**Group 4 Cyber Resiliency Project**

**Cyber Resiliency in Automotive Parts Manufacturing**

Alden Jettpace, Khalfan Alneyadi, and Oluwafewa Ayodeji

School of Informatics and Computing, Indiana University – Purdue University Indianapolis

IN-CIT-52800

Dr. Connie Justice

October 8, 2023

**Table of Contents**

[**Executive Summary 3**](#_qv1ej67oxcmb)

[**Introduction 3**](#_nnv7ef3izi0h)

[**Problem Statement 4**](#_oofl6u802c7c)

[**Background 5**](#_bf0qmw8by7ja)

[Auto Parts Manufacturing 5](#_h35vdjo37y1i)

[Critical Business Functions 5](#_c9mum0y20i0c)

[Cyber Resiliency 6](#_nezdni2jioye)

[CIA Triangle 7](#_opeclvw1eck5)

[Manufacturing Cyber Security Regulations 8](#_bbnwkcqyzbf6)

[Auto Parts Manufacturing Critical Assets 9](#_vvmis2ta3j1m)

[Auto Parts Manufacturing Cyber Risks 11](#_8xz3sigtt2x)

[**Robustness 12**](#_u0z4teugv679)

[People 12](#_pu1nwvcppyas)

[Processes 14](#_4z3s4h65w187)

[Technology 15](#_dt8gr255qr9i)

[**Redundancy 18**](#_mck1a1gf2l5)

[People 18](#_8j3ovd8ndx0y)

[Processes 20](#_5apb32e6jysn)

[Technology 23](#_lo8p4ubwzqqo)

[**Resourcefulness 25**](#_ysgmw7kowyp9)

[People 26](#_1htc0yfgad8p)

[Processes 28](#_q8gi9kck58s5)

[Technology 30](#_m7zzsyqnql5g)

[**Rapidity 32**](#_ttyxqy3d7j8y)

[People 33](#_86imxt8mjjsr)

[Processes 34](#_r9u7dgkx8rcx)

[Technology 36](#_eprdlby864no)

[**Results/Conclusions 38**](#_lgcjnbqhlf41)

[Outcome 1: People 39](#_cdjvmcy82rf6)

[Outcome 2: Processes 40](#_b182jlrdj82k)

[Outcome 3: Technology 41](#_2rrsbl196xk9)

[**Future Works 41**](#_99no3jlb5fkc)

[**References 42**](#_3m651uj966p)

# Executive Summary

Auto Parts Manufacturing companies require not just the safe and continuous production of quality automotive parts and the protection of associated cyber assets, but must also protect their supply chains and the information of their customers and clients. To achieve both these obligations, manufacturers must maintain security controls to ensure their systems remain resilient to cyber attacks, as well as to non-cyber disruptions. To ensure system robustness, the manufacturer must be able to successfully prevent or absorb attacks or disruptions. Robustness can be induced through employee cross-training, upholding and refining a standardized attack-response policy and disaster-response policy, and implementing technological controls that can prevent disruption of the software, databases, and automated production processes. Redundancy can be induced via maintaining on-call employees for shortages, physical records copies, backup manufacturing equipment and generators, and data backups and redundant servers. Resourcefulness can be induced via tracking employee observations and complaints, and maintain firewalls and intrusion detection systems for cyber assets. Rapidity can be induced via processes of ‘chain-of-command’ during attacks or accidents, as well as through practiced recovery plans.

# Introduction

The purpose of this paper is to serve as a framework for Security Assessment for Auto Parts Manufacturers, specifically in regards to their cyber assets. The recommendations within will be how controls for employees, policies, and technology can be implemented to ensure the manufacturer’s system and assets are resilient, as are their clients. The scope of this project is based on publicly available data on parts manufacturers, with no particular manufacturer in mind, but will name specific companies as examples of the obligations and risk of auto parts manufacturers. The content of this paper as a general advisory tool for any auto parts manufacturer, as well as to the clients they serve.

The general layout of the paper begins by describing the idea of cyber resiliency and the framework to induce it in our paper: the 4Rs. After describing the goals, regulations, and threats presented to automotive manufacturers and their cyber assets, we then describe how they can induce the 4R’s resilience aspects via controls involving people, procedures, and technology. In each, the aspect itself and its relation to car parts manufacturing is described. Each possible avenue of control implementation is discussed in subsections and include examples of the resiliency aspect as it relates to this avenue of implementation, what controls can be induced via this avenue, and the effects of lacking the resiliency aspect in this avenue. After discussing all four aspects of the 4Rs resiliency framework, we will conclude with a generalized summation of our findings and with a Future Works section to consider possible expansions on our findings to related fields.

# Problem Statement

Automotive Parts Manufacturing requires maintaining a minimum level of production standards, employee safety, production throughput, and obligations to clients including protecting their critical information. The problem of maintaining all these obligations during a cyber attack or other disruptive event requires implementing cyber resiliency via the attributes of robustness, redundancy, resourcefulness, and rapidity to recover disruptive incidents such as cyber attacks while still maintaining these said obligations.

# Background

## Auto Parts Manufacturing

It is hard to argue when the car was first invented, as the idea of a ‘driverless buggy’ was developed over many stages, from the first steam propelled road vehicle in 1769, to the more complicated but ‘official’ gasoline powered car, the 1886 Benz Patent Motor car, otherwise known as the Mercedes Benz [1]. As its development progressed, the car grew more and more complicated and so did the list of required parts to manufacture. Today, between the electrical system, engine system, and now with onboard computer systems, cars can have on average 30,000 individual parts, with just the engine requiring thousands of parts [2]. Like many processes, the production of a car is now a globalized process, requiring thousands of different manufacturers of different parts, each one supplying to several car manufacturers, repair shops, and parts stores. The producers of finished car parts from individual car parts are known as Tier 1 Suppliers, with the Ford Car Company relying on 1,400 Tier 1 suppliers to support their manufacturing [3][4].

Tier 1 car parts manufacturing can be divided into two main categories: Original Equipment Manufacturers (OEM), and Aftermarket Manufacturers. OEMs are parts manufacturing done by the manufacturers of the car itself, such as the Ford company producing parts through Ford Motorcraft [5]. Meanwhile, Aftermarket Manufacturing is parts for cars which are not manufactured by the car company itself [6]. This might include replacement parts for car repairs, or as third-party parts suppliers for car manufacturers.

## Critical Business Functions

Car parts manufacturing, like most other critical manufacturing processes, must be able to maintain a baseline minimum standard for safety, product quality, and maintain their contract obligations to clients, as well with their suppliers from Tier 2 and Tier 3 parts manufacturers. Thus, the business must not only protect the integrity of the production process and the safety of its workers, but also must be responsible for its obligations in the parts supply chain, ensuring not just smooth parts but also retaliation business relationships with other parts of the supply chain. Manufacturers represent an important part of the automotive production process and supply chain, as a slowdown between tiers of manufacturing, or between tier 1 manufacturers and their clients can end up halting the entire production process [7].

## Cyber Resiliency

The concept of cyber resilience as it relates to this paper is built off of the NIST frame which regards cyber resiliency as a specialized discipline of cyber security, focused not just on defending and recovering of cyber assets and system functionality in the event of a successful attack or disruption [8, pp. 75]. According to [9], resiliency is the aspect of being strong, hardy, and able to recover from damage. With the implication of survival of the resilient system in question, it means that for a manufacturer to have cyber resilience, it must be able to not only block potential attacks or disruptions the manufacturing process, but also must be able to maintain some minimum level of functionality after an attack, and be able to quickly recover lost or damaged assets and return to baseline levels of functionality.

There are several frameworks with which to design and measure the effectiveness of a cyber resilient system. This paper will utilize the high-level framework of the 4R’s, which defines resilience as a combination of four attributes which a system should possess: robustness, redundancy, resourcefulness, and availability [9]. Having these attributes within every aspect of the manufacturing process and IT system ensures that attack successes are rare, their losses low, and recovery times for manufacturing and supply-chains to be quick.

## CIA Triangle

Maintaining cyber resilience requires maintaining cyber security, which is formalized as the maintenance of the CIA Triangle of security objectives: Confidentiality, Integrity, and Availability.

Maintaining Confidentiality means ensuring that information pertaining to business functions or the cyber assets which support them is only available to authorized users [10, pp. 12]. This means that automotive parts manufacturers must ensure privacy of important production and distribution information. This information can pertain not just to employees but also to important intellectual property and patents, as well as to suppliers and customers. These last two are especially important as a manufacturer serves as an entry point to both of these entities by being trusted with their financial information for business purposes. To maintain confidentiality, employees should be trained for cybersecurity awareness, classify labels as restricted and enforce access controls, encrypt data, and use multi-factor authentication systems [11].

