5-14-2023

ENHANCING THE OPERATIONAL RESILIENCE OF CYBER-MANUFACTURING SYSTEMS (CMS) AGAINST CYBER-ATTACKS

Carlos Omar Espinoza Zelaya
Syracuse University

ABSTRACT

Cyber-manufacturing systems (CMS) are interconnected production environments comprised of complex and networked cyber-physical systems (CPS) that can be instantiated across one or many locations. However, this vision of manufacturing environments ushers in the challenge of addressing new security threats to production systems that still contain traditional closed legacy elements. The widespread adoption of CMS has come with a dramatic increase in successful cyber-attacks. With a myriad of new targets and vulnerabilities, hackers have been able to cause significant economic losses by disrupting manufacturing operations, reducing outgoing product quality, and altering product designs. This research aims to contribute to the design of more resilient cyber-manufacturing systems.

Traditional cybersecurity mechanisms focus on preventing the occurrence of cyber-attacks, improving the accuracy of detection, and increasing the speed of recovery. More often neglected is addressing how to respond to a successful attack during the time from the attack onset until the system recovery. We propose a novel approach that correlates the state of production and the timing of the attack to predict the effect on the manufacturing key performance indicators. Then a real-time decision strategy is deployed to select the appropriate response to maintain availability, utilization efficiency, and a quality ratio above degradation thresholds

until recovery. Our goal is to demonstrate that the operational resilience of CMS can be enhanced such that the system will be able to withstand the advent of cyber-attacks while remaining operationally resilient.

This research presents a novel framework to enhance the operational resilience of cyber-manufacturing systems against cyber-attacks. In contrast to other CPS where the general goal of operational resilience is to maintain a certain target level of availability, we propose a manufacturing-centric approach in which we utilize production key performance indicators as targets. This way we adopt a decision-making process for security in a way that is aligned with the operational strategy and bound to the socio-economic constraints inherent to manufacturing.

Our proposed framework consists of four steps: 1) Identify: map CMS production goals, vulnerabilities, and resilience-enhancing mechanisms; 2) Establish: set targets of performance in production output, scrap rate, and downtime at different states; 3) Select: determine which mechanisms are needed and their triggering strategy, and 4) Deploy: integrate into the operation of the CMS the selected mechanisms, threat severity evaluation, and activation strategy.

Lastly, we demonstrate via experimentation on a CMS testbed that this framework can effectively enhance the operational resilience of a CMS against a known cyber-attack.

ENHANCING THE OPERATIONAL RESILIENCE OF CYBER-MANUFACTURING SYSTEMS (CMS) AGAINST CYBER-ATTACKS

by

Carlos Omar Espinoza Zelaya
B.S., Universidad Católica de Honduras, 2015
M.Eng., Cornell University, 2020

Dissertation
Submitted in partial fulfillment of the requirements for the degree of
Doctor of Philosophy in
Mechanical and Aerospace Engineering.

Syracuse University

May 2023

ACKNOWLEDGEMENTS

I was born in La Ceiba, Honduras 29 years ago. My mother, Arely Zelaya dropped out of school and put everything aside to make sure I had what I needed. She nurtured me with love, patience, and discipline. She taught me to work diligently, serve others, and remain faithful to my values. Today's accomplishments are one of the many fruits of her arduous labor, this is for you mami. I also want to thank my dad Franklin Echenique, my sisters Andrea and Gisselle, and my aunt Margarita for always supporting me and making me feel loved. I've also been fortunate to have friends that have provided me with a space to be happy. In no particular order, I want to thank Manuel Salinas, Vinh Pham, Samuel and Christina Cantillo, Rafael Reyes, Roberto Salinas, Diego Ramos, Eduardo Rivera, Marcio Zelaya, Lucas Raley, Maggie Pacheco, Marvin Gonzalez, Michael Tjaden, Arturo Boquin, Jared Mudachi, Chelsea Boudin, Julie DeLeo, Noah Rolince, Ash Zheng, Cyrus Li, Hilary Paul, Javier Moreno, Antony Morales, and Emily Hillenbrand.

My academic career has been possible thanks to the support and guidance of great professionals. Thanks to Professor Cole for bringing me to SU, Professor Moon for advising me, and Karen Davis for making me feel welcome. Professor Eric Gentsch, Marcella Purcell, and Sheri Minarski were always big supporters of my dreams. Thanks to all of you. Seriously. This is for all of you.

Table of Content

Table List

Figure List

Abbreviation List

Machine to Machine	M2M
Cyber-manufacturing System	CMS
Programmable Logic Controller	PLC
Supervisory Control and Data Acquisition	SCADA
Decentralized Denial of Service	DDOS
Cyber-Physical Production Systems	CPPS
Intellectual Property	IP
Internet of Things	IoT
Industrial Control Systems	ICS
UK Financial Conduct Authority	FCA
National Institute of Standards and Techniques	NIST
Cyber-augmented Manufacturing Networks	CMN
Material Requirement Planning	MRP
Customer Relationship Management	CRM
Contemporary Cloud Manufacturing-as-a-Service	CMaaS
Cyber-Physical Systems	CPS

Chapter 1: Introduction

This section focuses on laying the foundation of three important concepts. Firstly, defining what is a Cyber-manufacturing System (CMS), its key characteristics, and its vulnerabilities. Secondly, a brief look at the advent of cyber-attacks against CMS and their operational disruption potential. Lastly, the need for enhanced operational resilience is presented as a way to address those threats.

1.1 Motivation

Cyber-manufacturing systems (CMS) are interconnected production environments composed of complex and networked cyber-physical systems (CPS) that can be instantiated across one or many locations (Khargonekar and Kurose, 2015). The widespread adoption of CMS has come with a dramatic increase in successful cyber-attacks (Oueslati et. al., 2019). With a myriad of new targets and vulnerabilities, hackers have been able to cause significant economic losses by disrupting manufacturing operations, reducing outgoing product quality, and altering product designs. For the second year in a row, manufacturing was the top attacked industry, according to the X-Force incident response data (IBM, 2023). This research aims to contribute to the design of more resilient cyber-manufacturing systems.

Traditional cybersecurity mechanisms focus on preventing the occurrence of those attacks, improving the accuracy of detection, and increasing the speed of recovery strategies. More often neglected is addressing how to respond to a successful attack during the time from the attack onset until the system recovery. We propose a novel approach that correlates the state of production and the timing of the attack to predict the effect on the manufacturing key performance indicators. Then a real-time decision strategy is deployed that selects the appropriate response to

maintain availability, utilization efficiency, and a quality ratio above degradation thresholds until recovery. Our goal is to demonstrate that the operational resilience of CMS can be enhanced such that the system will be able to withstand the advent of the attack while remaining operationally resilient.

1.2 Cyber-manufacturing systems (CMS)

Cyber-manufacturing systems (CMS) are interconnected production environments that are enabled by an interdisciplinary effort from theengineering, computer science, and information science domains. They are comprised of complex, networked cyber-physical systems (CPS) that may be instantiated at one physical location or distributed across many (Khargonekar and Kurose, 2015). They represent the manufacturing ecosystem transition (Ribeiro and Björkman, 2017) from integrated and centralized to shared and distributed systems (Li et. al., 2018).

A CPS is composed of highly integrated computation, communication, control, and physical elements (Chen, 2017). CPS adoption in production networks enables the new potential for improved efficiency, accountability, sustainability, and

scalability (Frazzon et. al., 2013). It intertwines industrial big data and smart analytics to discover and comprehend invisible issues for decision-making (Lee et. al., 2016). The resulting data mining techniques pave the way for intelligent manufacturing (Liu and Jiang, 2016) with real-time, dynamic, self-adaptive, and precise control (Ying et. al., 2018). Moreover, by utilizing advanced information analytics, networked machines will be able to perform more efficiently, collaboratively, and resiliently (Lee et. al., 2015). Analogous terms (Moghaddam et. al., 2018) include intelligent manufacturing (Zhong et. al., 2017), cyber-physical production systems (Monostori et. al., 2016), Industry 4.0 (Wang et. al., 2016) (Xu et. al., 2018), and cloud manufacturing (Tao et. al., 2011).

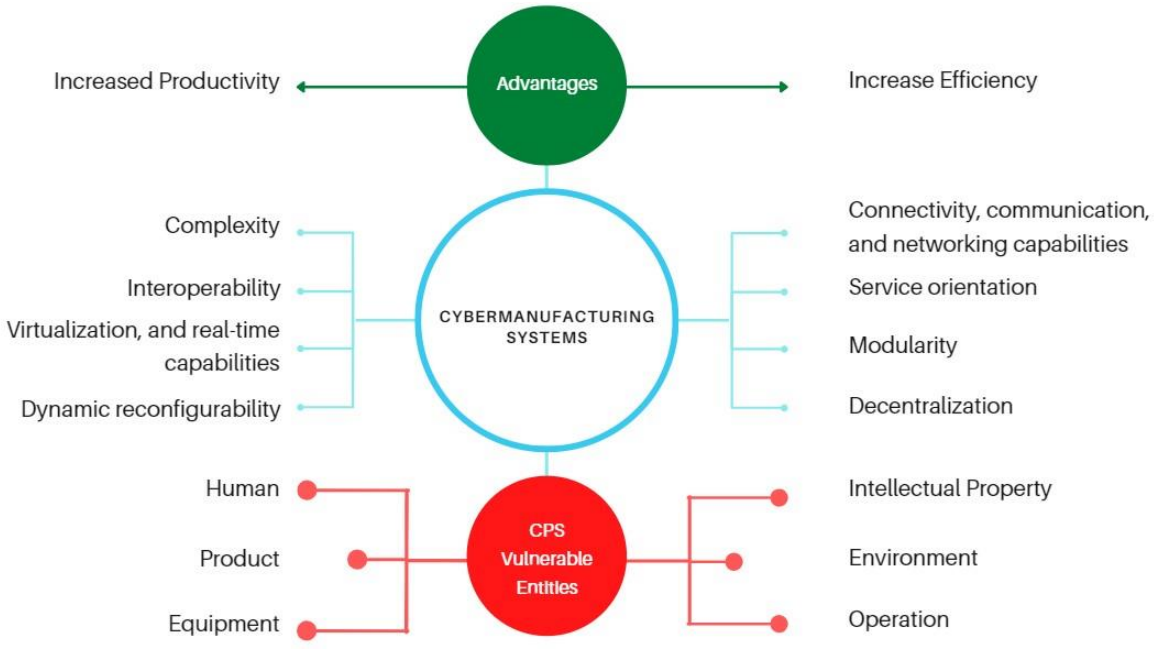

Figure 1: CMS characteristics, advantages, and CPS vulnerabilities

While CMS offers enhanced productivity and efficiency compared to traditional manufacturing (Jamwal et. al., 2020), its inherent properties open the door to new cybersecurity vulnerabilities (Pereira et. al., 2017). Cybersecurity threats have been recognized by industry and scholars as the top non-traditional risk (Department of Homeland Security, 2012) and information security risks (Atzori et. al., 2010).

The threats of Cyber-attacks manipulating the workflow system and processes are escalated through the challenges that are faced by the Industrial Internet. This can lead to disruption or outages causing enormous costs (Al-Salman and Salih, 2019). As outlined in the Industrie 4.0 roadmap (Kagermann et. al., 2013) in CPS-based manufacturing systems, it is not enough simply to add security features to the system at some later point in time. All aspects relating to safety, and in particular security, need to be designed into the system from the outset. According to a recent literature review (Alessia et. al., 2020), the following are common characteristics among factories that are transitioning towards the implementation of cyber-physical systems: (i) Complexity/heterogeneity encapsulation, (ii) Interoperability, (iii) Connectivity, communication, and networking capabilities, (iv) Service orientation, (v) Modularity, (vi) Decentralization, (vii) Virtualization, and real-time capabilities, (viii) Computational capabilities, (ix) Intelligence/smartness, (x) Cooperation, and collaboration, and (xi) Dynamic reconfigurability, and adaptability.

While all those characteristics are aimed towards increased efficiency and productivity, they open the door for new vulnerabilities that the traditional closed manufacturing systems were not exposed to. The following are cyber and physical entities that can be vulnerable to cyber-attacks: (i) Human, (ii) Product, (iii) Equipment, (iv) Intellectual Property, (v) Environment, and (vi) Operation (Wu and Moon, 2018). Figure 2 illustrates how we can represent the CMS as a series of Workstations, each of them comprised of Cyber-Physical Systems (Xu et. al. 2014), working together as a network to fulfill a target production goal. Their operation is governed by control systems that can include Supervisory Control and Data Acquisition (SCADA), Programmable Logic Controller (PLC) systems (Langmann and Stiller, 2019), sensing machine data systems (Leang et. al., 2019), and machine-to-machine (M2M) communication (Kim et. al., 2010).

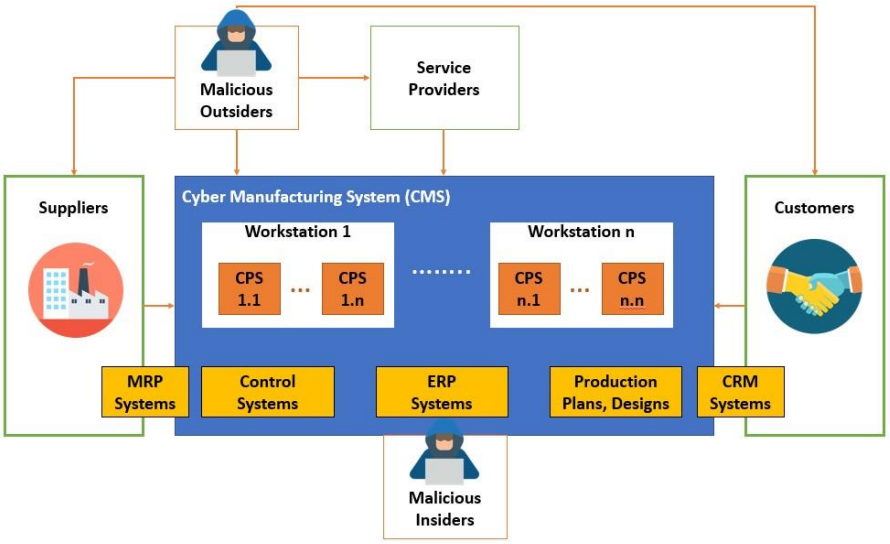

Figure 2: Sample generic layout of a CMS.

A general ledger of information on Finance, Human Resources, Manufacturing and logistics, Supply Chain Management, and Business Intelligence has been stored on Enterprise Resource Planning (ERP) software (Xu, 2011). More specific internal documentation on product specifications, designs, and production plans, is usually stored and executed in industry-specific software. The inherent nature of CMS is the close collaboration with suppliers and customers. This means developing integrations with Material Requirement Planning (MRP) in which procurement data is exchanged and orders are placed. From the customer perspective, setting in place Customer Relationship Management (CRM) as a tool to facilitate the logistics of how to get the products, in which amounts, and under what criteria to the final destination. Contemporary Cloud Manufacturing-as-a-Service (CMaaS) platforms now promise customers instant pricing and access to a large capacity of manufacturing nodes. clients can directly customize and configure parts parametrically, leading to an instant generation of downstream manufacturing processes (Hasan and Starly, 2020).

Added to the direct business partners, CMS also has a tight information relationship with other service providers. Auditors, consultants, outside maintenance calls, software support partners, collaborating companies, etc. All of these relationships have the aim to provide the CMS with value, as we mentioned before, however, this also opens the door to new attack vectors.

Malicious outsiders can find direct ways to target vulnerable components inside the CMS, but can also weaponize the connections established by suppliers, customers, or service providers to infiltrate and cause disruptions. While is more natural to think of these outsiders and build defense mechanisms to prevent their penetration, the advent of attack by insiders (Theoharidou et. al., 2005) is one of the most pernicious (Bishop et. al., 2014) given that they don't need to violate the access protocol.

The trustworthiness of subjects, the sensitivity of targets, and the applied security countermeasures need to be considered in the assessment of the likelihood of insider threats (Boulares et. al., 2017). Information security research is aiming to understand hackers, improve information security compliance, and mitigate cyber-physical threats (Crossler et. al., 2013).

1.3 Cyber-attacks against CMS

Recent years have seen a step increase in the materialization of cyber-attack threats against manufacturing (Oueslati et. al., 2019). For the second year in a row, manufacturing was the top-attacked industry, according to the X-Force incident response data (IBM, 2023). In 2022, backdoors were deployed in 28% of incidents,

beating out ransomware, which appeared in 23% of incidents remediated by XForce. Extortion was the leading impact on manufacturing organizations, seen in 32% of cases. Manufacturers notoriously have little-to-no tolerance for downtime, and this intolerance makes extortion a lucrative strategy for attackers. Data theft was the second-most common at 19% of incidents, followed by data leaks at 16% (IBM, 2023).

Table 1: Share of attacks by industry 2018 – 2022 (IBM, 2023).

Industry	2022	2021	2020	2019	2018
Manufacturing	24.8%	23.2	17.7	8	10
Finance and insurance	18.9%	22.4	23	17	19
Professional, business and consumer services	14.6%	12.7	8.7	10	12
Energy	10.7%	8.2	11.1	6	6
Retail and wholesale	8.7%	7.3	10.2	16	11
Education	7.3%	2.8	4	8	6
Healthcare	5.8%	5.1	6.6	3	6
Government	4.8%	2.8	7.9	8	8
Transportation	3.9%	4	5.1	13	13
Media and telecom	0.5%	2.5	5.7	10	8

Morphisec reported that one in five manufacturing companies in the U.S./U.K. has been victims of cyberattacks (Morphisec, 2021). Among the most common types of attacks are Malware (40%), Phishing (20%), DDOS Attacks (12%) (Mahjabin et. al., 2017), and Other / Unknown (11%). More concerning is that the average ransom paid has tripled to $321,000 and in 2020 the highest paid ever of $10 million. CISA Insights (CISA, 2021) even reported an increase in cyber-attack surface areas related to the COVID-19 pandemic.

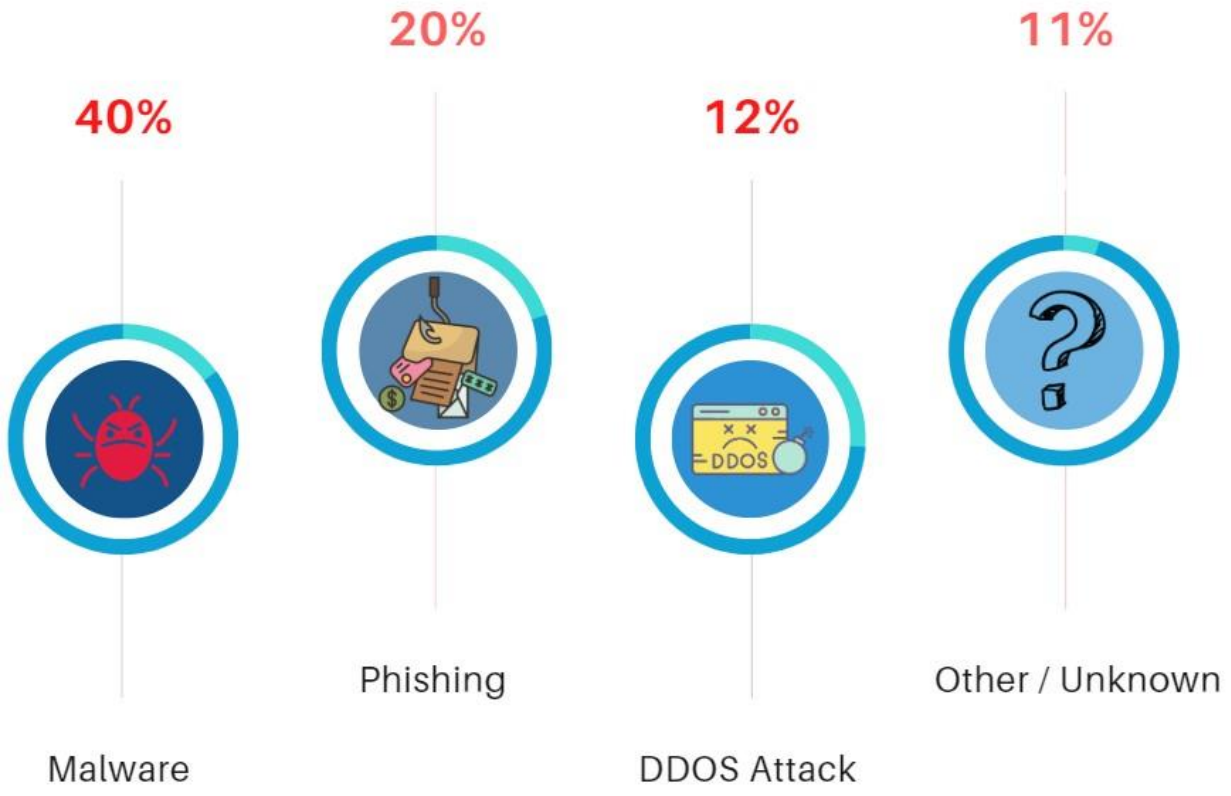

Figure 3: Most common attacks against CMS in 2021.

A recent taxonomy on the severity of cyber-attacks against CMS (Espinoza-Zelaya and Moon, 2022) classifies their effects around three themes:

(i) Operational Impact: The potential of a threat to inflict damage to the CMS such that the operations can't proceed as scheduled. This can either mean a disruption in the manufacturing operation, production quality, or product quality. Security incidents have consequences such as interruption or modification of an operational process, or sabotage to cause harm (Bicaku et. al., 2018).

(ii) Economic Impact: The direct monetary implications of dealing with the losses in production time, outsourcing production, backorder costs, extra hours, induced scraps, product quality, damage repair, and recovery. As well as the indirect costs of conducting forensic analysis, reporting security breaches, loss in public confidence, compromise to Intellectual Property (IP), implementation of new defense mechanisms, and associated training costs.

(iii) Nontangible Losses: Destruction or compromise of specifications, designs, data, and any other sensitive information. Enterprises have experienced cyberattacks that exfiltrate confidential and/or proprietary data, alter information to

cause an unexpected or unwanted effect and destroy capital assets (Hutchins et. al., 2015).

1.4 Recent attacks

The widespread adoption of CMS has come with a dramatic increase in successful cyber-attacks. With a myriad of new targets and vulnerabilities, hackers have been able to cause significant economic losses by disrupting manufacturing operations, reducing outgoing product quality, and altering product designs. Some notable examples are:

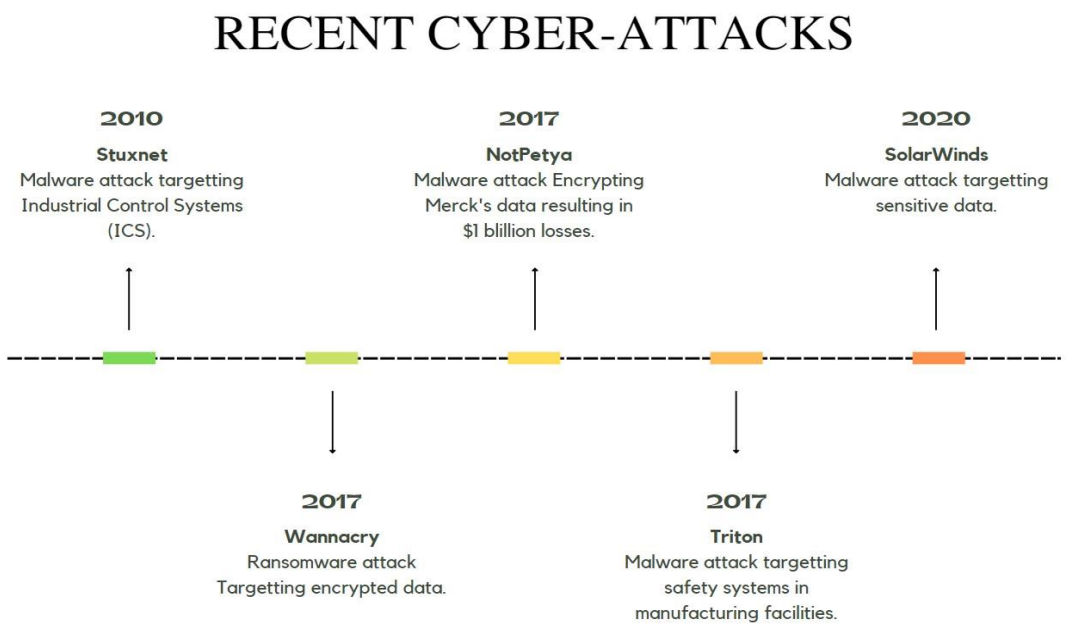

Figure 4: Recent cyber-attacks.

2010 - Stuxnet

The malware Stuxnet (Langner, 2011) was designed to sabotage the Iranian nuclear program by targeting industrial control systems (ICSs). Stuxnet target SCADA systems(Nicholson et. al., 2012) and interfered with the programmable logic controllers (PLC) (Ghaleb et. al., 2018) (Sandaruwan et. al., 2013). Stuxnet has challenged assumptions about environments not connected to the internet and the belief that network defenses will protect facilities from vulnerabilities in software applications (Collins and McCombie, 2012). The attack caused the fast-spinning centrifuges to tear themselves apart.

2017 – Wannacry

WannaCry ransomware (also known as Wana Decrypt0r, WCry, WannaCry, WannaCrypt, and WanaCrypt0r) was observed during a massive attack across multiple countries on 12 May 2017. According to multiple reports from security vendors, a total of 300,000 systems in over 150 countries had been severely damaged. The attack affected a wide range of sectors, including healthcare, government, telecommunications, and gas/oil production (Akbanov and Vassilakis,

2019). The attack exploited a vulnerability in the Windows operating system and demanded payment in exchange for restoring access to encrypted data.

2017 – NotPetya

In June of 2017, the biopharmaceutical company Merck & Co. was affected by the malicious worm NotPetya. The worm was based on ransomware, Petya, but it had been modified so that it was unable to revert its changes, resulting in the permanent encryption of data. Since the malware affected computer systems that are used to control Merck's manufacturing process, the attack resulted in shortages of the Gardasil vaccine and may have contributed to stock-outs of the Hepatitis B vaccine. The incident led Merck to borrow $240 million worth of Gardasil vaccine from the Center for Disease Control's stockpile, with a total estimated cost of the cyberattack close to $1 billion (Gutierres et. al., 2019).

2017 – Triton

This malware, discovered in 2017, was designed to target safety systems in industrial facilities, including those used in manufacturing. The hackers used

sophisticated malware, dubbed “Triton”, to take remote control of a safety control workstation. Some controllers entered a failsafe mode as the hackers attempted to reprogram them, causing related processes to shut down and allowing the plant to spot the attack (The Guardian, 2017).

2020 – SolarWinds

This cyber-attack targeted a software supply chain used by numerous organizations, including those in the manufacturing sector. The attack allowed hackers to gain access to sensitive data and systems across a range of industries. FireEye, a cybersecurity company, immediately tracked the attack back to a March 2020 update from SolarWinds, a Texas-based company that makes IT management software. The software in question, Orion, was corrupted by malicious code embedded in a software update that was then installed by around 18,000 SolarWinds customers. This kind of hack is known as a supply-chain attack since the infected software was corrupted during production and then pushed out by the victim company to its customers (Cianci, 2021).

1.5 Resilience

Dibaji (Dibaji et. al., 2019) proposes a framework to classify the mechanisms for a CPS to defend against cyber-attacks: (i) Prevention mechanisms: To postpone the onset of an attack, (2) Resilience mechanisms: To contain the maximum impact of the attack and operate as closely to normal as possible, and (3) Detection and isolation mechanisms: To identify the source of the attack, isolate the corrupted subsystems, and restore the normal mode as quickly as possible. From an operational perspective then, the notion of resilience becomes particularly interesting as it pertains to containing the attack and ensuring continued operation.

Figure 5: CMS defense mechanisms against cyber-attacks.

One of the earliest definitions of resilience was developed in 1973 in the study of ecological systems as follows: “The measure of the persistence of systems and the ability to absorb change and disturbance and still maintain the same relationships between state variables” (Holling, 1973). Another author (Bruneau et. al., 2003) defined resilience as “the ability of a system to reduce the chances of a shock, to absorb a shock if it occurs (abrupt reduction of performance) and to recover quickly after a shock (re-establish normal performance).” This later definition offers more insights into the systemic nature of resilience.

Figure 6: Resilience word cloud.

Starting from these definitions, many others have adopted the idea and defined what resilience meant in their fields. While all these definitions are unique to the characteristics of each system, common themes can be identified. The most common one is the ability to withstand a shock, followed by the speed of recovery. A less common but more comprehensive one is the systemic view that incorporates the previous two as equally important properties of a resilient system. The existing definitions of resilience can be classified into the following themes:

Emphasis on "Withstanding"

1 The measure of the persistence of systems and of the ability to absorb change and disturbance and still maintain the same relationships between state variables (Holling, 1973).

2 The capacity of a system to absorb a disturbance and reorganize while changing while retaining the same function, structure, identity, and feedback (Bruneau et. al., 2003).

3 Referring to the individual's predisposition to resist the potential negative consequences of the risk and develop adequately (Engle et, al., 1996).

4 The ability to sense, recognize, adapt, and absorb variations, changes, disturbances, disruptions, and surprises (Hollnagel et. al., 2006).

5 The intrinsic ability of a system to adjust its functioning before, during, or following changes and disturbances so that it can sustain required operations under both expected and unexpected conditions (Hollnagel et. al., 2010).

6 Resilience is the ability to withstand disruptions by maintaining functions and structures, reducing the magnitude/duration of disruptive states, and/or responding to disruptive events. Accordingly, resilience comprises both robustness (e.g., the capacity to absorb disruption shocks) and agility (e.g., the capacity to recover or reconfigure) (Mohsen et. al., 2019).

Emphasis on "Recovery"

1. The speed at which a system returns to a single equilibrium point following a disruption (Tilman, 1994).
2. The developable capacity to rebound from adversity (Luthans et al., 2006).
3. The speed at which a system returns to equilibrium after displacement, irrespective of oscillations indicates the elasticity (resilience) (Bodin et al., 2006).

4. Resilience is the fundamental quality to respond productively to significant change that disrupts the expected pattern of the event without introducing an extended period of regressive behavior (Home et al., 1997).
5. Resilience refers to the capacity for continuous reconstruction (Hamel et al., 2003).

Emphasis on "systemic ability"

1. Resilience can be understood as the ability of the system to reduce the chances of a shock, to absorb a shock if it occurs (abrupt reduction of performance), and to recover quickly after a shock (re-establish normal performance) (Bruneau et al., 2003).
2. Resilience is a property defined as the ability to withstand and recover from severe stresses induced by natural stresses or deliberate attacks (Dibaji et al., 2019).

