POLITÉCNICO DE LEIRIA | ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO

Cybersecurity in Industry 5.0

Investigating Cybersecurity Concepts in Industry 5.0 environments

Bruno Santos

School of Management and Technology
Department of Computer Engineering
Master in Cybersecurity & Digital Forensics

Leiria, September 2025

This page intentionally left blank.

POLITÉCNICO DE LEIRIA | ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO

Cybersecurity in Industry 5.0

Investigating Cybersecurity Concepts in Industry 5.0 environments

Bruno Santos
Student No. 2230456

Supervisor: Leonel Santos
Full Professor, Polytechnic University of Leiria

Co-supervisor: Rogério Luís de Carvalho
Associate Professor, University of Coimbra

School of Management and Technology
Department of Computer Engineering
Master in Cybersecurity & Digital Forensics

Dissertation

Leiria, September 2025

This page intentionally left blank.

Cybersecurity in Industry 5.0

Preparation of this work was facilitated by the use of the *IPLeiria-Thesis* template.

This page intentionally left blank.

Acknowledgements

I would like to express my sincere gratitude to Professor Leonel Santos of the Computer Science and Communication Research Centre Computer Science and Communication Research Centre (CIIC) at the Polytechnic University of Leiria, and to Assistant Professor Rogério Luís de Carvalho Costa of the Department of Informatics Engineering at the University of Coimbra, for their invaluable guidance, encouragement, and insightful feedback throughout the course of this dissertation.

I would also like to thank the project "Sustainable Stone by Portugal - Valuing Natural Stone for a digital, sustainable and qualified future (this work was supported by the Sustainable Stone by Portugal agenda funded by European Union/Next Generation EU under Grant 02/C05-i01.02/2022.PC644943391-00000051)."

This page intentionally left blank.

Resumo

A Indústria 5.0 representa a próxima fase da evolução industrial, centrando-se na colaboração entre humanos e máquinas, sustentabilidade e nas tecnologias avançadas. Embora estas inovações aumentem a produtividade e promovam a inovação, também alargam o panorama das ameaças cibernéticas, levantando preocupações quanto à segurança, integridade dos dados e privacidade. Os ciberataques nestes ambientes podem afetar ativos industriais, colaboradores e clientes, evidenciando a necessidade de uma cibersegurança robusta.

Este estudo explora as implicações da cibersegurança na Indústria 5.0, com o objetivo de normalizar o seu conceito e propor uma *framework* de alto nível para ajudar a sua implementação. Este trabalho analisa domínios chave da cibersegurança - protocolos de comunicação industrial, inventário de ativos, gestão de vulnerabilidades, inteligência de ameaças, segurança de *endpoints*, deteção e resposta a incidentes, segmentação de redes, arquitetura *Zero Trust* e o princípio do menor privilégio — avaliando a sua relevância e as adaptações necessárias no contexto da Indústria 5.0.

Os desafios e adaptações são testados através de casos de estudo nos setores de corte de pedra, e alimentar e bebidas. Algumas das conclusões incluem: aumento dos custos com cibersegurança, expansão dos vetores de ameaça e complexidade adicional devido aos objetivos de sustentabilidade e ética centrada no ser humano da Indústria 5.0. A *framework* criada é testada garantindo que os desafios estão contemplados, e sendo utilizada como estrutura para implementar as tecnologias da Indústria 5.0 presentes nos casos de estudo. A *framework* desenvolvida passou nos testes, ao contrário de outras que apresentaram lacunas em aspetos essenciais. Este trabalho estabelece uma base para compreender a cibersegurança na Indústria 5.0 e oferece uma abordagem estruturada para a sua implementação.

As direções futuras da investigação incluem a aplicação prática da *framework* e a expansão dos domínios da cibersegurança para incluir testes de penetração e formação dos trabalhadores, de forma a enfrentar riscos emergentes e garantir uma integração segura das tecnologias da Indústria 5.0.

Palavras-Chave: Cibersegurança, Áreas da Cibersegurança, Industria 5.0, Frameworks Industriais

This page intentionally left blank.

Abstract

Industry 5.0 represents the next phase of industrial evolution, focusing on human-machine collaboration and advanced digital technologies. While these innovations boost productivity and innovation, they also broaden the cyber threat landscape, raising concerns about safety, data integrity, and privacy. Cyberattacks in such environments can impact industrial assets, employees, and customers, underscoring the need for robust cybersecurity.

This study explores the cybersecurity implications of Industry 5.0, aiming to standardise its concept and propose a high-level framework to guide implementation. It examines key cybersecurity domains-industrial communication protocols, asset inventory, vulnerability management, threat intelligence, endpoint security, incident detection and response, network segmentation, zero trust architecture, and least privilege-evaluating their relevance and required adaptations in Industry 5.0 settings.

Challenges and adaptations are tested through a case study in the stone cutting sector. Some of the findings were: an increase in cybersecurity costs, expansion of threat vectors, and added complexity due to sustainability and human-centric ethics goals of Industry 5.0. The created high-level framework is tested by making sure these challenges are included in it, and by using it as a structured approach to implement Industry 5.0's technologies present in the case study. The developed framework passed the testing, while other frameworks lacked some key aspects. The work lays a foundation for understanding cybersecurity in Industry 5.0 and offers a structured approach for its implementation.

Future research directions include practical deployment of the framework and expansion of the cybersecurity domains to include penetration testing and workforce training. This is to address emerging risks and ensure secure integration of Industry 5.0 technologies.

Keywords: Cybersecurity, Cybersecurity Dimensions, Industry 5.0, Industrial Frameworks.

This page intentionally left blank.

AI Acknowledgement

I acknowledge the use of OpenAI ChatGPT (https://chatgpt.com) and Microsoft Copilot (https://copilot.microsoft.com/) to refine the academic tone and improve the linguistic accuracy of this work, including aspects of grammar, punctuation, and vocabulary.

This page intentionally left blank.

Contents

This page intentionally left blank.

List of Figures

This page intentionally left blank.

List of Tables

This page intentionally left blank.

Acronyms

AES Advanced Encryption Standard. (*p. 37, 38*)
AI Artifical Intelligence. (*p. 5, 61, 62, 64, 68, 71*)
AR Augmented Reality. (*p. 55*)
ARP Address Resolution Protocol. (*p. 21*)
ATT Adversarial Tactics and Techniques. (*p. 58, 85*)

BMI Brain Machine Interface. (*p. 54, 58, 66, 68, 71–73, 85*)

CAD Computer-Aided Design. (*p. 47, 79, 80, 84–87*)
CEF Common Event Format. (*p. 46*)
CIA Confidentiality, Integrity, and Availability. (*p. 13, 63*)
CIIC Computer Science and Communication Research Centre. (*p. i*)
CIP Common Industrial Protocol. (*p. 35*)
CK Common Knowledge. (*p. 58, 85*)
CNC Computer Numerical Control. (*p. 78–81, 83–91*)
CPS Cyber-Physical System. (*p. 3, 64*)
CRC Cyclic Redundancy Check. (*p. 63*)
CSV Comma-Separated Values. (*p. 46*)
CVSS Common Vulnerability Scoring System. (*p. 22, 23*)

DLR Device Level Ring. (*p. 35*)
DMZ Demilitarized Zone. (*p. 80*)
DoS Denial of Service. (*p. 22, 36, 37, 68, 69, 71, 73, 87*)
DP Decentralised Peripherals. (*p. 34, 36, 38, 64*)
DTLS Datagram Transport Layer Security. (*p. 35*)

EDR Endpoint Detection and Response. (*p. xii, xiii, 33, 39–46, 67, 68, 70, 81, 83, 87, 88, 90*)
EEG Electroencephalography. (*p. 69*)
ERP Enterprise Resource Planning. (*p. 61, 90*)
ESG Environmental, Social, and Governance. (*p. 78, 90, 92*)
EWS Engineering Workstation. (*p. 7, 40, 42, 47, 63, 80*)

GB GigaByte. (*p. 46*)
GDPR General Data Protection Regulation. (*p. 43, 53, 72, 82*)

HA High Availability. (*p. 14*)
HIPAA Health Insurance Portability and Accountability Act. (*p. 33, 43*)
HLFI 5.0 High-Level Framework for Industry 5.0. (*p. 76*)
HMAC Hash-based Message Authentication Code. (*p. 13*)
HMI Human-Machine Interface. (*p. 6, 7, 40, 42, 47, 79*)
HTTP Hypertext Transfer Protocol. (*p. 69*)
HTTPS Hypertext Transfer Protocol Secure. (*p. 81*)

IAM Identity and Access Management. (*p. 15*)
ICS Industrial Control System. (*p. 5, 7, 8, 14, 16–21, 58, 61, 63, 85*)
ID Identifier. (*p. 21, 54*)
IDS Intrusion Detection System. (*p. 45, 46*)
IEC International Electrotechnical Commission. (*p. 10, 12, 20, 31, 34*)
IEEE Institute of Electrical and Electronics Engineers. (*p. 2, 37, 64*)
IIoT Industrial Internet of Things. (*p. 8, 17, 18, 56, 62, 64, 66, 74, 75, 91*)
IIRA Industrial Internet Reference Architecture. (*p. xiii, 74, 75, 91*)
IMAP Internet Message Access Protocol. (*p. 81*)
IOC Indicator of Compromise. (*p. 25, 26*)
IoT Internet of Things. (*p. 11, 17, 34, 47, 53, 55, 57, 59, 61, 62, 67*)
IP Internet Protocol. (*p. 21, 25, 34–36, 38, 50, 63–65, 81*)
IPS Intrusion Prevention System. (*p. 45*)
ISO International Organization for Standardization. (*p. 20*)
IT Information Technology. (*p. 3, 7–9, 14–16, 18, 20–25, 33, 34, 39, 41, 42, 46–48, 56, 58–62, 74, 80, 85*)

JSON JavaScript Object Notation. (*p. 46*)

KPI Key Performance Indicator. (*p. 79, 90*)

LDAP Lightweight Directory Access Protocol. (*p. 15*)
LRC Longitudinal Redundancy Check. (*p. 63*)

MAC Media Access Control. (*p. 21*)
MATLAB Matrix Laboratory. (*p. 80*)
MES Manufacturing Execution System. (*p. 90*)
MFA Multifactor Authentication. (*p. 29, 30*)
MitM Man-in-the-Middle. (*p. 68, 69, 71, 73, 87*)
MS Microsoft. (*p. 40*)

NIST National Institute of Standards and Technology. (*p. xii, 20, 43, 44*)

OPC UA Open Platform Communications Unified Architecture. (*p. xii, 28, 37, 38, 63–67, 79, 90*)
OS Operational System. (*p. 46*)
OT Operational Technology. (*p. ix, xii, 1, 3, 5–16, 18–27, 31, 33, 39–42, 45–48, 50, 51, 56–62, 64, 67, 68, 74, 80, 85, 86*)

PCI DSS Payment Card Industry Data Security Standard. (*p. 43*)
PERA Purdue Enterprise Reference Architecture. (*p. 7, 8*)
PII Personally Identifiable Information. (*p. 54, 58, 72, 73, 82, 88, 92*)
PLC Programmable Logic Controller. (*p. 7, 17, 29, 30, 40, 42, 44, 47, 58, 61, 63, 64, 79, 81, 82, 90, 91*)
PoLP Principle of Least Privilege. (*p. 28–30, 59*)
POP3 Post Office Protocol 3. (*p. 81*)
PROFIBUS Process Field Bus. (*p. 34, 36, 38, 64*)
PROFINET Process Field Network. (*p. 34, 35, 38*)

RADIUS Remote Authentication Dial-In User Service. (*p. 37*)
RAID Redundant Array of Independent Disks. (*p. 13*)
RAMI Reference Architectural Model Industrie. (*p. xiii, 74–77, 91, 92*)
RBAC Role-Based Access Control. (*p. 15*)
RFID Radio-Frequency Identification. (*p. 90*)
ROI Return on Invenstment. (*p. 27*)
RS Recommended Standard. (*p. 36*)
RTU Remote Terminal Unit. (*p. 11, 34, 36, 38, 63, 64*)

SAE System Architecture Evolution. (*p. 37*)
SCADA Supervisory Control And Data Acquisition. (*p. 11, 13, 14, 40–42, 66*)
SHA Secure Hash Algorithm. (*p. 12, 13*)
SIEM Security Information and Event Management. (*p. xii, xiii, 20, 26, 41, 45–47, 49, 70–72, 81, 83, 88, 89*)
SMS Short Message Service. (*p. 29*)
SMTP Simple Mail Transfer Protocol. (*p. 81*)
SOAR Security Orchestration, Automation and Response. (*p. 49, 50*)
SOC Security Operation Center. (*p. 26, 46*)
SQL Structured Query Language. (*p. 40*)
SSH Secure Shell. (*p. 80*)
SSL Secure Sockets Layer. (*p. 28*)

TCP Transmission Control Protocol. (*p. 34, 36, 38, 63–65, 81*)
TLS Transport Layer Security. (*p. 12, 28, 35, 36, 38*)
TSN Time-Sensitive Networking. (*p. 35, 37*)

URL Uniform Resource Locator. (*p. 49*)
US United States. (*p. 17, 54*)
USB Universal Serial Bus. (*p. 33, 42*)

VPN Virtual Private Network. (*p. 33, 50*)

WPA Wi-Fi Protected Access. (*p. 37*)
WSN Wireless Sensor Network. (*p. 66*)

ZTA Zero Trust Architecture. (*p. xii, 52, 58, 61, 85, 86*)

This page intentionally left blank.

1 Introduction

Recent Industrial Revolutions have led to a significant increase in the digitalisation of industrial processes (Leng et al., 2022). With the widespread adoption of industrial digital systems, it is of great importance to implement robust cybersecurity measures to safeguard information, assets, and individuals. Failure to do so can have a significant impact on human beings, both physically and mentally. For instance, cyberattacks that alter the typical behaviour of collaborative robots can result in physical damage to the human and the robot, as well as the products (Hollerer et al., 2021; Jia et al., 2022). Furthermore, privacy data breaches can negatively impact the mental health of the people involved (Etela, 2021). A recent report on data breaches analysed 30,458 security incidents in 2023, of which 10,626 were confirmed data breaches (Business, 2024). The number of data breaches was a record high. In the manufacturing industry, 2,305 incidents were analysed, of which $\approx$ 37 % had confirmed data breaches. Furthermore, the compromised data in the data breaches was mainly personal data. These alarming numbers show that security incidents affect not only the organisations but also the employees and customers. In Industry 5.0, organisations must prioritise strong cybersecurity measures to protect all the people and assets involved.

With the new enabling technologies and concepts of Industry 5.0, the range of attacks increased, and the vitality of implementing strong cybersecurity measures is greater than ever. This work aims to help better understand the implications of Industry 5.0 in cybersecurity. Furthermore, it aims to help organisations understand and implement Industry 5.0. Both these objectives seek to help the implementation of cybersecurity in Industry 5.0.

This document begins by introducing foundational concepts such as Industry 5.0, the industrial revolutions, and Operational Technology (OT) cybersecurity, followed by a literature review on these topics. The literature review identified opportunities to study the implementation of cybersecurity in Industry 5.0 and create a high-level framework to define and help implement Industry 5.0 into an organisation. Also, the document includes a dedicated chapter outlining key dimensions of cybersecurity: Governance and Risk Management, Security Architecture and Design, and Security

Operations, while focusing on specific areas like threat intelligence, zero trust architecture, and endpoint security. Finally, these cybersecurity dimensions and areas are analysed within the framework of Industry 5.0.

If new challenges arise, then they will be put to the test with a case study representing a typical situation of the stone cutting industry. Moreover, if the current available frameworks fail to meet Industry 5.0's objectives, then a new one will be created. The high-level framework is going to be tested using the identified challenges in conjunction with the case study. The aim of the research is to create a framework that explains and helps implement Industry 5.0 when others don't meet Industry 5.0's objectives.

This document was partially created as part of the project "Sustainable Stone by Portugal - Valorização da Pedra Natural para um futuro digital, sustentável e qualificado". The project led to the writing and publishing of a paper. The paper is titled "Cybersecurity in Industry 5.0: Open Challenges and Future Directions", and it was presented at conference 2024 21st Annual International Conference on Privacy, Security and Trust. Later, the paper was published in Institute of Electrical and Electronics Engineers (IEEE) Xplore (Santos et al., 2024). The paper is the foundation for this document.

The contributions of this document are summarised as follows:

- Proposal of challenges and problems in cybersecurity specific areas in the context of Industry 5.0.
- Creation of a high-level framework that can encompass the challenges and explain Industry 5.0's different dimensions.
- Validation of the proposed challenges and framework with a case study.
- Give the initial footstep into understanding the implications of Industry 5.0 and the future in cybersecurity.

This document is organised as follows. Chapter 2 provides detailed background information and reviews related work in the literature. Then, Chapter 3 introduces detailed information on various cybersecurity dimensions: Governance and Risk Management; Security Architecture and Design; Security Operations. Chapter 4 uses the previous cybersecurity dimensions and applies them to Industry 5.0, with the objective of understanding its implications. Furthermore, Chapter 5 creates a high-level framework that encompasses the identified implications and explains Industry 5.0. Moreover, this chapter presents a case study in order to validate the implications and the high-level framework. Finally, this work concludes with Section 6.

2
Background

This section serves the purpose of introducing fundamental concepts related to the theme of this document, including industrial revolutions, Industry 5.0, enabling technologies, operational technology and industrial control systems, reference architecture models and cybersecurity. These topics are divided into sections to facilitate a more coherent organisation.

2.1 Industrial Revolutions

This section begins by reviewing essential background information related to the different industrial revolutions and the major differences between the two latest industrial revolutions. Furthermore, it points out the key enabling technologies of Industry 5.0, followed by a review of related work.

Many historians, economists, and scholars define industrial revolutions as periods of technological change with a high impact on society (Klingenberg et al., 2022). As of the writing of this work, there have been five known industrial revolutions. In the 1800s, the First Industrial Revolution, also known as Industry 1.0, developed mechanical production infrastructures for water and steam-powered machines. Industry 2.0, the Second Industrial Revolution, emerged in 1870 with the introduction of electric power and assembly line production. Industry 3.0 came into being in 1969, with the introduction of electronics, partial automation, and Information Technology (IT) (Maddikunta et al., 2022). Industry 4.0 evolved in 2011 with the concept of smart manufacturing by merging IT and OT in a Cyber-Physical System (CPS) to achieve mass automation and production (Maddikunta et al., 2022; Leng et al., 2022). Because Industry 5.0 is still in its initial stages, different definitions are being provided by industry practitioners and researchers. This work combines the definitions provided by European Comission, 2022 and Maddikunta et al., 2022. The definition is as follows: Industry 5.0 aims to achieve societal goals beyond efficiency and productivity, transforming industries into resilient providers of prosperity. For that objective, industries must respect the planet and lead the green transitions. Also, cybersecurity is a key component for

a resilient industry. Industry 5.0 also places the well-being of the industry worker at the centre of the production process, and instead of replacing humans with machines, a collaboration between both takes place. This collaboration is designed to use the creativity of human experts who work together with efficient, intelligent and accurate machines (Santos et al., 2024).

This human-centred approach, which is characteristic of Industry 5.0, appears to be a concept that is not well-received by employers. The rationale behind employers' decision to reintegrate human capital into the industry process is a subject that merits further scrutiny. The prevailing assumption was that the future would entail the replacement of human operators in the industry process. However, it can be beneficial for the organisation to invest in a new way. This novel approach signifies a paradigm shift towards a symbiotic relationship between humans and machines. Some of the new enabling technologies of Industry 5.0 aim at facilitating this relationship. This does not mean that all machines will be replaced and now benefit from the reintroduction of human operators. In the majority of tasks, the productivity of the traditional machine will still replace the human. However, some tasks can benefit from the collaboration (e.g. welding, painting and pick-and-place operations) (Robotics, 2025). The worker will be regarded as an investment, thereby facilitating the collaborative development of both the worker and the company (Directorate-General for Research and Innovation (European Commission) et al., 2021). This collaboration between humans and machines will leverage the strengths of both parties, which will lead to higher productivity and worker well-being (Directorate-General for Research and Innovation (European Commission) et al., 2021). The machines in question have been designed to adapt to the needs of the workers, rather than the other way around. It is evident that the companies will also benefit from a higher chance of attracting and retaining talent (Directorate-General for Research and Innovation (European Commission) et al., 2021).

2.2 Industry 5.0 Enabling Technologies

In 2020, the European Commission wrote a report listing 41 enabling technologies for Industry 5.0 (Directorate-General for Research and Innovation (European Commission) et al., 2020). This report was written based on a workshop with some of Europe's technology leaders. Other academic papers, such as those presented by Leng et al., 2022 and Maddikunta et al., 2022, also reference some of the same enabling technologies. This section will specifically concentrate on the European Commission report, as it provides more detailed information.

The report classifies and separates the enabling technologies into six different categories. Figure 2.1 illustrates the categories: Individualised Human-Machine Interaction; Digital Twins and Simulation; Data Transmission, Storage, and Analysis Technologies; Artificial Intelligence; Energy Efficiency, Renewables, Storage and Autonomy; and Bio-inspired Technologies and Smart Materials.

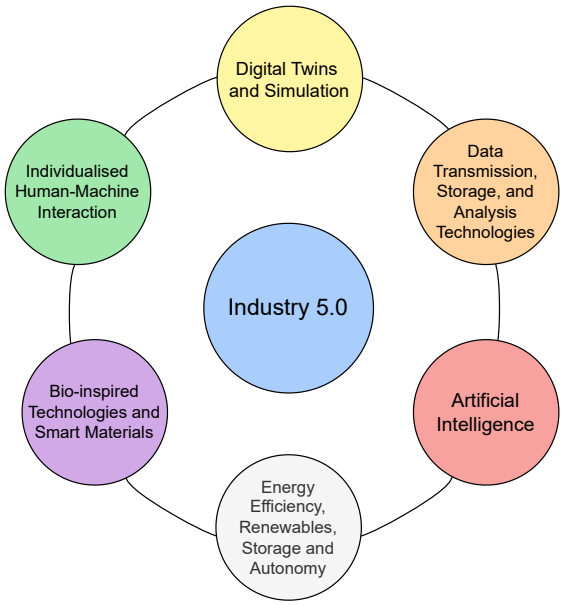

Figure 2.1: *Six categories of Industry 5.0's enabling technologies.*

We will not list all the enabling technologies to avoid unnecessary length. However, a random selection of enabling technologies was made. In individualised human-machine interaction, cobots, exoskeletons, and strain sensors improve worker satisfaction and reintegrate humans into the manufacturing process. Bio-inspired technologies and smart materials, like living and recyclable materials, are vital for a sustainable industry. Digital twins and simulations have a wide array of uses, including facilitating visibility and predictability of processes. Data transmission, storage, and analysis technologies, including cybersecurity, cloud infrastructure, big data analytics, and edge computing, contribute to security and resilience. Brain-machine interfaces, human-centred Artifical Intelligence (AI), and explainable AI enhance job satisfaction and reintegrate humans into manufacturing. Renewable energies and energy-autonomous sensors support the green transition in Industry 5.0.

Some of these technologies will be used throughout the chapters to exemplify and prove points.

2.3 Operational Technology

OT encompasses a broad range of programmable systems and devices that, through monitoring and/or controlling devices, processes, and events, interact with the physical environment. Examples of these systems are Industrial Control System (ICS), building automation systems, transportation systems, physical access control systems, physical environment monitoring systems, and physical environment measurement systems (Stouffer et al., 2023). The main focus of this work will be on ICS. Usually, OT systems consist of two parts: one primarily focused on producing an output, known as the process, and the other focused on maintaining conformance with specifications,

known as the controller (Stouffer et al., 2023).

OT systems typically consist of control loops, Human-Machine Interface (HMI), and remote diagnostic tools (Stouffer et al., 2023). A control loop includes sensors, controllers, actuators, and the controlled process, as can be seen in Figure 2.2. Sensors measure physical properties and send data to the controller, which applies algorithms and set points to issue commands to actuators. Actuators then adjust the process, and sensors continually provide feedback. Direct communication between sensors and actuators is uncommon. HMIs enable operators to configure control parameters and access system status or historical data. Remote diagnostic tools support monitoring, fault detection, and recovery. Control loops may also be nested or cascaded, with some loops depending on others.

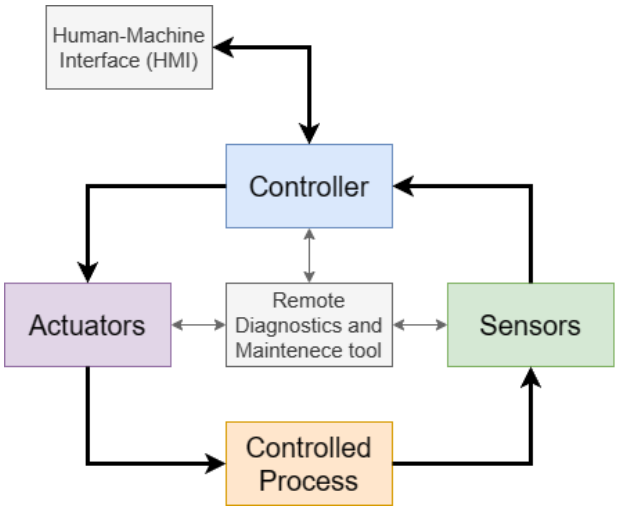

Figure 2.2: *Operation of basic OT system. Adapted from: Stouffer et al., 2023.*

OT systems exhibit several defining characteristics (Stouffer et al., 2023). Safety is paramount, as systems must detect and prevent unsafe conditions, with human oversight remaining essential in hazardous processes. Control timing requirements are also critical; many operations demand high speed, consistency, regularity, and synchronisation, which necessitate automated controllers when humans can't meet these requirements. The closer the computation is to the sensors and actuators, the lower the communication latency. Another challenge is the degree of geographic distribution variation, ranging from local processes managed by PLCs to large-scale infrastructures such as oil pipelines, where wide-area networks and mobile communications become essential. A hierarchical or centralised control structure further supports operators by providing a comprehensive system overview for informed decision-making. Control complexity is another factor, as simple algorithms may suffice in routine scenarios, whereas more intricate operations require human intervention. High availability is also paramount, which may involve redundancy or alternative implementations across communication and control layers. Furthermore, the impact of failures can be significant; in such cases, systems must maintain functionality either through redundant controls or by operating in a degraded yet stable state. Finally, cybersecurity require-

ments for OT will be analysed in detail in Section 2.6.

ICS are one of the many types of OT systems. An ICS can be defined as a combination of control components that act together to achieve an industrial objective, meaning that they control industrial processes (e.g., manufacturing, transportation of matter or energy) (Stouffer et al., 2023). Examples of ICS include Programmable Logic Controller (PLC) (Stouffer et al., 2023; Bhamare et al., 2020).

PLCs are industrial computers designed to control and monitor equipment through custom programming, operating in three stages: capturing input data from connected devices, executing program logic, and adjusting outputs accordingly. Introduced in the late 1960s as a replacement for hard-wired relay systems, PLCs revolutionised industrial control by offering greater flexibility, reliability, and efficiency, becoming a cornerstone of modern automation (Inductive Automation, 2025b).

2.4 Reference Architecture Models

Reference architecture models are widely accepted as a standardised approach to designing and implementing solutions for various industries. These models provide architects and developers with specific guidelines, best practices, and blueprints to follow when creating systems or other technical solutions. As a result, reference architecture models have become an essential tool for many businesses looking to streamline their development processes and create top-quality solutions (Nakagawa et al., 2021).

Developed in the early 1990s, the Purdue Enterprise Reference Architecture (PERA) divides an ICS network into multiple segments, and it was originally designed to define best practices when combining ICS and IT. The model could also be used to define the development and operation of any enterprise regardless of the industry or field of endeavour involved (Williams, 1993). With the increasing tendency to combine IT and OT systems, the model evolved, and one of its interpretations can be seen in Figure 2.3. It is worth noting that different researchers may represent this model slightly differently. The PERA model is normally divided into six levels across four different zones (Conti et al., 2021; Green et al., 2017):

- The Safety Zone includes devices and systems to ensure safety in ICS systems.
- The Control Zone is divided into four different levels:
  - The Level 0 contains sensors and actuators that act in the physical process.
  - The Level 1 contains controller devices such as PLC.
  - The Level 2 contains supervisory devices such as HMI.
  - The Level 3 contains Engineering Workstation (EWS) that manages and controls manufacturing operations in the industrial sites.
- The Demilitarised Zone controls and manages the data transported between the IT and OT systems.
- The Enterprise Zone is divided into two different levels that encompass the IT devices and systems, and the enterprise network.