Maintaining Integrity means ensuring that information or data on IT systems of the manufacturer are not tampered with or destroyed [10, pp.12]. The destruction of a new parts design can cost a manufacturer months if not years of work and resources, so even without taking the supply chain into account, maintaining data integrity is important. Besides personal data, client and supplier data should also be protected. To maintain integrity, the same controls for maintaining confidentiality can also be implemented: data encryption, enforcing access controls, and certification authorizers for websites [11].

Maintaining Availability means ensuring data and the business functions that they support are available when needed [10, pp.12]. For car manufacturers, this is ensuring that the critical data and information systems which support the manufacturing process, including measuring systems and sensors for automatic machinery, are working properly. This also means ensuring that the business is able to contact suppliers and deliver finished parts to customers. This requires not just protecting against attacks on the information system, but also of potential disasters which could damage equipment or cause power outages such as storms. To maintain availability, ensuring cyber resources such as software is up to date, as well as maintaining redundant resources which can be called upon in an emergency to ensure continued production and sales [11].

## Manufacturing Cyber Security Regulations

The nature of car parts manufacturing means it must not only follow the cyber security regulations set for all manufacturing facilities, but also one's specific to the manufacturing of cars. Besides these regulations, they must also as a business which can be presumed to be supplying medical insurance to their employees, and being trusted with client and supplier financial information must also abide by the cyber security regulations detailed within the Health Insurance Portability and Accountability Act of 1996 (HIPAA) as well as by the Payment Card Industry Data Security Standard (PCI DSS), taking steps to protect employee personal medical information, and client financial information through minimum standards for applied cyber security controls such as data encryption or access controls [10, pp. 59-72].

The ISA/IEC 62443 is a series of standards which are applied to a broad range of industry sectors, including building automation, medical devices, transportation, and evil chemical and oil production. Governed by the International Society of Automation (ISA) and the International Electrotechnical Commission (IEC), and applies a standard of safety, security, and reliability of control systems [12]. More specific car and OEM manufacturing regulations are governed by the World Forum for Harmonization of Vehicle Regulations (WP.29), a subset of the United Nations Economic Commission for Europe (UNECE), which governs vehicle regulations of note across UN countries. A recent regulation, Regulation No. 155 (UN R155), applies security standards across the entire life cycle of vehicles, including the production and supply chain of OEMs and Aftermarket Parts [13]. Lastly there is the ISO/SAE 21434: ISO/SAE 21434 is an international standard that specifically addresses the cybersecurity of road vehicles. It outlines a structured approach to managing and mitigating cybersecurity risks throughout the vehicle's lifecycle, from concept and design to production and operation.

## Auto Parts Manufacturing Critical Assets

The automotive parts manufacturing industry must be responsible for providing a quality product, safe working conditions, and reliability in the supply chain to its customers. The assets required to support this include, can be divided into 3 broad categories: Information Assets, Physical Assets, and Relational Assets. Due to the interconnected nature of such businesses, with assets supporting one another, there is often overlap between them, so it is important to secure all of these assets in tandem.

Information assets represent the many types of data and software resources that support the business, and include but are not limited to, customer and employee data, intellectual property data and designs, and software and embedded systems which store and organize the information assets and support the physical assets. The protection of information assets not only ensures the availability of the system, but also ensures confidentiality and integrity, as employee and customer data heavily supports the relational assets of the business. Not only would an attack on customer data allow the attacker to then target that business, but also would cause damage to the reputation of the parts manufacturer.

Physical assets are the physical components which allow manufacturers to perform their critical business functions and would include not only the manufacturing equipment itself, such as robots and Computer Numerical Control (CNC) machines, but also support infrastructure such surveillance systems and power supply, as well as hardware systems such as server rooms, routers, and workstation computers. Some of these assets, such as the power supply or surveillance are intended to support the critical business functions without necessarily directly being one, as detecting potential threats through a surveillance system ensures a safe business environment. Meanwhile, ensuring the protection of manufacturing equipment is directly related to ensuring a functional minimum of production performance in event of attack. For example, CNC machines, which are vital for precision machining, should be secured with robust access controls to prevent unauthorized use or tampering.

Relational assets are ephemeral assets which represent the good or bad relationships the parts manufacturer has with other entities such as suppliers, customers, and other participants in the supply chain. A smooth supply chain is essential for sourcing raw materials and distributing manufactured automotive components. Securing both the supply and distribution chains is vital to meet customer demands and ensure timely component delivery. Protecting the supply chain, alongside all other assets, will in turn ensure employee well-being, customer relations, and overall security, which ensures a good brand reputation and thus long term success for the manufacturers. Ensuring supply chain security can include measures like vendor assessments and monitoring to prevent disruptions in the manufacturing process. Meanwhile, besides securing all other assets, reputation can be secure by implementing employee wellness programs and adhering to ethical business practices.

## Auto Parts Manufacturing Cyber Risks

For each associated asset for car parts manufacturing, there are also a bevy of associated risks of probable attacks on the business itself, and the unique vulnerabilities of the assets or their connections between each other. Ensuring the cyber security of a parts manufacturer is especially important as due to them being an in-between point on a larger supply chain, they can act as an entrypoint for attacks on other connected entities such as customers or suppliers. Even if related entities information is secured, a disruption of the parts manufacturers business functions can still affect these entities by the supply chain, a problem which is exacerbated thanks to the system of Just-In-Time production.

Just-In-Time production is a process of only producing for individual orders to ensure as little unused inventory as possible. This relies on maintaining a constantly shifting series of orders, customers, and suppliers with the information flow between these entities being maintained in real time. Because there is no inventory, unplanned downtime in any one entity on the supply chain ensures there are no quick replacements, and thus translates into downtime for all entities further down the chain [14]. A common attack on car manufacturers has been ransomware attacks, with even attacks on suppliers causing disruptions for parts and car manufacturers. In February of 2022, Toyota was forced to temporarily suspend production at 14 facilities after a successful ransomware attack on one of its suppliers, Kojima Industries. While only supplying small components, a lack of a stockpile meant Toyota was forced to establish a backup network between itself and Kojima [15].

Another growing problem has been the issue of the cyber resiliency of the car parts themselves. As the vehicles themselves become more connected and autonomous, they are susceptible to hacking, potentially leading to accidents or unauthorized control of the vehicle. Already, studies have demonstrated that with just a vehicle identification number, one could access parking cameras, lock and unlock the stores, and even completely stop the engine. Spireon, a telematics company, had enough holes that researchers were able to send arbitrary commands to 15.5 million vehicles, including an entire police fleet [16]. Thus, manufacturers must now consider the cyber resiliency of the very items which they produce.

# Robustness

According to [9], Robustness can be defined as being “strong, vigorous, healthy” with a robust system being one which does not degrade much at all in functionality for most threats, but can fail easily for a select few. As defined for 4R’s, robustness is the ability to withstand disaster forces without large losses in performance. Taking into account its use as a subset of security, the Robustness of a car parts manufacturer would be its ability to prevent the success of attacks, as well as the damage which successful attacks can do to critical business functions. However, not all threats are intentional attacks, and so accidents must be considered. The main threats which are present for a car parts manufacturer are weather effects or outages, workplace injuries and accidents, and deliberate cyber attacks.

## People

The idea of "people control" is widely explored in relation to how corporations manage and impact their workforce in the disciplines of organizational psychology and management studies. Researchers have studied an array of strategies used by businesses to exert control over their workers, including but not limited to performance reviews, incentive schemes, and management practices. Through giving the employees the proper information and incentives, car parts manufacturers can ensure that employees are able to not only adjust well to the stress of attack conditions, but also have the proper view of the security process and risks of the enterprise.

In order to better understand the potential security risks to car production, training is necessary. Appropriate training and awareness initiatives are essential for providing staff members with the information and abilities required to identify and address any cyber threats. Effective training initiatives can dramatically lower the possibility of successful cyberattacks. According to recent research, it's critical to update these programs often in order to stay ahead of changing cyber threats and to improve employee preparedness by offering practical, scenario-based training [17]. Besides scenario training such as what to do when a specific piece of equipment malfunctions, such training could include the signs of ransomware on the system, which have become a serious problem for supply chains. Being made aware of the trends in cyber threats which might affect them and their equipment, employees both on the line and in the IT department should be made aware of company policies, including password policies and outside-work USB policy [18].