The following observations can be made from these definitions: (i) Resilience is a systemic property, (ii) It deals with the ability to: a. Reduce the chance of failure, b. Withstand the effects of failure and c. Recover from failure, (iii) The source of failure can be the system itself, a natural disaster, or a deliberate man-

made attack. Given that resilience may not be an inherent property of CMS, it needs to be bestowed through the implementation of mechanisms. Following the observations that a resilient system (i) reduces the chance of failure, (ii) withstands the effects of failure, and (iii) recovers from failure.

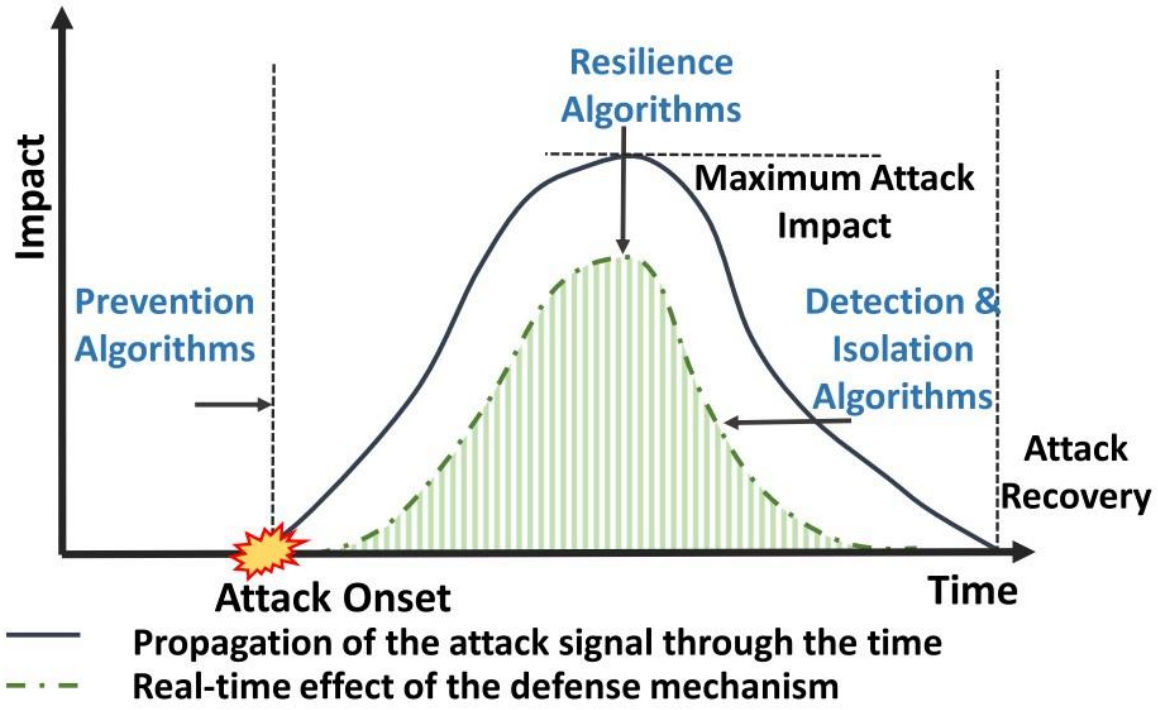

Figure 7:CMS defense mechanisms according to Dibaji et. al., 2019.

There exists an increasing academic interest in studying the resilience of engineering systems. In the context of supply chain management, a literature review (Tukamuhabwa et. al., 2015) found that while a wide range of strategies for

improving resilience is identified—such as redundancy, increasing flexibility, collaboration within the supply chain, improving agility among others; very limited research has been conducted into choosing and implementing an appropriate set of strategies for improving supply chain resilience. Much of the research has been conceptual, theoretical, and normative. When it comes to manufacturing, resilience is found as part of the "Triple R"—responsiveness and robustness, and resilience—and refer as the key objectives to gain a competitive edge (Kristianto et. al., 2017).

Resilience may not be an inherent property of the system and needs to be established by implementing resilience-increasing mechanisms (Dibaji et. al., 2019) Such mechanisms can be: (i) game theory, (ii) event-triggered control, (iii) mean subsequence reduced algorithms, or (iv) trust-based approaches. Applications of such methods have been seen especially in power and transportation systems applications. Defense mechanisms have been characterized as (i) prevention algorithms—to postpone the onset of an attack, (ii) resilience—to contain the maximum impact of the attack and operate as close to normal as possible, and (iii) detection and isolation—to identify the source of the attack, isolate the corrupted subsystems, and restore the normal mode as quickly as possible (See Fig 7).

1.6 Operational resilience

Operational resilience refers to the ability of an organization to continue operating through disruptive events, such as natural disasters, cyber-attacks, or other unexpected incidents. It involves the ability to absorb and adapt to shocks, maintain critical business functions, and quickly recover from disruptions. There are several definitions of operational resilience, including:

1. The National Institute of Standards and Technology (NIST) defines operational resilience as " The ability of an information system to continue to (i) operate under adverse conditions or stress, even if in a degraded or debilitated state while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs (NIST, 2011)".

2. The UK Financial Conduct Authority (FCA) defines operational resilience as " the ability of firms, financial market infrastructures and the financial sector as a whole to prevent, adapt and respond to, recover and learn from operational disruption (FCA, 2017)".

3. The extent to which a firm's operations can absorb and recover from disruptions. The disruption absorption dimension is defined as the ability of a firm to maintain the structure and normal functioning of operations in the face of disruptions. The recoverability dimension is defined as the ability of a firm to restore operations to a prior normal level of performance after being disrupted. (Essumann et. al., 2020).

A more refined definition is provided in NIST Special Publication 800-160, Volume 2, Revision 1 titled ”Developing Cyber-Resilient Systems: A systems security engineering approach” (Ross et. al., 2021): “operational resilient systems are those that can withstand cyber-attacks, faults, and failures and continue to operate in a degraded state to carry out their mission”. For the scope of this research, we define a resilient CMS as one capable of continued operation despite degradation in its performance product of the successful advent of a cyber-attack while maintaining KPI above acceptable thresholds. During this time the system will aim to: (i) minimize the degradation of performance, (ii) maximize availability, and (iii) ensure that ongoing functioning is correct. Resilience, however, is not an inherent property of CMS so it needs to be bestowed via the implementation of mechanisms.

For this dissertation, we will focus on those resilience-enhancing mechanisms that can be used in the time comprised from the attack onset until the system recovery. Thus, we propose the following categories for resilience-enhancing mechanisms: (a) adaptive response: dynamic reconfiguration, dynamic resource allocation, and adaptive management, (b) redundancy: backup, surplus capacity, replication, and (c) segmentation: predefined segmentation and dynamic isolation. A resilient CMS then should be able to assess in real-time the severity of the threat and respond with a mechanism that reduces the expected degradation of the system while satisfying the economic constraints (See Fig. 8).

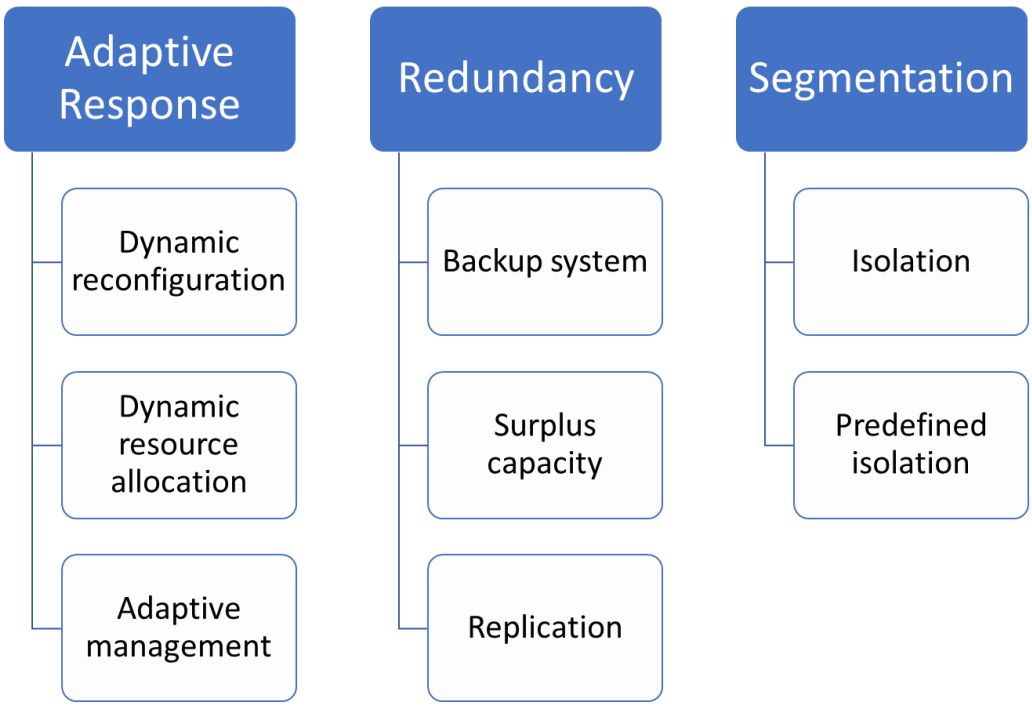

Figure 8: Resilience enhancing mechanisms classification.

Chapter 2: Problem statement

This chapter outlines the challenge that operational disruptions caused by cyberattacks pose for Cyber-manufacturing systems, highlights the call for increased resilience by government, academia, and industry; and presents a definition of the problem.

2.1. Cybersecurity operational risks of CMS

How to address system failures caused by cyber-attacks remains one of the main success factors in the widespread adoption of CMS. The impact of interruptions due to cyber-attacks ranges from loss in operational margins, to value reduction in stakeholder shares, and all the way to complete inability to recover. In 2012, the United States Secretary of Homeland Security, Janet Napolitano launched the first strategy document, "US Strategy for Global Supply Chain Security" (Department of Homeland Security, 2012) and called for increased global dialogue on risk and resilience. The goal of the strategy is to foster a global supply chain system that is prepared for, and can withstand, evolving threats and hazards and can recover rapidly from disruptions.

The World Economic Forum report titled “Building Resilience in Supply Chains” (Bhatia et. al., 2013) recognizes cyber risk as the most pressing non-traditional risk within a supply chain context, and perhaps the only issue where a seemingly small failure could cause rapid and widespread disruption. At the same time, Accenture research indicates that more than 80% of companies are now

concerned about supply chain resilience, significant supply chain disruptions have been found to cut the share price of impacted companies by 7% on average.

Such interruptions result in a significant penalty to the organization. This includes reductions in stock market value (Hendricks and Singhal, 2003) and declines in operating income, return on sales, and return on assets (Hendricks and Singhal, 2005). Further, there are even extreme cases where supply chains have completely collapsed and never recovered from disruption.

A recent taxonomy on the severity of cyber-attacks against cyber-manufacturing systems (Espinoza-Zelaya and Moon, 2022) categorized them into three general themes: i) Operational Impact: loss of effective production time due to inability to yield the expected output, ii) Economic Impact: direct financial costs (because of the attack, mitigation, or recovery), opportunity costs, and other indirect expenses, and iii) Intangible Losses: integrity breaches against original patents, loss of intellectual property (IP), ruined reputation or other intangible assets.

From a production manager's perspective, the goal is to utilize resources in the most efficient way possible to fulfill the production schedule. This means having enough capacity to overcome disruptions in manufacturing operations. The challenge of cyber-risk is that their effects are uncertain, and most of the time decisions need to be taken when the true potential has not been identified.

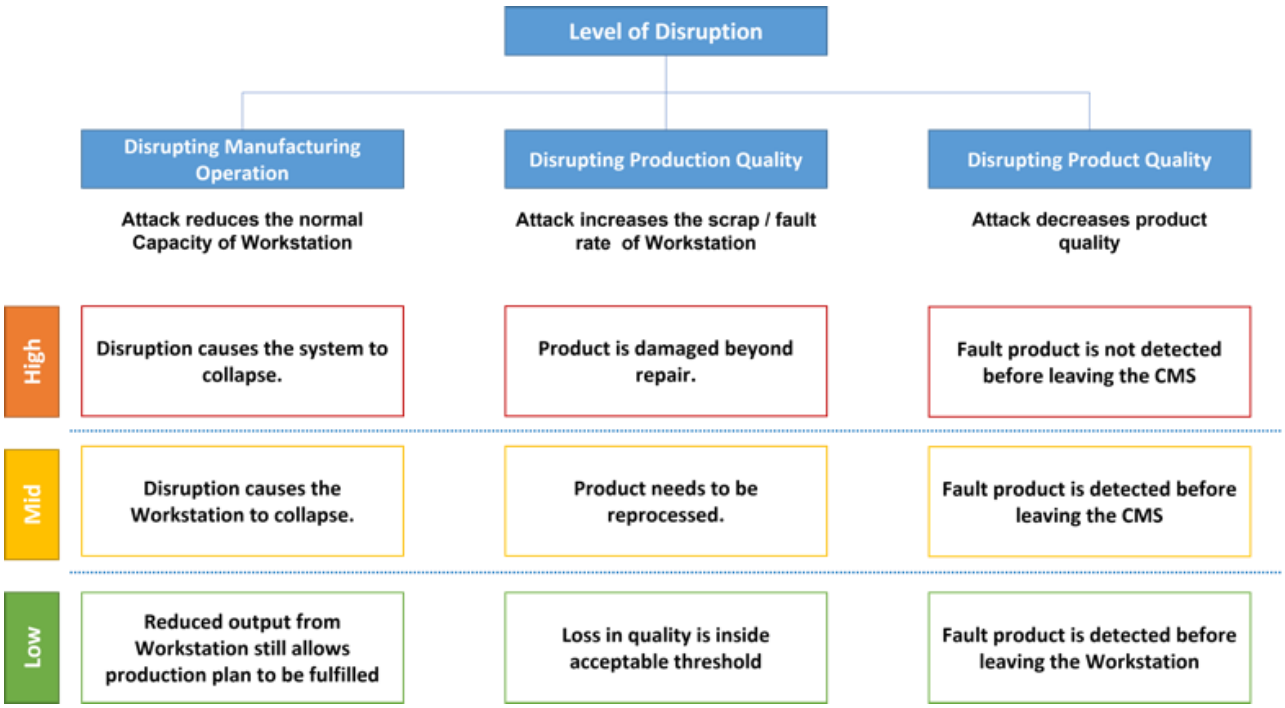

Figure 9: Operational impact level of disruption.

The operational impact that a cyber-attack can cause can be understood in its ability to disrupt three dimensions:

a) **Disrupt Manufacturing Operations:** The attacker can reduce the capacity of a workstation by compromising its CPS components, the control systems, or the production planning mechanisms. An example of this is a ransomware attack in which the perpetrator blocks a component and the CMS can no longer utilize it. A low-impact attack on this dimension would result in a reduced output in that workstation. While less than expected, the system can still fulfill its goals due to available overall capacity. A mid-impact disruption would be to deem that

workstation is nonfunctioning, while a high one would cause cascading disruptions affecting the system as a whole.

b) **Disrupting Production Quality**: The attacker can cause the workstation to produce subpar quality output. An example can be a spoofing attack in which the attacker feeds false data into the sensor of a machine causing it to damage the pieces as a consequence. The low impact would imply that while the system is compromised is still within the acceptable threshold. Mid-impact implies a scenario where the product needs to be reprocessed due to not being compliant with the specification, and a high impact is a situation where the product is damaged beyond repair.

c) **Disrupting Product Quality:** The threat can change the configuration, specification, or executive order of a given product. Attackers can change internal configurations of the product which can result in affected performance, while on the outside appearing normal. A low impact would be if non-compliance can be detected in the workstation and the malicious threat repaired. A mid-impact is the product being detected before leaving the CMS by the Quality Assurance mechanisms set in place. High impact is when these defective products reach the customers.

General considerations to measure the severity of each of these three dimensions are to evaluate the ability of the system to detect and characterize the damage potential of threats, to reduce the adverse effects, and to recover to normal functionality. At the same time the timing in which they all occur, as well as the state of the production system will determine how much damage they can all cause. There is not an absolute value of the severity of a threat that can be inferred just from the architecture of a system, but rather the impact is a function of the current conditions at the time of the advent of the cyber-attack.

2.2. Resilient cyber-manufacturing systems against cyber-attacks

A resilient CMS is one capable of detecting, withstanding, and recovering from failures induced by cyber-attacks while still fulfilling its expected levels of production and service with acceptable levels of security, integrity, and profitability. It is designed with an architecture that aids in the prevention of cyber threats, runs routinely anomaly detection tasks, withstands the adverse effects of unforeseen disruptions, and recovers to its normal state after isolating and expelling the malicious entities (Espinoza-Zelaya and Moon, 2021).

Furthermore, the following are characteristics of resilient CMS according to Espinoza-Zelaya and Moon:

(i) Is designed with an architecture that aids in the prevention of malicious external or internal threats.

(ii) Routinely runs jobs to detect anomalies on both cyber and physical components.

(iii) Systematically addresses the failure modes of its components and isolates disturbing effects before it collapses the whole system.

(iv) Expels malicious actors and fixes their access exploiting methods.

(v) Withstands the disturbance of a cyber-attack while continuing profitable operations.

(vi) Recovers from the attack before a critical window of time when the system collapses.

While the nature of resilience is systemic, the scope of this research is the ability to withstand cyber-attacks during the operational disruptions that arise from it until the recovery of the system.

2.3. Problem statement

Traditional cybersecurity mechanisms focus on preventing the occurrence of those attacks, improving the accuracy of detection, or increasing the speed of recovery. More often neglected is addressing how to remain operational during the window of time comprised from the advent of a cyber-attack until the system recovers. The need for trustworthy CMS capable of continued operation despite the advent of cyber-attacks calls then for increased operational resilience. Without adequate operational resilience, the CMS cannot withstand disruptions arising from cyber-attacks while maintaining availability, utilization efficiency, and a quality ratio above degradation thresholds until recovery. Failure to withstand the attack and maintain operational resilience results in system collapse. Resilience, however, may not be an inherent property of the system and needs to be bestowed by implementing resilience-increasing mechanisms.

Chapter 3: Literature Review and Research Objectives

The notion of bestowing cyber-physical systems (CPS) with resilience has seen an increased interest from the research community. The review of literature that focuses on that topic is presented, as well as the few that specifically refer to resilience applied to Cyber-manufacturing systems (CMS) under cyber-attacks.

Literature review

Bruneau (Bruneau et. al., 2003) defined a resilient system as one that shows: (a) Reduced failure probabilities, (b) Reduced consequences from failures, in terms of lives lost, damage, and negative economic and social consequences, (c) Reduced time to recovery (restoration of a specific system or set of systems to their "normal" level of performance).

Consequently, three categories will be utilized to classify the articles.

(i) Reduce Failure Probability: Mechanisms aimed to prevent the advent of a cyber-attack.

(ii) Reduce Consequences from Failure: From the onset of the attack, the explorations of mechanisms offset the effects and mitigate the damage.

(iii) Reduce Time to Recovery: Methods of returning to the initial state of the system before it was altered by the attacker.

A requirement for any article to be included in any category is that it needs to be applicable in the context of CMS under failure caused by a cyber-attack.

3.1 Objectives

(i) Identify existing resilience literature in other engineering fields that can be applicable in the context of resilient CMS under cyber-attacks.

(ii) Propose a classification framework.

(iii) Identify possible research gaps.

3.2 Methodology

The criteria for selecting papers for this review are as follows:

1. Articles published up to August 2022 in a peer-reviewed, archival journal.
2. Articles containing the keywords:
    a. Resilience
    b. Manufacturing/network / CPS
3. Articles will be classified according to the framework:
    a. Reduce Failure Probability
    b. Reduce Consequences from Failure
    c. Reduce Time to Recovery

4. Articles that deal with resilience against sources of disruption other than cyber-attacks will also be included. Given that they need to have a global understanding of what it means for a CMS to be resilient.

It is important to note that they may exist other existing papers that were not included in this survey. Given that resilience may not be an inherent property of CMS, it needs to be bestowed through the implementation of mechanisms (Espinoza-Zelaya and Moon, 2022). Following the observations that a resilient system (i) reduces the chance of failure, (ii) withstands the effects of failure, and (iii) recovers from failure, categories of resilience-increasing mechanisms are:

1. reduce the probability of successful cyber-attacks,
2. reduce the time to detection of cyber-attacks,
3. reduce the adverse effects of successful cyber-attacks, and
4. reduce the time to recover from cyber-attacks.

Next, examples of such mechanisms in each of the categories are presented. Resilience-increasing mechanisms are listed in no particular order as their effectiveness depends on many factors that are specific to CMS.

3.3 Reduce the probability of a successful cyber-attack.

The first line of resilience-increasing mechanisms is those that make it harder for an attacker to successfully perform exploitation. Usually, these mechanisms are set in place during the design stage of CMS. Their implementation involves the assessment of the threats, the system vulnerabilities, and the selection of appropriate counter measures.

A clear example is Cyber resilience protection for the industrial internet of things: A software-defined networking approach (Babiceanu et al., 2019). In this work, the author proposes an integrated modeling environment in which a virtual manufacturing system is ensured through cybersecurity and resilience mechanisms. Resilience is demonstrated by the system restoring itself to the required state after the security breach, by isolating the penetrated components and re-distributing the tasks among the non-affected components. Later the author outlines a series of trustworthiness requirements (Babiceanu et. al., 2020) where trustworthiness is defined to complement system dependability requirements with cybersecurity requirements, such that the resulting manufacturing cyber-physical system delivers services that can justifiably be trusted.

Open manufacturing: a design-for-resilience approach (Kusiak et al., 2020) shows a complexity reduction algorithm that addresses resilience at the design stage. A framework for Model-Driven Engineering of resilient software-controlled systems (Parri et al., 2021) provides a hardware/software framework supporting operation and maintenance of software-controlled systems enhancing resilience by promoting a Model-Driven Engineering (MDE) process to automatically derive structural configurations and failure models from reliability artifacts.

While traditionally authors have focused on threats coming from outside actors, a recent surge of literature exposes the liabilities that can come from insiders who already have access to the CMS and prose a threat. Security Enhancement Against Insiders in Cyber-Manufacturing Systems (Song et al., 2020) proposes an applied blockchain architecture. The paper demonstrates how blockchain technology can help prevent the data from unintended manipulation or data injection by insiders.

Another application of blockchain in preventing threats can also be found in Design Guidelines and a Prototype Implementation for Cyber-Resiliency in IT/OT Scenarios based on Blockchain and Edge Computing (Balistri et al., 2021). The authors utilize Blockchain to securely store in distributed ledgers topology information and access rules, maximizing the cyber-resiliency of industrial networks. Copyright protection (Holland et. al., 2017) is addressed with the use of

digital rights management as a key technology for the successful prevention of intellectual property theft.

Other studies show the adversarial nature of defending against threats and how those mechanisms should incorporate the ability to deal with an intelligent adversary. In Advancing Cyber-Physical Systems Resilience: The Effects of Evolving Disruptions (Nguyen et al., 2019) the authors build an adversarial network that learns the behavior of the system to improve its attacks. This allows us to build a more resilient system that can counter better an attacker that does not just perform random attacks, but intelligent and effective incursions. A final example can be found in the predictive formal analysis of resilience in Cyber-Physical Systems (Mouelhi et. al., 2019) which explores the capability of a system to maintain a safe operation within its ambient environment.

It is natural to put a lot of emphasis on preventing attacks from occurring, but as we have learned from multiple intrusion reports across all industries in recent years, it is always possible that an attacker can breach security mechanisms. It is then a concern of a resilient CMS for the active monitoring of possible attacks. Reducing the time in which the system can identify a threat has a direct effect on reducing the potential failure that can arise from it. In Towards Industrial Intrusion Prevention Systems: A Concept and Implementation for Reactive Protection. (Vargas et al.,

2018) the authors show how to detect intruders as soon as they ensure to respond to them promptly. This paper addresses this issue by introducing a concept for reactive protection that integrates the automatic execution of active responses that do not influence the operation of the underlying Industrial Automation System.

A particular characteristic of CMS is the presence of both cyber and physical data. Traditional IT methods usually focus on performing detections of anomalies purely with digital readings. In Alert Correlation for Cyber-Manufacturing Intrusion Detection (Wu et al., 2019) the authors illustrate an alert correlation method based on temporal and attribute-based similarity analyses. Intrusion detection message exchange format (IDMEF) is introduced, along with a new physical intrusion detection alert (PIDA) format for reporting and correlating physical alerts with cyber alters.

Validation of the integrity of data is another way in which breaches can be identified before failures have occurred. In A Recursive Watermark Method for Hard Real-Time, Industrial Control System Cyber-Resilience Enhancement (Song et al., 2020) a novel recursive watermark (RWM) algorithm for hard real-time control system data integrity validation is presented. A recent architecture for preventing and detecting cyber-attacks in cyber-manufacturing systems (Prasad and Moon, 2022) highlights the importance of addressing those risks from the design stages.

Similarly, the need for personalized production in supply chains requires a system that can achieve recoverability for operation resilience as outlined in the architectural framework for a cyber-physical logistics system for a digital-twin based supply chain (Park et. al., 2020).

3.4 Reduce adverse effects of a successful cyber-attack.

The crucial window of time in which a cyber-attack is successful and the system has been contained is where the majority of the losses occur. As we explored before, the main characteristic of a resilient system is the ability to withstand this phase. Perhaps one of the most obvious mechanisms to withstand losses is the inclusion of redundant components that can replace the compromised parts of the CMS and keep production going. In Cyber-Physical Systems, a new formal paradigm to model redundancy and resiliency (Lezoche et al., 2018) we are presented with a way to optimize the modeling of CPS systems emphasizing their redundancy and resiliency.

The study of manufacturing networks under disruption requires the ability to understand in real-time the state of the system. Resilience informatics for Cyber-augmented Manufacturing Networks (CMN): Centrality, flow, and disruption (Nguyen et al., 2018) presents a Cyber-augmented Manufacturing Network (CMN)

model along with three informatics developed for understanding resilience. The CMN model captures the main components of a manufacturing network under disruption and their relationships. The three informatics and their eight indices provide important insights into the manufacturing networks under disruption.

Another challenge that needs to be addressed is how the control hierarchies affect the CMS's ability to withstand disruptions. Paradigm shifts toward distributed manufacturing control architectures are explored in the Resilience of cyber-physical manufacturing control systems (Mohsen et al., 2019). It aims to answer the question of how the transition to semi-heterarchical control structures affects the resilience of manufacturing control structures against cascade and non-cascade disruptions in the control process.

During the withstanding phase, the CMS needs to be able then to take real-time decisions that minimize the impact of the attack. In Resilient control for serial manufacturing networks with advance notice of disruptions (Hu et al., 2013) the authors explore Real-time resilient control for manufacturing systems through mathematical analysis. An optimal control problem is developed for a simple type of serial network called a Decreasing Storage Cost and Decreasing Capacity (DSCDC) network given disruptions with a warning.

The notion of resilience involves the ability of the system to adapt to better withstand. CPS-Based Self-Adaptive Collaborative Control for Smart Production Logistics Systems (Guo et al., 2021) illustrates a self-adaptive collaborative control (SCC) mode is proposed for smart production-logistics systems to enhance the capability of intelligence, flexibility, and resilience.

Newer trends like the Digital Twin (DT) and Reinforcement Learning (RL) can also be used to enhance the resilience of the system. The treatment of the withstanding phase as an optimization problem can aid in the identification of optimal policies to reduce losses. In Digital Twin and Reinforcement Learning-Based Resilient Production Control for Micro Smart Factory (Park et al., 2021) the RL policy network is learned and evaluated by coordination between DT and RL. The DT provides virtual event logs that include states, actions, and rewards to support learning. These virtual event logs are returned based on vertical integration with the MSF. As a result, the proposed method provides a resilient solution to the CPPS architectural framework and achieves appropriate actions for the dynamic situation of a micro smart factory.

A New Concept of Digital Twin Supporting Optimization and Resilience of Factories of the Future (Bécue et. al., 2020) introduces a holistic Digital Twin approach integrating models of human behavior and capacities for security testing that can enable new services for the optimization and resilience of factories of the

future. Control applications that require hard real-time channels are highlighted in a recursive watermark method for hard-time industrial control system cyber-resilience enhancement (Song et. al., 2020). Blockchain applications for cyber-physical systems in manufacturing (Ho et. al., 2019) proposes a framework that involves the utilization of secondary validation and collaborative distribution concepts. Conventional and blockchain manufacturing simulators were developed to investigate the effects of blockchain technologies on manufacturing systems in terms of time and product quality.

A final question that arises naturally is which measures are more appropriate measures to quantify resilience. In Resilience Quantification for Probabilistic Design of Cyber-Physical System Networks (Wang et al., 2018) the authors present generic system performance metrics, which are entropy, conditional entropy, and mutual information associated with the probabilities of successful prediction and communication. A new probabilistic design framework for CPS network architecture is also proposed for resilience engineering, where several information fusion rules can be applied for data processing at the nodes.

3.5 Reduce the time to recover from a cyber-attack.

Lastly, a resilient system should set in place recovery mechanisms that allow a prompt transition to its normal state. It should also include the ability to incorporate learning from the attack into the prevention mechanisms to mitigate the risk of it occurring again. In SVM-Based Dynamic Reconfiguration CPS for Manufacturing (Shin et al., 2018) modeling of a shopfloor and a dynamic reconfigurable CPS scheme is presented that can predict the occurrence of anomalies and self-protection. The authors utilize a Support Vector Machine to restrain overloading in the manufacturing process. In addition, a CPS framework based on machine learning for Industry 4.0 is developed that can dynamically reconfigure through self-healing.

3.5 Ad-hoc results

The research interest in resilience in the context of CPS is relatively new. Most papers presented in this literature review are from within the last five years. As a complement to the direct results, we also performed a reference-checking process to identify relevant papers that could also help understand the current state of the art. Table 2 provides a list of such articles.

Table 2: Ad hoc literature review results.

Journal	Article Name	Total Articles
Procedia Manufacturing	Through-life cyber resilience in future smart manufacturing environments. A research program.	1
International Journal of Industrial Engineering: Theory, Applications, and Practice	Adaptivity of complex network topologies for designing resilient supply chain network	1
International Journal of Production Research	A control engineering approach to the assessment of supply chain resilience	1
Expert Systems with Applications	Intelligent contingent multi-sourcing model for resilient supply networks	1
ASME Journal of Mechanical Design	Resilience-Driven System Design of Complex Engineered Systems	1
Risk Management	Improving the Resilience and Performance of Organizations Using Multi-Agent Modelling of Complex Production-Distribution Systems	1
Production Planning & Control	A digital supply chain twin for managing the disruption risks and resilience in the era of Industry 4.0	1

3.6 Analysis

While currently there is a common notion of the importance of cybersecurity many authors mention how in the manufacturing field, this is a relatively new priority. Thus, a lot of these large legacy systems have been built without the awareness of the economic implications that can cascade from failures induced by cyber-attacks. The general direction of the field is steaming from the study of Cyber Physical Systems. While CMS is composed of CMS there exist many inherent differences dealing with the nature of manufacturing, the ever-changing customer requirements, and the uncertainty that arises from dealing with stochastic demand for products. The study of resilience thus also includes the ability to withstand variation in demand, breakdowns, system reconfigurations, and our specific topic, the advent of cyber-attacks.

