measures to prevent the introduction of security risks, such as the use of materials susceptible to unauthorized access or modification.

Lastly, the CHENG plays a critical role in overseeing the security aspects of AM components [25]. The CHENG, or any other designated approval authority, is responsible for reviewing and approving the security restrictions and procedures. This involves collaboration with relevant stakeholders to ensure comprehensive input and alignment with security protocols. Once approved, these security measures are formally documented in the TDP and rigorously implemented throughout the manufacturing and inspection processes.

3.2 The NAVAIR Process

The NAVAIR process, illustrated in Figure 3.3, is highly similar to the process used by NAVSEA. However, the written instruction provides differing definitions and slightly more detailed steps. The submitter is required to collaborate with the NAVAIR AM Support Team for the development and submission of a TDP, irrespective of its classification level. Additionally, four specified methods are outlined for the submitter to employ when seeking approval.

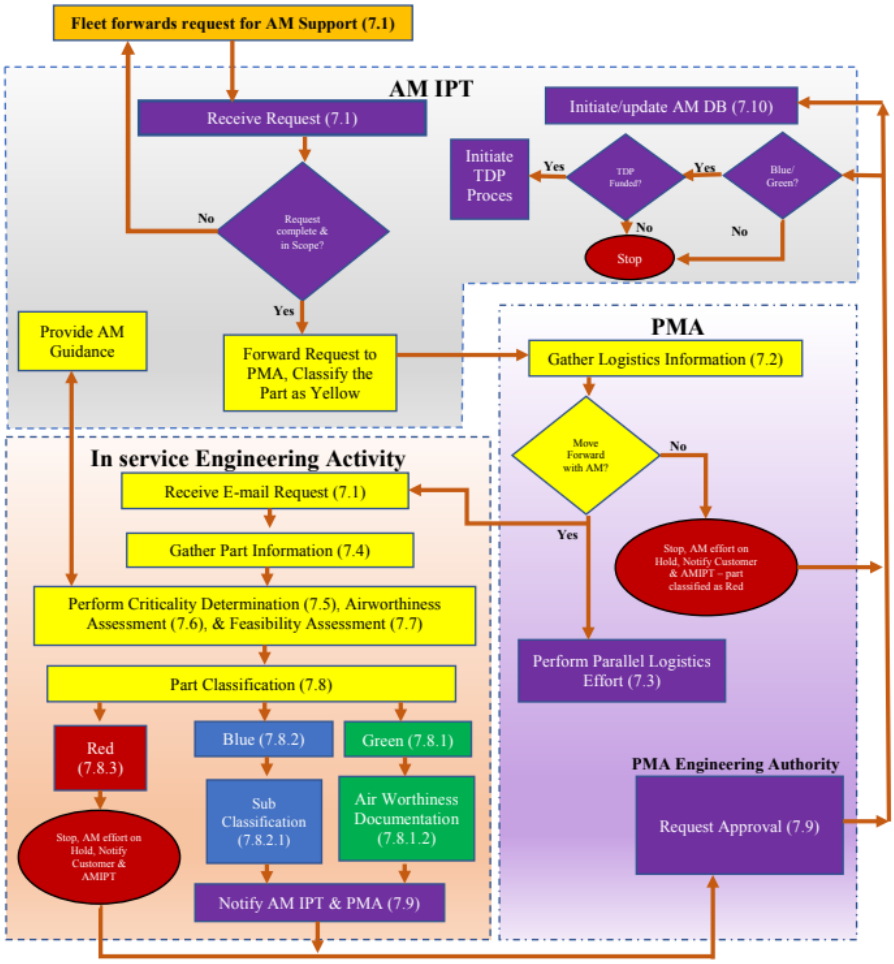

Figure 3.3. Part Approval and Classification Workflow. Source: [26, figure 1].

The initial approach entails sending a direct email to the onshore NAVAIR AM Integrated Product Team (IPT). The second method involves constructing and submitting requests through the Joint Technical Data Integration (JTDI) website. This is one outlet the USN uses to incorporate a centralized database into Navy AM, where several requests and previously approved part information can be stored. To use the latter, users must first gain access via a CAC and then request an account from the website administrators before accessing the request forms and other essential AM information. The third method involves direct customer support, known as In-Service Support Activity (ISSA), typically with the original

component manufacturer. All collaborations at this level are then forwarded to the AM IPT. The final method involves direct emails or phone calls to NAVAIR shore command for support. When all this information is assembled, a qualified Cognizant Engineer classifies the data as either red, blue, or green before stamping their approval and submitting the TDP to a NAVAIR Program Manager for final approval. All approved requests are then uploaded to the JTDI for future reference and fleet availability [26].

3.2.1 Network Infrastructure

When placing these printers onboard USN ships, the consensus seems to be that a non-networked system is preferable. Confining the equipment to their maker spaces or an entirely isolated network area on the ship has been the standard practice. However, previously mentioned practices, such as emails and JTDI, must still be conducted through the ship's network and, therefore, the Internet. Since the USN is not fully prepared to implement these printers into the network, transferring data directly to the printer via a USB drive or SD card is considered standard procedure once the data is approved.

The eventual goal is to find a way to integrate this technology into the ship's network safely and avoid depending on external storage while protecting these systems against the dangers of the internet. The USN has already been working to improve this process. In November of 2022, the USS Bataan (LHD-5) installed a Phillips Additive Hybrid printer with Computer Numerical Control (CNC) to test for a thriving environment in which a secure, streamlined AM workflow process could be accomplished [24]. CNC in 3D printers is not a security but a precision feature that mainly utilizes Subtractive Manufacturing (SM), or removing material from a block of material until the desired 3D object is printed. This functionality is more prominent in advanced printers that intricately engage with G-code, distinguishing them from other printers in precision and control [27].

The installation marked a significant milestone as it represented one of the earliest documented instances of a Digital Manufacturing Environment/Ecosystem (DME) – a term denoting a secure network boundary designed to segregate AM equipment and workstations from the host network. In practical terms, this arrangement ensured the isolation of AM data and files from the broader ship's network, protecting against unauthorized access and potential cyberattacks [28]. Before its implementation, a model testing phase conducted

by NAVSEA on shore validated the efficacy of this approach. Subsequently, upon integration onboard, a "secure connection" [24] was successfully established between the ship's Consolidated Afloat Networks and Enterprise Services (CANES) network and all assets supporting the AM equipment (details of the connection are not available). The DME could provide a scalable, proof-of-concept secure network boundary that separates the equipment and workstations from the host network. Its effectiveness remains to be seen, but this has not shown significant signs of failure in the Fleet [24].

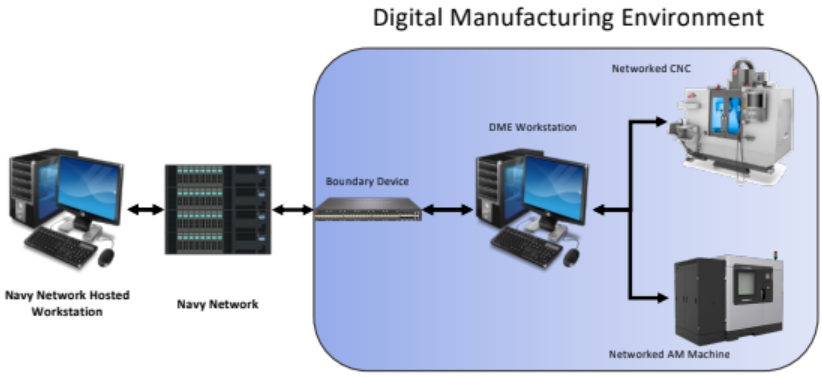

Figure 3.4. USS Bataan DME Design. Source: [29].

3.2.2 Innovations at NIWC Pacific

Experiments have been in the works at facilities such as Naval Information Warfare Command Pacific (NIWC PAC), focused on optimizing the AM workflow within the Fleet. At NIWC PAC, the Digital Advanced Manufacturing Ecosystem (DAME) team has been actively developing applications, including SecurePrint [29], to make significant contributions to the ongoing efforts in enhancing AM security.

In the prototype model, SecurePrint 1.0 [29], the purpose of the application was to encrypt cleartext AM traffic by tunneling the unsecured data over port 22, thereby encrypting all traffic over the wire to and from the connected printer. The DAME team used an Ultimaker S5 [30] and Stratasys F900 [31] as the test subjects and ensured that both printers were patched up-to-date before using the command line to run the application [29]. SecurePrint operates by implementing a series of security measures, commonly referred to as hardening steps [29]:

- Update binaries
- Change default passwords to randomized passwords
- Remove root access to the device
- Apply configuration changes (Security Technical Implementation Guide (STIG)s) and industry-specific configurations
- Establish/Create SSH-Key access for devices or servers within the manufacturing environment
- Change firewall settings (lockdown to only port 22)

The printer must also be located at the localhost or 127.0.0.1 address before a user can load the software. If the process runs successfully, a tunnel is established over port 22, ensuring the encryption of all traffic over the wire to the printer through the Secure Shell (SSH) protocol [29].

Ongoing development efforts culminated in the release of SecurePrint 2.0, marked by substantial improvements to the user interface as it transitioned from a Command Line Interface (CLI) to an intuitive Graphical User Interface (GUI). This upgraded version delivers a user-friendly solution tailored for both small and large organizations, ensuring reliability and a comprehensive set of features to meet diverse 3D printing requirements. SecurePrint 2.0 boasts the following key features [29]:

- Integrated 3D Printer Hardening
- Secure printing to compatible devices
- Stand-alone or network-connected CAC authentication
- Role-Based Access Control
- Robust logging and auditing
- Data-at-rest encryption

- Importable configuration settings for printers
- Command-line interface supporting select administrative features
- Configurable add-on services, such as NTP server configuration
- Centralized Syslog server for offloading printer system logs

Despite the significant advancements in SecurePrint 2.0, which represent a substantial improvement, full connectivity remains a challenge. The application allows printers to be networked, even in a standalone network, yet it falls short of complete STIG compliance. Additionally, it lacks monitoring through the Host-Based Security System (HBSS) and direct scanning by the Assured Compliance Assessment Solution (ACAS). The ongoing development aims to address these challenges and enhance compatibility with various features within the USN network [29].

Another version of SecurePrint developed by the DAME team is SecurePrintZT [29], which aims to implement elements of SecurePrint 2.0 and Zero Trust practices into a ship's network. While still in development, this application's idea is to allow direct printing to devices onboard USN vessels without risking the problems of installing these devices directly onto a ship's network. The same concept of establishing a DME is necessary for SecurePrintZT to connect on a logically and physically separate network. The intent is to configure a Blackbox dedicated device with two network interface cards on separate DOD Information Network (DODIN) and printer networks while providing network protection assurance on both sides. If successful, the DODIN would be protected from potentially unsecured printers while integrating current repositories. Additionally, this would allow for much more flexibility when it comes to installing any new printers in any future endeavors. Figure 3.5 summarizes how these workflow elements might be pieced together [29].

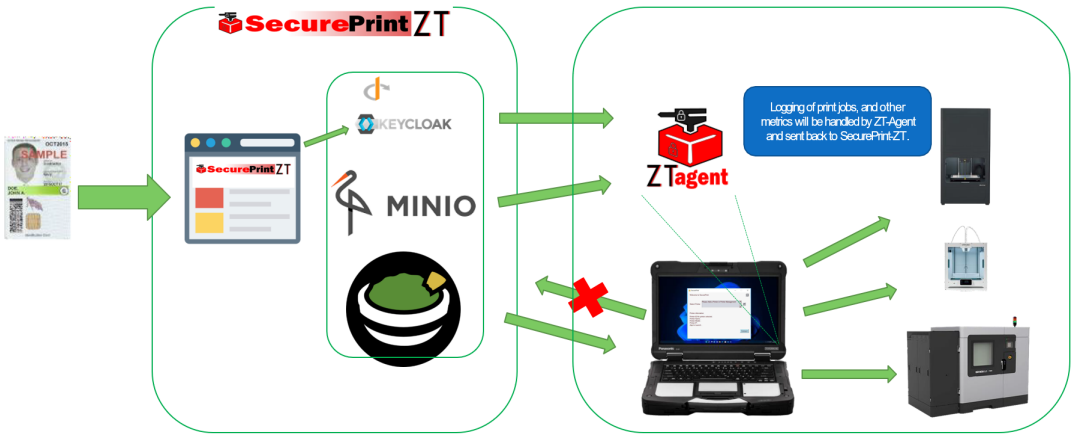

Figure 3.5. SecurePrintZT General Overview. Source: [29].

3.3 Project Hivemind

Another notable USN project still in development at Naval Service Warfare Center (NSWC) Carderock Division that has been gaining headway is titled Project Hivemind. This technology presents a promising architecture that helps establish the integrity of part data in transfer. In this research, the overarching question was, "How can the USN ensure that the approved parts are the ones that get fabricated in the face of external and internal threats?" Project Hivemind [20] seeks to achieve integrity, decentralization, and a unified total order of AM data by establishing a repository as a comprehensive solution.

Project Hivemind is structured around three key components:

- Submitter
- Approver
- Fabricator

These are also referred to as "nodes" and are used to propose, review, and reject any changes to the repository data while in transit. The submitter represents the bottom-level operator that develops the work package before comparing it with a repository and sending it to the approver. The approver also checks the work package against an available repository along with any available review tools. With the final blessing from the approver node, the box

makes its way to the fabricator node, where it will proceed to production. Rejection at any point will fall back to the submitter node for revision. Figure3.6 details this process.

