

NAVIGATING THE NEXUS

Industry 4.0 Implementation and the Turbulent Waters of Cybersecurity and Process Safety

Abstract

The allure of Industry 4.0, characterised by the fusion of cyber-physical systems, the Internet of Things (IoT), and artificial intelligence, is undeniable. However, beneath the surface of this revolution lies a treacherous conundrum: the tension between the relentless push for innovation and the lurking spectres of cyber threats that pose grave risks to security and process safety

Contents

1-	Executive Summary	5
2-	List of Abbreviations	6
3-	Introduction	9
3.1	Background and Context	9
3.2	Problem Statement	10
3.3	Study Objectives	10
3.3.1	To Investigate Industry 4.0 Implementation Drivers:	10
3.3.2	To Analyse Cybersecurity Challenges:	10
3.3.3	To Examine Process Safety Implications:	10
3.3.4	To Identify Conflict Resolution Strategies:	10
3.3.5	To Develop Recommendations:	10
3.4	Significance of the Study	11
3.4.1	Industrial Resilience:	11
3.4.2	Safety and Well-being:	11
3.4.3	Economic Impact:	11
3.4.4	Policy Formulation:	11
3.4.5	Academic Contribution:	11
3.4.6	Strategic Decision-Making:	11
3.5	Scope & Limitations	11
3.5.1	Scope of the Dissertation:	11
3.5.2	Limitations of the Dissertation:	12
4-	Drive for Automation and Industry 4.0	13
4.1	Industry 4.0: Concepts and Evolution	13
4.2	Cybersecurity in the Age of Industry 4.0	15
4.3	Cyber threat from Industry 4.0	15
5-	Process Safety	16
5.1	An introduction to Process Safety	16
5.2	Process Safety Gone Wrong	16
5.3	COMAH Regulations	19
5.3.1	COMAH Management	19
5.4	NIS Regulations	19
5.4.1	NIS2 Directive	20
5.5	Cyber Security threat on IACS	20
5.6	Understanding IACS	21
6-	IT Cyber Security Vs OT Cyber Risk	22

6.1	IT Previous Ignorance of OT	22
6.2	Connected Devices Search Engines – Invites to Hack?	23
6.3	Anatomy of a Cyber Attack	24
7-	Triton Cyber Attack Case Study	27
7.1	Motivations and Drivers for the Attack	27
7.1.1	Targeted Safety Systems	28
7.1.2	The Attack Vector	28
7.1.3	The Detection of the Attack	29
7.2	Challenges and Implications	29
7.2.1	Detection Difficulty	29
7.2.2	Response Complexity	29
7.2.3	Industry Wake-up Call	29
8-	Existing Industrial Risks	30
8.1	Threat Landscape in Industry 4.0	30
8.2	Assessing Cyber Risks – (safety & security)	30
8.3	Best Practice Protection from Attack	31
8.3.1	Network Segmentation:	32
8.3.2	Regular Patching and Updates:	32
8.3.3	Change Default Credentials:	32
8.3.4	Disabling Unnecessary Services:	32
8.3.5	Implement Network Access Controls:	32
8.3.6	Security by Obscurity Is Not Enough:	32
8.3.7	Monitor and Audit:	32
8.3.8	Consider Using a VPN or Proxy:	32
8.3.9	Security Awareness Training:	32
8.3.10	Regularly Assess Exposure:	32
8.4	Vulnerabilities in Cyber-Physical Systems	32
8.4.1	Interconnectedness and Interoperability Challenges	33
8.4.2	Inadequate Authentication and Authorisation Mechanisms	33
8.4.3	Lack of Standardised Security Protocols	33
8.4.4	Limited Over-the-Air (OTA) Security Updates	33
8.4.5	Real-Time Operating System (RTOS) Vulnerabilities	33
8.4.6	Physical Attacks on Cyber-Physical Systems	33
8.4.7	COVID Implications	34
9-	Recommendations	35
9.1	Strategies for Mitigating Cyber Risks	35
9.1.1	Risk Assessment and Threat Modelling	35
9.1.2	Defence in Depth Approach	35
9.1.3	Continuous Monitoring and Anomaly Detection	36
9.1.4	Secure-by-Design Principles	36
9.1.5	Employee Training and Awareness Programs	38
9.1.6	Collaboration and Information Sharing	38

9.1.7	Incident Response and Recovery Planning	38
9.2	Applying Lessons Learned by Process Safety to Cybersecurity	38
9.2.1	Process Hazard Analysis (PHA) for Industry 4.0 Systems	38
9.2.2	Functional Safety and SIL Certification	38
9.2.3	Redundancy, Diversity and Hardening	39
9.2.4	Emergency Shutdown Systems (ESD) and Cyber-Physical Integration	39
9.2.5	Cybersecurity-Enabled Process Safety Training	39
9.2.6	Asset Management and Lifecycle Security	39
9.2.7	Regulatory Compliance and Industry Standards	40
10-	Conclusion	41
11-	References	42

Table of Figures

Figure 1: The role of Cyber Security best practice for COMAH and NIS regulations	15
Figure 2: Buncefield Oil & Gas Fire, Hemel Hempstead.(Lewis, 2015)	17
Figure 3: Aftermath of Buncefield Fire (Buncefield Major Incident Investigation Board, 2005)	18
Figure 4: NIS2 Directive implementation Timeline (Molina, 2023)	20
Figure 5: Increased use of COTS and increased connectivity leading to a Credible Threat to Safety (Butcher, 2019)	21
Figure 6: Example of the IT system and the OT system (IAIANI et al., 2021)	22
Figure 7: Drilldown to an OT device in Philadelphia listing potential vulnerabilities.	23
Figure 8: Shodan.io showing freely available information that can be used for exploitation.....	23
Figure 9: Anatomy of cyber-attack (Li & Liu, 2021).	26
Figure 10: Illustration of Triton Attack Route overcoming the Cybersecurity Zones (Stoler, 2018)	27
Figure 11: SIS Controller Remote Access Switch (McMillan, 2018).....	28
Figure 12: A usual Risk scoring matrix based on Likelihood & Consequence (Kaya, 2018)	30
Figure 13: Process Safety & Cyber Risk Assessment Comparison (Butcher, 2019)	31
Figure 14: Example of IACS Zone Criticality (Health & Safety Executive (HSE), 2017)	31

1- Executive Summary

This study examines the ardent insistence to encourage and promote Industry 4.0 adoption by its advocates, alongside the implications that can have on the Process Safety sector and Essential Service providers.

Due to the huge potential for a catastrophic incident both these sectors are scrutinised by the Health & Safety Executive (HSE). The HSE will have periodic interventions with these organisations focusing on specific hazard topics which the target organisation must present to show how these hazard topics are managed on-site. Threats triggered from cyber incident are becoming increasingly likely due to the implementation of interconnected devices in the field and the HSE are now including the management of threats from cyber-attack as one of their intervention topics.

Over the last few decades device architecture has been developed for the Safety Instrumented Systems (SIS) in these sectors and the selection of equipment has been carefully calculated based on the necessary integrity these devices need to have to ensure correct operation in the event of an incident. As technology moves forward however these stand-alone ‘dumb’ devices are becoming obsolete in favour of interconnected ‘smart’ versions.

The push for Industry 4.0 comes from a myriad of suppliers who are promoting their off-the-shelf ‘smart’ products to become the next big thing. They highlight the benefits of interconnectivity for improving management visibility of processes, maximising efficiencies, and reduced downtime as well as stressing that competitors will become one step ahead if their target audience doesn’t immediately embrace their product and implement a plan to replace all their existing device architecture. But is that the right thing to do?

Machine designers are finding that ‘smart’ devices are becoming the only option open to them and that would be fine were it not for the fact that these ‘smart’ off-the-shelf devices are in their relative infancy when it comes to being faced with the interconnected domain and their exposure to the cyber-world.

The investigation in this report shows that the benefits from industry 4.0 devices in the Process Safety and Essential Services sectors bring with them threats that, if not considered carefully, could compromise the designed and calculated safety systems that have been preventing incidents for decades. By looking at historic events as an example it illustrates the potential of catastrophic consequences within the Process Safety Sector showing that field device abnormal behaviour can and has led to devastating outcomes.

By examining a case study of a real-life cyber-attack which shows that safety systems in these industries are already being targeted by hostile threat actors whose intent can only be to cause at the very best, maximum disruption for the target organisation and at the worst, national destabilisation of a target country. We also see how this attack was orchestrated by a persistent co-ordinated attacker that was prepared to wait for months to upload malware to provide increasing levels of access to the target system.

The study reveals the tools such as shodan.io that are being used by cyber security professionals that are also free to be used by threat actors with malicious intent. The level of detail provided by these tools shows hackers exactly which devices have not been kept updated and which exploitation they can use to circumvent the vulnerable devices providing an avenue into the organisations wider system.

Research into best practices to protect system security have been compiled and presented in this report along with a number of recognised vulnerabilities and recommendations that should be applied to minimise the cyber-security risk.

2- Statement regarding copyright

Declaration Statement: Michael Waite

I certify that this is all my own work and that all other sources of information, data, images, etc. have been acknowledged and referenced. This work has not been previously accepted in substance for any other degree and is not being concurrently submitted in candidature for any other degree.

Signed: 

Date: 7th March 2024

3- List of Abbreviations

ACL	– Access Control List
AI	– Artificial Intelligence
ALARP	– As Low As Reasonably Practicable
APT	– Advanced Persistent Threat
AR	– Augmented Reality
BPCS	– Basic Process Control System
CA	– Competent Authority
CIM	– Common Information Model
CIMAH	– Control of Industrial Major Accident Hazards
COTS	– Commercial Off The Shelf
CPS	– Cyber–Physical Systems
COMAH	– Control Of Major Accidents and Hazards
CIM	– Common Information Model
CLOPA	– Cyber Layers Of Protection Analysis
CPS	– Cyber–Physical Systems
DDoS	– Distributed Denial of Service
DSP	– Digital Service Provider
EA	– Environmental Agency
EC&I	– Electrical Control and Instrumentation
ESD	– Emergency Shutdown System
HMI	– Human Machine Interface
HSE	– Health and Safety Executive
IACS	– Industrial Automated Control System
IDS	– Intrusion Detection System
IEC	– International Electrotechnical Commission
IEEE	– Institute of Electrical and Electronic Engineers
ISA	– International Society of Automation
ISO	– International Organisation for Standardisation
IT	– Information Technology
IoT	– Internet of Things
LES	– Loss of Essential Service

LOPA – Layers Of Protection Analysis

MAH – Major Accident Hazard

MATTE – Major Accident To The Environment

MBSE – Model-Based Systems Engineering

NIS – Network and Information Services

OES – Operators of Essential Services

OG – Operational Guidance

ONR = Office for Nuclear Research

OSHA – Occupational Safety and Health Administration

OT – Operational Technology

OTA – Over The Air

PHA – Process Hazard Analysis

PSM – Process Safety Management

RAT – Remote Access Trojan

RDP – Remote Desktop Protocol

RTOS – Real Time Operating System

SIEM – Security Information and Event Management

SIL – Safety Integrity Level

SIS – Safety Instrumented Systems

USNM – United States National Museum

VLAN – Virtual Local Area Network

VPN – Virtual Private Network

VR – Virtual Reality

4- Introduction

In the modern industrial landscape, the digital transformation brought forth by Industry 4.0 has ushered in a new era of unprecedented technological advancement and efficiency. The promise of smart factories, autonomous systems, and seamless data integration has ignited a burning desire among industries worldwide to adopt these transformative technologies. The allure of Industry 4.0, characterised by the fusion of cyber-physical systems, the Internet of Things (IoT), and artificial intelligence, is undeniable. However, beneath the surface of this revolution lies a treacherous conundrum: the tension between the relentless push for innovation and the lurking spectres of cyber threats that pose grave risks to security and process safety.

The implementation of Industry 4.0 presents a paradox of progress. On one hand, it promises increased productivity, reduced downtime, and enhanced competitiveness. On the other hand, it exposes organisations to vulnerabilities that were inconceivable in traditional industrial settings. Cybersecurity breaches and disruptions in process safety can lead to catastrophic consequences, both in terms of financial losses and potential harm to human lives. As the boundaries between the physical and digital realms blur, it becomes increasingly vital to address the growing concerns surrounding the security and safety of Industry 4.0 systems.

This dissertation embarks on a journey to explore the intricate interplay between the fervent drive to implement Industry 4.0 and the ever-evolving landscape of cyber threats. It seeks to shed light on the conflicts that emerge when organisations strive to achieve operational excellence and innovation while safeguarding their assets, data, and the welfare of their workforce. By delving into case studies, analysing real-world incidents, and assessing existing frameworks, this research aims to provide a comprehensive understanding of the challenges and opportunities presented by the convergence of Industry 4.0 and cybersecurity.

In the pages that follow, we will navigate the turbulent waters of this conflict, examining the motivations driving Industry 4.0 adoption, the vulnerabilities inherent in the digital infrastructure, and the strategies and solutions available to mitigate cyber risks. Ultimately, this dissertation aspires to contribute to the discourse surrounding Industry 4.0 by offering insights and recommendations that can help organisations chart a course toward a safer and more secure future within the realm of Industry 4.0.

4.1 Background and Context

In the grand theatre of technological progress and industrial transformation, conversations about Industry 4.0 are often met with enthusiasm and excitement. It's a stage where the spotlight shines brightly on the promises of efficiency, automation, and innovation. Advocates of Industry 4.0 extol the virtues of smart factories, interconnected machines, and data-driven decision-making with unwavering conviction. Yet, amid these resounding accolades, there exists a subtle but palpable undercurrent—a moment of disquieting stillness, a silence that speaks volumes.

Picture this: a room filled with professionals, executives, and enthusiasts, gathered to discuss the myriad advantages of embracing Industry 4.0 technologies. The air is abuzz with anticipation as speakers passionately articulate the potential for increased productivity, reduced operational costs, and a competitive edge in the global market. Heads nod in agreement, and the atmosphere brims with optimism.

