Dealing with Toxic Fumes in Production Environments

Carl L. Rumberg

Department of Cybersecurity, Old Dominion University

Professor Akeyla Porcher

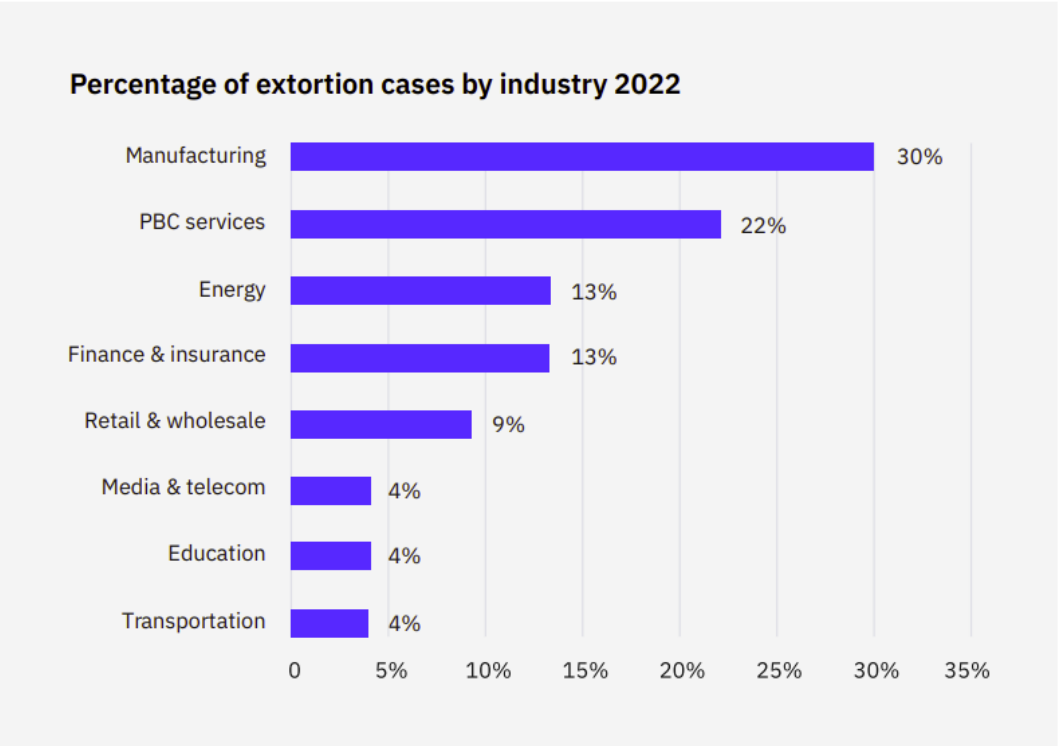
6/21/2023

Introduction

Modern manufacturing places heavy emphasis on efficiency and automation in order to reduce costs while simultaneously maximizing profits. While automation is taking a portion of human labor out of these environments, many still require human workers to either monitor machines on-site or perform other tasks. With this in mind, human safety should be at the absolute forefront of all manufacturer's minds. While there are many measures in place to protect people from moving machinery, falls from height, and much more, the existence of toxic fumes can be a "silent killer." Unlike the previously mentioned physical dangers, toxic fumes often cannot be seen, smelled, or otherwise detected via human senses. Some toxic fumes may slowly wear down the health of staff working in manufacturing, while others may have much faster detrimental effects. While not all manufacturing processes or plants involve toxic fumes, it is of the utmost importance to staff safety and environmental health that toxic fumes be constantly monitored to ensure non-critical levels are reached.

Another issue faced in modern manufacturing is the prominence of cyberattacks. There is no shortage of cyberattacks happening everyday, and these attacks seem to be on an exponential slope. Prime targets of late have been critical infrastructure and manufacturing. The below chart, taken from the IBM Security X-Force Threat Intelligence Index 2023, shows data for extortion cases in 2022 (Worley et al., 2023).

Figure 1



As shown in the chart, the majority of cyberattacks resulting in extortion from 2022 reside within the manufacturing industry. With the advent of the cyberattack "industry" and the rise in sophistication and collaboration between hacker groups, the threat to manufacturing via cyberattacks cannot be understated.