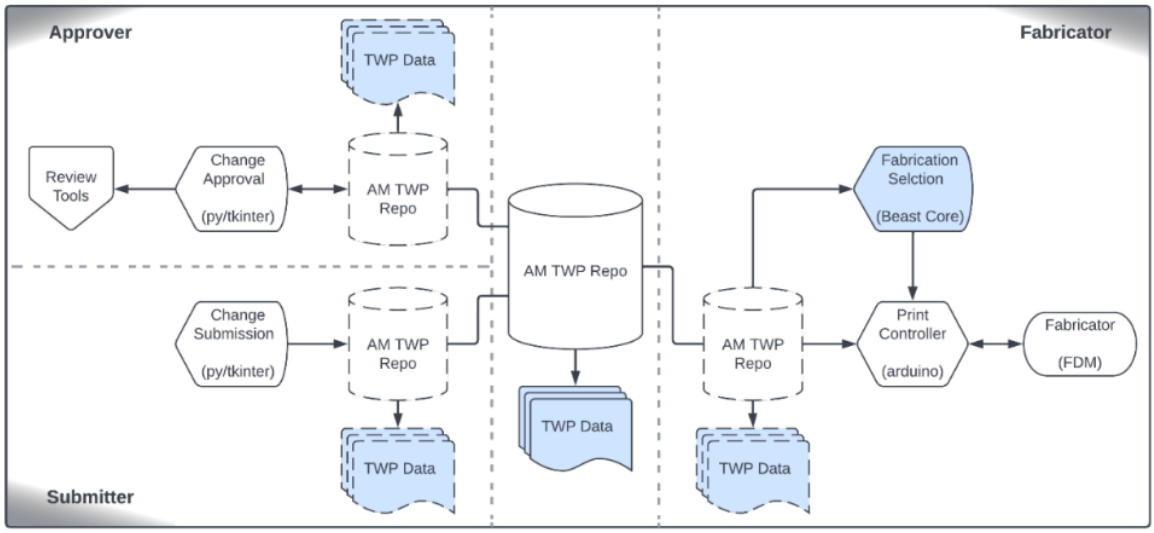

Figure 3.6. Hivemind Concept Flow. Source: [20].

Project Hivemind is undergoing assessment against a defined set of functional goals designed to ensure the robustness and efficiency of the system in handling the digital thread of AM part files. These objectives encompass the protection of AM part files from unauthorized alterations or deletions, the facilitation of a streamlined approval process wherein only authorized users can endorse files for printing, the provision of a user-friendly interface for efficient file management, and the support of scalability to accommodate a substantial volume of AM part files without compromising system performance [20]. Enhanced blockchains, serving as invaluable tools, necessitate the entirety of the blockchain for seamless operation and continuity assurance. Progress for NSWC is contingent on refining the fabricator User Interface (UI) for a more streamlined experience and incorporating an off-chain storage system to handle extensive data volumes efficiently [20].

But perhaps the most significant hole yet to be filled in this research is the mystery of authenticity in the grand scheme. Ensuring that parties on each end are reliable is a considerable success factor and leaves an open end for further exploration [20]. While the above methods attempt various solutions, until the threat model is clearly defined it is not possible to assess the achieved security and functional optimality of the possible solutions. In the next chapter, we will broaden our perspective to see how the USCG handles its AM data.

CHAPTER 4:
USCG Application

The USCG has also expressed great interest in factoring AM technology into their surface assets but is also experiencing the same if not more, difficulties as their USN colleagues. While the USN AM process is still undergoing refinement, the USCG aspires to align with their progress. As it stands, there is no official written guidance or expectations when it comes to AM data security in the USCG. USCG uses a series of forms and expectations regarding how AM parts are used and approved in their force but is still awaiting official guidance. Understanding the intent and goals behind these processes might help achieve a more standardized security procedure further down the line.

4.1 Triage Process

The USCG utilizes a "triage system" [32], which aims to address the importance of the part being submitted. Four players have a role in determining the necessity level, including a requester, a technical authority, a TWH, and an AM IPT. The requester completes and submits an AM request form to the tech authority for approval. This request form is to be digitally routed and obtains essential information regarding the sender and the part in question. The form requires names, emails, phone numbers, manufacturing information, pictures of related equipment, and the reason for requesting AM approval. A digital signature from an approving authority or designated appointee is also required before the submission is continued [32].

Should the part be disapproved, it is categorized as red. If a stamp of approval is given, the part is evaluated for criticality and feasibility by the tech authority, TWH, and AM IPT. If the part is deemed not feasible, the part is categorized as red. It is categorized as blue if the part is considered feasible but not critical. If the part is essential for mission success or safety, it is also categorized as blue. If not, then it is categorized as green. Once a part is given a categorization, this process is concluded. Figure 4.1 shows this process's intended chain of events.

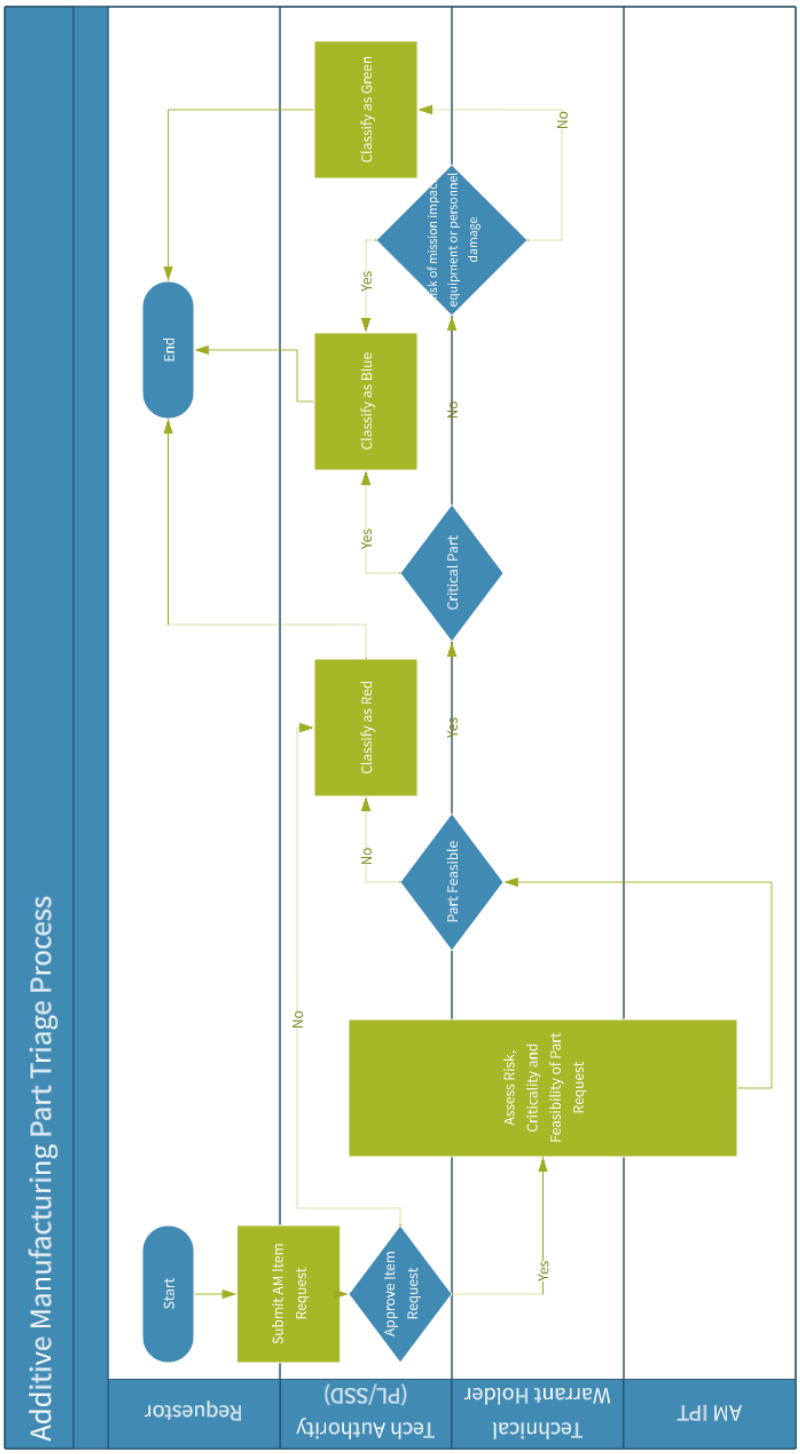

Figure 4.1. USCG Part Triage Process. Source: [32].

4.2 Determining Criticality

The USCG also requires that a certain level of criticality be applied to all part information routed. Similar to the NAVSEA process, several considerations must be addressed in what is known as their Surface Forces Logistics Center (SFLC) AM Criticality Assessment Process [33]. These include whether the part will replace an existing part, if the part is essential to mission success or safety, and whether all dimensions and specifications are met. Risk assessment is heavily factored into these considerations, and failure to meet requirements would result in disapproval.

The following steps in the chain deal with the availability of materials, whether the environment can support printing the part, and whether the printing process is vetted and approved for the relevant application. In each phase, the expectation is to reference a separate series of sources to validate approval. These include a separate approved parts list and a vetted printing process source. The final step addresses whether the printed part will be a permanent installation. Should the part be intended for a permanent replacement, then a TWH is required [33]. Figure 4.2 depicts this process in detail.

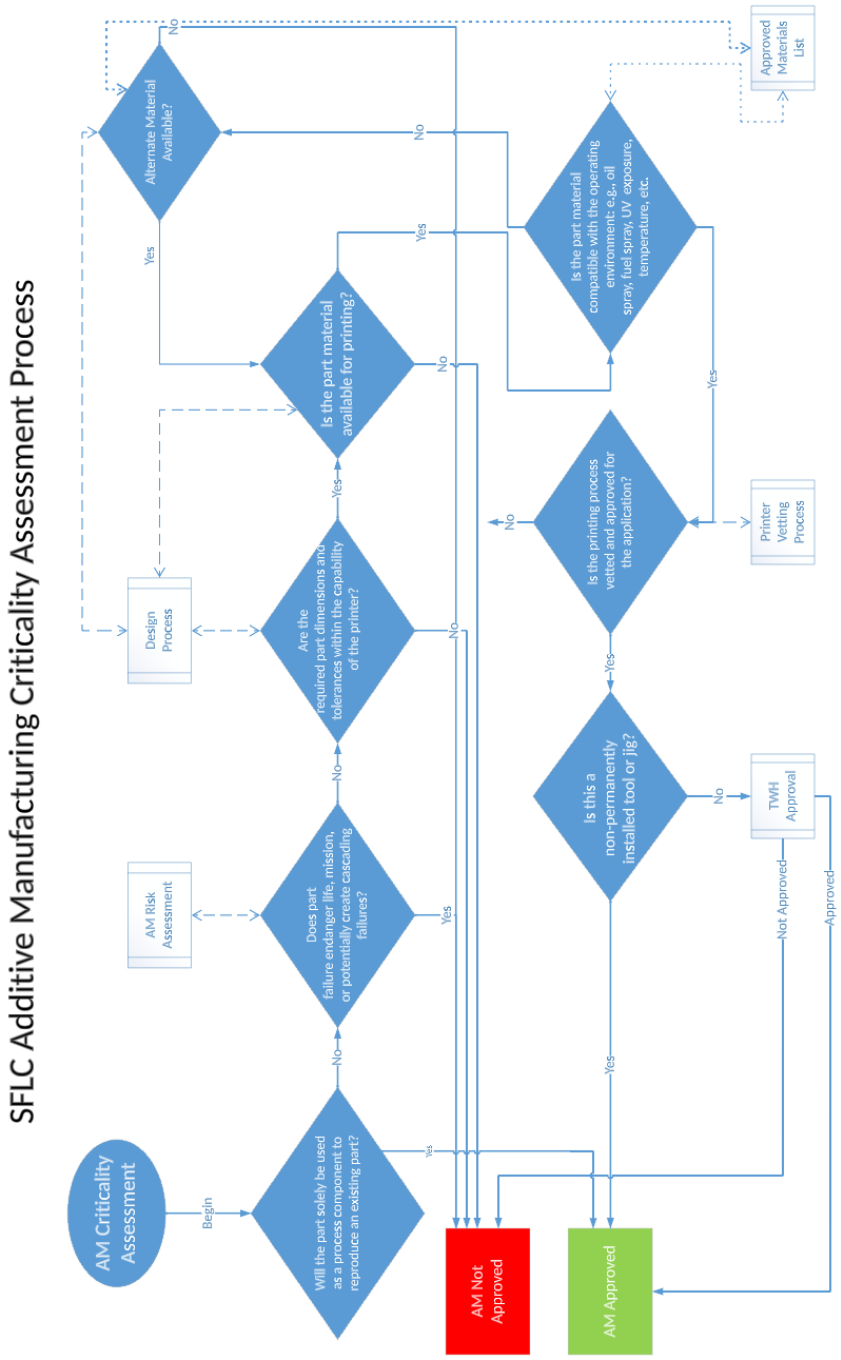

Figure 4.2. SFLC Additive Manufacturing Criticality Assessment Process. Source: [33].

4.3 Technical Data Package Development Process and Part Deployment

TDPs are also extensively used as a tool for AM in the USCG. However, this process, illustrated in Figure 4.3, is reserved for parts classified as green or blue. Once the desire for a TDP is established, the AM IPT deploys a team from the SFLC who works closely with an Electronic Systems Support Detachment (ESD) to design the submitted part, performing technical analysis as necessary. Should the part not be feasible, then the process is concluded. If approved, then the part is printed and must undergo a long series of quality assurance practices along with requirements for Fit, Form, and Function (FFF), which must be met. Should the part fail in any part of this phase, the process halts. Otherwise, the part is used, and the schematic information is uploaded to the USCG database, Technical Information Management Branch (TIMB) [34].