The requirements to satisfy the security constraints while fulfilling the demand in a profitable way make this a valuable challenge. The implementation of resilience mechanisms needs to bestow the CMS with the ability to reduce the probability of an attack, withstand the adverse effects, and recover from it. Some general observations that can be done from the studying of the papers included in this survey are as follow:

- One key factor for the widespread adoption of CMS / Industrie 4.0 / Smart Factories and analogous is the ability to face cybersecurity risks. Resilience against such threats will be an effective systemic ability.

- Inherently a CMS is not resilient against the myriad of threats it can face. A strategy needs to be implemented to deal with cyber-attacks in an economically viable way.

- Resilience has been studied in the context of CPS, and while a lot of these insights and mechanisms can be applied to CMS further analysis needs to be done to incorporate the production-specific factors.

- Any effective strategy to bestow a CMS with resilience needs to address the different sources of disruptions on top of cyber-security. Thus, the alignment with the operational strategy is a key success factor.

3.6 Research direction

Security against cyberattacks is a key success factor for the adoption of a Cyber Manufacturing System. In the fulfillment of this goal, resilience is a promising

research field. Research directions identified by the authors of the papers included in this paper can be grouped as follows:

Simulation

- Implementation of IoT (Gubbi and Buyya, 2013) testbed with cyber resilience scenario simulation and testing the ability of the simulated SDN network to maintain the system in its required state of security.
- Implementation of Blockchain towards increase resilience in real-world industrial plants.

Modeling

- Manufacturing Networks design and redesign based on the support of resilience informatics.
- Frameworks and principles of Manufacturing Networks resilience control and management.
- Validation of resilience informatics in general Manufacturing Networks models.
- Utilize Reinforcement Learning towards system self-global redundancy modeling.

Real-Time Decision Making

- Interaction dynamics and protocols from a multi-agent systems standpoint incorporate the heterogeneity and dynamism of industrial control units.
- Real-time control policies for achieving resilient operations under disruptions.

Metrics

- Define more adequate resilience metrics for control systems.

3.7 Research Objectives

Hypothesis

"Enhancing the operational resilience of a cyber-manufacturing system enables it to withstand the advent of a known cyber-attack without experiencing degradation on its manufacturing Key Performance Indicators (KPIs) below thresholds."

Objectives

1. To develop a framework to enhance the operational resilience of a CMS against known cyber-attacks.
2. To demonstrate the severity of a cyber-attack against a CMS is correlated with the state of the system at the time of the advent.
3. To demonstrate via experimentation on a testbed the resilience of a CMS against known cyber-attacks.
4. To compare a traditional availability-driven cyber-security approach against the operational resilience framework.

Chapter 4: Enhancing the resilience of CMS against operational disruptions.

The previous chapters presented the challenge that cyber-manufacturing systems face from operational disruptions that arise from cyber-attacks. As the notion of enhancing operational resilience arises in recent literature as an effective way to ensure continued operation under degradation in performance, the natural question of how to bestow a CMS with it follows. This chapter outlines this dissertation's hypothesis and research objectives.

4.1 Operational resilience enhancing framework

Traditional cybersecurity mechanisms focus on preventing the occurrence of those attacks, improving the accuracy of detection, or increasing the speed of recovery. More often neglected is addressing how to remain operational during the window of time comprised from the advent of a cyber-attack until the system recovers. The need for trustworthy CMS capable of continued operation despite the advent of cyber-attacks calls then for increased operational resilience. Operational resilient systems are those that can withstand cyber-attacks, faults, and failures and continue to operate in a degraded state to carry out their mission (Ross et. al., 2021).

Thus, an operational resilient CMS is capable of withstanding disruptions arising from cyber-attacks while maintaining availability, utilization efficiency, and a quality ratio above degradation thresholds until recovery. Resilience, however, may not be an inherent property of the system (Dibaji et. al., 2019) and needs to be bestowed by implementing resilience-increasing mechanisms. We propose the following categories of resilience-enhancing mechanisms: (a) adaptive response: dynamic reconfiguration, dynamic resource allocation, and adaptive management, (b) redundancy: backup, surplus capacity, and replication, and (c) segmentation:

predefined segmentation and dynamic segmentation. This research presents a novel framework to enhance the operational resilience of cyber-manufacturing systems against cyber-attacks. In contrast to other CPS where the general goal of operational resilience is to maintain a certain target level of availability, we propose a manufacturing-centric approach in which we utilize production key performance indicators as targets. This way we adapt the decision-making process for security in a way that is aligned with the operational strategy and bound to the socioeconomic constraints inherent to manufacturing.

Figure 10: Framework for enhancing the operational resilience of a CMS.

The framework consists of four steps: 1) Identify: map CMS production characteristics and goals, cyber risks, threat severities, and resilience enhancing mechanisms; 2) Establish: set targets of performance in production output, scrap rate, and system downtime; 3) Select: determine which mechanism are needed and their triggering strategy and 4) Deploy: integrate into the operation of the CMS the selected mechanisms, threat severity evaluation, and activation strategy.

4.2 Operational resilient CMS against cyber-attacks

According to NIST Special Publication 800-160, Volume 2 cyber-resilient systems are those that "can withstand cyber-attacks, faults, and failures and continue to operate in a degraded or debilitated state to carry out the mission-essential functions of the organization" (Ross et. al., 2021). The question of how to bestow a system with such a property has remained the focus of recent research efforts. A recent definition of resilient CMS against cyber-attacks is: "A resilient CMS is one capable of detecting, withstanding, and recovering from failures induced by cyberattacks while still fulfilling its expected levels of production and service with acceptable levels of security, integrity, and profitability" (Espinoza-Zelaya and Moon, 2021).

Furthermore, the mechanisms by which those goals are achieved can be classified as their ability to either (Espinoza-Zelaya and Moon, 2022):

a) Reduce the probability of a successful cyber-attack.
b) Reduce the time for detection of a cyber-attack.
c) Reduce the adverse effects of a successful cyber-attack.
d) Reduce the time to recover from a cyber-attack.

Fig. 11 illustrates how each of those goals deals with the threat of cyber-attacks. The focus of this work lies on those operational resilience mechanisms that act upon the time from the onset of the attack until the system recovery. Their main objective is to limit the degradation in performance that the system can experience.

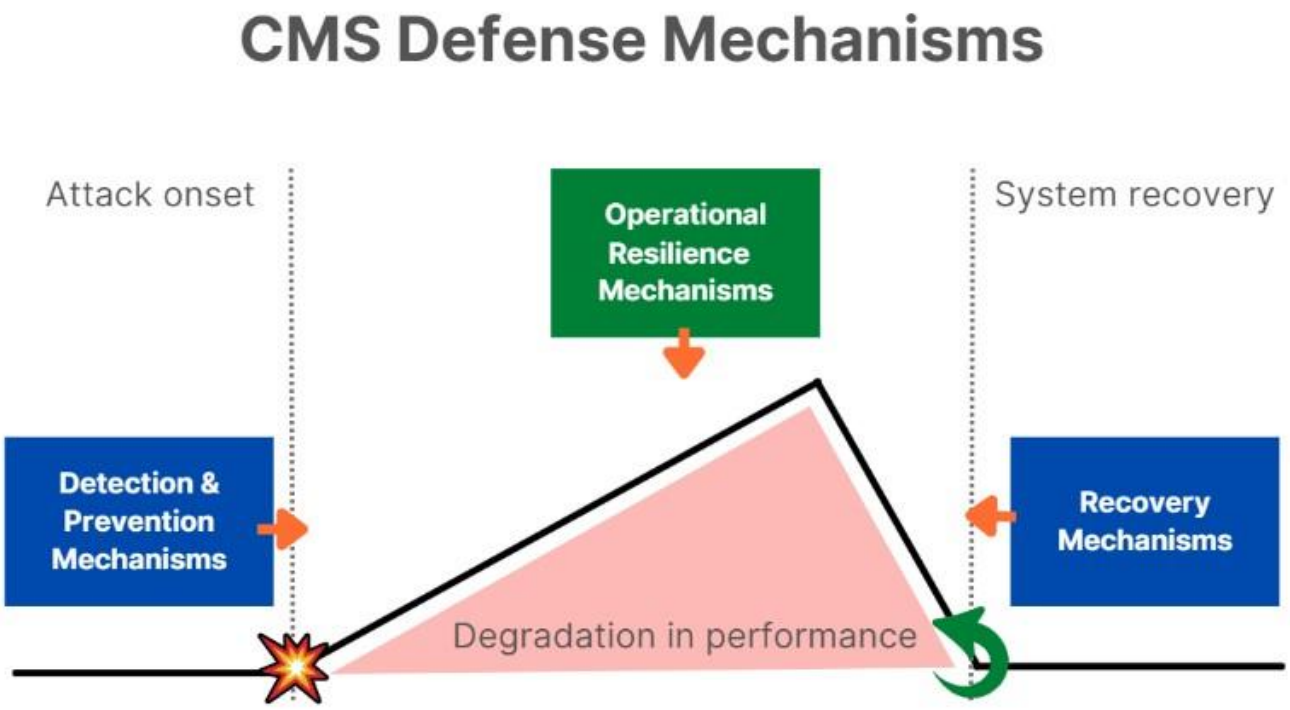

Figure 11: CMS Defense Mechanisms against cyber-attacks.

4.3 Goals of CMS

Key Performance Indicators (KPIs) are the quantifiable and strategic measures of success factors for an enterprise. The ISO 22400 standard (International Standards Organization ISO, 2014) describes 34 unique KPIs to manage manufacturing operations. We propose utilizing the following three KPIs as a means to measure the performance of the CMS:

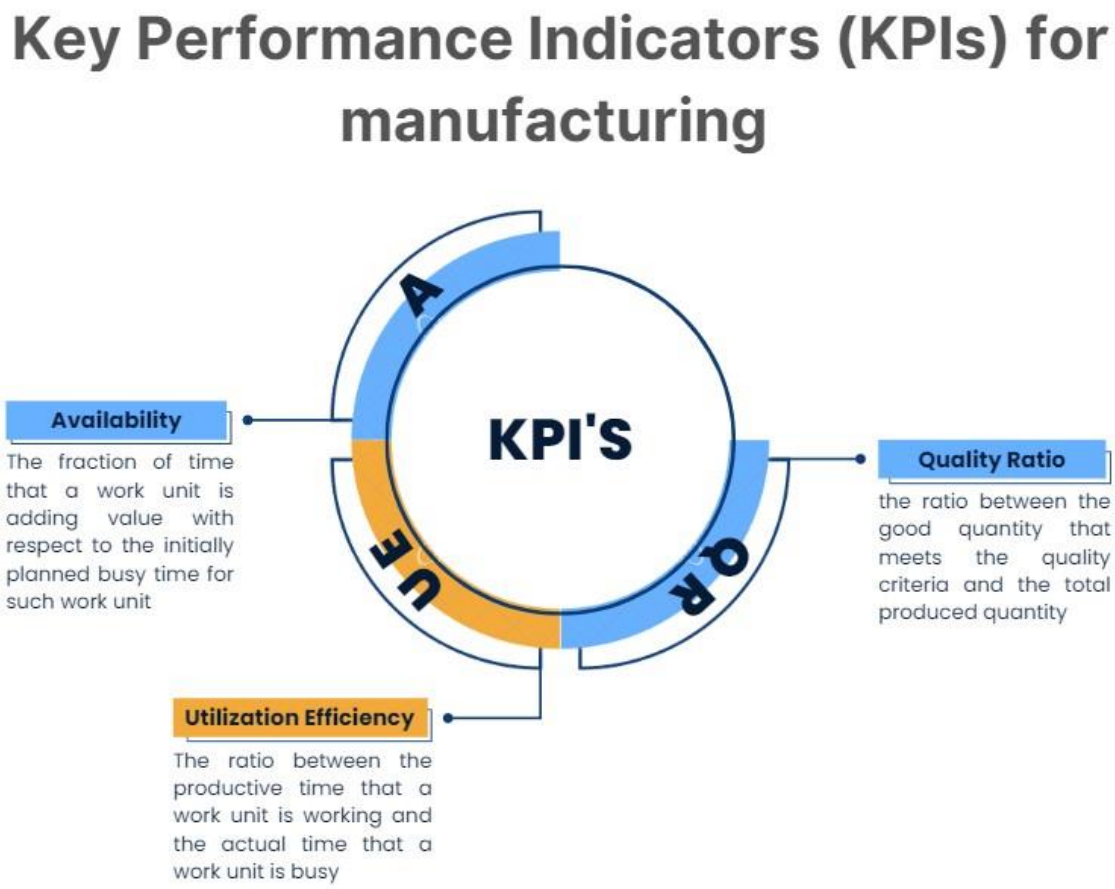

Figure 12: Key Performance Indicators (KPIs) for manufacturing.

Availability: It shows the fraction of time that a work unit is adding value concerning the initially planned busy time for such a work unit.

$$Availability = \frac{Actual\ Production\ Time}{Planned\ Busy\ Time} \qquad (1)$$

Utilization efficiency: It is calculated as the ratio between the productive time that a work unit is working and the actual time that a work unit is busy.

$$Utilization\ Efficiency = \frac{Actual\ Production\ Time}{Actual\ Busy\ Time} \quad (2)$$

Quality Ratio: It is calculated as the ratio between the good quantity that meets the quality criteria and the total produced quantity.

$$Quality\ Ratio = \frac{Good\ Quantity}{Produced\ Quantity} \quad (3)$$

We then define an operational resilient CMS as one capable of withstanding disruptions arising from cyber-attacks while maintaining availability, utilization efficiency, and a quality ratio above degradation thresholds until recovery. Our proposed framework consists of the following steps:

1. **Identify:** The CMS architecture needs to be assessed, to determine the characteristics of the production system, goals, states, and constraints. The vulnerabilities are ranked and a model is established to relate to a cyber-attack model, attack vectors, methods, and consequences are mapped. Lastly, resilience enhancing mechanisms available are identified.

2. **Establish:** The goal of operational resilience is to continue operation under performance degradation, the limits that are deemed acceptable depend on the production goals of the CMS and change depending on the manufacturing conditions. Consequently, targets of performance are set in production terms, and availability, output, and scrap rate are determined for each of the system states. Lastly, a threat severity assessment algorithm is established to determine the expected operational disruption of known threats in different operation conditions.

3. **Select:** From the available resilience-enhancing mechanisms select the ones that enable the system to satisfy the performance targets and minimize the total cost.

4. **Deploy:** Lastly, an operational strategy needs to be deployed to guarantee the effectiveness of the solution. Such a strategy must include the procedure of decision-making and mechanisms activation rules. This process should be iterative as new threats and mechanisms can alter the operational resilience of the system.

4.4 Identify

The first step to enhance the operational resilience of a cyber-manufacturing system against cyber-attacks consists in identifying potential threats. According to the taxonomy for secure manufacturing systems (Wu and Moon, 2018), there are six categories of potentially affected entities: human, product, equipment, intellectual property, environment, and operation. Each category is further decomposed by attack target and attack method. For the scope of this dissertation only those with operational disruption potential as considered. Thus, we identify all the threats with the potential of doing one of the following: (i) Reduce the capacity of the workstation, (ii) Reduce the quality of the output of the workstation, or (iii) Reduce the quality of the product.

Each threat can be mapped using the attack tree model (Jürgenson and Willemson, 2010) the analysis begins by identifying one primary threat and continues by dividing the threat into sub-attacks. A tree is formed having the primary threat in its root and elementary attacks in its leaves. Using the structure of the tree and the estimations of the leaves, then we estimate the potential downtime from the root node. After the threats are mapped to its CMS target, we identify the available operational enhancing mechanisms. NIST Special Publication 800-160 (Ross et.al.,

2021) describes 14 cyber resilience techniques from which we selected the ones aimed at increasing operational resilience as described in Fig. 13.

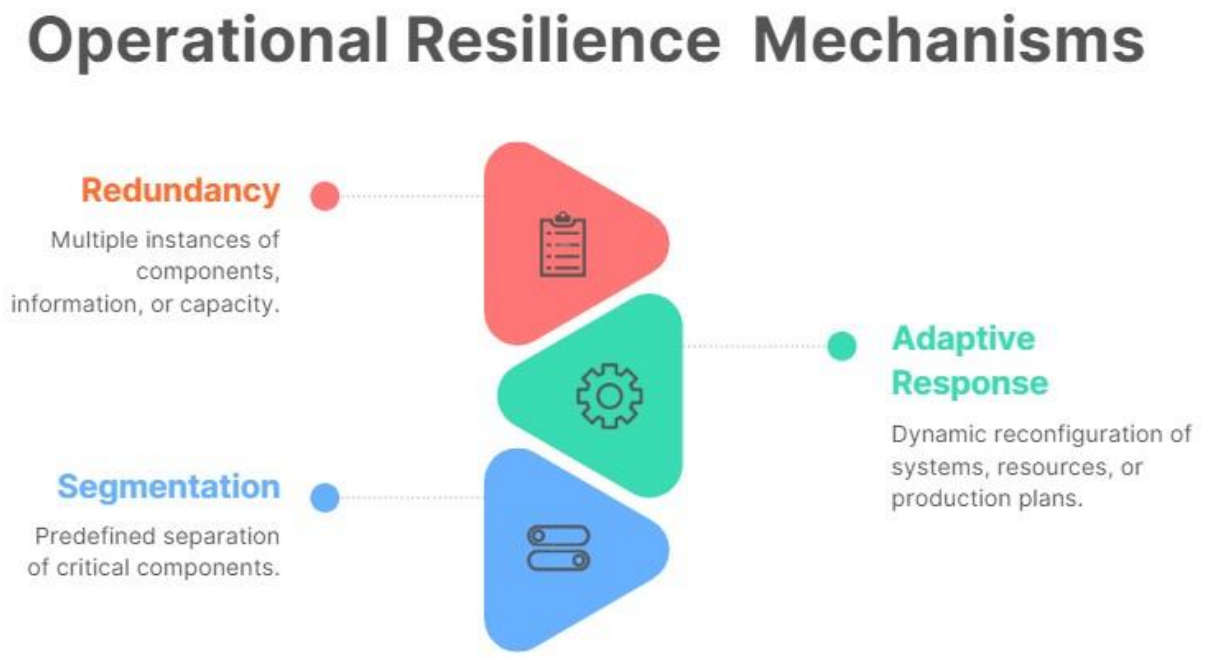

Figure 13: Operational Resilience Mechanisms.

We propose the following categories:

(i) **Adaptive response**: Implement agile courses of action to manage risks.

a. **Dynamic reconfiguration**: Make changes to individual systems, system elements, components, or sets of resources to change functionality or behavior without interrupting service.

i. *Examples:* Dynamically change router rules, access control lists, intrusion detection, and prevention system parameters, and filter rules for firewalls and gateways.

b. **Dynamic resource allocation**: Change the allocation of resources to tasks or functions without terminating critical functions or processes.

   i. *Examples*: Employ dynamic provisioning, reprioritize messages or services, implement load-balancing, emergency shutoff capabilities, and preempt communications.

c. **Adaptive management**: Change how mechanisms are used based on changes in the operational environment as well as changes in the threat environment.

   i. *Examples*: Disable access dynamically, implement adaptive authentication, provide for the automatic disabling of a system or service, dynamic deployment of new or replacement resources or capabilities, and automated decision-making supported by artificial intelligence (AI) or machine learning (ML) for rapid response and dynamic changes when human operators are not available.

(ii) **Redundancy**: Provide multiple protected instances of critical resources.

a. **Backup**: Back up information and software (including configuration data and virtualized resources) in a way that protects its confidentiality, integrity, and authenticity. Enable safe and secure restoration in case of disruption or corruption.

i. *Examples:* Retain previous baseline configurations and maintain and protect system-level backup information (e.g., operating system, application software, system configuration data).

b. **Surplus capacity**: Maintain extra capacity.

i. *Examples:* Maintain spare parts (i.e., system components) and address surplus capacity in service-level agreements with external systems.

c. **Replication**: Duplicate cyber-physical components.

i. *Examples:* Provide an alternate audit capability, create a shadow database, maintain one or more alternate processing and/or storage sites, maintain a redundant secondary system, provide alternative

security mechanisms, and implement a redundant name, and address resolution service.

(iii) **Segmentation**: Define and separate system elements based on criticality and trustworthiness.

a. **Predefined segmentation**: Define enclaves, segments, micro-segments, or other restricted types of resource sets based on criticality and trustworthiness so that they can be isolated if necessary.

i. *Examples:* Use virtualization to maintain separate processing domains based on user privileges, cryptographic separation for maintenance, and partition applications from system functionality.

b. **Dynamic segmentation:** Change the configuration of enclaves or protected segments, or isolate resources while minimizing operational disruption.

i. *Examples:* Dynamic isolation of components.

4. 5 Establish

Unlike other cyber-physical systems, CMS needs to be subordinated to the socioeconomical constraints in which they operate. Production factors such as scheduling, order management, and customer expectations need to be analyzed to determine target performance levels that need to be maintained even under the advent of a cyber-attack. The second step of the framework is to correlate the vulnerabilities and operational resilience mechanism, to the performance degradation limit and the time that needs to be available.

Figure 14: Operational Resilience Matrix.

By monitoring these metrics at the time of the advent of a cyber-attack we can determine if the CMS remained operationally resilient. The goal is to sustain the acceptable targets of performance during the time that goes from the onset of the attack until the recovery of the system.

4.6 Select

The selection of the mechanisms is now a matter of engineering design. Given that we have identified a series of threats that need to be addressed and the available resilience-enhancing mechanisms, a model can be developed to map the possible responses of the system during different operating conditions. The goal of this step is to generate a rational selection of mechanisms that satisfy the expected performance at a feasible cost. More work needs to be developed to generate a systemic way of selecting mechanisms. Our proposed framework shows the correlation between the state of the system at the advent of the attack and the impact on the target Key Performance Indicators (KPIs). The selection policy of which mechanism to trigger should then be aligned to a threat severity estimation.

4.7 Deploy

The final step of the framework is to deploy the selected resilience-enhancing mechanisms and operate them according to an activation strategy. It needs to be made operational alongside a threat severity assessment strategy (Espinoza-Zelaya and Moon, 2022). The procedure to validate that the CMS is operational and resilient against the known threats it faces is the focus of the next step of this dissertation.

4.8 Preliminary Results

In previous research (Espinoza-Zelaya and Moon, 2022) a Cyber-Manufacturing System testbed has been established in a laboratory to show the dynamic between the attacker, the exploitation of a vulnerability, and the current state of the system at the time of its advent and their effect on the severity of the threat. Additive manufacturing (AM), or three-dimensional (3D) printing as it is often referenced, is on the rise due to the open-sourced nature of the printing processes and reduced cost and capital barriers relative to traditional manufacturing (Kennedy et. al., 2017). It offers a new paradigm for engineering design and manufacturing that could have significant security implications (Campbell and Ivanova, 2013).

A Cyber-Manufacturing System (CMS) is represented as a connected network of n workstations W_i organized in a logical value-added sequence to fulfill a target flow G. Each of these workstations is comprised of a set of Cyber-Physical Systems that while providing higher productivity and network capabilities than traditional manufacturing, have given rise to new cyber-risk challenges. Failing to fulfill the target flow during a production cycle of length t results in a per unit back-order cost b. The state of the system at any given discrete time step between $[0, t]$ can be represented by the produced output P, Work in Progress before each workstation WIP_i, the remaining available production time before the cycle ends, and the remaining orders to fulfill.

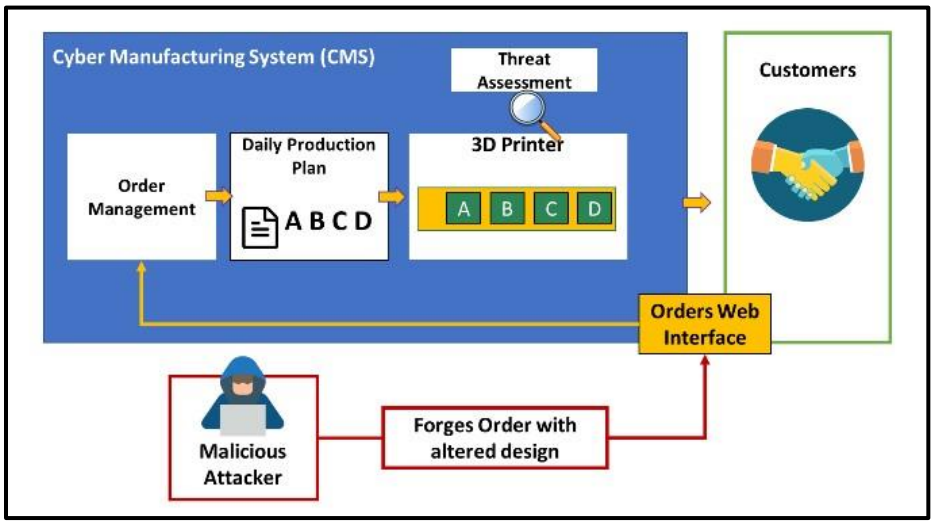

Figure 15: Testbed cyber-manufacturing system.

To deal with the advent of cyber-attacks this CMS has implemented a series of defense mechanisms that we refer to as "resilience enhancing mechanisms". We

consider a CMS resilient when it has set in place mechanisms to fulfill the following goals:

1. Prevent a successful cyber-attack.
2. Detection of a cyber-attack.
3. Reduce the adverse effects of a cyber-attack.
4. Recovery from a cyber-attack.

A cyber-attack A_{ij} can occur against a Cyber-Physical System that comprises a given workstation W_i causing a disruption that can (i) Reduce the capacity of the workstation, (ii) Reduce the quality of the output of the workstation, or (iii) Reduce the quality of the product.

A Cyber-Manufacturing System testbed has been established in a laboratory to show the dynamic between the attacker, the exploitation of a vulnerability, and the current state of the system at the time of its advent and their effect on the severity of the threat. It consists of a single workstation comprised of the following Cyber Physical components: (i) Order management system: A server that receives orders from a web interface that customers can place containing a CAD file and billing information regarding a product (SKU). (ii) Order Scheduling: Orders are aggregated and put in a production plan to be completed in a given production cycle. This includes the scheduling of the orders to optimize the warming-up period of the

machine. (iii) 3D Printer: Orders are transferred at the beginning of each cycle to the printer's internal storage. Before proceeding to print each SKU, the machine needs to warm up to a target temperature, after each SKU is finished it has to adjust this temperature to the specifications of the next one. A key part of the process is to schedule them in an order that minimizes these warmup times. Another consideration is that orders arrive at different rates, in some production cycles the system may have more idle time than in others. Each cycle consists of $t = 90\ min$. For simplicity, we are working with only one SKU=1 that takes 20 min to warm up and then 8 min to print. Between each order, there's an idle time of 3 min. Figure 16 shows a sample schedule of 5 orders of the same SKU. As we can see after the last order is completed there is 18 min available in production time.

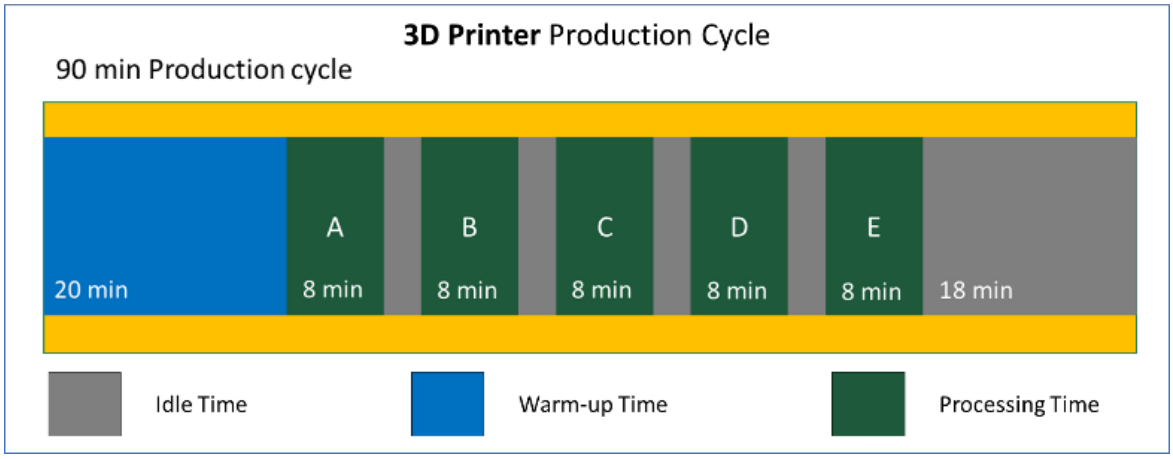

Figure 16: Sample scheduling of 5 orders into the 3D printer.

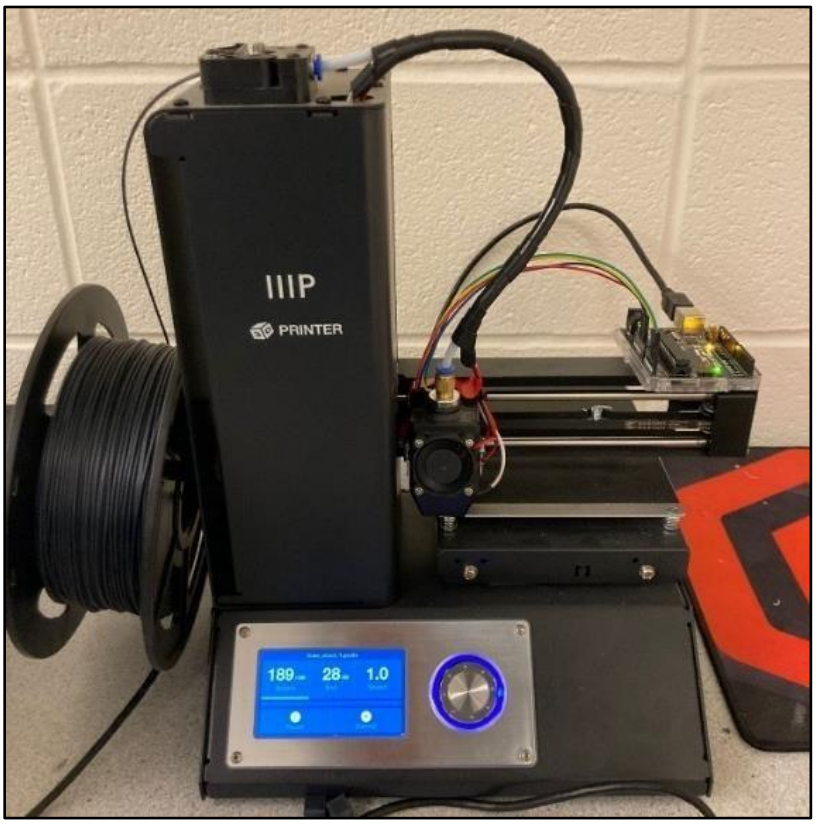

Figure 17: IIIP 3D printer Monoprice mini.