Systems to detect and alert upon toxic fume detection certainly already exist on the market, however our innovation aims to take a step above the rest and include robust cybersecurity measures to mitigate the previously mentioned challenges faced today. The importance of securing sensor systems designed to protect human lives and environmental health against cyber threats should be the next big step for manufacturers. Our innovation seeks to implement proper access control, authentication, and encryption schemes into smart sensor systems. The lack of these measures in competing brands could lead to tampering of the sensor

itself, unauthorized access, threshold/data manipulation, and overall brings the reliability and integrity of these sensors into question.

Literature Review

For this section, literature will be reviewed in order to describe the problem as well as the innovation. The first four articles reviewed will address the problem itself through analyzing: toxic fumes in manufacturing, human health risks, environmental hazards, and cyberattacks in manufacturing(in that order). The last three articles will address the innovation via analyzing and connecting ideas found from: programmable logic controllers, cybersecurity in manufacturing, and cybersecurity measures our product would involve(in that order).

Toxic Fumes in Manufacturing

The first article showcases a proposed sampling method for fumes and toxic gasses found within Malaysian small to medium enterprises(SMEs) (Hariri et al., 2012). The enterprises that were testing using this proposed method all utilize welding in their processes, thus toxic fumes stemming from welding is the focus of the study. In one of the samples taken from the study,

While the sampling process in question is interesting, it lies outside of the scope of what is necessary for our purposes, however it is important to note that air samples were taken **before** work had begun to ensure no abnormalities, and again **after** work had begun. The results of the sampling process showed traces of Manganese(Mn) and Ferum(Fe) with 5.9% and 21.67% mass respectively (Hariri et al., 2012). The National Institute for Occupational Safety Health(NIOSH) states that the "recommended airborne exposure limit is **5 mg/m^3**" for Ferum fumes and **3 mg/3^3** for Manganese fumes (CDC, 2019). According to the CDC, some studies show that metal workers exposed to much lower levels of manganese perform "more poorly" on tests of

"brain function and motor skills" (CDC, 2019). Also according to the CDC, exposure to iron oxide(Ferum) fumes can cause: pneumoconiosis, metal fume fever, and more. The results shown from the study sample show that workers in Malaysia certainly face risks from toxic fume inhalation.

Considering welding is a very common industrial process, it is fair to assume that the results of their study could be shared across all environments involving welding, regardless of physical location. While the ultimate solution is providing better ventilation/filtration in workplaces, this is a great use case for sensors to detect said fumes in order to notify staff of unsafe conditions.

Human Health Risks

This article addresses the threat of toxic fumes found within manufacturing, specifically the existence of heavy metal fumes found within Iranian salt factories. The study aimed to test the pollutant levels within the factory to ensure that they were below the permissible limits. This was done via "personal monitoring in the breathing zone of the workers during shift work" according to the NIOSH 7300 method for fume measurement (Kalteh et al., 2021).

A health risk assessment was performed for the samples taken in the environment utilizing the USEPA method, which is a complex formula that involves: average daily inhalation intake, concentration of the related compound, exposure time, exposure frequency, exposure duration, and average lifetime (Kalteh et al., 2021). All of the levels for toxic fumes were below their respective permissible limits in regard to the samples taken. However, of the three "units," or sections of the manufacturing plant, the laboratory unit showed that workers within the unit were at risk of "resultant" adverse health effects. In the maintenance unit, numbers showed a "high potential for cancer risk in lifetime" (Kalteh et al., 2021). The same result was found within the samples for the metal-works unit. The researchers noted that the levels they gained

from their study in the salt factory were much lower than the determined levels from welding and waste recycling industries. All of this research points to the overwhelming need for constant monitoring of said fumes, instead of occasional sampling. Occasional sampling every 3 months or so leaves risk for high levels of fumes for the duration between tests, which doesn't adequately protect workers from fume volatility caused by frequent changes in production, abnormalities, ventilation faults, and more.

Environmental Hazards

This study focuses strictly on environmental pollution caused by plastic manufacturing, and real-time sensing challenges brought forth by the processes in question. The process, according to the study, is "Cured-in-place-pipe(CIPP), which is a means of repairing buried infrastructure such as pipes (Noh et al., 2023). The process is being used throughout "Asia, Europe, Oceana, and North America," and involves setting up temporary worksites where needed. While the process itself is again outside the scope of information needed for our purposes, the data obtained from the sensor difficulties is important as it highlights a need for better sensors.