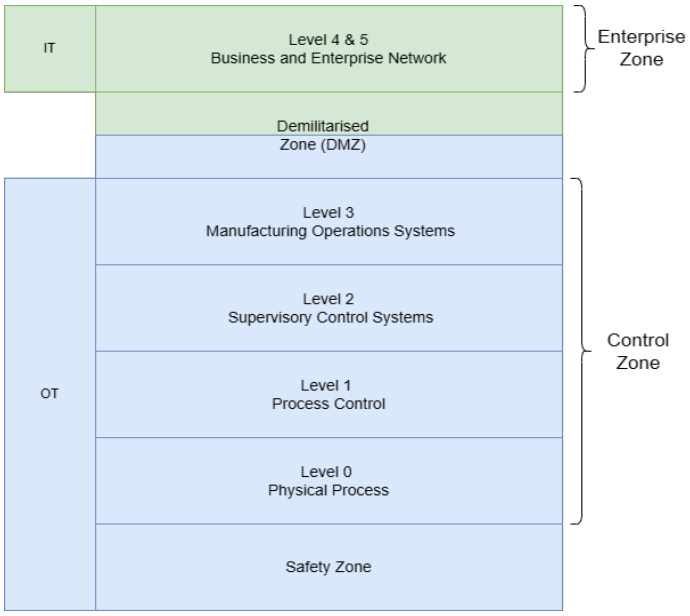

Figure 2.3: *Purdue Enterprise Reference Architecture. Adapted from: Conti et al., 2021 and Green et al., 2017.*

While the PERA model continues to serve as a benchmark for good practices in ICS security architecture, recent advancements in internet-based technologies are reshaping the landscape. These technologies arise in Industry 4.0, including the use of Industrial Internet of Things (IIoT) devices and the use of cloud-based industrial applications (Bécue et al., 2021).

2.5 Cybersecurity

Cybersecurity has long been a cornerstone of IT, safeguarding sensitive data, enabling secure internet connectivity, and detecting as well as preventing cyberattacks. Its importance is equally pronounced in OT environments, where the protection of critical infrastructure is paramount. Even brief delays or unplanned downtime can halt operations in manufacturing facilities, power plants, or water supply systems. Implementing robust OT security measures mitigates these risks by ensuring continuous protection and minimising disruptions. As these systems become increasingly interconnected, their exposure to new vulnerabilities rises, making comprehensive security essential to preventing unauthorised access to industrial networks (Fortinet, 2025a; Palo Alto, 2025c).

OT and IT differ in several fundamental ways. OT systems are typically autonomous, isolated, self-contained, and reliant on proprietary software. By contrast, IT systems are highly connected, less autonomous, and generally operate on widely used platforms such as Windows or iOS. These distinctions extend to security priorities: IT security is primarily concerned with safeguarding data confidentiality, ensuring that sensitive information is accessible only to authorised users. OT security, on the other hand, emphasises the safety and availability of industrial systems and processes, where

uninterrupted operation is critical (Fortinet, 2025a; Palo Alto, 2025c).

Despite their clear distinctions, IT and OT cybersecurity share notable similarities and are becoming increasingly interconnected. Historically, OT devices were isolated from the public internet and even from internal networks, accessible only to authorised personnel. Today, however, many OT systems can be monitored and controlled through IT infrastructures or remotely via the internet. Both domains aim to enhance organisational efficiency, are progressively adopting advanced technologies such as artificial intelligence, machine learning, and cloud computing, and are witnessing a growing convergence of skills within a more interdisciplinary workforce (Fortinet, 2025a; Palo Alto, 2025c).

2.6 Pillars of Operational Security

OT security is founded on a set of core pillars that collectively ensure the safe, reliable, and secure operation of industrial systems. These pillars are: Safety, Confidentiality, Integrity, Availability, Authentication, Authorisation, and Determinism (Stouffer et al., 2023; Trend Micro, 2020). These pillars address both the traditional concerns of industrial control and the modern demands of cybersecurity. Safety remains paramount, protecting human lives, the environment, and physical assets (Stouffer et al., 2023). Meanwhile, Confidentiality, Integrity, and Availability uphold the core tenets of cybersecurity, ensuring that systems function correctly, data remains unaltered, and services are accessible when needed (Stouffer et al., 2023; Trend Micro, 2020). Authentication and Authorisation control access to critical systems, preventing unauthorised manipulation (Stouffer et al., 2023; doronbasson, 2025), while Determinism ensures predictable system behaviour, which is an essential requirement for time-sensitive and safety-critical operations in OT environments (Stouffer et al., 2023; Hartrup, 2025).

Among these pillars, Safety and Availability are typically considered the most critical in OT contexts, as system failure can result in catastrophic physical consequences and significant operational downtime (Tullman-Botzer, 2025a; Stouffer et al., 2023). Confidentiality is normally the least important pillar in OT security, contrasting with IT security, as the primary focus in OT is on operational continuity and safety rather than data secrecy (Stouffer et al., 2023; Tim Mullen, 2025). However, confidentiality can be very useful in particular cases. For example, if an attacker can discover important information by analysing the data traffic (e.g. confidential recipe), then confidentiality in this situation is advised (Tim Mullen, 2025). Integrity ensures that control commands and sensor data are accurate and trustworthy (Stouffer et al., 2023). Authentication and Authorisation are also vital, particularly as OT networks become more connected and exposed to external threats (Stouffer et al., 2023). Determinism, while often overlooked, plays a key role in maintaining predictable system responses, especially in real-time control (Stouffer et al., 2023). Figure 2.4 shows all the pillars of OT security.

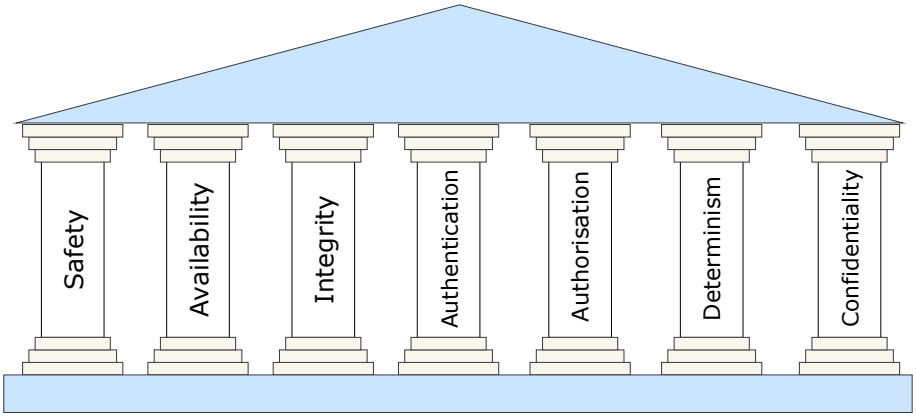

Figure 2.4: *Pillars of OT Security: Safety, Availability, Integrity, Authenticaiton, Authorisation, Determinism and Confidentiality. Adapted from: Bidwai, 2025.*

2.6.1 Safety in OT

Functional safety can be defined as the aspect of OT systems that ensures they operate correctly and safely even in the presence of faults, abnormal conditions, or system failures. The primary objective of this approach is to detect and mitigate the risks that could lead to hazardous situations, with a view to protecting people, equipment and the environment. Robust functional safety systems have been shown to enhance system reliability and ensure compliance with critical safety regulations (BlastWave, 2025f).

The implementation of functional safety in OT systems can be achieved through a variety of methodologies, including risk reduction, failure detection, redundancy, fail-safe mechanisms and adherence to industry standards. Risk reduction strategies are implemented to minimise hazards, such as automatically shutting down a chemical reactor when temperatures exceed safe thresholds. Real-time failure detection mechanisms are designed to identify faults and initiate appropriate responses. Control systems are an example of such mechanisms; they detect sensor failures and switch to backup readings. Redundancy is also critical, with duplicate components such as dual power supplies being employed to maintain functionality during faults. Fail-safe mechanisms are designed to ensure that systems revert to a safe state in the event of failure, as exemplified by the closure of valves in a gas pipeline during a pressure surge. Furthermore, adherence to regulatory standards, such as International Electrotechnical Commission (IEC) 61508 for functional safety, ensures that systems meet industry-accepted safety and reliability benchmarks (BlastWave, 2025f).

The implementation of functional safety in OT environments poses a number of challenges, attributable to the complexity and diversity of the systems involved. Interconnected systems can complicate the identification of failure modes, necessitating comprehensive hazard and operability studies to identify and mitigate potential risks. Legacy equipment frequently exhibits deficiencies in contemporary safety features or incompatibility with more recent systems. These issues can be addressed through retrofitting with external safety controls or upgrading outdated components. The ne-

cessity of regular maintenance, encompassing testing and calibration, for functional safety systems is paramount. The establishment of routine maintenance schedules and the utilisation of automated testing tools are of the essence in ensuring the efficacy of these systems. Furthermore, there is frequently a necessity to balance safety with productivity, as overly conservative safety mechanisms have the potential to impede operational efficiency; optimising safety thresholds can assist in maintaining this balance. Furthermore, the growing threat of cyberattacks represents a major risk to safety systems, with the potential for attackers to target such systems in order to induce hazardous conditions. This emphasises the necessity for robust protective measures such as firewalls, access controls, and continuous monitoring (BlastWave, 2025f).

2.6.2 Confidentiality in OT

In the domain of OT cybersecurity, confidentiality is of paramount importance. The implementation of stringent access control measures is imperative to ensure that sensitive information is only accessible to authorised individuals. This encompasses a wide range of data, including operational procedures, system configurations, and proprietary information. Whilst ensuring the confidentiality of such information is of paramount importance, it should be noted that even the most sophisticated hackers may find it of limited use. However, it is imperative to acknowledge that specific processes are inherently sensitive in nature or may involve support systems that necessitate the transmission of confidential data. Consequently, a thorough evaluation of the specific situation is imperative to accurately assess the risks and impact on confidentiality. Depending on the sensitivity of the data concerned, breaches of confidentiality have the potential to result in a number of adverse outcomes, including industrial espionage, competitive disadvantage, or the manipulation of critical systems by adversaries. It is evident that such actions have the potential to result in process disruptions and even safety incidents (OT Security Glossary, 2025; Tim Mullen, 2025).

In order to ensure the requisite confidentiality, it is necessary to employ encryption. Encryption can be defined as the process of encoding data in order to protect it from unauthorised access or tampering during its transmission or storage. In order to ensure the confidentiality of the information, we can utilise either symmetric or asymmetric encryption techniques. Symmetric encryption is a cryptographic method that utilises a single key for both the encryption and decryption processes. Asymmetric encryption is a cryptographic method that utilises a pair of keys: a public key for encryption and a private key for decryption (BlastWaveConfidentiality, 2025).

The utilisation of encryption techniques facilitates the secure transmission of information within the OT domain. The encryption of communications between Remote Terminal Unit (RTU) and Supervisory Control And Data Acquisition (SCADA) systems is a capability that can be provided. Furthermore, with the integration of the Internet of Things (IoT) into the OT, encryption can be employed in the data transmitted between the IoT and the Cloud or a central control system. It is imperative that remote

access traffic is encrypted to ensure optimal security. In order to prevent unauthorised access to stored data, encryption is also a possible solution. Furthermore, encryption is imperative in the authentication and authorisation processes to ensure the protection of credentials and tokens (BlastWaveConfidentiality, 2025).

Legacy OT systems frequently encounter substantial obstacles when attempting to implement encryption due to constraints in computational capacity or obsolete firmware that is unable to support contemporary encryption standards. In order to address this issue, organisations may consider deploying encryption gateways or upgrading legacy equipment where feasible. Encryption can also result in latency, which can have a detrimental effect on time-sensitive operations. Therefore, it is imperative to optimise encryption algorithms and prioritise critical data flows in order to maintain adequate performance. The management of keys across distributed systems introduces an additional layer of complexity. The utilisation of centralised key management systems has been demonstrated to facilitate streamlined processes and enhance security measures. Furthermore, interoperability issues may arise as devices and protocols differ in their support for encryption methods. The adoption of industry-standard protocols, such as Transport Layer Security (TLS) and IEC 62351, has been shown to facilitate compatibility across systems (Jones, 2021). Finally, human error, in particular the failure to adequately configure encryption settings, has the potential to expose data to vulnerabilities. It is evident that this risk can be mitigated by the provision of adequate training and the employment of automated tools for the purpose of configuration validation (BlastWaveConfidentiality, 2025).

2.6.3 Integrity in OT

Integrity can be defined as the process of ensuring the integrity of data by preventing corruption. In the event of data being altered or rendered unreliable, the consequences for an organisation can be severe. Unauthorised access to OT assets has the potential to raise concerns regarding integrity, which could result in a compromise to the quality and safety systems. In the event of a compromise of these systems, it may be necessary to discard the product or shut down the system. In the event of compromised integrity, if this is not identified and mitigated, the result may be reputational damage and the potential endangerment of customers. In the most unfavourable of circumstances, the consequences may encompass severe impairment or harm to site personnel and equipment. This is evidenced by the Oldsmar and Stuxnet attacks (Tim Mullen, 2025; BlastWave, 2025c).

A variety of technologies are employed to support data integrity in operational environments, ensuring the accuracy, authenticity, and resilience of data against tampering. The blockchain technology provides an immutable record that enables secure data validation, for example, in the validation of sensor data logs. The employment of checksum and hashing algorithms, such as Secure Hash Algorithm (SHA)-256, serves to verify the integrity of data during both transmission and storage. Digital signatures

serve to enhance data integrity by authenticating both the source and the content. For instance, they can be used to confirm the authenticity of updates to SCADA systems. Real-time data integrity monitoring tools, such as Tripwire, facilitate the expeditious detection of unauthorised alterations to critical system files. Furthermore, Redundant Array of Independent Disks (RAID) configurations offer protection against data loss due to storage failures, as evidenced by their utilisation in fault-tolerant database storage systems (BlastWave, 2025c).

The implementation of integrity in OT systems can present significant challenges, particularly in the context of legacy systems. These devices have limited processing power and may lack security features such as the use of hashing. It has been demonstrated that complex hashing algorithms, such as SHA-256 and SHA-1, require greater processing power than their simpler counterparts, including MD5. The utilisation of simplified algorithms may potentially lead to the occurrence of hashing collisions, whereby two inputs result in identical hashes. In the context of message authentication mechanisms that utilise hashing algorithms, such as Hash-based Message Authentication Code (HMAC), there is often a requirement to manage and store secret keys. This process can present significant challenges in OT environments. In order to ensure the security of these keys, it is essential to implement effective storage methods and key rotation practices. The majority of OT systems were not designed for this purpose. Another concern regarding OT environments pertains to the issue of speed, and it has been demonstrated that hashing may indeed compromise this. Impairment of high-speed operations within an OT environment has the potential to result in production and safety issues. It is imperative that a middle ground be established between the utilisation of simpler and more complex hashing methods. To provide an illustration, in the context of systems that place significant emphasis on data integrity, it is likely that the implementation of more complex hashing algorithms would be a superior strategy. In the event of the system operating at high speeds, it is possible to use a hash that is both lighter and simpler. In scenarios where both data integrity and high-speed operation are imperative, a compromise must be made to achieve a satisfactory outcome (BlastWave, 2025c).

2.6.4 Availability in OT

Availability is defined as the assurance that systems, data and services are accessible to authorised users as and when required. This is particularly significant in OT environments, where system downtime can result in substantial disruption, safety hazards and financial losses. In this context, it may be the most important element of the Confidentiality, Integrity, and Availability (CIA) triad. Manufacturing and infrastructure systems rely heavily on uninterrupted availability. In certain instances, loss of availability could compromise the safety of consumers and producers. Depending on the type and length of the loss of availability, this can result in situations that are economically, ecologically and life-threatening. Examples of attacks on availability include the

Colonial Pipeline attack, the Springhill Memorial Hospital ransomware attack and the Sandworm attacks on Ukrainian infrastructure (Tim Mullen, 2025; BlastWave, 2025g).

A structured approach is required to ensure High Availability (HA) in OT environments. This begins with defining critical systems by identifying processes and devices that demand continuous operation, such as safety instrumented systems in a refinery. Automated failover mechanisms must be implemented to guarantee immediate switchovers; for example, redundant SCADA servers can be configured for automatic failover. HA components must be continuously health-monitored to ensure system readiness, with tools tracking the status of standby controllers. HA systems should be designed to accommodate future expansion, such as the seamless integration of additional servers, to ensure scalability. Regular maintenance, including testing redundant components during planned downtime, supports system reliability. Personnel must be properly trained to manage HA configurations and respond effectively to alerts. This training can be reinforced through failover drills involving both operators and IT teams. Finally, comprehensive documentation of failover procedures, covering both automatic and manual processes, provides essential guidance such as step-by-step instructions for activating redundant systems (BlastWave, 2025g).

Implementing HA systems is challenging due to cost, with redundancy and failover solutions expensive to deploy and maintain. Organisations should prioritise HA implementation for critical systems where downtime incurs the highest cost. The complexity of designing and maintaining HA infrastructures demands expertise and planning, which can be mitigated through the use of standardised HA solutions and personnel training. Legacy systems can lack support for modern HA features; this can be addressed by deploying intermediary devices or modernising legacy infrastructure. Maintaining data synchronisation between primary and backup systems is also challenging, requiring real-time replication and synchronisation tools. Testing and validating HA configurations can be disruptive if not carefully managed; simulation environments enable safe validation without impacting operational workflows (BlastWave, 2025g).

2.6.5 Authentication and Authorisation in OT

Authentication can be defined as the process of verifying the identity of a user, system, or device prior to authorisation of access to resources. The prevailing paradigm of OT systems has historically prioritised the assurance of operational availability over considerations of security. Consequently, the integration of security controls, such as authentication, which are customary in the IT domain, has been conspicuously absent in OT systems (BlastWave, 2025a).

Authentication is normally managed by the following 3 ways (Aveva, 2025):

1. ICS software that facilitates the management of application accounts;
2. Using Windows accounts;
3. Using authentication systems.

Authentication systems, such as Active Directory and Lightweight Directory Access Protocol (LDAP), which are colloquially designated as "authentication servers", function as a repository for and provide centralised management for all system accounts and individual user accounts. An authentication protocol is employed for all communication between authentication servers and the user or server requesting authentication (Aveva, 2025).

As previously discussed at the commencement of this section, OT environments encounter certain challenges in the implementation of authentication methods. Legacy systems frequently exhibit deficiencies in their capacity to support contemporary authentication methods. These devices frequently operate under resource constraints, with limited computational capacity that hinders the implementation of advanced authentication mechanisms. Furthermore, the implementation of sophisticated authentication procedures has the potential to result in operational interruptions, which may in turn disrupt critical workflows or lead to system downtime. The issue is further compounded by insider threats, as authenticated personnel may still pose risks without robust access control measures. The increasing necessity for remote access and monitoring introduces further authentication complexities, particularly with regard to ensuring secure connectivity. Furthermore, the risk of IT credential theft, where compromised credentials from IT networks can affect OT environments, underscores the importance of segregating IT and OT authentication systems to mitigate potential cross-domain security breaches (BlastWave, 2025a).

Authorisation can be defined as the process of granting or denying access to a network, system, or application based on the credentials of the user. As with authentication, authorisation in OT systems encounters similar issues. The majority of OT systems, particularly those of a legacy nature, were not designed to incorporate or support authorisation systems (BlastWave, 2025b).

Authorisation can be enforced by (BlastWave, 2025b):

- Grant users and systems only the minimum permissions necessary (Least Privilege);
- Implement Role-Based Access Control (RBAC);
- Combine role-based and time-based controls for additional security.
- Isolate critical systems with specific authorisation rules for each segment;
- Use Identity and Access Management (IAM) systems to streamline policy enforcement;
- Evaluate roles and permissions periodically to remove unnecessary access.

As with authentication, authorisation faces the problem of legacy systems, insider threats and operational interruptions. Moreover, the specific access requirements of temporary users, such as contractors, present a considerable challenge in the implementation of relevant policies. A further issue encountered during the implementation of a unified authorisation policy pertains to the heterogeneity of the systems and vendors in use (BlastWave, 2025b).

2.6.6 Determinism in OT

Despite the fact that determinism is not a frequently discussed topic, it is nevertheless an essential component of an OT system. Determinism is the theoretical position that the output and behaviour of a system can be predicted with a high degree of precision, based on the initial conditions and the set of rules that govern the system. In such systems, the same input will invariably yield the same output, with no variation or randomness. Deterministic systems have been shown to facilitate reliable and consistent outcomes, rendering them essential in OT. To illustrate this point, one may envisage a robotic arm engaged in an assembly line, required to execute precise movements in perfect synchrony with a conveyor belt. It is imperative to acknowledge that delays or variations in response time have the potential to culminate in production failures or safety incidents (Staff, 2025; Hartrup, 2025; Stouffer et al., 2023).

To ensure determinism in OT systems, we need to make sure the right communication protocols are used. This topic will be further discussed on Section 3.2.3. Some protocols are designed with determinism in mind, while others, especially legacy protocols, were not designed for that. Legacy OT systems were designed as simply as possible in order not to lose determinism. These legacy systems were designed very strictly and rigidly by not allowing anything to interfere with the process. Nowadays, these machines have other needs, such as increased flexibility in communication with different types of devices and the use of encryption in some cases. These new needs require communication protocols to have built-in tools, such as isochronous real-time mode, which ensures precise cycle times for industrial automation.

The implementation of determinism in OT can face some challenges, especially with legacy OT systems. These systems were not designed with determinism in mind. These systems prioritise continuous operation and availability, often at the expense of predictability and strict timing guarantees. Moreover, achieving deterministic behaviour across such heterogeneous and ageing infrastructures is technically challenging. The integration of determinism requires uniform timing, communication protocols, and processing behaviours, which are difficult to enforce in systems composed of diverse and outdated components.

2.7 Related Work

The convergence of OT and IT has transformed industrial processes, significantly improving efficiency and productivity. Yet, this increased connectivity has also introduced greater cybersecurity vulnerabilities. This subsection provides a state-of-the-art overview of cybersecurity in ICS, drawing on contemporary research to outline major developments and to identify future research directions. Furthermore, it examines the enabling technologies of Industry 5.0, their pivotal role in shaping the next industrial revolution, and the security challenges associated with their deployment.

In 2015, a survey paper reviewed and analysed standards, guidelines and best prac-

tices from governments, industrial standardisation bodies, and publications related to industrial control systems (Knowles et al., 2015). The authors reinforce the need for the creation of more standards outside the United States (US).

In 2018, a paper addressed security issues concerning IIoT (Panchal et al., 2018). According to the authors, although IIoT can increase industrial assets' performance and profit, it can also lead to significant property damage and life-threatening situations. A study of the security threats and attacks related to IIoT is made, as well as some preventive countermeasures. A penetration test when implementing IIoT and after is also recommended.

In the same year, a paper analysed vulnerabilities and attack detection in PLC (Yilmaz et al., 2018). The PLC used was Siemens S-7 1200 PLC. However, according to the author, similar implementations can be used in other models or brands. As most communication protocols in the PLC are unencrypted, the author used tools such as Wireshark to collect information about the PLC system. According to the results of the analysis, the paper emphasises that detection-based solutions are more effective than prevention-based solutions.

In 2019, a paper reviewed possible cyberattacks on ICS, discussed unresolved security issues with the existing cybersecurity solutions, presented security solutions and classified them (Asghar et al., 2019). The author also draws attention to the fact that connecting ICS to enterprise networks, to accommodate new business requirements, requires additional cybersecurity solutions. The author divides cybersecurity solutions into intrusion detection and cryptography. In intrusion detection, any divergence from the normal traffic is considered malicious traffic. In cryptography, the objective is to create a secure communication channel between ICS devices. The paper also reviews risk assessment methodologies and metrics that could help network administrators predict the potential risk of equipment failure, personal safety risk, and potential cyberattacks.

In 2020, a survey paper reviewed and analysed approaches to ICS security (Bhamare et al., 2020). The authors are alert to the security issues associated with the continued rise of integration between cloud-based computing and ICS. They also refer to the need for new schemes for intrusion detection for ICS systems at the process control level. According to the authors, a good solution is to utilise machine learning techniques.

In 2021, a paper documented the evolution of cyberattacks in ICS (Miller et al., 2021). The authors identified threat actors, initial access, impact, infrastructure and location of 43 attacks on ICS. With this data, a list of recommendations based on the observed threat trends was crafted. Some of the trends observed were a shift from internal to external threat actors, a shift from single perpetrators to organised groups, an increase in attacks in the chemical and energy sectors and an increase in the use of spear-phishing as initial access in more complex ICS that use IoT. The authors also propose a methodology for the analysis of attacks in ICS.

Still in 2021, Farsi et al., 2021 identified possible enabling technologies of Industry 5.0. The authors also created a framework that works as a roadmap for the implemen-

tation of the enabling technologies in the short, medium and long term. The roadmaps also included cultural and organisational goals. The framework underwent validation via a comprehensive literature review and surveying a diverse group of participants from various industrial sectors.

In 2022, Maddikunta et al., 2022 discussed the key enabling technologies of Industry 5.0 and their possible application and potential, and presented security and privacy challenges for the future. The future challenges identified by the authors were: security, privacy, human-robot co-working in factories, scalability, lack of skilled workforce and compliance with regulations.

Still in 2022, Leng et al., 2022 presented key enabling technologies, discussed security and privacy challenges, and built a tri-dimension system architecture for the implementation of Industry 5.0. The authors express their privacy and security concerns by saying that the human-centric Industry 5.0 will generate a lot more data related to humans, posing challenges to the cybersecurity of this industrial revolution. The architecture proposed for the implementation of Industry 5.0 by the authors is divided into enablers, implementation path and applicability.

In a recent work in 2024, Hassan et al., 2024 discussed the risks and mitigations of the adoption of Industry 5.0. The authors started by identifying the enabling technologies for Industry 5.0, followed by the identification of risks and countermeasures. The identification of risks and mitigations was done based on a review of other literature. Furthermore, the authors also categorise the risks into cybersecurity risks, workforce and training risks, operational and implementation risks, and other risks.

Overall, the reviewed literature highlights the progressive evolution of research from ICS security towards the broader paradigm of Industry 5.0 and the increased interconnectivity between IT and OT. Early studies primarily emphasised the establishment of standards and the identification of vulnerabilities in ICS and IIoT, with particular attention to detection and prevention mechanisms (Knowles et al., 2015; Panchal et al., 2018; Yilmaz et al., 2018). Subsequent works expanded the focus to include comprehensive surveys of cyberattacks, classification of countermeasures, and the integration of machine learning for intrusion detection (Asghar et al., 2019; Bhamare et al., 2020; Miller et al., 2021). More recent contributions extend beyond traditional ICS security by situating these concerns within the emerging framework of Industry 5.0, emphasising the enabling technologies, roadmaps for implementation, and the socio-technical challenges associated with human-centric industrial systems (Farsi et al., 2021; Maddikunta et al., 2022; Leng et al., 2022; Hassan et al., 2024).

Collectively, the literature reveals a fragmented industrial security landscape in which technical solutions advance in isolation from organisational, regulatory, and human-centric considerations, leaving significant opportunities for holistic approaches. A framework to define the Industry 5.0 concept and borders is necessary in order to standardise research on the subject. Also, Industry 5.0 concepts and technologies need to be studied against all the areas of cybersecurity (e.g. intrusion detection and response).

3 Dimensions of Cybersecurity

Continuing the review of the existing literature, this chapter examines several key areas of cybersecurity within OT. It further provides a foundation for Chapter 4, which will investigate these domains in the specific context of Industry 5.0. The areas discussed were selected according to the author's research interests. It should be noted that cybersecurity extends beyond the scope of this chapter; important aspects such as penetration testing and workforce training, among others, are not addressed in this work.

The mentioned cybersecurity areas are: asset inventory, vulnerability management, threat intelligence, Zero Trust Architecture (ZTA), network segmentation, industrial communication protocols, endpoint security and incident detection and response. To better organise the chapter, three sections were created to group the areas by dimension. The dimensions are Governance and Risk Management, Security Architecture and Design, and Security Operations.