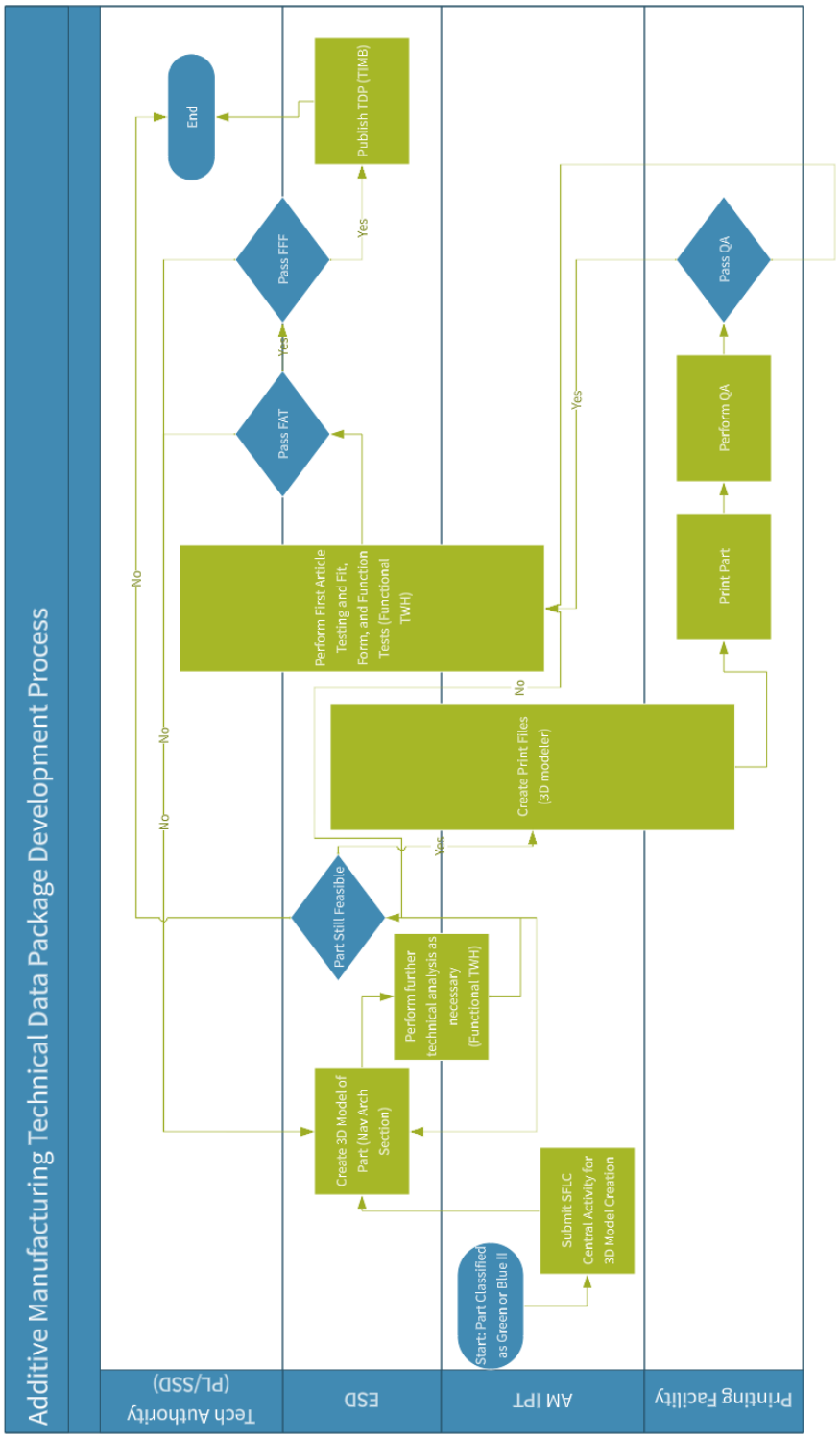

Figure 4.3. USCG AM TDP Development Process. Source: [34].

In this chapter, we observed the beginnings of AM policy development within the USCG. Of course, there are numerous steps to consider among all these processes. It is logical to assume that the USCG values efficiency given the amount of verification and careful thought put into each factor in the workflow of an AM package. However, the question regarding how this data should be protected still remains. Careful attention to this provides the necessary insight to understand the need for security among USCG AM systems.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 5:
USN Policy/System Analysis

While the USN may be a ways from standardizing an ideal AM security model across the Fleet, breaking down the current policies to better understand what is practical in the future is still very valuable. Existing instructions do not go into great detail regarding specific security practices, and there are several locations in the Navy's current data flow where vulnerabilities can fester. This chapter will dive further into the current structure of general AM policy within the USN and where problems could arise in the big picture.

5.1 Current Policy

As previously mentioned in Chapter 3, the Navy employs more than one existing AM policy. Although these policies exhibit slight variations, their similarities are pronounced enough to facilitate the design of a comprehensive network overview for the data transfer process. As mentioned in Section 3.2.1, there are two primary depictions of this model, differing only in whether the AM command and control station (3D printer) is isolated or integrated into the ship's network.

To understand the current status of Navy AM policy, a comprehensive examination is necessary. Figure 5.1 analyzes the start of the process in which the AM data is conceived and submitted for approval by some qualified personnel, ideally. The data is then evaluated for severity before reaching the approving authority. Either way, the information will need to go through an approval authority, and in this case, it would generally be a CHENG. However, if the level is deemed high, the existing policy states that additional approval from an outside AM expert or team is necessary for approval in the chain. Should the part be approved, then it may proceed onward to the printer.

This portion of the architecture is intended to function with internet connectivity for reasons as will be explained in Chapter 7. However, it should still be utilizable even if connectivity is lost. In the maritime setting, encountering difficulties in maintaining internet connectivity for data transfer is a common nuisance. However, the approval of AM data should not be contingent on such challenges if needed.

The ship's network interconnects all devices and users on board, providing a connection to the internet for various purposes. Emails are heavily relied upon in the case of uncertainty and are required when input from outside support is needed for higher severity approval. In addition to access to emails, a 3D schematic repository should be readily accessible for users as a centralized database for AM information already used in the DOD.

Should the approval go through for the AM data concerned, the remaining steps would include uploading the information to JTDI for future use and then downloading the data onto a flash drive or SD card, which would be transferred to its final destination at the designated standalone printer. While this process may change, the current utilization of this transfer method points towards the the system functionality that security should be incorporated with; namely, to avoid a disruption to expected functionality, we focus on securing the present workflow in a minimally invasive manner. Figure 5.1 illustrates the complete data flow of this chain.

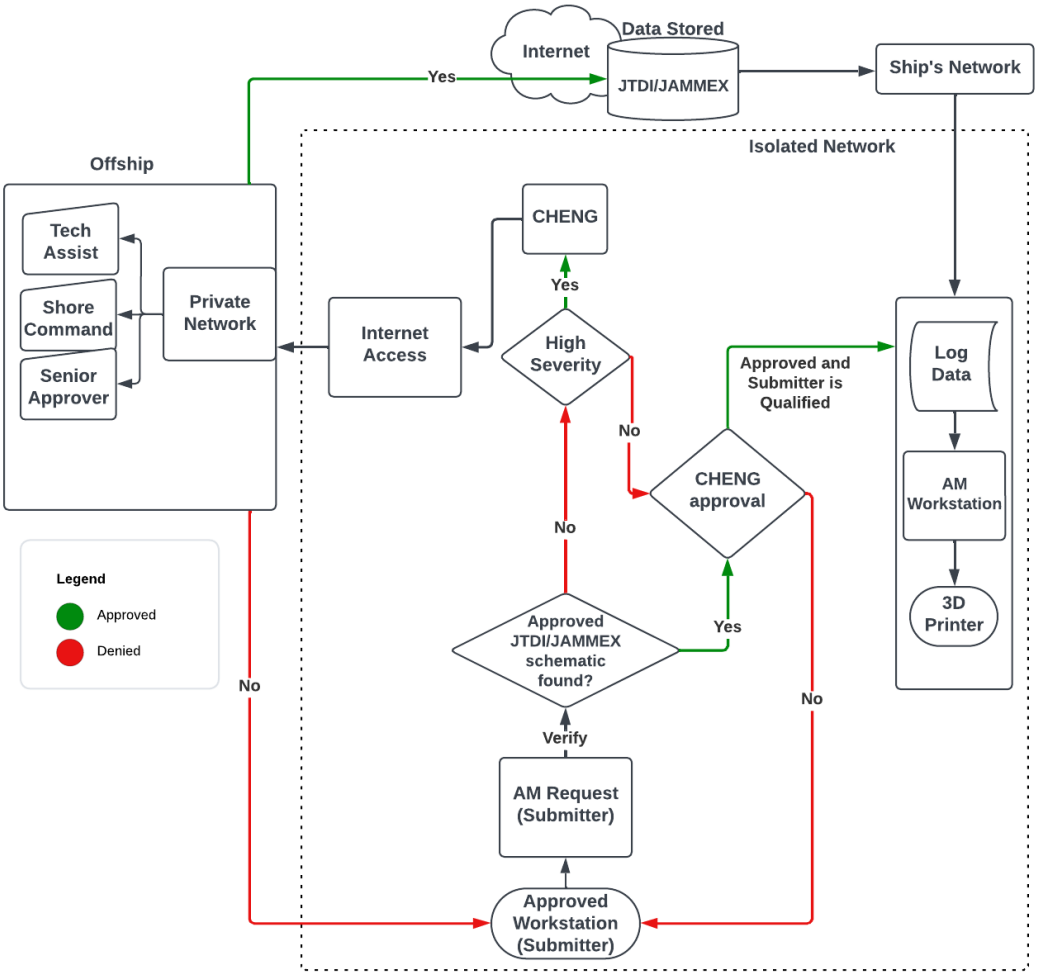

Figure 5.1. General Shipboard AM Data Flow

As for the other design, the only difference from the depicted model would be connecting the 3D printer directly to the ship's network. This would open up a new thread of problems, as discussed in Chapter 2.

Across the diverse approval chains in the USN AM policies, a consistent and prominent theme persists: the aspiration to integrate a dependable and comprehensive AM repository seamlessly into the workflow [20], [25], [35]–[37]. This is a top priority for developing teams so that these workflows and policies can be regulated from ship to ship while expediting the

processes in case a previously approved part is already available for reference.

The JTDI stands out as the primary database for AM within Navy policy, as it is already widely used across the Fleet [25], [26]. With nearly 340 approved entries, the database provides a comprehensive resource for users. However, its main limitation lies in its dependency on consistent user input, which poses a challenge to its effectiveness [38]. In the latest version of the DOD AM strategy, the Joint Additive Manufacturing Working Group (JAMWG) hopes that the Joint Additive Manufacturing Model Exchange (JAMMEX) will become the standardized AM database used across the entire DOD [39]. The JAMWG is a cross-cutting DOD community that believes that AM knowledge should not belong to any branch of service. JAMMEX provides a possible option for sharing data and instructions [39]. Although not fully acknowledged at present, the DOD anticipates that all branches of the military with AM needs will embrace and fully adopt JAMMEX in the near future [39].

5.2 Data Authentication and Confidentiality

Authentication is the procedure for validating the identity or origin of a person, device, or piece of information. Authentication is further coupled with integrity, together ensuring that data has not been changed since generation. In AM security, authentication and integrity must ensure that the generation and sharing of data, instructions, and ideas related to AM are limited to authorized users such as the router and approving authorities such as a CHENG, sponsors, etc. Chapter 3 along with Figure 5.1 helps furnish essential insights to guide our understanding of what should be involved when handling AM data in a maritime setting.

Once the idea, or "AM Request," is submitted, robust CAC signature authentication measures should be in place in the workflow until the data reaches the 3D printer. While it could be debated that signature authentication might not be needed between the submitter and initial approving authority (i.e., CHENG, Program Manager, Air (PMA)) within the confines of a ship, any entity involved in sharing beyond this initial authority should certainly require authentication. Authentication should be applied to the following endpoints that exist within USN current policies:

- AM Request → CHENG
- CHENG/Submitter → Tech Assist/Sponsor via email
- Verified data from repository and/or Tech Assist/Sponsor → AM C2 (NAVSEA or NAVAIR)
- Verified data from AM C2 → CHENG
- AM Request (submitter) and/or CHENG → Established 3D Printing setup

In addition to authenticating the endpoints, the AM data should be ensured of its confidentiality. While confidentiality is not the focus of this thesis, we will briefly cover considerations on it in under the current policies.

5.3 Vulnerabilities

While the policies already in place inform that anyone making AM requests should be designated, the initial submission has no specified guidance regarding security verification methods. There is no guidance anywhere that details authenticating data coming from any source. Ensuring that data in this process stems from a trusted and reliable source is crucial.

It may be reasonable to assume that some encryption method is used in this process, yet it is not mentioned anywhere. All directed emails are sent to unclassified addresses off-ship without security guidance, which leaves the data or even the actual printer open to malicious behavior. Email authentication methods, such as digital signatures or certificates, can only verify the identity or the origin of the last sender, but not the entire chain of custody or provenance of AM data or products [40]. Establishing a secure communication for the entire transport path of the data is imperative, surpassing the mere concept of a "channel." Even a signed email, though seemingly secure, falls short of guaranteeing the authenticity of the true approval for the use of a 3D schematic. In reality, it represents just one leg

of the journey, and as the information traverses through each endpoint, the final recipient gains insight only into the last hop, lacking details about the authentication details. This underscores the necessity for a comprehensive solution that ensures end-to-end encryption, safeguarding data and the actual 3D printer from potential malicious behavior [40].

The use of external storage is also highly unsafe in this process. By all accounts, the Navy and the rest of the DOD have eliminated the standard use of external drives in their networks and all connected devices [41]. Malicious software is only becoming more sophisticated as time passes and can easily worm itself into one of these storage devices uninvited. This can easily disrupt the system making the request or corrupt the 3D printer and/or any attached network. Simply put, USB and SD drives should not be the primary tool for AM data transfer.