And then, it happens—an abrupt pause, a momentary hush, an awkward silence. It occurs when a brave soul raises a question or makes a comment that strays from the celebratory narrative, a question about cybersecurity. In that instant, the collective enthusiasm wanes, replaced by an uncomfortable tension, as if an uninvited guest has entered the room—an elephant in the room, to be precise.

This elephant symbolises the undeniable truth that accompanies the digital revolution of Industry 4.0: the ever-present and ever-growing cyber risks that threaten the very foundations of this transformation. It represents the acknowledgment that, in the rush to embrace the future, we must confront the perils lurking in the shadows, including data breaches, system vulnerabilities, and the potential for catastrophic consequences in the realm of process safety.

The phenomenon of this awkward silence is not unique but rather emblematic of a broader dilemma. It embodies the juxtaposition of two seemingly conflicting perspectives—the relentless push for innovation and the sobering reality of cybersecurity and process safety concerns. It serves as a poignant reminder that, while Industry 4.0 offers boundless opportunities, it also poses formidable challenges that demand our attention.

It is in the wake of this silence that the motivation for this dissertation takes root. By delving into the unspoken tension between the advantages of Industry 4.0 and the imperative of safeguarding against cyber threats and process safety risks, we aim to shine a light on this complex and often-overlooked intersection. This study endeavours to explore, analyse, and provide insights into the multifaceted conflict between innovation and security, ultimately seeking to bridge the gap between these two perspectives.

As we embark on this journey, we recognise the significance of addressing this silence, not as a deterrent but as a catalyst for meaningful dialogue, action, and the pursuit of solutions that will pave the way for a safer and more secure Industry 4.0 landscape.

4.2 Problem Statement

The adoption of Industry 4.0 technologies is met with enthusiasm, yet a persistent silence surrounds the unspoken conflict between the pursuit of innovation and the imperative of cybersecurity and process safety. This conflict represents a critical challenge for industries worldwide, as they navigate the digital transformation. The problem at hand is to understand, analyse, and address this tension, balancing the advantages of Industry 4.0 with the need to safeguard against evolving cyber threats and process safety risks. Consequently, the central problem to be addressed in this dissertation is:

How can organisations effectively reconcile the relentless drive to implement Industry 4.0 with the growing concerns surrounding cybersecurity and process safety, ensuring both innovation and security coexist harmoniously in the industrial landscape of the future?

4.3 Study Objectives

4.3.1 To Investigate Industry 4.0 Implementation Drivers:

Examine the motivations and drivers behind the adoption of Industry 4.0 technologies within various industries.

4.3.2 To Analyse Cybersecurity Challenges:

Explore the evolving landscape of cyber threats, vulnerabilities, and attack vectors in the context of Industry 4.0.

4.3.3 To Examine Process Safety Implications:

Assess the potential impact of Industry 4.0 on process safety and analyse case studies of incidents and consequences.

4.3.4 To Identify Conflict Resolution Strategies:

Investigate existing frameworks and best practices for mitigating cyber risks and integrating process safety measures effectively.

4.3.5 To Develop Recommendations:

Formulate practical guidelines and policy recommendations to help organisations strike a balance between Industry 4.0 innovation and security.

4.4 Significance of the Study

The significance of this study is multifaceted and extends across various domains, with profound implications for industry, society, and academia:

4.4.1 Industrial Resilience:

In an era characterised by rapid digitalisation and automation, the study addresses a critical need for industries to remain resilient against evolving cyber threats while reaping the benefits of Industry 4.0. By offering insights into balancing innovation and security, this research can guide organisations in maintaining operational continuity and competitiveness.

4.4.2 Safety and Well-being:

The significance of this study transcends the corporate realm and directly impacts the safety and well-being of employees, communities, and the environment. As the line between digital and the physical blurs, ensuring robust process safety is paramount. This research contributes to safeguarding lives and the environment.

4.4.3 Economic Impact:

Industry 4.0 holds the potential to revitalise economies and boost productivity. However, security breaches and process safety incidents can have far-reaching economic consequences. The study's recommendations can help mitigate these risks, protecting both local and global economies.

4.4.4 Policy Formulation:

Policymakers and regulatory bodies grapple with the challenge of keeping pace with technological advancements. This research provides valuable insights for policy formulation and standards development, aiding in the creation of a regulatory framework that fosters innovation while ensuring public safety.

4.4.5 Academic Contribution:

Within the academic realm, this study contributes to the understanding of the complex interplay between Industry 4.0, cybersecurity, and process safety. It offers a foundation for future research and contributes to the development of new theories, models, and frameworks in these fields.

4.4.6 Strategic Decision-Making:

For industry leaders and executives, this research serves as a knowledge resource for informed decision-making. It offers guidance on strategy development, investment choices, and the alignment of technology adoption with security and safety priorities.

In summary, the significance of this study lies in its potential to harmonise the transformative potential of Industry 4.0 with the need for security and safety in a rapidly evolving technological landscape. By shedding light on this complex intersection, the research strives to equip stakeholders across industries, governance, and academia with the knowledge and tools necessary to navigate this critical nexus, ensuring a safer and more secure future.

4.5 Scope & Limitations

4.5.1 Scope of the Dissertation:

1. **Industry Focus:** This dissertation primarily examines the conflict between Industry 4.0 and cybersecurity/process safety within the context of the manufacturing and industrial sectors including essential service providers.
2. **Global Perspective:** The study considers a global perspective, encompassing examples and cases from different regions and industries to provide a comprehensive view of the conflict.

3. **Technological Aspects:** The research delves into the technological aspects of Industry 4.0, encompassing cyber-physical systems, IoT, data analytics, and automation, while also addressing the evolving cybersecurity landscape.
4. **Case Studies:** This dissertation includes selected case studies to illustrate real-world scenarios and demonstrate how organisations have grappled with the conflict imposed by hostile, persistent threat actors with intent to evoke a catastrophic incident.
5. **Recommendations:** The research aims to develop practical recommendations and guidelines for organisations to mitigate cyber risks while embracing Industry 4.0.

4.5.2 Limitations of the Dissertation:

1. **Temporal Constraints:** Given the rapidly evolving nature of technology and cybersecurity threats, this dissertation may not comprehensively cover the most recent developments. It will focus on insights available up to the knowledge cutoff date in February 2024.
2. **Industry Specifics:** The scope does not extend to a detailed examination of specific industries (e.g., healthcare, finance) that might also be implementing Industry 4.0. Instead, it concentrates on the broader manufacturing and industrial context.
3. **Cybersecurity Deep Dive:** While the dissertation addresses cybersecurity issues, it does not provide an exhaustive examination of specific cybersecurity techniques, tools, or practices but rather focuses on their relationship with Industry 4.0.
4. **Process Safety Variability:** Process safety measures can vary significantly between different industries and organisations. This research may not cover every nuance and variation but instead provides a general perspective.
5. **Policy and Legal Aspects:** While the study acknowledges the relevance of policy and legal considerations, it does not offer an in-depth analysis of specific regulatory frameworks or legal implications surrounding Industry 4.0 and cybersecurity.
6. **Cultural and Organisational Dynamics:** The dissertation recognises that cultural and organisational factors play a significant role in addressing the conflict but does not delve deeply into these aspects.
7. **Detailed Economic Analysis:** While economic implications are mentioned, the study does not provide a comprehensive economic analysis of the conflict's financial impact on organisations or economies.

5- Drive for Automation and Industry 4.0

The adoption of Industry 4.0, also known as the Fourth Industrial Revolution, is driven by several key factors. Firstly, companies aim for greater agility, enabling them to respond swiftly to market changes and customer demands. Second, flexibility is crucial – Industry 4.0 technologies allow manufacturers to adapt production processes and optimise resources. Third, improving manufacturing efficiency is a priority, achieved through integration of technologies like the Internet of Things (IoT), cloud computing, analytics, and AI. Fourth, a focus on customer centricity leads to personalised products and enhanced experiences. Fifth, embracing innovation through smart factories equipped with sensors, robotics, and data analytics is essential. Sixth, empowering the workforce with tools for real-time monitoring and collaboration enhances productivity. Seventh, environmental sustainability is addressed by reducing energy consumption and minimising waste. Finally, recognising the need for a competitive advantage, companies embrace Industry 4.0 for improved responsiveness and cost-effectiveness. In summary, Industry 4.0 revolutionises manufacturing by creating smart factories and enabling efficient, customer-centric production processes. (Santos *et al.*, 2018)

5.1 Industry 4.0: Concepts and Evolution

Industry 4.0 is characterised by the integration of digital technologies, such as artificial intelligence, cloud computing, big data, and the Internet of Things, into the manufacturing sector and related industries. Industry 4.0 aims to create smart factories that can enhance production processes, improve quality, reduce costs, and increase customer satisfaction.

The evolution of Industry 4.0 can be traced back to the previous industrial revolutions, which transformed the modes of production and consumption in different ways. The first industrial revolution, which started in the late 18th century, introduced mechanisation and steam power to replace manual labour and animal power. The second industrial revolution, which occurred in the late 19th and early 20th centuries, brought mass production and electrification, enabled by assembly lines using oil, gas, and electric power. The third industrial revolution, which began in the second half of the 20th century, involved the automation and digitisation of production systems, driven by computers, electronics, and telecommunications. (Corò and Volpe, 2020)

The fourth industrial revolution differs from the previous ones in several aspects.

It is not limited to the manufacturing sector, but affects various industries and domains, such as energy, transportation, health care, education, agriculture, and services.

It is not only about enhancing productivity and efficiency, but also about creating new value propositions and business models that leverage data and connectivity.

It is not a linear progression of technological innovations, but a complex and dynamic convergence of multiple technologies that interact and influence each other. (Popkova, Ragulina and Bogoviz, 2019)

The main concepts of Industry 4.0 include:

- **Cyber-physical systems (CPS):** These are systems that combine physical components with digital capabilities, such as sensors, actuators, software, and networks. Cyber-physical systems enable real-time data collection and analysis, as well as remote monitoring and control of physical processes.
- **Internet of Things (IoT):** This is the network of physical objects that are embedded with sensors, software, and other technologies that enable them to communicate and exchange data with other devices and systems over the internet. The Internet of Things enables interconnectivity and interoperability among cyber-physical systems.

- **Cloud computing:** This is the delivery of computing services, such as servers, storage, databases, networking, software, analytics, and intelligence over the internet. Cloud computing enables scalability, flexibility, and cost-effectiveness of data processing and storage.
- **Big data:** This is the vast amount of both structured and unstructured data which is created by various sources at high velocity and variety. Big data enables insights and patterns discovery that can support decision making and innovation.
- **Artificial intelligence:** This is the simulation of human intelligence processes by machines, such as learning, reasoning, problem-solving, perception, natural language processing, and creativity. Artificial intelligence enables automation and optimisation of complex tasks that require human-like capabilities. (Rojko, 2017)

Industry 4.0 offers many benefits for manufacturers and other stakeholders in the value chain. Some of these benefits are:

- **Improved quality:** By using sensors and analytics to monitor production parameters and detect defects or anomalies in real time, manufacturers can reduce errors and waste, ensure compliance with standards and regulations, and increase customer satisfaction.
- **Increased efficiency:** By using automation and optimisation techniques to streamline production processes and reduce downtime or bottlenecks, manufacturers can increase output and reduce costs.
- **Enhanced flexibility:** By using digital technologies to enable customisation and personalisation of products or services according to customer preferences or market demands, manufacturers can increase their competitiveness and differentiation.
- **Greater innovation:** By using data-driven approaches to generate new ideas or solutions for existing or emerging problems or opportunities, manufacturers can create new value propositions or business models that enhance their growth potential. (Mohamed, 2018)

Industry 4.0 also poses some challenges for manufacturers and other stakeholders in the value chain. Some of these challenges are:

- **Technical complexity:** By integrating multiple technologies from different domains and vendors, manufacturers need to ensure compatibility, reliability, security, and interoperability of their systems. They need different experts to work together to design them and their parts. If the experts do not understand each other well, they might miss or ignore some risks that could harm the system or its users in the early stages of engineering. This could make the product more expensive and less safe. Often Model-based systems engineering (MBSE) is used by using models to help the experts communicate better. But MBSE does not fully deal with the risks. Specifically, it does not consider how they affect each other. (Japs, Anacker and Dumitrescu, 2021).
- **Organisational change:** By adopting new ways of working and collaborating that require new skills, roles, and cultures, manufacturers need to manage the change process and ensure alignment and engagement of their employees and partners.

- **Ethical implications:** By using technologies that may affect human dignity, privacy, autonomy, or accountability, manufacturers need to consider the ethical and social impacts of their actions and ensure compliance with laws and norms.(Mohamed, 2018)

5.2 Cybersecurity in the Age of Industry 4.0

Most experts (75%) think cybersecurity is a priority, but very few (16%) say their company is ready for it. The main reasons for this are due to the absence of clear standards and guidelines as well as the shortage of technical and managerial skills to apply them (Lezzi, Lazoi and Corallo, 2018). This however is currently being addressed by CAs (Competent Authorities) worldwide in the UK it is by the EC&I (Electrical Control & Instrumentation) division of the HSE (Health and Safety Executive).

A report by Accenture (2019) and the Ponemon Institute states that the average cost of cyber-crime globally reached \$11.7 million per organisation in 2017. Cyber threats have evolved from targeting computers, networks, smartphones, and power grids to the manufacturing sector due to a lack of investment in cybersecurity.

According to a paper looking at the commercial costs, Cyber-attacks cost the U.S. manufacturing sector about \$240 billion and 42,220 jobs from 2002 to 2012. The industry is very vulnerable to hacking, only second to healthcare. This is mainly because of the readily connectivity of machines that use IIoT and the systems that control them remotely through the cloud. (Japs and Anacker, 2021)

5.3 Cyber threat from Industry 4.0

A cybersecurity research team showed how to hack an industrial robot from ABB in a report by Trend Micro in which they did four attacks. In the first one, they made the robot move wrong by changing its control system affecting product quality. In the second one, they altered the robot's calibration, making it less accurate. In the third one, they changed the robot's program, again leading to defects. In the fourth one, they lied about the robot's status. This could have led to an operator being injured or killed.(Maggi *et al.*, 2017) (Wu *et al.*, 2018).