According to the study, the photoionization detectors(PID sensors) were inadequate and showed incredibly high variances in their measurements. The PID sensors "overestimated styrene levels by a factor of 40 to 3,500" (Noh et al., 2023). According to the authors, "PID sensors should not be used to estimate air pollution magnitude, gas-phase styrene concentrations, and the capabilities of these sensing technologies, and their limitations require scrutiny" (Noh et al., 2023). These sensors failing to accurately detect the amount of volatile organic compounds(VOCs) and hazardous air pollutants(HAPs) will be an issue in the future regarding gaining accurate measurements in order to improve legislation regarding the usage of CIPP practices.

Cyber Attacks in Manufacturing

This article, titled “Bad Parts: Are Our Manufacturing Systems at Risk of Silent Cyberattacks?” highlights the need to protect manufacturing processes through providing historical examples and potential future scenarios, however places heavy emphasis on subtractive manufacturing via CNC machines and spoke heavily on G-code alteration. The first example is as follows,

> Recent cyberattacks have highlighted the risk of physical equipment operating outside designed tolerances to produce catastrophic failures. A related threat is cyberattacks that change the design and manufacturing of a machine's part, such as an automobile brake component, so it no longer functions properly (Turner et al., 2015).

Note that it is stated the “risk of physical equipment operating outside designed tolerances…” A similar scenario is highly imaginable by which current toxic fume sensors could have their thresholds for alarm covertly raised to highly unsafe levels, potentially leading to extreme health and environmental dangers.

The study further goes to state a number of potential attack surfaces, such as: design tool chain, controls, direct equipment, network, and quality control. The overwhelming majority of their analyses pointed to unsecure transfers of information such as CAD files lacking encryption-in-transit, lack of digital signatures, overwhelming USB usage, email transfers, and so forth. Furthermore they stated that the majority of machines used within production environments use outdated operating systems and versions, with “Windows XP being the most common” (Turner et al., 2015). The lack of even basic security measures being used within such environments does not inspire hope that toxic fume monitoring systems will be up-to-date with the current landscape of network security, and further points to the need for heightened security within vital sensors in the manufacturing industry.

Problem Review

Before proceeding with the innovation portion of the literature review, I will recap some of the larger points that create the problem at hand.

1. **Existence of Toxic Fumes in Manufacturing**

Most manufacturing utilizes processes that produce toxic fumes, whether it be plastic manufacturing, welding, machining, and so on. The monitoring of said fumes is of the utmost importance for safety and compliance.

2. **Environmental and Human Health Concerns/Compliance**

In order to stay compliant with human safety as well as environmental regulations, our sensors would be a great monitoring system. It would also quickly alert employees of unsafe levels in order to protect their health.

3. **Large Uptick in Cyberattacks on Manufacturing Sector**

As shown via the numbers from IBM's report, as well as seemingly weekly headlines, there is a substantial increase in cyberattacks in general, with the majority-by-sector hitting manufacturing. The manufacturing industry is behind in regards to technology, hence why they are being targeted so heavily.

The next three sections will tie literature review into the innovation itself.

Programmable Logic Controllers

At the heart of the innovation lies programmable logic controllers(PLCs). PLCs are "computer-based, solid-state, single processor devices that emulate the behavior of an electric ladder diagram capable of controlling many types of industrial equipment and entire automated systems" (Alphonsus & Abdullah, 2016). PLCs essentially take input, and make decisions based on their programming in order to issue commands to other components within the manufacturing

process. In regards to this innovation, a PLC would be fitted with a sensor to monitor for toxic fumes, and a network interface by which it could: communicate with the central monitoring system in order to log toxic fume data, issue alerts when levels reach above the desired threshold, and take modification commands from the central monitoring system. The product, once fitted with the appropriate sensor and network interface, would be deemed an Internet-of-Things(IoT) device.

Cybersecurity in Manufacturing

Overall network cybersecurity within manufacturing should be at the forefront of manufacturers mind's considering recent trends. While network security of manufacturing facilities lies outside the scope of our innovation, it should be noted that security measures should be implemented for the network that these sensors are a part of. Intrusion detection/ prevention systems(IDS/IPS), robust firewalls, and secure physical facilities should be a bare minimum for any production environment. While our sensors and monitoring system will be secure in and of themselves, tying a secure product into an unsecure network immediately negates any security benefits gained from the devices themselves.