3.1 Governance and Risk Management

Effective cybersecurity begins with strong governance and risk management practices that provide visibility and strategic control over digital assets and threats. Asset inventory ensures organisations maintain a comprehensive understanding of their hardware, software, and data, forming the foundation for informed decision-making. Vulnerability management builds on this by identifying and mitigating weaknesses that could be exploited by attackers, while threat intelligence empowers teams with timely insights into emerging risks and adversary tactics. Together, these elements enable proactive defence and informed prioritisation of security efforts.

3.1.1 Asset Inventory

An asset inventory in ICS/OT environments is a comprehensive inventory detailing all hardware and software/firmware components within these systems. This inventory

encompasses devices such as PLCs, sensors, actuators, HMIs, Firewalls, and associated software applications. Maintaining an accurate asset inventory is fundamental for effective cybersecurity and operational efficiency (OTBase, 2020).

In the context of Industry 5.0, the asset inventory emerges as a pivotal component within the framework of cybersecurity. It plays a crucial role in the management of threats and vulnerabilities, and in incident detection and response. Also, the number of connected devices in an ICS/OT network increases in Industry 5.0 due to the new emerging technologies. If the inventory is not well-maintained and up-to-date, it can affect the efficacy of the cybersecurity.

The creation and update of the asset inventory remains unchanged in Industry 5.0; however, the introduction of novel technologies necessitates registration, and the frequency of updates must be augmented to ensure the inventory remains up-to-date. Also, asset metrics such as carbon footprinting and energy efficiency should be present in the inventory, in accordance with the green transition.

Importance of Asset Inventory in Cybersecurity

As previously stated, asset inventory is a pivotal component of any cybersecurity framework. This is because we cannot safeguard what we don't know. Without understanding the hardware and software/firmware that we are supposed to defend, we cannot design a correct plan to protect them. By knowing the version of a software, we can identify known vulnerabilities in that software. Asset inventory is essential when doing any type of threat and vulnerability management. Also, by knowing the devices, we can plan which of them will need to send logs to our Security Information and Event Management (SIEM) infrastructure. This is useful for the detection and response of incidents. Many cybersecurity frameworks (e.g., International Organization for Standardization (ISO) 27001, National Institute of Standards and Technology (NIST), IEC 62443) require an up-to-date asset inventory for risk assessment and compliance efforts (OTBase, 2020; Mehta, 2025).

While doing threat and vulnerability management, the asset inventory is essential. With the inventory in hand, we can understand the different attack surfaces. By mapping assets to their criticality and business impact, we can prioritise risks. This is important because it makes security teams focus on the most critical risks. Also, by knowing the software/firmware versions, we can search for known vulnerabilities in these versions and apply security patches(Mehta, 2025). Another important aspect of the inventory regarding identifying risks is that it allows us to identify shadow IT/OT (CheckPoint, 2025). Shadow IT/OT is when an employee uses software/firmware or hardware not allowed by the corporate policies. These employees are creating security risks to the company by not following the policies, and an asset inventory can help identify these types of risks. We will talk more about threat and vulnerability management in Section 3.1.2.

An accurate asset inventory is also essential for incident detection and response,

as it provides security teams with visibility into all assets within an organisation's infrastructure (Libeer, 2024). When an incident occurs, the security team can identify which assets are being affected and assess the potential impact. Also, when creating the incident detection infrastructure, this inventory will be used to determine which assets should be monitored and what information we are going to monitor based on the software/firmware. We will talk more about incident detection and response in Section 3.3.2.

Creating and Updating an Asset Inventory

Establishing an asset inventory is a critical step in securing and managing IT and OT environments. The process involves identifying and documenting all assets, including hardware and software/firmware (Microminder, 2025). To identify these assets, we can use several different methods. One of the methods that can be used in an OT environment is physically going through the environment and tracing the assets. This method is not recommended as OT environments can be hazardous. Other methods, such as reviewing already existing data and analysing network packet captures, are safer and probably most efficient. Already existing data can be network diagrams, project files, system design specifications, change management records, purchase records, Address Resolution Protocol (ARP) tables, etc.

To capture network packets, we can use active or passive scanning (Attaxion, 2025). Passive scanning involves monitoring network traffic without directly interacting with devices, while active scanning involves sending probes or queries to networked devices to gather information. These types of scans can be done using tools such as Wireshark, Nmap and Nessus. In ICS/OT environments, active scanning can be considered harmful as it can create unexpected network congestion and potential disruptions.

To create the actual asset inventory, we need a place to store this type of information. Tools to centralise asset records can be as simple as an Excel Sheet or some service that provides Configuration Management Databases like ServiceNow (ServiceNow, 2025).

Each asset stored should be recorded with key attributes. These key attributes vary from environment to environment; however, some are a standard in almost every asset inventory (Microminder, 2025). Below is a list of some standard attributes:

- Asset Identifier (ID)
- Asset Name
- Asset Type
- Location
- Manufacturer
- Model
- Serial Number
- Internet Protocol (IP) Address
- Media Access Control (MAC) Address
- Software Version
- Firmware Version
- Installation Date
- Last Maintenance Date
- Maintenance Schedule
- Criticality
- Responsible Party
- Status

Updating regularly the asset inventory is a vital step in ensuring that the organisation's security posture remains robust against evolving threats (Microminder, 2025). Setting a monthly update schedule can help. Also, we must ensure that change management procedures include updating the asset inventory. Assets should be added or removed as they are connected or disconnected from the plant network.

The asset inventory is one of the most important pieces of information that an attacker can get their hands on. The inventory is the treasure map of the network for the attacker. The security of the asset inventory is imperative. It should follow security best practices when it comes to confidentiality, integrity, availability, authentication and authorisation.

3.1.2 Vulnerability Management

In Industry 4.0, the convergence of OT and IT has amplified the exposure of critical infrastructure to cyber threats, necessitating robust vulnerability management strategies. In Industry 5.0, the same problem is amplified by introducing many new technologies.

In Table 3.1, we define the terms: vulnerability, threat and risk. These terms will be used a lot in this section.

Table 3.1: *Definitions of Vulnerability, Threat and Risk* (*Kidd, 2025*).

Vulnerability	Threat	Risk
These are weaknesses or gaps in an organisation's people, processes or technology that could be exploited. However, they only pose a risk when there is a threat to exploit them (Kidd, 2025).	Potential malicious actors, events, or circumstances. These could be intentional or unintentional. They could exploit vulnerabilities to cause harm or disruption (Kidd, 2025).	The possibility of loss or destruction when a risk uses a weakness is judged by looking at how likely it is and the effect it would have. Good security management depends on constantly finding, ranking and reducing the most important dangers (Kidd, 2025).

Traditional IT-centric vulnerability management approaches often prove inadequate for OT systems due to their distinct operational requirements and risk profiles. The strategies that focus too much on Common Vulnerability Scoring System (CVSS) and frequent patching fall short. Vulnerabilities must be assessed based on the impact on the physical process and the safety, not just the technical aspect (Dragos Inc., 2024a). For example, imagine a vulnerability in OT systems that causes Denial of Service (DoS). Now, let's imagine that this vulnerability affects two different machines, one that generates 10000€ per hour and another that only generates 5000€ per hour. If this vulnerability is exploited, causing downtime on the machines, we can say for certain that the impact on business is greater on the first machine. This means that despite being the same vulnerability and having the same CVSS score, this vulnerability can cause a greater impact on one machine.

The vulnerability assessment should be based on risk and should not be too focused

on technical scores (Dragos Inc., 2024a). Risk should be the combination of threat, vulnerability, probability and impact (Ribeiro et al., 2024). Each organisation's needs are unique, and not every vulnerability's impact is the same in every environment (Dragos Inc., 2024a). The impact can make all the difference when classifying the risk of a vulnerability. Ultimately, the classification of risk should always be done in business terms. That is what the chief officers want to know. The impact of a vulnerability on the business, the cost if exploited, and how the company is doing compared to the competitors are examples of important questions when doing vulnerability management. If the patching of a vulnerability costs more than if it is exploited, the chief officers are probably not going to approve the patching.

Generally, OT systems need much higher uptime than IT systems (Dragos Inc., 2024a). Turning off OT systems greatly impacts business and can even be hazardous in some environments. Patching systems should be done first in test environments without any impact on production (Livingston, 2022). If the next maintenance phase isn't closed, compensating controls can sometimes be used to help lower the risk. Using the Purdue Model as an example, the higher levels, which are mainly composed of IT systems, should be patched actively. Also, patching the lower levels, which are mainly composed of OT systems, is limited.

OT Vulnerability Management Process

The vulnerability management process in OT needs to be risk-based and not only based on technical scores, such as CVSS. Initially, CVSS scores can be used to understand the capabilities of the vulnerability, but this score should be reevaluated according to the threat, impact and probability (Dragos Inc., 2024a).

Asset inventory is very helpful in this risk-based process (Dragos Inc., 2024a). It helps with identifying critical assets, which is useful to understand the possible impact and probability of the vulnerability. As previously explained, the same vulnerability can cause different impacts on different machines. The same applies to probability.

Having the network topology also helps with the vulnerability management process (Dragos Inc., 2024a), as it helps identifying data communication flows, which can be potential attack paths. Threat intelligence helps to prioritise vulnerabilities that are more often targeted by adversaries. Threat intelligence will be discussed in further detail in Section 3.1.3.

By having an asset inventory, network topology and a threat intelligence feed, we can start the OT vulnerability management process. The following list provides a step-by-step process:

1. Map your network topology;
2. Build the asset inventory;
3. Determine if active and/or passive scanning will be used;
4. Assess each vulnerability's risk based on the specific environment;
5. Determine if vulnerability can and should be remediated;

6. Verify if the remediation was successful;
7. Continually monitor for new vulnerabilities

In the next section, active and passive vulnerability scanning will be discussed, along with the problems and benefits of each.

Operational Risks of Vulnerability Scanning

As already described in Section 3.1.1, scanning can be passive and active. Passive scanning does not interact directly with devices and systems, while active scanning does. Active scanning can be a problem, especially for legacy OT systems.

Passive scanning does not introduce packets into the network and does not interfere with assets. This eliminates the risk of disrupting the operation of OT assets. Usually, passive scanning uses a network interface in promiscuous mode to capture network packets. This allows the scanners to collect information about the hosts. The downside of this technique is the limited information that is gathered (Attaxion, 2025).

Active scanning introduces data packets into the network. These are called probes, and they gather information from the hosts. The upside of this technique is that the amount of information we can gather is much higher. The downside is that on the lower levels of an OT environment, it can interfere with the operation. If active scanning in the lower levels is being considered, then it should be first tested in a testing environment (Attaxion, 2025).

Some tools that can be used for vulnerability management in OT are Nessus from Tenable, Qualys, Wireshark, InsightVM from Rapid7 and CrowdStrike (Gartner, 2025).

3.1.3 Threat Intelligence

Threat intelligence involves the collection, processing, analysis and dissemination of information about active or emerging cyber threats, as well as the integration of this information. Its primary purpose is to identify malicious cyber activities and adversaries, and to make this information accessible to decision-makers within an organisation. OT threat intelligence addresses the unique challenges and requirements of OT environments. Such systems are integral to critical infrastructure, including power plants, manufacturing facilities, gas pipelines and water treatment plants (Dragos Inc., 2024b).

Threat intelligence customises itself for the specific use case and security demands of a particular threat and customer environment. Although there are some similarities between operational networks and traditional IT in terms of cybersecurity approaches, the two are not synonymous. The threat landscape, consequences of incidents and decision-making calculus are not the same for IT and OT (Caltagirone, 2018).

Industrial enterprises integrate diverse intelligence streams to achieve a holistic perspective on cyber threats (Dragos Inc., 2024b):

- **Internal IT telemetry:** Useful for the early detection of risks before they impact OT networks, though inadequate in isolation.
- **OT-specific network surveillance:** Indispensable for identifying threats within OT infrastructures, with specialised platforms such as Dragos playing a pivotal role.
- **Collaborative intelligence sharing:** Exchanging proprietary data with trusted partners via formal arrangements and initiatives extends situational awareness and detection reach.
- **External intelligence feeds:** Sector-focused insights from commercial threat intelligence vendors and regulatory authorities contribute valuable contextual depth.

The threat intelligence context provides the necessary relevance around any threat. It is important to note that not all threats are of equal severity. The impact of threats is not uniform; indeed, some only affect specific industries, verticals, or geographic regions. A proportion of the identified threats is only of relevance to certain technological domains. Threats manifest in diverse forms, independent of their particular capabilities and infrastructure. The threat intelligence context is one such factor that addresses these and other issues, enabling defenders to determine whether they should be concerned and take action promptly. Furthermore, in the context of threat detection, the utilisation of threat intelligence facilitates quick prioritisation and more efficacious incident response, accompanied by a reduction in the time required for mitigation (Caltagirone, 2018).

Threat Intelligence Action Recommendations

Threat Intelligence delivers tailored technical and policy recommendations based on the specific threat, its characteristics, and its potential impact. Its scope spans from technical intelligence that supports detection and threat-hunting activities to strategic insights designed for senior executives or board-level briefings (Caltagirone, 2018).

Typically, such recommendations include detective guidance, such as technical indicators or signatures of malicious activity, which assist in identifying breaches within an environment. They may also provide policy guidance aimed at protecting the organisation from potential disruptions, thereby contributing to the prevention of threats.

In addition, threat intelligence often incorporates detailed descriptions of adversary behaviours, enabling proactive hunting for similar patterns. It may also suggest specific data collection practices to enhance the effectiveness of detection measures. Finally, it provides information on the scope and potential impact of the threat, supporting risk-based strategic decision-making at the organisational level.

Indicator of Compromise (IOC) are technical elements of information that are utilised to facilitate threat detection, constituting a component of threat intelligence action. It is a common practice for IOC to include IP addresses, domain names, file names, and file hashes, among other elements. The purpose of IOC is to facilitate the identification of compromises by way of comparison with organisational logs. These feeds are

typically utilised by SIEM platforms to generate alerts for a Security Operation Center (SOC), analogous to the generation of anti-virus alerts. It is important to note that indicators of compromise are not equivalent to threat intelligence. While they are indeed a component of threat intelligence, they do not, in and of themselves, contribute significantly to the value they offer. This is a key point to consider when evaluating the marketing messages of certain providers. Conversely, in order to facilitate comprehension amongst defenders, threat intelligence must be rendered with the assistance of full-formed threat intelligence, which is to be understood as a contextualised representation of IOC (Caltagirone, 2018).

Threat Intelligence Cycle

In the realm of OT-specific threat intelligence, the intelligence cycle and the interplay between data, information, and intelligence are closely interlinked. The intelligence cycle, comprising Planning and Direction, Collection, Processing, Analysis, and Dissemination, serves to convert raw data from OT environments into actionable intelligence (Dragos Inc., 2024b).

In Figure 3.1, we see all the phases of threat intelligence. The initial phase, entitled 'planning and direction', is the stage at which the objectives of the threat intelligence programme are established. Collection is defined as the process of gathering information to address intelligence requirements. Processing can be defined as the transformation of collected information into a format that is usable by the organisation. Analysis is a human process that converts processed information into intelligence, which can inform decisions. The dissemination process entails the effective transmission of the final intelligence output to the designated recipients (THE RECORDED FUTURE, 2025).

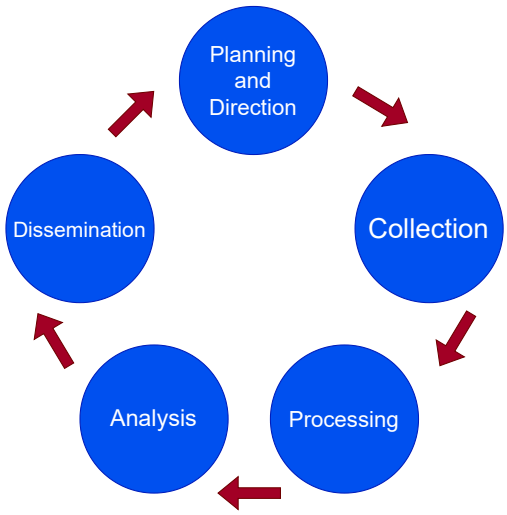

Figure 3.1: *Threat intelligence cycle* (*THE RECORDED FUTURE, 2025*).

The process commences with the collection of data from the operational environment, including OT-specific signals and network traffic. This raw data is subsequently processed into meaningful information, which is then examined in relation to the spe-

cific risks affecting the OT environment to generate intelligence. The intelligence cycle ensures that such intelligence is not only precise and pertinent but also effectively embedded within the organisation's security operations, thereby delivering actionable insights to support decision-making and strengthen the protection of critical infrastructure (Dragos Inc., 2024b).

Measuring Threat Intelligence Quality and Impact

Bad threat intelligence can be more damaging than having none at all. Substandard intelligence fosters poor decision-making, squanders valuable resources, and may produce consequences detrimental to business and operational integrity. It is therefore essential for organisations to rigorously assess potential threat intelligence providers, selecting only those committed to delivering consistently high-quality outputs (Caltagirone, 2018).

The quality of threat intelligence is best assessed across four principal dimensions: completeness, accuracy, relevance, and timeliness. Table 3.2 shows the definition of these concepts. Intelligence that fails to meet any of these criteria is unlikely to fulfil operational needs, risks consuming time and resources inefficiently, and may even have adverse effects (Caltagirone, 2018).

Table 3.2: *Threat intelligence should be measured through four dimensions: completeness, accuracy, relevance and timeliness* (*Caltagirone, 2018*).

Completeness	Accuracy	Relevance	Timeliness
Threat intelligence must provide sufficient detail to enable a proper response.	Inaccurate threat intelligence is worse than no threat intelligence, and any quality threat intelligence must be accurate.	Threat intelligence must address only relevant threats to the organisation and be delivered in a method that allows for effective action.	Threat intelligence must be produced and delivered quickly so that it can be used fast enough to make a difference.

Quantifying the impact and Return on Invenstment (ROI) of threat intelligence is inherently complex, as is the case with many security programme components. Nevertheless, two practical metrics offer considerable value in such evaluation: adversary dwell time and time to recovery. When effectively integrated into security operations, high-quality threat intelligence should contribute to the reduction of both (Caltagirone, 2018).

3.2 Security Architecture and Design

A resilient cybersecurity posture depends on thoughtful architectural design and strategic segmentation of systems. ZTA challenges traditional perimeter-based models by enforcing strict identity verification and access controls across all users and devices. Network segmentation complements this by dividing infrastructure into isolated zones,

limiting lateral movement and containing potential breaches. In industrial environments, secure communication protocols such as Modbus, Open Platform Communications Unified Architecture (OPC UA), and others are critical for safeguarding operational technology and ensuring the integrity of machine-to-machine interactions. These design principles collectively reduce attack surfaces and enhance systemic resilience.

3.2.1 Zero Trust Architecture

In the contemporary landscape, where cyberattacks are becoming both more sophisticated and widespread, organisations are acknowledging the imperative to enhance their cybersecurity frameworks. The effort under discussion is centred on two complementary approaches: the ZTA model and the Principle of Least Privilege. These approaches have been designed to safeguard devices, users and data from unauthorised access. While both of these approaches are critical components within a comprehensive security strategy, ZTA focuses on continuous verification and the assumption that threats may exist both inside and outside the network, whereas Least Privilege restricts user access rights to the minimum required for task execution. It is asserted that, when considered collectively, they offer a multifaceted protective measure against a threat landscape that is evolving and which can target both traditional systems and mobile platforms (Vigo, 2025; StrongDM Team, 2025).

ZTA is a security model predicated on the assumption of a complete absence of trust between disparate entities, with strict access controls being established in order to mitigate risk. In order to ensure that only authorised users are granted access to resources, it is necessary to verify each access request (StrongDM Team, 2025).

In the context of ZTA, it is imperative that all users and devices undergo rigorous authentication and authorisation procedures prior to being granted access to any system resources. It is evident that even in the event of an attacker successfully obtaining a user's credentials, they will be unable to access any resources without undergoing a verification process (StrongDM Team, 2025). ZTA incorporates several related components, including robust authentication methods, the implementation of access and authorisation controls, network segmentation, and the logging and monitoring of sessions (Dragos, 2024). As previously mentioned, the ZTA model is characterised by a comprehensive monitoring and analysis of all user activity, facilitating rapid detection of any suspicious behaviour. For that to happen, we need full TLS/Secure Sockets Layer (SSL) decryption and inspection capabilities, so malware and sensitive data transfers can be detected (A10 Networks, 2025). This approach enables security teams to respond expeditiously to any potential threats, thereby minimising the damage caused by cyberattacks (StrongDM Team, 2025). Figure 3.2 illustrates the key concepts talked about in this paragraph: always verify identities, robust authentication, access controls, logging and monitoring, network segmentation, Principle of Least Privilege (PoLP), full TLS/SSL visibility and inspection, and centralised management of all the concepts.

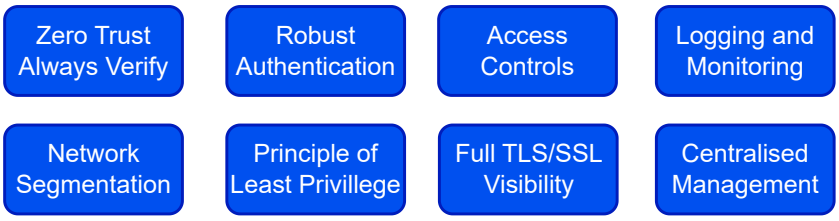

Figure 3.2: *Principle concepts of the ZTA model* (*A10 Networks, 2025*; *StrongDM Team, 2025*; *Dragos, 2024*).

To illustrate the practical implementation of ZTA, one may consider a scenario in which a technician is required to access a PLC to make modifications to the program instructions. Before access is granted, the technician must authenticate first. This can be done with something like a badge or even through a username and password (Martinez, 2025). The use of Multifactor Authentication (MFA) is also of significant benefit and forms a fundamental component of any effective ZTA. Examples of MFA include an Short Message Service (SMS) text, a voice call or an email message. To illustrate this point, consider a scenario in which a technician's badge is stolen. In such an event, the individual responsible for the theft would be unable to access the PLC due to the MFA challenge. In order to proceed, it is imperative that the user's account, having been successfully authenticated, should also pass the requisite authorisation check. It is imperative that the technician in question possesses the requisite permissions to facilitate the update of the PLC program. Even if the user is authorised, that does not mean that all the authorised users will have the same available permissions on the PLC. It should be noted that alternative access control policies may also be in place, such as the implementation of time-based or day-based restrictions on access to the PLC. In ZTA, the aforementioned steps should be subject to monitoring and logging. The operations in question should be subjected to close monitoring in order to identify any potential anomalies, such as a technician authenticating at an uncommon hour or day.

The PoLP is predicated on the principle that users should only be granted the minimum level of access required for their specific tasks, with the objective being to ensure a greater degree of control over data and systems. The PoLP is predicated on the concept that solely those users whose identity has been verified have the necessary permissions to execute jobs within certain systems, applications, data and other assets (Vaideeswaran, 2025).

The PoLP functions through the limitation of data, resources, applications, and application functions, such that they are accessible only to the extent that is required by a user or entity to execute their specific task or workflow. In the absence of the principle of least privilege, organisations are susceptible to the creation of over-privileged users or entities. This has the potential to increase the likelihood of breaches and the misuse of critical systems and data (Alto, 2025).

The PoLP is a key factor in enhancing an organisation's security posture. By implementing this principle, organisations can achieve a substantial reduction in their attack surface and the risk of malware propagation (Alto, 2025).

To reiterate the preceding example, if a technician were to access a PLC with the intention of updating the instructions of a program, a more comprehensive understanding of the PoLP would be achieved. In addition, the user will be required to authenticate themselves. During the authentication process, authorisation will be checked. The technician is granted access only to the specific PLC under their maintenance schedule and only during authorised time windows. Despite the user's access to the PLC, it is conceivable that he may not be granted complete access to all of its functions. In this particular instance, the technician is a PLC programmer, and the sole interaction he has with the PLC is to update the PLC program. It is imperative to acknowledge that the access management team is exclusively responsible for authorising access to a particular function of the PLC. In the event of a compromise of the technician's credentials and MFA, the malicious actor will be able to execute a very specific set of tasks. This serves to restrict the actions available to the malicious actor. This is merely an illustration of PoLP being employed to restrict the user's access.

As evidenced by both practical examples, there are a considerable number of similarities between ZTA and PoLP. The ZTA is a security model; in contrast, the PoLP is an access control practice (Vigo, 2025). The fundamental difference between the two can be attributed to the range of their respective scopes (Avigdor Book, 2023). ZTA uses multiple security practices like MFA, PoLP and micro-segmentation (Avigdor Book, 2023).

The prevailing security models have traditionally concentrated on perimeter-based defence mechanisms, such as firewalls and antivirus software. Whilst these approaches have been successful in the past, they are no longer sufficient in the current threat landscape. It is evident that cybercriminals have become increasingly sophisticated in their methods, and perimeter defences are no longer adequate in terms of counteracting the constantly evolving threats (StrongDM Team, 2025; Tullman-Botzer, 2025b).

A significant limitation of conventional security models is their assumption that threats are exclusively external to an organisation. However, this is no longer the case, as the prevalence of insider threats is on the rise. A further issue with conventional security models is that they have the capacity to create a false sense of security. It is evident that determined cybercriminals have the capability to circumvent perimeter defences. Following their successful infiltration of an organisation's network, these individuals can then proceed to navigate freely across the system and gain unauthorised access to sensitive data or systems (StrongDM Team, 2025).

In light of the limitations exhibited by conventional security paradigms, there has been an emergent tendency to adopt a ZTA and the PoLP. It is acknowledged by these security approaches that threats may originate from both internal and external sources within an organisation (StrongDM Team, 2025; Tullman-Botzer, 2025b).

3.2.2 Network Segmentation

Organisations can implement OT network segmentation as a key security practice. This process is used to block attackers and unauthorised users from accessing sensitive data and devices (Fortinet, 2025b).

Legacy OT networks were not designed with restrictions in mind, particularly in the case of networks running in an isolated and air-gapped environment with no external connections. Many OT environments adopt an 'implicit trust' approach to users and devices, permitting control and administration of any digital asset in the network from any location. This, regardless of the criticality of the asset to the organisation's operation or success, renders these traditional OT networks a highly attractive proposition to cybercriminals with a strong motivation to perpetrate crime (Fortinet, 2025b).

It has been suggested that segmenting an OT network into smaller sections, called zones, could give security professionals much more control and visibility into the organisation's networks, increasing the overall security of the network and assets. Cybersecurity industry experts say that network segmentation is one of the most effective methods for protecting operational technology from both internal and external threats (Fortinet, 2025b; Cybersecurity & Infrastructure Security Agency, 2025).

Zones and Conduits

The networks should be divided into a series of functional segments or "zones" (which may include sub-zones). Each zone should only be accessible by authorised and verified devices, applications, and users. For this aspect, conduits, typically firewalls, are needed. These conduits define the zone's boundaries and enable essential data and applications to move securely from one zone to another (Fortinet, 2025b).

A zone should contain a group of assets that share common security requirements. A conduit allows communication between and inside zones. As mentioned above, zones can have sub-zones. However, conduits cannot have sub-conduits. A zone can have more than one conduit. For example, the assets inside a zone use one or more conduits to communicate. A single conduit cannot traverse multiple zones. However, a single conduit can be used by two or more zones to communicate with each other (Kon, 2025). An example of the concept is in Figure Figure 3.3.

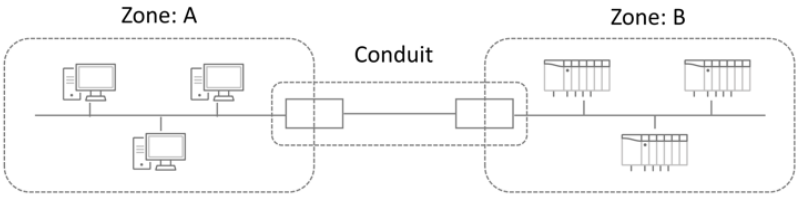

Figure 3.3: *Schematic representation of zones and conduits. Source: Trend Micro, 2020.*

Guidance on the definition of zones and conduits can be found in the IEC 62443, which employs the Purdue Reference Model. This model is employed to describe the

flow of data through industrial networks, and it divides the system into different hierarchical levels based on their response time and function. Many organisations choose to mirror the concepts of the Purdue levels into their network architectures, but care needs to be taken, especially with the new technologies that came with Industry 4.0 and 5.0 (Fortinet, 2025b).