With this example in mind, it is clear to foresee the possibilities of process safety related incidents being caused leading to major loss of life from a MAH (Major Accident Hazard) incident or the potential damage to a country's essential services infrastructure such as fuel supply or LES (Loss of Essential Service). Recommended good practise is identified by OG86 as a benchmark,(Health & Safety Executive (HSE), 2016) See illustration below:

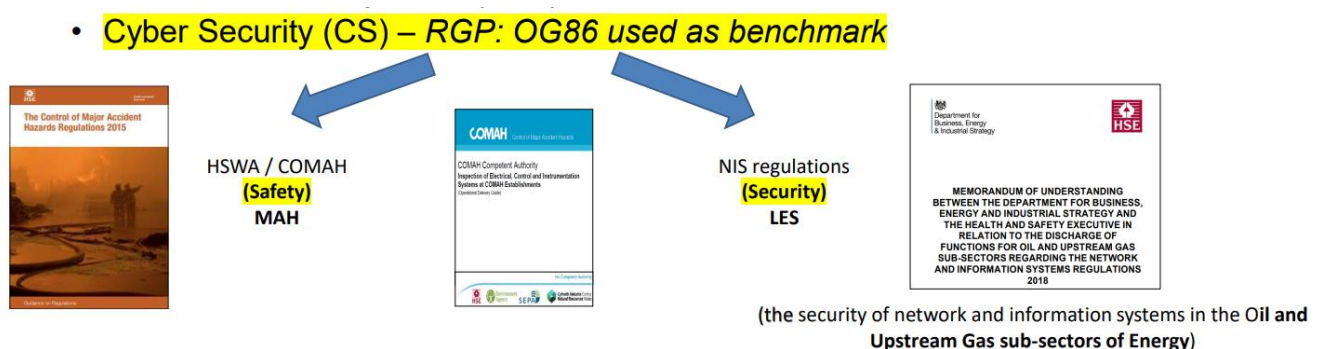


Figure 1: The role of Cyber Security best practice for COMAH and NIS regulations.

6- Process Safety

6.1 An introduction to Process Safety

Process safety is the discipline of engineering that focuses on preventing and mitigating the consequences of catastrophic events involving hazardous materials or energy sources. Process Safety aims to ensure the integrity and reliability of industrial processes and systems that handle, store, transport, or use flammable, explosive, toxic, or reactive substances. Process safety covers a wide range of industries, such as chemical, oil and gas, nuclear, pharmaceutical, and mining. Process safety is essential for protecting workers, the environment, the public, and the assets from potential harm or loss. (Skelton, 1997)

Process Safety Management (PSM) entails the application of a set of management principles and procedures to identify, comprehend, and control process hazards with the objective of safeguarding employees, corporate assets, and the environment. PSM primarily focuses on averting, preparing for, mitigating, responding to, and restoring from catastrophic releases of chemicals or energy associated with a facility's processes. Within the realm of PSM, a process encompasses any activity involving the storage, use, production, handling, or on-site movement of extremely hazardous chemicals or a combination of these activities.

As industries increasingly rely on software and computing systems for task automation, these technological advancements play a pivotal role in process safety. Computer control systems offer substantial advantages by enabling the automation of complex operations and performing intricate calculations. The reliability of computing systems arises from the efficiency of a couple of critical components carrying out a multitude of actions. Moreover, their flexibility allows for modifications tailored to specific applications. From a safety standpoint, automation minimises risks to the workforce by distancing them from the hazards, particularly in facilities engaged in processing hazardous chemicals. (Hardy, 2014).

6.2 Process Safety Gone Wrong

An example of where Process Safety can go wrong, and the catastrophic effects of such incidents cannot be better illustrated than by the Buncefield incident.

The Buncefield fuel depot fire, which occurred in December 2005, was the UK's biggest peacetime blaze. The Hertfordshire Oil Storage Terminal, also known as Buncefield, handled approximately 2.37 million metric tonnes of oil products each year, including petrol, diesel, and aviation fuel. The depot, located outside the town of Hemel Hempstead, about 40 km (25 miles) northwest of London, suffered significant damage during the incident.

Here's an overview of what happened...

In the early hours of Sunday, December 11, 2005, a series of explosions occurred at Buncefield. At least one of these initial explosions was massive in scale. A large fire quickly engulfed a high proportion of the site. Over 40 people were injured, fortunately with no fatalities. The incident caused significant damage to both commercial and residential properties nearby. Emergency services evacuated a large area around the site due to safety concerns.



Figure 2: Buncefield Oil & Gas Fire, Hemel Hempstead.(Lewis, 2015)

The fire burned for several days, destroying most of the site and emitting large clouds of black smoke into the atmosphere. Satellite images show that at one-point, black smoke covered much of southeastern England.

The Health and Safety Executive (HSE) and the Environment Agency (EA) conducted investigations into the incident.

A delivery of unleaded petrol from a pipeline reached a reservoir Tank in bund A around 05:30 on December 11. Unfortunately, the safety systems designed to shut off the petrol supply and prevent overfilling failed. As a result, petrol overflowed from the tank, initially collecting in bund A. The vapour cloud, formed by the mixture of petrol and air, spilled over the bund wall and dispersed westward toward the Maylands Industrial Estate. At 06:01 on Sunday 11 December 2005, the first of a series of explosions took place. The main explosion was massive and appears to have been centred on the Maylands Estate car parks. (Buncefield Major Incident Investigation Board, 2005)



Figure 3: Aftermath of Buncefield Fire (Buncefield Major Incident Investigation Board, 2005)

The CA secured convictions against five companies involved in the operation of Buncefield. These companies were ordered to pay almost £10 million in combined fines and costs.

Costs Associated with Buncefield:

- The explosion and fire at Buncefield was estimated to have cost just under £900 million.
- Businesses outside the site claimed around £500 million in insurance payouts.
- Local authorities claimed £4 million for handling the emergency.
- Public bodies incurred costs of around £7.4 million for emergency response.
- Hertfordshire Fire and Rescue incurred £4 million in costs.
- Hertfordshire County Council spent £2.2 million.
- At least £3 million in emergency costs were reclaimed from central government.

The Buncefield incident remains a significant event in terms of its impact on process safety and highlights the catastrophic consequences of failures of operational technology devices in the field.

6.3 COMAH Regulations

COMAH stands for Control of Major Accident Hazards. It is a set of regulations that aim to prevent and mitigate the effects of major accidents involving dangerous substances, such as explosives, flammable liquids and gases, and toxic chemicals. COMAH came into effect in April 1999 replacing the previous CIMAH (Control of Industrial Major Accident Hazards) regulations and applies to industrial sites that store, use, or produce these substances above certain thresholds. The regulations require operators to take all necessary measures to ensure the safety of workers, the public, and the environment. COMAH also imposes duties on local authorities, emergency services, and regulators to cooperate and coordinate their actions in case of an incident. (Thomas, 2003)

6.3.1 COMAH Management

COMAH management focuses on the following key steps:

- Identify the major hazards and scenarios that could lead to a major accident, such as fire, explosion, toxic release, etc. These are classified as either MAHs (Major Accident Hazards) or MATTEs (Major Accidents To The Environment).
- Assess the likelihood and consequences of each scenario and the risk level for people, environment and assets.
- Implement adequate measures to prevent, control and mitigate the major hazards, such as engineering design, operational procedures, emergency plans, etc.
- Monitor and review the performance of the measures and the compliance with the COMAH regulations and standards.
- Communicate and consult with relevant stakeholders, such as employees, regulators, local authorities, public, etc. on the major hazards and the measures taken to manage them.

These plans are required to be compiled into a Safety Case and submitted to the CA for review and approval. The CA in the UK is the HSE or Office for Nuclear Research (ONR) for nuclear establishments. (Timms, 2004)

6.4 NIS Regulations

The Network & Information Services (NIS) regulations are a set of rules that aim to ensure the security of network and information systems across the European Union. They apply to operators of essential services and digital service providers that offer services within the EU. The NIS regulations require these entities to take appropriate and proportionate measures to manage the risks posed by cyber threats, and to report any incidents that have a significant impact on the continuity of their services. The NIS regulations also establish a cooperation mechanism among EU member states, the European Commission and the EU Agency for Cybersecurity, to exchange information and best practices, and to coordinate responses to cross-border incidents. The NIS regulations are an important part of the EU's strategy to enhance its resilience and competitiveness in the digital age. (Legislation.gov.uk, 2018).

6.4.1 NIS2 Directive

The NIS2 directive is a proposal by the European Commission to revise and update the existing Network and Information Systems (NIS) directive, which aims to enhance the cybersecurity of critical infrastructure and essential services in the EU. The NIS2 directive introduces new requirements and obligations for operators of essential services (OES) and digital service providers (DSPs), as well as for member states and the EU institutions. The main objectives of the NIS2 directive are to increase the level of cyber resilience, to foster information sharing and cooperation, and to harmonize the rules and sanctions across the EU. (Molina, 2023)

Timeline of the NIS2 Directive:

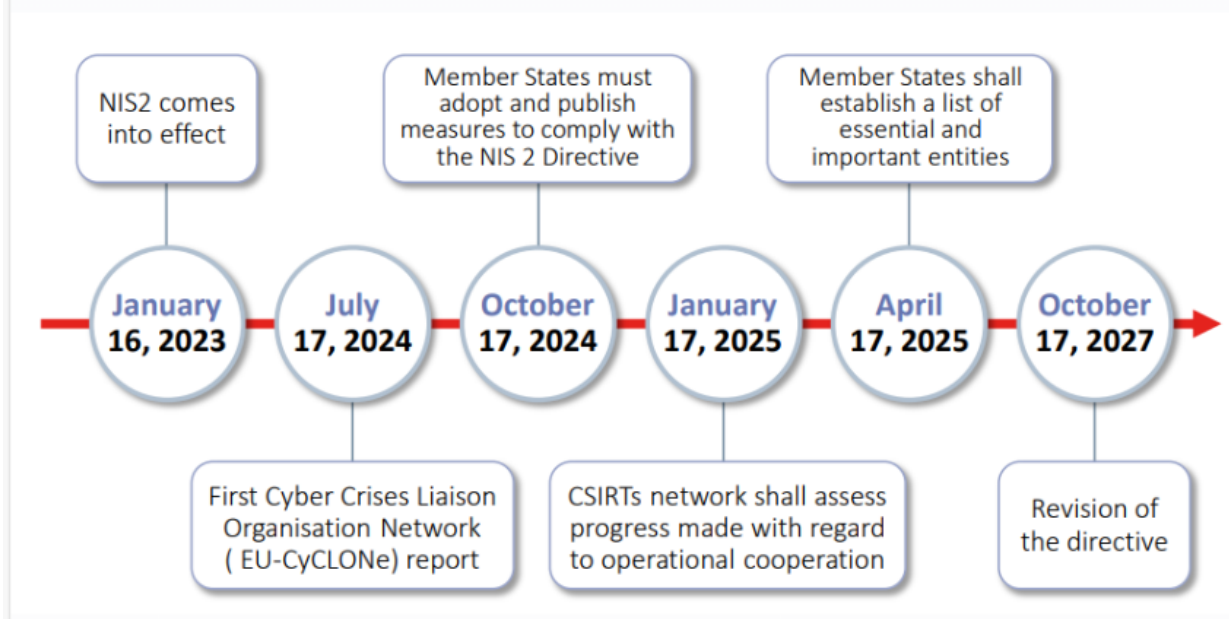


Figure 4: NIS2 Directive implementation Timeline (Molina, 2023)

6.5 Cyber Security threat on IACS

Cyber security is the practice of protecting computer systems, networks, and data from unauthorised access, manipulation, or damage. Industrial automated control systems (IACS) are systems that monitor and control industrial processes, such as manufacturing, power generation, water treatment, and transportation. IACS are often connected to the internet or other networks for remote monitoring and control, data analysis, and optimisation. However, this also exposes them to cyber threats, such as malware, ransomware, denial-of-service attacks, and espionage. Cyber-attacks on IACS are a credible threat and can have serious consequences for the safety, reliability, and efficiency of industrial operations, as well as the environment and human lives. (Monteiro, 2019)

The image below represents the threat of cyber-attack within the context of industrial systems:

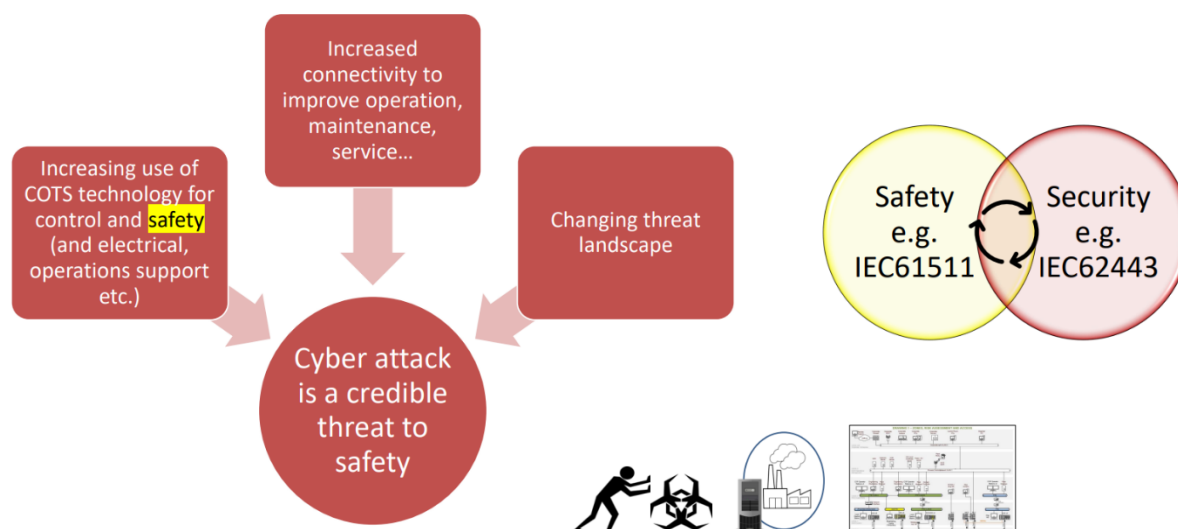


Figure 5: Increased use of COTS and increased connectivity leading to a Credible Threat to Safety (Butcher, 2019)

There is an increased use of Commercial Off-The-Shelf (COTS) being widely adopted for control, safety, electrical systems, and operations support. While this enhances efficiency, it also introduces potential vulnerabilities. Improved connectivity enables better operation, maintenance, and service but also raises concerns about cybersecurity risks. The evolving threat landscape includes sophisticated cyber-attacks as threat actors become increasingly complex in their attack methods. These attacks can directly impact safety in industrial environments. The need to address the area where the standard controlling Process functional safety (IEC61511) and IAC cyber-security standard (IEC62443) is crucial for mitigating these risks. (Butcher, 2019)

6.6 Understanding IACS

Industrial automated control systems (IACS) are computer devices that can run industrial processes automatically, without human intervention. They are widely used in industries like oil refining, chemical processing, and power generation, where raw materials are transformed into finished products through a series of steps. IACS devices allow engineers to observe and control the different parameters of an industrial process, such as temperature, pressure, and flow, from a remote location.