5.4 Security for Severity

The existing AM instructions place a high emphasis on different levels of severity in specific AM part requests. While there is a decent explanation regarding who should be involved in the process, the specifics of how each level should be handled securely can still be explored. Arguably, the most considerable concern is neglecting how specific equipment should be handled depending on its importance. While it may not be necessary for a high-ranking authority to approve something as simple as a standard screw, it certainly might be for a more critical component. Since such decision points are both necessary and outside the scope of this thesis, this In the following chapters, this research will aim to propose a data authentication approach that can deal with differing levels of security based on the severity levels of the AM parts in submission.

5.5 USCG Comparative Analysis and Summary

Understanding the complexities and potential vulnerabilities within the current policies of the USN regarding AM helps to shed light on similar challenges faced by the USCG. The USCG AM architecture involves various participants and authorities, each requiring distinct authentication points of their own, much like the USN. In essence, the examination of the USN AM policies provides a blueprint for understanding the challenges and areas of improvement, serving as a valuable reference point for enhancing security measures in the USCG's AM endeavors. The shared objective of securing additive manufacturing processes across maritime branches may necessitate collaborative efforts in addressing common vulnerabilities and implementing robust authentication measures. Chapter 6 can be found as a supplemental file presenting a field survey, before we move to Chapter 7 where we propose a design that takes existing military priorities, such as those previously mentioned, and incorporate them into an efficient AM data flow network.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 6:
Supplemental – Field Data

The current methods utilized among DOD personnel and ongoing AM experiments are valuable in understanding how to develop a secure data flow process. Moreover, the opinions, experience, and expertise gathered from personnel across the DOD can help higher-level authorities decide on a well-established policy. To gain a better grasp of how policy is perceived amongst varying personnel, this chapter takes a qualitative approach and analyzes the results of a questionnaire built to shed some light on existing problems. More specifically, the survey seeks to understand how AM schematic transfer is perceived, including how this data is generated, authorized, stored, and transferred.

The remainder of this chapter is presented as a supplemental, labeled as CUI. To access the supplemental material, contact the Dudley Knox Library for further details.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 7:
Proposed Solution

The prior chapters aggregate information on current procedures for AM schematic transfer. This chapter focuses on constructing a functional, secure shipboard AM data flow network for the USN based on the topics we have explored in the previous chapters, along with the insights gained from the supplemental chapter of this thesis. When transferring sensitive data across any network, the first critical thing to consider should be guaranteeing that all the elements of the CIA triad are satisfied. To accomplish this, we need to analyze existing practices and decide whether they should be adjusted or removed from the process entirely. Many components must mesh together to help ensure data integrity while abiding by the standards set forth by the chain of command onboard a ship or anywhere within the DOD.

7.1 Overview of Proposed Network-Integrated Solution

While Naval ships are not the only facilities within the DOD working on AM security, the following proposal proposes a step-by-step process to help develop a solution for the surface warfare community and perhaps even the DOD. Considering everything thus far, authentication is a primary focus of this proposal. There must be some formal method set in place that confirms the data authenticity between the sender and recipient of AM information – especially from the authorizing authority of the approved diagrams and the end-user. The next issue falls under tackling the different levels of severity. Figure 7.1 provides the workflow that proposes the signing of data to help enhance integrity while also satisfying some of the other hierarchical concerns discussed earlier in this thesis.

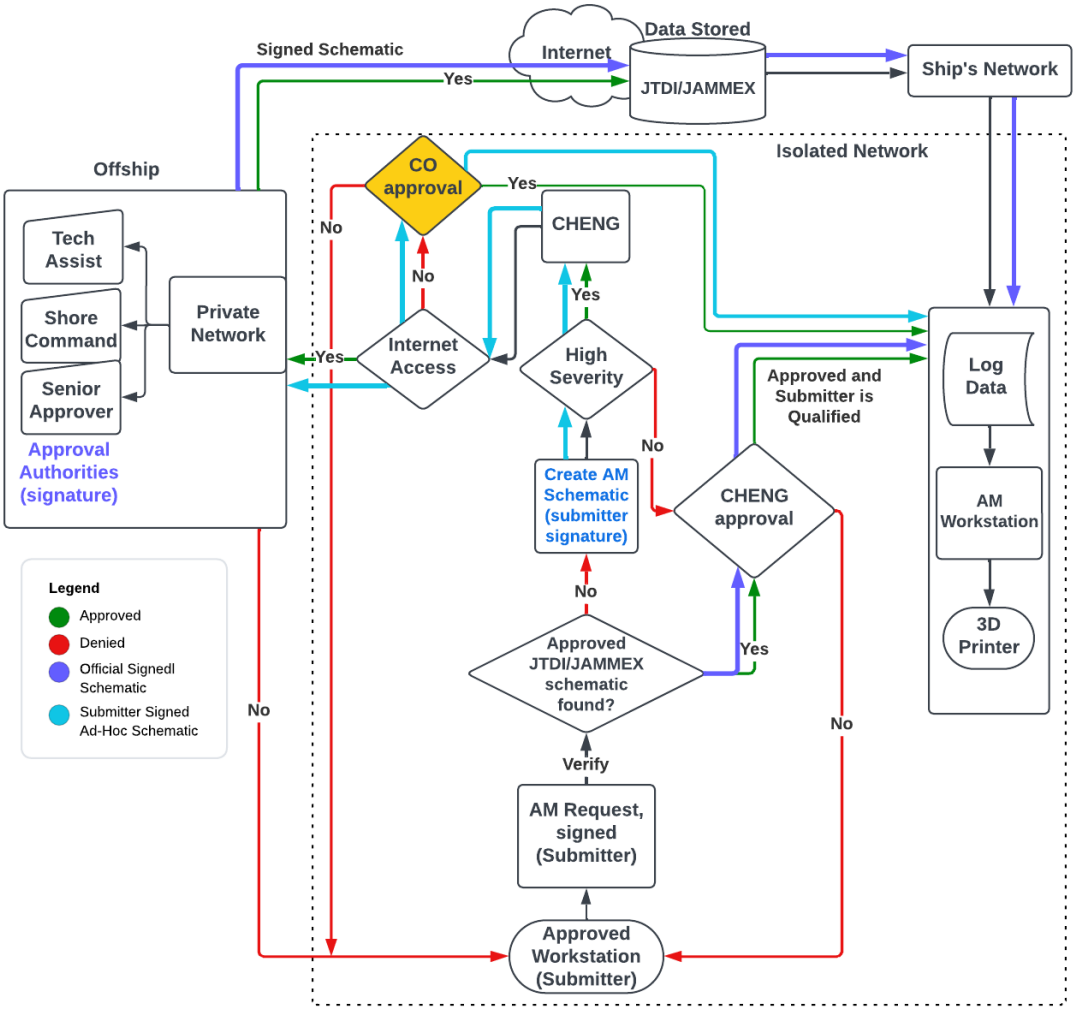

Figure 7.1. Proposed Shipboard Data Flow

The flow of data within the AM process begins at an approved workstation, likely equipped with PKI approval, installed on a ship's network. The ship's location determines whether the network has internet access, influencing certain aspects of the approval chain. From this workstation, a submitter, typically a junior serviceman or servicewoman, is tasked with creating a 3D schematic required for printing a replacement part and subsequently submitting it for approval.

As outlined in Chapter 3, the submitter should still check the ship's preferred database or backlog for previously approved parts to help streamline the routing process. If the part has already received approval and the submitter possesses the necessary qualifications, they can send the data to a DME housing the ship's printer as referenced in Chapter 3, Section 3.2.1. In cases where the part is on the database but the submitter lacks full qualifications, they should consult their command's equipment classification lists to determine if a specific classification level is required for the 3D schematic information. If the severity is low, the data may be sent to the CHENG for approval.[1] Upon CHENG's decision, if approved, the data is returned to the submitter, who uploads the approval data to the database before sending it to the printer within a DME for printing. In the event of CHENG denying the part, corrections are made by the submitter. For high-severity parts, the appropriate classification is assigned and routed to CHENG, where internet connectivity becomes a determining factor, referring to Chapter 3, Section 3.2.

When internet access is available, CHENG forwards the classified data to offship points of contact for assurance. If approved, the submitter proceeds to printing. In urgent cases, where offship input is not feasible due to lost connectivity at sea, the Commanding Officer (CO) may need to be involved in approving the data regardless of qualification or severity status. If the CO approves, the submitter loads the data into the database and proceeds to print. These detailed procedures, depicted in Figure 7.1, integrate considerations from various policies, aiming to meet the requirements for all stakeholders involved in AM within the maritime domain.

[1]Table 3.1 is useful for NAVSEA, but it is crucial to acknowledge that severity scales may vary across commands and branches of service within the DOD.

7.2 Authentication and Integrity

While a ship's network is constructed to provide degrees of authenticity and confidentiality, it does not offer authenticity of data to the origin end-point, e.g., the offshore approver. An internet connection involving sending information to an off-ship entity for review will always pose risks. Furthermore, even for on-ship approvals, a method of tracking the generating and approving authorities is necessary for record keeping. Depending on part sensitivity, confidentiality above and beyond what is offered by the basic infrastructure may be required. We do not explore this topic further, though, as the focus of this research is the data integrity of AM schematics.

The submitter of the work package and the PMA/CHENG should be qualified to recognize, edit, and route AM data. Furthermore, it might be necessary that these personnel be given special privileges for this shipboard process, such as specific access to workstation(s) designated for the sole purpose of AM. Being assured of exactly who has a hand to play in each step of the process is vital in knowing that the AM data being used is safe. Moreover, once a schematic is approved for use, the authenticity of that data needs to remain intact, attesting to integrity from the time of approval. Thus the data authenticity, once applied by the approvers, should remain intact with the schematic (see the blue line in Figure 7.1.

The final approvers, illustrated in Figure 7.1, consist of external entities, such as the original manufacturer of the component, the AM team within the parent command, the TWH, and/or the program manager that each contribute technical assistance.[2] Ideally, the original manufacturer of the specific part should be responsible for scrutinizing the AM data, leveraging their extensive knowledge to ensure the accuracy of all part parameters. However, the AM teams or a senior AM technician at the parent command associated with the asset should possess the most comprehensive knowledge required for assets to consult in such scenarios. They should also have the highest qualifications and experience to thoroughly assess and approve new AM data for utilization. These entities are explicitly identified in

[2]It is noteworthy to highlight that in exceptional circumstances, the highest authority at the parent command – be it an Admiral at NAVSEA or a General in the Marine Corps – could be included as an additional point of approval. In situations of utmost importance, such as when dealing with AM data related to critical components like a Main Reduction Gear (MRG) or a Array, Navy/Search Protect, Yellow 1 (AN/SPY-1) Radar, the significance is so paramount that notifying the Admiral or General becomes imperative. However, it is essential to recognize that their involvement does not mandate them to personally assume the approval risk, as their expertise might not align with the intricacies of the approval process.

the existing NAVSEA and NAVAIR instructions [25], [26] and should seamlessly integrate into the depicted data flow model.

7.2.1 Basic PKI Infrastructure

The integration of the CAC PKI serves as a robust cryptographic system that can provide entity authenticity utilizing infrastructure already in place. The CAC, housing an embedded chip, becomes a key component in this process. Upon user authentication through the entry of a Personal Identification Number (PIN), the CAC's private key, securely stored within the chip, is utilized to generate digital signatures. These cryptographic digital signatures derived over the data to be signed, provide a unique and non-repudiable means of authentication. The corresponding public key, an element of the user's digital identity attested to in the PKI, is employed to verify the digital signature, ensuring the integrity of the associated document or transaction.

This approach provides attestation that the approving authority approved the schematic, safeguards against unauthorized manipulation, and ensures the authenticity of crucial information, thereby enhancing the overall trustworthiness of the AM process. When a user signs an AM schematic using their CAC, a unique digital signature is generated based on the schematic's content, providing assurance that the data has not been tampered with or altered during its lifecycle.

7.2.2 Pulling a Pre-approved Schematic

The approval of AM data requires authentication through the use of signatures, as illustrated in Figure 7.1. In the case of utilizing either the JTDI or JAMMEX databases, submitters should expect that any schematics pulled from these databases are signed by the offship approval authorities and trusted for use. This also ensures that the subsequent authority, such as the CHENG or the following approving entity, can ascertain the creation source.

The submitter is responsible for initiating the schematic identification process by checking the availability of the required data in an approved database. If the data is present and has already been officially signed, as indicated by the purple arrow, the submitter can then route the data through the CHENG. Upon approval, the CHENG must append their signature, indicating they have reviewed the data. The AM data then proceeds to the printing stage, thus timestamping the approval for use.

The principle of "trust but verify" is a prevalent concept across all branches of the DOD, and it is firmly ingrained in this section of the network proposal. A submitter is required to possess fundamental qualifications for creating and reviewing data, as well as the capability to retrieve approved schematics from the relevant databases. However, as an additional layer of verification, the CHENG or another qualified authority with greater experience provides their approval, ensuring thorough scrutiny in the approval process.

7.2.3 Low Severity / Ad-Hoc Schematics

If the part is not available on these databases but is not considered low-severity, the CHENG has the authority to officially sign the data and permit it for printing. The signature of the CHENG serves as a catalyst for streamlining the printing process, particularly when dealing with new schematics categorized as low severity. By endorsing these schematics, the CHENG expedites their incorporation into the production pipeline, facilitating efficiency without compromising the rigorous review process.

7.2.4 New Approved Schematics

A designated workstation ensures a focused and secure environment for handling AM data, enhancing traceability and reinforcing the integrity of the submission process. When a submitter introduces a new 3D schematic that has not been uploaded to an approved database, it becomes up to them to begin a new signature chain. The utilization of the submitter's signature acts as a tangible marker, offering a transparent means of verification and fostering a heightened level of confidence in the authenticity of the submitted data among hierarchical stakeholders.

The blue arrow in Figure 7.1 represents a submitter-signed ad-hoc created schematic sent for approval through the data flow. The AM data traverses three possible entities along this line: the submitter, the CHENG or designated approval authority, and the CO. Each entity must sign the data to progress the flow. These stakeholders should possess the necessary expertise to be entrusted with authenticating the AM data, as it has potential impacts not only their own ship but also the broader DOD.