Figure Figure 3.4 exemplifies a high-level architecture divided into zones and sub-zones, based on the Purdue Reference Model. The figure shows an architecture that is divided into several levels (Depending on the reference, the Purdue Reference Model might have one more level above 4). These levels are divided based on function. The levels can also be divided into one or more sub-zones, which are represented in green. The different zones and sub-zones are connected through the conduits, which are represented in blue. The absence of representation of conduits inside the zones and sub-zones is to facilitate the comprehension of the figure.

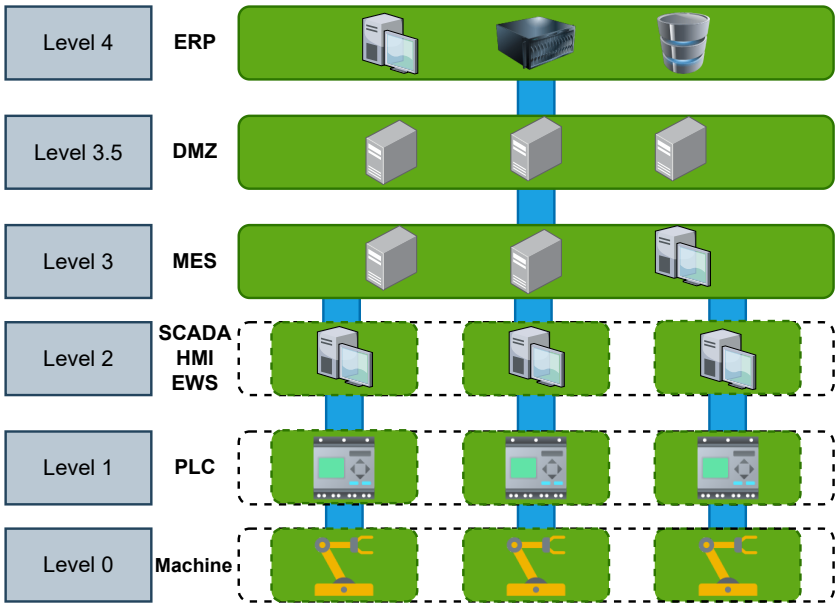

Figure 3.4: *Example High-level architecture divided into zones and sub-zones. Adapted from: Trend Micro, 2020.*

Air Gap

Air gap is a method of physically isolating a computer or network from other networks to prevent unauthorised access and data breaches. This process creates a literal "air gap" between the secured network and any other unsecured networks. Air gaps are an isolation method crucial for data integrity and security, and they can be deployed across various industries. The principle behind air gapping is that a device or network not connected to the internet or other systems cannot be hacked remotely. However, despite its efficacy, there is still concern over whether the air gap will die out as a method as new threats and technologies emerge (Fortinet, 2025c).

There are three types of air gap:

1. Physical Isolation;
2. Operational isolation;
3. Electronic isolation.

Physical air gaps, as the name suggests, involve physically isolating a computer or network. The isolated systems do not have any network interfaces connected to external networks. To transfer data from or to an air-gapped system should be done manually, with Universal Serial Bus (USB) drives, for example (Fortinet, 2025c).

Operationally isolated systems use procedures and human intervention to control and limit access. This can be done by using firewalls, Virtual Private Network (VPN) and monitoring technologies, like Endpoint Detection and Response (EDR), that can regulate data flow and the security of the devices (Fortinet, 2025c).

Electronic isolation involves isolating systems at an electronic level. This is usually done by using data diodes, which are unidirectional network gateways. This type of gateway will allow data to flow in only one direction, making it physically impossible to flow data in the opposite direction (Fortinet, 2025c). Data diodes can be particularly useful when talking about communications between OT and IT. The flow of the data should be from OT to IT and never the reverse. IT should not be able to start "conversations" with the OT.

Air gaps are employed in a variety of industries, including defence, finance and healthcare, for a number of reasons. These include the protection of sensitive data and external threats. Military and defence systems use air gaps to secure classified information, ensuring that highly sensitive operations and communications remain confidential and protected. Financial institutions implement air gaps as part of compliance standards to protect critical financial data and maintain operational integrity. In the healthcare sector, the implementation of air gaps is crucial for safeguarding medical records and sensitive health data, to prevent breaches that could result in violations of privacy laws, such as Health Insurance Portability and Accountability Act (HIPAA), and severe personal implications for patients (Fortinet, 2025c).

The benefits of adopting air gaps include increased threat mitigation, regulatory and audit compliance, and data integrity and control. However, the implementation of air gaps may be challenging. Normally, it requires separate physical infrastructure and that increases costs. Updating and patching air-gapped devices is difficult because they cannot connect to the internet (Fortinet, 2025c).

One thing that air-gapped systems do not defend against is insider threats. Even with robust physical security measures, the human factor can be a weak link. Insider threats, whether malicious or accidental, can compromise the integrity of an air-gapped system. This is why ensuring that only authorised personnel have access to air-gapped systems is crucial (Fortinet, 2025c).

3.2.3 Industrial Communication Protocols

Among specific networks, Process Field Network (PROFINET) leads with a 23% market share, followed by EtherNet/IP at 21%, and EtherCAT at 16% (Jansson, 2025).

Most used industrial ethernet protocols:

- PROFINET (23%)
- EtherNet/IP (21%)
- EtherCAT (16%)
- Modbus Transmission Control Protocol (TCP) (4%)

Most used fieldbus protocols:

- Process Field Bus (PROFIBUS) Decentralised Peripherals (DP) (7%)
- Modbus RTU (4%)

The increasing dominance of Industrial Ethernet highlights the need for higher-speed, lower-latency communication, which is critical for automation, robotics, and Industry 4.0 applications. As factories and industrial facilities integrate more connected devices, selecting the right networking technology ensures seamless data exchange and operational efficiency.

Moreover, the market trends impact long-term operational decisions. The decline of traditional fieldbuses suggests a shift away from legacy systems towards more scalable and flexible Ethernet-based solutions. Although wireless technologies have seen a slight decrease in market share, their role in industrial communication remains relevant, particularly in applications where wired connections are impractical.

Industrial Ethernet and Fieldbus

Industrial Ethernet is the same Ethernet that is used in homes, offices and data centres, with 2 major differences. The first is that in the industrial implementation, Ethernet is supplemented by industrial communication protocols designed to handle industrial processes such as PROFINET, EtherNet/IP and EtherCAT (Fluke, 2025).

Fieldbus is a group of protocols that are commonly used in an industrial environment that was standardised in IEC 61158. Fieldbus connections are similar to Ethernet as they allow for multiple field devices to connect to a single connection point, which will then connect to the process controller. Fieldbus protocols include PROFIBUS, Modbus RTU and DeviceNet (Goetzman, 2023).

Prior to 2018, fieldbus protocols held a dominant position in the market. However, following this date, industrial Ethernet gained significant ground, becoming the dominant technology. The transition to industrial Ethernet is driven by the necessity for high performance and the integration of factory installations with IT/IoT systems. Nowadays, industrial Ethernet protocols are faster than Fieldbus protocols and also allow for a flexible network topology. Some Ethernet protocols are now deterministic, which was a common problem with these types of protocols. Being deterministic means that

the protocol guarantees that data packets sent across the network will arrive at their destination port within a specified fixed time frame. Deterministic protocols are essential in industrial applications as a delayed packet can shut down an entire production system or injure workers (HMS, 2025).

Characteristics of Industrial Communication Protocols

In this section, the key characteristics of various industrial communication protocols will be analysed, focusing on authentication, availability, integrity, confidentiality, and determinism. Each protocol is assessed to determine its security mechanisms, redundancy features, and ability to support real-time communication. Understanding these characteristics is essential for evaluating their suitability in industrial automation environments, where reliability and security are paramount.

PROFINET is an industrial Ethernet protocol designed for real-time communication in automation systems. It is characterised by several key security and performance features, including authentication, availability, integrity, confidentiality, and deterministic data transmission. Authentication is ensured via cryptographic identity certificates. Availability is prioritised through system robustness and real-time communication mechanisms. Integrity is maintained through cryptographic checksums to prevent data manipulation. Confidentiality is supported but often deprioritised in favour of real-time performance. Finally, PROFINET achieves determinism through its isochronous real-time mode, which ensures precise cycle times for industrial automation (UK, 2024).

EtherNet/IP (Ethernet Industrial Protocol) is an industrial communication protocol that extends the Common Industrial Protocol (CIP) over standard Ethernet.EtherNet/IP supports both implicit and explicit communication. It provides scalability, flexibility, and integration with existing Ethernet networks but may require enhancements like Time-Sensitive Networking (TSN) for strict real-time applications. EtherNet/IP implements CIP Security, which provides authentication, integrity, and confidentiality via TLS and Datagram Transport Layer Security (DTLS) encryption. These mechanisms ensure that data is only accessible to authorised devices and protected from tampering. Availability is supported through Device Level Ring (DLR) redundancy. Regarding determinism, EtherNet/IP prioritises traffic but does not guarantee strict real-time performance without additional measures like TSN (SANS, 2024; *CIP Security™ | Common Industrial Protocol | ODVA Technologies* 2024).

EtherCAT (Ethernet for Control Automation Technology) is a high-performance industrial Ethernet protocol that prioritises speed and determinism, achieved through its unique method of processing data on the fly (B. Automation, 2024). Its architecture enables each node in the network to extract and insert data from a single contin-

uous frame without buffering, thereby supporting high availability and precise synchronisation through mechanisms such as cable redundancy and distributed clocks (Community, 2023). However, EtherCAT's design is primarily optimised for speed and determinism rather than security; it does not incorporate native mechanisms for authentication, integrity, or confidentiality. As a result, in applications where security is critical, additional measures-such as secure gateways, network segmentation, or dedicated encryption protocols-must be implemented (Toker et al., 2021; Community, 2023).

Modbus TCP is a widely adopted protocol in industrial automation, facilitating communication between devices over TCP/IP networks (Modbus Organization, n.d.). Despite its simplicity and ease of implementation, it lacks inherent security features, rendering it vulnerable to various cyber threats, including eavesdropping, data tampering, and unauthorised access. To address these vulnerabilities, recent research has proposed security enhancements such as implementing message authentication codes to verify the integrity and authenticity of messages. Additionally, employing TLS can provide encryption to ensure data confidentiality during transmission (SANS, 2024; Nardone et al., 2016).

PROFIBUS DP is a high-speed serial fieldbus standard widely used in industrial automation to connect sensors, actuators, and I/O modules to centralised controllers. It provides deterministic communication through cyclic data exchange, ensuring precise timing for control applications. Availability is maintained by its master-slave architecture, which reduces network congestion and optimises data flow. However, security was not a primary design focus, and PROFIBUS DP lacks built-in authentication, integrity verification, or confidentiality mechanisms. As a result, it is vulnerable to unauthorised access and DoS attacks. To mitigate these risks, best practices such as network segmentation, intrusion detection systems, and strict access control policies should be implemented (Watson et al., 2017; Bütün, 2022).

Modbus RTU is a serial communication protocol widely used in industrial automation (Modbus Organization, n.d.). It operates on a master-slave model over Recommended Standard (RS)-232 or RS-485. RS-232 is a point-to-point serial communication standard commonly used for connecting industrial devices (Nardone et al., 2016). RS-485 is a more advanced serial communication standard that supports multi-drop (multiple devices on the same bus) and long-distance communication (up to 1,200 metres) (Nardone et al., 2016). Modbus RTU provides deterministic communication by ensuring that only one master device controls data transmission at a time, eliminating data collisions. However, security was not a design priority, and the protocol lacks authentication, availability, integrity verification, and confidentiality mechanisms (SANS, 2024; Nardone et al., 2016).

802.11 Wi-Fi is a widely used wireless networking standard that provides flexible connectivity for industrial and commercial applications. In terms of security, IEEE 802.11 incorporates multiple mechanisms to ensure authentication, integrity, confidentiality, and availability. Authentication is managed through protocols such as Wi-Fi Protected Access (WPA), WPA2, and the latest WPA3, which use mechanisms like Pre-Shared Keys and Extensible Authentication Protocol to verify device identities. Authorisation can be ensured by using Remote Authentication Dial-In User Service (RADIUS) and RADIUS accounting (Cisco, 2025). Data integrity and confidentiality are enforced through encryption techniques, with WPA2 implementing Advanced Encryption Standard (AES) and WPA3 introducing stronger cryptographic measures, including System Architecture Evolution (SAE) to resist brute-force attacks (Portnox, 2025). Availability is a challenge in wireless networks due to potential DoS attacks, such as flooding authentication requests or jamming signals to disrupt communication (Ijemaru et al., 2018). Regarding determinism, IEEE 802.11 is inherently non-deterministic due to its contention-based access mechanism, which introduces variable latency. However, some determinism could be achieved by integrating it with TSN (Cavalcanti et al., 2022).

OPC UA is a platform-independent, service-oriented architecture designed for secure and reliable industrial communication. Security in OPC UA is multi-faceted, encompassing user authentication, application authentication, message integrity, and confidentiality. User authentication is achieved by clients transmitting user credentials to servers during session establishment, allowing servers to verify user identities. Application authentication involves the exchange of digitally signed X.509 certificates between clients and servers, ensuring that only trusted applications communicate within the network. Authorisation to resources is managed by the Authorisation Services that provide access tokens to clients on behalf of users that they pass to a server to be granted access to resources (OPC Foundation, 2025b). The Authorisation Services allow for the delegation of user authentication, user management and the assignment of users to roles to an external central entity (e.g. an OAuth2 server) (OPC Foundation, 2025a). Message integrity and confidentiality are maintained through the use of asymmetric encryption and digital signatures, preventing unauthorised access and tampering during data transmission. Availability in OPC UA is supported through redundancy mechanisms that ensure continuous operation even in the event of failures. OPC UA defines multiple redundancy models, including server redundancy and network redundancy, to enhance system reliability. Server redundancy enables automatic failover between primary and backup servers, ensuring minimal disruption in data exchange. Network redundancy, supported by features such as parallel connections and failover mechanisms, maintains communication stability in case of network failures. In terms of determinism, OPC UA's integration with TSN is a significant advancement. TSN is a set of IEEE standards that enhance Ethernet networks with features like time synchronisation and traffic scheduling, enabling deterministic data delivery (Founda-

tion, 2024a; Foundation, 2024c; Foundation, 2024b; B. I. Automation, 2024).

WirelessHART is an industrial wireless protocol designed for secure and reliable communication in process automation networks. Security is a core component, with authentication, integrity, and confidentiality enforced through AES-128 encryption, session keys, and message integrity checks. Authentication and Authorisation are managed using unique join keys that ensure only authorised devices enter the network. A WirelessHART gateway and the wireless sensors joining the network must be configured to control which devices are allowed to access the network. Availability is maintained through mesh networking, where devices serve as both sensors and routers, providing redundant communication paths to counter interference or node failures. Determinism is achieved via scheduled time slots for data transmission, minimising latency and ensuring reliable operation in industrial environments (Jim Cobb, 2024).

Modbus TCP Security enhances the traditional Modbus TCP protocol by integrating TLS to provide authentication, integrity, and confidentiality. Authentication is managed through X.509 certificates, ensuring secure identification of devices. Authorisation can be ensured by using the MODBUS Application Protocol (MBAP) protocol. The MBAP protocol provides the capability to perform role-based client authorisation. Data integrity and confidentiality are achieved using TLS encryption, protecting communication from interception and tampering. Availability is maintained by leveraging redundancy mechanisms and secure session handling. However, determinism remains a challenge due to the overhead introduced by encryption (Organization, 2024; Martins et al., 2022).

Table 3.3 summarises the security characteristics of the industrial communication protocols discussed in the paragraphs. If the protocol has the characteristic, it is marked with "✓"; if not, then it is marked with "-". The references used in the paragraphs are the same as those used to create the table. They are not present in the table to avoid cluttering it. Some of the table headers are abbreviated to avoid cluttering the header row. Authentication was abbreviated to AuthN, Authorisation to AuthZ, Availability to Avail. and Confidentiality to Confid.

3.3 Security Operations

Security operations focus on the real-time detection, analysis, and response to threats across an organisation's digital landscape. Endpoint security plays a vital role by protecting individual devices, such as laptops, servers, and mobile phones, from malware, unauthorised access, and other threats. Meanwhile, incident detection and response ensure that anomalies are swiftly identified and addressed, minimising damage and recovery time. These operational capabilities are essential for maintaining business continuity and defending against increasingly sophisticated cyberattacks.

Table 3.3: *Industrial protocols and their security features. AuthN - Authentication; AuthZ - Authorisation; Avail. - Availability; Confid. - Confidentiality*

Protocol	AuthN	AuthZ	Avail.	Integrity	Confid.	Determinism
PROFINET	✓	-	✓	✓	✓	✓
EtherNet/IP	✓	-	✓	✓	✓	✓
EtherCAT	-	-	✓	✓	-	✓
Modbus TCP	-	-	-	-	-	-
PROFIBUS DP	-	-	✓	-	-	✓
Modbus RTU	-	-	-	-	-	✓
802.11 Wi-Fi	✓	✓	-	✓	✓	-
OPC UA	✓	✓	✓	✓	✓	✓
WirelessHART	✓	✓	✓	✓	✓	✓
Modbus TCP Security	✓	✓	✓	✓	✓	-

3.3.1 Endpoint Security

In the modern industrial context, organisations are confronted with the challenge of numerous devices that remain unmonitored and vulnerable to security threats. The deployment of the aforesaid industrial devices occurred over a period spanning several years, with the primary focus of the initial development process being on ensuring reliability rather than incorporating cybersecurity considerations into the design (Microsoft, 2025).

In the event of inadequate management, devices can become susceptible to cyberattacks, representing a potential vulnerability in the security chain. There has been an observed increase in the connectivity of OT devices, with OT networks not always fully air-gapped, the distinction between IT and OT becoming less clear, and industrial control processes undergoing a transition from physical to digital (Microsoft, 2025).

It is evident that a considerable number of organisations have not adopted a comprehensive cybersecurity strategy to manage endpoints within OT environments. Instead, the focus is on perimeter or network-based security tactics, with a particular emphasis on transactions. There is a significant neglect of endpoint configuration, which results in endpoints becoming vulnerable to attacks (R. Automation, 2025).

The purpose of endpoint security is to protect individual devices and systems within the OT network from cyber threats. In essence, the process may be considered analogous to the deployment of a security guard for each device within a plant, factory or facility (R. Automation, 2025).

The most common way to ensure endpoint security is by using an EDR tool (CyberOne, 2025). Figure 3.5 illustrates how an EDR works in simple terms. In the illustration, a Threat Actor attacks an endpoint. The endpoint, which has the EDR agent installed (not illustrated in the Figure), is constantly sending data to the EDR solution. The EDR solution is composed of a database, big data and machine learning, a correlation/detection engine and other components. Cybersecurity/IT personnel will

consume the alerts generated by the EDR's correlation/detection engine. Based on the alerts configured, the EDR can automatically respond to an incident or the Cybersecurity/IT personnel can manually respond to it through the EDR capabilities (e.g. isolating an endpoint using the EDR).

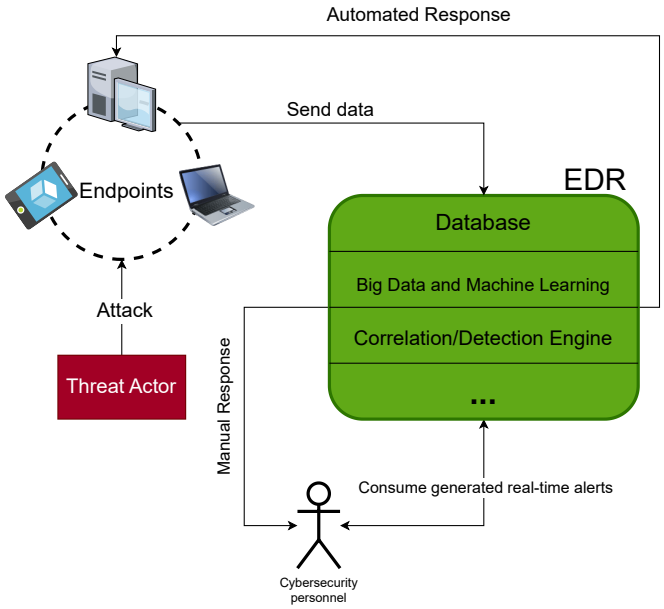

Figure 3.5: *Illustration of the operational workflow of an EDR system. Adapted from: Rhim et al., 2023.*

The manner in which EDR protects these devices from cyberattacks can be summarised as follows (CyberOne, 2025; R. Automation, 2025):

- Detect security incidents;
- Contain the incident at the endpoint;
- Investigate security incidents;
- Remediate endpoints to a pre-infection state;
- Create endpoint policies/rules, like firewalls;
- Keeping software up to date.

In order to implement an EDR solution, it is crucial that we have an asset inventory (Microsoft, 2025; SecurityThings, 2025). This may encompass software and/or hardware components deemed integral to the manufacturing process, including but not necessarily limited to: PLC, HMI, Historians, EWS and SCADA systems. Software for Manufacturing Execution System (MES), and applications for SCADA such as WinCC and Microsoft (MS) Structured Query Language (SQL) Server, are also to be considered. Furthermore, it is imperative to ascertain and incorporate all mission-critical applications that are operational within the factory automation or production control network into this classification (SecurityThings, 2025).

During the installation process, use a script or an installer package that incorporates the latest stable agent version of the EDR Solution. It is recommended that a test be conducted prior to the implementation of the system in a production environment.

The capacity of OT environments to perform multiple or selective push-to-deploy the agent software is contingent on the specific circumstances. The implementation of this process may be facilitated by the utilisation of group policies, under the condition that an Active Directory is present. Prior to the deployment of the agents, it is imperative to exercise extreme caution in the utilisation of machines that may be susceptible to disruption of operations. The use of an asset inventory and consultation with vendors is instrumental in ensuring minimal to no disruption (SecurityThings, 2025).

Orange Cyberdefense created a benchmark to compare EDR solutions in OT systems (Cyberdefense, 2021). The benchmark indicates that the EDR configuration is of paramount importance, and must be meticulously defined within an OT environment to avert any potential impact on availability. For instance, a poorly configured policy detected and blocked SCADA software from running. It is evident that this policy is not suitable for implementation in a production environment. One of the conclusions from this benchmark is that, in an OT environment, the reaction to a threat detection (e.g. terminating the affected process) should be executed with greater caution for the same reason as previously outlined: the potential impact on availability.

EDR solutions are also very important log sources and are an integral element of comprehensive monitoring strategies. The integration of an EDR solution with a SIEM system provides a comprehensive overview of the activities occurring on all endpoints, thereby facilitating the identification of any potential malicious activity (Faisal, 2025a).

It is important to note that EDR solutions represent only one element of a layered defence-in-depth model within the context of IT and OT environments. They should not be regarded as a panacea for all cybersecurity requirements. It is important to note that relying solely on EDR can leave IT and OT environments vulnerable to potential bypasses and tampering, which can result in security breaches (Faisal, 2025a).

Challenges of implementing EDR into OT systems

It is reasonable to conclude from the preceding discourse on the subject of EDR that they represent a highly effective solution for OT systems. Nevertheless, it is imperative to acknowledge that OT systems are characterised by distinct requirements and challenges that are not inherent to IT systems. In the context of OT, the utilisation of EDR is not a prevalent practice, owing to the fact that the technology in question has been found to be excessively intrusive for OT endpoints that are deemed to be sensitive. The level of control exerted by an EDR tool over an endpoint has the potential to influence processes that are too critical to be disabled in an OT system, such as a safety mechanism or a critical power generation device (Lund, 2025).

To illustrate this point, let us propose the implementation of an EDR on a safety mechanism. This EDR would be capable of detecting and responding to threats within the device. Should the EDR detect a threat, it is capable of isolating the machine or even quarantining legitimate processes in order to prevent the action of the threat. It is important to note that the isolation of the machine, or quarantine of legitimate

processes, has the potential to result in the machine's inability to respond adequately to hazards. This, in turn, can give rise to safety concerns (Lund, 2025).

In OT environments, the EDR logic and decisions must be completely transparent and customisable. Failure to do so may result in circumstances analogous to those delineated above. The ability to customise and the transparency of such systems are of paramount importance when selecting EDR solutions. The use of black-box processes and decisions within OT environments can be considered dangerous.

The heterogeneity, coupled with legacy systems and a lack of resources on most OT equipment, is also a challenge for the implementation of EDR (BlastWave, 2025e).

With all the challenges presented, EDR are still viable in OT; however, in very specific equipment. For example, EDR are still a useful tool to have on EWS, SCADA servers, personnel laptops/desktops and even some HMI (Smith, 2025). Depending on the Operating System used by these machines, we can use a traditional IT EDR. On the IT side, level 3 and above on the Purdue Model, the use of EDR is highly recommended. As seen before, most of the attacks come from the IT to the OT.

Let's imagine the case scenario where we need to update a PLC and no remote access is available. An engineer would have to go there physically with a laptop and connect via USB or Ethernet (Breen, 2019). In case the laptop that the engineer used was compromised, the infection could pass onto the PLC, leading to even greater problems. With an EDR installed on the laptop, we have an extra layer of security that can prevent these types of problems.

It is important to note that not all EDR solutions are designed to support OT environments. The selection and implementation of the EDR solution must be meticulously planned and considered to circumvent potential complications. In the event of an inventory of assets and software being available, the EDR provider can be consulted regarding potential conflicts. Furthermore, the deployment and configuration of the EDR can be optimised in order to avoid such conflicts. The provision of personalised support from the providers is of paramount importance to the success of the implementation, particularly in cases where the engineering and/or security team lacks experience in implementing and configuring EDR solutions in OT scenarios.

3.3.2 Incident Detection and Response

A security incident is defined as an occurrence that can jeopardise the safety, confidentiality, integrity, availability, authentication, authorisation, and determinism of an IT or OT system, or the information the system processes, stores, or transmits. It constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies (NIST, 2025).

Incident response is the structured process of identifying, managing, and mitigating the effects of cybersecurity incidents to minimise damage, recover operations, and prevent future occurrences. It serves as a critical component of an organisation's cybersecurity strategy, enabling a swift and efficient response to breaches, malware attacks,

data theft, and other threats. Incident response involves coordinated efforts from specialised teams and the use of frameworks, tools, and processes designed to address security events effectively (SANS, 2025; BlastWave, 2025h).

The importance of incident response lies in its capacity to minimise downtime through the rapid containment and resolution of security events, thereby reducing operational disruptions. It is also imperative to acknowledge the pivotal function it performs in the context of financial risk management, particularly with regard to its capacity to curtail substantial monetary losses that may be occasioned by data breaches, ransomware attacks or regulatory penalties. Moreover, a well-executed incident response can serve to preserve an organisation's reputation by demonstrating a proactive commitment to cybersecurity, thereby fostering trust among stakeholders. The primary function of this system is to ensure compliance with legal and regulatory frameworks, including, but not limited to, General Data Protection Regulation (GDPR), HIPAA, and Payment Card Industry Data Security Standard (PCI DSS). Finally, the process of incident response has been shown to enhance organisational preparedness (SANS, 2025).

In 2004, NIST proposed an incident response lifecycle in the first edition of the Special Publication 800-61 (Grance et al., 2004). As shown in Figure 3.6, the incident response lifecycle consisted of 4 phases:

- Preparation;
- Detection and Analysis;
- Containment, Eradication and Recovery;
- Post-Incident Activity.

Figure 3.6: *NIST 2004 First Incident Response Lifecycle. Source: Grance et al., 2004.*

Since the first edition, this version of the incident response lifecycle has been updated 3 times. In 2025, NIST added another key element into the lifecycle (Nelson et al., 2025). As can be seen in Figure 3.7, the plan is divided into: Incident Response, Lessons Learned and Preparation.

The Preparation phase is composed of Govern, Identify and Protect. Govern symbolises the cybersecurity risk management strategy, expectations and policies established, communicated, and monitored. Identify symbolises the understanding of the current cybersecurity risks that the company is exposed to. Protect symbolises the safeguards used to protect the organisation's cybersecurity risks.