Besides ensuring employees are trained for disaster scenarios and possible cyber attack risks, employees should also be incentivized to take this training seriously, in order to give a buy-in into the company and consider its security as a personal responsibility. Responding to working condition complaints, be they security-based or even about something as simple as a broken cafeteria microwave, ensures the workers have as little stress as possible and keeps up employee morale, making them more attentive and productive. Besides training, extra incentives could be offered, such as rewards for taking training courses, or for encouraging IT-based employees to host hackathons to showcase their understanding of the production facilities IT-system.

## Processes

As it is critical that both employees and business assets not be damaged, a way to prevent this from happening is the establishment of procedures for proper use of both physical and information assets. Improper handling of manufacturing equipment such as forklifts, industrial presses, or machining equipment can not only damage the equipment but also put employees at risk for serious injury. Meanwhile, improper handling of information assets such as customer information or intellectual property files can lead to a potential security failure for the company.

Procedures for ensuring proper handling of hardware could be safety training to ensure employees understand the proper and improper usage of equipment. Equipment certification policies such as for forklifts or machining equipment ensure less likelihood of accidental damage to critical manufacturing equipment, as well to employee injuries. Meanwhile, proper management and usage policies for information technology can include implementing access controls as well as USB policies to prevent the spreading of viruses to critical assets such as client personal information data [19][20].

The growing danger of direct car hacking thanks to their growing system and sensor integration requires that car manufacturers and parts manufacturers must consider not just the cyber resiliency of their own businesses but also for the products they manufacture. As cars contain more and more electronic components, manufacturers must implement a process of resilience testing for these products, as well as establish guidelines for that product's potential interactions with other components or software to ensure as few vulnerable endpoints as possible. According to [21], a script based security testing process based on the guidelines of the ISO/SAE 21434 regulation framework can act as a model for component CR testing and documentation, which can be utilized on production batches to ensure each meets the security standards for that product. With this, vulnerable car components could lead to security incidents upon the car itself, pressuring the manufacturers to initiate a recall to fix the issue, and this could damage the reputation of the manufacturer.

Besides securing their own assets, the nature of the car manufacturing as it is now requires efficient interactions between multiple suppliers, parts manufacturers and car manufacturers, as well as third party professionals and clients such as auto parts stores. Because of the nature of the supply chain, any disruption to any one of these entities can reverberate throughout the entire supply chain. By having a policy of establishing minimum security requirements not just for vendors of the IT system but also for suppliers and other business partners, they ensure that they also do not end up being affected by the possible security breaches of another link in the supply chain [22]. Going back to the electronics issue, a clause like this could be that a car manufacturer agrees that the parts manufacturer for a certain electronic part must have a set policy stand for the cyber resiliency of the component. Having these security-clause based contracts ensures that all participants on the supply chain are maintaining some understandable, minimal level of system security ensuring a further level of protection for each participant, as they no longer have to worry about shutting down production thanks to attacks on a supply, as was the case with Toyota [15].

## Technology

In addition to the People and Procedures that help provide robustness in the Automotive Manufacturing Industry, there are technologies that are paramount to the resiliency of an automotive manufacturing company.

Network segmentationis an architectural approach that divides a network into multiple segments or subnets, each acting as its own small network [23]. This allows network administrators to control the flow of network traffic between subnets based on granular policies. Creating boundaries between the operational technology (OT) and information technology (IT) networks reduces many risks associated with the IT network, such as threats caused by phishing attacks [24]. One example of where network segmentation will provide robustness is protection of production line equipment. Manufacturing plants have multiple production lines, each with its own control systems and sensors. Network segmentation helps isolate these systems from one another, preventing the spread of malware or issues in one line affecting others. Another example is Automotive supply chains involving numerous suppliers, many of whom require access to specific systems or data. Network segmentation allows manufacturers to grant controlled, limited access to suppliers, reducing the risk of supply chain-related cybersecurity incidents. An example of a software that helps provide Network segmentation is Cisco Identity Services Engine

Data Encryption is a way of translating data from plaintext (unencrypted) to ciphertext (encrypted). Users can access encrypted data with an encryption key and decrypted data with a decryption key [25]. Data Encryption is a fundamental cybersecurity measure that provides confidentiality and security for data at rest and data in transit. In the automotive manufacturing industry, where sensitive data and intellectual property (IP) are critical assets, encryption is essential for safeguarding valuable information. Automotive manufacturers invest heavily in research and development to create innovative vehicle designs, manufacturing processes, and technologies. Data encryption ensures that CAD files, design specifications, and other proprietary information are kept confidential and cannot be easily accessed or stolen by unauthorized parties. IoT devices and sensors are integral to modern automotive manufacturing, providing real-time data on equipment performance and quality control. Data encryption protects this data from interception and manipulation. For Example, A cyberattacker attempts to alter the data generated by quality control sensors on the production line. Data encryption ensures the integrity of this data, allowing prompt detection of tampering. An example of a software that helps provide Data Encryption is Microsoft Bit lock Defender

Network Access Control can be defined as the set of rules, protocols, and processes that govern access to network-connected resources such as network routers, conventional PCs, IoT devices, and more [26]. It is a crucial cybersecurity technology for enhancing cyber resiliency in the automotive manufacturing industry. NAC helps organizations manage and control access to their network, ensuring that only authorized and compliant devices can connect. NAC allows automotive manufacturers to enforce strict access controls for the critical systems and equipment used in production. Only authorized devices and personnel can access and interact with these systems, reducing the risk of unauthorized tampering or disruptions. Imagine An unauthorized device, such as an employee's personal laptop, attempts to connect to the production line network. NAC detects the unauthorized device and prevents it from accessing the network, ensuring the integrity of production processes. A common example is if a supplier’s employee brings a device to the manufacturing facility for collaboration. NAC assesses the device's security posture and ensures it complies with security policies before granting access. An example of a software that helps provide network access control (NAC) is Aruba ClearPass.

There are different technologies that provide robustness nevertheless, the examples and implementations above being simple, more broadly applicable ones that can easily be modified for the system specifications of the manufacturer. Implementing these measures is essential for safeguarding the industry's operations, reputation, and competitiveness in an increasingly digital and connected landscape.

# Redundancy

According to [9], Redundancy is the “extent to which systems, system elements, or other units are substitutable”, be it either in other systems being able to perform the tasks of others, or by having duplicates of these system elements. Redundancy in car manufacturing can take the form of redundant security procedures such as checking equipment multiple times during inspection, or the form of duplicate resources such as extra equipment. This ensures that in the event of an attack attempt, there is no single-point of failure in the manufacturing process or supply-chain, making sure that either no single system component can shut down the entire process, or at least ensure that such downtime is as short as possible [10, pp 116]. Redundancy can prove to be a very effective way of inducing redundancy, as the current business organization model in supply chains of Just-in-Time manufacturing encourages businesses to create as little supply and overhead as possible, to maximize profits. However, this practice makes even small shocks to supply or demand thanks to an attack have an inflated effect, thanks to the lack of flexibility in such a system [14]. Introducing alternatives to downed equipment, missing personnel, and the company approach to overhead can ensure the entire car manufacturing process operates efficiently even in the event of successful cyber-attacks.

## People

Redundancy, an important factor in establishing system resilience, extends beyond technology concerns to include the human aspect within an organization. Redundancy in people, like redundancy in technology and processes, is strategic planning to limit risks associated with the absence or departure of critical workers. One part of human redundancy is promoting a diversified skill set and knowledge base among employees. Cross-training personnel ensures that various team members can undertake critical duties competently, avoiding a single point of failure. Documentation of essential processes is a significant resource that allows others to step in and manage the procedures. Redundancy can be implemented not just on the individual level but also to teams. Creating backup or alternative teams capable of handling tasks during emergencies or unforeseen worker shortages adds to the organization's overall resilience. Effective collaboration and communication strategies improve team members' ability to work together fluidly, regardless of their regular positions.

Another aspect of people-related redundancy is the creation of a flexible workforce. Enabling remote work capabilities is a viable approach for maintaining company continuity amid disruptions like natural disasters or public health emergencies. Cross-site collaboration broadens the workforce by allowing work to continue even if one location is experiencing difficulties. In this way, workers can still be available even in the event of personal emergencies. Besides implementing redundant work capabilities, allowing more flexible means of communication can also improve a workplace’s ability to handle critical situations. For example, if there's a problem with worker emails, having a phone-system or even allowing texting to different departments can allow work to continue. Thus, encouraging employees to share casual, but not critical, contact information with each other can create alternative avenues of communication [27].