Equipment that necessitates the printing of high-severity data must undergo a meticulous review by AM experts and/or technical specialists to ensure the accuracy of every parameter before the manufacturing process can actually commence. The precision of schematic parameters is paramount, as inaccuracies pose a significant risk of equipment failure or, in extreme cases, loss of life. As such, AM experts and technical authorities should be the ultimate approving authorities for new schematic designs of high importance. Therefore, newly developed schematics must be transmitted to offship approval authorities, which may include the original manufacturers of the respective equipment under analysis or Fleet command authorities located at either NAVSEA Pacific or Atlantic. Upon their comprehensive review and approval, an official signature is affixed to the data, allowing it to be uploaded to an approved database (e.g., JTDI, JAMMEX).

The signatures obtained from offship entities carry significant weight, serving as a testament to the thorough scrutiny and approval of the data for widespread utilization. These signatures not only validate the integrity of the schematics but also convey a universal message of endorsement, instilling confidence in users across the USN, and potentially DOD, that the data is deemed fit for extensive deployment. Thus, the signature authority block must be recognizable, and easily validated based on available PKI infrastructure.

7.2.5 High Severity / Ad-Hoc Schematics

Certain situations may arise where reaching offship approving authorities is challenging, especially in scenarios such as a ship being at sea with limited connectivity in a high-stress environment. In situations of extreme urgency, the CO wields the authority to sign off on schematics, prioritizing the overarching mission value over potential risks to equipment. This decisive action ensures that critical components can be swiftly produced when time is of the essence, allowing for operational continuity in high-stakes scenarios. While the

CO's signature may suffice for internal use within the relevant ship, it does not qualify for widespread database inclusion.

Specifically, in instances of high severity, the submitter signs the data and sends it to the CHENG. The CHENG, upon endorsing the data with their signature, then proceeds to relay it to either the offship approving authorities (following the process outlined in Section 7.2.4) or directly to the CO. In such cases, the CO signs the data and approves the printing process.

A CO may not possess an extensive level of AM knowledge, but they still bear responsibility for the condition of equipment and personnel on their ship and are empowered to make decisions in urgent situations. In such instances, the CO's signature is sufficient for printing high-severity parts exclusively for their ship. Nevertheless, it is important to note that this approval is confined to the specific ship and is not eligible for broader use within the Fleet or DOD without offship approval. This process step should only be taken if the correct approval authorities cannot be reached.

7.2.6 Signature Authorities

In relation to Figure 7.1, the most appropriate places for digital signing would occur at:

- The approved workstation. The submitter signs to attest to the original creation of a schematic.
- The CHENG or the designated approval authority provides local approval for the use of the new schematic if appropriate (low severity).
- The CO provides local approval authority for high-severity schematics if offship authority cannot be reached.
- Offship entities, including technical assistance, parent commands, and equipment sponsors, review high-severity schematics. The evaluation and determination of the schematic's design quality are conducted before signing and returning it.

7.3 Blockchain Suitability

In assessing suitability for blockchain-related technologies, we focus on two notable projects: Project Hivemind and Blockchain Mergence. The exploration of these projects offered a small glimpse into blockchain's practicality and adaptability in varied operational contexts.

7.3.1 Project Hivemind

First, there is the question of the compatibility of Project Hivemind within the current architecture, such as outlined in Figure 7.1. To ascertain its compatibility, it is imperative to assess its scalability within the predefined design parameters. Decentralization, a core tenet of blockchain, serves as a foundational principle that mitigates the vulnerability of a single point of failure by distributing control across a network of nodes. However, successful decentralization in this context relies heavily on establishing a robust consensus regarding the legitimacy of data. In regards to Project Hivemind, this consensus depends entirely on the submitter, approver, and fabricator nodes. Blockchain typically relies on a substantial number of nodes to establish legitimacy in its operations. While a higher number of nodes provides immutability of the log, there is a potential risk if the number of nodes is low (i.e., the log is not guaranteed as immutable due to potential for collusion to maliciously forge or alter the log). The efficacy of blockchain security tends to improve with a greater number of nodes, and a network with only three nodes may not provide the security benefits [42]. Consequently, blockchain might not be the optimal solution in this particular instance.

For USN use of blockchain, the issue of trust becomes a critical consideration. While blockchain is adept at providing security in scenarios involving distributed, untrusted participants, its efficacy and security benefits diminish when applied to a network of inherently trusted entities. In a setting where nodes are established authorities, like in Project Hivemind, the extensive consensus-building features of blockchain may be redundant [42]. If each participant or node is inherently trusted and possesses the authority to sign for their designated roles, utilizing blockchain might not be the most optimal solution, as there is no imperative to address the consensus challenge among untrusted participants [42] and the blockchain itself add computational overhead. Alternate methods, such as traditional databases, could potentially offer quicker and more cost-effective solutions in scenarios where trust is already established. Blockchain, emphasizing unknown/distrusted participants and decentralization, may be better suited for environments requiring those features, but it might prove less useful for applications involving authorized participants or prioritizing simplicity and efficiency. If the decentralized consensus properties are not required, then blockchain introduces needless overhead, bandwidth, and operational costs. In many USN settings, a preference for a straightforward operational environment is common, as simplicity often correlates with enhanced efficiency in system outputs.

Introducing additional nodes could exacerbate the complexity of this process and reduce its scalability. Each node plays a crucial role in both verifying transactions and contributing to the establishment of consensus across the network. However, as the number of nodes increases, it has the potential to introduce elevated communication overhead and impose additional computational demands on the system, which a ship might struggle to support. This influx of nodes not only creates competition for resources but also has the potential to result in slower transaction confirmation times and increased latency. Furthermore, the broader network may face challenges in maintaining synchronization and coherence, as each additional node adds complexity to the overall consensus-building process.

Based on the discussed considerations, it appears that the extended configuration for the proposed network may involve incorporating five nodes (submitter, CHENG, CO, and two or more offship authorities), taking into account the potential influence of internet accessibility on the overall design. Project Hivemind has yet to demonstrate scalability beyond three nodes, which underscores the necessity for future work in this area.

Irrespective of wired or wireless connection, inadequate connectivity among entities in a blockchain network can significantly impede the consensus process, causing delays in reaching an agreement. When connectivity issues arise, transactions face inconsistent validation across nodes, creating disparities in the blockchain's state among different participants. Nodes experiencing poor connectivity encounter difficulties actively participating in the consensus process, posing a risk to network distribution and security. Ineffectual contribution from these nodes undermines the decentralization of decision-making, potentially compromising the overall integrity of the blockchain network. This is a notable downside of any blockchain-based solution, not unique to Project Hivemind, and raises the question of whether such blockchain-based solutions would be usable at all in a ship-based context.

While blockchain provides the advantage of immutable logs that could present a definitive record of transfer and approval sequencing for AM schematics, such an advantage cannot be gained if lack of connectivity impedes efficient and regular connection with the blockchain. In addition, blockchain requires a sufficient number of nodes, well beyond three or five, in order to grant the immutability property. Consequently, in situations where connectivity is erratic or the node count is insufficient, the potential of blockchain to deliver its intended advantages may be nullified, not only significantly reducing its effectiveness in certain

operational contexts but also adding issues for other systems due to bandwidth costs. These factors present compelling arguments when considering the use of Project Hivemind. Therefore, a thorough examination of these challenges is essential if any blockchain-based solution is considered further.

Separately in this work, Project Hivemind underwent a brief examination to assess its efficacy within a WiFi setting during this thesis. Details on a basic setup for Project Hivemind can be found in Appendix B.3.

7.3.2 Blockchain Mergence

Blockchain Mergence tackles the challenge of managing supply chain item records through two methods, blockchain and local signature chains, emphasizing adaptability to external tracking variations and diverse DOD classification levels. It proposes using local signature chains (e.g., shipboard) for operations like device registration and repair, using authenticated through PKI. The concept includes a device chain for managing immediate time history, using digital signatures for authentication in recording authorized changes to components. In a global view (e.g., DOD-wide), it then supports storage of such chain records on a blockchain.

We create a scenario as a concept of operations (CONOP) to see how it might be possible to adjust the local component of Blockchain Mergence to onboard ship use. The scenario is described as follows:

7.3.3 CONOP

1. Fireman Timmy discovers a broken part inside some unknown piece of equipment.
2. Instead of waiting for a backup part, Timmy considers 3D printing the part as an alternative solution.
3. With the prerequisites of AM schematic creation experience, Timmy checks the approved database (JTDI/JAMMEX) to determine if the part exists and is approved for use.
4. If the part is already approved and available:
    - The print data will be downloaded and routed for final approval on a TDP.

- Request for final approval is routed to CHENG, or someone who is a qualified authority, unless Fireman Timmy has appropriate qualifications, in which case he can proceed to printing the part himself.
    - If approved: Return the TDP to Fireman Timmy with the stamp of approval. Fireman Timmy will review and update the data in the repository as needed. Subsequently, the authorized information will be transferred to a segregated network, which will then record and prepare the data for printing through a dedicated user interface, such as a laptop or 3D printer.
    - If disapproved: Route back to Fireman Timmy to address discrepancies.

5. If the part is not available in the database:
    - Proceed to check if the part is classified as low or high severity.
        - If low severity:
            - Route to CHENG for final edits and/or approval.
                - If approved: Return to Timmy with the stamp of approval and signature. Upload the signed and approved schematic to the database and transfer it to the segregated network, which will then record and prepare the data for printing through a dedicated user interface, such as a laptop or 3D printer.
                - If disapproved: Route back to Timmy to address discrepancies.
        - If high severity:
            - Submit to CHENG for necessary edits/input.
                - If discrepancies exist, it's returned to Timmy for resolution.
            - If the part is critical, the schematic may require global approval and signature from offship Tech Assist or an onshore authority.
            - PMO/CHENG reviews changes and submits to CO for final approval.
                - If CO approves and signs: Return to Timmy, who uploads the approved and signed part to the database and submits it to the connected workstation for printing.
                - If CO disapproves: Return to CHENG for further resolutions with Timmy.

This operational concept emphasizes scalability by highlighting the ability to initiate 3D

printing locally without requiring consensus from multiple parties. The local component of Blockchain Mergence offers a compelling perspective, especially concerning the ad-hoc segment depicted in Figure 7.1. In the local component, a blockchain is not used, but rather a signature chain records a ledger of authorized participant actions; it plays a pivotal role in ensuring the immutability of AM data with a high level of confidence. This familiarity with the participants contributes significantly to maintaining the integrity of the data. Notably, the resource requirements within such a controlled environment are minimal, making it a viable solution for smaller-scale such as shipboard implementations where the efficiency of the ledger is pronounced.

There remains a consideration for consensus in offship/'global Blockchain Mergence component' uses, and the concern for scalability is reduced. Under the global component, the blockchain network could involve multiple trusted USN entities responsible for handling or logging AM data. Figure 7.1 suggests a potential use for the Blockchain Mergence global component, considering that the bandwidth and overhead constraints of blockchain would only be a significant factor a portion of the time vs. at each step as in Project Hivemind. However, when deploying this technology in a broad scale USN maritime environment, one can reasonably assume that all entities on a shared blockchain would exclusively comprise USN assets. In such a scenario, the inherent immutability of blockchain, designed to establish trust in a decentralized environment, might be considered redundant (as noted above under Section 7.3.1), as all blockchain members are inherently trusted. This could potentially render blockchain technology a deadweight in such a trusted, closed system.

Details on a basic setup for the global part of Blockchain Mergence can be found in Appendix C.2, where this project looked at its potential applicability in a simulated scenario that mirrored the local dataflow architecture but applying the global blockchain functionality.

7.4 Summary

This chapter discussed how the workings of a contemporary AM data flow within the Surface Fleet might operate, underscoring the importance of maintaining integrity through the deployment of digital signatures. The next chapters will explore blockchain projects, Project Hivemind and Blockchain Mergence, to identify any possible contributions this technology might offer to AM data security.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 8:
Conclusion and Future Work

In this thesis, we have gained an extensive understanding of the current state of AM security within the USN and DOD.The military's stance on AM security appears ambiguous, with conflicting and unclear guidance creating uncertainty about the preferred direction. Many official documents do not address the major concerns highlighted by end-users of this technology. Though small in numbers, the questionnaire helped us gain a broad insight into how different DOD parties currently think AM should be handled and where they think it currently resides. Ultimately this research serves as a building block for what is to come in terms of policy analysis and AM workflow security exploration.

We also investigated Blockchain and dissected Project Hivemind and Blockchain Mergence options. Project Hivemind faces scalability challenges beyond its three-node design, and the connectivity and bandwidth demands, common to all blockchain solutions, can undermine the effectiveness of such systems in a ship-based context. Furthermore, if the nodes in Project Hivemind are already trusted authorities, the inherent property of distributed consensus among untrusted participants may become less essential. In scenarios where all participants are inherently trusted and have the authority to sign, the need for the consensus mechanism designed for untrusted parties is diminished. Emphasizing the trustworthiness of the entities involved instead, and appropriate training, could result in a more streamlined, efficient solution that may be preferable to blockchain in the context of maritime operations. Careful consideration of these challenges is essential before deploying any blockchain-based solution, like Project Hivemind, in maritime operations.

With Blockchain Mergence, we explored a potential approach to the integrity of AM data by showcasing the integration of CAC signatures within a conceptualized AM data flow. The Blockchain Mergence *local component* holds significant potential, given that the entities authorized to manage AM data are expected to be inherently trusted members with signing keys and the signature chain adds little functional overhead to the current architecture. The Blockchain Mergence local component also aligns well to supporting the proposed solution in Chapter 7. However, like for Project Hivemind, it was concluded that the Blockchain

Mergence *global (blockchain) component* might not be necessary within a shipboard setting due to blockchain's costs on bandwidth and the inherent trust in the participating nodes (e.g., approvers such as the PMA and CHENG).