The Lessons Learned phase is between the other two phases, interacting directly with both. After each incident, the Lessons Learned phase will feed the Preparation phase with new information. This new information can lead to an update on all three

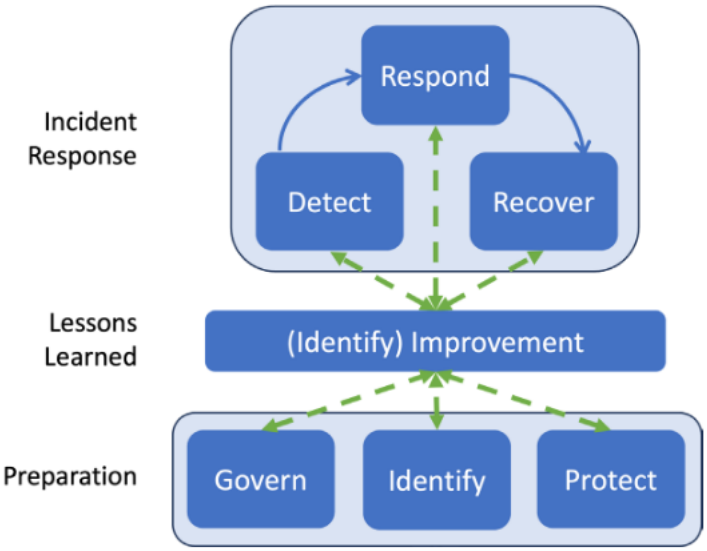

Figure 3.7: *NIST 2025 Incident Response Lifecycle. Source: Nelson et al., 2025.*

elements of the Preparation phase (e.g. update in cybersecurity risk policies and updating EDR rules).

The Incident Response phase is composed of three sub-phases: Detect, Respond and Recover. The first two phases of this incident, Detect and Respond, will be analysed in-depth in this Section.

Before we deep dive into the Detect and Respond sub-phases, let's briefly compare the 2004 and 2025 Incident Response lifecycles. The latest lifecycle presented by NIST added some needed changes, like the lessons learned during incident response should be shared as soon as they are identified, not delayed until after recovery concludes. It also modified the Preparation step to be composed of 3 important elements.

The Govern element, which is associated with policies and regulations, is becoming more and more important as cybersecurity advances. For example, with the new NIS2, affected organisations must follow security best practices or face heavy fines. Another important part of the Govern element is the company's policies that regulate and limit the possible malicious behaviours of the workers. For example, prohibiting the use of external electronics that have not been approved or limiting the access of workers to only the necessary resources. These policies should also have the Protect element to ensure that they do not bypass the policy. For example, devices using an EDR can block the connection and use of external devices in that device. Also, to limit the access of the workers, we could use authentication methods and Role-Based Access Control. With these things in mind, the addition of the Govern element into the Incident Response lifecycle is very welcome.

The Identify element is also very important in ensuring a complete Incident Response lifecycle. By identifying internal and external cybersecurity risks, the organisations can better prepare policies (Govern) and safeguards (Protect). Examples of internal cybersecurity risks are a user with excess permissions (e.g. break glass account)

or a PLC with a vulnerable version. Examples of external threats could be natural disasters or a nation-state group of hackers. External threat actors can vary depending on the type of organisation they attack. For example, some threat actors will aim for the health sector and others for the insurance companies. The motives of the threat actors can also vary (e.g. monetary, activism, revenge). The ability and funding of the external threat actors can also vary.

The 2025 Incident Response lifecycle is much more complete and has a more holistic view. However, this more holistic view adds more complexity to a process that is already complex in nature. Some companies, especially new companies or companies that are not experienced in cybersecurity, will find it harder to take these many elements into consideration while developing their incident response plan. This is the case for many companies, where the main business is centred around OT. In an initial phase, while the companies are still developing their cybersecurity practice, the 2004 or even the 2012 Incident Response lifecycle (which was not talked about in this Chapter, but is very similar to the 2004 version) can be used, and the effectiveness would still be great. For more mature companies, the 2025 version should be preferred.

Incident Detection

This section will dive deeper into the Detect sub-phase of Incident Response. Due to the safeguards not being impregnable, there is a need to proactively detect security incidents.

During the Detect phase, potential security incidents are identified, verified, and analysed in order to determine their scope, impact, and the response actions that are appropriate. This phase is pivotal in establishing the foundations for an effective incident response. It ensures that incidents are detected promptly, verified accurately, and thoroughly analysed(LetsDefend, 2025).

Security incidents can be detected through a variety of channels, including (LetsDefend, 2025):

- SIEM systems;
- Intrusion Detection System (IDS)/Intrusion Prevention System (IPS);
- EDR systems;
- Antivirus software;
- Firewall and Web Application Firewall alerts;
- System logs (e.g. Windows Security Events and Linux system logs);
- Reports and External sources.

The automated detection of security incidents can be summarised into 2 steps: the ingestion of data and the correlation of that data (Stellar Cyber, 2025b). The correlation of the data will be done through the use of rules and/or a correlation engine. This correlation process will generate alerts. Let's take the EDR system as an example. The EDR will be consuming data generated by the device where the EDR is installed. The

EDR is not sentient, and so it needs a correlation engine to understand what is going on on the device. If a threat is detected by the EDR, it will follow the procedures to contain that threat (e.g. isolating the machine from the network) and generate an alert in the centralised platform, which is normally a webpage. The centralised page is where the majority of configurations are made, and where all the alerts from all the devices are gathered. This type of tool is capable of ingesting the data and correlating it. However, not all the channels mentioned above are capable of that. For example, the system logs that are generated by the Operational System (OS) will not be correlated without the use of another tool. Another problem is the variety of tools that can be used to generate the alerts. A security incident analyst would need a way of centralising all the alerts from all the different sources to effectively detect and respond to the incidents. This is where the SIEM systems come into play. A SIEM can be used to ingest large amounts of data, correlate the data using top-tier correlation engines, and create custom rules that will define what correlation is needed to generate an alert.

SIEM systems collect and analyse log data from multiple sources, such as firewalls, IDS, EDR and applications. A SIEM is a centralised system to detect incidents. This centralised system aggregates logs from multiple sources within an organisation and then uses rules and correlation engines to generate alerts indicating potential security incidents (LetsDefend, 2025). The log sources vary depending on the type of tools used and the vendors of those tools, and to easily ingest logs into this centralised system, the logs normally follow a common format. The most common formats for these logs are Common Event Format (CEF), Comma-Separated Values (CSV), JavaScript Object Notation (JSON) and Syslog (Stellar Cyber, 2025a).

The integration of OT into the prevailing IT infrastructure is a pivotal consideration in the implementation of a SIEM. In the majority of cases, the most efficacious solution is to collect all the logs and attempt to derive some sort of meaning from them. In the event that it is not possible to create alerts with the logs, or if the logs are not conducive to an investigation, it is not necessary for them to be ingested by the SIEM (Rommer, 2025). This is especially true when most SIEM solutions charge for GigaByte (GB) of ingested logs, and if no control is made on the ingestion of logs, the bill will be huge (Logpoint, 2023). Two approaches can be adopted in order to ascertain the usefulness of the logs. The bottom-up approach involves the review of available logs to identify valuable alerts. In contrast, the top-down approach entails the definition of a set of use cases and the attempt to derive what logs would be needed for the use case (Rommer, 2025). The asset inventory is also a helpful tool to know which machines and applications need to be monitored and what logs we can collect from them.

As previously discussed, a fundamental distinction between IT and OT security lies in their respective primary objectives. Specifically, IT security is designed primarily to protect data and systems, whereas OT security is focused on safeguarding personnel and assets. Consequently, security is not the primary concern; rather, it serves as a means of averting any potential compromise to safety. It is therefore recommended that the majority of security logs be used for monitoring processes in OT, as this is a

necessary and effective approach. It is important to note that some specialised SOC can detect process violations. These deviations from standard processes can be indicative of an attack from internal or external sources, highlighting the necessity for comprehensive monitoring and analysis to ensure system integrity and security (Rommer, 2025).

In Figure 3.8, we have an example of the components that make a SIEM (Podzins et al., 2019). Starting from left to right, we have the data sources. In OT, an example of data sources is PLC, sensors, HMI and IoT. In IT, these data sources can be EWS, Data Historians and servers in general. Some of these machines will be able to provide system logs and application logs. For example, in EWS, we may have logs from Windows events, such as logins and process creation, and have logs from applications such as Computer-Aided Design (CAD). To obtain logs from systems and applications, the sources must allow for that. Some applications or systems are not designed to create logs. Following the flow of the image, the logs need to be collected and aggregated somewhere; in this case, we are talking about a SIEM. This step is made in conjunction with the log normalisation. As we talked before, a way of normalising logs is to have standard log formats. The collected and normalised logs will then be aggregated and stored in a storage. It can be local or cloud-based, depending on the solution. The logs will then be ingested into the Rule Correlation Engine, which, according to the created rules, will generate the alerts into the SIEM. The SIEM normally has some kind of dashboard to showcase the alerts. Finally, the Security Analysts can then analyse and respond to the incidents based on the alerts shown in the Dashboard and using the logs collected (Podzins et al., 2019).

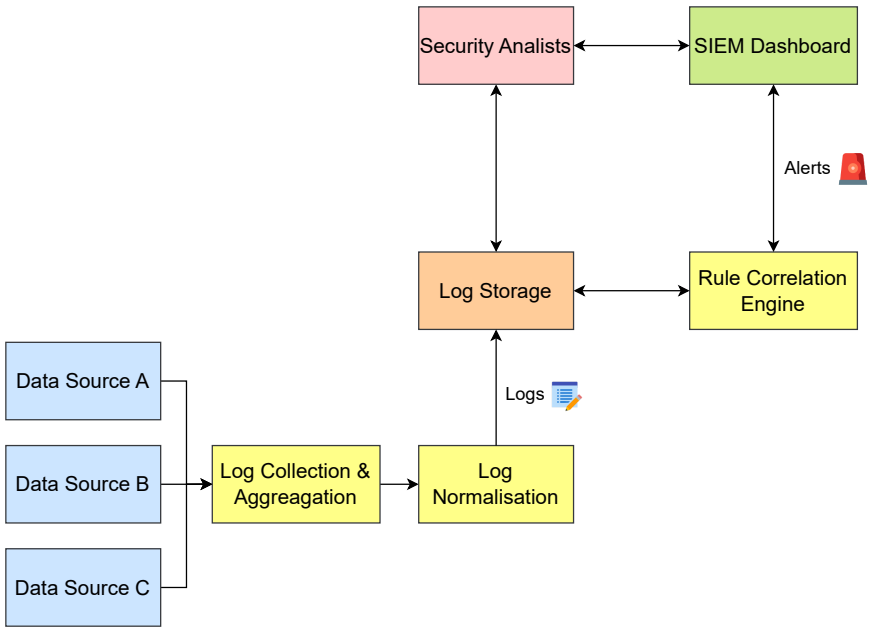

Figure 3.8: *Example of SIEM Components and Workflow. Adapted from: Chennupati, 2020.*

Incident detection in OT can present some challenges, such as legacy systems often

having no logging or monitoring capabilities, limiting visibility into system and application events. Resource constraints, such as insufficient personnel or inadequate tools, further hinder effective detection and response mechanisms. The integration of IT and OT systems introduces additional complexity, complicating monitoring and coordination efforts. Moreover, low latency requirements inherent in real-time operations necessitate rapid detection and minimal downtime, placing pressure on detection and response protocols. Lastly, the prevalence of false positives can overwhelm security analysts, reducing overall efficiency and potentially leading to alert fatigue (BlastWave, 2025d).

The analysis component of the Detect sub-phase will not be the focus of this study, as it is known to exhibit significant variations across organisations and between analysts. Furthermore, it is imperative to acknowledge that each incident type necessitates a distinct analytical approach. The subsequent subsection will address the incident response component in greater detail.

Incident Response

This subsection will address the incident response component of an Incident Response Plan. The incident response process will vary considerably depending on the nature of the incident, the affected devices, and the company's business plan. For instance, the response to an incident will vary considerably depending on whether the incident is related to malware or social engineering. Furthermore, the response to incidents will be contingent on the type of device (i.e. whether it is a workstation or a server) and the operating system (Windows or Android). Also, in the event of the detection of malware on a device, the isolation of the machine may not be possible due to significant production issues, depending on the company's business plan. It is acknowledged that certain companies may possess a business plan that permits the immediate isolation of the affected devices.

Incident response is defined as a structured approach to the management and mitigation of the impact of security breaches. The process entails the implementation of containment measures, with the objective of curtailing the propagation of threats. This is achieved by the isolation of affected systems, in addition to the execution of strategies that are both short-term and long-term in nature. The primary objective of these strategies is to minimise any potential damage. Following the containment and eradication of the threat, the focus shifts to the removal of any malicious elements, the resetting of any compromised accounts, and the patching of any vulnerabilities. This process is supported by a root cause analysis to prevent the recurrence of the issue. The final phase, designated 'recovery', is intended to restore systems, data and configurations to normal operation using backups. At the same time, this phase ensures continuous monitoring for residual threats or vulnerabilities (SANS, 2025).

The adoption of optimal practices is imperative for the efficacy of incident response endeavours. The establishment of a cross-functional response team, with clearly de-

fined roles and responsibilities, provides a structured foundation for action. The development of comprehensive response plans, tailored to specific threats, is essential for ensuring preparedness and consistency. Regular training of employees and response teams has been demonstrated to enhance their ability to recognise and respond to incidents effectively. The maintenance of comprehensive documentation pertaining to incidents, encompassing the actions undertaken and the ensuing outcomes, is instrumental in fostering continuous enhancement and accountability. Furthermore, the utilisation of sophisticated instruments such as SIEM systems, threat intelligence platforms and automated response solutions serves to augment response capabilities (SANS, 2025).

Incident response playbooks function as vital templates for the management of cybersecurity incidents. The primary objective of these guidelines is to standardise the management of incidents, thereby ensuring a coherent sequence of actions and decisions. The provision of specific, easily comprehensible instructions to team members is instrumental in ensuring that they are equipped with the necessary knowledge to respond effectively to a wide range of incident types (Palo Alto, 2025a).

The playbook is a document that outlines the specific roles and responsibilities of each individual involved, thereby ensuring that each person is aware of their contribution and the consequences of their actions.Figure 3.9 illustrates an incident response playbook for a phishing incident. The playbook shows the workflow from the receipt of the suspicious email, which passes through an analysis of the Uniform Resource Locator (URL) and attachments, to the creation of an email to notify the user if the email was malicious or not. This systematic approach facilitates effective responses during actual incidents, while also contributing to the efficacy of training programmes and ensuring optimal preparedness among personnel. In the context of emergent threats and technological advancement, the playbook undergoes a process of refinement to ensure its continued relevance and efficacy (Palo Alto, 2025a).

Some incident response tools allow for the automation of playbooks by automating the tasks. A prevalent approach to automating responses to security incidents is the implementation of a Security Orchestration, Automation and Response (SOAR) solution. SOAR aims to alleviate the strain on security teams by incorporating automated responses to a variety of events. It is also possible to program a SOAR system in such a manner that it is able to adapt to the specific requirements of an organisation. This affords teams the capacity to determine the manner in which SOAR can facilitate the realisation of high-level objectives, including the optimisation of time management, the reduction in staffing requirements, and the allocation of current staff to engage in creative projects (Fortinet, 2025d). SOAR ingest alert data, and these alerts subsequently trigger playbooks that automate or orchestrate response workflows or tasks. Although the terms 'security automation' and 'security orchestration' are often used interchangeably, the two platforms serve different roles. Security automation is concerned with the simplification and optimisation of security operations, as it addresses a multitude of discrete tasks. In contrast, security orchestration integrates disparate

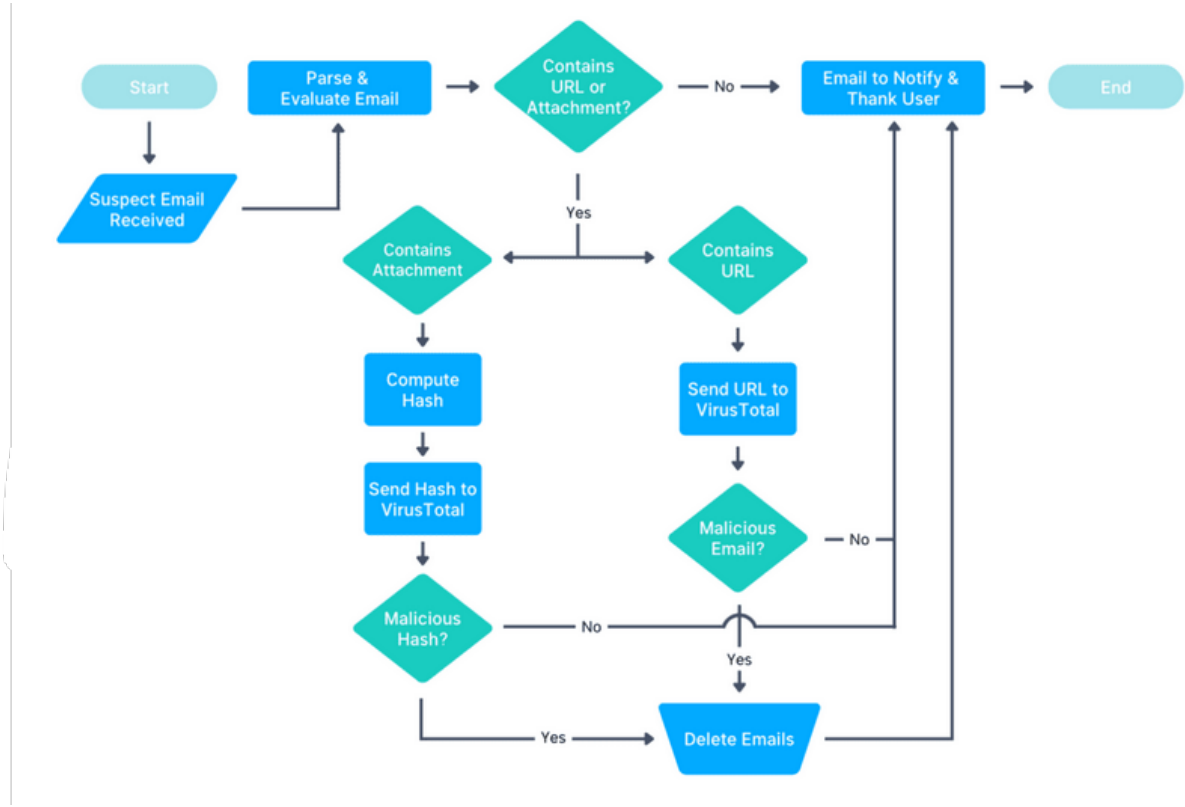

Figure 3.9: *Example incident response playbook for phishing. Source: Katie Bykowski, 2025.*

security tools, thereby facilitating seamless interconnectivity and a streamlined workflow process from initiation to completion. It has been demonstrated that the optimal functioning of these entities is most effectively achieved through their collaborative integration, with the adoption of security groups by these entities resulting in the maximisation of efficiency and productivity (Palo Alto, 2025b).

Let's imagine a situation where we need to analyse an uncommon number of failed user login attempts. Following a specified number of unsuccessful attempts at logging in, a predetermined playbook is initiated. This playbook is designed to engage with the user, identify any potentially expired passwords that may have triggered the unsuccessful attempts, and examine any recent password changes that could have also triggered the unsuccessful attempts. In addition, the IP address utilised for the logins can be examined. Should the IP address appear to originate from an unusual location, the user's account may be blocked.

Another example of the usefulness of a SOAR is when responding to incidents related to logins from unusual locations. Let's imagine a situation where we receive a successful login from France, while the user is known to work in Portugal. In order to evaluate the validity of the action, it is possible to initiate a playbook to contact the user and verify whether the IP address belongs to a VPN provider. In the event that the use of a VPN is confirmed and said use is prohibited by company policy, an immediate block of the account can be automated.

OT environments face several challenges that hinder effective incident response.

Limited visibility is a significant issue, as many OT systems lack the necessary tools to detect and analyse cyber incidents. This is further complicated by the presence of legacy systems, which often do not support modern security measures, thereby increasing vulnerability. Resource constraints, including a shortage of personnel with OT-specific expertise, also impede timely and effective responses. Moreover, the complexity of OT environments, characterised by diverse and interconnected systems, makes containment and recovery efforts particularly challenging. Lastly, incident response actions carry inherent safety risks, as they may inadvertently disrupt critical processes or compromise system integrity (BlastWave, 2025d).

4

Industry 5.0 and the Cybersecurity Dimensions

This chapter builds upon the previous discussion by delving into the cybersecurity dimensions, but in an Industry 5.0 environment. Its primary objective is to identify and analyse the emerging problems and challenges that arise from this new industrial paradigm. These concerns will be critically examined and contextualised. In the following chapter, a case study will be employed to evaluate these challenges in practice. Furthermore, the insights gained will be mapped against the proposed high-level framework to assess its relevance and robustness in addressing the cybersecurity demands of Industry 5.0.

The chapter is organised the same way as the previous one. Three sections divide the cybersecurity dimensions. Starting from governance and risk management by assessing asset inventory, vulnerability management and threat intelligence. Then, security architecture and design technologies, such as ZTA, network segmentation and industrial communication protocols, are assessed. Finally, the security operations, like endpoint security and incident detection and response, take place.

4.1 Governance and Risk Management

As Industry 5.0 redefines the relationship between human ingenuity and intelligent digital ecosystems, cybersecurity must transcend traditional reactive postures and embrace proactive, strategic foresight. Central to this evolution are governance and risk management technologies that not only fortify digital assets but also harmonise security with innovation, ethical accountability, and human-centric values. This section explores the challenges and demands of Industry 5.0 on core cybersecurity pillars, such as asset inventory, vulnerability management, and threat intelligence.

4.1.1 Asset Inventory

In the context of Industry 5.0, the asset inventory assumes a pivotal role, not only for operational efficiency but also for aligning with the core pillars of sustainability, resilience, cybersecurity, and human-centricity. Industry 5.0 calls for an integrated view of assets that supports broader socio-environmental and technological goals.

As asset inventories expand to include environmental and personal metrics, the challenge of data governance becomes increasingly critical. Industry 5.0 environments often involve heterogeneous systems-from legacy industrial control systems to cloud-native IoT platforms-necessitating interoperable data formats and semantic consistency. Moreover, the integration of sensitive data (e.g., biometric access logs or pollutant emissions) raises concerns around data ownership, privacy, and compliance with regulations such as GDPR. Therefore, asset inventory systems must embed robust data governance protocols, including encryption, access control, and audit trails, to ensure trustworthiness and regulatory alignment in human-centric industrial ecosystems.

With increased emphasis on sustainability, organisations are increasingly required to monitor and report pollution levels, as regulatory frameworks impose penalties for exceeding predefined environmental thresholds (Martina Vass, 2024). To this end, an extended asset inventory system can incorporate environmental metrics by including specific fields for pollutant emissions, enabling real-time monitoring and regulatory compliance. Moreover, sustainability goals demand improved asset lifecycle tracking from acquisition and operational use to decommissioning and recycling (CompareSoft, 2025). Embedding lifecycle data within the asset inventory allows organisations to assess environmental impact at each stage, optimise resource usage, and align with circular economy principles.

Resilience and cybersecurity, two interdependent pillars of Industry 5.0, further underscore the importance of maintaining a comprehensive asset inventory. A detailed and continually updated inventory supports multiple cybersecurity functions, including vulnerability management, threat intelligence, endpoint security, and incident response. Without full visibility of hardware, software, and interconnected systems, it becomes challenging to implement effective security measures or respond to threats proactively. Furthermore, modern industrial ecosystems are increasingly interconnected, making disruptions-whether from cyberattacks, geopolitical instability, or environmental events-more impactful and harder to contain. A robust asset inventory must therefore include not only local assets but also critical upstream and downstream dependencies, such as supplier equipment, logistics infrastructure, and third-party digital services. By mapping these external assets and their interdependencies, organisations can identify single points of failure and implement redundancy strategies, such as alternative suppliers, backup systems, or modular asset configurations. This expanded visibility enables proactive risk mitigation and ensures continuity of operations under adverse conditions.

The human-centric dimension of Industry 5.0 also introduces new complexities to

asset management. Technologies such as cobots and Brain Machine Interface (BMI) necessitate a redefinition of asset relationships. For instance, associating human operators with specific cobots in the inventory allows organisations to track usage patterns and determine access controls based on shifts or task assignments. In the case of BMI, it becomes essential to record which individuals are authorised and equipped to use these sensitive interfaces, ensuring both safety and cybersecurity integrity. Furthermore, Industry 5.0 extends asset inventory beyond technical specifications to include ethical and ergonomic considerations. For example, when tracking usage of BMI, it is not sufficient to log device ID and access permissions; inventories must also account for other metrics such as neurodata and modulating neural signals (Berrick, 2025). Similarly, cobot-human pairings should reflect ergonomic data such as posture analytics and fatigue indicators. These new data could contain Personally Identifiable Information (PII), which creates the need for secure access control of the asset inventory, confidentiality of the data and compliance with regulations. These dimensions require asset inventories to evolve into socio-technical registries, capturing not only what assets exist, but how they interact with and impact human operators.

Sepio, a company that sells asset inventory and management products, published an article in 2023 talking about the importance of asset inventory to track environmental, social and governance goals (Atar, 2025). Also, the US government provided a use-case in the transportation industry, looking at the importance of using asset sustainability metrics in asset inventory and management. They found that sustainability metrics helped in short and long-term decisions for program and budgeting. The insight provided by these metrics increased with the length of the analysis period (Proctor et al., 2025). These two real-life examples help us understand that some of the mentioned Industry 5.0 concepts and problems are already being addressed by some companies.

In Figure 4.1 is a summary of the possible changes to asset inventory in Industry 5.0. Asset inventories in Industry 5.0 should incorporate environmental metrics and lifecycle data to support pollution tracking, regulatory compliance, and sustainable resource management. A comprehensive asset inventory enhances organisational resilience by enabling key cybersecurity functions such as vulnerability management, threat detection, and incident response. Furthermore, the increase in interconnectivity in industrial ecosystems must be met with an increase in supply chain visibility and asset redundancy planning. The human-centric nature of Industry 5.0 necessitates associating human operators with emerging technologies like cobots and brain-machine interfaces within asset inventories to ensure operational clarity and secure access control. Also, asset inventories can now correlate data to know how the machines interact with the human operators. These new data should be secured as they can be PII.

Lastly, it is important to note that the best practices established during Industry 4.0 remain relevant and applicable in Industry 5.0. However, they must be expanded to accommodate the additional dimensions introduced by the new industrial paradigm.

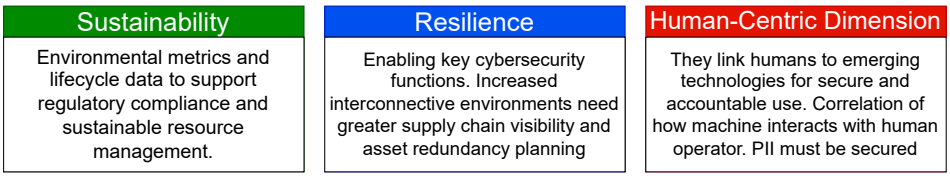

Figure 4.1: *Summary of asset inventory in Industry 5.0.*

4.1.2 Vulnerability Management

In the context of Industry 5.0, vulnerability management faces heightened complexity due to the exponential increase in the number of connected devices. The proliferation of smart sensors, edge devices, and autonomous systems demands a significant expansion in scanning capabilities. Traditional scanning infrastructures, once sufficient for more homogeneous environments, must now accommodate a vast array of devices, each with distinct protocols and configurations. Consequently, security teams are required to develop more scalable and adaptive scanning frameworks that can cope with the sheer volume and diversity of assets present in advanced industrial ecosystems.

Furthermore, the heterogeneity introduced by IoT deployments, particularly at the lower layers of the Purdue Model, challenges conventional patch management and scanning strategies. Unlike traditional systems, where patching policies could be applied uniformly across specific network layers, Industry 5.0 necessitates a device-specific approach. IoT devices, often deployed in resource-constrained and legacy-prone environments, require tailored patching schedules and methods. Similarly, the choice between active and passive scanning must now be evaluated per device, rather than per level, taking into account the operational sensitivity and communication capabilities of each asset. This shift demands a more granular and context-aware vulnerability management methodology to ensure resilience in highly interconnected industrial landscapes.