Kinetic cyber-attack

One of the key advantages of additive manufacturing (AM) is its digital thread, which allows for rapid communication, iteration, and sharing of a design model and its corresponding physical representation (Sturm et. al., 2017). While this enables a more efficient design process, it also presents opportunities for cyber-attacks to impact the physical world. One example is kinetic attacks, which cause physical damage to the system from the cyber domain. In AM, kinetic cyber-attacks are

realized by introducing flaws in the design of 3D objects (Chhetri et. al., 2016). For this scenario we simulate an attacker gaining access through phishing of one of the CMS customers' login data. With this login information, they manage to inject into the system order with a design flaw. Instead of a normal cube, the attacker gives an altered CAD file that contains a structural flaw that cannot be detected by a person with simple eyesight. Figure 18 shows the altered CAD design and Figure 19 is a comparison of the normal cube against the output of the altered CAD design in different instances of this attack being performed successfully.

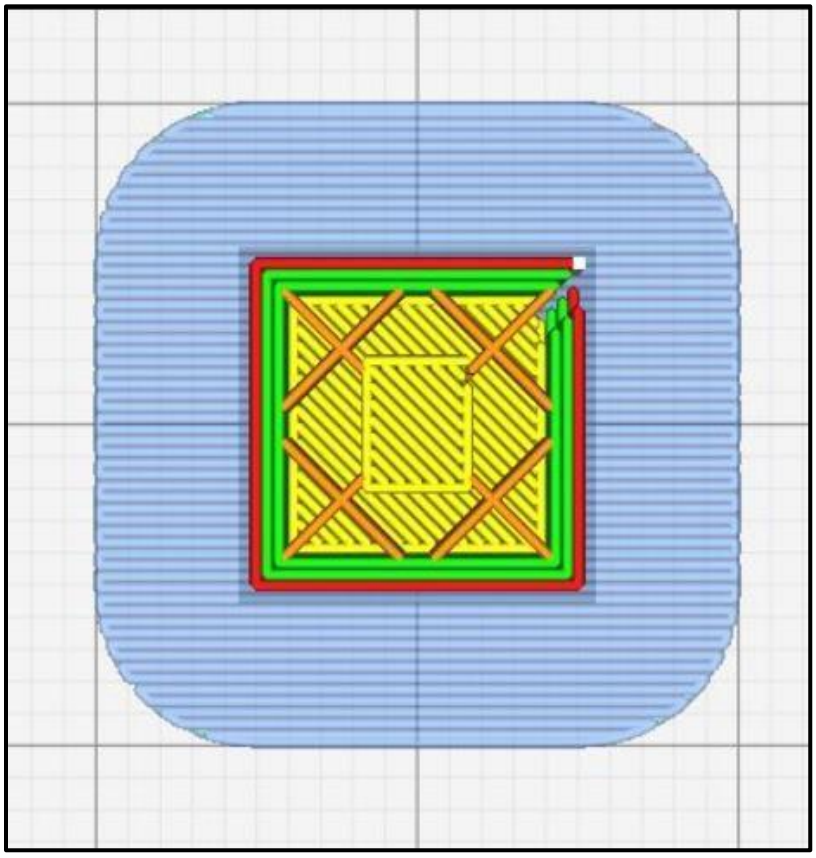

Figure 18: Altered CAD design.

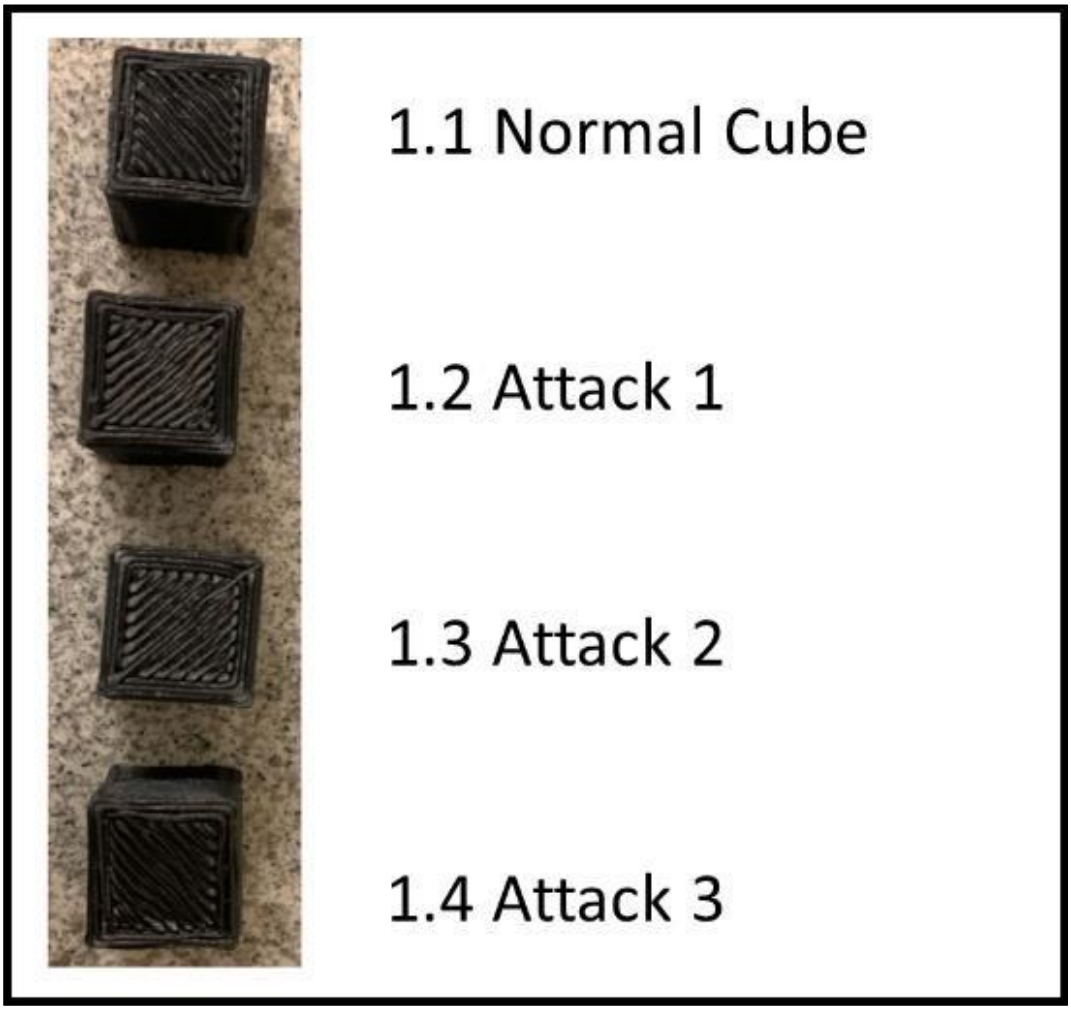

Figure 19: Comparison of the normal cube and altered.

The effect that this can have on the CMS cannot be estimated just with this description. It will be a function of the CMS's ability to detect this threat, react promptly, and prevent other instances of it. By utilizing existing customer login information, the attacker is also able to perform this exploit, and deliver the payload without leaving a trace.

Resilience mechanisms

Dealing with this attack is complex in the sense that the perpetrator does not violate the security of the system but rather utilizes a trusted actor to inject a false CAD file. Given that the output from the printer looks the same as a normal cube the detection of this attack needs to be performed as the machine is being used. The detection mechanism set in place is an anomaly detection system that captures readings from an accelerometer sensor placed on the actuator of the 3D printer. While machine learning has become a fundamental tool for computer security, its adaptability is also a vulnerability that can be exploited by attackers (Barreno et. al., 2010).

We implemented a Python Machine Learning library for anomaly detection called Pycaret. By capturing the normal behavior of the axis X, Y, and Z of the printer working in this piece we establish a baseline. Then in real-time, as other orders are being printed data from the accelerometer gets fed into this system, and the time series consisting of the difference between the baseline and observed measures is the input of the algorithm. Figure 20 shows the scores that the algorithm produces to evaluate what is an anomaly. This system has an accuracy of 95.54%. This means that given that a flag was raised the probability of an attack is $P_{attack} = 0.95$.

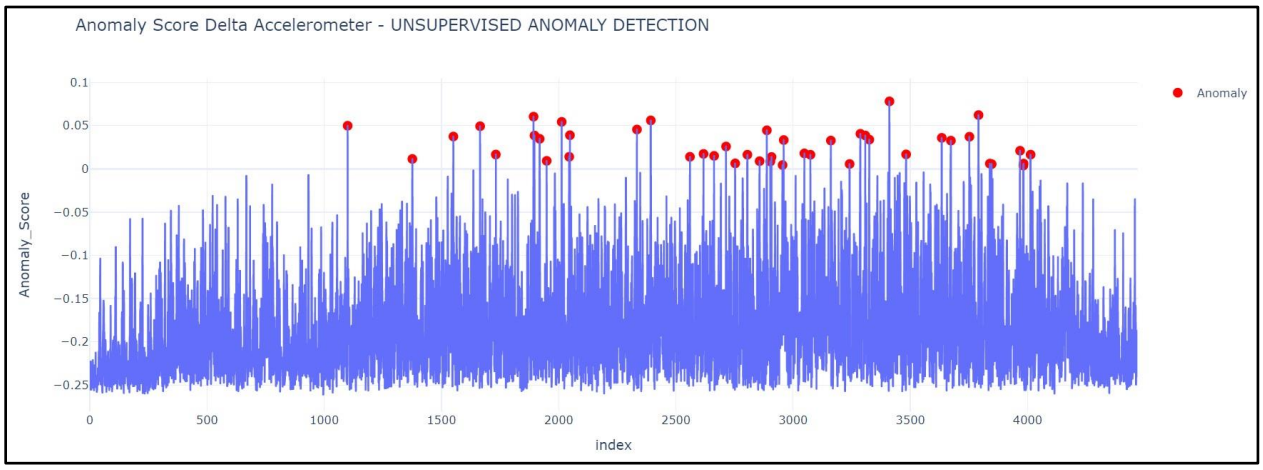

Figure 20: Anomaly sensor detection flags.

For this system, manual verification is needed to determine if the order that the printer is working on has been altered. Because at the beginning of the cycle, these files are transferred from the scheduling system to the printer an operator needs to manually check whether the file is compromised or not.

This check takes $TTD_{11} = 3\ min$. In case there is a corrupted file the operator needs to restart the printer, check every other file scheduled for that day, and then transfer the right designs back. This recovery process takes $TTR_{11} = 20\ min$.

Assessing the severity of cyber-attack

After mapping the target CMS, the attacker strategy and exploit, and the system resilience mechanisms a flowchart containing the logic of the threat assessment model can be presented. The basis of this model is that the expected cost of a threat is a function of the current state of the system and the response that is triggered when the attack is first detected. Attack trees (Mauw and Oostdijk, 2006) (Saini et. al., 2008) are well-recognized formalisms for security modeling and analysis (Audinot et. al., 2018). The quantitative input values are assigned to the actions represented by the leaves of the tree and a simple risk-analysis method is used to estimate the cost of the attack (Buldas et. al., 2006).

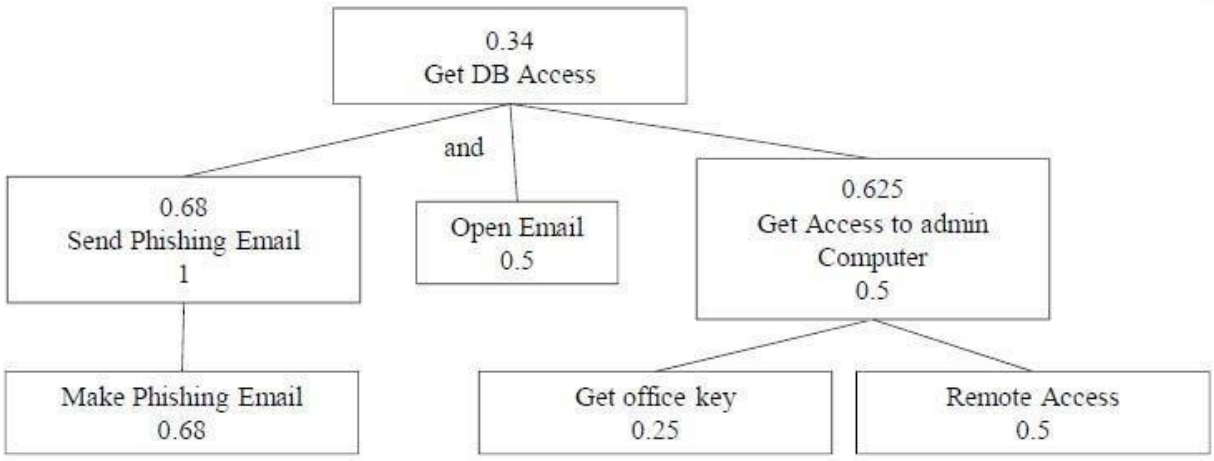

Figure 21: An Example Attack Tree (Torkura et. al., 2018)

For our system, the first step is to receive a flag from the anomaly detection mechanism set in place. However, as we saw before, there exists the possibility of a false positive that needs to be taken into consideration. For this, we establish the decision tree depicted in Figure 22. Once a flag is raised, the modeler needs to enumerate the possible decisions that the system can take. Following those is the probability of Attack / No Attack given that a flag was raised. Then the outcomes of those decisions are weighted.

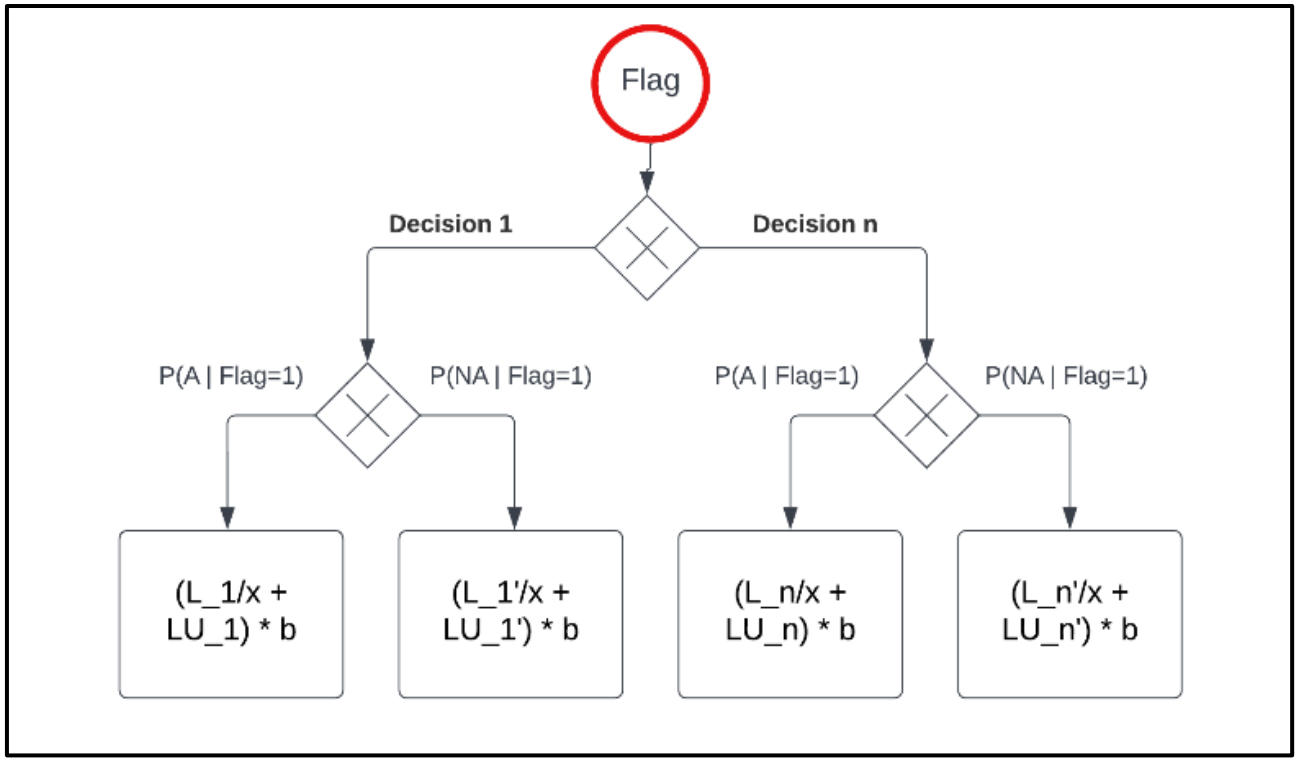

Figure 22: Decision tree.

The equation to calculate the financial impact of that branch of the decision tree is as follows:

$$\left(\frac{n}{x} + {}_{L}\, LU_n\right) * b \qquad (4)$$

Where L_n represents the potential to disrupt the required production time to fulfill the production goals. In this sense, our operational impact only adds to the severity of the attack if the downtime impacts the schedule. If the downtime occurs when the workstation is idle, or if the reduction of capacity still allows the schedule to be fulfilled then is not taken into consideration. To quantify the impact, we look at the added WIP in the system as a consequence, as well as the difference between the expected output vs the target.

However, this only has an economic effect if considered it is bigger than the remaining available production time. LU_n on the other hand, represent the direct loss in units as a consequence of the decision. The addition of these two terms multiplied by the backorder cost of not fulfilling the demand gives us the expected severity of the attack. In cases where the cost of recovery changes with each decision then the term cr_{ij}needs to be added. The short term includes repairs, replacement, extra shifts,

fees, wasted material, and other indirect costs. The long-term costs include the necessary adaptation the system requires, auditing fees, and others.

One of the biggest multipliers of the severity of a threat is the breaches against the integrity of the CMS Intellectual Property. It is complicated to give a numerical value to those non-tangible losses, but it should be assessed. Can the exploitation of a given threat provide access to sensible data regarding customers' private information, business-sensitive documents, or others? This evaluation is more qualitative and should always be done to correctly prioritize which threats pose a bigger danger to the system.

Cyber-attack execution and severity assessment

We ran an experiment in which the system behaves according to the flowchart in Figure 17. Customers place orders through a web interface and these get scheduled in a production cycle. The attacker induces its altered CAD file before the system transfers the files to the 3D printer. So, before the production cycle starts the payload is already there. The CMS behavior is governed by simple automated logic, if there are orders on schedule for that cycle the machine starts to warm up. Once it reaches the conditions for printing it starts working. During the time that it takes to print the order the anomaly detection system is monitoring the behavior of the accelerometer.

If no flag is raised the system finishes printing, checks if there are orders left, and continues the cycle until it finishes the orders scheduled for that cycle. The threat severity assessment gets triggered once an attack flag is raised. As we established before, the probability of an attack given that a flag has been raised is 0.95. With this knowledge a decision tree is established with the following branches: a) Stop printing, attack, b) Stop printing, no attack, c) Continue printing, attack and d) Continue printing, no attack.

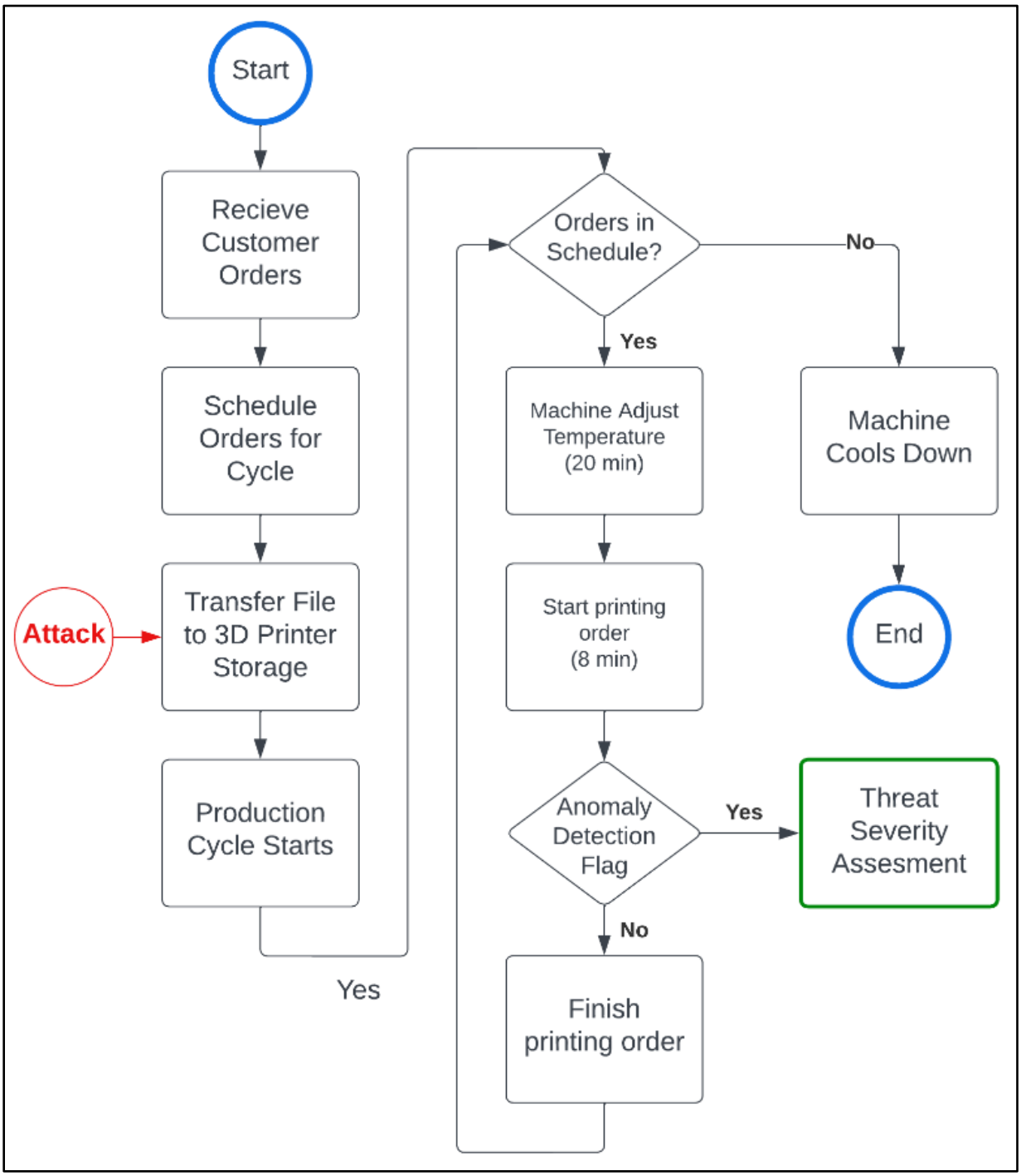

Figure 23: Flowchart of cyber-manufacturing system operation.

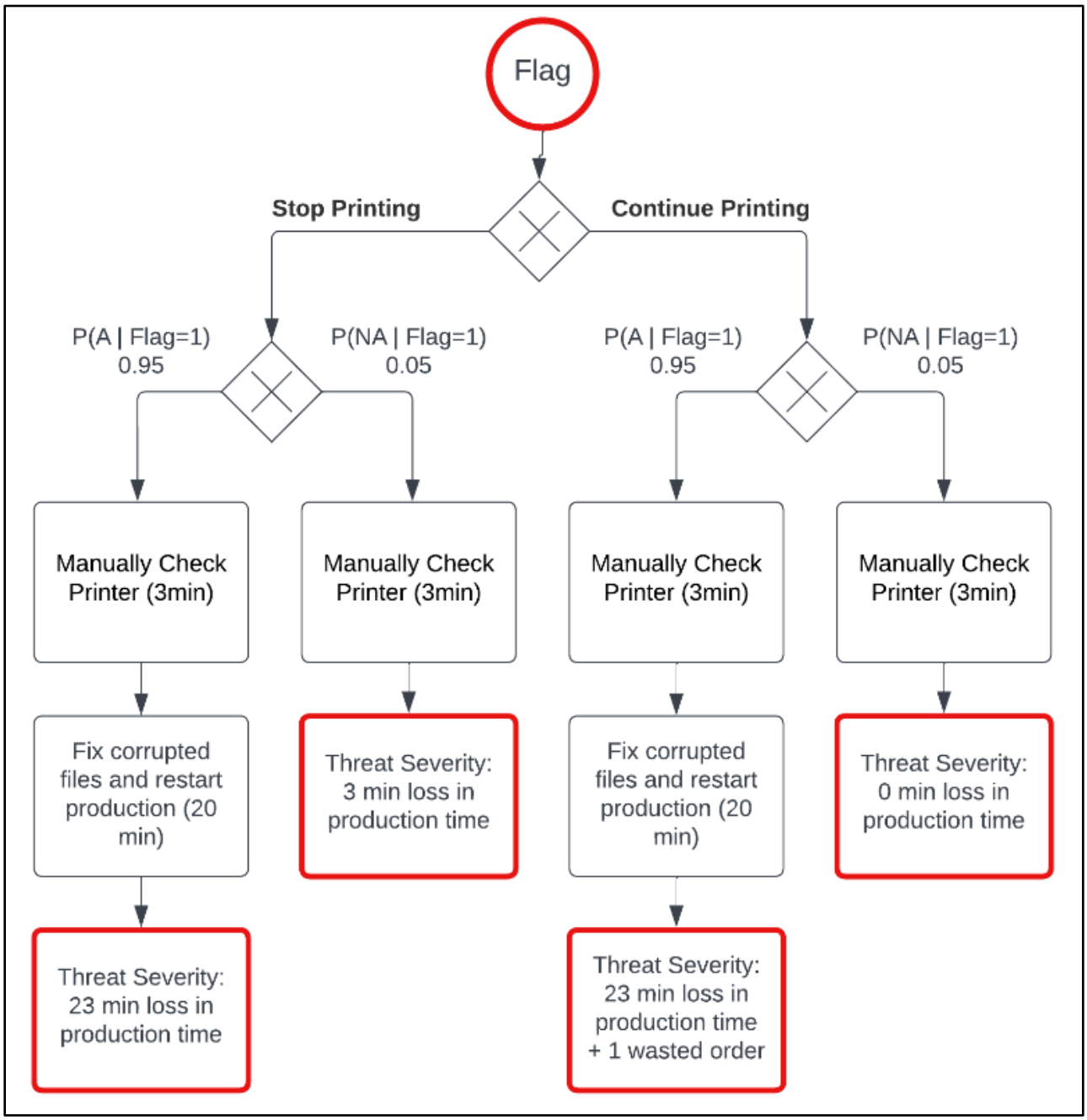

Figure 24:Flowchart of threat severity assessment.

At the advent of the attack the CMS has to determine whether to stop or not stop the printing of the current piece, then :

a) Stop printing of g: 0.59b

$$0.^{95}\left(\frac{23-18}{8}\right) * b + 0.05\left(\frac{0}{8}\right) * b \qquad (5)$$

b) Continue Printing: 1.54b

$$0.^{95}\left(\frac{23-18}{8} + 1\right) * b + 0.05(0) \qquad (6)$$

While the threat would cause a total of 23 min of downtime this system with the current schedule has 18 min available of idle time. Thus, it can recover that time leaving only 5 min of net operational impact. We can conclude that the severity of this attack if we stop printing when we detect an anomaly will be lower than if we continue printing. This is, however, only true in the conditions in which this particular attack happened.

Chapter 5: Experimental Validation.

We propose a novel approach that correlates the state of production and the timing of the attack to predict the effect on the manufacturing key performance indicators. A real-time decision strategy is deployed that selects the appropriate response to maintain availability, utilization efficiency, and a quality ratio above degradation thresholds until recovery. Our goal is to demonstrate that the operational resilience of CMS can be enhanced such that the system will be able to withstand the advent of the attack while remaining operationally resilient.

5.1 Resilient CMS Simulation

The objective of this research is to demonstrate that the operational resilience of a Cyber-manufacturing system can be enhanced such that the target KPIs are maintained above the degradation threshold during the advent of a cyber-attack. To show the effectiveness of that strategy, the operation of a CMS needs to be simulated in realistic conditions. We start by initializing a discrete-event simulation that models the behavior of our testbed additive manufacturing CMS. Following are the variables utilized to track the state of the system during the length of the cycle.

5.2 Simulation Variables

Production control

$d = 30$; the number of working days.

$m = 480$; the number of minutes per day.

$runtime = d * m$; the total runtime of the simulation.

$orders = discrete\ uniform\ distribution\ [x, X]$; number of orders per day.

$st = Normal\ distribution\ [\mu, \sigma]$; processing time per order.

$QR = calculated\ value$ [0,1]; quality rate.

$pt = \sum_{i=}^{i=orders_0} st_i$; total daily processing time.

$idle = m - pt$; total daily idle time.

$output = sum\ of\ orders\ processed\ per\ day.$

$scrap = sum\ of\ defective\ orders\ per\ day.$

Manufacturing Key Performance Indicators (KPIs)

$scrap\ rate = scrap/output$; rate of defective pieces.

$fill\ rate = output/orders$; rate of fulfilled orders.

$utilization = pt/m$; utilization of the server.

$downtime = 1 - utilization$; utilization of the server.

Cyber-attack model

$Cyber\_attack_i = [A_i, TTD_i, TTR_i, QR *_i]$; Properties of cyber-attack i.

$A_i = discrete\ uniform\ distribution$ [0,$runtime$]; the advent of cyberattack i.

$TTD_i = calculated\ value$; Time to detect the attack i.
$TTR_i = calculated\ value$; Time to recover from the attack i.

$QR *_i = discrete\ uniform\ distribution\ [0, runtime]$; resulting quality rate consequence of the advent of attack i.

$Resilience\_mechanism_{ij} = [TTR'_{ij}, QR'_{ij}, c_{ij}]$; Properties of resilience mechanism j that acts to counter cyber-attack i.

$TTR'_{ij} = calculated\ value$; Time to detect the attack i.

$QR'_{ij} = calculated\ value$; Time to recover from the attack i.

$c_j = calculated\ value$; cost of resilience mechanism j.

5.3 Simulation Assumptions

1. A cyber-attack will occur at a random point in the production cycle. Its impact on the quality rate will last from the onset until the system recovers. This equals the time to detect it (TTD) plus (Time to recover).
2. The system can activate a resilience mechanism during the window of the attack, the decision to do so will depend on the operational resilience strategy.
3. Orders arrive every day at the beginning of the cycle. Every order must be fulfilled the same day, they are not carried over.

4. At the end of each day, the manufacturing KPIs are calculated. The operational resilience target is to maintain them above the degradation threshold every day.