According to Mullet et al., " the integration of heterogeneous equipment into the industrial cyber environment makes cybersecurity considerations mandatory in the design strategy of companies" (Mullet et al., 2021). As previously stated, especially with the upcoming of various IoT devices becoming more and more integrated into manufacturing, cybersecurity is a measure that absolutely must be taken.

In regards to the innovation, it has already been stated why the smart sensors are necessary to protect human lives and the environment, and the next section will address the measures our product will put in place to live up to the high cybersecurity standards of today.

Cybersecurity Measures

This article focuses on IoT device security, with emphasis on device authentication and access control. According to Ali et al., “Due to huge number of IoT devices and machine to machine communication feature of IoT, legacy authentication and authorization techniques are not viable for it” (Ali et al., 2016). They further state a potential solution to authentication/ authorization being the usage of digital certificates provided by a certificate authority(CA) for each device. This is similar to the authentication scheme our smart sensors will be using. Two-factor and biometric authentication would be used to prevent unauthorized users from masquerading as authenticated users with high-level access, either to log in to sensors to manipulate settings or to gain access to the surrounding network. Individual sensors could be assigned different digital certificates, creating a public-key infrastructure(PKI) for the network and the systems monitoring the sensors themselves. This would ensure that mutual authentication could be performed when sensors communicate with devices throughout the network. The below chart shows recommendations from various researchers regarding authentication and encryption techniques, note that many share the idea of using digital certificates(or a similar solution), and either Kerberos or PKI.

Figure 1

Various security recommendations from researchers.

Ref #	*Authentication*	*Access control*	*Environment*	*Security*
Chen et al. [6]	Nil	Group Access	Distributed IoT System	IPsec
Rivera et al. [7]	OAuth 2.0	User managed Access Model	Multi-Agent IoT system	TLS
Ouaddah et al. [9]	Nil	Organization bases access control	Inter Organizations	Web services
Gaikward et al. [10]	Kerberos	Nil	Smart Homes (IoT)	AES, SHA1
Periera et al. [11]	Credentials, shared key, password	Service Level Access control	Nil	DTLS light implementation
Mahalle et al. [12]	Group Authentication	Nil	Wi-Fi	Light weight cryptographic function
Panwar et al. [13]	Digital certificates	Nil	Nil	DTLS
Santoso et al. [31]	Elliptic Curve Cryptography	Nil	Smart Homes (IoT)	Encryption, Wi-Fi
Lee et al. [32]	Light weight Cryptography	Nil	Nil	Light weight XOR operation
Park et al. [33]	Simple certificates	Nil	Nil	PKI
Zhao et al. [34]	Elliptic Curve Cryptography	Nil	Nil	SHA1

Ali et al. also mention the importance of encryption, stating that they are absolutely essential to network security, in order to uphold the confidentiality and integrity of data transmitted over the network. For these reasons, our product would utilize the usage of PKI. As digital certificates mutually authenticate both parties in an exchange, the key pairs of each party are also used to encrypt communications between said two parties. This would ensure that any communications performed between sensors and monitoring systems would be confidential and secure from tampering.

Relation of Innovation to Other Classes

Interpreting the American Past

This innovation relates heavily to the American past, as past trends can point directly to the significance of this product. Following trends found in the history of American industrial development, there have been large transformations made possible by large technological advancements, and also a growing emphasis on the safety of workers. Our product would not only be considered a technological advancement, but also has a large focus strictly on the safety of workers in industrial/manufacturing environments. Historically the safety of workers was not taken into heavy consideration, however nowadays through organizations such as OSHA, worker safety is of the utmost importance in the workplace. The American commitment to improving workplace regulations in order to protect citizens is bolstered by our innovation.

Introduction to Criminology

Criminology is the study of crime and criminal behavior, and within the class students are taught that some of the best responses to crime are proactive measures. Imagine a scenario by which a manufacturing plant's ventilation system is only working at 50%, meaning that toxic fumes are not being ventilated quickly enough to keep fume levels within safe parameters for staff working within the building. Without our innovation, it would be easy for business owners to cut costs by running the ventilation as is, instead of paying potentially large amounts of money to get it fixed in order to keep their staff safe. This is because without the innovation, there wouldn't be a solid method to determine that toxic fume levels are unsafe for staff, until staff become ill. In this manner our innovation is a proactive measure to not only protect staff and the environment, but also a proactive measure to prevent potential negligence from business owners seeking to save money.

Just as criminologists seek to address root causes of crime and criminal behavior, our smart sensor aims to address the underlying risks of working in production environments, ultimately creating a safer workplace.