From a human-centric standpoint, the integration of cyber-physical systems with human operators - such as collaborative robots (cobots), augmented reality interfaces, and digital twins - introduces new moral obligations. A vulnerability in these systems is no longer a technical flaw with operational consequences; it becomes a potential threat to human dignity, autonomy, and safety. For example, a compromised cobot could inadvertently harm a worker, or a hijacked Augmented Reality (AR) interface could distort critical information during a high-risk task. Vulnerability management must therefore incorporate ethical risk assessments that go beyond traditional threat modelling, considering the psychological, physical, and social impacts of cyber incidents. This human-centricity means that a vulnerability is no longer just a risk to a production line's uptime; it is a potential threat to life and limb. Patching, therefore, must be approached with an unprecedented level of urgency and human safety in mind.

Furthermore, the sustainability pillar of Industry 5.0 adds a new dimension to risk assessment, as a cyberattack could lead to significant resource waste, energy consumption, or environmental damage. Vulnerability management in this context must con-

sider the potential for harm to both people and the planet, moving beyond purely economic and operational metrics. For instance, ransomware targeting industrial control systems might force emergency shutdowns, resulting in the disposal of partially completed products or the release of hazardous substances. Vulnerability management must therefore align with sustainability goals by prioritising resilience in systems that have high environmental impact.

In Figure 4.2, we can see an example of the vulnerability management process before Industry 5.0 and Industry 4.0. We can see that the decision of using active or passive scanning, and the decision of using active patching or limited patching, relied on the levels of the Purdue model. In the lower levels of the Purdue model, passive scanning and limited patching are used.

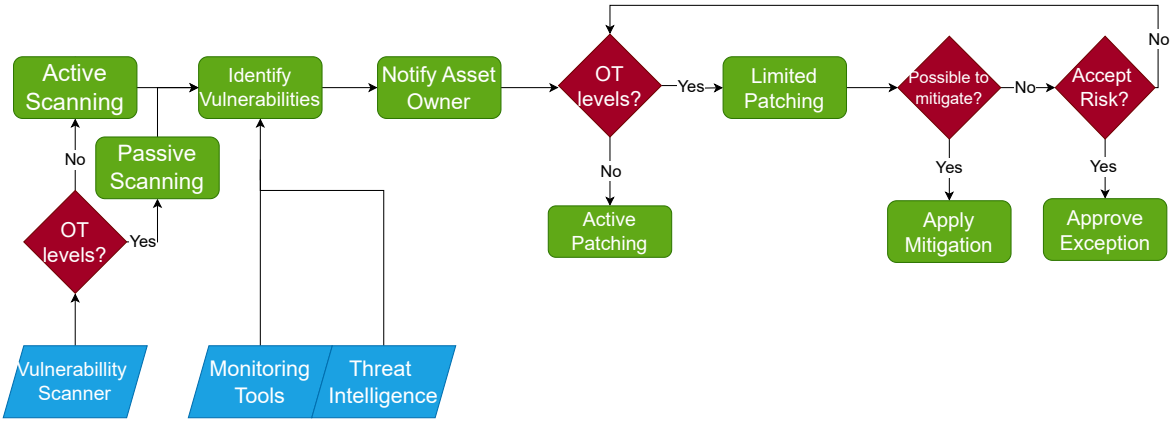

Figure 4.2: *Vulnerability management process workflow. Adapted from: McMaster University, 2025.*

Nowadays, this decision process cannot be used. In the OT levels, there are also other IT or IIoT devices. The boundaries between levels are becoming diluted, and the types of devices used in the levels are becoming diverse. We cannot just look at the levels now; we must also look at each asset individually. Figure 4.3 makes some changes in the decision process of using active or passive scanning and the use of active or limited patching, represented in purple. The decisions now need to be looked at on an individual level for each asset.

In conclusion, vulnerability management and patching in Industry 5.0 are distinguished by their integration of human-centric, ethical, and sustainability principles. These considerations demand more comprehensive, adaptive, and socially responsive security practices compared to prior industrial revolutions. As the boundaries between humans and machines continue to blur, the cybersecurity landscape must evolve to ensure not just the protection of assets but the safeguarding of values fundamental to a resilient and inclusive digital-industrial future.

4.1.3 Threat Intelligence

The evolution towards Industry 5.0 introduces significant shifts in the priorities and challenges of threat intelligence. Unlike previous industrial paradigms, threat evalua-

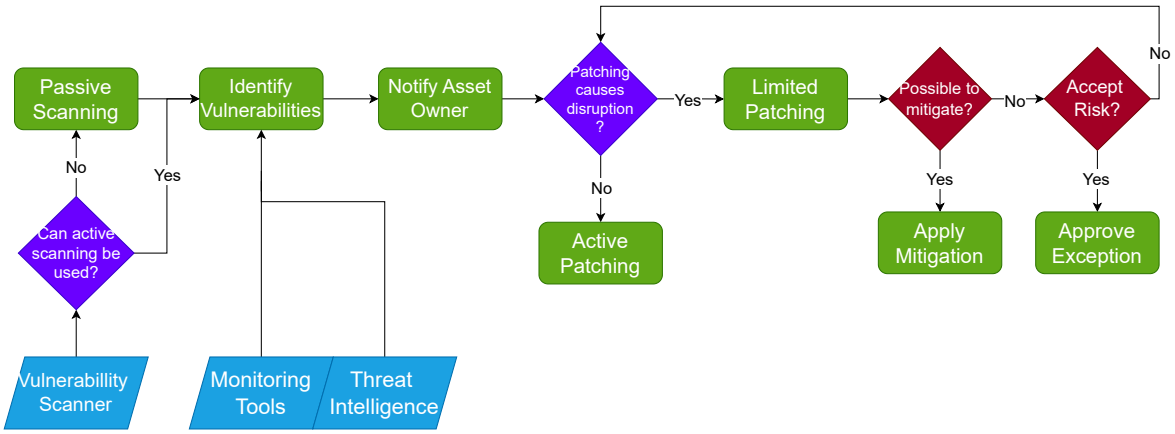

Figure 4.3: *Vulnerability management process workflow in Industry 5.0. Adapted from: McMaster University, 2025.*

tion now encompasses broader concerns, including the safety and well-being of workers, as well as environmental impact. This expansion necessitates a redefinition of what constitutes a critical threat, recognising that attacks compromising physical safety or ecological stability can be as damaging as those affecting productivity.

Industry 5.0 environments are characterised by an increased heterogeneity and volume of devices. Companies are not only integrating more OT devices but also diversifying their infrastructure instance, through the adoption of renewable technologies such as solar panels. This broader device ecosystem expands the attack surface and creates new threat vectors. A threat actor specialising in targeting solar panel systems, for example, may now consider a previously unrelated organisation as a viable target due to the integration of such systems.

Moreover, the objectives of industrial enterprises have shifted beyond mere productivity gains. Emphasis is now placed on resilience and sustainability, altering how threats are prioritised and understood. Regulatory frameworks have intensified, with penalties imposed for non-compliance, particularly in areas such as carbon emissions. This regulatory pressure introduces new strategic incentives for threat actors, who may exploit sustainability targets to disrupt operations or inflict reputational and financial harm. As companies adopt a more holistic operational model, they inevitably face a broader and more complex threat landscape, necessitating adaptive and forward-looking threat intelligence capabilities.

Resilience in Industry 5.0 extends beyond internal systems to encompass the broader supply chain ecosystem, where disruptions can cascade across interconnected partners, vendors, and logistics networks. Threat intelligence must therefore evolve to include supply chain visibility, enabling organisations to detect vulnerabilities not only within their own infrastructure but also across third-party dependencies. For example, a cyberattack on a supplier's IoT-enabled warehouse or a logistics provider's fleet management system can indirectly compromise production continuity. To mitigate such risks, organisations are increasingly adopting collaborative threat intelligence platforms

that aggregate and analyse data from across the supply chain, identifying emerging threats and weak links in real time.

The human-centric nature of Industry 5.0 demands that threat intelligence extend beyond technical vulnerabilities to include risks affecting cognitive, emotional, and physical safety. Emerging technologies such as BMI and cobots introduce new threat surfaces where adversaries may exploit biometric data or manipulate operator behaviour. Consequently, threat intelligence must incorporate behavioural analytics and psychological and physical safety metrics to detect and mitigate threats that compromise human dignity and operational integrity.

Despite the emergence of novel technologies and socio-technical systems in Industry 5.0, foundational threat intelligence frameworks such as the MITRE Adversarial Tactics and Techniques (ATT)&Common Knowledge (CK) for ICS matrix (MITRE, 2025) remain highly relevant. At their core, cyber-physical attacks-whether targeting traditional PLC or advanced brain-machine interfaces-continue to compromise the same fundamental security principles: integrity, confidentiality, availability, safety, authorisation, authentication and/or determinism. However, some modifications/adaptations may need to take place. For example, if the MITRE ATT&CK for ICS matrix is utilised, and if a breach of PII happens in a BMI, there is no impact related to the theft of PII, only "Theft of Operational Information". In Industry 5.0, OT is highly connected, not only with IT but with the human operators. This hyperconnectivity needs to be integrated into the matrix.

This traditional framework can allow organisations to accommodate emerging assets without abandoning proven methodologies. However, some novel threats and impacts do not seem to be encompassed in the matrix. Care is advised while applying this framework in an environment where machines collaborate closely with the human operator and use PII.

In summary, threat intelligence in Industry 5.0 must evolve to address a wider array of concerns, including human welfare, environmental sustainability, and regulatory compliance. The diversification of connected devices broadens the attack surface, while the shift towards holistic, resilient, and sustainable operations redefines both threat priorities and attacker motivations. Consequently, organisations must adopt a more integrated and proactive approach to threat intelligence, aligning security strategies with the expanded scope and values of Industry 5.0.

4.2 Security Architecture and Design

In the era of Industry 5.0, where human-centric innovation converges with intelligent automation, a resilient cybersecurity posture demands thoughtful architectural design and strategic segmentation of systems. ZTA and network segmentation will be tested against Industry 5.0's demands. Also, industrial communication protocols must be evaluated and challenged to meet Industry 5.0's requirements.

4.2.1 Zero Trust Architecture

To streamline the explanation of Zero Trust within the context of Industry 5.0, the PoLP will not be addressed explicitly, as it is inherently integrated into the Zero Trust paradigm.

From a cybersecurity and resilience perspective, Zero Trust is a cornerstone for secure operations in Industry 5.0. The traditional, well-defined boundaries between IT and OT have become significantly less distinct. These domains now operate in an increasingly converged and interconnected manner. This convergence introduces elevated risks, particularly the potential for lateral movement by threat actors, where the compromise of a single device may lead to widespread access across the network. Zero Trust mitigates such risks by enforcing strict identity verification, continuous monitoring, and micro-segmentation.

The implementation of Zero Trust Architecture in Industry 5.0 environments is significantly complicated by the presence of heterogeneous and legacy systems, particularly within OT domains. Many industrial devices were not designed with modern cybersecurity principles in mind and lack support for identity-based access controls, telemetry, or secure communication protocols. This creates a fragmented security landscape where enforcing uniform Zero Trust policies becomes technically and operationally challenging.

Another critical challenge lies in establishing identity verification for novel devices, such as cobots and IoT devices. These devices often operate with constrained resources, proprietary firmware, or limited interoperability, making it difficult to integrate them into centralised identity and access management systems. Additionally, the sheer volume and diversity of endpoints in Industry 5.0 ecosystems necessitate advanced microsegmentation strategies and continuous monitoring frameworks that can scale horizontally. Without robust automation, Zero Trust risks becoming unmanageable in such complex environments, potentially leading to security gaps or operational bottlenecks.

In terms of sustainability, the direct contribution of Zero Trust is limited. However, its role in preventing cyberattacks that could negatively impact environmental systems and critical infrastructure offers an indirect but important contribution to sustainable practices. Its role in safeguarding critical infrastructure indirectly supports environmental resilience. Cyberattacks on smart grids, water treatment facilities, or industrial control systems can lead to cascading failures with severe ecological consequences. By minimising the attack surface and preventing lateral movement, Zero Trust helps ensure the integrity and availability of systems that underpin sustainable operations. In this sense, Zero Trust contributes to the broader sustainability agenda by enhancing the robustness of digital ecosystems that manage energy, waste, and resource flows.

However, the implementation of Zero Trust itself may introduce sustainability trade-offs, particularly in terms of energy consumption and computational overhead. Continuous authentication, real-time telemetry, and the possibility of AI-driven anomaly detection require substantial processing power and network bandwidth, which can in-

crease the carbon footprint of cybersecurity operations. To align with Industry 5.0's sustainability goals, future Zero Trust frameworks must incorporate energy-efficient protocols and intelligent data reduction techniques. This calls for a holistic design approach where security and sustainability are not treated as competing priorities but as co-dependent pillars of resilient digital transformation.

Regarding human-centricity, a defining principle of Industry 5.0, Zero Trust faces additional challenges. The growing integration of human-machine interfaces and personalised technologies complicates the consistent enforcement of Zero Trust principles. These technologies, while empowering human operators, introduce new vectors that must be secured, necessitating sophisticated and adaptable Zero Trust frameworks.

Furthermore, the continuous monitoring inherent to Zero Trust raises concerns about privacy and user autonomy. While telemetry and behavioural analytics are essential for detecting anomalies and enforcing least-privilege access, they may inadvertently infringe on personal privacy, especially in environments where humans and machines collaborate closely. Balancing the need for granular security with ethical considerations requires the development of transparent, consent-based monitoring frameworks and adaptive trust models that respect individual rights. As Industry 5.0 evolves, Zero Trust must expand beyond technical enforcement to include socio-technical dimensions, ensuring that security mechanisms empower rather than constrain human agency.

Zero Trust Architecture emerges as a foundational cybersecurity paradigm for Industry 5.0, offering critical safeguards in an era defined by IT/OT convergence, intelligent automation, and human-machine collaboration. Its emphasis on continuous verification, micro-segmentation, and identity-centric controls directly enhances system resilience against increasingly sophisticated and lateral cyber threats. While its direct contribution to sustainability may appear limited, Zero Trust indirectly supports environmental and infrastructural integrity by preventing disruptions to critical systems. Moreover, the human-centric goals of Industry 5.0 introduce new challenges, such as privacy concerns in the traditional Zero Trust implementations. Addressing these challenges requires a reimagining of Zero Trust principles to accommodate dynamic, context-aware, and ethically grounded security models. As Industry 5.0 continues to evolve, the integration of Zero Trust must be both technically rigorous and philosophically aligned with its core values of resilience, sustainability, and human empowerment. Figure 4.4 illustrates the differences and challenges of the Zero Trust model in Industry 5.0, in the fields of sustainability, resilience and the human-centric dimension.

4.2.2 Network Segmentation

In Industry 5.0, some aspects of segmenting networks need to change. These aspects are the rigidity of the Purdue Reference Model and the difficulty of network segmentation.

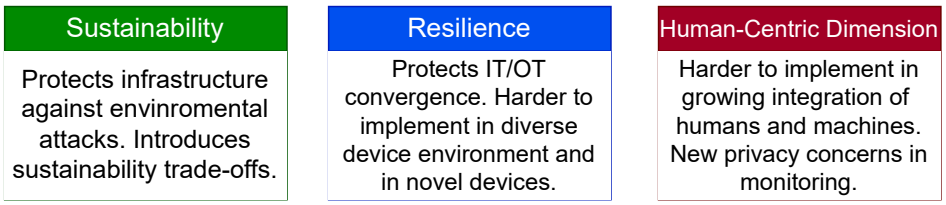

Figure 4.4: *Summary of ZTA in Industry 5.0.*

As mentioned before, the Purdue Reference Model is used to divide the architecture of an industrial plant into predefined hierarchical levels. With the introduction of IoT in Industry 4.0, these hierarchical levels changed. Now we have technologies, like IoT devices, that communicate with both OT and IT environments, like the cloud. The rigid structure of the Purdue Reference Model does not allow for this type of conduit. In Industry 5.0, we will have new technologies that will, once again, challenge the Purdue Reference Model. For example, technologies like strain sensors will need conduits between the device, which is on the machine's zone, and the IT. These types of devices will not be communicating with PLC, and they will going to need to skip some levels to communicate with the IT environment. Also, technologies like AI are emerging, and they are normally in the cloud. If AI is used in the OT levels, there is going to be a need for the OT levels to communicate with the cloud, like IoT does.

Figure 4.5 illustrates an updated version of Figure 3.4. This new version extends the high-level architecture to the concepts of Industry 5.0. The figure shows that an IoT device, in this case a strain sensor worn by a Worker, doesn't fit into the previously defined levels of the Purdue Model (Faisal, 2025b). IoT devices must be separated from the other zones for security reasons, and they must not share conduits with the other zones. The only conduit needed is for the Cloud/Internet or into the Enterprise Resource Planning (ERP) if the solution is on-prem.

All these new technologies will change the Purdue Reference Model into becoming more flexible and dynamic. This does not mean that we should abandon any sense of strict communication. Not every device needs to communicate with everything; devices should only communicate with other devices strictly if necessary. Principles like least privilege and zero trust will be cornerstones to securely implement these new technologies, in an ever-growing, complex and dynamic ICS network.

The increased difficulty of segmenting networks comes from the addition of so many new devices into the industrial process. Not only that, but as we discussed in the previous paragraph, these new devices have some new communication requirements.

Air Gap in Industry 5.0

The introduction of new technologies in Industry 5.0 makes the application of air-gapped systems increasingly challenging, as maintaining complete isolation conflicts with the need for real-time data exchange and automation. However, in high-security

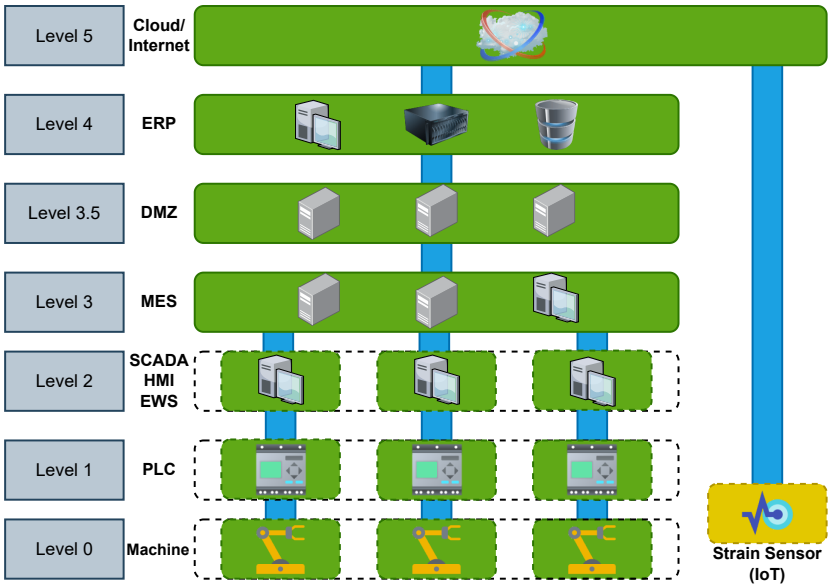

Figure 4.5: *Example architecture of zones and conduits in Industry 5.0. Adapted from: Trend Micro, 2020.*

sectors such as defence and nuclear power, where adopting these new solutions is less common, air-gapping remains a necessary security measure. These industries prioritise absolute protection over efficiency, ensuring that critical systems remain isolated from external networks to prevent cyber threats.

As Industry 5.0 promotes hyper-connectivity, many technologies, such as IoT and IIoT devices, must communicate with OT systems, making fully isolated networks rare. The need for interoperability between IT and OT environments results in complex, interconnected infrastructures where air-gapping is impractical.

Furthermore, many Industry 5.0 technologies depend on cloud services and internet connectivity, making air-gapping infeasible for their operation. However, while complete isolation from external networks is often unrealistic, critical systems should still be segregated from one another to limit potential attack vectors. A hybrid approach, combining Zero Trust principles with selective air-gapping of high-risk assets, ensures both security and functionality in increasingly connected industrial environments.

Industry 5.0 Applied Scenario: Air Gap in Smart Manufacturing Let's imagine a scenario where an automotive manufacturer transitions to Industry 5.0. In this smart manufacturing plant, cobots work alongside human operators, IoT devices, such as strain sensors, are worn by the Workers, and AI systems receive real-time machine data to predict maintenance and possible malfunctions. In this configuration, traditional air-gapping of IT and OT, so that attacks cannot cross from one to the other, would hinder operational efficiency. Air-gapping these two would slow down production and be against Industry 5.0's broader connectivity principle, as the new enabling technologies wouldn't work optimally or work at all.

Industry 5.0 Applied Scenario: Air Gap in High-Risk Environments Conversely, a nuclear power plant remains a prime example where a physical air gap remains appropriate and essential. In such high-risk, high-regulation settings, the model sacrifices all Industry 5.0's advantages in favour of maximal resilience and containment. The regulatory and safety requirements of such environments justify the use of complete isolation.

4.2.3 Industrial Communication Protocols

In Table 3.3, we can see that some protocols do not have authentication features. Protocols that do not have authentication features should not be used if security is a priority. Without authentication, an adversary that has gained access to a client (e.g. EWS) can easily manipulate the industrial process by communicating with the PLC (Alvey, 2024).

Protocols that lack availability features decrease the probability that a machine will produce or be available to produce at any given time. Also, during the industrial process, if availability is compromised then the security of the process can also be compromised. For example, in a water treatment plant, the job of the machines is to filter, process, treat, and provide drinking water. Compromising any part of the system can disrupt the entire production process and can even hinder the population that utilizes its services (Cybiant, 2018).

Some protocols, like Modbus TCP and RTU, also lack some integrity features. Despite having error checking through the calculation of Longitudinal Redundancy Check (LRC) and Cyclic Redundancy Check (CRC), it does not provide error correction (Modbus Organization, n.d.).

Confidentiality in industrial environments is the least important of the CIA triad, being availability the most important. This is because the data that is transmitted using these protocols is not important, and with the additional confidentiality comes additional performance costs. The only time that it is recommended is when, from the transmitted data we can gather important information like a recipe that is used (Koelemij, 2023).

Some protocols, such as Modbus TCP and 802.11 Wi-Fi, lack determinism. Deterministic protocols have real-time communication with extremely low data loss rates, packet delay and latency. Deterministic protocols are essential in industrial environments (CoreTigo, 2025).

When it comes to only privacy and safety, protocols such as Profinet, EtherNet/IP, OPC UA and WirelessHART are probably the best options, as they offer all the security features. However, not all security features are always needed depending on the infrastructure, and some of them can impair others. For example, as already explained, the case of confidentiality impacting performance. There must be a balance between building the most secure infrastructure and manufacturing performance. Also, not all ICS allow for the use of these secure protocols.

Does Industry 5.0 Need New Protocols?

The progression from Industry 4.0 to Industry 5.0 represents a significant evolutionary shift in the industrial paradigm. While Industry 4.0 prioritised automation, digital integration, and machine-to-machine communication through technologies such as the IIoT, CPS, and AI, Industry 5.0 reorients the focus towards human-centricity, sustainability, and resilience. This phase reintroduces the human as an active agent in manufacturing, promoting collaboration between people and intelligent machines. This new collaboration might require new OT protocols or changes to the existing protocols. Communication systems must now support adaptive, decentralised, and context-aware architectures capable of engaging with human operators and accommodating dynamic operational conditions.

Legacy protocols such as Modbus RTU, PROFIBUS DP, and Ethernet-based systems like Profinet, Ethernet/IP, and EtherCAT have served as the backbone of industrial automation. These protocols are optimised for real-time control, device synchronisation, and deterministic data transfer. Newer frameworks such as OPC UA, Modbus TCP Security, WirelessHART, and IEEE 802.11 (Wi-Fi) have introduced additional features such as semantic modelling, encryption, and wireless capability. However, they remain largely rooted in the operational assumptions of Industry 4.0.

Industry 5.0 introduces new requirements, notably real-time human-machine collaboration, decentralised and context-aware communication, and enhanced cybersecurity. Many existing protocols reveal their limitations. Fieldbus systems such as Modbus and PROFIBUS, for example, were never designed with modern security demands. Even more advanced protocols like EtherCAT and Profinet, though suitable for deterministic control, lack native support for dynamic reconfiguration and complex human-machine interfaces.

Security by Design

With the increased interface between humans, machines, and cloud-edge systems, security becomes a foundational concern. Protocols must provide end-to-end encryption, strong identity authentication, and context-sensitive access control. Existing solutions, such as Modbus TCP Security and OPC UA, introduce some security features, yet many older protocols remain insecure by design. These vulnerabilities expand the attack surface in Industry 5.0 scenarios.

In Table 3.3, we see that OPC UA and WirelessHART check all the security features needed for Industry 5.0. These protocols were recently developed and introduced into the industrial world, and so they have more modern features, such as security by design. Older industrial protocols were not developed with security in mind. Before proceeding any further, it is imperative to understand that no protocol can work alone in an industrial environment. Some protocols are better suited for certain activities and others for other activities. For example, WirelessHART is mostly used for IIoT, and it was not developed to be used in PLC or Cobots. Every protocol has its place in an in-

dustrial environment, and no industrial protocol can replace all the others because it has all the security features.

We will not be analysing the other protocols as they fail to meet the security requirements for the resistance pillar in Industry 5.0. It is important to reinforce that this does not mean that only these 2 industrial communication protocols will be found in an industrial environment that transitioned to Industry 5.0. For example, some cobots are developed using Modbus TCP/IP and Profinet (Universal Robots, 2025a). However, this doesn't mean that using these protocols is a good idea for security and resilience. The objective is to gradually transition away from these insecure protocols and begin using the new ones.

OPC UA and WirelessHART in Industry 5.0 enabling technologies

To assess the readiness of these two protocols for Industry 5.0, we can examine their application in the new enabling technologies. If we see that they are being used, we can conclude that for some enabling technologies, the protocols are Industry 5.0 ready.

This section assesses the readiness of OPC UA and WirelessHART in relation to key enabling technologies, namely cobots, exoskeletons, mental and physical strain sensors, brain-machine interfaces, renewable energy sources, and energy harvesting systems. Each technology will be evaluated in terms of its compatibility within the context of these industrial communication protocols.

In surveying the literature and technical interventions, evidence confirms that cobots are indeed being integrated with OPC UA, although less clearly with WirelessHART. For example, Universal Robots' cobots can be equipped with the software Rocketfarm URCap to function as OPC UA servers or clients (Universal Robots, 2025b). On the other hand, documentation for cobots using WirelessHART is scarce. We found an article that refers to a FANUC cobot working in conjunction with a multi-protocol Honeywell pressure transmitter that supports WirelessHART, but it does not explicitly demonstrate WirelessHART communication being used directly by the cobot itself (Charbonneau, 2018). Thus, while OPC UA integration with cobots is substantiated by both vendor and community sources, WirelessHART usage in cobot deployments remains unconfirmed in the academic and industrial literature.

In reviewing extant literature and technical documentation, integration of exoskeletons with OPC UA is evident. For instance, (Wei, 2022) article proposes a method for real-time gait monitoring of a powered exoskeleton using a digital-twin framework inspired by industrial robotics, explicitly suggesting compatibility with OPC UA real-time data streams. Similarly, (Bances et al., 2020) article describing lower-limb exoskeleton rehabilitation with digital twins likewise aligns with OPC UA's real-time interoperability paradigms. Conversely, references to WirelessHART in exoskeleton contexts are scarce. Doebbert et al., 2022 touch on WirelessHART in a broader sense, but does not document direct WirelessHART communication being implemented in an exoskeleton itself. However, because of the properties of WirelessHART, such as

security, real-time and reliability, the paper indirectly states that the protocol could be used. Thus, while OPC UA alignment with exoskeleton technologies is supported in the literature, corroborated examples of exoskeletons using WirelessHART remain unsubstantiated to date.

In the context of mental and physical strain sensors, integration with OPC UA is supported by recent developments. A doctoral thesis from Simon Fraser University created and tested a new data exchange architecture based on OPC UA to build a digital twin of an IIoT device and monitor real-time sensor data (Abdelsattar, 2023). This implies potential alignment with OPC UA's structured and interoperable communication models. In contrast, no direct implementations of WirelessHART in strain sensors have been identified. While one study applies Wireless Sensor Network (WSN) to strain sensing (C. Liu et al., 2015) and another validates WirelessHART in WSN within industrial environments (Adriano et al., 2018), no documented use explicitly combines WirelessHART with mental or physical strain measurement. Hence, although OPC UA shows demonstrable readiness for use in strain sensor systems, WirelessHART's suitability remains largely theoretical within this specific application area.