A special type of IACS is a safety instrumented system (SIS), which is designed to protect people, plants, and the environment from hazardous situations. An SIS does not control the process itself, but rather intervenes when the process goes out of control and poses a risk of harm. An SIS comprises of 3 components: a sensor, a logic solver, and a final control element. The sensor collects data from the process and detects if there is an emergency. The logic solver is a controller that executes pre-programmed actions based on the sensor data. The final control element is a switch or a valve that performs the actions decided by the logic solver.

For example, imagine a SIS that detects a high risk of explosion due to a pressure rise in a tank. This could be caused by a failure of the basic process control system (BPCS). The SIS sensor would see the high pressure and inform the logic solver. The logic solver would then send a signal to the final control element, which would open a valve to release the excess pressure and stop the process. This way, the SIS acts as a “last line of defence” and prevents a disaster. (Stoler, 2018).

7- IT Cyber Security Vs OT Cyber Risk

7.1 IT Previous Ignorance of OT

A network system can be divided into two parts: the Information Technology (IT) system and the Operational Technology (OT) system. The IT system contains hardware, software, and peripheral equipment dedicated to the storage, retrieval, and transmission of information or data. In contrast, the OT system is responsible for directly monitoring and controlling industrial devices, processes, and events. It is evident that cybersecurity considerations for the process safety and essential services sectors must extend to both the IT and OT segments of the network architecture but until now OT has been seen as an area for engineering to manage and maintain with little support provided by IT management. This leaves an installation's OT vulnerable to attack. See Image in Figure 6 below:

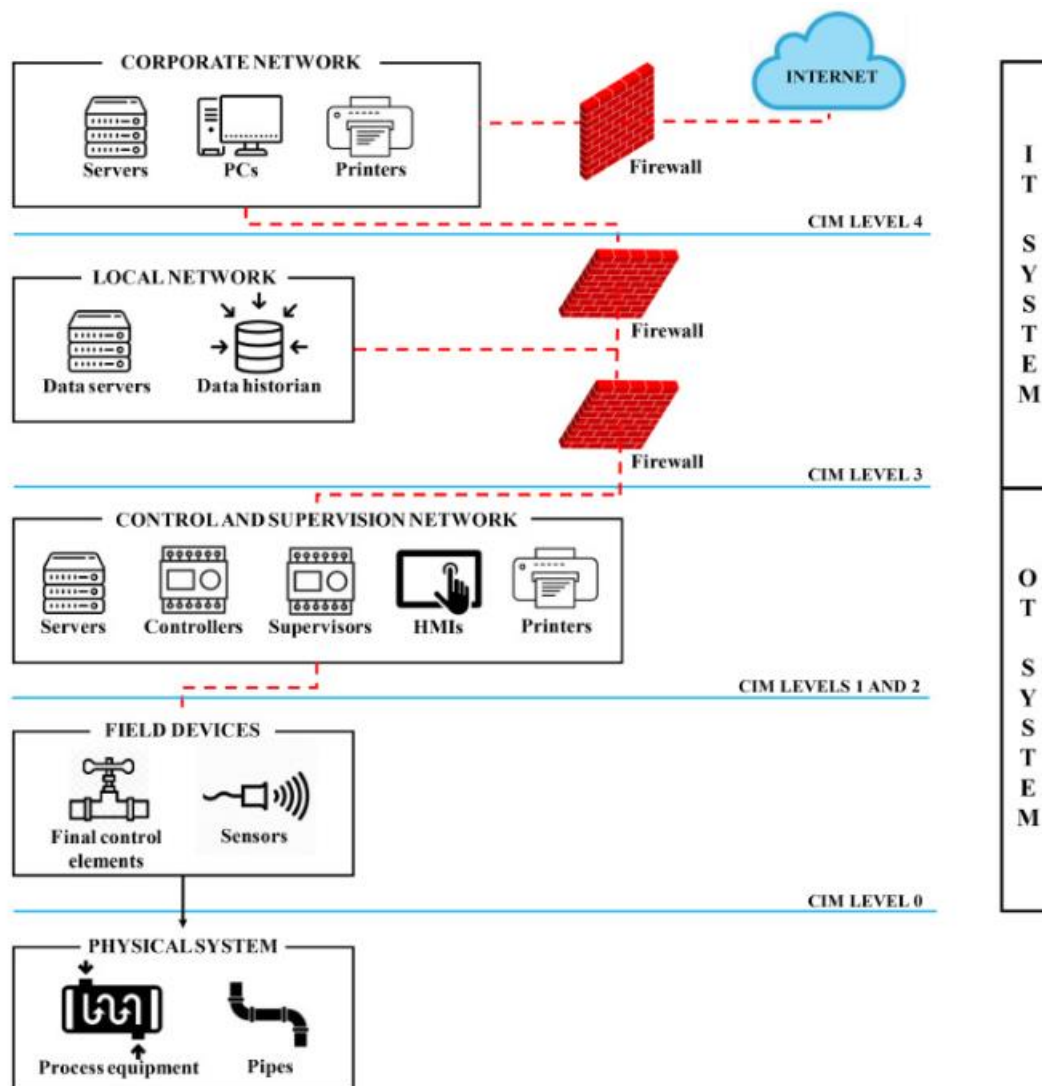


Figure 6: Example of the IT system and the OT system (IAIANI et al., 2021)

Of particular concern are fixed installations involved in the manufacturing and storage of chemical and petroleum products, such as Seveso sites in the EU. These installations pose a primary risk due to the existence of substantial quantities of hazardous substances and challenging process conditions. Importantly, malevolent actors may exploit these inherently hazardous conditions to instigate events with high severity for the population, the environment, and the affected business itself, resulting in asset and brand damage. Obviously, beyond motivations, the origin of the threat and the capabilities of the attacker significantly influence the potential impact across various dimensions. (IAIANI et al., 2021).

7.2 Connected Devices Search Engines – Invites to Hack?

It’s hard to imagine but there exist search engines for vulnerabilities like open ports that are available on the internet. An example of one of these search engines is Shodan.io. Shodan scours the internet for devices connected to the internet. It provides information on a device’s software, services, and vulnerabilities. Types of indexed devices can vary from anything between a small desktop to a nuclear power station and anything in between. (Zolotykh, 2021)

As an example, a quick search using Shodan just looking at power plants reveals 59 devices that are linked to the keywords and are available to be further interrogated. Shodan shows the country the device is in, the ports open for access, the software and version it is running and provides a full list of the vulnerabilities that exist for the device:

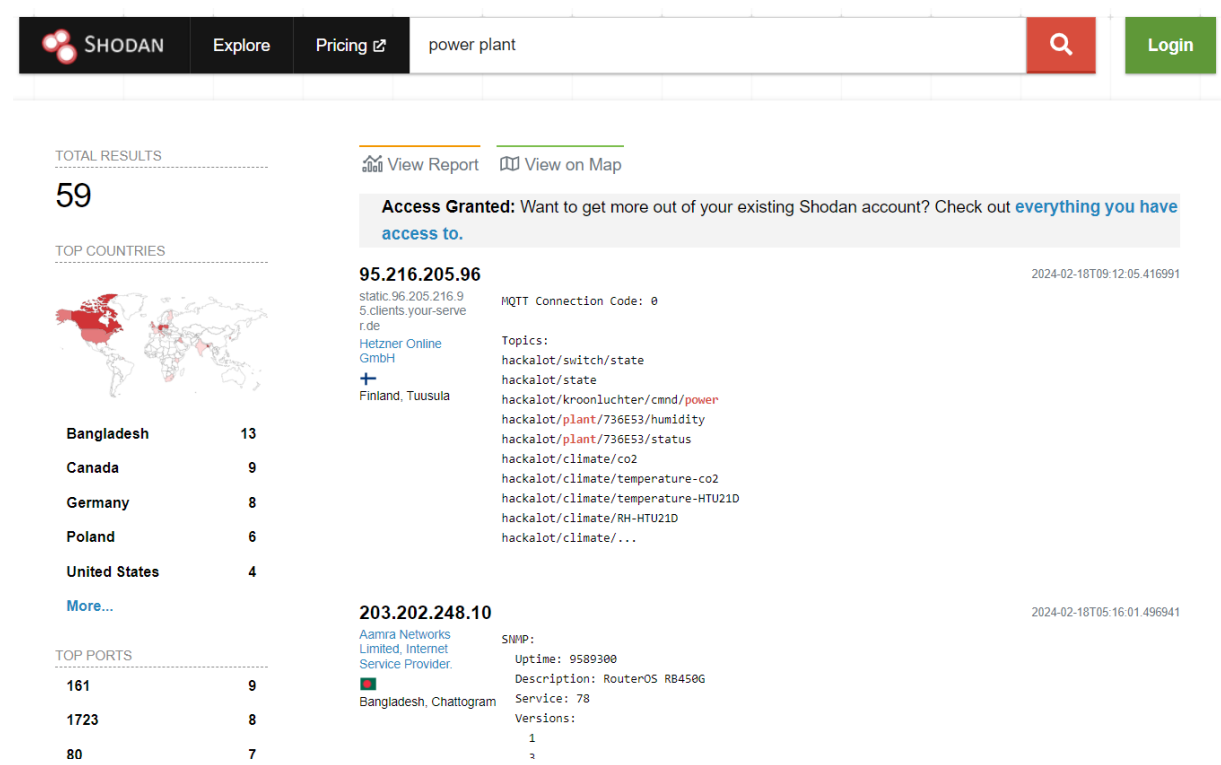


Figure 7: Drilldown to an OT device in Philadelphia listing potential vulnerabilities.

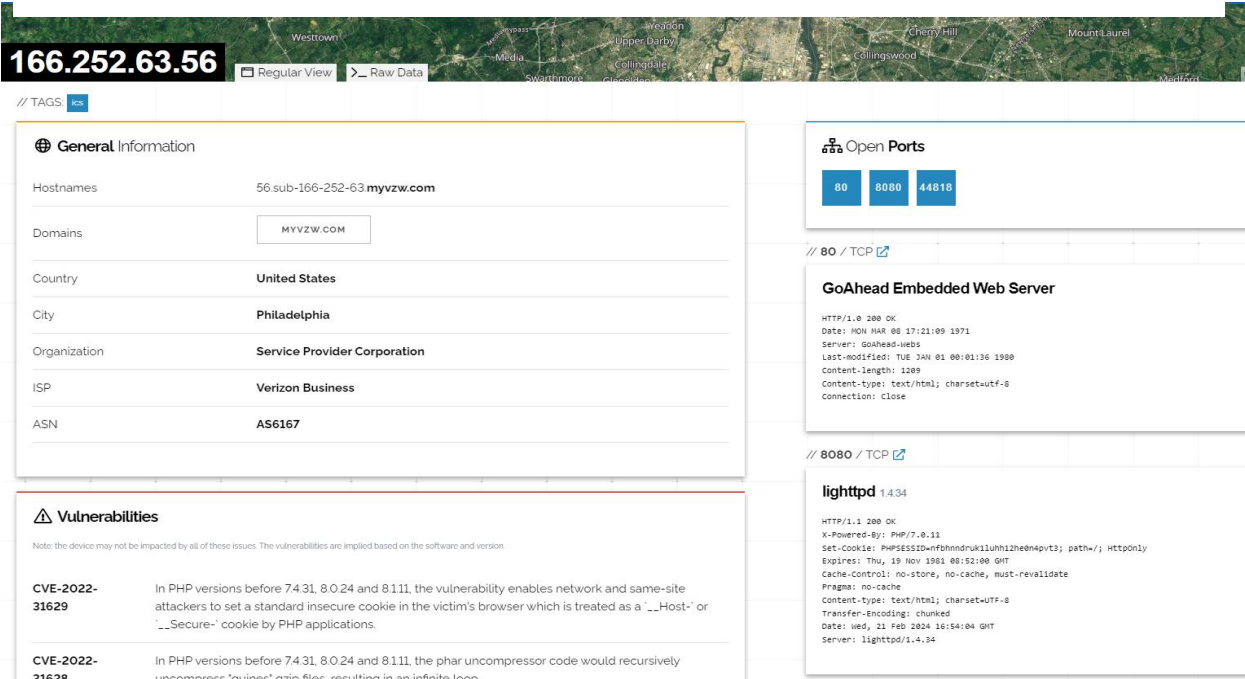


Figure 8: Shodan.io showing freely available information that can be used for exploitation.

The image in Figures 7 & 8 above shows a randomly selected OT device in Philadelphia, USA, for illustration. Shodan provides the open ports on the device and the known vulnerabilities associated with the versions of software available.