Introductory Chemistry

Chemistry class highlights the importance of precision and accuracy in measurements taken, as well as the hazards of dealing with toxic chemicals or fumes. Our innovation could certainly be used outside of the manufacturing sphere, and be used in waste management facilities, water recycling plants, or chemistry labs. The sensors themselves would allow peace-of-mind to chemists and others within labs as they could rest assured that if toxic fumes are emitted, whether on purpose or on accident within the lab, the sensors would detect and alert all to their presence. Furthermore, the usage of our sensors would promote the concept of "green chemistry," a type of chemistry that places emphasis on sustainable chemical practices in order to protect the environment. The sensors could provide the data necessary to immediately detect and mitigate toxic fumes created via their processes, and help chemists find processes that produce less hazardous substances.

The logged data taken from our sensors could provide good data for analysis by chemists. The sensors could be outfitted to detect specific chemicals of the chemists choosing, and could help via their logged data for chemists to make more informed decisions on their processes.

Innovation Effectiveness

The effectiveness of our innovation could be measured in a number of ways, I will list a few below with detailed explanations.

1. **Reduced Cybersecurity Attacks/Incidents:** The number of successful cybersecurity attacks related to the sensing system should be either zero, or significantly lower than the

previous baseline prior to implementation. This can be monitored via logging of unauthorized access attempts(failed and successful vs. baseline) or the tampering of settings for smart sensors**.**

2. **Compliance with Standards:** If the production environment, after implementation of these measures, is compliant with industry standards taken from credible parties such as NIST or the ISO, it is a certain sign of success.
3. **Alert System Evaluation Tests:** Through testing the sensors prior to sending them to customers, as well as on a regular basis to ensure their consistent reliability, the effectiveness of the system could be measured. For example, if the sensors are placed in a mock-production environment and toxic fumes are pumped into the space, the sensors should alert right away when fumes above the set threshold are detected. Testing could also be done to determine the rate of false positives or false negatives, if any at all.
4. **Comparison to Similar Systems:** Our smart-sensing system could be compared to more traditional methods of fume detection, such as the sampling methods mentioned from the Iranian salt factory example. If our product can detect fumes as well, or better, than that of the methods used by scientists using OSHA or NIOSH methods, it can be assumed that the sensors are working effectively.
5. **User Feedback:** Simply put, if the users within production and system administrators are happy with the usability and effectiveness of the measures, it is a good sign that everything is working as intended without difficulty.

Turning the Innovation to Reality

There are a multitude of things that would need to be done in order to turn this innovation into reality. First of all, a fair amount of research and development would likely be necessary to

fully-flesh out the idea. This research could include: exploring options as far as sensing technologies go(what type of sensors work best, what type of sensors can detect the widest range of fumes, etc.), what are the requirements for toxic fume detection in production environments(where should sensors be placed, would increased airflow in buildings throw sensor readings off, etc.), and designing for the hardware casing and software portions of the product.

After initial research, a fair amount of prototyping and testing would need to be done to see what works and what doesn't. While the product is meant strictly for fume detection, should it still look aesthetically pleasing? Are certain casing styles for the sensor more expensive to produce, thus increasing the cost unnecessarily for the customers? Does the placement of the sensing apparatus on the body of the sensor greatly affect its sensing capabilities? Are there any vulnerabilities or flaws within the software for the sensor and its monitoring system? All of these questions could gain answers by many rounds of prototyping and improving the product. After a "final" prototype is created, a fair amount of field testing would be required in various production environments to ensure their proper function and reliability throughout different areas. During this phase, data from field tests as well as feedback from a handful of users could greatly help in making the true final product.

Creating of the central monitoring system. A fair amount of software development would be required in order to create a software that would communicate with, and log data from, all of the sensors that a manufacturer may place within their facilities. The system could include a dashboard that shows real-time data taken from sensors that includes their location within the building. The monitoring system would also have to be connected to some sort of alert system, whether that be a traditional fire alarm-esque system, or it could also connect to staff members personal devices for additional coverage, however that would add to the amount of software development needed.

Once the product is finalized, a plan for mass-production and sourcing of required materials would be needed. This could consist of building manufacturing facilities, hiring staff, and sourcing supply chains, or it could consist of partnering with similar manufacturers in order to reduce overall cost.