Several circumstances can result in the use of redundancy. External circumstances can have a substantial influence on a firm during an economic downturn, forcing managers to make the painful decision to let go of staff, even if they have been contributing constructively to the company. This proactive step is used to help the organization manage financial issues and guarantee its long-term viability. The choice to terminate a firm, whether to seek other initiatives, retire, or change careers, can all result in redundancy. Employees may be let go in such instances owing to the total end of business activities, necessitating a comprehensive and thoughtful transition management strategy [28].

Certain job titles can become outdated due to changes in technology or business procedures, resulting in redundancy. Adoption of an electronic phone system, for example, may reduce the requirement for a traditional receptionist function. Employees with duplicate job titles may be impacted in these cases when the firm adapts to technological improvements. Furthermore, insufficient money for a specific project or overall financial limits within a company might result in redundancy. In such cases, employers may be forced to make difficult decisions in order to match the personnel with available resources, therefore avoiding financial losses and safeguarding the organization's economic health.

Furthermore, when a company decides to migrate to a new site, redundancy may emerge as a result of the financial limitations involved with the shift. The difficulties of assisting every employee's move, along with the necessity to reduce for a smooth transition, may push businesses to make smart employment decisions. Employers must examine issues such as long-term sustainability of employment, increasing company demands, and the skill sets necessary for future growth when reviewing potentially redundant functions. Best practices for dealing with redundancy include communicating clearly with impacted personnel, offering support services such as career counseling or retraining, and adhering to legal and ethical norms [29].

## Processes

Internally, without considering the supply chain, redundancy can improve the efficiency of the production through the process of duplicate security processes as well as duplicate repair or machine parts in order to ensure that attacks are both less likely to succeed, and in the event that they do, easily repairable, hence a proper application of redundancy can also induce rapidity into the manufacturing process.

One important application of redundancy is in safety measures for equipment, specifically in the use-procedures of Lock-Out Tag-Out, or LOTO. LOTO is the practice of not walking away from equipment until the employee is done using it, has powered it down or disconnected it from a power source, waiting for it to cool, or locking it. The OSHA standard for The Control of Hazardous Energy 29, CFR 1910.147, provides a general industry guideline for controlling industrial and electric devices [30]. Following these guidelines ensures that employees always understand the current state of the equipment, its intended uses and stress limits, as well as any signs that the equipment may be actively dangerous or not, with redundant steps such as checking twice on functions to ensure power is off. To ensure that such procedures are followed, the employees should be trained on proper equipment use and LOTO procedure, with regular monitoring and occasional surveys, as well as annual audits of the LOTO procedures.

Another place where redundancy can be induced to the production process itself to ensure the quality of the parts manufactured. Due to the scale of the production process, much of modern manufacturing is now automated, but these rely on sensor units and internal applications to ensure the material is properly in place before getting to work. For non-automatic processes, ensuring that every “n-th” component or batch on the line undergoes quality control and performance testing helps to ensure fewer parts recalls, and maintains the company’s reputation for quality [31]. Another way would be ensuring employees practice redundancy in their own actions, such as the classic phrase ‘Measure Twice, Cut Once’. These measures ensure that quality is maintained if technological sensors which could better guarantee quality are offline in the event of a cyber-attack.

While most manufacturers have embraced redundancy to ensure safety and product quality, far fewer have attempted to induce redundancy into the production process and supply chain, as it is seen as inefficiency. In the modern production model of Just-In-Time production, components are produced to fulfill orders in real time, in order to ensure as little overhead or redundant components as possible. While this increases profitability in optimal conditions, it has little flexibility in meeting supply and demand shocks [14]. For example, a single producer of electronic components suffering a cyber-attack resulted in Toyota temporarily ceasing production in 14 factories. Other examples of the costs of the inflexibility of the Just-In-Time model can be found in the sudden demand shocks during COVID, as well as the supply shocks which began with the current conflict in Ukraine.

Because of the lack of surplus parts to fulfill orders in the event of a downed system means that orders could no longer be fulfilled, freezing the rest of the supply chain until backchannels could be established and the problem resolved, meaning that the entire production process effectively had no production, well below a possible minimum threshold. Producers must be willing to balance the possible costs of such overhead in parts with the potential costs of lost business thanks to downtime [10, pp. 169]. Besides ensuring they will not slow the supply chain from possible attacks on them, they can also protect themselves from inefficiencies placed on the supply chain by attacks on their suppliers. By having multiple Tier 2 and Tier 3 suppliers for the same materials or sub-components, while they might lose the efficiency of bulk contracts with a highly efficient supplier, it ensures that they are less likely to be affected by attack-induced downtime or inefficiencies on their suppliers [32]. By the nature of globalization, businesses can no longer afford to think only of their own individual success and efficiency and must begin considering the possible effects of their fellow actors in the market and in the supply chain and realize that they themselves owe their own responsibility to this chain to ensure healthy business relations, good reputation, and overall loss reduction.

## Technology

Besides the redundancy provided by people and procedures in the Automotive Manufacturing Industry, essential technologies play a pivotal role in ensuring the resilience of automotive manufacturing companies.

In the automotive manufacturing industry, the importance of data backups in a multi-cloud environment cannot be overstated. Some of the popular cloud data storage providers are AWS, Azure, Google Cloud Platform (GCP), Oracle and Alibaba. Multi-cloud backup solutions provide redundancy by storing critical data across multiple cloud service providers. This ensures that if one cloud provider experiences a service disruption or a cyberattack, the data remains accessible from alternative sources, minimizing downtime and data loss. According to a report [32] by Gartner on cloud infrastructure and platform services, having a multi-cloud strategy enhances resilience by reducing dependence on a single provider.

Having physical backups of critical data in another location adds an extra layer of redundancy for cyber resilience in automotive manufacturing. In the event of a catastrophic event like a cyber-physical attack or a natural disaster, physical backups stored in a different geographical location can be crucial for recovery without relying solely on digital backups. Critical Backups should be routinely conducted, stored offsite, rotated, and periodically validated. The National Institute of Standards and Technology (NIST) emphasizes the importance of offsite backups for disaster recovery in its guidelines. [33]

Industrial Control Systems (ICS) also play a pivotal role in the automation and control of manufacturing processes in the automotive industry. These systems encompass supervisory control and data acquisition (SCADA) systems, programmable logic controllers (PLCs), and other technologies that manage and monitor production processes ranging from assembly line robotics to quality control inspections. In an automotive manufacturing plant, redundant ICS can ensure continuous operation even if one control system fails.

For instance, if a PLC unit responsible for managing the robotic arms in the welding section of the assembly line, experiences a sudden hardware failure due to a cyberattack. A redundant system will have a failover counterpart that is not connected to the affected network, an automated failover mechanism detects hardware failures, seamlessly transitions control to the redundant system, and ensures real-time data synchronization, thereby guaranteeing continuous and resilient production operations. Software solutions like TOSIBOX and MDT AutoSave provide functionalities for implementing redundant ICS in automotive manufacturing. These tools facilitate version control, change management, and backup/restore capabilities, ensuring that critical control system configurations are duplicated and ready to take over in case of a failure. NIST stresses the importance of redundant implementation for critical systems, systems that have high up-time requirements and systems that require ongoing antivirus updates such that signature updates can be performed without impacting operations [34]

In the domain of automotive manufacturing, securing cyber resilience is crucial, and the significance of data backups and redundant implementation of Industrial Control Systems (ICS) cannot be overstated. These measures serve as a strong safety net, mitigating the potentially severe consequences of cyber threats on critical operations. By prioritizing data backups and redundancy in ICS, automotive manufacturers not only protect valuable information but also strengthen their ability to sustain uninterrupted production, ultimately bolstering the overall resilience of their cyber infrastructure in the face of evolving threats.

# Resourcefulness

According to [9], Resourcefulness is “ability to diagnose and prioritize problems and initiate solutions by identifying and mobilizing material, monetary, informational, technological, and human resources”. In other words, it is the awareness of the manufacturers’ goals, legal obligations, assets, possible threats, and possible vulnerabilities. After these are known, critical business functions and the assets which support them must be prioritized by importance, as defined by its business goals, as well as the value provided by that business function. Thus, car parts manufacturers should routinely perform a Risk Assessment to determine the current vulnerabilities in the IT system [10, pp. 14].