While Shodan can provide valuable insights for legitimate purposes, it can also be misused by malicious actors. Here are some of those considerations:

Attack Surface Discovery: Shodan allows hackers to discover exposed devices, services, and vulnerabilities. Armed with this information, they can target specific systems for attacks.

Exploitation: By identifying vulnerable services (e.g., outdated software versions), hackers can exploit known security flaws. For example, if a device is running an unpatched version of a web server, attackers might use known exploits to compromise it.

Botnet Recruitment: Shodan helps attackers find Internet of Things (IoT) devices with weak security. These devices can be recruited into botnets for distributed denial-of-service (DDoS) attacks or other malicious activities. A botnet is a network of private computers that hackers have infected with malicious software. These hackers then control these computers remotely, often without the knowledge of their owners.

Sensitive Data Exposure: Shodan reveals banners containing metadata about services. If a service is misconfigured, sensitive information (such as default credentials or private data) may be exposed.

Market Research for Attacks: Hackers can use Shodan to identify lucrative targets. For instance, they might search for specific industrial automated control systems (IACS) or critical infrastructure components.

Ransomware Targeting: Shodan assists in tracking vulnerable systems. Attackers can use this data to identify potential victims for ransomware attacks.

Privacy Concerns: Shodan's data collection raises privacy issues. Devices that unintentionally expose sensitive information become vulnerable.

The responsible use of tools like Shodan is obviously crucial. Ethical hackers, security professionals, and researchers leverage it for legitimate purposes, but malicious actors can exploit the same information for nefarious deeds. Vigilance and proper security practices are essential to protect against these potential threats. (Rae, Chowdhury and Jochen, 2019)

7.3 Anatomy of a Cyber Attack

Cyber-attacks encompass a broader spectrum than the traditionally defined information operations. Information operations are actions that attempt to influence, corrupt, disrupt or usurp the information and decision making of adversaries while defending one's own information.

According to the USNM (United States National Museum) strategy for cyberspace operations, it outlines that computer network operations should also detection of utilisation enabling acts. Unlike network attacks and defence, utilisation enabling operations focus more on collecting and analysing information than disrupting networks. Importantly, these operations may serve as a precursor to an attack. Such operations can extend to disseminating information and propaganda for specific purposes. Additionally, computer network exploitation enabling operations may aim to steal crucial computer data. In this context, tools like Trap Sniffers and Trap Doors prove valuable for cyber espionage. Trap Doors allow external users to access software without the computer user's knowledge, while Sniffers serve as tools for stealing usernames and passwords. (Li and Liu, 2021).

In the context of malware cyber-attacks, perpetrators aim to infect targeted systems with malicious code. These deliverables play a crucial role in the outcome of an attack that may serve various purposes:

Information Gathering: The deliverable might seek to extract information from the intended target system.

Backdoor Creation: It could establish a backdoor within the compromised system, which can be exploited later for different objectives.

Forcing Execution: The deliverable may force the system to execute malicious code or instructions, potentially modifying or deleting data and other programs.

For internal penetrations (where outbound capabilities are involved), the most common deliverables include viruses, worms, and executable scripts. (Janczewski and Colarik, 2008)

The anatomy of a cyber-attack is made up of these key steps and illustrated in Figure 9 below:

1. **Reconnaissance:** Before launching an attack, cybercriminals identify and select their target. They gather information about the target's vulnerabilities, such as outdated software, unpatched systems, and potential entry points. Reconnaissance can be passive (e.g., browsing a company's website or public records) or active (e.g., pinging the system or port scanning).
2. **Weaponisation:** After gathering sufficient data, attackers create a malicious payload designed to exploit the identified vulnerabilities. This payload could take the form of a virus, worm, or other malware.
3. **Delivery:** The weaponised payload must be delivered to the victim. Common delivery methods include phishing emails, malicious downloads, or infected websites. In some cases, attackers exploit trusted relationships by sending malicious files from compromised accounts to lure victims into executing the payload.
4. **Exploitation:** Once delivered, the malware exploits the identified vulnerability (software, hardware, or human). This is where the actual attack begins as the malware activates and carries out its intended function.
5. **Installation:** After successfully exploiting a vulnerability, many types of malwares attempt to establish a more permanent foothold on the victim's system. This could involve creating backdoors, modifying system settings, or installing additional malicious software.
6. **Command and Control:** With the malware installed, the compromised system often connects back to a command-and-control server operated by the attackers. This server can issue commands to the malware, receive stolen data, or further direct the attack.
7. **Actions on Objectives:** Having gained access and control, attackers can now achieve their end goal. This might involve data exfiltration, destruction of critical data, or using the compromised system as a launching pad for attacks on other targets.

Each stage of an attack presents an opportunity for detection and defence. By understanding this anatomy of a cyber-attack, organisations can better prepare to mitigate risks and respond effectively when incidents occur. (Makhdoom *et al.*, 2019)

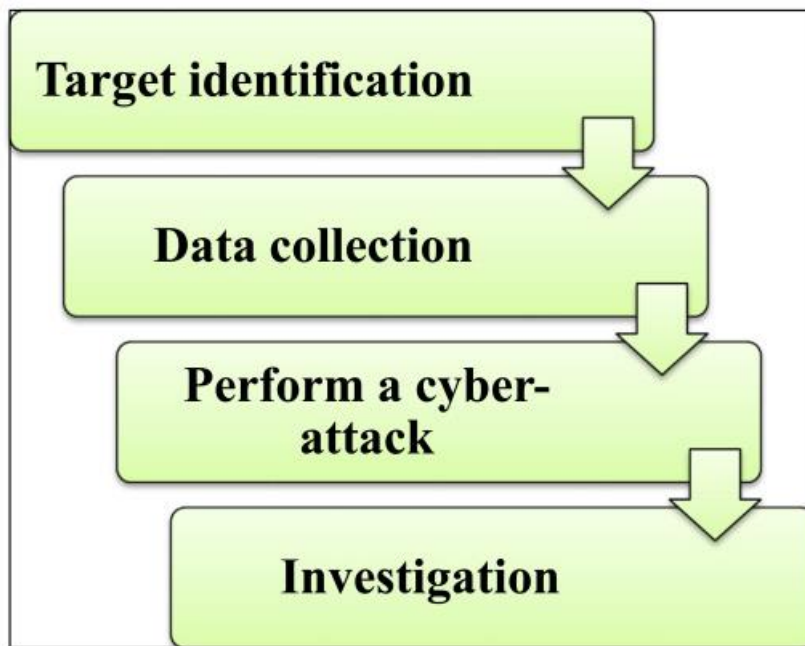


Figure 9: Anatomy of cyber-attack (Li & Liu, 2021).

8- Triton Cyber Attack Case Study

In 2017, a cyberattack targeted a petrochemical plant in Saudi Arabia. The attackers exploited a previously unknown vulnerability in a Schneider Electric SE product. The attackers got into the Safety Instrumented System (SIS) and uploaded malware to it. In order to achieve this the attackers worked out how to get through the cybersecurity zones to gain access to a temporary engineering laptop and waited over a period of months to be able to upload their payload to the SIS OT. (Gibbs, 2017).

See illustration below:

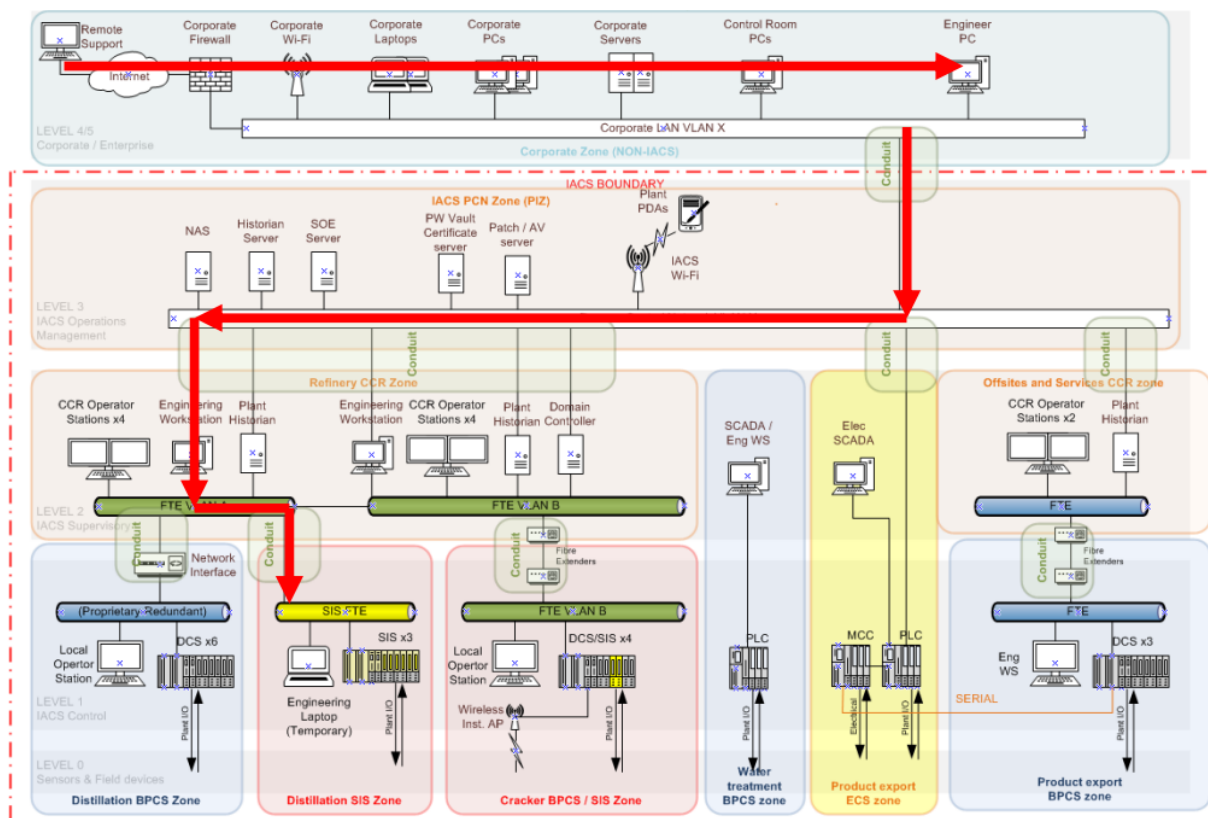


Figure 10: Illustration of Triton Attack Route overcoming the Cybersecurity Zones (Stoler, 2018)

Their goal was to gain control over the safety shut-off system, which is crucial for preventing catastrophic events. The malicious software, known as Triton, raised concerns about the security of critical infrastructure. Experts suspect that a nation-state orchestrated the attack, possibly with a political agenda. This incident highlights the growing threat to industrial cybersecurity and the need for robust defences against such attacks.

8.1 Motivations and Drivers for the Attack

The Triton malware attack had several motivations and drivers. The invaders primary motivation was likely to cause disruption and physical damage. By compromising the safety system, they could trigger false alarms, shut down critical processes, or even cause equipment failures.

By targeting safety systems, it provided a strategic advantage. If successful, it could disrupt production, impact supply chains, and harm the reputation of the target. Notably, they targeted a specific production plant and specific systems.

Lastly, the involvement of a nation-state suggests that the attack may have broader geopolitical implications. It could be part of a larger cyberwarfare strategy, a pre-cursor for a further military operation or an attempt to weaken the rival nation's critical infrastructure.

8.1.1 Targeted Safety Systems

The Triton malware attack specifically aimed at infiltrating and reprogramming the automated safety systems of a petrochemical plant. Safety systems within industrial facilities play a pivotal role in preventing accidents, mitigating risks, and safeguarding human lives. These systems are designed to automatically respond to abnormal conditions, shut down processes, or trigger emergency protocols when necessary.

In the context of the Triton attack, the targeted safety system was specifically responsible for ensuring the safe operation of critical equipment within the petrochemical plant. This included shutting down processes in case of leaks, fires, or other hazardous situations. (Newswire, 2018).

8.1.2 The Attack Vector

The attackers exploited a vulnerability in the safety system's software. It appears the invaders were attempting to install a Remote Access Trojan (RAT). These RATs are designed to give an attacker complete control over the target system. Traditionally IACS networking is designed to ensure segregation between infrastructure and control, however in this case there had been a trend in integrating both the BPCS and the SIS on the same network. Therefore, gaining access to the basic process control system network via a PC on the network also allowed SIS access.

This design can obviously be dangerous where joined with remote engineering access. A usual practice on many establishments is to permit engineering access to the BPCS network via remote desktop protocols (RDPs). Once these RDPs were compromised the attacker had access to both process control and safety network and uploaded the first stage malware, an executable named 'Triton.exe' to the engineering laptop.

The Triton executable accessed a protocol utilised by engineering laptops to normally download updates to the SIS device. They reverse engineered the protocol to instead download new malicious code to the SIS device. With this code installed however they still had two problems to overcome.

1. The SIS controller was protected by a physical switch, see below:



Figure 11: SIS Controller Remote Access Switch (McMillan, 2018)

2. The malicious code downloaded to the SIS device was not persistent. When an engineer initiated a 'download all' command. The malicious code was overwritten by correct historical code effectively deleting the attackers code and thwarting the attack.

To defeat these problems, the invaders designed a second stage malware. This malware written inside the SIS device was created to write itself into the firmware memory instead of the usual user memory. They did this by utilising a bug in the original SIS software which they knew about that gave their code a higher level of security access as a supervisor malware.

Once in the firmware the malware code registered itself to be called by the operating system whenever a certain network command was received. The malware code was therefore called before the normal code thereby side stepping the key switch and enabling malicious code insertion whatever the key switch position.

The invaders now had a RAT ready to be activated that is called before the normal SIS operating system prepared to accept instructions from a PC on the same network.

8.1.3 The Detection of the Attack

With the RAT in place the attackers had the ability to read and write code freely. However, before they were able to take full and potentially catastrophic advantage of it the SIS was shut down following an unrelated controller error entering a fail-safe state.