Plans for deployment and installation of our product would also be required in order to build a customer-base. Things such as sensor placement, network connectivity, power supplies, and regular maintenance would have to be tailor-made to each customer considering their personal needs and pre-existing infrastructure. Some companies may need sensors only in defined areas of their environments that deal with potential for toxic fumes, while others may need them throughout their whole environment. Other companies could struggle to bring power and network connectivity to the sensors due to lack of pre-existing cable runs, and so on.

The last thing that would be required for this innovation to be turned into reality would be the constant strive to improve the product, the efficiency and cost of manufacturing, and potentially grow the product into a line of sensors for various uses. This would be heavily based upon sales data and consumer feedback, as well as industry trends.

Next Steps

I've learned quite a bit about entrepreneurship and innovation development through this project, mainly that I have much more to learn about both subjects. This project has taught me about interdisciplinary thinking through the work necessary to combine information regarding industrial environments, toxic fume sensing, entrepreneurial processes, and cybersecurity into one singular product. I believe that in order to truly create this innovation, a team of purely cybersecurity majors would be severely lacking in all regards to the cybersecurity portion of the product, and a team of experts in all fields related to the product would need to be brought in. The largest point learned through this project is the importance of having subject-matter experts

on a product-development team, as a cybersecurity professional alone has little hope of worming their way through the rigorous steps required to make this innovation.

The largest thing that I would do differently if I had to do this project again would be to choose an innovation tailored more heavily to cybersecurity. While it was very enjoyable stepping out of my comfort zone in order to think through this project, I feel that I have rudimentary knowledge in some aspects of the product and was not incredibly suited to this type of innovation. That being said, I do not regret following through with the proposal as I feel I learned my limitations and also the importance of having teams of various experts within the workforce.

References

Ali, I., Sabir, S., & Ullah, Z. (2016). Internet of Things Security, Device Authentication and Access Control: A Review. *International Journal of Computer Science and Information Security (IJCSIS)*, *14*(8). https://doi.org/https://doi.org/10.48550/arXiv.1901.07309

Alphonsus, E. R., & Abdullah, M. O. (2016). A review on the applications of Programmable Logic Controllers (plcs). *Renewable and Sustainable Energy Reviews*, *60*, 1185–1205. https://doi.org/10.1016/j.rser.2016.01.025

Centers for Disease Control and Prevention. (2019, October 30). CDC - NIOSH Pocket Guide to Chemical Hazards - iron oxide dust and fume (as Fe). Centers for Disease Control and Prevention. https://www.cdc.gov/niosh/npg/npgd0344.html

Centers for Disease Control and Prevention. (2023, March 7). Welding and Manganese. Centers for Disease Control and Prevention. https://www.cdc.gov/niosh/topics/welding/default.html

Hariri, A., Yusof, M. Z., & Leman, A. M. (2012). Sampling method for welding fumes and toxic gasses in Malaysian small and Medium Enterprises (smes). *Energy and Environment Research*, *2*(2). https://doi.org/10.5539/eer.v2n2p13

Kalteh, S., Mozaffari, S., Molaei, I., & Maleki, R. (2021). Health risk assessment of metal fumes in an Iranian mineral salt company. *Journal of Air Pollution and Health*. https://doi.org/10.18502/japh.v5i3.5389

References

Mullet, V., Sondi, P., & Ramat, E. (2021). A review of cybersecurity guidelines for manufacturing factories in industry 4.0. *IEEE Access*, *9*, 23235–23263. https://doi.org/10.1109/access.2021.3056650

Noh, Y., Xia, L., Zyaykina, N. N., Boor, B. E., Shannahan, J. H., & Whelton, A. J. (2023). Regulatory significance of plastic manufacturing air pollution discharged into terrestrial environments and real-time sensing challenges. *Environmental Science & Technology Letters*, *10*(2), 152–158. https://doi.org/10.1021/acs.estlett.2c00710

Turner, H., White, J., Camelio, J. A., Williams, C., Amos, B., & Parker, R. (2015). Bad parts: Are our manufacturing systems at risk of silent cyberattacks? *IEEE Security & Privacy*, *13*(3), 40–47. https://doi.org/10.1109/msp.2015.60

Worley, M., Caridi, C., Alvarez, M., Bakken, K., Bedard, Y., Brancati, M., Bedell, C., & Chung, J. (2023). IBM Security X-Force Threat Intelligence Index 2023. https://www.ibm.com/downloads/cas/DB4GL8YM