8.1 Future Work

- A direct shipboard implementation and user study on the proposed solution for securing AM systems stands out as an essential initial step for future research.
- A wider participant pool for qualitative research could bolster any argument to be made for any lack of direction or guidance when it comes to securing AM data.
- The blockchain methodologies discussed in this thesis have not undergone testing within a ship's network, offering a potential realm for new discoveries or validation of theoretical conclusions.
- Conducting experiments to simulate malicious activities targeting AM data traffic holds promise for identifying subtle vulnerabilities within the AM data flow.

The landscape of AM data security remains an open book awaiting further exploration. Numerous uncharted territories and undiscovered insights will always beckon further investigation. However, the abundance of ideas and collective experiences within both the DOD and industry places this technology on a trajectory toward a more secure platform for AM data.

APPENDIX A:
Additive Manufacturing Security System Questionnaire

This survey uses 'AM schematic transfer' to include how 3D print schematics are generated, authorized, stored, and transferred. 'Instructions' for AM schematic transfer may include policy or official directions, namely formal processes, guidance documents, and procedures. 'Informal processes' for AM schematic transfer may include accepted practice at the command that is not documented, or other informal guidance given. Informal processes may also include guidance direction prepared by others working on AM, that has not yet been authorized as official policy.

If the question does not apply to your command, enter N/A.

Part I: Instructions and Guidance Documents

1. Is there an instruction that your branch or command uses when it comes to AM schematic transfer? Please provide the name of the instruction if possible.
2. How are these instructions helpful in practical system use contexts? Please explain your answer.
3. Does your command and/or other commands follow these instructions regularly?
4. Are there informal processes for AM schematic transfer that are not officially authorized but have been developed as 'good practice'/'normal practice'? If so, please explain what they are.
5. Do users have to undergo a qualification process before working with additive manufacturing at your command? If so, where? What does the qualification process cover?

Part II: Printer Types and Practical Schematic Use

6. What kind of printer does your command utilize? Provide the name of the model if possible.
7. Is the printer connected to the internet or does it operate on an isolated network?
8. Is there a centralized database to acquire pre-made AM schematics? If so, please provide the name.
    a. What kind of connection is used to connect to that database (Internet, VPN/intranet, email requests, etc.)?
    b. On a scale of 1 to 10, where 1 represents no edits and 10 represents a complete re-creation of the schematic, how much editing on average is normal after obtaining the AM schematic? Please explain.
9. How is an additive manufacturing schematic meant to be created and routed to your command's 3D printer? Include the titles of approving authorities and expected security practices if possible.
10. For the process described in the previous answer, what are the security measures for AM schematics transfer? Please elaborate.
11. What needs to be improved or changed to establish an efficient and secure additive manufacturing package flow?
12. Provide any other relevant information that pertains to your command or branch's existing AM security practices or design.

Part III: Demographic Questions

13. Are you currently:
    a. Active military or DoD civilian?
    b. If active military, which branch?
14. Current Rank:
15. Designator:
16. Which command are you currently stationed at?
17. How would you describe your technical background?
18. How many years of experience do you have working with additive manufacturing systems?
19. How long have you worked with additive manufacturing systems in the military/DoD?

APPENDIX B:
Exploration: Project Hivemind

Up to this point, we have analyzed several perspectives on AM data security while also identifying flaws, opportunities for improvement, and a baseline working solution. In the following two chapters, we will explore further solution proposals on the use of blockchain, and what further security guarantees it can provide as well as the usability considerations in employing it as an additional tool.

By delving into blockchain applications, we might be able to uncover additional security guarantees this technology can offer in the context of AM data and the specific architecture, or conversely indications that it is not necessary. This chapter will focus on Project Hivemind, and analyze how its security approach might be practical for users in the Fleet and beyond.

B.1 Hivemind Setup

For this thesis, a Project Hivemind prototype was delivered to the student from NSWC Carderock Division to aid in the research and further exploration of the technology. The assembly included two Dell laptops, each equipped with a 64-bit Windows 10 OS, along with a Prusa i3 MK3 3D printer linked to an Intel Next Unit of Computing (NUC) Pro i3, also known as a mini-computer, inside of a Pelican case. The printer was compatible with 1.75 mm filament material ranging from PLA to PETG. Initially, this design was built to center around an Ethernet-based connection. Table B.1 provides a simple look into the assembly along with the IP addresses of each device.

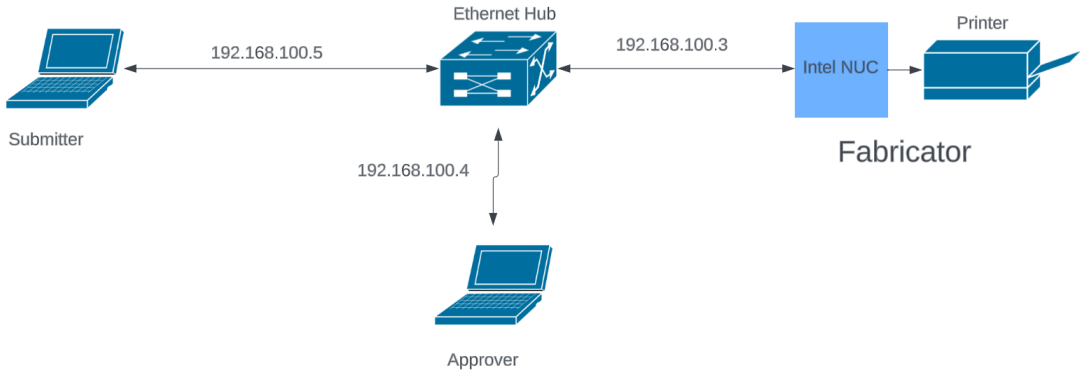

Figure B.1. Project Hivemind Ethernet Setup

Once all equipment was interconnected, Command Prompt was used to ping the other Dell Laptops, otherwise known as nodes henceforth, to confirm connectivity so that the process could begin. The Submitter has the choice of three base models to either submit directly or submit with edits to the next node, the Approver. The Approver has the power to analyze the part from the Submitter and either return the schematic back for readjustments or continue to send it to the Fabricator node.

At the Fabricator node, the NUC required a mouse and keyboard to be provided by the user in order to help maneuver the touchscreen monitor, but additional assembly was easily remedied. If the Approver adhered to guidance and submitted the schematic information correctly, then all that was necessary was for the Fabricator node to refresh. This would facilitate the addition of a new Transaction ID (TXID) to the blockchain along with the corresponding part information and pave the way for the subsequent processing by the Prusa printer. Multiple runs were taken through this step-by-step process to assess any signs of abnormalities.

Testing was previously conducted within the parameters of an Ethernet-connected environment [43]. To help build on the data surrounding this research and shed light on unexplored topics, we explored how Project Hivemind might work using a WiFi connection. This was constructed using an Xfinity home router connected to the open internet. Additionally, the

nslookup command in Command Prompt was used to discover the IPv4 addresses at each node. And since the Ethernet addresses had already been hard-coded into the Hivemind Python code, it was suspected that the same would be required for the WiFi addresses. Table B.2 represents the setup for a WiFi Hivemind run with appropriate IP addresses.

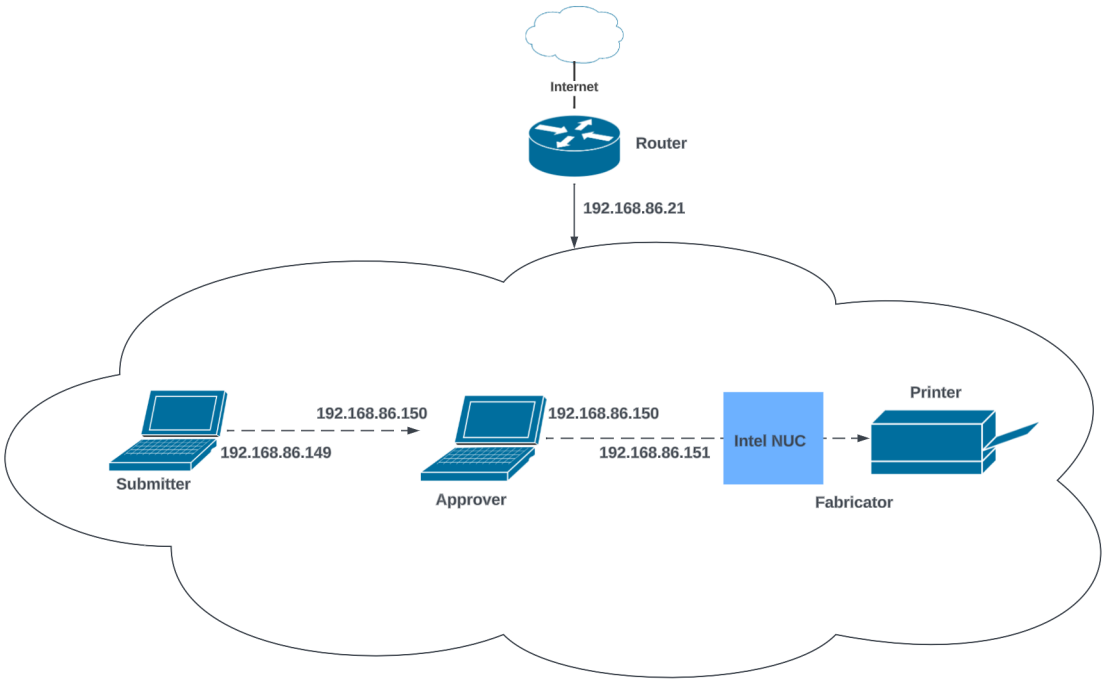

Figure B.2. Project Hivemind WiFi Setup

After the connection was assured amongst all nodes, the WiFi run presented no obvious signs of malfunction. To advance this analysis, the next phase involved conducting multiple runs to record data by examining latency-related patterns. This approach aims to discern how the AM data traffic behaves differently in a WiFi environment.

B.2 Hivemind Latency

To capture the required information for this experiment, we use Wireshark and a Python script to help process and visualize the latency and packet loss, across three successful

runs (out of ten attempted), including both Ethernet and WiFi connections. Given the limited sample size, predicting the average packet loss is impractical. Nevertheless, the packet loss samples obtained from one Ethernet run and three WiFi runs offer a preliminary intuition of the observed differences. Refer to Table B.1 for the packet loss data across these runs. The essential Python function developed to acquire latency information was titled `calculate_latency()` and centered around the `scapy` library to cycle through the `pcapng` files. The `matplotlib` library was then used to plot the data. The following is a snippet of code used for this purpose.

Category	Lost Packets	Total Packets	Packets Lost (%)
Eth_Submitter	0	1000	0.00%
Eth_Approver	9	1331	0.68%
Eth_Fabricator	57	1618	3.52%
Fabricator Run 1	153	1446	10.58%
Fabricator Run 2	54	999	5.41%
Fabricator Run 3	208	961	21.64%
Submitter Run 1	64	653	9.80%
Submitter Run 2	105	799	13.14%
Submitter Run 3	643	1093	58.83%
Approver Run 1	67	679	9.87%
Approver Run 2	53	566	9.36%
Approver Run 3	472	934	50.54%

Table B.1. Project Hivemind Packet Loss Results. The 'Category' column delineates various runs on each node within the Project Hivemind setup. Runs prefixed with 'Eth' denote nodes whose operations occurred over an Ethernet connection, while all other runs were executed using a WiFi connection, with corresponding run numbers assigned to each node.

```
from scapy.all import *
import numpy as np
import matplotlib.pyplot as plt

def calculate_latency(pcap_file):

  packets = rdpcap(pcap\_file)
  latencies = []

  prev\_timestamp = None

  for packet in packets:
    if hasattr(packet, "time"):
      timestamp = packet.time
      if prev\_timestamp is not None:
        latency = (timestamp - prev\_timestamp) * 1000.0  # Convert to
                                                          float (milliseconds)
        latencies.append(latency)
      prev\_timestamp = timestamp

  return latencies
```

To review, latency is the time it should take for data or a request to go from the source to the destination. It is usually measured in milliseconds (ms), and the closer it is to zero, the better [44]. The graphs represented in Figures B.3, B.4, B.5, and B.6. were developed to analyze the latency of an Ethernet-connected run alongside three WiFi runs from the Submitter, Approver, and Fabricator nodes.