The asset owner was then prompted to start an investigation into the controller error which ultimately provided detection of the malware thereby stopping the attack in its tracks.

The investigative report states that the invaders were there to impose significant damage and would likely have had they not been stopped. An attacker that was in control of both process control units and safety systems that are designed solely to be the last line of defence from a major incident can only point to that conclusion. (Stoler, 2018).

8.2 Challenges and Implications

8.2.1 Detection Difficulty

Safety systems are often isolated from the regular IT network to prevent unauthorised access. The code is meant to remain unchanged and controlled by strict procedure. For that reason, there would be no normal need to inspect these systems for code changes. Therefore, detecting an attack on these isolated systems would have been challenging.

8.2.2 Response Complexity

Responding to safety system breaches requires specialised knowledge and coordination. Shutting down processes abruptly can have unintended and dangerous consequences even under normal circumstances. Following a system infiltration the extent of abnormal system behaviour would be unknown and simply by following existing shutdown procedures could have triggered an unintentional catastrophic event.

8.2.3 Industry Wake-up Call

The Triton attack served as a wake-up call for industrial organisations to enhance their cybersecurity practices. It underscores the need for robust defences, continuous monitoring, and collaboration between IT and OT teams. It also highlighted the potential risks posed by cyber threats targeting these essential components.

The researchers who analysed the attack speculated that the ultimate goal of the hackers was to combine Triton with another type of malware, such as Stuxnet, which was used to sabotage Iran's nuclear program in 2010. Stuxnet manipulated the industrial-control systems that regulate nuclear centrifuges, causing them to self-destruct. By combining Triton and Stuxnet, the attackers could have disrupted both the normal operation and the emergency response of the plant, resulting in a devastating scenario. (McMillan, 2018).

9- Existing Industrial Risks

Cyber-attack is a known risk to Major Hazard industries. Since the Triton attack many more examples exist of attacks carried out on safety instrumented systems (SIS), basic process control systems (BPCS) and electrical power control systems and other associated Industrial Automated Control Systems (collectively called IACS).

9.1 Threat Landscape in Industry 4.0

The assessment of external threats faced by the process safety sector encompasses numerous motivations that range across the spectrum. It is essential to consider attackers with these diverse motivations, including disgruntled employees or contractors (motivated by revenge, ego, or curiosity), terrorists (destructive motives driven by revenge, political or monetary advantages), activists (motivated by political gains or rebellion), and criminals (motivated by status, challenge, or financial gain). In the context of the Process and Essential Services industries, attackers may be drawn to specific company profiles, such as multinational corporations or companies holding a principal position in a particular sub-sector, providing opportunities to access exclusive data, among other factors. Additionally, the political views and location of the targeted plant can serve as a motivating factor. (Dhirani, Armstrong and Newe, 2021)

9.2 Assessing Cyber Risks – (safety & security)

In the process world Risk Assessment is a function of likelihood and consequence, this gives a Risk factor, however that is not the case with the cyber security world.

		Consequence				
		Negligible 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Likelihood	5 Almost certain	Moderate 5	High 10	Extreme 15	Extreme 20	Extreme 25
	4 Likely	Moderate 4	High 8	High 12	Extreme 16	Extreme 20
	3 Possible	Low 3	Moderate 6	High 9	High 12	Extreme 15
	2 Unlikely	Low 2	Moderate 4	Moderate 6	High 8	High 10
	1 Rare	Low 1	Low 2	Low 3	Moderate 4	Moderate 5

Figure 12: A usual Risk scoring matrix based on Likelihood & Consequence (Kaya, 2018)

In the cyber security world Risk Assessment is instead a function of:

- Threat
- Vulnerability
- Target Attractiveness
- Attacker Capabilities and Persistence over Time

- Consequences can be variable based on intent, either to hijack, disable or damage the system.

Likelihood is not generally appropriate for cyber risks. There is a lack of historical data, and the changing threat landscape is often driven by unpredictable behaviours and motives of attack. (van Haastrecht *et al.*, 2021).

Below is a comparison between Process Safety and Cyber Risk Assessment which illustrates the difficulty in predicting cyber risk and its impact:

Process Safety Risk Assessment	Cyber Risk Assessment
Can systematically identify hazards and their causes, consequences	Link between cyber threats, vulnerabilities and process safety hazards not clear.
Reasonable to assume no malicious intent. Hazards and their causes can be considered individually	Malicious intent a key feature. Need to consider multiple contingencies (double jeopardy) and common cause failures.
Likelihood based upon predictable failure rates based upon experience etc.	Likelihood not predictable
Risk controls specific to each hazard scenario – can identify and manage robustly.	Often process risk controls part of a ‘system’ – need to protect whole system from cyber risks.
Independent risk controls designed to reduce risk to ALARP v established risk tolerability criteria	Cyber risk controls arranged as ‘defence in depth’. No RTC and can sometimes only slow an attack.
<u>Therefore</u> : Can systematically and with some confidence identify the required risk controls and manage these robustly – e.g. safety systems	<u>Therefore</u> : difficult to predict cyber risk and impact of cyber risk controls on process risk

Figure 13: Process Safety & Cyber Risk Assessment Comparison (Butcher, 2019)

An alternative approach is therefore necessary to assess cyber risk. One such approach is identified in the publication Operational Guidance OG86 by Health & Safety Executive (HSE), (2017) in which they suggest that the likelihood is assumed that it will eventually happen. Instead, the method focuses on splitting the network into zone criticality and providing an assessment of consequence for each of those zones. This then highlights the areas that need a greater level of security and continual monitoring.

Once these Critical zones have been identified, methods for access can be stepped up as

Major accident		Loss of Essential Service	
Relevant Zone	Critical Zone	Relevant Zone	Critical Zone
Control system zone	Safety system zone	Plant Information zone	Control system zone
Plant Information zone		IACS DMZ	Safety system zone
IACS DMZ			

Figure 14: Example of IACS Zone Criticality (Health & Safety Executive (HSE), 2017)

countermeasures such as disabling the ability to remotely access, separate passwords or biometric controls.

9.3 Best Practice Protection from Attack

Most of the cyber-risks can be addressed with generally simple best practice technical and organisational control measures. An organisation should implement the following as a bare minimum to protect against cyber-attack threat.

9.3.1 Network Segmentation:

Isolation of critical devices (such as servers, industrial automated control systems, or sensitive equipment) from the public internet. Use of firewalls and VLANs (Virtual Local Area Networks) to segment the network. The Triton attack case study showed that the attackers would not have had access to the SIS had this been the case. Restricting unnecessary external access also minimises exposure. (Stone, 2021)

9.3.2 Regular Patching and Updates:

Keeping software, firmware, and operating systems up to date. Regularly applying security patches to address known vulnerabilities. Search engines such as Shodan have been shown to often detect outdated software versions, so staying current is crucial.

9.3.3 Change Default Credentials:

Many devices come with default usernames and passwords. These should be changed immediately on installation to unique, strong credentials. Of course, avoiding using common or easily guessable passwords.

9.3.4 Disabling Unnecessary Services:

Any services or protocols that are not essential for your device's functionality should be disabled to further reduce the risk. A threat actor can scan for open ports and services, so minimising exposure reduces risk.

9.3.5 Implement Network Access Controls:

Use of access control lists (ACLs) to restrict inbound and outbound traffic as well as whitelisting only necessary IP addresses or ranges will add a further layer of protection.

9.3.6 Security by Obscurity Is Not Enough:

Historically hiding devices from a network would be a method of protection from malicious intent but relying solely on hiding the devices won't protect them anymore. We must assume that attackers will find them eventually and focus on robust security practices instead.

9.3.7 Monitor and Audit:

Regularly monitoring of the network for unusual activity is crucial. Setting up intrusion detection systems (IDS) or security information and event management (SIEM) tools will provide an early warning in the event of an attack. Regular audit of access logs will help detect unauthorised access attempts.

9.3.8 Consider Using a VPN or Proxy:

If possible, network traffic should be routed through a virtual private network (VPN) or proxy server. This adds further layers of protection since the threat actor will not directly see the device's IP address.

9.3.9 Security Awareness Training:

Education of staff about security risks and best practices is essential to ensure everyone understands the importance of protecting sensitive devices.

9.3.10 Regularly Assess Exposure:

Use of tools like Shodan by an organisation's own IT department to check what information is publicly accessible and address any findings promptly.

Even with all these actions taken it remains that no system is completely immune, however following these steps will significantly reduce the risk. (Hennig, 2018)

9.4 Vulnerabilities in Cyber-Physical Systems

The integration of Cyber-Physical Systems (CPS) within Industry 4.0 brings forth a new frontier of vulnerabilities that demand meticulous attention. The security threats can be divided into three layers, the physical layer, the network layer and the application layer.

1. In the physical layer there are vulnerabilities in physical attacks where an attacker could tamper with sensors, cut cables, or compromise control systems. Environmental hazards such as flood, earthquake or fire can disrupt CPS operations and supply chain attacks could compromise components for manufacture, shipping, or installation.
2. In the network layer vulnerabilities exist in the communication channels, protocols and data exchanges between CPS devices. They can include unauthorised access, eavesdropping and data interception as well as Denial of Service attacks disrupting communication.
3. In the application layer vulnerabilities exist from exploiting weaknesses in code and replacing with malicious code. There are also vulnerabilities from weak access authorisation mechanisms and malicious authorised users (disgruntled employees). (Gao *et al.*, 2013)

9.4.1 Interconnectedness and Interoperability Challenges

The interconnected nature of Cyber-Physical Systems, spanning sensors, actuators, and communication networks, introduces a complex web of dependencies. Ensuring seamless interoperability between diverse components becomes a challenge, as discrepancies in standards and protocols may create vulnerabilities that malicious actors can exploit. The very connectivity that enhances efficiency also opens avenues for potential disruptions.

9.4.2 Inadequate Authentication and Authorisation Mechanisms

Establishing robust authentication and authorisation mechanisms is paramount within Cyber-Physical Systems. Weaknesses in these mechanisms can lead to unauthorised access, manipulation of control systems, and compromise of critical infrastructure. Striking a balance between accessibility for legitimate users and stringent security measures is a delicate yet crucial aspect of securing CPS.

9.4.3 Lack of Standardised Security Protocols

The absence of standardised security protocols across the spectrum of Cyber-Physical Systems poses a considerable challenge. Diverse technologies, each with its own set of protocols, may lack universally accepted security standards. This heterogeneity complicates the task of implementing cohesive security measures, leaving potential vulnerabilities unaddressed and exposing systems to exploitation.

9.4.4 Limited Over-the-Air (OTA) Security Updates

Many Cyber-Physical Systems operate in environments where frequent physical access for updates is impractical. Consequently, ensuring the security of Over-the-Air (OTA) updates becomes a critical concern. Inadequate encryption or authentication mechanisms in the update process can be exploited by threat actors, potentially leading to the compromise of CPS functionality.

9.4.5 Real-Time Operating System (RTOS) Vulnerabilities

The deployment of Real-Time Operating Systems (RTOS) in Cyber-Physical Systems introduces a unique set of vulnerabilities. The need for predictable and rapid response times in RTOS can sometimes come at the expense of robust security features. Vulnerabilities in RTOS can be exploited to manipulate system behaviour in ways that compromise both safety and security. (Serino and Cheng, 2020)

9.4.6 Physical Attacks on Cyber-Physical Systems

Beyond digital vulnerabilities, Cyber-Physical Systems are susceptible to physical attacks. Tampering with sensors, manipulating actuators, or gaining unauthorised physical access to components can have cascading effects on the entire system. Securing CPS necessitates a comprehensive approach that considers both digital and physical dimensions.

9.4.7 COVID Implications

In an article in CPO magazine written by Breth and Douglas, (2020) they examine how cyber threat actors took advantage of the turmoil COVID brought to governments worldwide. By using phishing emails and malware under the guise of government advice around pandemic response they were able to infiltrate an extensive and yet unquantified myriad of attacks.

Many of the malware planted on systems is likely to still be lurking undetected since hackers will leave these backdoors to systems for years to come. Couple this with the languid pace of upgrading computer systems in the world's government services domain and it is likely that many of these systems are already compromised waiting for a command when all pieces for an effective attack are in place and the disruption can be maximised.

They observe that worldwide governments emergency planning is generally focussed on natural disasters, acts of terror and disease outbreak. When a major disaster is encountered a government will have risk mitigation planned and set up to minimise the effects and protect its citizens, however the execution of these plans is more often through the use of outdated computer systems with little or outdated security protocols that can be easily overcome by a persistent and knowledgeable threat actor.

They argue that governments play down the risk posed by cyber threat on critical infrastructure and suggest that governments become far more transparent in reporting and sharing information on cyber-attacks that have been discovered and/or thwarted so that the cyber security worldwide community as a whole can benefit from the lessons learned.

10- Recommendations

10.1 Strategies for Mitigating Cyber Risks

The use of the ever-evolving technologies of Industry 4.0 is key to effective operation and maintenance. Avoidance of these technologies is just simply not an option, however their implementation into the workplace for organisations that have major accident hazard or loss of essential service potential needs to be carefully controlled with proactive and comprehensive mitigation strategies. Currently organisations are using retrofitted security methods (between the assets) to manage their cyber security risk. (Knowles *et al.*, 2015)

Future methods that will need to be employed are secure by design (within the assets), which focus on security of critical functions. Effectively addressing the complex and evolving cybersecurity challenges in the realm of Industry 4.0 demands a strategic and comprehensive approach. This section delineates key cybersecurity strategies that organisations can employ to fortify their defences and foster a resilient environment in the face of dynamic cyber threats.

10.1.1 Risk Assessment and Threat Modelling

As with any other management of hazards, the foundation of effective cybersecurity lies in a thorough understanding of those potential risks and threats. By conducting comprehensive risk assessments and employing threat modelling techniques, organisations can identify vulnerabilities and prioritise their mitigation efforts. This essential proactive approach enables targeted security measures and resource allocation based on the specific, identified threat landscape.