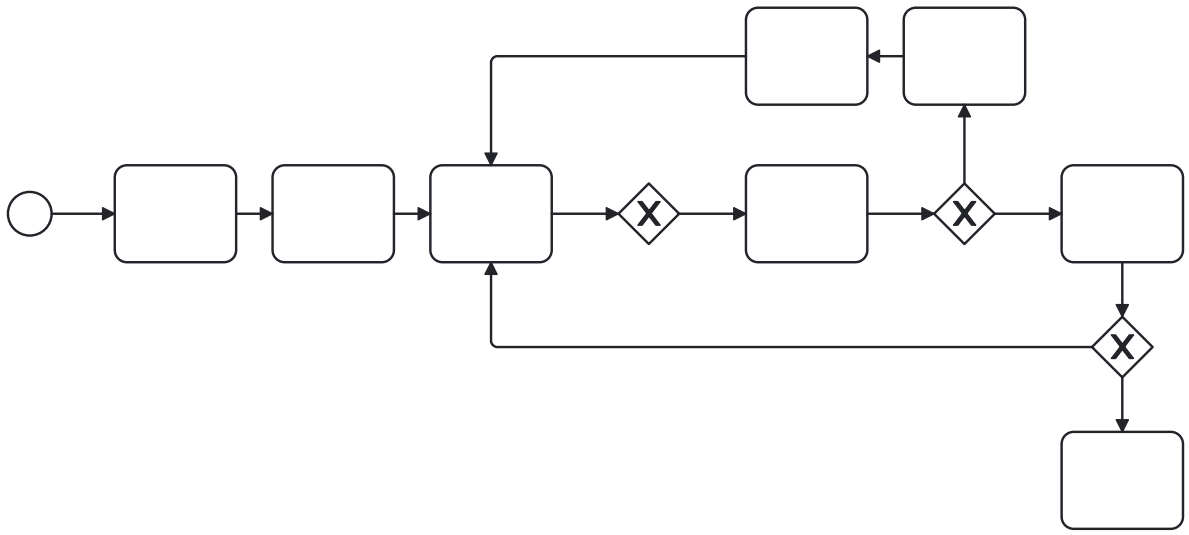

Figure 25: Simulation Flowchart.

5.4 Simulation Code

Our goal is to simulate the behavior of this discrete cyber manufacturing system, for the level of flexibility we need we chose to build the simulation from scratch. In a google collab notebook, we initialize our variables. The first step is to import standard libraries. Matplotlib will be used to generate plots and graphs. NumPy is

used to manage the resulting data as arrays, pandas will allow aggregating daily results into data frames. (https://github.com/coespino93/Dissertation-code)

```
# Carlos Espinoza
# Enhancing the operational resilience of Cyber-manufacturing Systems (CMS) against cyber-attacks
# Code
import matplotlib as mpl
import matplotlib.pyplot as plt
from matplotlib import style
import numpy as np
import pandas as pd
from scipy.interpolate import griddata
from scipy import stats
from sklearn.linear_model import LinearRegression
```

Figure 26: Code Snippet (Python Libraries)

From SciPy we obtained the "grid data" module that allows us to build multidimensional data structures and the stats package to handle the statistics calculation. Lastly, from "sklearn" we import the Linear Regression package that will be utilized to build the prediction tool.

The second step is to initialize the simulation variables that we defined before. The clock gets started in 0, for this simulation there are 30 working days, and 480 working minutes per day. Runtime gets calculated by multiplying days and working minutes. Orders are generated with the NumPy random integer function for each day. Daily processing time, however, gets determined until the simulation is running.

```
# Production Variables

clock = 0 # Timestamp measured in mins
days = 30 # number of working days of the simulation
working_minutes = 480 # number of minutes per day
runtime = days*working_minutes # runtime of simulation
o = [np.random.randint(30, 60) for d in range(days)] # number of total orders per day
daily_processing_time = [] # processing time of each order
do = [o[n]+mo[n] for n in range(days)] #daily orders
to = sum(do) # total orders for production cycle
quality_rate = 0.9 # % of orders printed correctly
```

Figure 27: Code Snippet (Production Variables)

The clock runs in increments of 1 minute, the start of each day then occurs in intervals of "working minutes" from 0 until the end of the runtime. The clock jumps to the value of warm-up given that the machine needs time to reach the temperature before starting the printing process. Then for every order received on that day, the processing time gets generated following a normal distribution utilizing the NumPy random normal function.

```
# Start each day
if clock in [s for s in range(0, runtime, working_minutes)]:

  # Processing time per each order mean =8, sd = 2
  time = warm_up # warm up time at the beginning of each working day
  output = 0
  scrap = 0

  # Generate processing time per order
  for order in range(do[day]):
    daily_processing_time.append(np.random.normal(8, 2))
```

Figure 28: Code Snippet (Initialization)

Now the work of the scheduler consists of checking how much remaining time there is each day, and if there is enough time to process a given order. It only schedules the order into the printer if it can be completed before the shift ends. The moment it realizes it cannot do so any longer, it breaks the cycle and finishes the working day. A random float is generated after each order is printed to determine and compared to the current quality rate, if the float falls in the range [0, Quality Rate] the order is considered good, adding one item to the output. If the order is defective, scrap increases and the scheduler will attempt to reprocess the order if there's enough time in the current cycle.

```
# Check remaining time
for order in range(do[day]):
  if time + daily_processing_time[order] >= working_minutes:
    break
  time = time + daily_processing_time[order]

  #Quality output

  if np.random.rand() < quality_rate:
    output = output + 1

  else:

    scrap = scrap + 1

    # Reprocess bad order
    if time + daily_processing_time[order] <= working_minutes:

      time = time + daily_processing_time[order]
      output = output + 1
```

Figure 29: Code Snippet (Printing Orders).

Each day ends with either the system printing the last order in the queue or the time reaching working minutes. Daily KPIs are calculated and appended into a data frame. For each production date then the system can capture the minute at which the last piece was printed, the utilization of the machine, the downtime of the system, the fill rate, the orders that were scheduled, the output, the scrap rate, and the resilience. This last value is a binary that evaluates if the KPIs were below the target threshold.

```
    # Calculating daily KPIs

    S.append(time) # Daily uptime
    I.append(working_minutes - time)  # Daily idle time
    U.append(time / working_minutes) # Daily utilization
    D.append(1-(time / working_minutes)) # Daily downtime
    F.append(output / o) # Fill rate
    P.append(output) # Production output
    W.append(scrap) # Scrap orders
    WR.append(scrap/output) # Scrap rate
    resilience = 1 if output / o > 0.9 else 0
    Results.append([minute, time / working_minutes, 1-(time / working_minutes), output / o, o, output, scrap / output, resilience])

    # advance to next working day
    quality_rate = 0.9

df = pd.DataFrame(Results, columns=['minute', 'Utilization', 'Downtime', 'Fill Rate', 'Orders', 'Output', 'Scrap Rate', 'Resilience'])
```

Figure 30: Code Snippet (KPI calculation).

To model the uncertain nature of the advent of the attack a random seed from a range [0, runtime] gets hidden in the simulation. The attack itself is modeled as a three-element list; the first characteristic is the Time to Detect (TTD). This calculated value arises from the study of the system, which is the number of minutes that it will take to notice the advent of the attack. The second element is the Time to

Recover (TTR). As we are modeling a real system, recovery protocols are set in place, they will however take time. Lastly, and perhaps more important, is to model the effect the attack has on the system. For our purpose, we convert this into a new quality rate which will last during the time it takes to detect the attack, until the system recovers.

```
15 # Attacks characteristics
16 mo = [0 if np.random.rand() < 0.90 else 1 for d in range(days)] # number malicious orders per day
17 attack2 = [np.random.randint(20, working_minutes), np.random.randint(1, days)*working_minutes] # time and day of advent of attack 2
18 A2 = [50, 100, 0.5] # Effects of attack 2, TTD = 50 min, TTR = 100 min, QR = 0.5
19 attack3 = [np.random.randint(20, working_minutes), np.random.randint(1, days)*working_minutes] # time and day of advent of attack 3
20 A3 = [200, 480, 0.4] # Effects of attack 3, TTD = 200 min, TTR = 480 min, QR = 0.4
21
```

Figure 31: Code Snippet (Attack characteristics)

```
# Advent of attack

if clock == attack3[1]:
  print("Attack 3 occurred on day " + str(int(attack3[1]/480)) + ' at: ' + str(attack3[0]) + ' mins')
  for order in range(do[day]):
    if time + daily_processing_time[order] >= working_minutes:
      break
    time = time + daily_processing_time[order]
    if time > attack3[0]:
      quality_rate = A3[2]
    if time < A3[0] + A3[1]:
      quality_rate = 0.9
```

Figure 32: Code Snippet (Advent of Attack)

A conditional statement is set into the logic of the simulation that evaluates if the clock equals the advent of the attack. It prints a statement that is used for the analysis and it swaps the current quality rate for the degraded version product of the attack. This quality rate will be utilized in the system until the time that it takes to detect and recover from it (TTD + TTR). The objective of this simulation is to

determine a policy by which to activate an operational resilience mechanism. We model those into the system as a three-element list. It contains the new time to recover in case the mechanism is triggered, the quality rate while the mechanism takes act and the cost of it.

```
22 # Resilience mechanisms
23
24 R2 = [50, 0.8, 5] # Resilience mechanism characteristics TTR = 50, QR = 0.8, cost = 5
25 R2 = [150, 0.7, 10] # Resilience mechanism characteristics TTR = 150, QR = 0.7, cost = 10
```

Figure 33: Code Snippet (Resilience Mechanisms)

The decision to activate a mechanism is taken by the prediction of the effect of the cyber-attack on the manufacturing KPIs. Thus, a mechanism is only triggered when is needed. The system utilizes the prediction mechanism and if the values exceed the threshold, then the mechanism gets triggered, else the attack is just withstanding with the normal recovery strategy set in place.

```
# decide on resilience
if prediction > threshold:
    activation = 1
    quality_rate = R2[1] #Attach resilience rate

else:
    activation = 0
    quality_rate = A3[2]  # Attack quality rate prevails
```

Figure 34: Code Snippet (Resilience mechanism activation)

5.4 System baseline (No attack)

To get a baseline of the performance of the simulated CMS we ran a 30-day cycle in which no attacks occurred. The following are the figures that describe the system in each of those days. The baseline manufacturing utilization oscillated between 62% and 99%. This can be explained because each day the number of orders differs, so while the system is always able to have enough capacity, some days the extra wiggle time to deal with unforeseen events is less than ideal.

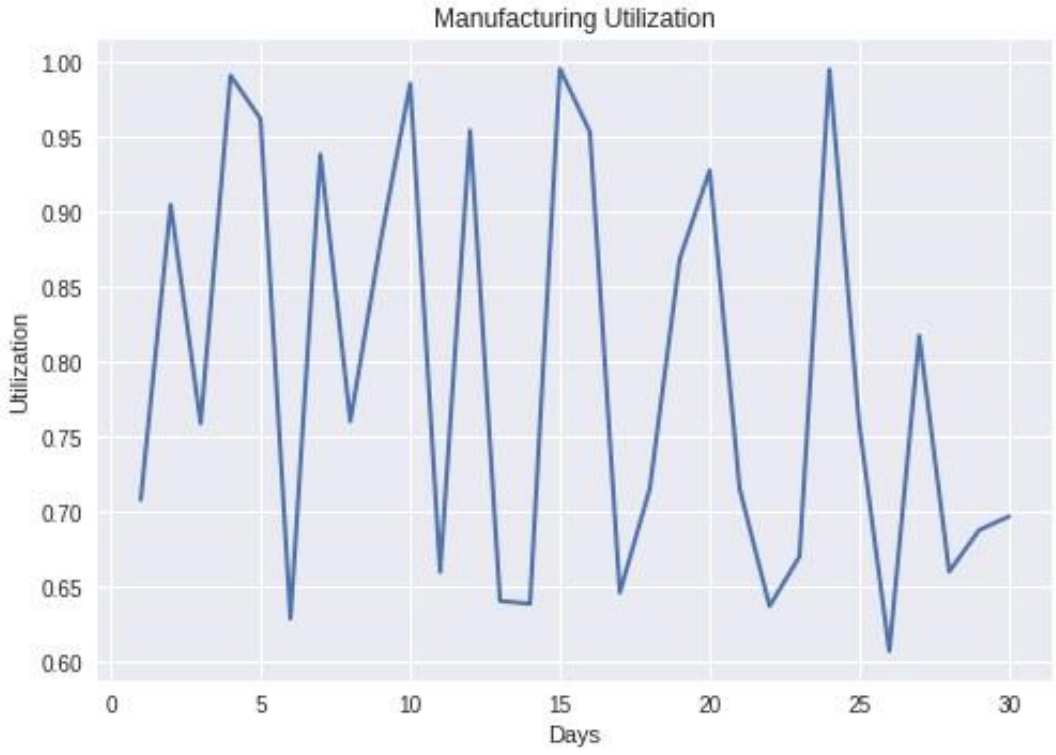

Figure 35: Baseline Manufacturing Utilization.

Next is the manufacturing fill rate. While most of the time the system has enough capacity to fulfill all its orders, there are some days on which the rate can drop below 90%. A combination of excess scrap rate, and large orders/processing times can be utilized to understand this behavior.

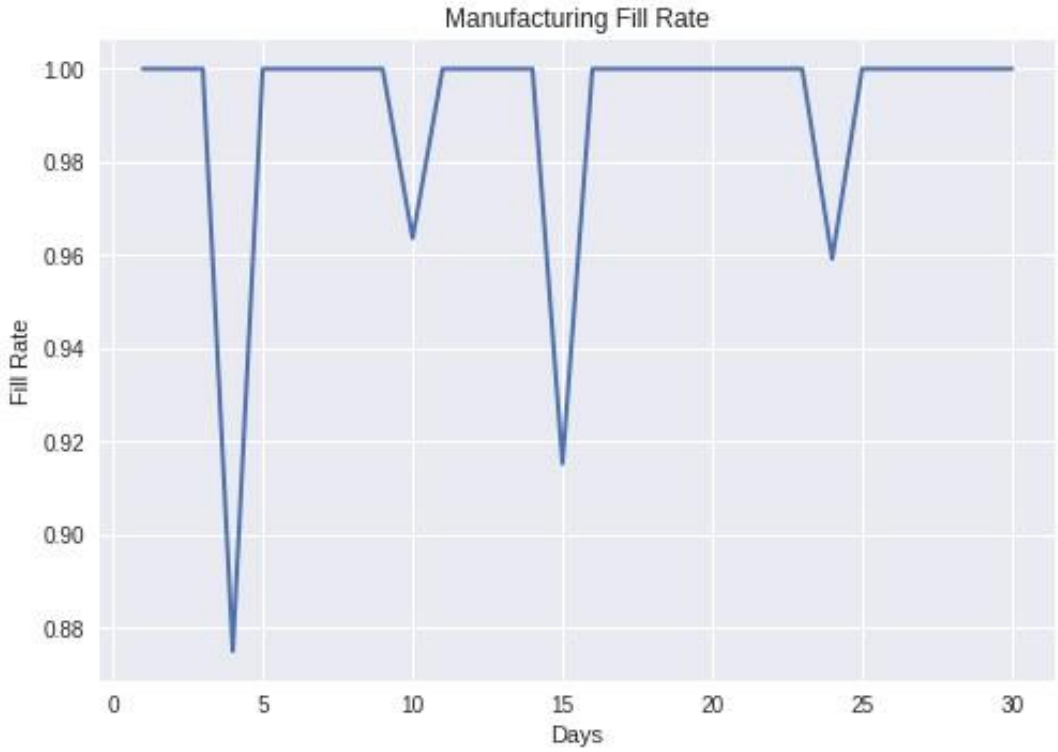

Figure 36: Baseline Manufacturing Fill Rate.

Lastly, we take a look at the Scrap Rate. While this simulation sets the value of the quality rate at 90% that does not mean that every day the scrap rate will be 10%. Because they are independent of each other, the behavior on each day can go

even up to 20% or as low as 1%. This highlights how uncertain manufacturing processes are.

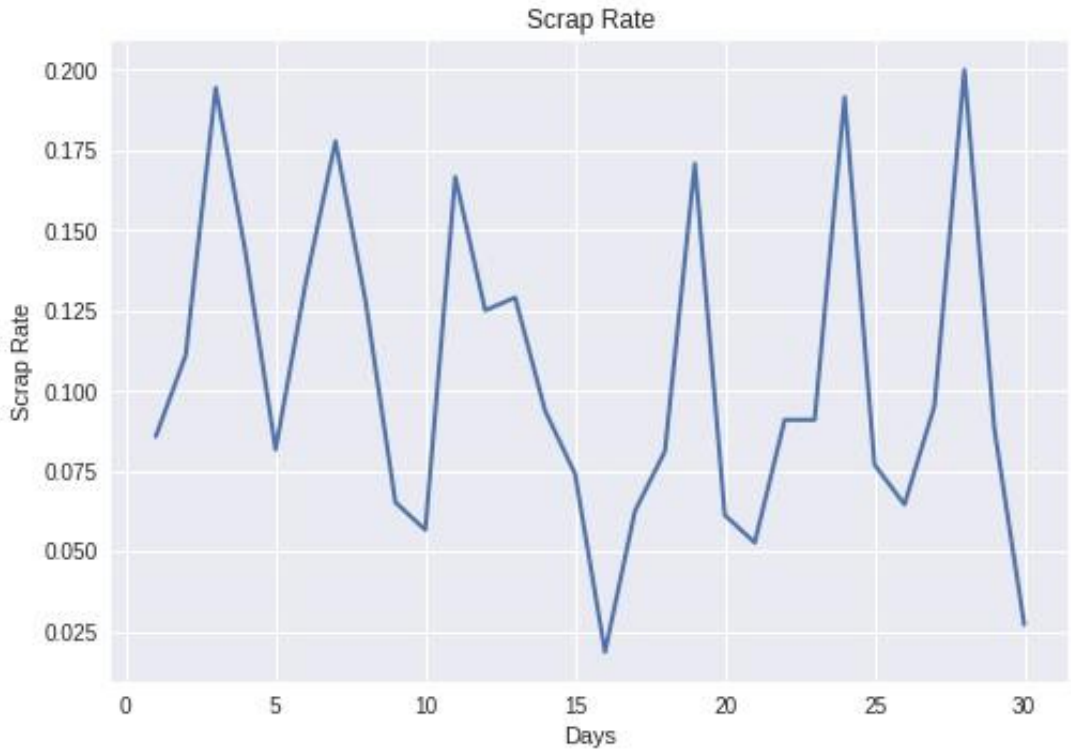

Figure 37: Baseline Scrap Rate.

Now is important to understand the aggregated result for the whole cycle and how they can be sometimes deceiving. Because the vast majority of days the CMS can fulfill the demand completely, we observed that the average fill rate over the 30 days is 99%. The scrap rate as expected is calculated at 10%, and the utilization is around 82%. If we take a look at the comparison of orders vs outputs, we can notice that on certain days the system would be more susceptible to an attack than others. Even though this is a one-product-only system and the variability of the demand is

known, everyday indicators are still independent of each other. Thus, looking at the aggregated statistics may lead us to believe we are more equipped to deal with interruptions than we are.

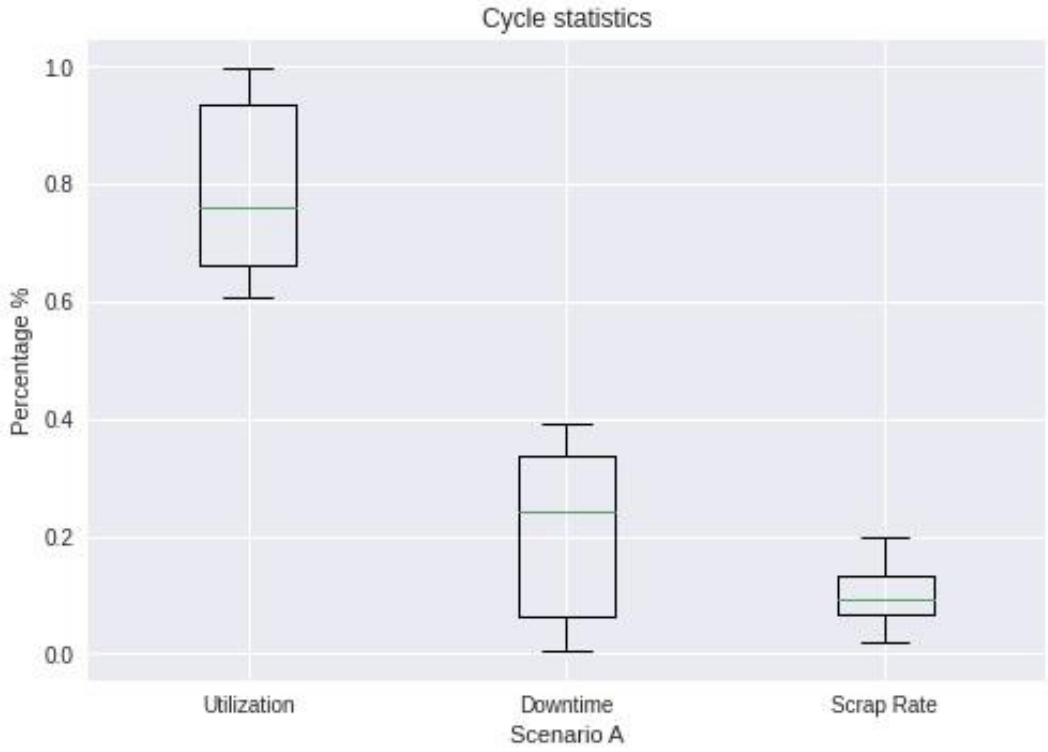

Figure 38: Baseline Cycle statistics.

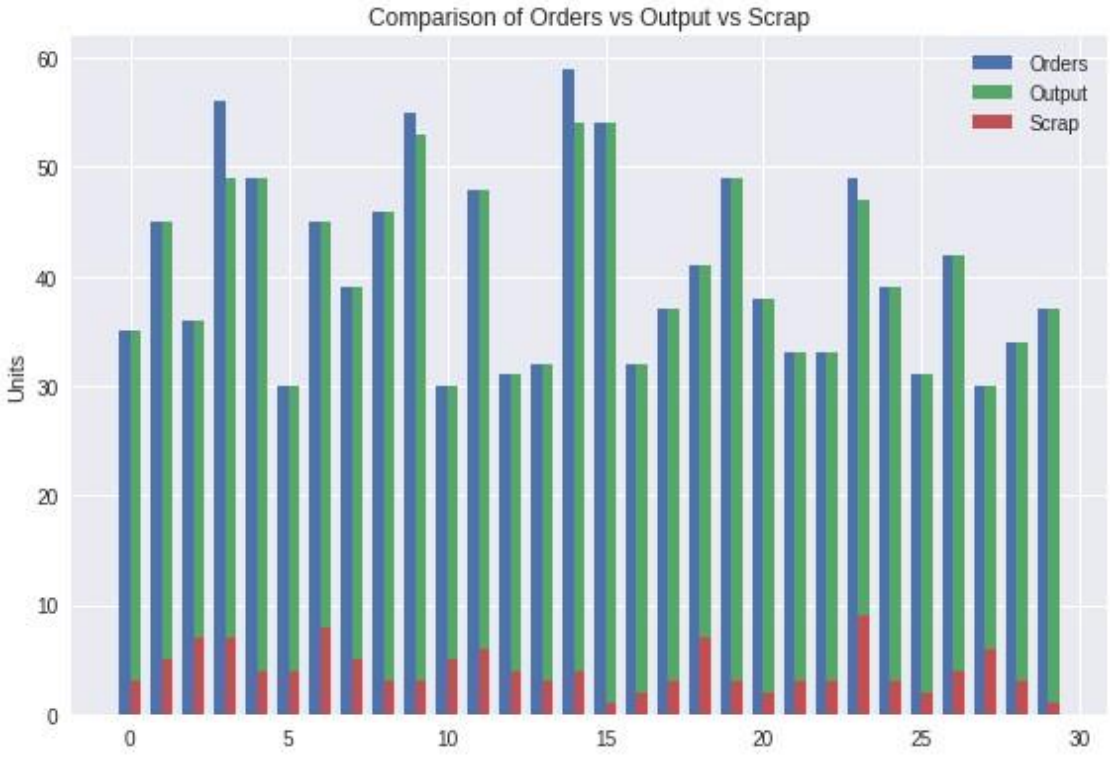

Figure 39: Baseline Comparison of Orders vs Output vs Scrap Rate.

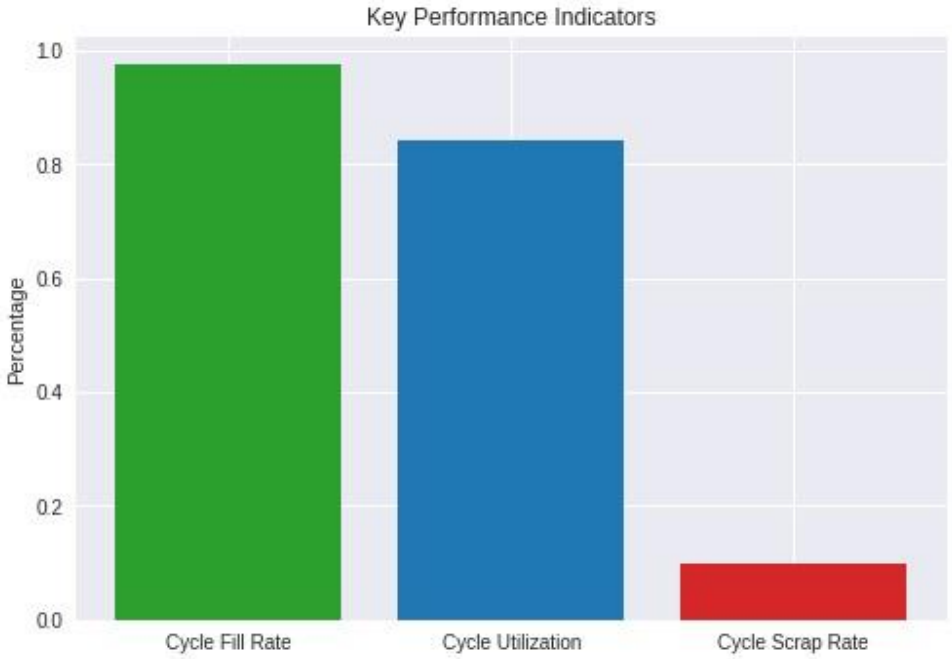

Figure 40: Baseline Cycle Key Performance Indicators.

5.5 CMS attack scenario (No resilience)

An attack is now introduced into the system, it can occur at any point in the run time as described before. In this sample occasion, the advent of the attack happened on day 17, minute 368. As expected, the attack caused the utilization of that day to reach neat 100% given that the system had to deal with the stress of it. Surprisingly the manufacturing fill rate was 100%. This is a result of a fortuity combination in which that day's number of orders, and the timing of the attack, allowed the system to still fulfill its orders. The system remained resilient even though no action was taken.

Figure 41: Attack scenario (no resilience) Manufacturing Utilization.

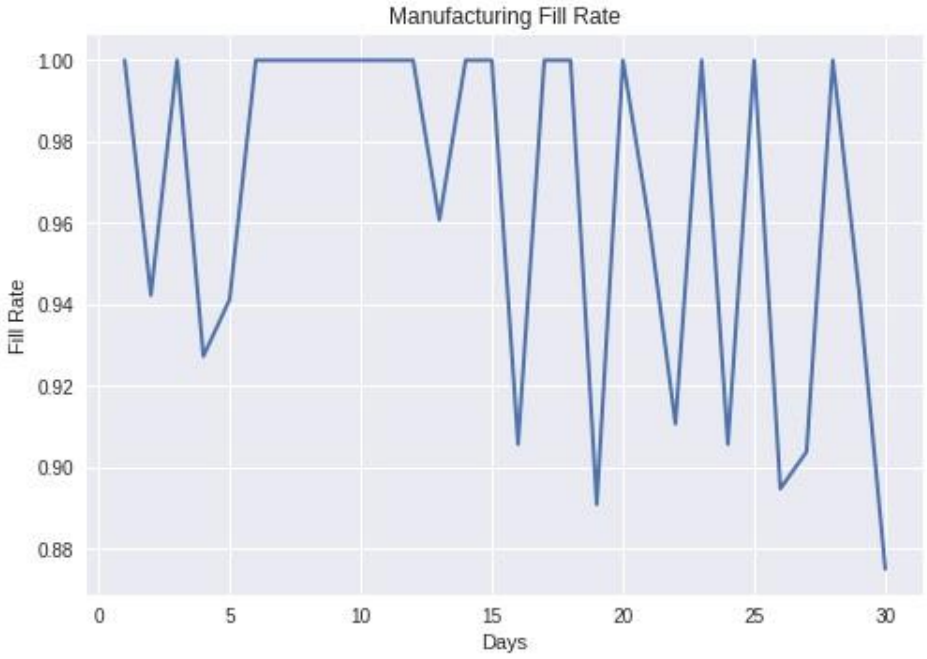

Figure 42: Attack scenario (no resilience) Manufacturing Fill Rate.