Thus, resourcefulness can be induced by engineering business technology and procedures, as well as its approach to individuals such as employees or customers, around building a state of awareness, ensuring that the manufactures is not only aware of the state of the system, but also of the possible cause and cure for any changes to that state, such as an inability to access data thanks to a ransomware attack.

For manufacturers, this state of awareness is not just for the state of their own system, but also awareness of the state of fellow actors in the supply chain, as any delay on an entity lower in the supply chain translates into delays for all above them. Just the same, delays in their own production can lead to a loss of reputation with those above them in the supply chain. By establishing rapport with trusted actors and creating a system of more open information sharing among them, manufacturers can ensure shared Resourcefulness, and reap the benefits of everyone’s system resiliency.

## People

Manufacturing facilities are large in scale, especially for car manufacturing, and different parts of the manufacturing process, such as welding or machine-tooling, may rarely if ever interact with each other, much less with entire other departments such as IT departments or emergency response teams. This lack of communication between departments leads to specialization which means in the event of an emergency, other departments cannot be relied upon to help solve the issue because they do not have the necessary knowledge to be of much help. And while cross training can improve matters, departments may still be wary of accepting ‘outside help’ if a sense of interdepartmental cooperation is not fostered.

Collaboration is recognized as being supremely important within a workplace, with survey’s finding that as many as 75% of responders regarding it as such. By encouraging cross-collaboration, certain informal understandings of how systems work and their unique ticks which can act as signals for optimal or suboptimal performance, and thus an indicator of a possible emergency or cyber-attack, can be understood by more employees, leading to a greater sense of a facilities resources, vulnerabilities, and possible response tactics [35].

One way to encourage this sense of familiarity and information sharing is through project teams. The designing and production of a possible new car axel or brake system requires the expertise of several departments including marketing, material suppliers, engineers, and line-workers. Projects such as these not only can produce a possible new IP for the benefit of the manufacturer, but also encourage information sharing across departments, each offering their expertise to the other and explaining project notes. Encouraging this trust and information sharing must still be balanced with access control policies such as password sharing. [35]

Employees can also offer their own unique concerns and possible expertise about the running of the facility or the quality of the equipment and possible security concerns via the setting up of a suggestion box. A suggestion box would allow disaster response teams to get a better sense of employees' understanding and opinion of the current response systems and what they regard as weaknesses to them, or with possible unforeseen problems with equipment that might indicate an undetected cyber threat. For example, if an attack manages to send a feed of false information about the state of equipment function on a machine-parts line, then IT and emergency response teams would assume nothing is amiss or be unable to pinpoint the exact cause of failure to meet production goals. By allowing the employees who actually work with the equipment to voice their concerns, IT departments could be made aware of the discrepancy between their sensors and actual equipment performance, and thus of possible faults in their security system. Having some system to allow employees to voice their concerns will, such as a suggestion box or ideas board, will give security teams a finer detailed sense of not only the subsystems of the facility, but also a glimpse into employee understanding or lack thereof of these systems, which can help inform future information security decisions [36].

Besides dissecting internal views of cyber security weaknesses, outside experts can also be contracted to probe the IT system for possible faults. While security teams will conduct their own internal Red-Team tests of the system, they might through their familiarity with the system develop blind spots to internal problems. As demonstrated in [16], a small team of outside researchers managed to find enough faults in the cyber security of the cars of companies like Nissan, Honda, and Kia to remotely access and control 15.5 million vehicles produced by these companies. Hiring such researchers to conduct security audits and probes of the system can reveal previously unknown vulnerabilities, increasing total system awareness for the manufacturer.

## Processes

Because of the strength of machinery involved, as well as potential for burns or other injuries, not only should manufacturers of all types have a robust emergency response plan for cyber-attacks, but also for injuries or handling extreme weather events. Such a plan can be developed from a Risk Assessment, with a subset being reserved for Hazard Assessment, relating to possible injury scenarios or emergencies and their possible causes. Should a cyber-attack lead to such an injury, such as causing an inability to properly shutdown stamping machines or other production equipment, first and foremost plans must be in place to clear the area of the accident and safely treat the injured [37]. Having regular training sessions for employees about proper emergency response can help accidents be relatively resolved before an Emergency Response Team responds and helps encourage situational awareness among employees.

In the event of bizarre or suboptimal equipment or system behavior, or in the event of long-term problems, a Root Cause Analysis can be used to identify the issue and point to possible solutions, such as with a Fishbone Diagram or Pareto Charts. A fishbone diagram is a way to visualize the process of information gathering to determine the problem, the probable causes, and the solution. Taking the problem as the ‘head’ of the fish, such as the inability to properly shutdown equipment, the ‘ribs’ of the fish are the factors determined to be contributing to the problem, based on broad categories such as materials or sensors. These can then be subdivided into smaller ‘ribs’ for what in these categories is contributing to the problem such as suppliers of materials, or timing delays on the sensor. Enough brainstorming of this type will give a thorough understanding of the causes of any potential problems and become a groundwork for solutions [38].

Pareto Charts are a more data-driven visualizer of Root Cause Analysis. By utilizing visualization software, the frequency of specific types of problems such as Ransomware incidents can be tracked over time. By visually ranking the likelihood of problems, as well as the causes, it allows Incident Response Teams can then address the most significant or most common defects first, giving them a ranked prioritization of issues relative both to their likelihood and the overall goals of the manufacturer. For example, one of the key interests of manufacturers is the possible causes of downtime. With Pareto Charts, all the recorded instances of downtime and how long they occurred are measured against the reason, be it planned maintenance or an outside attack. With this, Response Teams can then prioritize their approach to any unplanned downtime occurrence by examining the most likely causes first [38].

Besides securing their own assets, the nature of the car manufacturing requires efficient interactions between multiple suppliers, parts manufacturers and car manufacturers, as well as third party professionals and clients such as auto parts stores. Because of the nature of the supply chain, any disruption to any one of these entities can reverberate throughout the entire supply chain. Because of the already interconnected nature of the business, many manufacturers and suppliers have responded by establishing a policy of Open Data Sharing, ensuring that each actor in the supply chain is aware of the current state of the others to best coordinate actions in event of sudden shocks. One modern example of this is Catena-X, a German ‘consortium’ of car manufacturers, parts manufacturers, and suppliers acting together as a sort of pseudo mega-company organized with a standardized information flow to ensure efficiency [39]. If a company wished to join such an entity, it would require having policies and procedures built around securing this exchange of information, ensuring efficient management of the supply chain.

## Technology

Besides the resourcefulness provided by people and procedures in the Automotive Manufacturing Industry, essential technologies play a pivotal role in ensuring the resilience of automotive manufacturing companies. Resourcefulness in the technology sector of manufacturing requires having sensors both for equipment and for the network connected to them to automatically notice current system status and possible signs of intrusion or data compromise.

One example of an all encompassing system observation tool is a Security Information and Event Management (SIEM) system. A SIEM system is a comprehensive solution that combines security information management (SIM) and security event management (SEM) functionalities. SIEM systems collect, aggregate, correlate, and analyze log data generated throughout an organization's technology infrastructure [40]. SIEM plays a crucial role in enhancing cyber resiliency in the automotive manufacturing industry by providing threat detection, supply chain security and compliance management solutions. If suspicious behavior is monitored, such as a surge in login attempts to a critical production control system, then the SIEM system, integrated into the network, quickly identifies this abnormal behavior and triggers an alert. Security personnel are promptly notified and can take immediate action to investigate the incident, isolate compromised systems, and block the attacker's access. This rapid response helps prevent production disruptions and safeguards valuable manufacturing data.

Furthermore, the automotive manufacturing industry relies on intricate supply chains involving numerous suppliers and vendors. To enhance cyber resiliency, SIEM systems are deployed to continuously assess the security posture of these external partners. They identify vulnerabilities or breaches in the supply chain, helping manufacturers proactively address security issues. Consider a situation where a key supplier in the automotive manufacturing chain experiences a data breach. SIEM's monitoring capabilities extend to the supply chain, and it quickly detects unusual access patterns and data exfiltration from the supplier's systems. The SIEM generates alerts, enabling the manufacturer to assess the impact on their operations. By having a well-defined incident response plan in place, the manufacturer can work with the supplier to contain the breach, mitigate potential supply chain disruptions, and meet regulatory requirements. This proactive approach minimizes the risk of cyber incidents affecting the entire production process and ensures compliance with industry-specific standards such as ISO 21434.