10.1.2 Defence in Depth Approach

A robust defence strategy involves deploying multiple layers of security mechanisms, a concept known as defence in depth. Organisations should implement a diverse array of measures, including firewalls, intrusion detection systems, encryption protocols, and access controls. This layered approach minimises the impact of potential breaches and fortifies the overall security posture.

A method employed by the COMAH industries along these lines is by using LOPA (Layers Of Protection Analysis). LOPA follows a Risk Assessment technique known as a HAZOP (Hazard and Operability Study) by identifying likely hazard scenarios and indicating if the risk is 'credible'. However, the risks identified by the HAZOP tend to be qualitative, identifying if mitigating safeguards exist or need to be implemented. LOPA allows a review team to quantify the effectiveness of existing safeguards and determine if the risk-gap that remains is either 'Tolerable', 'ALARP' (As Low As Reasonably Practicable) or 'Intolerable'. If intolerable levels of protection are calculated, then further layers of protection are required to reduce the risk-gap further (Willey, 2014)

As a spin on this established method in the Process Safety industry an article by Tantawy, Abdelwahed and Erradi (2022) published by IEEE (Institute of Electrical and Electronic Engineers) suggests adapting this approach to the world of cyber-risk management which they termed as CLOPA (Cyber Layers Of Protection Analysis). This seems like an excellent approach to not only identify necessary cyber security measures but also quantifying their effectiveness by using an established and effective existing methodology. The approach provides far greater confidence that the protective measures in place prevent or mitigate the hazard as expected. It also seems obvious that adapting the existing measures that exist to protect against these catastrophic events from MAHs, MATTEs or LES should be the best approach rather than inventing new untested methods.

10.1.3 Continuous Monitoring and Anomaly Detection

With a threat environment that is ever-evolving, continuous monitoring is imperative. Organisations should implement advanced anomaly detection systems that provide real-time insights into the network and system activities. Rapid identification of deviations from normal behaviour enables swift response and mitigation, reducing the potential impact of cyber incidents. One method of this is Sample Mode-switching where the system switches from normal mode to secure mode to isolate the compromised components and maintain the production or switch to emergency mode to restore a power supply the system uses different criteria and mechanisms to trigger and execute the mode-switching, depending on the context and the requirements. (Riegler and Sametinger, 2021).

10.1.4 Secure-by-Design Principles

Integrating security considerations from the design stage is essential for Industry 4.0 systems in Process Safety systems. By adhering to secure-by-design principles, organisations can proactively address potential vulnerabilities before implementation.

As with an approach to make a building weather resistant a builder will place tiles so that the upper tiles overlap the lower tiles and flashing is placed over windows and doors, this is following one known principle, that water will flow downwards and will run off in a waterfall fashion. In a similar vein, understanding fundamental principles of a cyber-attack puts you in a good position to implement practises that work in your favour to ward off an attack. The principles to understand during defence design are:

1. Principle of Least Privilege

The Principle of Least Privilege is a fundamental concept in secure design. It emphasises that individuals should be granted only the minimum level of access required to perform their specific tasks. For example, consider a system that stores sensitive customer financial data. In this scenario:

- An administrator perhaps doesn't require access to very sensitive information.
- But, an account manager likely would need that access.

It is important to ensure that the account manager only has access to data from accounts they manage. By adhering to this principle, you minimise the risk of unauthorised access. If an attacker gains account access, their ability to access critical information is limited, thus reducing potential damage. (Boersma, 2019)

2. Principle of Separation of Duties

This principle builds upon the previous principle. While the latter focuses on granting individuals only the necessary privileges for their specific tasks, the former emphasises that a solitary person shouldn't wield excessive authority.

Separation of Duties shifts the focus from privilege to job scope. It aims to prevent roles from becoming too extensive. When someone's responsibilities are overly broad, they may require numerous permissions, potentially compromising security.

It wouldn't be prudent for the salesperson (those who make sales) to also approve discounts. Such a situation could lead to biased decisions, where the salesperson discounts software to improve their sales figures. Instead, a separate role (such as a manager) should handle discount approvals to maintain checks and balances.

By adhering to the Principle of Separation of Duties, organisations reduce the risk of poor decisions and maintain a more secure environment.

3. Principle of Failing Securely

The Principle of Failing Securely acknowledges that failures are inevitable. To illustrate this concept, consider an electronic lock mechanism. Imagine a security card is needed to access sensitive areas. By applying the Principle of Least Privilege, the aforementioned security card will grant access to only the specific areas necessary for your job. But what if the power is unexpectedly lost?

If the system were to fail open, all locks would cease functioning. Suddenly, the system provides access to every door in the building. For those with malicious intent, this is an opportune moment.

In contrast, a system that adheres to Failing Securely ensures that all doors remain locked during such an event. Rather than granting access to all doors, you have no access to any of them.

This principle extends to software design as well. The design for the system to Fail Securely would grant access to specific parts of the system when each step of the process successfully completes.

4. Principle of Open Design

This Principle emphasises that the security of your system should not depend solely on the secrecy of its implementation. This principle holds particular significance for security models such as cryptography. Cryptographic systems that are well-designed are made public, allowing them to undergo rigorous scrutiny by experts worldwide before being put into practical use.

The same philosophy applies to any software system. Consider a scenario where a system fails to adhere to secure practices (like not failing securely). Such a system may depend on the assumption that “no one would ever discover its vulnerabilities.” Although it may be unlikely for an attacker to deduce a bug granting system access, it isn’t impossible. Moreover, if an adversary had access to the source code, weaknesses can quickly be identified. Instead, prioritising secure design principles ensures the system’s safety, regardless of whether a malicious actor acquires access to the code.

5. Principle of Avoiding Security by Obscurity

Security by Obscurity shares similarities with the Principle of Open Design. Consider a scenario where software includes a fixed undisclosed username and password. Upon authorisation, the account gains complete access to all other accounts within the system. This setup’s security hinges on keeping the access details for this account confidential. However, eventually, an increasing quantity of people will obtain access to this privileged account. A few employees may depart the business but may not forget the access details. The application security at that point will rely on those former employee’s goodwill.

While it can be said that most security involves secrets (as in passwords, etc.), a more robust design avoids the existence of an account with full access altogether. If such an account is necessary, avoid hard coding the credentials. Instead, treat it as a regular account. When an employee with access to this account departs, promptly change the password. This approach ensures better security, even if the code is accessed by malicious actors.

6. Principle of Minimising Attack Surface Area

The Principle of Minimising Attack Surface Area focuses on enhancing security by reducing the exposed components of an application. For example, Data centres generally lack numerous windows. Although this design choice partly benefits cooling, it also stems from the fact that windows are vulnerable (as in they can be broken easily). Even if the doorways have best locks available, they won’t be effective if an intruder enters through a window.

Now, consider parts of the software as equivalent to a window. They may appear aesthetically pleasing, but they could inadvertently reveal functionality that highlights vulnerabilities or bugs. The Principle of Minimising Attack Surface Area prompts the question on if a particular feature is truly required. By simplifying or redesigning a feature, the overall security of the application improves. (Daswani, Kern and Kesavan, 2007).

This Secure-by-design approach minimises the need for retrofitting security measures and fosters the development of inherently secure industrial ecosystems.

10.1.5 Employee Training and Awareness Programs

Recognising the human element in cybersecurity, organisations should invest in comprehensive training programs. Employees play a pivotal role in maintaining a secure environment, and awareness programs enhance their ability to identify and respond to potential threats. Educating personnel on topics like phishing, password security, and social engineering contributes to a resilient security culture.

10.1.6 Collaboration and Information Sharing

Given the interconnected nature of Industry 4.0, collaboration among stakeholders in the Process Safety & Essential Services industries is paramount. Establishing forums for information sharing about emerging threats, vulnerabilities, and best practices enhances the collective cybersecurity posture of the industrial community.

10.1.7 Incident Response and Recovery Planning

Despite robust preventive measures, organisations must be prepared for the eventuality of a cyber incident. Developing comprehensive incident response and recovery plans ensures a coordinated and effective response in the aftermath of a security breach. This includes clear protocols for communication, investigation, containment, and system restoration.

10.2 Applying Lessons Learned by Process Safety to Cybersecurity

The integration of Industry 4.0 technologies into the Process Safety Sector introduces not only cybersecurity challenges but also raises profound implications for process safety. This section explores existing process safety measures essential for those organisations embracing Industry 4.0, aiming to adopt good Process Safety practises to ensure the reliability, resilience, and integrity of critical industrial systems.

10.2.1 Process Hazard Analysis (PHA) for Industry 4.0 Systems

An integral aspect of process safety in the Industry 4.0 landscape is the rigorous application of Process Hazard Analysis (PHA). Organisations must conduct thorough assessments of potential hazards associated with the implementation of new technologies. This should be extended to include analysing the interplay between cyber threats and physical processes to identify vulnerabilities that could compromise safety.

10.2.2 Functional Safety and SIL Certification

The concept of Functional Safety, governed by standards such as IEC 61508 and IEC 61511, plays a pivotal role in adopting Industry 4.0 devices and should follow a PHA using the methods previously described for HAZOP and CLOPA.

Where risk gaps are identified as being ‘intolerable’ an organisation will prioritise the implementation of Safety Instrumented Systems (SIS) and obtain Safety Integrity Level (SIL) certification for critical components, to ensure that the likelihood of failure does not result in a dangerous state. Similarly, this should be applied to cyber threat scenarios to ensure a failure does not result in an unsecured state. This ensures that safety functions operate effectively, even in the presence of cyber-attacks.

10.2.3 Redundancy, Diversity and Hardening

As Industry 4.0 expands across critical domains, safeguarding against cyber-attacks becomes paramount. To mitigate attacks on critical infrastructure that pose substantial risks to public health and safety a range of security techniques are available, including redundancy, diversity, and hardening. However, no single technique can comprehensively address the diverse spectrum of cyber-attacks that a determined and resourceful attacker might launch.

A combined approach that integrates these three key strategies would therefore be preferred; these are:

Redundancy: Deploying additional components and devices to enhance system robustness.

Diversity: Utilizing multiple implementation variants to reduce vulnerability.

Hardening: Reinforcing individual components to withstand attacks.

To enhance the robustness of process safety in Industry 4.0 context, organisations should incorporate redundancy, diversity and hardening into their cyber security design. These designs will provide backup and contingency options, minimising the risk of catastrophic failures due to both technological malfunctions and cyber incidents. (Laszka *et al.*, 2020)

10.2.4 Emergency Shutdown Systems (ESD) and Cyber-Physical Integration

Controlled shutdown in an emergency in the Process safety sector is deliberate and planned. Standard responses to accident scenarios are developed and must be presented to the HSE via a Safety Case. The Safety Case is reviewed periodically and contains all information necessary to control and mitigate in the event of an incident. (Timms, 2004)

The convergence of cyber and physical systems necessitates a holistic approach to Emergency Shutdown Systems (ESD). Organisations should ensure that these systems are not only responsive to physical safety concerns but are also equipped to detect and respond to cybersecurity threats. Cyber-physical integration of ESD systems ensures a synchronised response to protect both personnel and assets. This approach then needs to be documented within the Safety Case.

10.2.5 Cybersecurity-Enabled Process Safety Training

As Industry 4.0 introduces new technologies and complexities, organisations must invest in comprehensive training programs that bridge the gap between cybersecurity and process safety.

Employees involved in the operation and maintenance of industrial processes should receive training that addresses the intersection of cyber threats and safety protocols thereby avoiding inadvertently compromising the system integrity. ESD standard responses that have been reviewed and developed in the safety case needs to be trained and practised by the identified incident responders.

10.2.6 Asset Management and Lifecycle Security

The security of industrial assets throughout their lifecycle is paramount for sustained process safety. Organisations should implement robust asset management practices, incorporating cybersecurity considerations from procurement to decommissioning. This includes regular assessments, updates, and retirement strategies that account for evolving cyber threats.

A structured Management of Change procedure is needed to maintain control and document the modifications made.

10.2.7 Regulatory Compliance and Industry Standards

Adherence to regulatory requirements and industry standards is foundational for maintaining process safety in Industry 4.0. Organisations should stay abreast of evolving regulations related to both cybersecurity and process safety. Compliance with standards such as ISA/IEC 62443 – Security for Industrial Automated Control Systems and OG86 ensures a structured and comprehensive approach to managing safety and security risks.

For NIS and COMAH sites it is now a requirement to ensure Cyber security protocols are considered when submitting their Safety Case to the HSE. Currently HSE interventions are being aimed at Essential service providers such as Oil, Gas, Electricity, Nuclear Sectors with intention to extend this to top tier COMAH sites in the near future. (Health & Safety Executive (HSE), 2016)

Ensuring process safety in the era of Industry 4.0 demands a strategic blend of traditional safety measures and cybersecurity considerations. By embracing proactive hazard analysis, functional safety, redundancy, cyber-physical integration, training, asset management, and regulatory compliance, organisations can create a resilient framework that safeguards both human and industrial assets.

11- Conclusion

There is a drive to implement industry 4.0 operational technology and all the benefits that that will bring but this carries with it the double-edged sword of cyber security risk. There is no going back with technological advancement and the implementation of an interconnected world seems inevitable.

This study shows that certainly in the world of Process Safety managed by COMAH regulations and Essential Services supply managed by NIS regulations, the implementation of interconnected devices must only be embraced when alongside designed robust cyber security measures. The two cannot be separated since they are so highly dependent on each other and the consequences of getting it wrong are too disastrous.

An industry 4.0 assessment is normally conducted to determine if an organisation is prepared for industry 4.0 implementation, but this generally focuses on supply chain management and downstream logistical engagement to ensure maximum benefits of interconnected devices are realised. The assessments aim is to help maximise profits, throughput and reduce inventory. The cyber risk assessment to determine consequences and vulnerabilities of an attack are generally not considered, this study shows that that needs to change for these sectors.