In the case of BMI, no direct evidence has been found in the academic or industrial literature to support the use of either OPC UA or WirelessHART within such systems. While BMI rely on high-throughput, low-latency data exchange-characteristics addressed by some industrial communication protocols-there is currently no documentation or implementation demonstrating the integration of OPC UA or WirelessHART in BMI applications. Consequently, both protocols appear to have limited or no established presence in the domain of BMI at this time.

In the context of renewable energy sources and energy-harvesting systems, there is clear evidence supporting the use of OPC UA, whereas WirelessHART remains largely confined to experimental sensor-network applications. OPC UA is employed in SCADA-based control systems for renewable energy infrastructures such as wind and solar power plants, offering secure, scalable, and interoperable data exchange (Eureka, 2025; Lee et al., 2023). In contrast, WirelessHART has been demonstrated in research involving solar-powered wireless sensor nodes (Ibrahim et al., 2017), confirming its viability for energy-harvesting contexts, but without direct deployment in the control or monitoring of renewable energy assets. Therefore, OPC UA demonstrates a high level of technological readiness in renewable and energy-harvesting applications, while WirelessHART's role appears limited to only sensor-based energy-harvesting.

In Figure 4.6 is a summary of the capabilities of the industrial protocols in some of the new enabling technologies of Industry 5.0. The analysed technologies are represented on the left, and the analysed protocols, OPC UA and WirelessHART, are represented on the right. The protocols are represented in rectangles of green, yellow and red. The green rectangles represent direct evidence of the use of the protocol in the technology. The yellow rectangles represent indirect evidence, and the red rectangles represent no evidence of the use of the protocol in the technology.

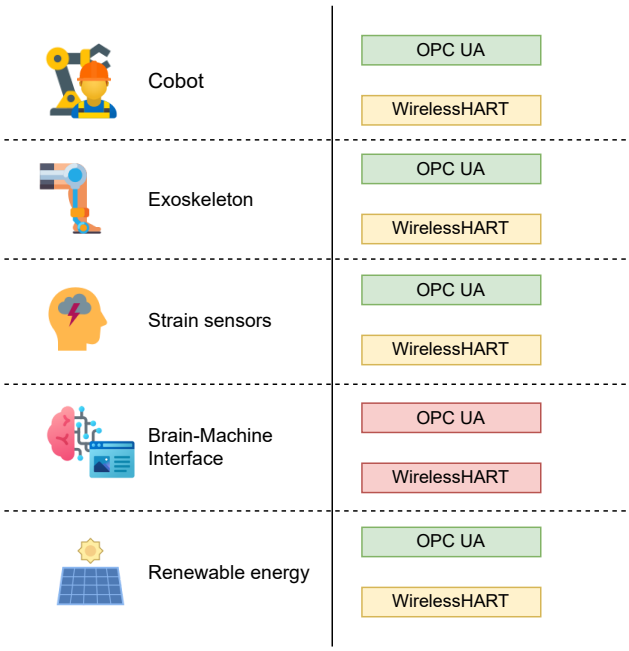

Figure 4.6: *Readiness of OPC UA and WirelessHART against Industry 5.0 enabling technologies. Green rectangles represent readiness. Yellow rectangles represent more or less prepared. Red rectangles represent no evidence of readiness.*

4.3 Security Operations

In the context of Industry 5.0, where human insight and intelligent systems coalesce, security operations must evolve to meet the demands of hyper-connected, adaptive environments. Endpoint security and incident detection and response are vital dimensions of cybersecurity, providing real-time threat detection, analysis and response. In this section, these dimensions will be challenged by Industry 5.0's demands and requirements.

4.3.1 Endpoint Security

In the context of Industry 5.0, endpoint security is a critical component for ensuring both cyber resilience and operational continuity. However, the heterogeneity and proliferation of devices, including IoT sensors, cobots, and other OT assets, pose significant challenges. Traditional endpoint security solutions such as EDR tools and antivirus software are frequently incompatible with these devices due to limitations in processing power, operating system support, or architectural constraints. Furthermore, the growing number of endpoints increases the total cost of security implementation, particularly for EDR solutions that are licensed on a per-device basis, thereby straining organisational budgets.

Furthermore, Industry 5.0 brings with it a transformation in the threat landscape,

characterised by the convergence of cyber-physical systems, human-machine interfaces, and AI-driven automation. Unlike traditional industrial environments, Industry 5.0 introduces new attack surfaces through its new enabling technologies such as BMI, wearable technologies and cobots. EDR systems must be able to detect and respond to these new attack vectors.

As can be seen in Table 4.1, multiple possible attacks and countermeasures in these technologies have already been studied. The most common attack is the DoS, which occurs in almost all technologies. The Man-in-the-Middle (MitM) attack has also been identified multiple times in various technologies. In contrast to the potential cyberattacks, the countermeasures appear to be unique for each Industry 5.0 enabling technology. Accordingly, the new enabling technologies of Industry 5.0 increase the cybercriminals' attack surface.

From a sustainability perspective, endpoint security may not directly alter ecological impact under normal conditions. Nonetheless, the evolving threat landscape introduces novel vectors such as environmentally targeted cyberattacks. For instance, malicious actors could seek to manipulate industrial processes to exceed regulated carbon emission thresholds, thereby triggering financial penalties. While presently speculative, such threats necessitate detection mechanisms within endpoint security frameworks. EDR may already have these detection mechanisms; however, further investigation is advised. Failure to identify and mitigate these attacks not only increases an organisation's environmental footprint but also carries reputational and regulatory consequences.

In terms of human-centricity, a cornerstone of Industry 5.0, endpoint security must adapt to safeguard both human data and human safety. Devices such as Strain Sensors may process personal data of their users, requiring compliance with data protection standards. Additionally, endpoint security solutions must balance cyber protection with the physical and psychological safety of users. Overly aggressive threat mitigation, such as indiscriminate process termination, could inadvertently disrupt critical functionalities, thereby endangering human operators. This echoes earlier concerns regarding the deployment of EDR solutions in OT environments, where incorrect policy enforcement can have direct human safety implications.

Figure 4.7 illustrates an example workflow of an EDR system in Industry 5.0 that is installed in an OT machine that emits CO2 and in a strain sensor. The figure shows a Threat Actor attacking the machine in order to increase the CO2 emission levels. This type of attack represents the evolving threat landscape that encompasses emerging risks such as environmentally targeted cyberattacks, where malicious actors manipulate industrial processes to exceed carbon emission thresholds and incur financial penalties. The figure also shows that the data sent by the strain sensor to the EDR solution needs to be protected/anonymised for the user's protection and to adhere to demanding data protection regulations.

In summary, the implementation of endpoint security in Industry 5.0 demands a multifaceted approach that accounts for increased device diversity, evolving threat

Table 4.1: *Review of Literature on Cyberattacks and Countermeasures of Industry 5.0 enabling technologies.*

Enabling Technologies	Possible Cyberattacks	Countermeasures
Cobots	Physical tampering of data cables. Locally connected USB devices. DoS because of a shutdown button on the web application. Brute force of valid user names. Privilege escalation. Exploiting Outdated Software. Cross-site scripting. MitM attack (Hollerer et al., 2021).	Physical access control. Apply the zero trust model. Removing the shutdown button from the web application. Usage of responses which do not indicate the existence of user accounts. Implementation of different access types. Updating the outdated software. Applying the missing Hypertext Transfer Protocol (HTTP) headers (Hollerer et al., 2021).
Strain sensors	MitM attacks. Overflow-based malicious code injection. Firmware attack (J. Liu et al., 2016).	Encrypted data payloads of packets. Revising the programming errors. Encrypt and decrypt the firmware on the wearable device with public key or symmetric key. Avoid wearing a smartwatch when typing confidential information (J. Liu et al., 2016).
Brain-machine interfaces	Side-channel attacks to reveal a user's private information (Martinovic et al., 2012). Narrow period pulse attacks (Meng et al., 2023). Backdoor attacks (Jiang et al., 2023).	Not to expose the raw data from Electroencephalography (EEG) devices to third-party applications. Adding noise to the EEG raw data before making it available to the applications that must use it (Martinovic et al., 2012). Fine-tuning. Stochastic activation pruning (Meng et al., 2023). Fine-tuning. Input preprocessing (Jiang et al., 2023).
Energy-autonomous sensors	Eavesdropping. DoS attacks. Side channel attacks. Device Tampering. Replay attacks. Spoofing attacks. MitM attacks. Malware injection (Tedeschi et al., 2020).	Provide a framework that as more energy becomes available, authentication and confidentiality are strengthened. Use precomputation techniques that anticipate the execution of the most energy-demanding tasks when the device is fully powered (Tedeschi et al., 2020).
Renewable energy sources	Meter fraud attacks (Tang et al., 2023). Adversarial learning attack against deep learning-based renewable energy forecasts (Ruan et al., 2024). Ramp attack (Sarangan et al., 2018).	Convolutional neural network-based detector (Tang et al., 2023). Use an anti-ramp attack algorithm (Sarangan et al., 2018).

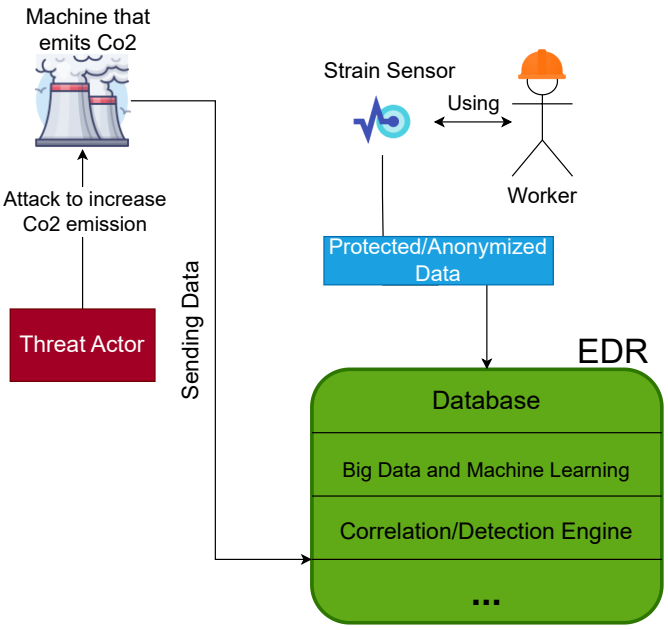

Figure 4.7: *Example workflow of EDR system in Industry 5.0 and its issues.*

landscapes, and heightened human-centric concerns. While technical constraints and cost scalability hinder widespread deployment of conventional tools like EDR, the necessity for robust protection remains. Additionally, endpoint security must evolve to detect unconventional threats, including those with environmental implications, and ensure that human safety and data privacy are not compromised. These considerations underscore the need for adaptive, context-aware endpoint security strategies tailored to the unique demands of Industry 5.0.

4.3.2 Incident Detection and Response

Industry 5.0 introduces new paradigms in industrial operations, emphasising human-centricity, sustainability, and resilience. However, these advancements also complicate both incident detection and response processes within the cybersecurity domain.

From a resilience and cybersecurity perspective, the proliferation of heterogeneous smart devices increases the volume and diversity of logs to be collected. This not only heightens the operational complexity but also imposes additional financial burdens when log ingestion is priced per gigabyte, as is common with SIEM platforms (EdB-MSFT, 2025). The increased heterogeneity of log sources complicates filtering mechanisms, introduces greater noise, and may lead to delayed or missed detections. These new devices pose a new threat to organisations as they increase the attack surface and the attack vectors, leading to new alerts/rules being created when it comes to incident detection. As previously seen in Table 4.1, this increase in attack vectors requires unique countermeasures. In terms of response, this elevated noise level challenges the log analysis of an incident analyst. Furthermore, the presence of multiple device types may necessitate varied and potentially unfamiliar response strategies. For example, a

security incident affecting a BMI may require neurological signal data isolation and immediate disconnection procedures, which differ substantially from responses typical of conventional industrial control systems.

The most common attack is the DoS, which occurs in almost all technologies. The MitM attack has also been identified multiple times in various technologies. In contrast to the potential cyberattacks, the countermeasures appear to be unique for each Industry 5.0 enabling technology. Accordingly, the new enabling technologies of Industry 5.0 increase the cybercriminals' attack surface.

In Industry 5.0, sustainability is not merely a corporate value but a measurable operational imperative. Cybersecurity systems must evolve to detect incidents that pose environmental risks, such as unauthorised emissions, energy overconsumption, or hazardous waste mismanagement. Real-time telemetry from industrial assets-such as CO2 sensors, water usage meters, and temperature regulators-can be integrated into SIEM platforms to flag anomalies that may indicate sabotage, misconfiguration, or system failure. For example, a sudden spike in emissions from a smart manufacturing unit could signal either a mechanical fault or a deliberate attack aimed at bypassing environmental controls. These detection mechanisms must be context-aware, capable of distinguishing between benign fluctuations and malicious activity, and should incorporate historical baselines, seasonal patterns, and operational thresholds to reduce false positives. The integration of environmental data into cybersecurity workflows reflects a broader shift toward cyber-eco resilience, where digital security and ecological integrity are treated as interdependent domains.

Responding to sustainability-related incidents in Industry 5.0 requires a coordinated, multi-stakeholder approach that aligns with both internal governance and external regulatory mandates. As such, cybersecurity teams must collaborate with environmental compliance officers, legal departments, and public relations units to ensure that responses are timely, transparent, and legally sound. Automated incident response platforms can assist by generating pre-configured workflows for environmental breaches, including alert escalation, forensic data capture, and regulatory reporting. Moreover, AI-driven predictive analytics can be employed to anticipate sustainability risks before they materialise, enabling proactive mitigation strategies. This convergence of cybersecurity and environmental stewardship exemplifies the Industry 5.0 vision, where technological advancement is harmonised with ecological responsibility and long-term resilience.

Regarding human-centricity, the increase in connected devices complicates detection and response activities by introducing sensitive personal data into security logs. A pertinent example involves BMI generating logs that may contain neurological patterns or other personal identifiers. Such data must be anonymised or pseudonymised, ideally at the point of generation or, if not feasible, before SIEM ingestion. Analysts involved in incident response must not have access to raw personal data, in compliance with privacy regulations and ethical considerations. Additionally, in Industry 5.0, there is a need to create alerts for when technologies that interact directly with

humans exhibit unusual behaviour, potentially leading to physical or mental damage.

The human-centric objectives of Industry 5.0 demand a reconfiguration of incident response protocols to account for ethical and psychological dimensions that were previously peripheral in industrial cybersecurity. The inclusion of PII in security logs or forensic analysis raises profound ethical questions about consent, data minimisation, and the right to cognitive privacy. Incident response teams must be trained not only in technical remediation but also in ethical decision-making, ensuring that personal data is anonymised or pseudonymised at the point of collection and that access controls prevent unauthorised exposure. Regulatory frameworks such as the GDPR provide a baseline, but Industry 5.0 calls for more nuanced policies that address the unique risks posed by direct human-machine integration.

Figure 4.8 illustrates an example of the operational workflow of a SIEM system in Industry 5.0. In the figure, a Threat Actor attacks a machine to increase the CO2 emissions. The machine sends its logs to the SIEM system. The SIEM system is correctly configured to detect these types of attacks by looking at the levels of the CO2 emissions. If the level surpasses a threshold, an alert is generated. Cybersecurity personnel will then consume these alerts from the SIEM. The figure also represents a worker using a BMI, which is sending its logs into the SIEM system. These logs, because they can have the worker's personal information, must be anonymised and protected. The SIEM also generates alerts when a technology that could harm the worker behaves abnormally.

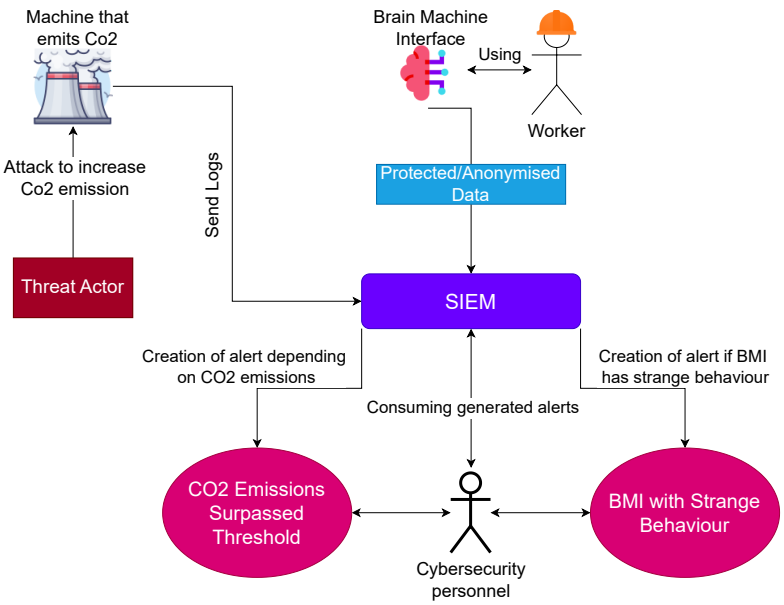

Figure 4.8: *Illustration of the operational workflow of a SIEM system in Industry 5.0.*

Industry 5.0 introduces a transformative shift in industrial operations by prioritising human-centricity, sustainability, and resilience, but these advancements also complicate cybersecurity incident detection and response. The proliferation of diverse devices expands the attack surface and generates vast, heterogeneous log data, increasing operational complexity and financial costs for SIEM platforms. Common attacks like

DoS and MitM persist across technologies, yet countermeasures must be tailored to each enabling technology. Sustainability-driven cybersecurity now includes monitoring environmental telemetry, such as CO2 emissions and energy usage, to detect sabotage or system failures, requiring context-aware analytics and multi-stakeholder response coordination. Human-centricity adds further challenges, as sensitive personal data from devices like BMI must be anonymised to comply with privacy regulations. Ethical considerations around cognitive privacy and consent demand reconfigured incident response protocols and enhanced analyst training. Overall, Industry 5.0 necessitates integrated, adaptive cybersecurity frameworks that align technological innovation with ecological and human values.

4.4 Summary

Industry 5.0 introduces a transformative shift in industrial operations by prioritising human-centricity, sustainability, and resilience, but these advancements also complicate the implementation of the cybersecurity dimensions. Some challenges are transcendental across multiple dimensions, such as privacy concerns related to PII, introduction of new attack vectors and surfaces, increase in number and heterogeneity of devices and sustainability metrics.

The identified challenges of Industry 5.0 in the respective cybersecurity dimensions, in this chapter, will be tested in the next chapter through a case study. The case study is about the stone cutting industry, which will be used to confirm that organisations could face these challenges while transitioning to Industry 5.0.

Furthermore, the problems and challenges found will be tested against the created high-level framework, which defines the different dimensions of Industry 5.0.

5
High-Level Framework

This chapter will present and detail the developed high-level framework. Furthermore, it will highlight the significance of creating this new framework and explain why the existing frameworks do not facilitate the complete transition to Industry 5.0. Existing high-level Industry 4.0 frameworks will be analysed, namely Industrial Internet Reference Architecture (IIRA) and Reference Architectural Model Industrie (RAMI) 4.0. Likewise, two academic high-level frameworks for Industry 5.0 will also be analysed.

The IIRA provides a model for businesses to develop future products and business strategies by merging OT and IT (Consortium, 2022). As can be seen in Figure 5.1, the model focuses on the IIoT and is organised into four different Viewpoints: Business Viewpoint, Usage Viewpoint, Implementation Viewpoint and Functional Viewpoint. These Viewpoints are created to identify and classify the common preoccupations of an IIoT architecture. The Business Viewpoint identifies the participants involved in the system along with their business views, values, and objectives. The Usage Viewpoint focuses on the system's expected business outcomes. The Implementation Viewpoint looks at the technologies that are required to implement the functional components of the system and their communication schemes. Finally, the Functional Viewpoint examines the functional components of the system and how they interact with each other and with the external environment (Consortium, 2022).

The RAMI 4.0 gives companies a framework for developing future products and business models, with the major goal of improving the manufacturing process through digitalisation (Plattform Industrie 4.0, 2018). RAMI 4.0 consists of a three-dimensional coordinate system that describes all crucial aspects of Industry 4.0. The three axes are the Layers Axis, the Life Cycle & Value Stream axis and the Hierarchy Levels axis. The Life Cycle & Value Stream axis represents the life cycle of facilities and products, from the first idea to decommissioning. The Layers axis is divided into six layers, each representing the decomposition of an asset into its properties. The Hierarchy Levels axis represents the flexible communication model, in which systems and machines can communicate across hierarchy levels (Plattform Industrie 4.0, 2018; Li et al., 2020).

Leng et al. built a three-dimensional architecture for the implementation of Indus-

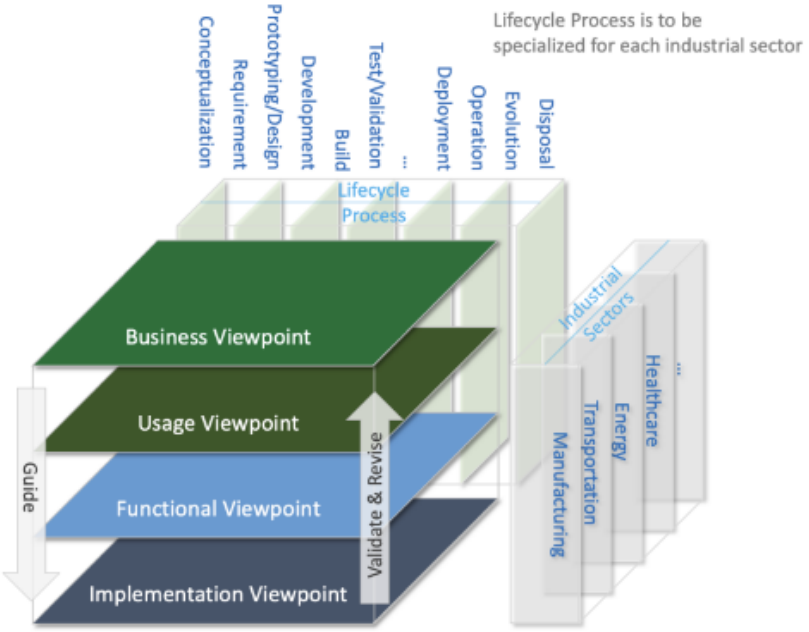

Figure 5.1: *Relationship among IIRA viewpoints. Source: Consortium, 2022.*

try 5.0 (Leng et al., 2022). This architecture was made to stimulate discussion on the different components of Industry 5.0. Furthermore, the architecture is composed of the technical dimension, reality dimension, and application dimension. The technical dimension represents the enabling technologies. The reality dimension represents the implementation path. Finally, the application dimension represents the different application sectors of Industry 5.0 (Leng et al., 2022).

Both IIRA and RAMI 4.0 are high-level reference architectures, which lack detailed information and are more general on how to implement Industry 4.0. The IIRA model includes cybersecurity concerns in almost every Viewpoint. However, the guidance on how to implement such cybersecurity measures is not detailed or explained. For example, the model says that security functions, such as encryption and authentication, are needed in every functional component but does not elaborate further. The model addresses users in the Usage Viewpoint, which is ideal for a human-centred Industry 5.0 implementation. However, the IIRA focus too much on IIoT systems, and Industry 5.0 is much more than that. Despite RAMI 4.0's much broader focus, it lacks even more detailed information on how to implement cybersecurity measures. Furthermore, this model does not address the human side of the manufacturing process. Neither of these models addresses the green transition process. The two academic high-level frameworks for Industry 5.0 share a common deficiency: a failure to address cybersecurity. Despite not addressing cybersecurity, both of these frameworks do address the other major requirements of Industry 5.0, although the coverage is broad.

In order to create a new high-level framework, it is first necessary to identify the problems of the existing frameworks in a deeper sense. RAMI 4.0 will be considered the base of this new high-level framework. In this case, the analysis will begin in each

axis of RAMI 4.0 to identify the modifications required for Industry 5.0. Figure 5.2 highlights the different aspects of RAMI 4.0 that need to be modified to accommodate Industry 5.0. The yellow rectangles represent the aspects that need to be modified to accommodate the green transition. The blue rectangle represents cybersecurity, and the pink rectangle represents the human-centred manufacturing process. The Layers axis must represent properties such as sustainability and resilience of the products/assets, as well as security and privacy aspects. Furthermore, the Life Cycle & Value Stream axis must demonstrate the recyclability and reuse of the products during development and use, accompanied by clean production. The Hierarchy Levels axis should be reworked to accommodate the cybersecurity, social and environmental aspects. In this dimension, the organisational structure is depicted as a hierarchy. However, this hierarchy is outdated, as products can now communicate across different levels of the hierarchy, making it more flexible.

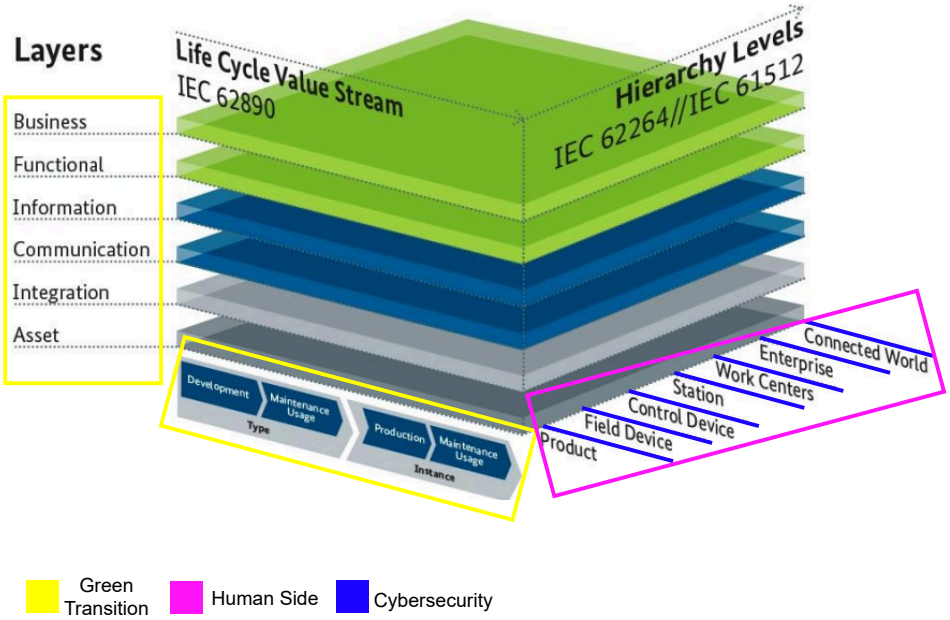

Figure 5.2: *Highlight of RAMI 4.0's aspects that need modification. Adapted from: Plattform Industrie 4.0, 2018.*

5.1 High-Level Framework for Industry 5.0

Based on the identified problems, the new high-level framework, which from now on will be referenced as High-Level Framework for Industry 5.0 (HLFI 5.0), was developed to help people better understand the different components of Industry 5.0. HLFI 5.0 can be viewed in Figure 5.3. The Layers axis was renamed as the Properties axis to better represent the vertical axis. The properties are divided into physical and digital. For example, the sustainability property is purely physical, while the privacy & security are digital. Taking as a base RAMI 4.0, the Properties axis represents the different properties of an asset. Compared to RAMI 4.0, the properties added were privacy &

security, resilience and sustainability. These properties reflect the need for the organisation to be resilient, which requires a good cybersecurity posture, and to align with sustainability values.

Starting from the bottom, the Physical Asset represents the actual physical asset being implemented. The Resilience property represents the properties that allow the asset to safely adapt to disruptions and not cause any damage if disrupted. The Sustainability property represents the properties of an asset related to sustainability, such as energy consumption. The Integration property represents the physical connection of the asset with the others, while the Communication property is the "language" that is spoken between the connections. The Information property constitutes the data and information that the assets hold and communicate with others. The Functional property is the functions of the asset, while the Privacy & Security property represents the privacy and security concerns that an organisation must have with the asset. Finally, the Business property represents the organisation's business goals for the asset. A more practical example of the properties will be done in Section 5.2.4.