Within an automotive manufacturing facility, various devices and machines must communicate with each other to ensure smooth production processes. In the event of a cyberattack that disrupts the primary network, a mesh network can come to the rescue. Imagine a situation where a cyber incident compromises the central network infrastructure. Devices in the plant would then automatically switch to a self-healing mesh network. This alternative communication method allows devices to maintain connectivity and continue production, minimizing downtime and production losses.

Besides integrating complex network sensor systems, manufacturers can also maintain situational awareness via utilizing alternative communication protocols. These protocols serve as backup means of communication, ensuring that critical functions can continue even when primary network infrastructure is compromised. They play a vital role in maintaining operational continuity and reducing the impact of cyber incidents. Such communication protocols are of paramount importance in the automotive manufacturing industry, particularly during cyberattacks.

One such example of alternate communication protocols is Satellite Communication. Imagine an automotive manufacturing plant located in a remote area with limited access to traditional communication networks. In such a scenario, a cyberattack targeting the primary network infrastructure could disrupt communication and data exchange. However, by having satellite communication systems in place, the plant can maintain connectivity even during network outages caused by cyber incidents. Satellite communication, provided by companies like Inmarsat or Iridium, ensures that critical data can still be transmitted, enabling remote plant operations to continue seamlessly.

# Rapidity

According to [9], Rapidity is “the capacity to restore function in a timely manner”, meaning it is the ability to quickly absorb and recover from an attack or disaster event such as a medical emergency. The swiftness of the response and recovery must be balanced with maintaining the other CIA goals, ensuring that in the attempt at quickly restoring data availability we do not sacrifice data confidentiality [10, pp. 12].

Car manufacturers and parts manufacturers practice rapidity by quickly limiting the damage done within an emergency or cyber-attack, and by ensuring a speedy recovery. In the case of a medical emergency then, rapidity would be the speed or responding to the injured, clearing the scene, engaging medical response procedure, and stopping immediate risk. The rapidity would also include the speed at which the person recovers or that facility production returns to normal after the incident has been resolved.

Car manufacturers must not just consider the rapidity of their own facilities, but also in how they adjust to the changing conditions caused by emergencies in related facilities. When its supplier suffered a ransomware attack which caused them to halt their own production, Toyota had to halt its production for 24 hours before establishing a backup network between themselves and their supplier, with a full recovery being estimated as taking two weeks [15]. In this case then, the rapidity of attack absorption was 24 hours, while the rapidity of recovery was estimated to be two weeks. Thus, when engineering for system rapidity, consideration must be made not just for response to attacks and long-term recovery, but also for speed of adjustment to changes in circumstances by way of attacks on related entities such as suppliers.

## People

Theoretically, all the previous controls mentioned such as cross training and hiring of outside experts should not only improve the other aspects of resiliency, but also but their accumulative effect improve the rapidity of response and recovery to events, as having more hands able to handle a variety of tasks will help incidents be quickly resolved.

However, in the event of an injury, even if the incident is quickly resolved, workplace efficiency is still compromised as a necessary employee is now no longer able to work. Shortages in workers in any department, be it in IT or on the factory floor, can be mitigated by having an ‘on-call’ system of employment, where employees have a contract obligation to work under call-in in exchange for extra compensation, or to have contract workers which are called on in case of sudden shifts in production quotas or available workers. These gaps could also be filled by externally hired contractors.

Incident response teams can also be established, with certain employees being given temporary leadership positions and authority in the event of a sudden emergency such as a natural disaster, or a very severe cyber-attack. Different teams could be trained to specialize for specific scenarios to have a more efficient response to these scenarios, as they will not require as much time remembering specific response plans for vastly different scenarios and could by their specialization could quickly respond to different by similar scenarios. An injury response team could, for example, quickly adjust training for treating a broken arm for that of a leg or rib in case of a workplace accident. Just the same, cyber-incident response teams could also be diversified to treat specific attacks or even specific symptoms such as inability to access certain files, or sudden alterations in equipment performance.

Finally, an informal network of ‘local experts’ can be identified in the company, where employee’s skill sets not related to their current position are identified so in the event of an emergency, those with skill sets that are suitable for the situation at hand can be called upon. If a line-employee also has some experience with cyber security but for some reason was not hired to that position, if a cyber security profession is needed, they could be called upon as a resource.

## Processes

Just as clearly defined incident response plans can improve the Resourcefulness and Robustness, it can also improve the Rapidity, as employees will quickly know, or be able to guess, what is wrong, the proper immediate response procedures, and response teams and managers can begin the process of brainstorming possible long-term fixes to prevent future incidents.

Ways to improve the speed of the response and implementation of pre-made response procedures is to train via a series of easily memorable codes such as ‘Code Red’ or ‘Code Orange’. Using codes such as these which can be informally ranked by their name to the seriousness of the response can help employees not only remember these plans, but also get into the right mindset of implementation. As worker safety should be paramount, ‘Code Red’ type codes should be implemented for physical dangers such as a workplace injury or a natural disaster such as a tornado. Meanwhile, more long-term problems such as ongoing cyber-attacks, while still of great concern, should have less immediate code-terms such as ‘Code Yellow’.

Another way to improve the speed of response procedures is to have measurable benchmarks for the implementation, so a minimum and maximum response time can be understood. 3 NIST recommended measurements are Maximum Tolerable Downtime, Recovery Time Objective, and Recovery Point Objective. The Maximum Tolerable Downtime represents the total amount of outage time in the production and supply-chain interaction. These represent an overall measurement of response to cyber-attacks, unconcerned with specific equipment performance and instead how their interactions affect the ability to provide a minimum of performance. [33, pp. 17].

Recovery Time Objectives and Recovery Point Objectives are a more specific look at the system itself by understanding how its subsystems and components contribute to the system itself. Recovery Time Objectives represent the maximum amount of time that a system component or resource can remain unavailable before there is noticeable impact on other system resources or the critical business functions. These can be applied to each of the system components and thus can give an accurate hierarchy for importance of the components and necessity of response to improper performance by measuring how quickly the system can break down without them. This in turn informs what technologies are best suited for the system itself, and for managing the Maximum Tolerable Downtime. The Recovery Point Objective, meanwhile, represents the point in time a backup from prior to a cyber attack can be recovered. Thus, this represents the maximum allowed data loss in the event of a cyber-attack, and can be used to create a triage-system based on this maximum allowed loss balanced with system component recovery times and the Maximum Tolerable Downtime [33, pp. 17].

## Technology

In today's interconnected world, the Automotive Manufacturing Industry faces an ever-increasing threat landscape in cyberspace. Cyberattacks have the potential to disrupt production lines, compromise intellectual property, and endanger customer safety. Therefore, in addition to the procedures that provide rapidity in cyber resiliency there are three key technologies that play a critical role in achieving cyber resiliency.

Intrusion Detection and Prevention Systems (IDPS) are cybersecurity technologies designed to monitor network traffic and system activities in real-time, aiming to detect and respond to unauthorized access, malicious activities, and security threats promptly. IDPS can be host-based or network-based and use various detection methods, including signature-based, anomaly-based, and behavior-based approaches [41]. Consider an automotive manufacturing plant responsible for producing Engine Control Modules for a new vehicle model. An IDPS deployed in this facility continuously analyzes network traffic and system logs. In the scenario, an attacker gains unauthorized access to the plant's network through a compromised vendor's account. The IDPS detects this unusual activity and triggers an alert. A well-trained security analyst can evaluate if the alert is a threat or not and act accordingly. An example of an IDPS is Snort, an open-source network intrusion detection system. Snort uses signature-based and anomaly-based detection techniques to identify known threats and unusual patterns in network traffic. When a match is found, it can generate alerts or take predefined actions to block malicious traffic.

Security Orchestration, Automation, and Response (SOAR) systems are integrated cybersecurity platforms that combine orchestration and automation capabilities with incident response and case management. These systems streamline security operations, accelerate incident detection and response, and enable organizations to coordinate and automate actions across their security infrastructure. Imagine an automotive manufacturer's Security Operations Center (SOC) overwhelmed with alerts from various security tools due to a suspected data breach. Without SOAR, security analysts would spend valuable time manually investigating each alert. With SOAR, the system can automatically prioritize alerts, correlate data from multiple sources, and initiate predefined response actions. One of the leading SOAR platforms is Palo Alto Networks Cortex XSOAR. It enables organizations to create and execute automated workflows for incident response, allowing for rapid identification, containment, and resolution of security incidents [42].