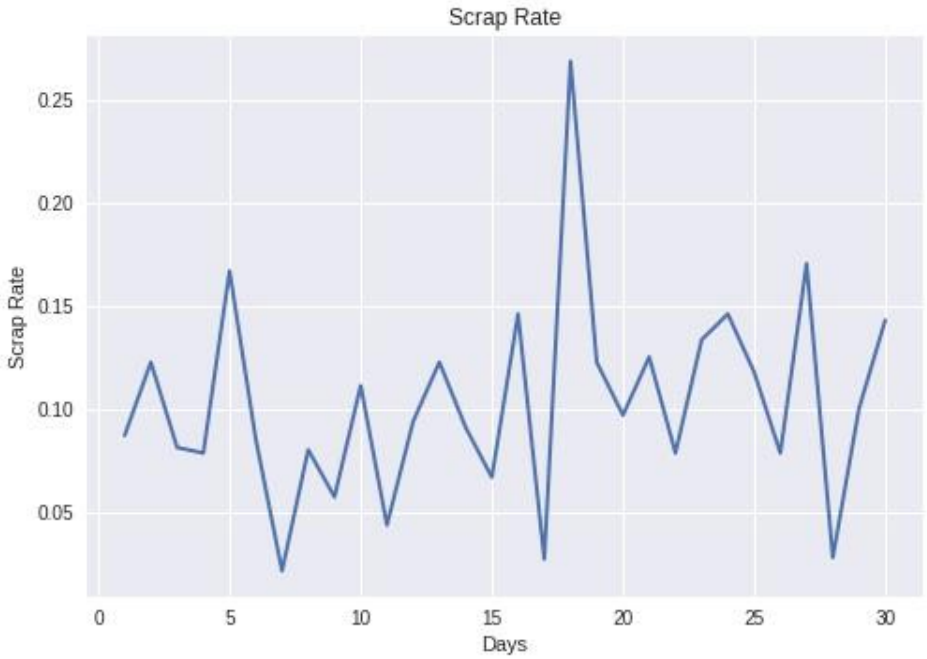

Figure 43: Attack scenario (no resilience) Scrap Rate

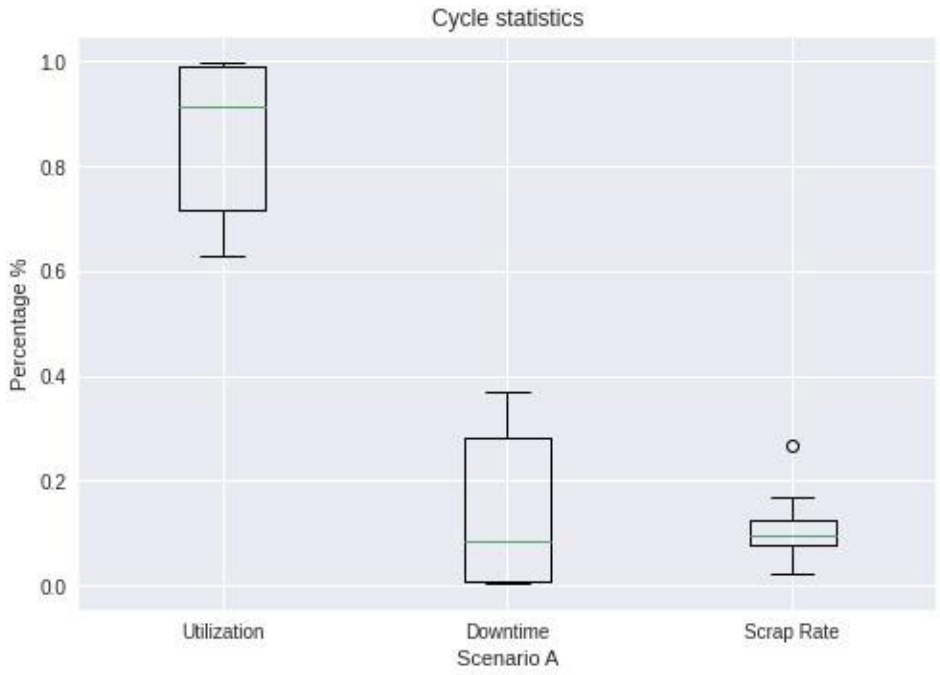

Figure 44: Attack scenario (no resilience) Cycle statistics.

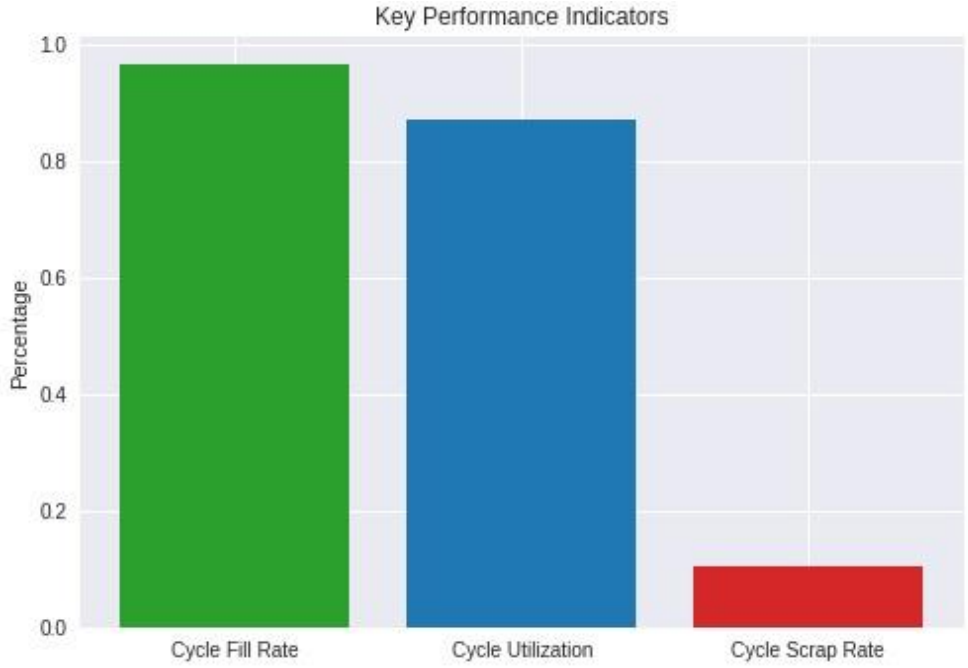

Figure 45: Attack scenario (no resilience) Key Performance Indicators.

Paradoxically enough, the cycle fill rate fell to 98% in comparison with our baseline. The attack, however, had no negative effect on any of the manufacturing indicators. This seems to put into evidence that the severity of a cyber-attack is not only a function of its characteristics but rather a function of the timing and the current state of the CMS.

5.6 CMS exhaustive attack scenario

Following the insight that a cyber-attack severity against a CMS cannot be estimated based only on the characteristics of the attack but rather it has to be in conjunction with the current state of the system. We devise an exhaustive experiment in which we analyze the behavior of the CMS if the attack were to occur at every minute. For this scenario, we run 480 iterations of the same working day. The orders were calculated before running it as well as the processing time. Figures 46 and 47 show how after minute 400 for instance, the Fill Rate never drops below 90% and the scrap rate never surpass 22%. This knowledge of the system can help us understand when an operational resilience mechanism is needed. The advent of that particular attack at a certain time can’t degrade the system below its threshold.

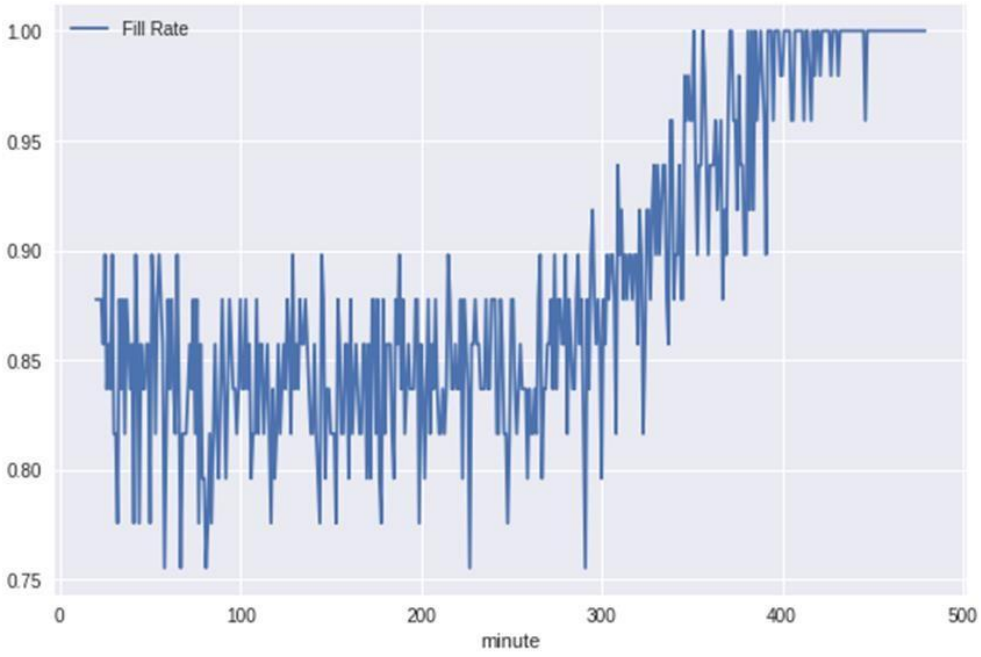

Figure 46: CMS exhaustive attack scenario Fill Rate.

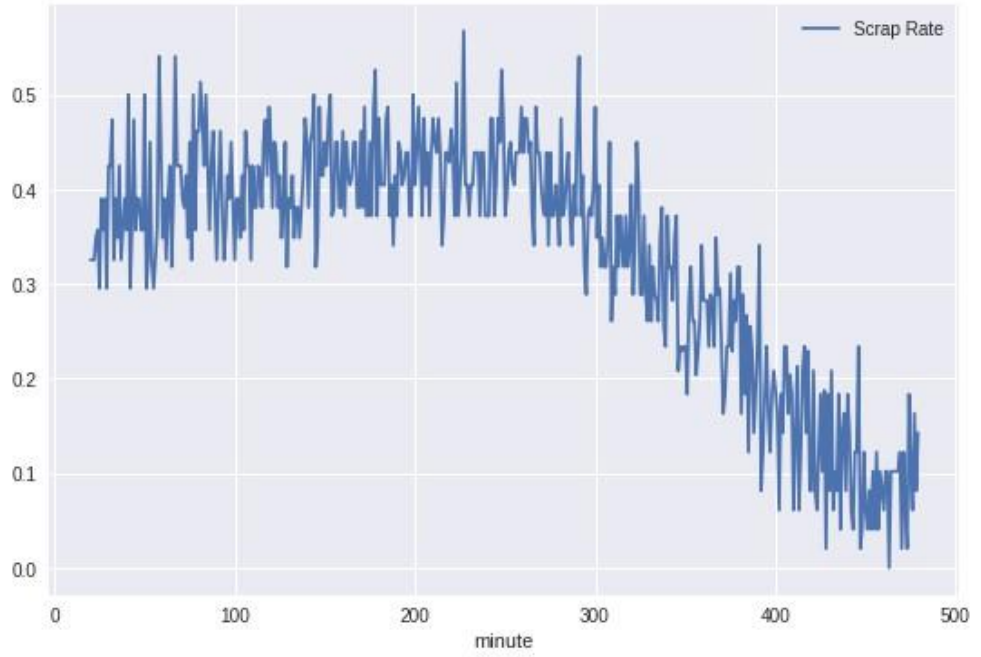

Figure 47: CMS exhaustive attack scenario Scrap Rate.

The other important production factor that can be used to determine the effects of the attack is the number of orders in the cycle. So, following that notion, another experiment is set in which the experiment is repeated not only 480 times but a combination of that and every possible number of orders that the system can receive within the observed distribution. This type of work generated a large number of data points that can be plotted to further understand how these two variables affect the ultimate severity of the attack in the production KPIs. Is important to remember that in these simulations we are allowing the attacker to be successful.

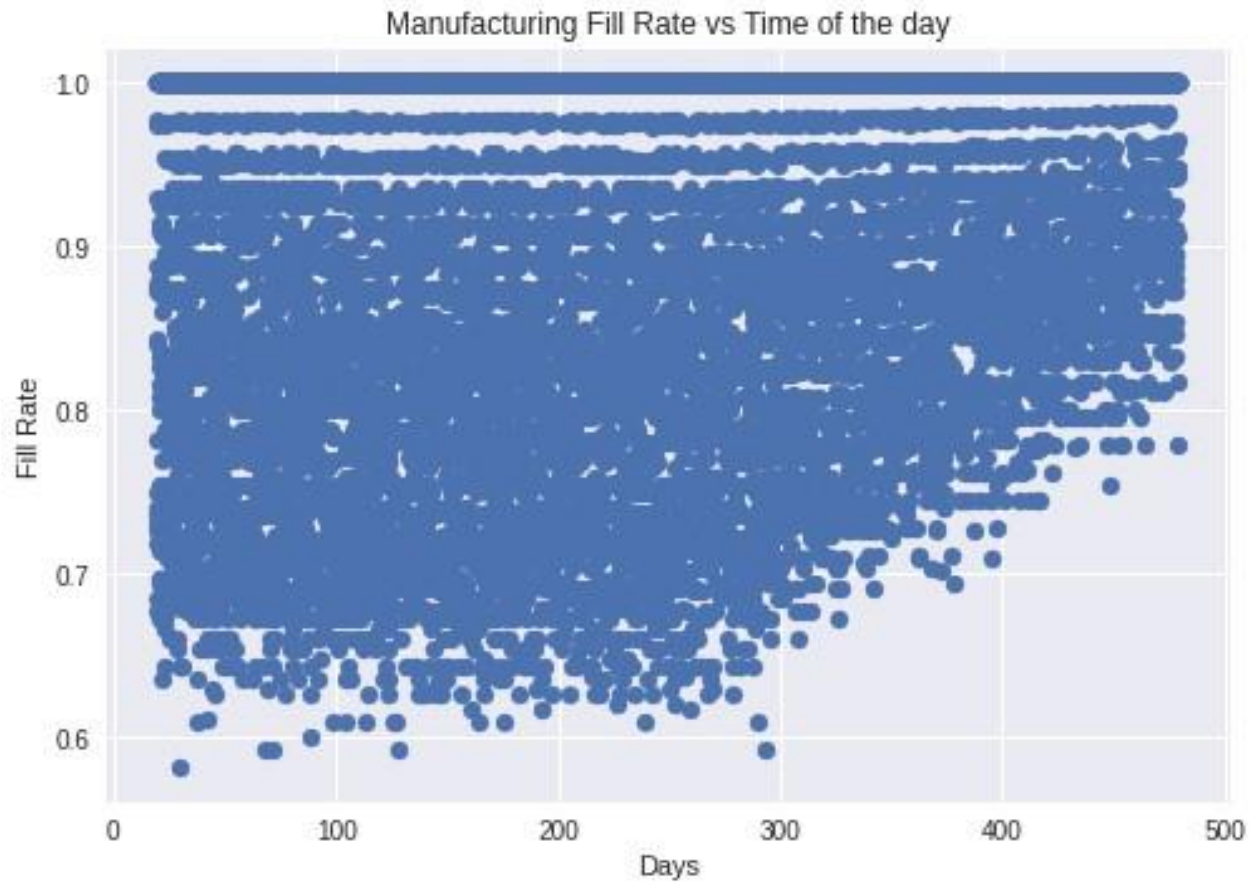

Figure 48: CMS exhaustive attack scenario Fill Rate vs Time of the day.

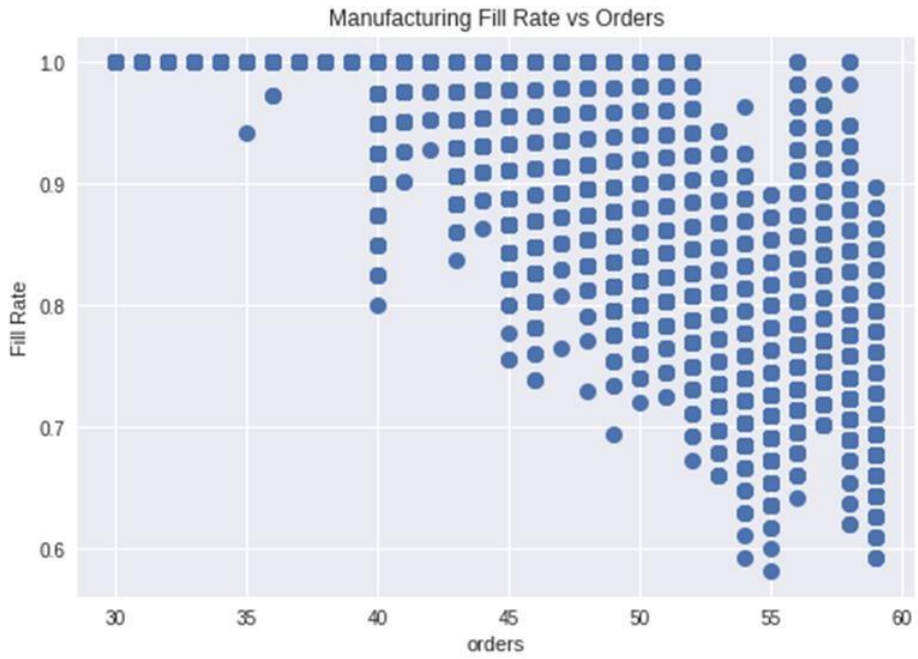

Figure 49: CMS exhaustive attack scenario Fill Rate vs Orders.

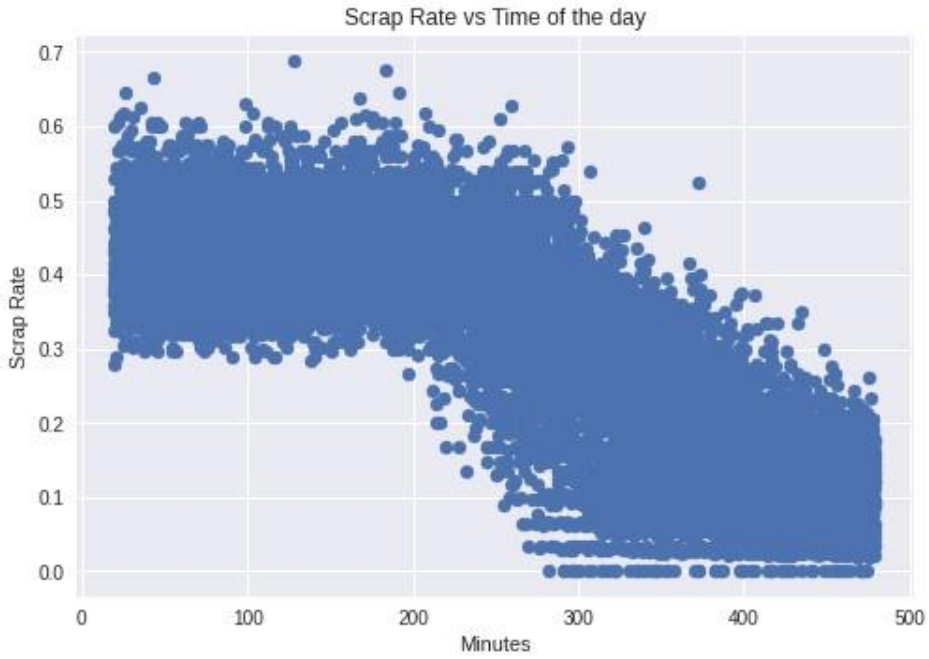

Figure 50: CMS exhaustive attack scenario Scrap Rate vs Time of the day.

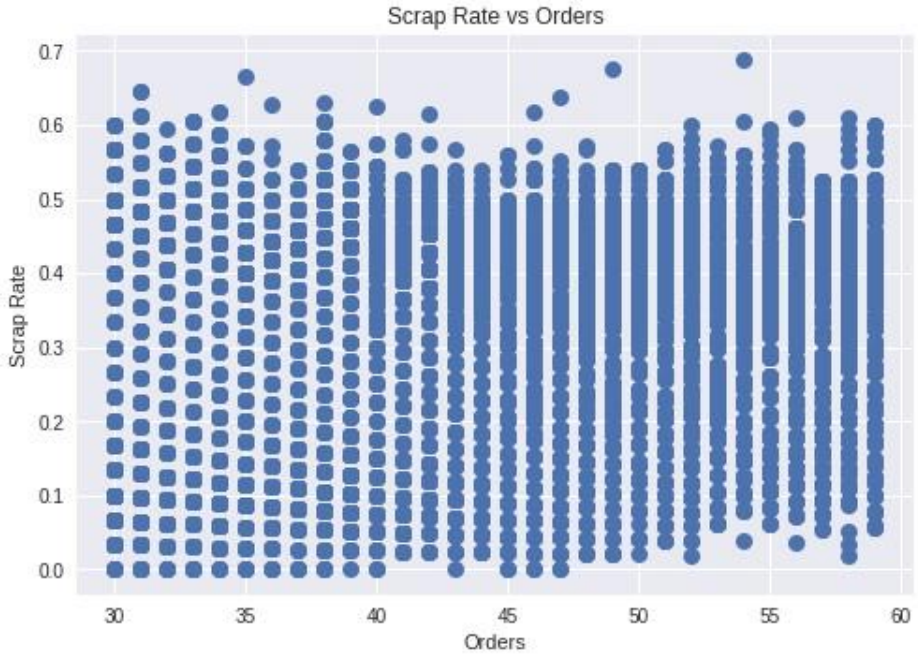

Figure 51: Figure 39: CMS exhaustive attack scenario Scrap Rate vs Orders.

Visually one can already infer that there is a correlation between the number of orders, the minute of the advent of the attack, and the ultimate effect on the target KPI. For a more comprehensive view, we elaborate a 2-dimensional heat map in which both the Scrap Rate and Fill Rate are plotted against the number of orders received and the minute of the attack. From this, we can realize that there are critical areas in which the attack cannot affect the KPIs below degradation thresholds. In these regions, the system does not need to trigger any resilience mechanism.

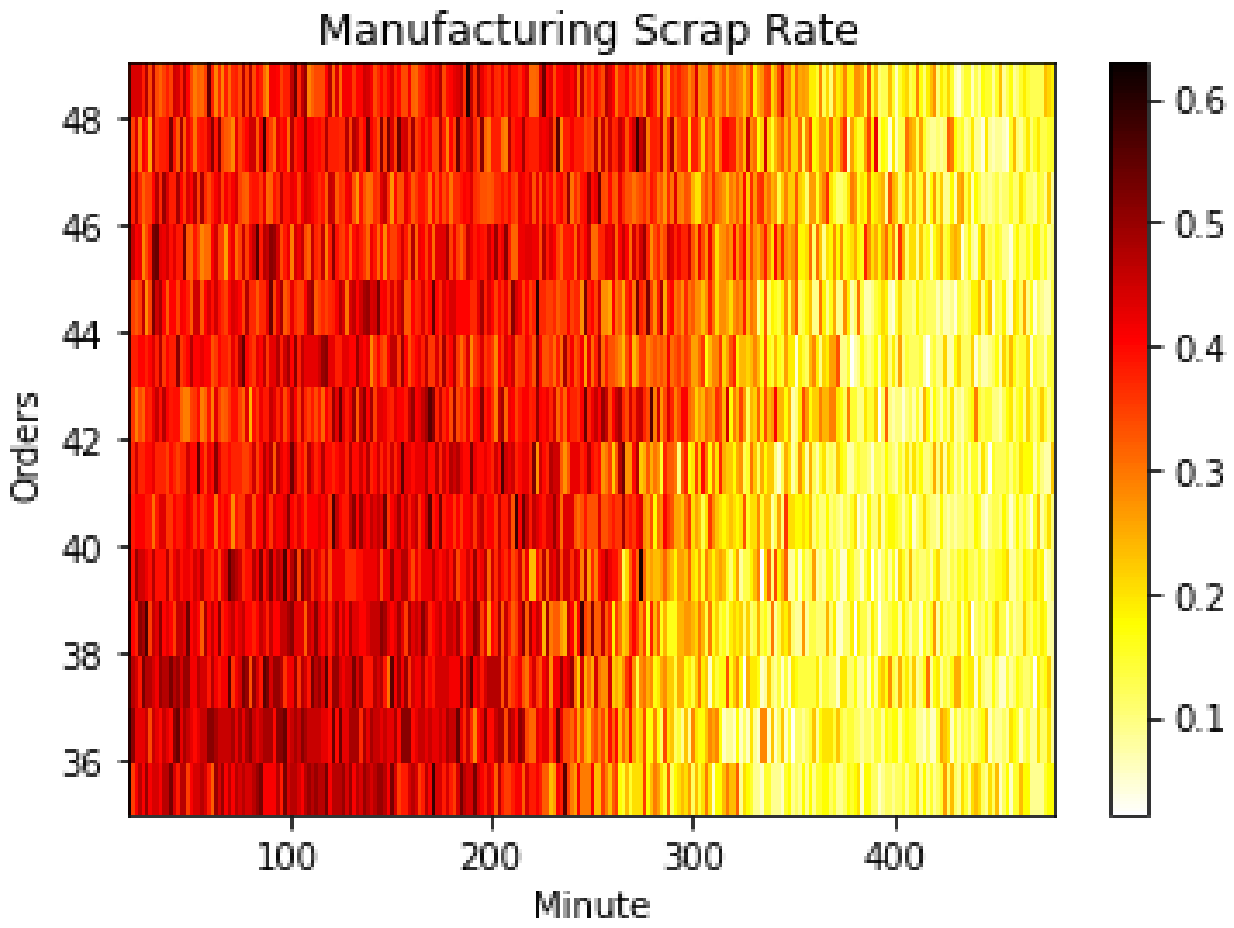

Figure 52: CMS exhaustive attack scenario Manufacturing Scrap Rate vs Orders vs Minute.

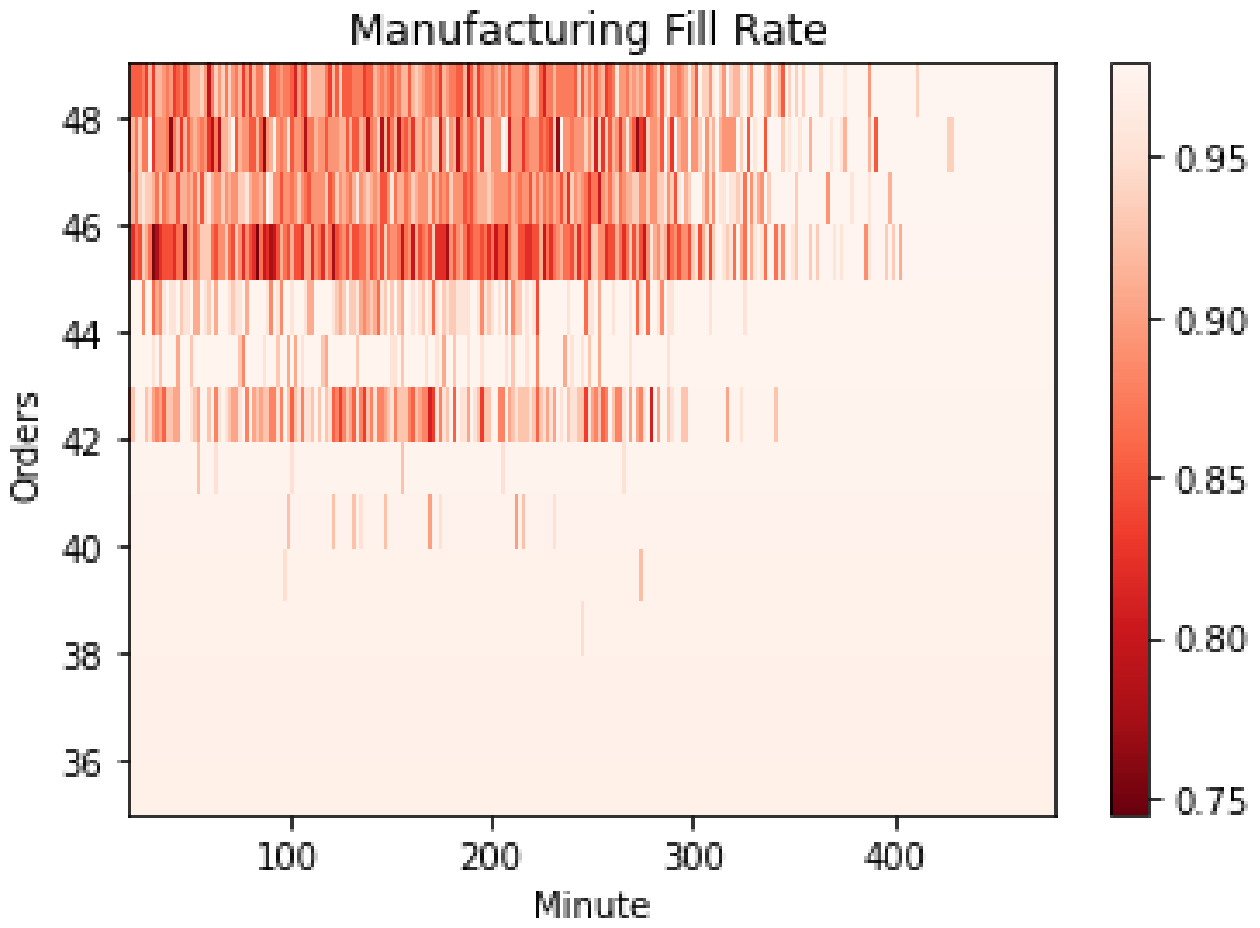

Figure 53: CMS exhaustive attack scenario Manufacturing Fill Rate vs Orders vs Minute.

The final step in our analysis is then to build a prediction tool that enables us to determine the need for a resilience mechanism. The system should activate any extra layer of defense in case the attack has the potential to degrade the system below the threshold. Utilizing a linear regression one can obtain a prediction with a mean square error of only 1% that can effectively determine the effect of the attack in the target indicator (Scrap Rate as an illustration).

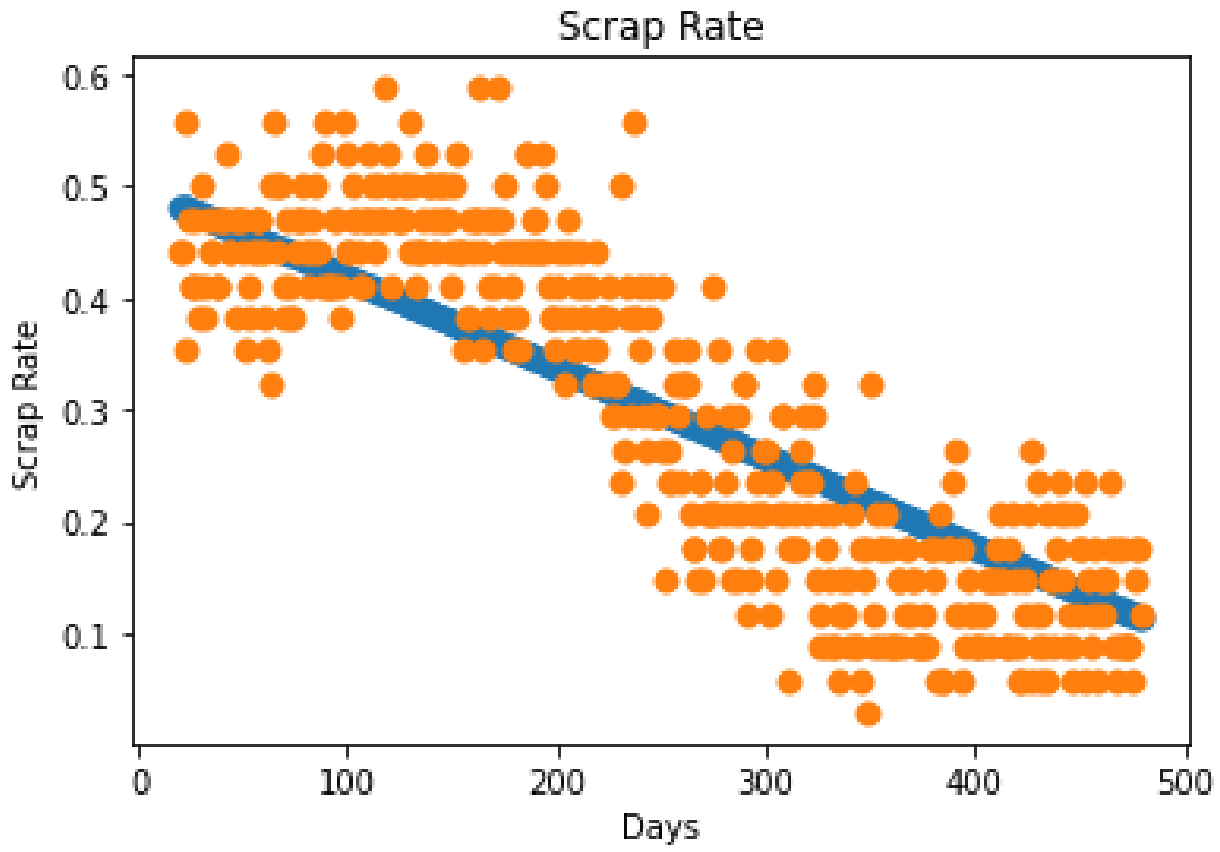

Figure 54: CMS exhaustive attack scenario Scrap Rate Linear Regression

Table 3: CMS exhaustive attack scenario Linear Regression.