Whereas previously a breach in cyber security would lead to informational loss or unlucky individuals becoming targeted generally for some financial gain. With Process Safety or Essential Services now being targeted the stakes are much higher, the cyber risk must be appropriately analysed, and the consequences completely understood. Unless this is recognised the measures needed so that effective prevention and mitigation controls are designed into the system to ward off an attack or minimise or lessen the damage caused cannot be put onto place.

The need to design in security in these interconnected field devices is paramount for the safety of nations and prevention of an otherwise inevitable catastrophe. Adopting industry 4.0 in these sectors of industry it seems is currently being addressed by some nation's competent authorities as the realisation of the consequences of not controlling its take-up are becoming more apparent.

There is a sense that the authorities are playing down the risk with plans such as NIS2 to address the gaps laid out over several years. This may be due to the lack of resource and cost to implement the changes quickly or it may be that they do not want to cause industrywide panic to the sector. Either way the industry should be made aware of the clear and present danger so that appropriate efforts are made to remove systemwide vulnerabilities.

12- References

- Accenture (2019) ‘Accenture/Ponemon Institute: The Cost of Cybercrime’, *Network Security*, 2019(3), p. 4. Available at: [https://doi.org/10.1016/S1353-4858\(19\)30032-7](https://doi.org/10.1016/S1353-4858(19)30032-7).
- Boersma, E. (2019) *7 Application Security Principles You Need to Know* | *Cprime Blogs*, *CPrime*. Available at: <https://www.cprime.com/resources/blog/security-by-design-7-principles-you-need-to-know/> (Accessed: 6 March 2024).
- Breth, J. and Douglas, C. (2020) ‘Cybersecurity Needs its Place in Emergency Management Now’, *CPO Magazine*.
- Buncefield Major Incident Investigation Board (2005) ‘Buncefield major incident investigation’, *Initial Report to the Health and Safety Commission and the Environment Agency of the investigation into the explosions and fires at the Buncefield oil storage and transfer depot, Hemel Hempstead, on 11th December*, pp. 4–203.
- Butcher, N. (2019) *Cyber Security - A Regulators Perspective*.
- Corò, G. and Volpe, M. (2020) ‘7 Driving factors in the adoption of Industry 4.0 technologies An investigation of SMEs’, in *Industry 4.0 and Regional Transformations*.
- Daswani, N., Kern, C. and Kesavan, A. (2007) ‘Secure Design Principles’, in N. Daswani, C. Kern, and A. Kesavan (eds) *Foundations of Security: What Every Programmer Needs to Know*. Berkeley, CA: Apress, pp. 61–76. Available at: https://doi.org/10.1007/978-1-4302-0377-3_3.
- Dhirani, L.L., Armstrong, E. and Newe, T. (2021) ‘Industrial IoT, Cyber Threats, and Standards Landscape: Evaluation and Roadmap’, *Sensors (Basel, Switzerland)*, 21(11), p. 3901. Available at: <https://doi.org/10.3390/s21113901>.
- Gao, Y. *et al.* (2013) ‘Analysis of security threats and vulnerability for cyber-physical systems’, in *Proceedings of 2013 3rd International Conference on Computer Science and Network Technology*, pp. 50–55. Available at: <https://doi.org/10.1109/ICCSNT.2013.6967062>.
- Gibbs, S. (2017) ‘Triton: hackers take out safety systems in “watershed” attack on energy plant’, *The Guardian (London)*. Available at: <https://search.proquest.com/docview/2829533640>.
- van Haastrecht, M. *et al.* (2021) ‘A Threat-Based Cybersecurity Risk Assessment Approach Addressing SME Needs’, *The 16th International Conference on Availability, Reliability and Security*, pp. 1–12. Available at: <https://doi.org/10.1145/3465481.3469199>.
- Hardy, T.L. (2014) ‘Case studies in process safety: Lessons learned from software-related accidents’, *Process Safety Progress*, 33(2), pp. 124–130. Available at: <https://doi.org/10.1002/prs.11638>.
- Health & Safety Executive (HSE) (2016) *Cyber security - Electrical, Control and Instrumentation (E, C&I) - HSE, Operational Guidance (OG) 86*. Available at: <https://www.hse.gov.uk/eci/cyber-security.htm> (Accessed: 3 March 2024).
- Health & Safety Executive (HSE) (2017) *Operational Guidance OG86: Cyber Security for Industrial Automated Control Systems*.
- Hennig, N. (2018) *Privacy and security online : best practices for cybersecurity*. Chicago, IL.
- IAIANI, M. *et al.* (2021) ‘Analysis of Cybersecurity-related Incidents in the Process Industry’, *Reliability Engineering & System Safety*, 209, p. 107485. Available at: <https://doi.org/10.1016/j.ress.2021.107485>.
- Janczewski, L. and Colarik, A.M. (2008) *Cyber warfare and cyber terrorism*. Hershey, Pa: IGI Global (Gale eBooks). Available at: <https://doi.org/10.4018/978-1-59140-991-5>.

- Japs, S. and Anacker, H. (2021) 'RESOLUTION OF SAFETY RELEVANT SECURITY THREATS IN THE SYSTEM ARCHITECTURE DESIGN PHASE ON THE EXAMPLE OF AUTOMOTIVE INDUSTRY', *Proceedings of the Design Society*, 1, pp. 2561–2570. Available at: <https://doi.org/10.1017/pds.2021.517>.
- Japs, S., Anacker, H. and Dumitrescu, R. (2021) 'SAVE: Security & safety by model-based systems engineering on the example of automotive industry', *Procedia CIRP*, 100, pp. 187–192. Available at: <https://doi.org/10.1016/j.procir.2021.05.053>.
- Kaya, G. (2018) *Good risk assessment practice in hospitals*.
- Knowles, W. *et al.* (2015) 'A survey of cyber security management in industrial control systems', *International Journal of Critical Infrastructure Protection*, 9, pp. 52–80. Available at: <https://doi.org/10.1016/j.ijcip.2015.02.002>.
- Laszka, A. *et al.* (2020) 'Integrating redundancy, diversity, and hardening to improve security of industrial internet of things', *Cyber-Physical Systems*, 6(1), pp. 1–32. Available at: <https://doi.org/10.1080/23335777.2019.1624620>.
- Legislation.gov.uk (2018) *The Network and Information Systems Regulations 2018: guide for the health sector in England*. Legislation.gov.uk. Available at: <https://doi.org/https://www.gov.uk/government/publications/network-and-information-systems-regulations-2018-health-sector-guide/the-network-and-information-systems-regulations-2018-guide-for-the-health-sector-in-england>.
- Lewis, K. (2015) 'Buncefield explosion: "I thought a plane landed on us"'. Available at: <https://doi.org/https://www.bbc.co.uk/news/uk-england-beds-bucks-herts-34919922>.
- Lezzi, M., Lazoi, M. and Corallo, A. (2018) 'Cybersecurity for Industry 4.0 in the current literature: A reference framework', *Computers in Industry*, 103, pp. 97–110. Available at: <https://doi.org/10.1016/j.compind.2018.09.004>.
- Li, Y. and Liu, Q. (2021) 'A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments', *Energy Reports*, 7, pp. 8176–8186. Available at: <https://doi.org/10.1016/j.egyr.2021.08.126>.
- Maggi, F. *et al.* (2017) 'Attacks on smart manufacturing systems', *robossec.org* [Preprint]. Available at: <https://robossec.org/downloads/wp-attacks-on-smart-manufacturing-systems.pdf> (Accessed: 3 March 2024).
- Makhdoom, I. *et al.* (2019) 'Anatomy of Threats to the Internet of Things', *IEEE Communications Surveys & Tutorials*, 21(2), pp. 1636–1675. Available at: <https://doi.org/10.1109/COMST.2018.2874978>.
- McMillan, R. (2018) 'New Type of Cyberattack Targets Factory Safety Systems; Malicious software Triton was able to manipulate Schneider Electric devices' memory and run unauthorized programs by leveraging a previously unknown bug', *WSJ Pro. Cyber Security* [Preprint]. Available at: <https://www.proquest.com/trade-journals/new-type-cyberattack-targets-factory-safety/docview/2171064569/se-2?accountid=130472>
https://libkey.io/libraries/1422/openurl?ctx_ver=Z39.88-2004&ctx_enc=info:ofi/enc:UTF-8&rft_id=info:sid/ProQuest&rft_val_fmt=journal&rft.genre=article&rft.jtitle=WSJ+Pro.+Cyber+Security&rft.atitle=New+Type+of+Cyberattack+Targets+Factory+Safety+Systems%253B+Malicious+software+Triton+was+able+to+manipulate+Schneider+Electric+devices%2527+memory+and+run+unauthorized+programs+by+leveraging+a+previously+unknown+bug&rft.au=McMillan%252C+Robert.&rft.aulast=McMillan&rft.aufirst=Robert&rft.date=2018-01-18&rft.volume=&rft.issue=&rft.space=&rft.isbn=&rft.btitle=&rft.title=WSJ+Pro.+Cyber+Security&rft.issn=&rft_id=info:doi/.
- Mohamed, M. (2018) 'Challenges and Benefits of Industry 4.0: An overview', *International Journal of Supply and Operations Management*, 5(3), pp. 256–265. Available at: www.ijssom.com (Accessed: 3 March 2024).

- Molina, J. (2023) *nis2 for operational technology*. Available at: https://www.google.com/search?q=nis2+for+operational+technology+molina&rlz=1C1CHBF_e_nGB895GB896&oq=nis2+for+operational+technology+molina&gs_lcrp=EgZjaHJvbWUyBggAEEUYOTIGCAEQRRg80gEJMTYzN2owajElqAIAAsAIA&sourceid=chrome&ie=UTF-8 (Accessed: 3 March 2024).
- Monteiro, J. (2019) 'Security analysis of an IACS environment: pentesting, exploitation and evaluation of a specialized cyber-detection platform'. Available at: <https://estudogeral.uc.pt/handle/10316/88028> (Accessed: 3 March 2024).
- Newswire, P.R. (2018) 'CyberX Sponsors SANS Webcast on "Anatomy of the TRITON ICS Cyberattack"', *PR Newswire*. Available at: <https://search.proquest.com/docview/2019017105>.
- Popkova, E.G., Ragulina, Y. V. and Bogoviz, A. V. (2019) 'Fundamental Differences of Transition to Industry 4.0 from Previous Industrial Revolutions', in *Industry 4.0 Industrial Revolution of the 21st Century. Studies in Systems, Decision and Control.*, pp. 21–29. Available at: https://doi.org/10.1007/978-3-319-94310-7_3.
- Rae, J.S., Chowdhury, M.M. and Jochen, M. (2019) 'Internet of things device hardening using shodan.io and shoVAT: A survey', in *IEEE International Conference on Electro Information Technology*. Available at: <https://doi.org/10.1109/EIT.2019.8834072>.
- Riegler, M. and Sametinger, J. (2021) 'Multi-mode Systems for Resilient Security in Industry 4.0', *Procedia Computer Science*, 180, pp. 301–307. Available at: <https://doi.org/10.1016/j.procs.2021.01.167>.
- Rojko, A. (2017) 'Industry 4.0 Concept: Background and Overview', *International Journal of Interactive Mobile Technologies (iJIM)*, 11(5), p. 77. Available at: <https://doi.org/10.3991/ijim.v11i5.7072>.
- Santos, B. *et al.* (2018) 'Industry 4.0: an overview', *iaeng.org*, 2. Available at: http://www.iaeng.org/publication/WCE2018/WCE2018_pp415-420.pdf (Accessed: 3 March 2024).
- Serino, A. and Cheng, L. (2020) 'Real-Time Operating Systems for Cyber-Physical Systems: Current Status and Future Research', in *2020 International Conferences on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics)*, pp. 419–425. Available at: <https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData-Cybermatics50389.2020.00080>.
- Skelton, B. (1997) *Process safety analysis: An introduction*. Available at: https://books.google.com/books?hl=en&lr=&id=49Yb4EfZYwkC&oi=fnd&pg=PA1&dq=process+safety+introduction&ots=TVstToALYR&sig=DqzlgBtkdo8P6oOtkHoWeFVmk_E (Accessed: 3 March 2024).
- Stoler, N. (2018) *Anatomy of the Triton Malware Attack, Cyberark The Identity Security Company*. Available at: <https://www.cyberark.com/resources/threat-research-blog/anatomy-of-the-triton-malware-attack>.
- Stone, M. (2021) *What is network segmentation? NS best practices, requirements explained, AT&T Cybersecurity*. Available at: <https://cybersecurity.att.com/blogs/security-essentials/network-segmentation-explained> (Accessed: 3 March 2024).
- Tantawy, A., Abdelwahed, S. and Erradi, A. (2022) 'Cyber LOPA: An Integrated Approach for the Design of Dependable and Secure Cyber-Physical Systems', *IEEE Transactions on Reliability*, 71(2), pp. 1075–1091. Available at: <https://doi.org/10.1109/TR.2022.3163652>.
- Thomas, R. (2003) 'COMAH safety report regime-evaluating the impact on new entrant establishments', *Symposium Series* [Preprint], (149). Available at: <https://www.icheme.org/media/10011/xvii-paper-59.pdf> (Accessed: 3 March 2024).

Timms, C. (2004) 'IEC 61511/an aid to COMAH and safety case regulations compliance', *Measurement and Control*, 37(4), pp. 115–122.

Willey, R.J. (2014) 'Layer of Protection Analysis', *Procedia Engineering*, 84, pp. 12–22. Available at: <https://doi.org/10.1016/J.PROENG.2014.10.405>.

Wu, D. *et al.* (2018) 'Cybersecurity for digital manufacturing', *Journal of Manufacturing Systems*, 48, pp. 3–12. Available at: <https://doi.org/10.1016/j.jmsy.2018.03.006>.

Zolotych, M. (2021) 'Study of Crawlers of Search Engine “Shodan.io”', in *Proceedings - 2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology, USBEREIT 2021*. Available at: <https://doi.org/10.1109/USBEREIT51232.2021.9455018>.