Behavioral Analytics and User Entity Behavior Analytics (UEBA) are cybersecurity technologies that focus on monitoring and analyzing user and system behavior to identify anomalies and potential security threats [43]. These systems establish a baseline of normal behavior and raise alerts when deviations from this baseline occur. Consider an automotive manufacturing facility where employees have specific roles and access levels. UEBA technology continuously analyzes user behavior and flags any unusual activities, such as an employee accessing sensitive design files from a remote location, which is outside their typical behavior. One example of a UEBA solution is Splunk User Behavior Analytics (UBA). Splunk UBA uses machine learning and advanced analytics to detect deviations in user behavior and prioritize security incidents based on risk.

By detecting threats in real-time, orchestrating incident response, and monitoring user behavior, IDPS, SOAR, and UEBA technologies can help protect the automotive manufacturing sector from cyberattacks, ensuring the continued production of safe and innovative vehicles. As the industry evolves, embracing and implementing these technologies becomes increasingly crucial in the ongoing battle against cyber threats.

# Results/Conclusions

This cyber resiliency framework was constructed as a living document to study the 4R’s of cyber resiliency (Robustness, Redundancy, Resourcefulness, Rapidity) as it relates to the people, processes, and technology involved in Car Parts Manufacturing. Each of the aspects of the 4Rs and how it could be induced into the business via its attributes, broken down into the following categories:

1. Employees and fellow actors in the supply chain (ie: suppliers, direct customers, tertiary customers)

2. Processes, Procedures, Broader Business Approaches, and documentation thereof

3. Infrastructure, technologies, equipment, and networks.

Throughout our research, online sources were required in order to understand how cyber resiliency related to the business of manufacturing, and specifically of car parts manufacturing, and what recent challenges they have faced in that field. The most important information was how work accidents, ransomware attacks, and supply or demand shocks such as was the case during the COVID pandemic affected this environment, and the possible solutions to correcting these issues. The general outcomes of our studies are documented in the sections below:

## Outcome 1: People

Due to the dangerous nature of manufacturing, employee safety must be paramount, with injuries not just made rarer, but also quickly managed and empty spots on the production line quickly refilled while the injured employee recovers. Solutions to induce these can include safety exercises and training, as well as maintaining emergency incident response teams and on-call employees to fill in gaps. Not only will these practices ensure processes go smoothly, but ensuring a safe environment will improve employee retention. Another way to improve retention, and to fill potential information gaps, is by making employees feel heard via an employee suggestion box.

Besides ensuring employee safety, employees must also be prepared to respond to suddenly changing conditions thanks to cyber attacks causing usually relied upon systems becoming unavailable. This can be accomplished via training, both on security response for IT teams, but also for cross-collaborative training for line-employees in order to be made familiar with other equipment in the facility, and with the potential problems and solutions for said equipment. And should this training still not be enough, managers can try to identify ‘local experts’ who can be called upon in the event of a specific emergency, or if necessary hire-out to outside contractors to resolve a cyber attack incident. By implementing these solutions, manufacturers will induce the 4R’s attributes of resiliency into the manufacturing process with regards to employees.

## Outcome 2: Processes

The purpose of the process controls was to consider broadly categorized but common problems faced by car parts manufacturers when it came to internal procedures, and consider examples of controls that could be implemented to counteract them. Common problems included vulnerability not just to equipment such as networks, but also manufactured parts such as processors for automobiles. As such, implementing equipment and product quality testing procedures, USB-use policies, and issue documentation charts such as Fishbone Charts fit under these broad categories.

Besides internal controls, processes must also be considered in relation to other actors in the supply chain. Due to the increasingly complex supply chain systems which manufacturers and their clients rely on, it becomes more important these days to think not of separate levels of clients, such as wholesalers or other car manufacturers, nor of separate levels of suppliers, such as Tiers 1 through 3, but instead of all as fellow actors in the supply chain. Thus, procedures must be implemented not just to ensure better cyber resiliency within a single manufacturer, but also to ensure better informed and trusted relations with these other actors. This could include only making contracts with fellow actors who maintain a minimum standard of system security to minimize the risk of slowdowns, broadening the number of suppliers even at the risk of relying on inefficient manufacturers in order to continue production, or entering Open Information Agreements with trusted actors in the supply chain. By considering how individual actors affect, and are affected by, the larger supply chain, manufacturers can better implement controls which induce resiliency into the system.

## Outcome 3: Technology

The manufacturing sector is experiencing a significant increase in cyberattacks, including data breaches, ransomware attacks, and viruses. Therefore, ensuring cyber resiliency is crucial for the success of companies in the manufacturing industry. Because it's not a matter of if a cyberattack will occur but rather when, how resilient will the systems be against the attack shapes the implementation of technology. The goal of technology controls is to identify and assess existing technologies that can enhance Cyber Resiliency in the Automotive Manufacturing Sector.

Data encryption is a key component of achieving robustness since the manufacturing industry holds critical data, from intellectual property to customer personal information. The loss of such data could severely impact the company's reputation and survival. Another way is implementing redundant Industrial Control Systems (ICS), which ensures that if one system fails due to an attack, another can take over without disrupting production.

Once strategies for making automotive manufacturing systems robust and redundant are in place, it's essential to identify technologies that are resourceful and provide rapid responses during a cyberattack. Alternative communication methods play a vital role in resourcefulness, as attackers may attempt to limit internal communication during an attack. Options like satellite phones for remote locations or secure cellular communication on isolated devices can help maintain communication.

To increase the speed of response, employing Security Orchestration and Automation Response (SOAR) technology can expedite the response to well-known attacks and scale up as needed. This allows the Security Operation Center to prioritize critical threats efficiently. While the manufacturing sector is renowned for its efficiency through processes like Six Sigma, there is room for improvement in cyber resilience. The technologies identified in this paper offer solutions to address these gaps.

# Future Works

Automotive manufacturers and specifically parts manufacturers have multiple options for inducing cyber resiliency as well as general system resiliency, relating to their employees and business partners, their internal business processes, and their technology. Some of these controls, such as the establishment of information sharing networks between business partners might require specialized laws to be in place in order to ensure that these new forms of networks do not develop into monopolies or cartels, so legal and political president might be considered in the long term as new controls against cyber attacks are fond and implemented.

Such controls apply not just to automotive manufacturers, but many other forms of manufacturing, both for consumer products such as phones or airline parts, or for larger scale infrastructure projects such as power grids. The main requirements for manufacturing remain relatively unchanged across most fields: well functioning equipment, safe and talented workers, and safe supply chains between business partners. Studying the more exacting structural differences between the manufacturers by type could lead to broadly applicable controls and standards for specific manufacturers, leading to faster implementation of effective cyber resilience.

# References

[1] U.S. Government, “Who Invented the Automobile,” loc.gov. <https://www.loc.gov/everyday-mysteries/motor-vehicles-aeronautics-astronautics/item/who-invented-the-automobile/> (accessed October 27, 2023)

[2] Collectors Autosupply, “How Many Parts are in a Car?” collectorsautosupply.com. <https://collectorsautosupply.com/blog/how-many-parts-are-in-a-car/> (accessed October 27, 2023)

[3] “Tiers 1, 2, and 3 in Automotive Supply Chains.” royaleinternational.com. <https://www.royaleinternational.com/2022/12/tiers-1-2-and-3-in-automotive-supply-chains/> (accessed October 27, 2023)

[4] “Responsible Material Sourcing.” corporate.ford.com. <https://corporate.ford.com/social-impact/sustainability/responsible-material-sourcing.html#:~:text=With%20around%201%2C400%20Tier,to%20use%20in%20our%20vehicles> (accessed October 27, 2023)

[5] <https://parts.ford.com/shop/en/us>

[6] “OEM Parts: Everything You Need to Know.” caranddriver.com. <https://www.caranddriver.com/research/a33216493/oem-parts/> (accessed October 27, 2023)

[7] K. Baxter, “What is the Supply Chain in the Automotive Industry?” blog.intekfreight-logistics.com <https://blog.intekfreight-logistics.com/what-is-supply-chain-automotive-industry> (accessed October 27, 2023)

[8] R. Ross *et. al*., “Developing Cyber Resilient Systems: A Systems Security Engineering Approach,” *NIST Special Publication 800-160* Vol. 2, Dec. 2021, doi/url: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2.pdf>

[9] M. Bishop, M. Carvalho, R. For and L.M. Mayron, “Resilience is More than Availability,” *Proceedings New Security Paradigms Workshop,*  pp. 95-104, 2011.