Mean Square Error:	0.01
Coefficient of determination:	0.654
Intercept:	0.447
Slope:	[-0.0008, 0.0015]

We can conclude then:

- Target cycle KPIs is an unreliable source, and resilience policy needs to be evaluated each day, and at the time the attack happens.
- The severity of the attack is correlated to the timing, the same attack on different states of the production cycle has vastly different results.
- Estimation of Fill rate based on orders and timing of the attack.

$$KPI = a_1 * minute + a_2 * orders$$

- A policy can be enforced to determine if a resilience mechanism is needed to preserve operational resilience at the advent of the attack.

5.7 Demonstration of Operational resilience framework

1. Identify

The objective of this framework is to utilize the experimental results as the basis for a strategy for enhancing the operational resilience of a cyber-manufacturing system (CMS). Thus, now that we understand how the different conditions in which an attack occurs correlate with its impact on the manufacturing Key Performance Indicators (KPIs) we can proceed to deploy the strategy.

Figure 55 summarizes the results of the identification phase. Our system consists of an online order management tool, a scheduler that works at the beginning of each day, and a 3D printer that utilizes additive manufacturing to fulfill orders. In normal operating conditions, the system can expect a Fill Rate of 95% and a Quality Rate of 90%. Availability varies considerably as a consequence of the demand, and as long as the previous targets are met, is not a special concern. For our study, we utilize the kinetic attack described in the earlier section, in which an attacker injects a flawed design into our system resulting in an increased scrap rate. This will last for as long as it takes us to detect and recover from it. An anomaly detection mechanism is installed in the accelerometer to help detect deviations and a manual recovery procedure is set in place which will solve the issue.

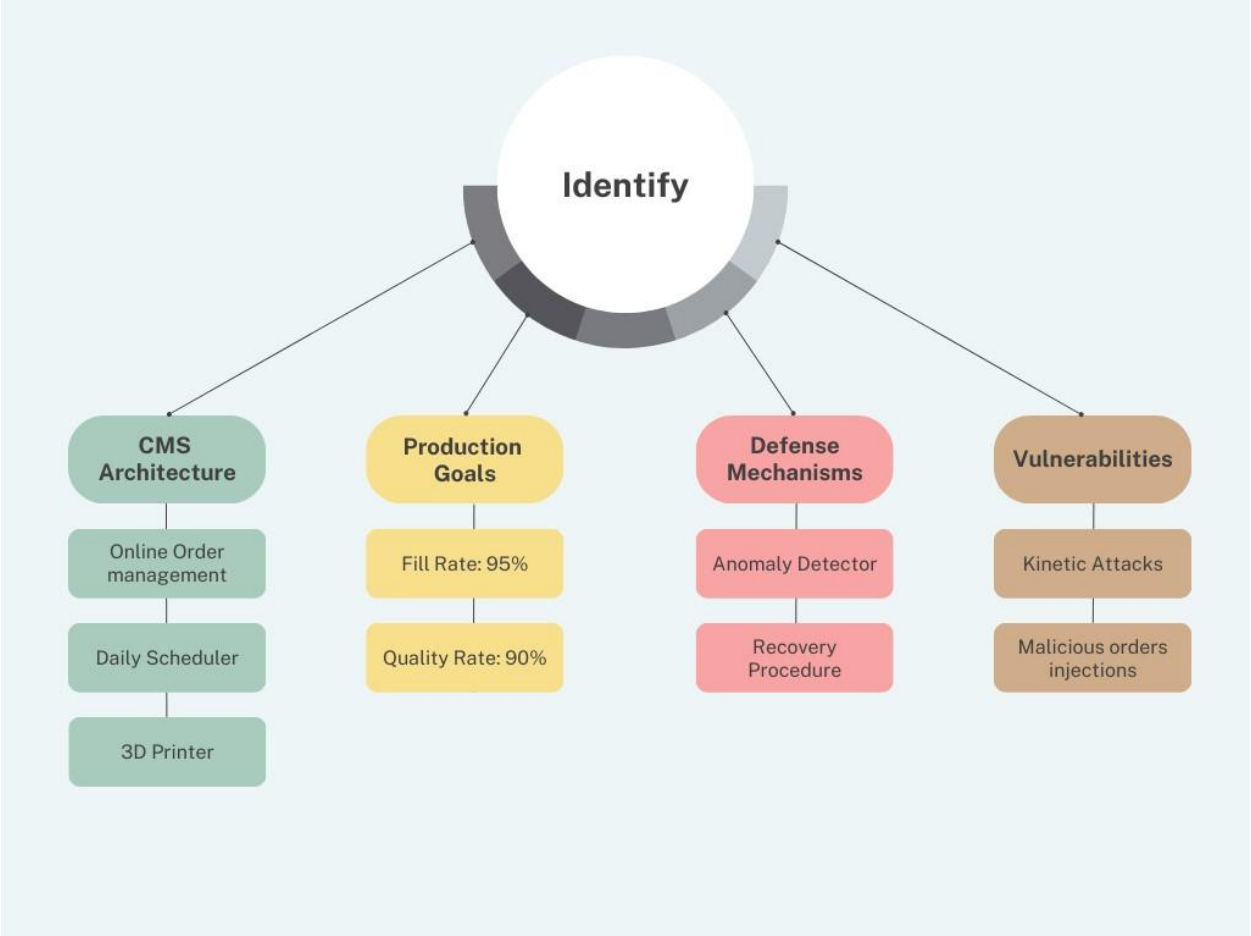

Figure 55: Step 1: Identify.

2. Establish

The main difference between our approach and the current state of the art is the correlation of security targets with the goals of the system. The exhaustive analysis of the advent of the same cyber-attack on the CMS under different operation conditions allowed us to establish a correlation between KPIs and the timing/number of orders. For this particular study, we are going to show the established step against

a kinetic attack. While the attack directly impacts the quality rate, its effect is also felt in the fill rate of the system. It is a managerial decision to establish appropriate degradation thresholds as the decision-making process will depend on them. In our case, the Fill Rate must never go below 85% on any given production day, nor the Quality Rate below 80%.

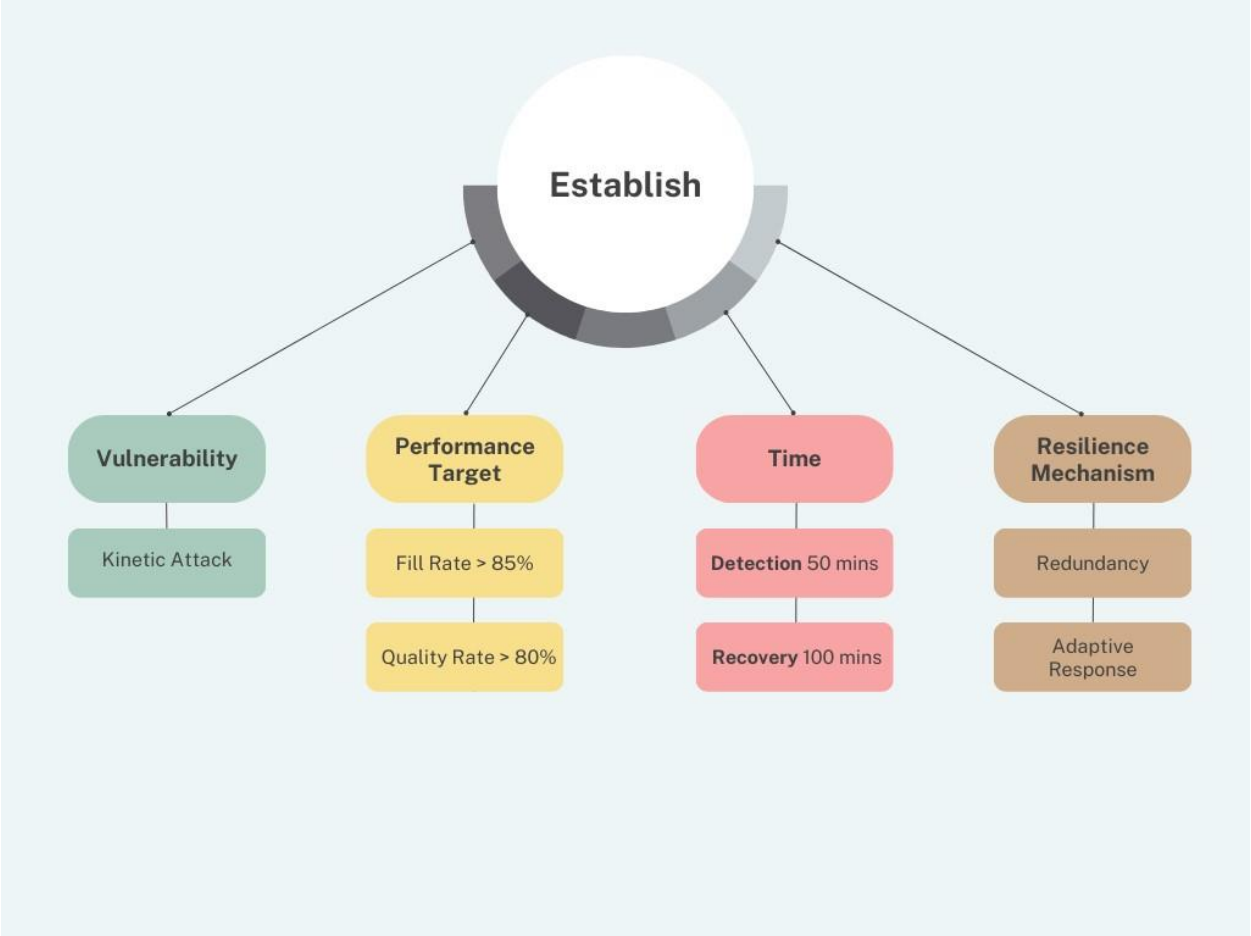

Figure 56: Step 2: Establish.

From figures 52 and 53 we can map the critical regions in which an attack could lower the KPIs below their threshold. Thus, establishing the zones in which a

response is needed. For maintaining the operational resilience regarding Fill Rate only if the attack happens before minute 350 and when there are more than 42 orders a response is needed. It is important to note that the system should always attempt to recover, but no more action is needed in terms of operational resilience. The system cannot be degraded below the threshold under those circumstances by that attack.

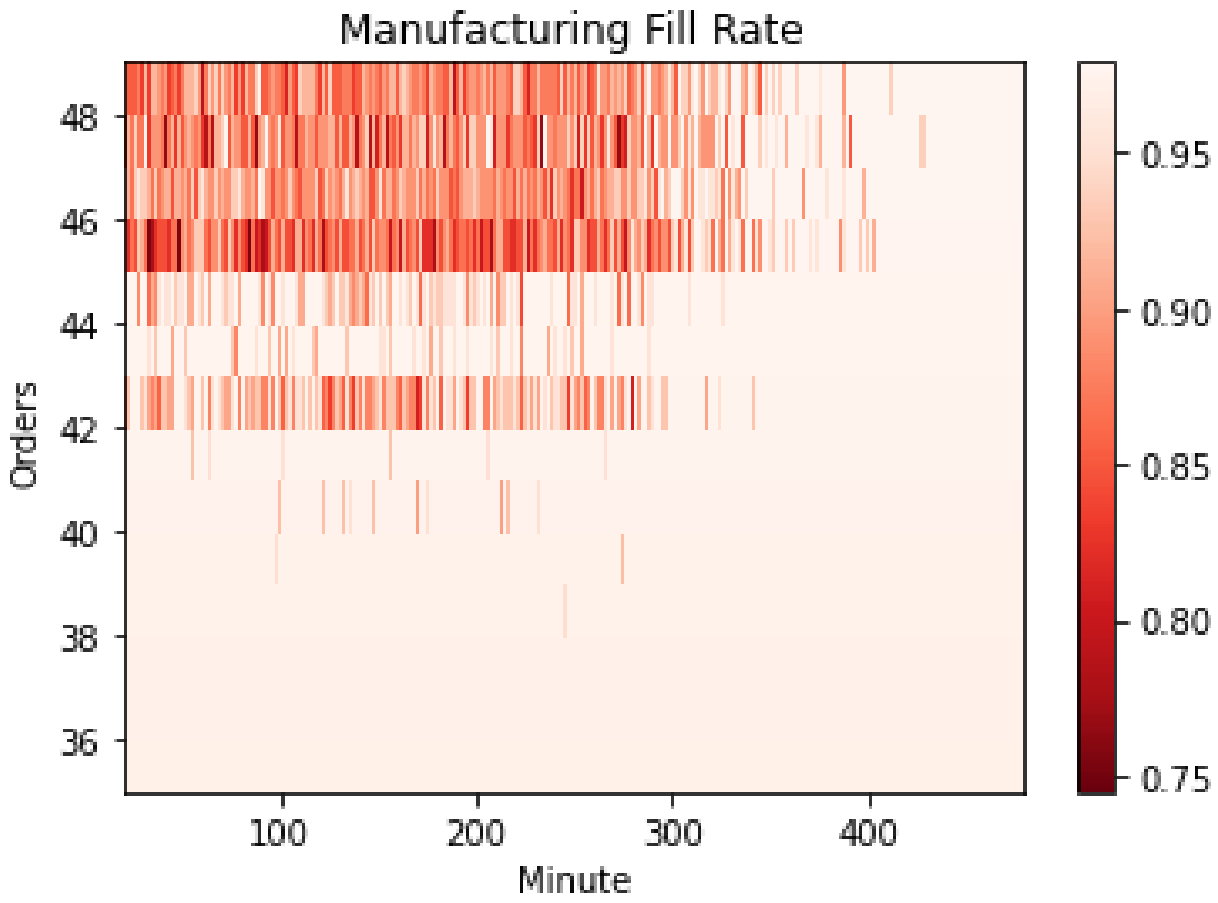

Figure 57: Fill Rate response region.

3. Select

With the knowledge of the response region against this particular attack we can select the appropriate response. Our goal is to know when our system should not simply react to cyber-attacks, so we do not induce more stress into our system by responding to a threat without the potential to degrade the CMS below thresholds. In that critical region, redundancy should be considered, either a different printer or back order.

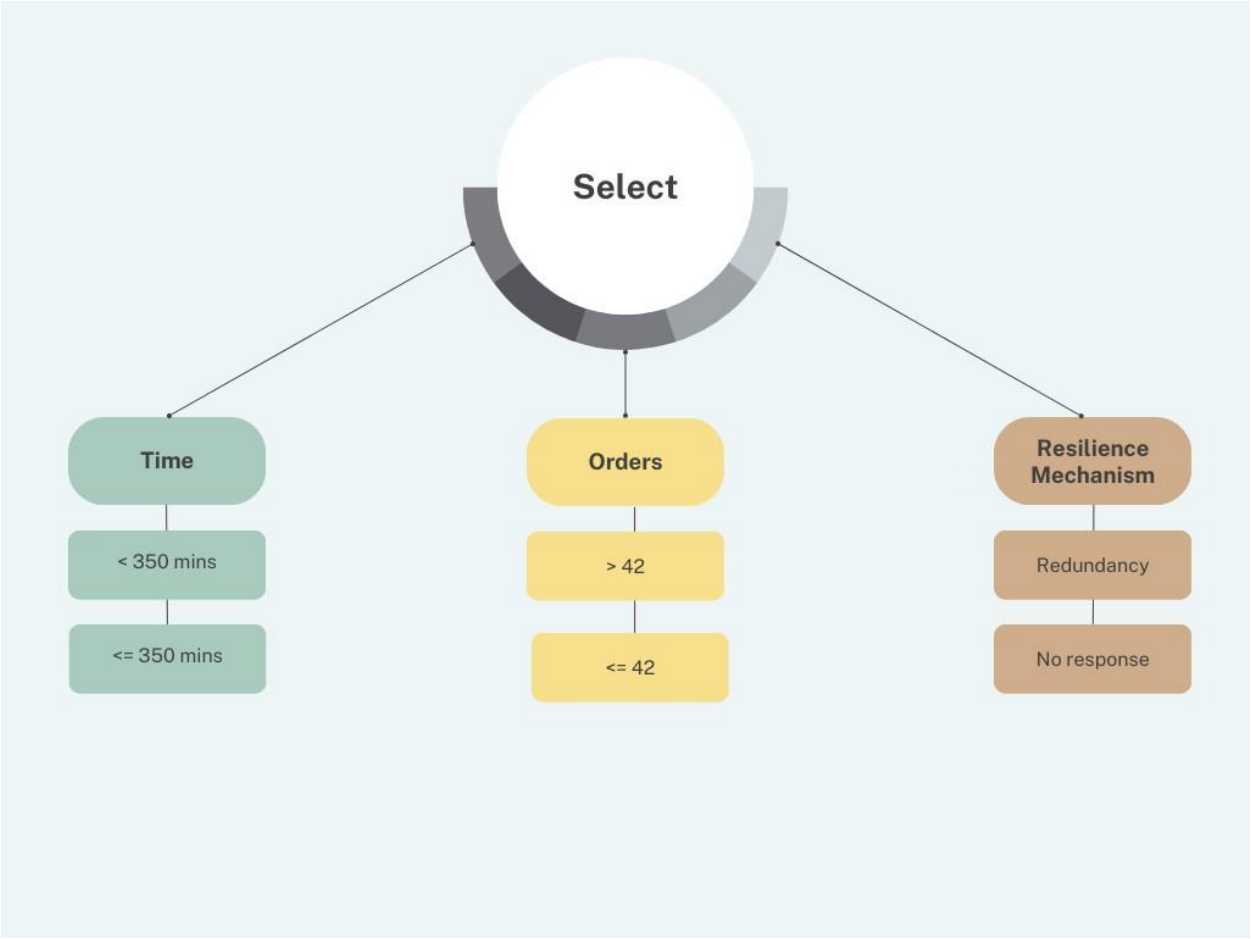

Figure 58: Step 3: Select.

4. Deploy

Lastly and perhaps more crucial is the deployment of a strategy that enhances the operational resilience of the system such that the known attacks don't degrade the performance below the threshold. We propose continuous monitoring of threats with an estimation of their effect on the target KPIs. Thus, the activation of each mechanism will follow the policy generated.

Chapter 6: Conclusions and Future Work

This research proposes an operational resilience-enhancing framework for Cyber-manufacturing systems against cyber-attacks. It consists in identifying the manufacturing goals and cyber-vulnerabilities, establishing performance targets, selecting resilience-enhancing mechanisms, and deploying them into the operation of the system. This chapter presents the summary of the work, contribution, and expected impact on the field. Finally, the future work required to complete the dissertation is presented.

6.1 Summary

This dissertation proposes a novel framework to enhance the operational resilience of cyber-manufacturing systems against cyber-attacks. Cyber manufacturing systems (CMS) are interconnected production environments comprised of complex and networked cyber-physical systems (CPS) that can be instantiated across one or many locations. While it offers enhanced productivity and efficiency than traditional manufacturing, its inherent properties open the door for new cybersecurity vulnerabilities. Defense mechanisms need to be implemented to prevent, detect, and recover from cyber-attacks. Furthermore, CMS demands the ability to remain operational during the window of time comprised of the advent of a cyber-attack until the system recovers. This is a property known as operational resilience, a system's ability to withstand cyber-attacks, faults, and failures and continue to operate in a degraded state to carry out its mission. Thus, an operational resilient CMS is capable of withstanding disruptions arising from cyber-attacks while maintaining availability, utilization efficiency, and a quality ratio above degradation thresholds until recovery.

The framework consists of four steps: 1) Identify: map CMS production goals, vulnerabilities, and resilience-enhancing mechanisms; 2) Establish: set targets of performance in production output, scrap rate, and downtime at different states; 3)

Select: determine which mechanisms are needed and their triggering strategy, and 4) Deploy: integrate into the operation of the CMS the selected mechanisms, threat severity evaluation, and activation strategy.

This novel approach correlates the state of production and the timing of the attack to predict the effect on the manufacturing key performance indicators. Then a real-time decision strategy is deployed that selects the appropriate response to maintain availability, utilization efficiency, and a quality ratio above degradation thresholds until recovery. Our goal is to demonstrate that the operational resilience of CMS can be enhanced such that the system will be able to withstand the advent of the attack while remaining operationally resilient. react to the threats, analyze the expected severity in real-time, and taking decisions based on the performance targets. We expect that the system will be able to withstand the advent of the attack during the time that it takes to recover from it, thus remaining operationally resilient.

6.2 Contribution

This research aims to contribute to the design of more resilient cyber manufacturing systems. In support of this statement, this dissertation describes the following contributions.

Operational Resilience of Cyber-manufacturing Systems (CMS) against cyber-attacks. It provides a theoretical foundation for understanding operational resilience in the context of cyber-manufacturing systems against cyber-attacks. An analysis of the current state-of-the-art literature is presented which shows that simply applying concepts derived from cyber-physical systems (CPS) is not enough to capture the socioeconomic nature of manufacturing. It shows that the widespread adoption of CMS and the realization of the 4^{th} industrial revolution is contingent on addressing the security concerns raised by the growing materialization of cyber threats.

Framework to improve the operational resilience of Cyber-manufacturing Systems CMS against cyber-attacks. This work provides a framework that connects the technical analysis of vulnerabilities, defense mechanisms, and production goals to the implementation of a policy to determine the need for a

response. It allows the characteristics of the CMS to dictate the response to a cyber threat and provides a clear path to the implementation of an operational policy.

Correlating the effects of a cyber-attack with the current state of the Cyber-manufacturing System (CMS). Through simulation, we prove that the same attack can have vastly different consequences in the manufacturing of Key Performance Indicators (KPIs) as a function of the current state of the system. This seems to put into evidence that the severity of a cyber-attack is not only a function of its characteristics but rather a function of the timing and the current state of the CMS.

Predicting the effect of a cyber-attack on the Cyber-manufacturing System (CMS) on the Key Performance Indicators (KPIs). Lastly, this work shows a prediction tool for the effect of a cyber-attack on the KPIs with a 1% mean square error. Modeling a system and conducting an exhaustive simulation of the advent of an attack can allow the decision-making to know in advance the damage potential a threat has at every point in time. With this, a policy can be enforced in which a reaction is only needed when the prediction shows that the degradation of the system will be below the acceptable threshold.

6.3 Limitations and Future Work

While recent years have shown that manufacturing is now the most targeted industry by attackers obtaining data from real attacks remains the biggest challenge in understanding them. Companies don't make those datasets widely available so simulation is the tool that can better allow us to study the operational resilience of cyber-manufacturing systems under attack.

Future work should focus on introducing more complexity, as our work was focused on proving that a correlation between the state of the system and the severity of cyber-attack exist; now we can consider studying other types of the production system. Vary the scheduling policies, introduce more attacks, vary the resilience mechanisms available, allow for orders to carry over, and other practical manufacturing considerations. The foundation has been established and we know that the severity of the attack is determined by the state of the CMS, thus, future experimentation can incorporate more nuanced details. The exploration of more complex systems will enable the modeler to build more accurate optimization equations to select the appropriate resilience response to the threats. Furthermore, implementing more sophisticated attack methodologies will showcase the limitations of this approach in which we assume a fixed effect of each attack.

There is a clear path in which the inclusion of game theory concepts will open the doors to the exploration of the adversary nature of cyber-attacks. Technologies like reinforcement learning (RL) and Digital Twin (DT) can also be explored as they will allow us to model more complex behaviors and find out the optimal resilience enhancing policy at each of the different system states. Perhaps the most important insight of this work is that the effect the cyber-attack has on the system is dependent on the current state of the production indicators. This knowledge can be leveraged so that the system operational resilience policy can be optimized as a function of the production constraints and aimed to optimize for the current production targets.

Lastly, we believe is important to deploy this strategy in a real system. The next steps of this research should be developed around exploring in real time the advent of cyber-attacks in which the behavior of the system can be used to learn and enhance the initial understanding that one can generate from simulation.

References

Akbanov, M. and Vassilakis, V. “WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention and Propagation Mechanisms.” *Journal of Telecommunications and Information Technology*. 2019. Vol. 1, pp. 113-124. DOI:10.26636/jtit.2019.130218.

Allen, P., Datta, P., and Christopher, M. “Improving the Resilience and Performance of Organizations Using Multi-Agent Modelling of a Complex Production–Distribution Systems.” *Risk Management*. 2006. Vol. 8, pp. 294–309. DOI:10.1057/palgrave.rm.8250019.

AL-Salman, H. I., and Salih, M. H. “ A review Cyber of Industry 4.0 (CyberPhysical Systems (CPS), the Internet of Things (IoT) and the Internet of Services (IoS)): Components, and Security Challenges.” *Journal of Physics: Conference Series*. 2019. Vol. 1424. DOI:10.1088/1742-6596/1424/1/012029.

Atzori, L., Iera, A., and Morabito, G. “The Internet of Things: A survey.” *Computer Networks*. 2010. Vol. 54(15), pp. 2787–2805. DOI:/10.1016/j.comnet.2010.05. 010.

Audinot, M., Pinchinat, S., and Kordy, B. " Guided Design of Attack Trees: A System-Based Approach." *2018 IEEE 31st Computer Security Foundations Symposium (CSF)*. 2018. Pp. 61-75. DOI:10.1109/CSF.2018.00012.

Babiceanu, R. and Seker, R. "Trustworthiness Requirements for Manufacturing Cyber-physical Systems." *Procedia Manufacturing*. 2017. Vol. 11, pp. 973-981. DOI:10.1016/j.promfg.2017.07.202.

Babiceanu, R. and Seker, R. "Cyber resilience protection for industrial internet of things: A software-defined networking approach." *Computers in Industry*. 2019. Vol. 104, pp. 47-58. DOI:10.1016/j.compind.2018.10.004.

Balistri, E., Casellato, F., Collura, S., Giannelli, C., Riberto, G., and Stefanelli, C. "Design Guidelines and a Prototype Implementation for Cyber-Resiliency in IT/OT Scenarios based on Blockchain and Edge Computing." *IEEE Internet of Things Journal*. 2021. DOI: 10.1109/JIOT.2021.3104624.

Barreno, M., Nelson, B., Joseph, A. D., and Tygar, J. D. "The security of machine learning." *Machine Learning*. 2010. Vol. 81(2), pp. 121–148. DOI:10.1007/s10994010-5188-5.

Bécue, A., Maia, E., Feeken, L., Borchers, P., and Praça, I. "A New Concept of Digital Twin Supporting Optimization and Resilience of Factories of the Future." *Applied Sciences*. 2020. Vol. 10(13), pp. 4482. DOI:10.3390/app10134482.

Bhatia, G., Lane, C., and Wain, A. " Building Resilience in Supply Chains." *World Economic Forum*. 2013. URL:http://www3.weforum.org/docs/WEF_RRN_MO_BuildingResilienceSupplyChains_Report_2013.pdf.

Bicaku, A., Schmittner, C., Tauber, M., and Delsing, J. "Monitoring Industry 4.0 applications for security and safety standard compliance." *2018 IEEE Industrial Cyber-Physical Systems (ICPS).* 2018. Pp. 749–754. DOI:10.1109/ICPHYS.2018.8390801.

Bishop, M., Conboy, H. M., Phan, H., Simidchieva, B. I., Avrunin, G. S., Clarke, L. A., Osterweil, L. J., and Peisert, S. "Insider Threat Identification by Process Analysis." *2014 IEEE Security and Privacy Workshops*. 2014. Pp. 251–264. DOI:10.1109/SPW.2014.40.

Bodin, P., and Wiman, B. "Resilience and Other Stability Concepts in Ecology: Notes on their Origin, Validity, and Usefulness." *ESS Bulletin*. 2006. Vol. 2, pp. 33-43.

Boulares, S., Adi, K., and Logrippo, L. "Insider Threat Likelihood Assessment for Flexible Access Control." *In E. Aïmeur, U. Ruhi, & M. Weiss (Eds.), ETechnologies: Embracing the Internet of Things*. 2017. Vol. 289, pp. 77–95. DOI:10.1007/978-3-319-59041-7_5.

Bruneau, M, Chang, S., Eguchi, R., Lee, G., O'Rourke, T., Reinhorn, A., Shinozuka, M., Tierney, K., Wallace, W., and Winterfeldt, D. "A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities." *Earthquake Spectra*. 2003. Vol. 19(4), pp. 733-752. DOI:10.1193/1.1623497.

Buldas, A., Laud, P., Priisalu, J., Saarepera, M., and Willemson, J. "Rational Choice of Security Measures Via Multi-parameter Attack Trees." *In J. Lopez (Ed.), Critical Information Infrastructures Security*. 2006. Pp. 235–248. DOI:10.1007/11962977_19.

Campbell, T. A., and Ivanova, O. S. "Additive Manufacturing as a Disruptive Technology: Implications of Three-Dimensional Printing." *Technology & Innovation*. 2013. Vol. 15(1), pp. 67–79. DOI:10.3727/194982413X13 608676060655.

Carías, J., Labaka, L., Sarriegi, J., and Hernantes, J. "Defining a Cyber Resilience Investment Strategy in an Industrial Internet of Things Context." *Sensors*. 2019. Vol. 19(1), pp. 138. DOI:10.3390/s19010138.

Cianci, Jessica. "The SolarWinds Software Hack: A Threat to Global Cybersecurity." 2021. *Jolt Digest.* URL:https://jolt.law.harvard.edu/digest/thesolarwinds-software-hack-a-threat-to-globalcybersecurity.

Chen, H. “ Applications of Cyber-Physical System: A Literature Review.” *Journal of Industrial Integration and Management*. 2017. Vol. 2(3), pp. 1750012. DOI:10.1142/S2424862217500129.

Cheng, Y., Chen, K., Sun, H., Zhang, Y., and Tao, F. “Data and knowledge mining with big data towards smart production.” *Journal of Industrial Information Integration*. 2018. Vol. 9, pp. 1–13. DOI:10.1016/j.jii.2017.08.001.

Chhetri, S. R., Canedo, A., and Faruque, M. A. A. “KCAD: Kinetic Cyber-attack detection method for Cyber-physical additive manufacturing systems.” *2016 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*. 2016. Pp. 1–8. DOI:10.1145/2966986.2967050.