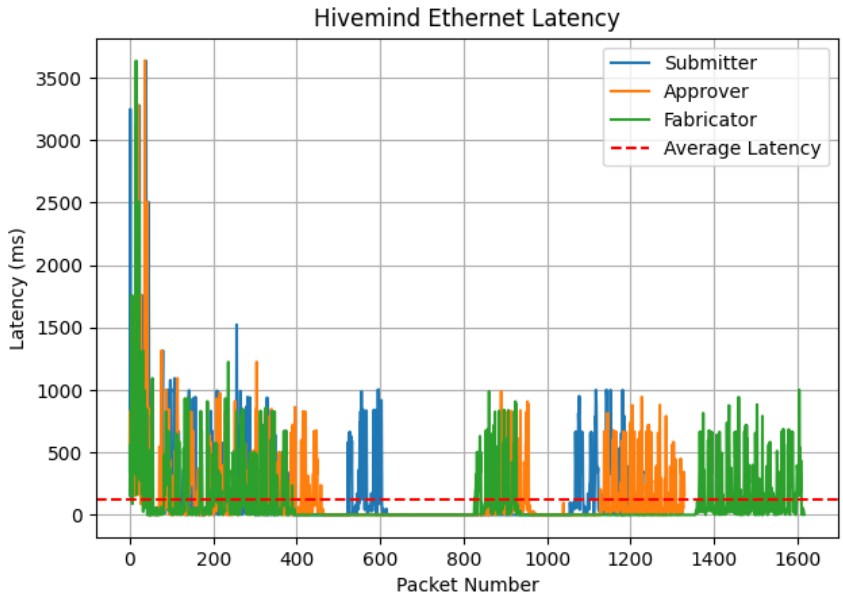

Figure B.3. Latency Over Ethernet Connection

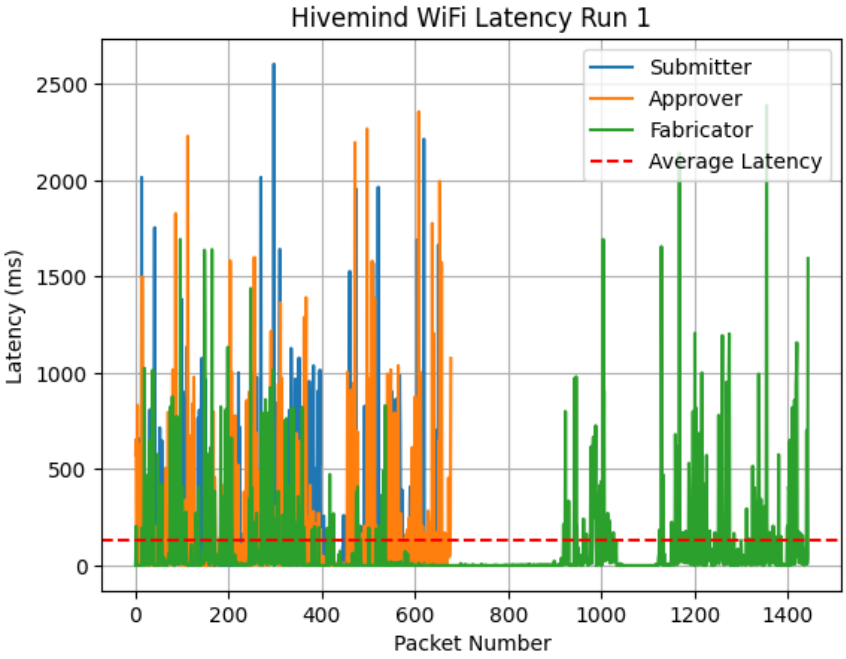

Figure B.4. Latency Over WiFi Connection: Run 1

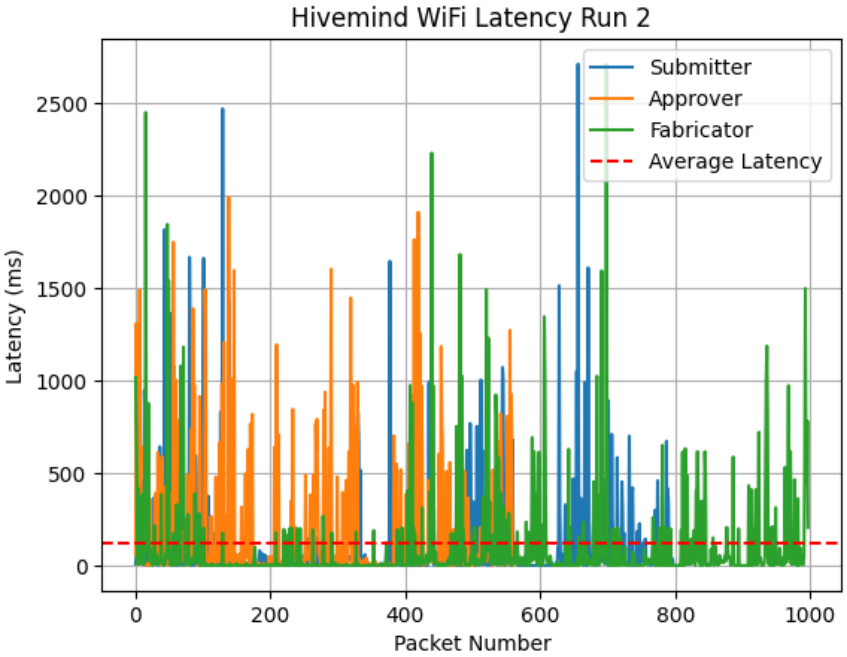

Figure B.5. Latency Over WiFi Connection: Run 2

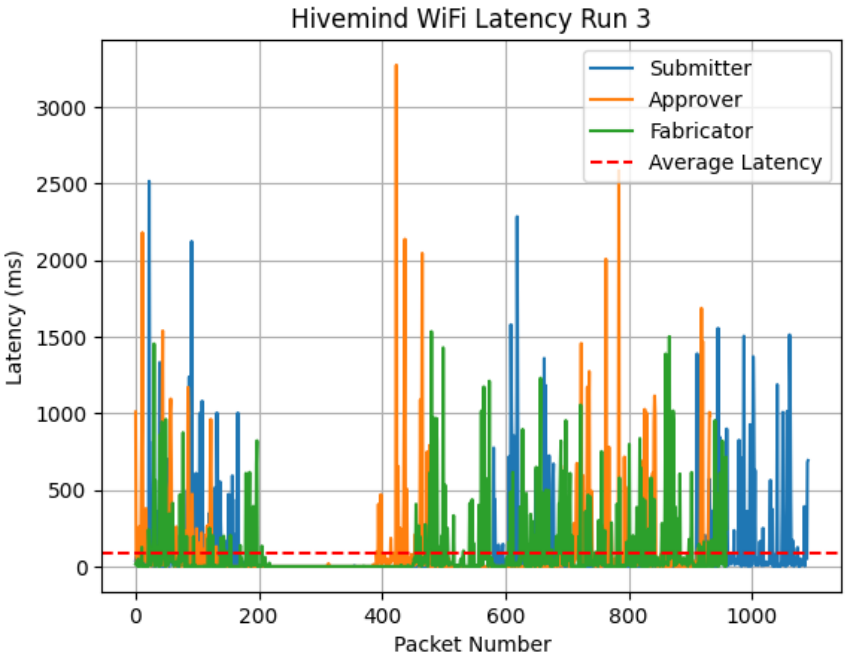

Figure B.6. Latency Over WiFi Connection: Run 3

High latency can indicate congestion, packet loss, or misconfiguration in the network. Looking at the various results from these latency measurements, it is clear that the Ethernet connection came out in front with the lowest latency, though that is to be expected. The spikes in latency are not so harsh compared to the WiFi tests, indicating a more efficient network. On the contrary, the WiFi results were sporadic and unpredictable, with signs of possible congestion or packet loss. Since this experiment was connected via WiFi to the open internet and transferred data without a firewall up and running, it can be predicted that such irregularities might have occurred.

The configuration process for this setup extended over several weeks, with unexpected bugs surfacing intermittently, posing challenges to the efficiency of subsequent runs. A total of ten test runs were carried out through both Ethernet and WiFi, a number influenced by challenges stemming from program and hardware issues, leading to unresponsiveness in some runs where data did not reach the Fabricator node. Out of these runs, only one on the Ethernet side successfully reached the Fabricator node. Graph B.3 illustrates the average latency throughout the Hivemind process, spanning from the Submitter to the Fabricator nodes. Meanwhile, for the WiFi setting, three successful runs were conducted, as depicted in graphs B.4, B.5, and B.6. These graphs individually showcase a glimpse into the latency behavior of the Submitter, Approver, and Fabricator, providing insights into their performance across the three runs.

This experimental exploration of Project Hivemind provides background on how the Hivemind setup functions. It shows preliminary insights on networking latency (Ethernet or WiFi) but is not intended as an exhaustive test. At three successful test runs, this represents a taste of investigation only.

B.3 Summary

In its current state, Project Hivemind stands as a commendable recommendation for securing AM data within a small, Ethernet-connected setting. However, the experiments' findings in a WiFi environment suggest that it may not be the most efficient option in such conditions. Given the intricate interplay of various components in the Fleet's AM data flow policies in Chapter 3,

APPENDIX C:
Exploration: Blockchain Mergence

In this appendix, we discuss a basic setup for experimentation with Hyperledger Fabric (HLF) to apply it to Blockchain Mergence. This is an example setup for use of the global blockchain component of Blockchain Mergence.

C.1 Understanding the Foundation

As mentioned in Chapter 2, Blockchain Mergence relies on using blockchain to build an updateable record management system that integrates an integrity-protected item history [19]. The primary tool used in these thesis to build an example of the global component stems from Hyperledger Fabric [45]. This tool is a powerful blockchain platform designed for businesses. It is "permissioned," meaning only known participants can join the network. An essential step in using Hyperledger Fabric for Blockchain Mergence is ensuring that each participant in the chain was able to authenticate themselves with the use of a CAC. Hyperledger Fabric uses PKI to ensure everyone on the network is who they say they are. Each node, network administrator, and user needs a public certificate and private key to prove their identity. These identities need to be issued by a trusted organization, and the military has several who could make use of this [45]. Fabric is also fast and efficient, and it does not require a cryptocurrency.

C.1.1 Installation

Installing the correct tools and software onto a Windows system was the first step. Up until this point, this project had only ever operated on a MacOS system and there were certain steps, according to the Hyperledger Fabric resources, that involved much more tedious detail on a Windows OS. The following applications and tools were used in the setup of Blockchain Mergence:

- **Docker Desktop:** an open platform that simplifies application development, deployment, and management. This must always be running in the background during testing.

- **WSL2:** Windows Subsystem for Linux ver. 2. This provides a bash environment for the Fabric samples, which can also be interpreted as a Linux environment.
- **Ubuntu-20.4:** stands in as a virtual environment used to run WSL2 inside the Windows OS.
- **Github:** used as a central software repository anytime changes were made to code.
- **Netbeans:** an integrated development environment for Java.
- **Another Neat Tool (ANT):** used for software compilation and running.

After installing all necessary components, the next step involved ensuring the existing product could run inside the new environment. After a few failed attempts, correct adjustments were made, and brainstorming could begin on building off of what had already been established.

The Fabric demonstration establishes a test network where only two peers can work and communicate with each other on what is called a channel where transactions are exchanged within the framework of an agreed-upon "smart contract" [45]. Smart contracts are programs that run on the Hyperledger Fabric blockchain and control how assets are created, changed, and transferred. To be valid, smart contract transactions typically need to be agreed upon by multiple organizations. Smart contracts are deployed on the network in packages called chaincode. Chaincode must be installed on the peers of an organization and then deployed to a channel before it can be used.

C.2 Translating and Developing the Model

An essential step is clearly conveying that each participant in the chain was able to authenticate themselves with the use of a CAC. Hyperledger Fabric uses PKI to ensure everyone on the network is who they say they are. Each node, network administrator, and user needs a public certificate and private key to prove their identity. These identities need to be issued by a trusted organization, and the military has several who could make use of this [45].

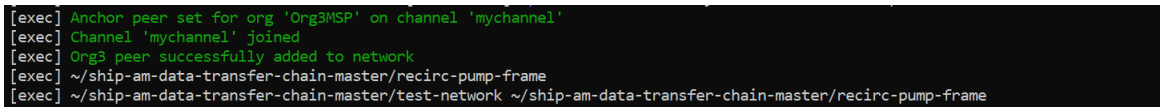

Figure C.1. Channel Addition of Third Party

The subsequent figures depict the story being told during the experimentation with the global component Blockchain Mergence setup. Initially designed with two entities on the blockchain, Figure C.1 illustrates the addition of a third party to the 'mychannel' channel. The network was then executed, showcasing a small-scale scenario where a submitter (FN Timmy), an offship entity (Fleet Technical Support Center, Pacific (FTSC PAC)), and the CHENG engaged in a network conversation, as illustrated in Figure C.2.

In this scenario, FN Timmy submits a request for approval of a 3D schematic (# 00001), authenticating with his CAC. FTSC PAC is depicted utilizing their CAC for authentication and stands by for assistance. The CHENG uses their CAC to acknowledge FN Timmy's request and approves the 3D schematic. Once officially approved, the CHENG successfully reissues the data back to FN Timmy, enabling him to proceed and route the approved data to the designated printing location, as illustrated in Figure C.3.

It should be noted that the above scenario uses the global component of Blockchain Mergence (i.e., recording on a blockchain) even though the scenario mirrors the case where the local component of Blockchain Mergence (ledger with signature chain) would be used. We apply this simply to show that Blockchain Mergence can thus function similarly to Hivemind, where the submitter and all approvers have recorded actions put on the blockchain, the difference being that in Blockchain Mergence each entity digitally signs to prove authority of the action.