[10] Gibson, *Managing Risk in Information Systems,* 2nd ed. Burlington, MA: Jones & Bartlett Learning, 2015.

[11] “What is the CIA Triad?” fortinet.com. <https://www.fortinet.com/resources/cyberglossary/cia-triad#:~:text=The%20three%20letters%20in%20%22CIA,and%20methods%20for%20creating%20solutions> (accessed October 27, 2023)

[12] “ISA/IEC 62443 Series of Standards.” isa.org. <https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards> (accessed October 27, 2023)

[13] VicOne, “UN R155: Understanding UN Regulation No. 155 and Its Requirements.” vicone.com. <https://vicone.com/why-vicone/un-r155> (accessed November 5, 2023)

[14] S. Anderson *et. al.* “What are the Main Problems with a JIT (Just in Time) Production Strategy.” investopedia.com. <https://www.investopedia.com/ask/answers/040215/what-are-main-problems-jit-just-time-production-strategy.asp> (accessed November 5, 2023)

[15] Reuters. “Cyber Attack on Toyota’s Supply Chain Shuts its 14 Factories in Japan for 24 Hours.” CNN Business. <https://www.cnn.com/2022/03/01/business/toyota-japan-cyberattack-production-restarts-intl-hnk/index.html> (accessed November 5, 2023)

[16] J. Gitlin. “Hackers Discover that Vulnerabilities are Rife in the Auto Industry.” arstechnica.com. <https://arstechnica.com/cars/2023/01/hackers-discover-that-vulnerabilities-are-rife-in-the-auto-industry/> (Accessed November 5, 2023).

[17] M. Wolden, R. Valverde, & M. Talla. “The effectiveness of COBIT 5 information security framework for reducing cyber attacks on supply chain management system.” *IFAC-PapersOnLine*, *48*(3), 1846-1852.

[18] A. Yeboah-Ofori, S. Islam. “Cyber Security Threat Modeling for Supply Chain Organizational Environments”. *Future internet*, *11.* doi: <https://doi.org/10.3390/fi11030063>

[19]The Manufacturer. “Improving Cyber Resiliency in Manufacturing.” themanufacturer.com <https://www.themanufacturer.com/articles/improving-cyber-resiliency-in-manufacturing/> (accessed November 5, 2023)

[20] A. Coos. “Automotive Companies and Data Security.” endpointprotector.com. <https://www.endpointprotector.com/blog/automotive-companies-and-data-security/> (accessed November 5, 2023)

[21] N. Marko et. al. “A Process to Facilitate Automated Automotive Cybersecurity Testing.” [IEEE 93rd Vehicular Technology Conference (VTC2021-Spring)](https://ieeexplore.ieee.org/xpl/conhome/9448628/proceeding), June 2021, doi: [10.1109/VTC2021-Spring51267.2021.9448913](https://doi.org/10.1109/VTC2021-Spring51267.2021.9448913)

[22] P. Roth & J. Titley. “Practical Considerations for Auto Suppliers Navigating Supply Chain Disruptions.” varnumlaw.com.

<https://www.varnumlaw.com/insights/practical-considerations-for-auto-suppliers-navigating-supply-chain-disruptions/> (accessed November 5, 2023)

[23] Paloalto Networks. “What is Network Segmentation?” paloaltonetworks.com. <https://www.paloaltonetworks.com/cyberpedia/what-is-network-segmentation> (accessed November 5, 2023)

[24] Cica. “Layering Network Security Through Segmentation.” cisa.gov. <https://www.cisa.gov/sites/default/files/publications/layering-network-security-segmentation_infographic_508_0.pdf> (accessed November 5, 2023)

[25] IBM. “What is Encryption?” ibm.com. <https://www.ibm.com/topics/encryption> (accessed November 5, 2023)

[26] Solar Winds. “What is Network Access Control?”. Solarwinds.com. <https://www.solarwinds.com/resources/it-glossary/network-access-control> (accessed November 5, 2023)

[27] D.V. Gibson and B.E. Mendleson. “Redundancy,” *The Journal of Business Communication,* vol. 21, no. 1, pp. 43-61, Jan. 1984, doi/url: <https://doi.org/10.1177/002194368402100105>

[28] J.I. Jenssen and A. Greve, “Does the Degree of Redundancy in Social Networks Influence the Success of Business Start-Ups?” *International Journal of Entrepreneurial Behavior & Research,* vol.8, no. 5, pp. 254-267, 2002, doi/url: [10.1108/13552550210448357](http://dx.doi.org/10.1108/13552550210448357)

[29] “What is Redundancy? Definition and Meaning.” Market Business News. <https://marketbusinessnews.com/financial-glossary/redundancy-definition-meaning/> (accessed November 13, 2023)

[30] [“What is lockout tagout?”, bradyid.com, https://www.bradyid.com/what-is-lockout-tagout](https://www.bradyid.com/what-is-lockout-tagout) (accessed November 12, 2023)

[31] [“The Importance of Redundancies in Manufacturing,” gesrepair.com, https://gesrepair.com/the-importance-of-redundancies-in-manufacturing/#:~:text=Redundancy%20for%20quality&text=Redundancies%20for%20quality%20provide%20safeguards,in%20the%20quality%20control%20process](https://gesrepair.com/the-importance-of-redundancies-in-manufacturing/#:~:text=Redundancy%20for%20quality&text=Redundancies%20for%20quality%20provide%20safeguards,in%20the%20quality%20control%20process) (accessed November 11, 2023)

[32] [J. Stone, “Redundancy No Longer Out of Favor in Manufacturing”, jacksonlewis.com. https://www.jacksonlewis.com/insights/redundancy-no-longer-out-favor-manufacturing](https://www.jacksonlewis.com/insights/redundancy-no-longer-out-favor-manufacturing) (accessed November 11, 2023)

[32] M. Rimol, “Gartner Top 10 Trends Impacting Infrastructure & Operations for 2020”, gartner.com.

<https://www.gartner.com/smarterwithgartner/gartner-top-10-trends-impacting-infrastructure-operations-for-2020> (accessed November 12, 2023)

[33] M. Swanson *et. al.* “Contingency Planning Guide for Federal Information Systems,” *NIST Special Publication 800-34 Rev. 1*, May 2010, doi/url: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf>

[34] K. Stouffer *et. al.* “Guide to Operational Technology (OT) Security,” *NIST Special Publication NIST SP 800-82r3*, Sept. 2023, doi/url: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf>

[35] A. Kumar, “11 Ways to Improve Cross-Departmental Collaboration.” Saviom.com.<https://www.saviom.com/blog/improve-cross-departmental-collaboration/> (accessed November 16, 2023)

[36] Indeed. “Ideas for Using a Suggestion Box in the Workplace.” Indeed.com.<https://www.indeed.com/hire/c/info/suggestion-box#:~:text=Better%20communication%3A%20A%20suggestion%20box,problems%20but%20also%20suggest%20solutions>. (accessed November 16, 2023)

[37] US Gov. “Emergency Response Plan.” Ready.gov.<https://www.ready.gov/business/emergency-plans/emergency-response-plan> (accessed November 16, 2023)

[38] E. Fogg. “Root Cause Analysis: A Complete Guide for Manufacturers.” Machinemetrics.com.<https://www.machinemetrics.com/blog/root-cause-analysis> (accessed November 16, 2023)

[39] E.Garsten. “Open Data Sharing Key To Automaker Survival, Study Says.” Forbes.com.<https://www.forbes.com/sites/edgarsten/2021/06/21/open-data-sharing-key-to-automaker-survival-study-says/?sh=bd20c2ee46c9> (accessed November 16, 2023)

[40] Microsoft. “What is SIEM?”. Microsoft.com. <https://www.microsoft.com/en-us/security/business/security-101/what-is-siem#SIEM-defined> (accessed November 18, 2023)

[41] Juniper Networks. “What is IDS and IPS?”. Juniper.net. <https://www.juniper.net/us/en/research-topics/what-is-ids-ips.html> (accessed December 2, 2023)

[42] “What is SOAR?” paloaltonetworks.com. <https://www.paloaltonetworks.com/cyberpedia/what-is-soar#:~:text=Security%20orchestration%2C%20automation%20and%20response,all%20within%20a%20single%20platform> (accessed December 2, 2023)

[43] “What is UEBA?” fortinet.com. <https://www.fortinet.com/resources/cyberglossary/what-is-ueba> (accessed December 2, 2023)