Collins, S. and McCombie, S. “Stuxnet: the emergence of a new cyber weapon and its implications.” *Journal of Policing, Intelligence and Counter Terrorism*. 2012. Vol. 7(1), pp. 80-91. DOI:10.1080/18335330.2012.653198.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. Computers & Security. 2013. Vol. 32, pp. 90–101. DOI:10.1016/j.cose.2012.09.010.

Cybersecurity & Infrastructure Security Agency. “Cyber Threats to Critical Manufacturing Sector Industrial Control Systems (ICS).” 2021. URL:

https://www.cisa.gov/sites/default/files/publications/CISA%20Insight%20Control%20Systems%2023Dec2021_508%20Updated.pdf.

Department of Homeland Security. “National Strategy for Supply Chain Security.” United States Federal Government. Washington D.C. 2012. URL:https://obamawhitehouse.archives.gov/sites/default/files/national_strategy_for_global_supply_chain_security.pdf.

Dibaji, S., Mehran, P., Mohammad, F., David B., Annaswamy, A., Johansson, K., and Chakrabortty, A. "A systems and control perspective of CPS security." *Annual Reviews in Control.* 2019. Vol. 47, pp. 394-411. DOI:10.1016/j.arcontrol.2019.04.011.

Engle, P.L., Castle, S., and Menon, P. “Child development: Vulnerability and resilience.” *Social Science & Medicine*. 1996. Vol. 43(5), pp. 621-635.

Espinoza-Zelaya, C. and Moon, Y. "Taxonomy of severity of cyber-attacks in cyber-manufacturing systems." *Proceedings of the ASME 2022 International Mechanical Engineering Congress and Exposition. Volume 2B: Advanced Manufacturing*. Columbus, Ohio. October 30-November 3, 2022. DOI:10.1115/IMECE2022-94492.

Espinoza-Zelaya, C. and Moon, Y. "assessing the severity of cyber-attacks against cyber-manufacturing systems." *Proceedings of the ASME 2022 International*

Mechanical Engineering Congress and Exposition. Volume 2B: Advanced Manufacturing. Columbus, Ohio. October 30-November 3, 2022.

Espinoza-Zelaya, C. and Moon, Y. “Resilience Enhancing Mechanisms for Cyber-Manufacturing Systems against Cyber-Attacks.” *IFAC-PapersOnLine.* 2022. Vol. 55 (10), pp. 2252-2257. DOI:10.1016/j.ifacol.2022.10.043.

Espinoza-Zelaya, C. and Moon, Y. "Resilient Cyber-Manufacturing Systems Under Cyber Attacks." *Proceedings of the ASME 2021 International Mechanical Engineering Congress and Exposition. Volume 2B: Advanced Manufacturing*. V02BT02A011. Virtual, Online. November 1–5, 2021. DOI:10.1115/IMECE202170019.

Essuman, D., Boso, N., and Annan, J. “Operational resilience, disruption, and efficiency: Conceptual and empirical analyses.” *Int J Prod Econ*. 2020. DOI:10.1016/j.ijpe.2020.107762.

Frazzon, E. M., Hartmann, J., Makuschewitz, T., and Scholz-Reiter, B. “Towards Socio-Cyber-Physical Systems in Production Networks.” *Procedia CIRP*. 2013. Vol. 7, pp. 49–54. DOI:10.1016/j.procir.2013.05.009.

Ghaleb, A., Zhioua, S., and Almulhem, A. “On PLC network security.” *International Journal of Critical Infrastructure Protection.* 2018. Vol. 22, pp. 62–69. DOI:10.1016/j.ijcip.2018.05.004.

Gubbi, J., Buyya, R., Marusic, S., and Palaniswami, M. “Internet of Things (IoT): A vision, architectural elements, and future directions.” *Future Generation Computer Systems*. 2013. Vol. 29(7), pp. 1645–1660. DOI:10.1016/j.future.2013.01.010.

Guttieres, D., Stewart, S., Wolfrum, J., and Springs, S.L. “Cyberbiosecurity in Advanced Manufacturing Models.” *Front Bioeng Biotechnol*. 2019. DOI:10.3389/fbioe.2019.00210.

Guo, Z., Zhang, Y., Zhao, X., and Song, X. "CPS-Based Self-Adaptive Collaborative Control for Smart Production-Logistics Systems." *IEEE Transactions on Cybernetics*. 2021. Vol. 51(1), pp. 188-198. DOI:10.1109/TCYB.2020.2964301.

Hamel, G., and Välikangas, L. “The Quest for Resilience.” *Harvard business review*. 2003. Vol. 81(9), pp 52-63.

Hasan, M., and Starly, B. “Decentralized cloud manufacturing-as-a-service (CMaaS) platform architecture with configurable digital assets.” *Journal of Manufacturing Systems.* 2020. Vol. 56, pp. 157–174. DOI:10.1016/j.jmsy.2020.05.017.

Hendricks, K. and Singhal V. “The effect of supply chain glitches on shareholder wealth.” *Journal of Operations Management.* 2003. Vol. 21. pp. 501–522.

DOI:10.1016/j.jom.2003.02.003.

Hendricks, K. and Singhal, V. "An Empirical Analysis of the Effect of Supply Chain Disruptions on Long-run Stock Price Performance and Equity Risk of the Firm." *Production and Operation Management.* 2005. Vol. 14(1), pp. 35-52. DOI:10.1111/j.1937-5956.2005.tb00008.x.

Ho, N., Wong, P.-M., Soon, R.-J., Chng, C.-B., and Chui, C.-K. "Blockchain for Cyber-Physical System in Manufacturing." *Proceedings of the Tenth International Symposium on Information and Communication Technology*. 2019. Pp. 385–392. DOI:10.1145/3368926.3369656.

Holland, M., Nigischer, C., and Stjepandic, J. "Copyright Protection in Additive Manufacturing with Blockchain Approach." *Advances in Transdisciplinary Engineering*. 2017. DOI:10.3233/978-1-61499-779-5-914.

Holling, C. "Resilience and Stability of Ecological Systems*." Annual Review of Ecology and Systematics.* 1973. Vol. 4, pp. 1-23.

Hollnagel, E., Woods, D., and Leveson, N. "Resilience Engineering : Concepts and Precepts." 2006.

Hollnagel, E. "How Resilient Is Your Organisation? An Introduction to the Resilience Analysis Grid (RAG)." *Sustainable Transformation: Building a Resilient Organization*. 2010.

Home, J.F., and Orr, J. “Assessing behaviors that create resilient organizations.” *Employment Relations Today*. 1997. Vol. 24(4), pp. 29-39. DOI:10.1002/ert.3910240405.

Hutchins, M. J., Bhinge, R., Micali, M. K., Robinson, S. L., Sutherland, J. W., and Dornfeld, D. “Framework for Identifying Cybersecurity Risks in Manufacturing.” *Procedia Manufacturing*. 2015. Vol. 1, pp. 47–63. DOI:10.1016/j.promfg.2015.09.060.

Hu, Y., Li, J., and Holloway, L. "Resilient Control for Serial Manufacturing Networks With Advance Notice of Disruptions." *IEEE Transactions on Systems, Man, and Cybernetics: Systems*. 2013. Vol. 43:1, pp. 98-114. DOI:10.1109/TSMCA.2012.2189879.

IBM. “X-Force Threat Intelligence Index 2023.” 2023. URL:https://www.ibm.com/reports/threat-intelligence.

ISO 22400 Automation Systems and integration - Key performance indicators (KPIs) for manufacturing operations management 2014.

Ivanov, D. and Dolgui, A. “A digital supply chain twin for managing the disruption risks and resilience in the era of Industry 4.0.” *Production Planning & Control*. 2021. Vol. 32(9), pp. 775-788. DOI: 10.1080/09537287.2020.1768450.

Jamwal, A., Agrawal, R., Manupati, V., Sharma, M., Varela, L., and Machado, J. “Development of cyber-physical system based manufacturing system design for process optimization.” *IOP Conference Series: Materials Science and Engineering.* 2020. Vol. 997, pp. 012048. DOI:10.1088/1757-899X/997/1/012048.

Jürgenson, A., and Willemson, J. “Serial Model for Attack Tree Computations.” *In D. Lee & S. Hong (Eds.), Information, Security and Cryptology – ICISC 2009*. 2010. Pp. 118–128. DOI:10.1007/978-3-642-14423-3_9.

Kagermann, H., Wahlster, W., & Helbig, J. “Securing the future of German manufacturing industry: Recommendations for implementing the strategic initiative Industrie 4.0.” 2013. Pp.19–20. URL:https://www.din.de/blob/76902/e8cac883f42bf28536e7e8165993f1fd/recommendations-for-implementing-industry-4-0-data.pdf.

Kennedy, Z. C., Stephenson, D. E., Christ, J. F., Pope, T. R., Arey, B. W., Barrett, C. A., and Warner, M. G. “Enhanced anti-counterfeiting measures for additive manufacturing: Coupling lanthanide nanomaterial chemical signatures with blockchain technology.” *Journal of Materials Chemistry C*. 2017. Vol. 5(37), pp. 9570–9578. DOI:10.1039/C7TC03348F.

Khargonekar, P. and Kurose J. "NSF 15-06 Dear Colleague Letter: Cybermanufacturing Systems." National Science Foundation. 2015. URL: https://www.nsf.gov/pubs/2015/nsf15061/nsf15061.jsp.

Kim, B. H., Ahn, H.-J., Kim, J. O., Yoo, M., Cho, K., and Choi, D. "Application of M2M technology to manufacturing systems." *2010 International Conference on Information and Communication Technology Convergence (ICTC).* 2010. Pp. 519-520. DOI:10.1109/ICTC.2010.5674785.

Kristianto, Y., Gunasekaran, A. and Helo, P. "Building the "Triple R" in global manufacturing." *International Journal of Production Economics.* 2017. Vol. 189, pp. 607-619. DOI:10.1016/j.ijpe.2015.12.011.

Kusiak, A. "Open manufacturing: a design-for-resilience approach." *International Journal of Production Research*. 2020. Vol. 58, pp. 1-12. DOI:10.1080/00207543.2020.1770894.

Langmann, R., & Stiller, M. "The PLC as a Smart Service in Industry 4.0 Production Systems." *Applied Sciences*. 2019. Vol. 9(18), pp. 3815. DOI:10.3390/app9183815.

Langner, R. "Stuxnet: Dissecting a Cyberwarfare Weapon." *IEEE Security Privacy*. 2011. Vol. 9(3), pp. 49–51. DOI:10.1109/MSP.2011.67.

Leang, B., Ean, S., Kim, R.-W., Chi, S.-Y., and Yoo, K.-H. “Extracting Sensing Data from PLCs in Smart Manufacturing Machines.” *2019 International Conference on Internet of Things (IThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. 2019. Pp. 1249–1250. DOI:10.1109/iThings/GreenCom/CPSCom/SmartData.2019.00208.

Lee, J., Bagheri, B., and Jin, C. “Introduction to cyber manufacturing.” *Manufacturing Letters*. 2016. Vol. 8, pp. 11–15. DOI:10.1016/j.mfglet.2016.05.002.

Lee, J., Bagheri, B., and Kao, H.-A. “ A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems.” *Manufacturing Letters*. 2015. Vol. 3, pp.18–23. DOI:10.1016/j.mfglet.2014.12.001.

Lee, Y., Mari, S., Memon, M., Park, Y., and Kim, M. “Adaptivity of complex network topologies for designing resilient supply chain networks.” *The International Journal of Industrial Engineering: Theory, Applications and Practice*. 2015. Vol. 22, pp.102-116.

Lezoche, M. and Panetto, H. “Cyber-Physical Systems, a new formal paradigm to model redundancy and resiliency.” *Enterprise Information Systems*. 2020. Vol. 14(8), pp. 1150-1171. DOI:10.1080/17517575.2018.1536807.

Li, Z., Wang, W. M., Liu, G., Liu, L., He, J., and Huang, G. Q. “Toward open manufacturing: A cross-enterprises knowledge and services exchange framework based on blockchain and edge computing.” *Industrial Management & Data Systems*. 2018. Vol. 118(1), pp. 303–320. DOI:10.1108/IMDS-04-2017-0142.

Liu, C., and Jiang, P. “A Cyber-physical System Architecture in Shop Floor for Intelligent Manufacturing.” *Procedia CIRP*. 2016. Vol. 56, pp. 372–377. DOI:10.1016/j.procir.2016.10.059.

Luthans, F., Vogelgesang, G., and Lester, P. “Developing the Psychological Capital of Resiliency.” *Human Resource Development Review*. 2006. Vol. 5, pp. 2544. DOI:10.1177/153448430528.

Mahjabin, T., Xiao, Y., Sun, G., and Jiang, W. “ A survey of distributed denialof-service attack, prevention, and mitigation techniques.” *International Journal of Distributed Sensor Networks*. 2017. Vol. 13(12), pp. 1550147717741463. DOI:10.1177/1550147717741463.

Mauw, S., and Oostdijk, M. “Foundations of Attack Trees.” *In D. H. Won & S. Kim (Eds.), Information Security and Cryptology—ICISC 2005*. 2006. Pp. 186–198. DOI:10.1007/11734727_17.

Moghaddam, M., Cadavid, M. N., Kenley, C. R., and Deshmukh, A. V. “Reference architectures for smart manufacturing: A critical review.” *Journal of*

Manufacturing Systems. 2018. Vol. 49, pp. 215–225. DOI:10.1016/j.jmsy.2018.10.006.

Mohsen, M., and Abhijit, D. “Resilience of cyber-physical manufacturing control systems.” *Manufacturing Letters*. 2019. Vol. 20, pp. 40-44. DOI:10.1016/j.mfglet.2019.05.002.

Monostori, L., Kádár, B., Bauernhansl, T., Kondoh, S., Kumara, S., Reinhart, G., Sauer, O., Schuh, G., Sihn, W., and Ueda, K. “Cyber-physical systems in manufacturing.” *CIRP Annals.* 2016. Vol. 65(2), pp. 621–641. DOI:10.1016/j.cirp.2016.06.005.

Mouelhi, S., Laarouchi, M., Cancila, D., and Chaouchi, H. "Predictive Formal Analysis of Resilience in Cyber-Physical Systems." *IEEE Access*. 2019. Vol. 7, pp. 33741-33758. DOI:10.1109/ACCESS.2019.2903153.

Morphisec. “Morphisec’s Manufacturing Cybersecurity Threat Index.” 2021. URL: https://engage.morphisec.com/2021-manufacturing-cybersecuritythreatindex.

Napoleone, A., Macchi, M., and Pozzetti, A. “A review on the characteristics of cyber-physical systems for the future smart factories.” *Journal of Manufacturing Systems.* 2020. Vol. 54. pp. 305-335. DOI:10.1016/j.jmsy.2020.01.007.

National Institute of Standards and Technology. “NIST Special Publication 80039, Managing Information Security Risk: Organization, Mission, and Information System View.” 2011. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf.

Nguyen, W., Ashwin S., and Nof, S. “Advancing Cyber-Physical Systems Resilience: The Effects of Evolving Disruptions.” *Procedia Manufacturing*. 2019. Vol. 39, pp. 334-340. DOI:10.1016/j.promfg.2020.01.365.

Nguyen, W. and Nof, S. “Resilience Informatics for Cyber-augmented Manufacturing Networks (CMN): Centrality, Flow and Disruption.” *Studies in Informatics and Control*. 2018. Vol. 27. DOI:10.24846/v27i4y201801.

Nicholson, A., Webber, S., Dyer, S., Patel, T., and Janicke, H. “SCADA security in the light of Cyber-Warfare.” *Computers & Security*. 2012. Vol. 31(4), pp. 418– 436. DOI:10.1016/j.cose.2012.02.009.

Oueslati, N. E., Mrabet, H., Jemai, A., and Alhomoud, A. “Comparative Study of the Common Cyber-physical Attacks in Industry 4.0.” *2019 International Conference on Internet of Things, Embedded Systems and Communications (IINTEC)*. 2019. Pp. 1–7. DOI:10.1109/IINTEC48298.2019.9112097.

Park, K., Son, Y., and Noh, S. “The architectural framework of a cyber physical logistics system for digital-twin-based supply chain control.” *International Journal of Production Research.* 2020. DOI:10.1080/00207543.2020.1788738.

Park, K., Son, Y., Ko, S., and Noh, S. “Digital Twin and Reinforcement Learning-Based Resilient Production Control for Micro Smart Factory.” *Applied Sciences*. 2021. Vol. 11(7), pp. 2977. DOI:10.3390/app11072977.

Parri, J., Patara, F., Sampietro, S. et al. “A framework for Model-Driven Engineering of resilient software-controlled systems.” *Computing 103*. 2021. Pp. 589–612. DOI:10.1007/s00607-020-00841-6.

Pereira, T., Barreto, L., and Amaral, A. “Network and information security challenges within Industry 4.0 paradigm.” *Procedia Manufacturing*. 2017. Vol. 13, pp. 1253–1260. DOI:10.1016/j.promfg.2017.09.047.

Prasad, R., and Moon, B. “Architecture for Preventing and Detecting CyberAttacks in Cyber-Manufacturing Systems.” *The 10th IFAC Triennial Conference on Manufacturing Modeling, Management and Control (MIM 2022)*. Nantes, France, June 22–24, 2022.

Ribeiro, L., and Björkman, M. “Transitioning From Standard Automation Solutions to Cyber-Physical Production Systems: An Assessment of Critical Conceptual and Technical Challenges.” *IEEE Systems Journal*. 2018. Vol. 12(4), pp.

3816–3827. DOI:10.1109/JSYST.2017.2771139.

Ross, R. , Pillitteri, V. , Graubart, R. , Bodeau, D. and McQuaid, R. “Developing Cyber-Resilient Systems: A Systems Security Engineering Approach, Special Publication (NIST SP).” *National Institute of Standards and Technology.* 2021. DOI:10.6028/NIST.SP.800-160v2r1.

Saini, V., Duan, Q., and Paruchuri, V. “Threat Modeling Using Attack Trees.” *Journal of Computing Sciences in Colleges*. 2008. Vol. 23.

Sandaruwan, G. P. H., Ranaweera, P. S., and Oleshchuk, V. A. “PLC security and critical infrastructure protection.” *2013 IEEE 8th International Conference on Industrial and Information Systems*. 2013. pp. 81–85. DOI:10.1109/ICIInfS.2013.6731959.

Seok, H., Kim, K., and Nof, S. “Intelligent contingent multi-sourcing model for resilient supply networks.” *Expert Systems with Applications*. 2016. Vol. 51, pp. 107119. DOI:10.1016/j.eswa.2015.12.026.

Song, J., and Moon, Y. “Security Enhancement Against Insiders in CyberManufacturing Systems*.” Procedia Manufacturing*. 2020. Vol. 48, pp. 864-872. DOI:10.1016/j.promfg.2020.05.124.

Song, Z., Skuric, A. and Ji, K. "A Recursive Watermark Method for Hard RealTime Industrial Control System Cyber-Resilience Enhancement." *IEEE Transactions on Automation Science and Engineering*. 2020. Vol. 17(2), pp. 1030-

1043. DOI:10.1109/TASE.2019.2963257.

Shin, H., Cho, K., and Oh, C. “SVM-Based Dynamic Reconfiguration CPS for Manufacturing System in Industry 4.0.” *Wireless Communications and Mobile Computing*. 2018. Pp. 1-13. DOI:10.1155/2018/5795037.

Spiegler, V., Naim, M., and Wikner, J. “A control engineering approach to the assessment of supply chain resilience.” *International Journal of Production Research.* 2012. Vol. 50(21), pp. 6162-6187. DOI: 10.1080/00207543.2012.710764.

Sturm, L. D., Williams, C. B., Camelio, J. A., White, J., and Parker, R. “Cyberphysical vulnerabilities in additive manufacturing systems: A case study attack on the .STL file with human subjects.” *Journal of Manufacturing Systems*. 2017. Vol. 44, pp. 154–164. DOI:10.1016/j.jmsy.2017.05.007.

Tao, F., Zhang, L., Venkatesh, V. C., Luo, Y., and Cheng, Y. “Cloud manufacturing: A computing and service-oriented manufacturing model.” *Proceedings of the Institution of Mechanical Engineers, Part B: Journal of Engineering Manufacture*. 2011. Vol. 225(10), pp. 1969–1976. DOI:10.1177/0954405411405575.

Theron, P. “Through-life cyber resilience in future smart manufacturing environments. A research programme.” *Procedia Manufacturing*. 2018. Vol. 16, pp. 193-207. DOI:10.1016/j.promfg.2018.10.157.

Theoharidou, M., Kokolakis, S., Karyda, M., and Kiountouzis, E. “The insider threat to information systems and the effectiveness of ISO17799*.” Computers & Security*. 2005. Vol. 24(6), pp. 472–484. DOI:10.1016/j.cose.2005.05.002.

Tilman, D., and Downing, J. “Biodiversity and stability in grasslands.” *Nature*. 1994. Vol. 367, pp. 363–365. DOI:10.1038/367363a0.

Tukamuhabwa, B., Stevenson, M., Busby, J., and Zorzini, M. “Supply chain resilience: definition, review and theoretical foundations for further study.” *International Journal of Production Research.* 2015. Vol. 53(18), pp. 5592-5623. DOI:10.1080/00207543.2015.1037934.

The Guardian. “Triton: hackers take out safety systems in 'watershed' attack on energy plant”. 2017. URL: https://www.theguardian.com/technology/2017/dec/15/triton-hackers-malware-attack-safety-systems-energy-plant.

Torkura, K., Sukmana, M., Ihsan H., Meinig, M., Kayem, A., Graupner, H., Cheng, F., and Meinel, C. “Securing Cloud Storage Brokerage Systems Through Threat Models.” *32nd IEEE International Conference on Advanced Information Networking and Applications (AINA 2018).* 2018. DOI:10.1109/AINA.2018.00114.

United Kingdom Financial Conduct Authority. “Operational Resilience.” 2017. URL: https://www.fca.org.uk/firms/operational-resilience.

Vargas, C. and Vogel-Heuser, B. “Towards Industrial Intrusion Prevention Systems: A Concept and Implementation for Reactive Protection.” *Applied Sciences*. 2018. Vol. 8, pp. 2460. DOI:10.3390/app8122460.

Wang, S., Wan, J., Li, D., and Zhang, C. “Implementing Smart Factory of Industrie 4.0: An Outlook.” *International Journal of Distributed Sensor Networks.* 2016. Vol. 12(1), pp. 3159805. DOI:10.1155/2016/3159805.

Wang, Y. “Resilience Quantification for Probabilistic Design of Cyber-Physical System Networks.” *ASCE-ASME J. Risk and Uncert. in Engrg. Sys., Part B: Mech. Eng*. 2018. DOI:10.1115/1.4039148.

Wu, M. and Moon, Y. “Taxonomy for Secure CyberManufacturing Systems.” *Proceedings of the ASME 2018 International Mechanical Engineering Congress and Exposition. Volume 2: Advanced Manufacturing*. V002T02A067. Pittsburgh, PA, November 9–15, 2018. DOI:10.1115/IMECE2018-86091.

Wu, M., and Moon, Y. “Alert Correlation for Cyber-Manufacturing Intrusion Detection.” *Procedia Manufacturing*. 2019. Vol. 34, pp. 820-831. DOI:10.1016/j.promfg.2019.06.197.

Xu, L. D. “Enterprise Systems: State-of-the-Art and Future Trends.” *IEEE Transactions on Industrial Informatics*. 2011. Vol. 7(4), pp. 630–640. DOI:10.1109/TII.2011.2167156.

Xu, L. D., He, W., and Li, S. “Internet of Things in Industries: A Survey.” *IEEE Transactions on Industrial Informatics*. 2014. Vol. 10(4), pp. 2233–2243. DOI:10.1109/TII.2014.2300753.

Xu, L. D., Xu, E. L., and Li, L. “Industry 4.0: State of the art and future trends.” *International Journal of Production Research*. 2018. Vol. 56(8), pp. 2941–2962. DOI:10.1080/00207543.2018.1444806.

Youn, B. D., Hu, C., and Wang, P. "Resilience-Driven System Design of Complex Engineered Systems." *ASME. J. Mech. Des*. 2011. Vol. 133(10), pp. 101011. DOI:10.1115/1.4004981.

Zhong, R. Y., Xu, X., Klotz, E., & Newman, S. T. “Intelligent Manufacturing in the Context of Industry 4.0: A Review.” *Engineering*. 2017. Vol. 3(5), pp. 616–630. DOI:10.1016/J.ENG.2017.05.015.

Carlos Omar Espinoza Zelaya

coespino@syr.edu Syracuse, NY 13210 Tel: (607) 379-1015

EDUCATION

Syracuse University, College of Engineering and Computer Science, Syracuse, NY
Ph.D. in Mechanical and Aerospace Engineering, **GPA 3.7** **Expected May 2023**

Cornell University, College of Engineering, Ithaca, NY
Master of Engineering in Systems Engineering, **GPA 3.5** **May 2020**

Catholic University of Honduras, School of Engineering, Tegucigalpa, Honduras
Bachelor of Science in Industrial Engineering, **Magna Cum Laude, GPA: 93%** **Apr 2015**

ENGINEERING EXPERIENCE

Research Excellence Fellow, *Syracuse University*, Syracuse, New York
June 2021 - Present

- Conduct independent research on the Resilience of Cyber-Manufacturing Systems (CMS) under cyber-attacks.
- Develop optimization models for decision-making under stress and uncertainty.
- Design simulation experiments and resilience algorithms to withstand attack scenarios.

Senior Quantitative Advisory Intern, *Ernst & Young*, New York, New York
June 2022 – August 2022

- Design and development of a platform to manage financial risk models' lifecycle.
- Financial Services Risk Management Consultant engaging in Fundamental Review of the Trading Book (FRTB).
- Developing, Testing, Validating and Documenting Financial Risk Models.

Teaching Assistant, *Syracuse University*, Syracuse, New York **Aug 2020 – May 2023**

- ECS 526 Statistics for Engineering.
- MAE 548 - Engineering Economics and Technology Valuation.
- MEE 435 Manufacturing Processes
- ECS 104 Computational Tools for Engineering
- Lead class discussions, hold office hours and explain core concepts to graduate students.

Senior Process Analyst, *Presidential Unit of Social Protection,* Tegucigalpa, Honduras
Oct 2017 – Jul 2019

Responsible for the digital transformation and design of implementation strategy of public social policies.

- Crafted an investment plan of 58 million dollars in primary health care infrastructure, leading the analysis of Operational Expenses.
- Designed a housing digital platform for 800k workers to register, get qualified, and access financing options.
- Served as a liaison in the structuring of a $150 million Infrastructure Investment Fund of Honduras with the United Nations Office for Services and Projects (UNOPS), the secretary of state, and multiple financial institutions.

Product Owner, *Agile Solutions*, Tegucigalpa, Honduras / Rio de Janeiro, Brazil
Jun 2015 – Sep 2017

Responsible for the overall management of apps for agriculture, healthcare, and tax management.

- Led the design, development, and implementation of 12 custom Quality Assurance apps for agriculture to integrate with SAP Enterprise Resource Planning software overcoming a 3-month delay in the project schedule.
- Develop functional specifications for All Tax TIMP (Tax Intelligence Management Platform) based on customer requirements.
- Conceptualize a patient experience app from more than 200 hours of healthcare shadowing with physicians to help deliver better primary care.

Industrial Risk Intern, *National Electrical Energy Company*, Tegucigalpa, Honduras
Sep 2014 – Dec 2015

Responsible for proactively identifying risks and devising mitigation plans.

- Implemented a Dengue mitigation strategy for all the power stations in the south-central region of the country.
- Implemented a standardized documentation protocol to investigate the occurrence of workplace accidents.
- Performed the on-site inspections of 5 power stations and evaluated their work conditions.

PUBLICATIONS

1st Author of "Resilient Cyber-Manufacturing Systems under cyber-attacks" ASME 2021 International Mechanical Engineering Congress and Exposition IMECE2021.

4th Author of "Recovery-by-Learning: Restoring Autonomous Cyber-Physical Systems from Sensor Attacks" RTCSA 2021, the 27th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications.

1st Author of "Resilience Enhancing Mechanisms for Cyber-Manufacturing Systems against CyberAttacks." IFAC-PapersOnLine.

1st Author of "Taxonomy of the severity of cyber-attacks in cyber-manufacturing systems" ASME 2022 International Mechanical Engineering Congress and Exposition. Volume 2B: Advanced Manufacturing. Columbus, Ohio. October 30-November.

1st Author of "Assessing the severity of cyber-attacks against cyber-manufacturing systems" ASME 2022 International Mechanical Engineering Congress and Exposition. Volume 2B: Advanced Manufacturing. Columbus, Ohio. October 30-November.

1st Author of "Framework for enhancing the operational resilience of cyber-manufacturing systems (CMS) against cyber-attacks" North American Manufacturing Research Conference (NAMRC) 51. 2023.

SKILLS

Soft Skills: Leadership, empathy, listening, public speaking, openness to feedback, teamwork, decisionmaking, stress management, creativity, resourcefulness, analytical thinking, and negotiation.

Hard Skills: System simulation and optimization, financial modeling, statistical analysis, Machine Learning, forecasting and demand planning, supply chain optimization, process analysis, and continuous improvement. QFD (Quality Function Deployment), Lean Manufacturing, Six Sigma, service design, wireframes, requirement gathering, Design Thinking, use cases, proposal drafting, vulnerabilities analysis, systems architecture, and failure mode analysis.

Tools: Python, R, C+, JavaScript, HTML, CSS, Vensim, Arena, Office, Jira, Trello, SysML, BPMN 2.0, Lucidchart.

Languages: Spanish (native); English (fluent); Portuguese (fluent)

Selected Coursework: Model-Based Systems Engineering • Systems Dynamics • Design of Manufacturing Systems • Principles of Supply Chain Management •Financial Accounting •Project Management • Cornell University Sustainable Design Project • Systems Analysis and Optimization • Artificial Intelligence for Manufacturing Systems • Intelligent and Secure Cyber-Physical Systems • Machine Learning and AI for Engineers.

AWARDS / POSITIONS

Syracuse University Fellow of Research Excellence 2021-2022, Recipient of the Honduras Presidential Scholarship 2019, Cornell University Master of Engineering Committeemerit–based fellowship, Cornell

University Master of Engineering Students Advisory Board Member, Syracuse University Graduate Student Organization – Mechanical and Aerospace Engineering Representative.

ACTIVITIES/INTERESTS

GSBA – Graduate School BIPOC Alliance steering committee member, SHPE – Society of Hispanic Engineers, BLISTS – Black and Latinx Information Science and Technology Society, INCOSE – Cornell Chapter; Cornell Sports Taekwondo Team; Brazilian Jiu Jitsu; Olympic weightlifting; rock climbing, salsa dancing; classical guitar; chamber music; art history; poetry; ballet; craft beers; soccer; hockey; baseball