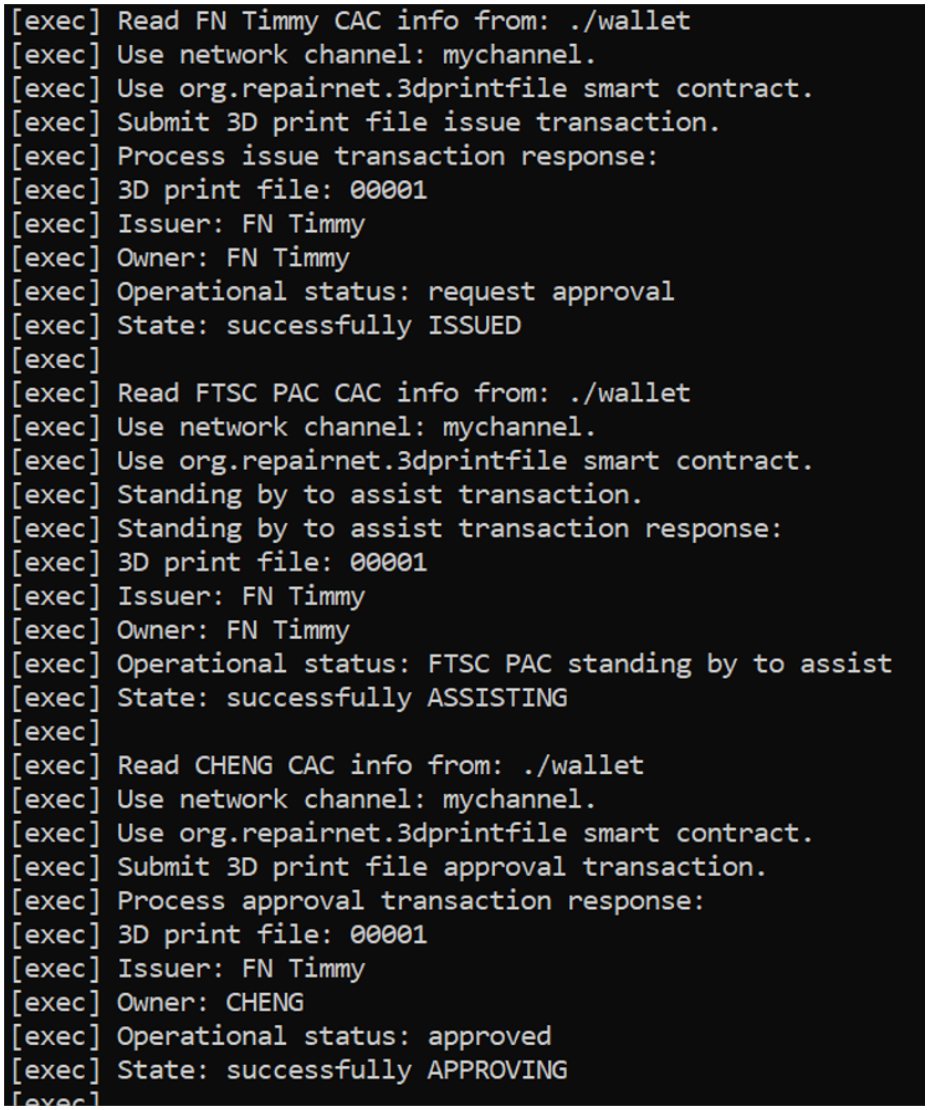

Figure C.2. Global Blockchain Mergence Component Example using HLF, authentication is established using FN Timmy's CAC and network is established. FN Timmy submits a 3D schematic as the owner and requests assistance/approval, FTSC PAC is added to the network standing by for assistance, CHENG's CAC is read and added to the network and shows CHENG's approval status of the 3D schematic. Transactions are exchanged within the framework of an agreed-upon "smart contract."

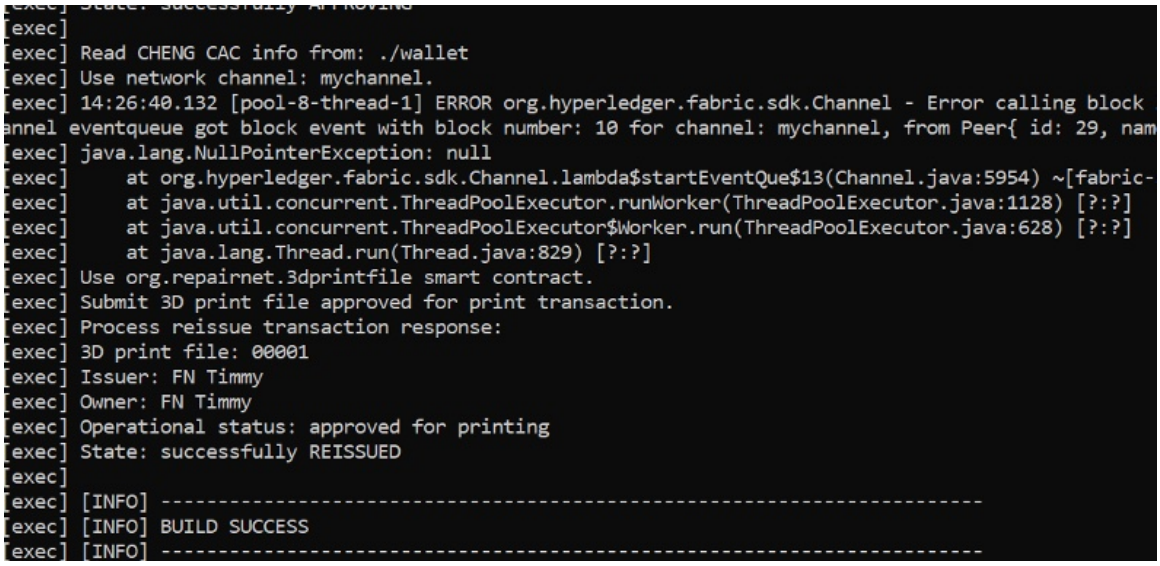

Figure C.3. Global Blockchain Mergence Component Example using HLF, end with truncated view. Status shows FN Timmy is in receipt of the 3D schematic, with a status of "successfully REISSUED."

Figure C.4. Global Blockchain Mergence Component Example Using Hyperledger Fabric, end with full view

List of References

[1] "What is blockchain and how does it work" [Online]. Available: https://www.synopsys.com/glossary/what-is-blockchain.html#:~:text=Definition,a%20timestamp%2C%20and%20transaction%20data.

[2] R. Linke. "Additive manufacturing, explained." Dec. 2017 [Online]. Available: https://mitsloan.mit.edu/ideas-made-to-matter/additive-manufacturing-explained

[3] L. M. Graves, J. Lubell, W. King, and M. Yampolskiy, "Characteristic aspects of additive manufacturing security from security awareness perspectives," *IEEE Access*, vol. 7, p. 103833–103853, Jul. 2019 [Online]. Available: https://doi.org/10.1109/access.2019.2931738

[4] S. E. Zeltmann, N. Gupta, N. G. Tsoutsos, M. Maniatakos, J. Rajendran, and R. Karri, "Manufacturing and security challenges in 3D printing," *JOM*, vol. 68, no. 7, p. 1872–1881, 2016 [Online]. Available: https://doi.org/10.1007/s11837-016-1937-7

[5] M. Yampolskiy *et al.*, "Security of additive manufacturing: Attack taxonomy and survey," *Additive Manufacturing*, vol. 21, p. 431–457, Apr. 2018 [Online]. Available: https://doi.org/10.1016/j.addma.2018.03.015

[6] P. Walters, "The risks of using portable devices," United States Computer Emergency Readiness Team, 2011 [Online]. Available: https://www.cisa.gov/sites/default/files/publications/RisksOfPortableDevices.pdf

[7] D. of Defense Chief Information Officer, "Online information management and electronic messaging," DOD INSTRUCTION 8170.01, 2019 [Online]. Available: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/817001p.pdf

[8] CDNetworks, "Data transmission: What is it? everything you need to know - CDNetworks," CDNetworks, 2021 [Online]. Available: https://www.cdnetworks.com/enterprise-applications-blog/everything-you-need-to-know-about-data-transmission/

[9] R. Lecount. "USB Flash Drive Malware: How it works and how to protect against it." Mar. 2021 [Online]. Available: https://www.thesslstore.com/blog/usb-flash-drive-malware-how-it-works-how-to-protect-against-it/

[10] M. Yampolskiy and J. Gatlin, "Data security in additive manufacturing," *Additive Manufacturing Design and Applications*, p. 1–7, 2023 [Online]. Available: https://doi.org/10.31399/asm.hb.v24a.a0006962

[11] R. Walsh. “Email security protocols: What are SMTP, TLS, S/MIME, etc..” Dec. 2020 [Online]. Available: https://proprivacy.com/email/guides/email-security-protocols

[12] J. Lubell, “Protecting additive manufacturing information when encryption is insufficient,” *Progress in Additive Manufacturing 2021*, p. 177–191, 2022 [Online]. Available: https://doi.org/10.1520/stp164420210125

[13] L. Haghnegahdar, S. S. Joshi, and N. B. Dahotre, “From IOT-based Cloud Manufacturing Approach to Intelligent Additive Manufacturing: Industrial internet of things—an overview,” *The International Journal of Advanced Manufacturing Technology*, vol. 119, no. 3–4, p. 1461–1478, 2022 [Online]. Available: https://doi.org/10.1007/s00170-021-08436-x

[14] S. Editor. “Shipping and maritime industry powered by cloud computing - sea news.” Aug. 2020 [Online]. Available: https://seanews.co.uk/shipping-news/shipping-and-maritime-industry-powered-by-cloud-computing/

[15] C. Nachreiner. “The security issues 3D printing should solve before going mainstream.” May 2020 [Online]. Available: https://www.helpnetsecurity.com/2018/08/08/security-issues-3{D}-printing/

[16] S. Nevil. “What is proof of work (POW) in blockchain?” May 2023 [Online]. Available: https://www.investopedia.com/terms/p/proof-work.asp

[17] A. Raja Santhi and P. Muthuswamy, “Influence of blockchain technology in manufacturing supply chain and logistics,” *Logistics*, vol. 6, no. 1, p. 15, 2022 [Online]. Available: https://doi.org/10.3390/logistics6010015

[18] V. Narula and P. Shrikrishna. “Additive manufacturing and blockchain.” Moog Inc. East Aurora, NY, USA. September 2017.

[19] B. Hale, D. Brutzman, and T. Norbraten, “Blockchain mergence for distributed ledgers supporting fleet logistics and maintenance,” Ph.D. dissertation, Graduate School of Defense Management, Naval Postgraduate School, Monterey, CA, 2021 [Online]. Available: https://dair.nps.edu/handle/123456789/4411

[20] S. Ziv, “Project hivemind architecture overview,” Naval Surface Warfare Center, Carderock, Mar. 2023.

[21] J. Straub, “3D printing cybersecurity: Detecting and preventing attacks that seek to weaken a printed object by changing fill level,” *SPIE Proceedings*, 2017 [Online]. Available: https://doi.org/10.1117/12.2264575

[22] S. Moylan, A. Cooke, K. Jurrens, J. Slotwinski, and M. A. Donmez, "A review of test artifacts for additive manufacturing," *National Institute of Standards and Technology: U.S. Department of Commerce*, May 2012 [Online]. Available: https://doi.org/10.6028/nist.ir.7858

[23] N. Banks, D. J. Ferreira, J. A. McCauley, J. T. Trinh, and K. S. Zust, "Navy additive manufacturing afloat capability analysis," M.A. thesis, Naval Postgraduate School, Monterey, CA, 2020 [Online]. Available: http://hdl.handle.net/10945/64681

[24] NAVSEA, "Navsea 05T afloat additive manufacturing," Surface Fleet Summit, 2023. 10-12 January 2023.

[25] L. C. Selby, *Guidance on the Use of Additive Manufacturing*, Ser O5T/2018-024, Department of the Navy. Washington, DC, USA, Aug. 2018.

[26] *Standard Operating Procedure for Additive Manufacturing Process and Procedures*, NAVAIRINST 4790.1, NAVAIR Sustainment Group. Patuxent River, MD, Mar. 2022.

[27] S. S. is a contributing writer for 3DSourced and S. is a contributing writer for 3DSourced. "Cnc vs 3D printing: Subtractive vs additive manufacturing." Nov. 2023 [Online]. Available: https://www.3{D}sourced.com/guides/cnc-vs-3{D}-printing/

[28] A. Parrott and L. Warshaw. "Industry 4.0 and the digital twin." May 2017 [Online]. Available: https://www2.deloitte.com/us/en/insights/focus/industry-4-0/digital-twin-technology-smart-factory.html

[29] N. PAC, "Digital advanced manufacturing ecosystem secureprint," Naval Information Warfare Center, Pacific, 2023.

[30] Printers (various), Ultimaker, New York, NY, USA, 2023. Available: https://ultimaker.com/3d-printers/.

[31] Printers (various), Stratasys, Eden Prairie, MN, USA, 2023. Available: https://www.stratasys.com/en/3D-printers/printer-catalog/fdm-printers/f900-printer/.

[32] United States Coast Guard, "Additive manufacturing part triage process," 2023. Chart was provided courtesy of the USCG.

[33] United States Coast Guard, "Sflc additive manufacturing criticality assessment process," 2023. Chart was provided courtesy of the USCG.

[34] United States Coast Guard, "Additive manufacturing technical data package development process," 2023. Chart was provided courtesy of the USCG.

[35] E. Muncy, “Additive manufacturing security system questionnaire 1,” Unpublished Thesis Questionnaire, 2023.

[36] E. Muncy, “Additive manufacturing security system questionnaire 2,” Unpublished Thesis Questionnaire, 2023.

[37] E. Muncy, “Additive manufacturing security system questionnaire 3,” Unpublished Thesis Questionnaire, 2023.

[38] E. Muncy, “Additive manufacturing security system questionnaire 5,” Unpublished Thesis Questionnaire, 2023.

[39] D. D. for Strategic Technology Protection and Exploitation, “Department of defense additive manufacturing strategy,” Joint Defense Manufacturing Council, Washington, D.C., Jan. 2021 [Online]. Available: https://www.cto.mil/wp-content/uploads/2021/01/dod-additive-manufacturing-strategy.pdf

[40] B. Hale and C. Komlo, “On end-to-end encryption,” Cryptology ePrint Archive, Paper 2022/449, 2022. https://eprint.iacr.org/2022/449 [Online]. Available: https://eprint.iacr.org/2022/449

[41] J. H. S. D. Allen, S. Administrator, and J. H. Svan. “DOD bans the use of removable, flash-type drives on all government computers.” Nov. 2008 [Online]. Available: https://www.stripes.com/news/dod-bans-the-use-of-removable-flash-type-drives-on-all-government-computers-1.85514

[42] K. C. Tran. “What is byzantine fault tolerance (bft)?: Beginner’s guide.” Jul. 2019 [Online]. Available: https://decrypt.co/resources/byzantine-fault-tolerance-what-is-it-explained

[43] S. Ziv, “Project hivemind: Blockchain for data integrity, usability, accountability, and scalability on the edge,” 2022. Presentation for NSWC Carderock Division.

[44] T. Keary. “Latency vs throughput - Understanding the difference; meaning.” Nov. 2022 [Online]. Available: https://www.comparitech.com/net-admin/latency-vs-throughput/

[45] GitHub. (2020). Repository for the Open-Sourced Hyperledger Fabric Framework Source Code. [Online]. Available: https://github.com/hyperledger/fabric#releases

Initial Distribution List

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California