The Asset Life Cycle axis was also renamed to better explain the axis. In this axis, all the assets must be recycled or reused. First, an asset is acquired by internal or external production of the asset. The internal product is sold to the client, and then he decides what to do with the product. However, the product must be developed with materials that are good for recyclability and reuse. Also, the process of production should be relatively clean, and production waste should also be recycled and/or reused. Assets that are externally produced and used by an organisation, should they reach the decommissioned state, they must be recycled and/or reused. This axis makes sure organisations align with Industry 5.0's sustainability goals and circular economy.

The Hierarchy Levels axis was renamed to the Context axis. This axis represents the areas that should be taken into account when transitioning to Industry 5.0. Some assets will represent different roles in different contexts. The Hierarchy axis is composed of:

- Cybersecurity Context;
- Economic Context;
- Natural Environment Context;
- Social Context;
- Organisational Context.

The Cybersecurity Context of an asset is essential for resilience. The Natural Environment Context is key for Industry 5.0's sustainability goals, and the Social Context is a must in order to encompass human-centric ethics. The hierarchy levels present in RAMI 4.0 were replaced by the organisational context because not all assets in Industry 5.0 can have hierarchical-based communication, and there are other contexts that Industry 5.0 demands (e.g. sustainability context). A physical strain sensor located on the factory floor, which communicates directly with the cloud, cannot be fitted in a normal hierarchical-based communication.

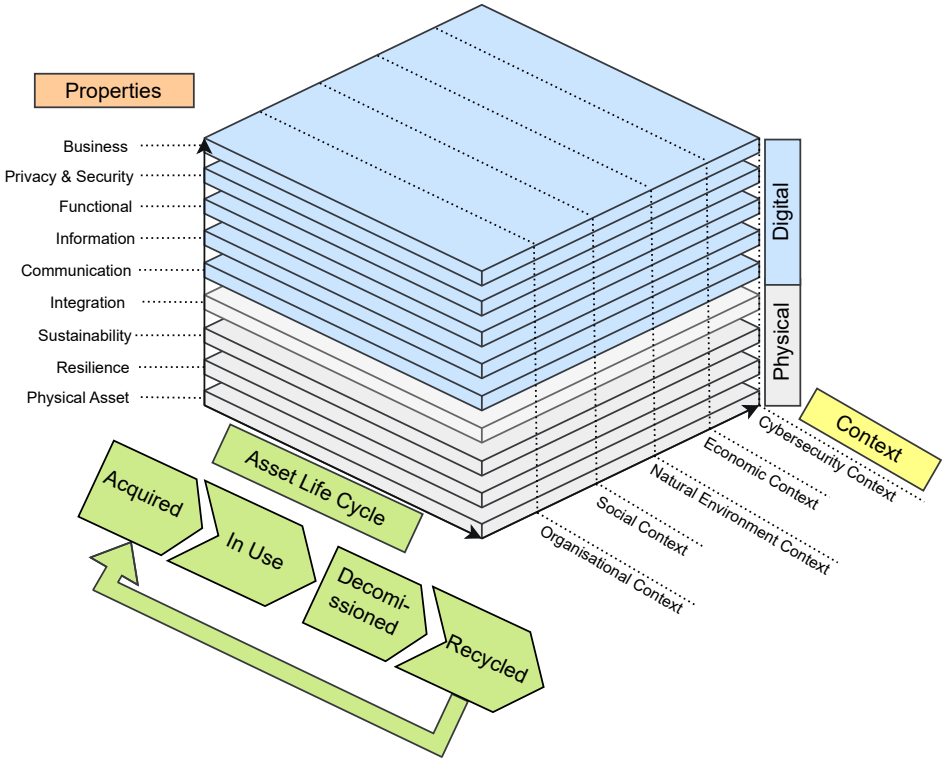

Figure 5.3: *Developed High-Level Framework for Industry 5.0.*

In the next section, a case study will be created to simulate the stone cutting industry. This case study will be used to validate HLFI 5.0 and the challenges of Industry 5.0 encountered in the last chapter.

5.2 Case Study - Natural Stone Cutting Industry

This section begins by presenting a simplified architectural diagram of a typical stone cutting industrial plant. This visual representation outlines all the levels of an architecture, from the physical process (Level 0) to the Cloud/Internet (Level 5). By mapping these elements, the case study establishes a concrete context for analysing the challenges discussed in Chapter 4. These previously abstract problems, ranging from sustainability issues to human-centric ethical problems, are now grounded in a real-world industrial setting, demonstrating their tangible presence and impact within the stone cutting industry.

Following this contextualization, the case study is going to be used in RAMI 4.0 by trying to implement a cobot through it. Then, it proceeds to align the previously identified problems with HLFI 5.0 to interpret Industry 5.0 principles. Each issue is matched to a corresponding dimension of the framework. This mapping not only validates the relevance of HLFI 5.0 but also illustrates its adaptability to real-life industrial scenarios. Furthermore, the same implementation of a cobot is done, but now through HLFI 5.0. By bridging theoretical constructs with practical observations, the section

confirms that the proposed framework and challenges are not merely conceptual but are equipped to guide the evolution of traditional manufacturing environments toward Industry 5.0 readiness.

A detailed description of Figure 5.4 provides a clearer understanding of the stone cutting industry case study. At the foundation, Level 0 represents the physical process Trend Micro, 2020, which integrates three main components: a solar panel system, a collaborative robot (cobot), and a Computer Numerical Control (CNC) machine. The solar panel system generates renewable electricity to partially offset the high energy demand of stone cutting operations (Huawei, 2025). This not only reduces electricity costs but also improves the company's Environmental, Social, and Governance (ESG), a sustainability metric increasingly valued by both investors and customers (Sustain, 2024). The cobot, equipped with sensors, actuators, and grippers, assists human operators in handling heavy and irregularly shaped stone slabs, reducing workplace injuries and improving ergonomics (Mirmex Motor, 2025). Modern cobots can handle payloads of up to 50 kg (FANUC, 2025), making them suitable for lifting and positioning raw materials into the CNC machine. The CNC machine itself, equipped with a diamond-tipped blade, performs precision cutting by gradually removing material until the programmed shape is achieved (Tile, 2025). At this level, the three machines operate independently of one another and do not communicate directly Trend Micro, 2020. Despite this, the CNC machine and cobot are located in the same place: the factory floor MATICS, 2025. The solar panel system is located on top of the building Huawei, 2025, generating energy for the machines despite not communicating with them directly.

Level 1 consists of the basic controllers that directly govern the physical process and act as the first layer of automation intelligence (Trend Micro, 2020). The charge controller manages the solar panel system by regulating voltage and current, preventing overcharging, and ensuring stable energy delivery to the facility (Morningstar, 2025). In parallel, a PLC is deployed to the Cobot and a CNC controller to the CNC machine. The PLC receives continuous input from sensors—such as torque, position, and payload sensors in the cobot (Industrial Shields, 2025). The CNC controller is specifically designed to handle tasks such as multi-axis interpolation, toolpath execution, and real-time motion coordination (Radonix, 2025). This enables the cobot to safely handle heavy stone slabs and the CNC machine to execute cutting operations with accuracy. By enforcing safety interlocks and deterministic control, Level 1 ensures that the physical process remains stable and reliable under varying operating conditions (Trend Micro, 2020). Communication at this level is deliberately constrained. Controllers interact only with their respective machines and with supervisory systems in Level 2, rather than with each other directly (Trend Micro, 2020). This design reduces complexity and enhances security, while still allowing higher levels to coordinate process-wide optimisation. The protocol used for the Cobot is OPC UA (Universal Robots, 2025b), a modern protocol developed with security in mind. The CNC machine and the solar panel system use a traditional protocol, Modbus TCP (MDCplus, 2025). This protocol

was not developed with security in mind. However, both these protocols can guarantee low-latency and fault-tolerant data exchange. In this way, Level 1 provides the essential bridge between raw sensor data at Level 0 and the supervisory visualisation, logging, and design functions at Level 2, forming the backbone of safe and efficient stone cutting operations. In terms os location, the PLC and CNC controllers are located beside the cobot and CNC machine (MATICS, 2025). This will allow for less wiring and better response times. The charge controller is in a separate and dedicated room, which allows for a more controlled environment with less dust and vibrations from the other machines.

At Level 2, supervisory control is established (Trend Micro, 2020) through systems such as an HMI, a log collector, and a CAD workstation. The HMI provides real-time visualisation of industrial processes, enabling operators to monitor Key Performance Indicator (KPI) such as CNC throughput, energy consumption, and machine input/output states (Inductive Automation, 2025a). The log collector aggregates operational data from the controllers, indirectly capturing information from the solar panels, cobot, and CNC machine (Solar Winds, 2025). This includes metrics such as energy generation, robotic movements, and task completion times. Both the log collector and the HMI gather information about the physical process through the controllers. They use the communication protocols mentioned previously. The CAD workstation plays a critical role in CNC operations, allowing engineers to design stone specifications with high precision, in specialised software, thereby reducing the likelihood of human error (Industries, 2024). The CAD project is then exported to a G-code file, which is the programming language CNC machines understand. This file is then pasted into a USB drive, which is used on the CNC controller. The CNC controller reads the code and executes the machine operations (Industries, 2024). These 3 computers are located in the control room, which is physically located above the factory floor. These room has large observation windows where the engineers and supervisors can oversee the physical process (Vestal, 2022).

Level 3 represents the final layer of the OT domain (Trend Micro, 2020) and consists of a Data Historian and an EWS. The Data Historian is a specialised software system designed to store time-series data from the physical process, enabling long-term analysis of productivity, efficiency, and bottlenecks (influxdata, 2023). The Data Historian queries the controllers for data in a fixed time interval of five minutes. The EWS provides a more general-purpose environment, hosting applications such as the Data Historian itself, as well as technical programming and analysis tools like Matrix Laboratory (MATLAB) and Python (Illinois, 2025). The MATLAB and Python are used to process data from the Log Collector and Data Historian and use it for statistical analysis, anomaly detection, or trend forecasting (Murad, 2023). This level supports advanced diagnostics, optimisation, and engineering tasks. The EWS is located in the control room (Vestal, 2022), while the Data Historian is in a separate room for the servers.

Between the OT and IT domains lies Level 3.5, the Demilitarized Zone (DMZ)

(Trend Micro, 2020). This layer is protected by firewalls that strictly regulate communication between Levels 3 and 4, preventing lateral movement from the IT network into the OT environment (Zscaler, 2025). The DMZ contains a Jump Server and a Patch Server. The Jump Server acts as a secure entry point for external operators, who may connect remotely via Secure Shell (SSH) and multi-factor authentication (forense.io, 2025). Once authenticated, they can access the Patch Server, which centralises the management of software and firmware updates (Firch, 2024). This avoids the exposure of the Patch Server to the internet. In computers and servers, such as Log Collector, CAD Workstation, and EWS, a software is installed so it can report the software and firmware versions to the Patch Server (Firch, 2024). Based on that, the Patch Server compares the versions received to the catalogue of available updates and determines if an update is needed (Firch, 2024). However, on the machines and controllers, this software is not installed. Instead, the vendors alert and make available the new update for the machine, which an engineer has to download and apply manually to the machine or controller (Belal, 2025). This architecture ensures that critical OT assets are not directly exposed to external networks. Both these servers are located in a separate room for servers.

Level 4 corresponds to the enterprise IT domain, where business operations are managed (Trend Micro, 2020). This includes web servers, email servers, and desktop systems used by white-collar employees. The web server hosts the company's online platform, enabling customers to order personalised stone cutting services (Mozilla, 2025). The email server is maintained on-premises to ensure full control over sensitive communications and to allow the implementation of custom security measures such as encryption and access control (Ellis, 2023). Both these servers are exposed to the internet, with a Firewall protecting them. The Firewall has strict rules in order to protect the exposed web and email servers. The rules are the following (HostSailor, 2024):

- Allow inbound TCP traffic on ports 80 and 443 from any IP address to the Web Server IP.
- Allow inbound traffic on Simple Mail Transfer Protocol (SMTP) ports (25, 465) from any IP to the Email Server IP, in order to receive email.
- Allow Internet Message Access Protocol (IMAP)/Post Office Protocol 3 (POP3) ports (143, 993, 110, 995) only from trusted internal IP ranges to the Email Server IP. This allows internal IP to retrieve email from the server but not external IP.
- Block all other inbound traffic.

The desktops on Level 4 are for business purposes only. In these desktops, logistics, production planning and scheduling, compliance management and financial analysis are done. This level bridges the industrial process with customer-facing and administrative functions. Level 4 is located outside the factory floor and the control rooms' building, in an office.

Finally, Level 5 extends into the cloud (Sangfor Technologies, 2025), where advanced cybersecurity and monitoring solutions are deployed. A SIEM system gathers

logs from all devices across the network. For Windows and Linux machines, dedicated agents transmit logs directly to the cloud, while for Level 0 and Level 1 devices (Industrial Defender, 2025a), data is first aggregated by the log collector and Data Historian before being forwarded. An EDR solution is also deployed, with agents installed on compatible systems such as the cobot and its controller. However, due to technical restrictions, EDR agents cannot be installed on all machines and controllers. The gathered logs from the agents, log collector and data historian are sent to the cloud via Hypertext Transfer Protocol Secure (HTTPS) (Datadog, 2025). This makes sure the logs are confidential. Also, a certificate is used for integrity purposes. Integrity and confidentiality are key to maintaining privacy and confidence in the logs.

Furthermore, in the SIEM, a multitude of use-cases were deployed by the security team (Splunk, 2025). One of the use-cases takes a look at the pollution levels of the CNC machine. If it surpasses a certain threshold, it generates an alert for the engineers to see and take action. The EDR has multiple out-of-the-box detections and responses. However, in the cobot and PLC, which are the only machines that have the EDR, the response is disabled. On these machines, the EDR is only there to detect anomalies, as a response could cause disturbance on the machine (Industrial Defender, 2025b). If the machine were holding a 40kg stone, this could be dangerous for the operator and the stone. The security team, in conjunction with the risk team and the managers, decided to take the risk of disabling the response of the EDR in these two situations. Together, the SIEM and EDR solutions provide centralised visibility, threat detection, and incident response capabilities, ensuring the resilience and security of the entire stone cutting operation.

This case study uses enabling technologies from Industry 5.0, such as a Cobot and renewable energy sources like a solar panel system. These technologies were chosen because they serve a purpose in the stone cutting industry, and they serve the purpose of showing the challenges that they bring to security with their implementation.

5.2.1 Governance and Risk Management

In this case study, asset inventory is made through software in the cloud. The software is irrelevant for the case study. The presented case study, despite being simple, already presents a diverse array of formats. This heterogeneous environment makes the creation of an asset inventory slightly harder. For example, the data being stored in the asset inventory by a cobot and by an PLC is completely different. Some cobots are movable, PLC are usually static, which creates the need to save information about a cobot's location but not the PLC location. Which tasks the cobot is used for is also useful information; the PLC always has the same task, which is controlling the cobot. Furthermore, A cobot needs to be associated with one or more users; the PLC does not. In a PLC, we might need to know what code or version of the code is being used; the cobot does not need this. These simple examples show how an increasingly heterogeneous environment can complicate the asset inventory by needing to store different

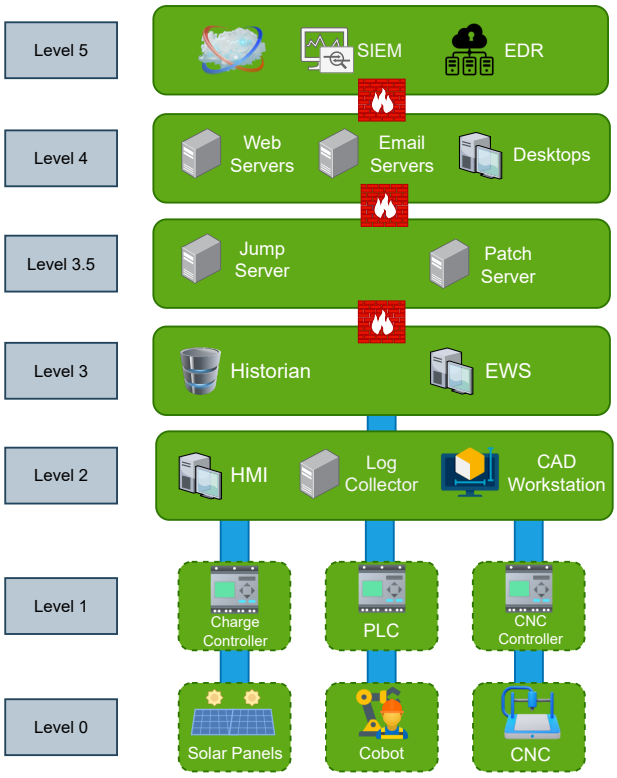

Figure 5.4: *Case study's architecture for stone cutting industry.*

attributes for every single machine.

Still in the asset inventory, one might find problems related to the sensitivity of the data stored. In this case study, the human operator uses facial recognition and the fingerprint to unlock the cobot. This type of information might be useful in an asset inventory in order to better identify the human operator. However, this raises concerns about the storage of the PII. The storage of PII must comply with strict regulations, such as GDPR, in order to protect the human operator. Using encryption, tight access control and audit trails are ways to prevent PII from being used for the wrong causes.

The asset inventory should play a crucial part in achieving Industry 5.0's sustainability goals. In this case study, the asset inventory includes a field in every device for pollutant emissions and energy consumption. In the case of the solar panel system, the fields are empty. Cobots, computers and servers themselves do not have a direct impact on air pollution; however, they increase the energy consumption. In the CNC machine, air pollution is generated through airborne particles and emissions from cutting fluids and machining processes (Great, 2024). The CNC energy consumption is also taken into account in the asset inventory. Furthermore, a field for lifecycle tracking is present in every asset record. The possible values are: acquired, in use, decommissioned and recycled. This field allows for better resource usage tracking and aligns with a circular economy. These fields are just some examples of the new needs for asset inventories. Also, these fields allow for better monitoring of pollutant emissions that might be required to be controlled by regulation and that might result in fines if

not.

As previously mentioned, asset inventory is key for cybersecurity, and resilience supports multiple cybersecurity functions, including vulnerability management, threat intelligence, endpoint security, and incident response. However, modern industrial ecosystems are increasingly interconnected, which implies that disruptions are more impactful and harder to contain. In this case study, the stone used by the CNC is directly dependent on a local mine. The clients of this stone cutting industry are directly dependent on this CNC machine working. Also, the used SIEM and EDR solutions are in the cloud, and directly depend on the availability of the service from the providers. Access to these solutions is dependent on the availability of the organisation's internet. The safety and privacy of the clients and workers are directly dependent on the SIEM and EDR solutions. The asset inventory of the case study contains a field for upstream and downstream dependencies of each asset. The CNC machine will have the stone from the local mine as the upstream dependency and the selling of the personalised stone cutting to the client as the downstream dependency. These allow the organisation to identify single points of failure, such as the stone from the local mine. With this attribute in the asset inventory, the organisation can search for alternative suppliers of stone.

Asset inventory also faces some modifications needed because of new technologies that connect machines to humans. Technologies such as cobots and strain sensors now need to be associated with a human operator. Furthermore, a schedule of use by the operator should also be integrated into the asset inventory. This allows for tracking of usage patterns and simplifies access control configuration. In this case study, the asset inventory has a field for the owner where the human operator is associated. Sometimes, more than one user can be associated with the cobot, depending on the vacations and holidays. There is also a field detailing the schedule of use for the human operator. In this case, the human operator works the standard, 9 AM to 1 PM and 2 PM to 6 PM.

Vulnerability management in Industry 5.0 faces the challenge of a heterogeneous environment, especially when it comes to scanning capabilities. In the case study, there are novel devices that use novel technology. The vulnerability management software needs to be able to handle these new technologies. While scanning the internal network, the software must be able to identify the cobot and the solar panel system, and their respective software, firmware and hardware versions. If the software is not able to, then it leaves the security professionals blinded about the vulnerabilities that the machines possess. Another problem that arises with a heterogeneous environment is the patching and scanning of the devices and machines. In traditional environments, the type of devices and the type of patching and scanning used were separated by the levels. Traditionally, in level 0, only passive scanning and patching were used because of the sensitivity of the machines and the physical process. In this case study, the solar panel system and the cobot were developed with these problems in mind, and so active scanning and patching can be used because they are supported. The CNC, on the other hand, is old and has limited resources; an active scan could lead to disruptions in pro-

duction, and so passive scanning and patching should be used. The type of scanning and patching is now dependent on the device on the individual level, not on the whole level.

In Industry 5.0, the close interaction between machines and humans introduces new moral obligations when it comes to vulnerability management. In this case study, a cobot is used by a human operator. A vulnerability in the cobot could potentially harm the operator. For this type of machine, the vulnerability score should take the harm to the operator into consideration. A vulnerability like this should be urgently remediated. Vulnerability management must therefore consider the psychological, physical, and social impacts of vulnerabilities. Patching, therefore, must be approached with an unprecedented level of urgency and human safety in mind.

Cyberattacks could lead to resource waste and excessive energy consumption, and vulnerability management should take that into account. For Industry 5.0, the sustainability pillar should change how vulnerability management is done. Vulnerability management should consider the harm to both humans and the environment. If the cobot used in this case study has a vulnerability that allows the threat actor to significantly increase the energy consumption, the vulnerability management software should classify the vulnerability a little bit higher in Industry 5.0 than it did in other industrial revolutions. If the CNC has a vulnerability that allows the threat actor to slightly alter the CAD design to use more material, then the impact scoring of the vulnerability should have resource waste as an increasing vector.

With the increase in the number of devices and machines and the heterogeneity of the environment, new challenges arise for Threat Intelligence in Industry 5.0. These challenges are related to the increase in attack surface and vectors. In this case study, the introduction of the solar panel system into the network introduces new attack vectors for threat actors. Furthermore, threat actors that specialise in attacking this type of infrastructure can now consider the organisation as a target. The introduction of penalties imposed by excessive air pollution by an organisation also introduces perverse incentives for threat actors. In this case study, the CNC machine causes air pollution when cutting the stone. If a threat actor manages to exploit the machine to increase the air pollution to a level where the organisation is fined, then, despite not gaining anything, the threat actor could be incentivised to create these problems for organisations. A larger and more heterogeneous environment necessitates adaptive threat intelligence capabilities.

In Industry 5.0, threat intelligence should also extend beyond internal systems to encompass supply chains, where disruption can create a cascading effect, affecting the resilience of an organisation. In this case study, it was previously identified that the CNC machine has an upstream dependency on stone from the local mine and a downstream dependency on selling the stone to clients. If any cyberattack occurs at the mine, which stops the extraction of the stone, the CNC machine organisation will be affected, which in turn causes the client to be affected, and the organisation. The case study organisation does not have visibility into the threats that come from the lack of cyber-

security in the mine. To resolve the problem, organisations could adopt collaborative threat intelligence platforms. In the previous case of the cyberattack at the mine, if a collaborative threat intelligence platform had been used between the organisations, the mine could have shared early indicators of compromise or suspicious activity with the case study organisation. This proactive exchange of threat data would have enabled the anticipation of potential disruptions and activated contingency plans, such as sourcing alternative materials or adjusting production schedules.

With the introduction of new technologies in Industry 5.0, such as cobots and BMI, threat intelligence must account for new attack vectors related to the human-machine interaction. These new attack vectors could cause risks to mental and physical safety. In the case study, the cobot could be manipulated by a threat actor to cause phyisical damage to the human operator. Threat intelligence must contain information if the attack is capable or not of cause mental and phyisical damage.

Threat intelligence frameworks such as MITRE ATT&CK for ICS, are able to classify this new type of attack. If a threat actor manipulates the cobot in order to cause physical damage to the operator, the impact, according to the framework, is loss of safety, manipulation of control and maybe loss of control. However, if an attack involves stealing personal data from our asset inventory, for example, the facial recognition or the fingerprint used to unlock the cobot, then there is no classification for this impact on the matrix.

5.2.2 Security Architecture and Design

With the integration of solar panels, cobots, and legacy CNC machinery, the case study organisation exemplifies the complexity of implementing ZTA in Industry 5.0. The convergence of IT and OT domains creates a network topology that increases the risk of lateral movement. In this case study, the CAD Workstation sometimes has access to the internet to download some CAD files shared by an external partner. If the CAD files are compromised, the workstation could be compromised. If the CAD workstation is compromised, then the CNC machine could also be compromised. If a threat actor compromises the CAD workstation, they could potentially pivot across the network to reach the CNC machine. ZTA mitigates this by enforcing strict identity verification and micro-segmentation, but the heterogeneous nature of these assets complicates policy enforcement.

The CNC machine, a legacy OT asset, lacks support for modern identity-based access controls and secure telemetry. This makes it difficult to integrate into a unified Zero Trust framework. For example, while the cobot may support biometric authentication, the CNC machine may rely on outdated protocols or hardcoded credentials. This fragmentation creates operational blind spots where Zero Trust policies cannot be uniformly applied. Identity verification for novel devices like cobots also presents challenges. The cobot in the case study uses facial recognition and fingerprint authentication, but integrating these into a centralised identity management system is non-trivial.

Proprietary firmware and limited interoperability hinder seamless integration.

Moreover, this simple case study only has three machines and three controllers. If a real industrial plant were taken into account, where, possibly, hundreds of machines were present, the manual configuration and management of policies and micro-segmentation would be almost impossible. Automation of these tasks is essential with the constant increase in the number of devices and the complexity of environments.

From a sustainability perspective, ZTA indirectly supports environmental resilience by preventing cyberattacks that could disrupt critical infrastructure. In this case, safeguarding the CNC machine from manipulation helps avoid excessive air pollution and regulatory penalties. However, the continuous authentication and telemetry required by ZTA may increase energy consumption, especially when applied to resource-constrained devices like controllers. To align with Industry 5.0's sustainability goals, the organisation must adopt energy-efficient protocols and intelligent data reduction techniques within its ZTA implementation.

Human-centricity introduces further complexity. The cobot's interaction with human operators demands adaptive trust models that respect user autonomy while ensuring safety. Continuous monitoring of operator behaviour may raise privacy concerns, especially if biometric data is used for authentication. In the case study, telemetry from the cobot could be used to detect anomalous behaviour, but this must be balanced against ethical considerations. Transparent, consent-based monitoring frameworks are essential to ensure that Zero Trust mechanisms empower rather than constrain human agency.

The case study organisation's architecture is made in a traditional segmentation model like the Purdue Reference Model. This shows that an organisation can still follow the Purdue Reference Model even using some of the new enabling technologies of Industry 5.0. However, if the organisation decides to implement something like an IIoT device that connects to the cloud, then the traditional network segmentation will start to have problems.

This case study in stone cutting also shows that air-gapping is hard to use in this type of industry. The CNC machine needs to connect to the CAD workstation and to the Log Collector. The solar panel system needs to be able to talk with the Log Collector, and the same goes for the cobot.

5.2.3 Security Operations

The case study organisation's deployment of an EDR solution in the cloud (Level 5 of the architecture) reflects a forward-thinking approach to endpoint security. However, the heterogeneity of its environment, including cobots, CNC machines, solar panel controllers, and strain sensors, exemplifies the limitations of traditional endpoint protection. For instance, the CNC machine operates on legacy firmware that does not support modern EDR agents, while the solar panel system has constrained processing capabilities, making it incompatible with conventional antivirus or telemetry-heavy tools.

These architectural constraints hinder uniform endpoint protection and increase the complexity of securing the entire asset inventory.

The licensing model of the cloud-based EDR solution also presents cost scalability issues. As the organisation expands its use of Industry 5.0 technologies, the number of endpoints grows rapidly. Each new cobot or controller adds to the licensing burden, potentially straining cybersecurity budgets. In this case study, a new CNC machine, which allows for the installation of an EDR agent, will soon arrive at the plant. The organisation must account for the extra money that will be spent to install the new agent on the CNC machine. Sometimes these licenses can cost up to thousands of euros for a single agent. If the organisation is not willing to pay, then the machine will have to stay unprotected.

The evolving threat landscape in Industry 5.0 introduces new attack surfaces that the case study must address. For example, the cobot's human-machine interface could be exploited to cause physical harm to operators, while the CNC machine could be manipulated to exceed carbon emission thresholds, triggering environmental penalties. The EDR system must be capable of detecting these unconventional threats, including DoS and MitM attacks, which are prevalent across Industry 5.0 technologies. Countermeasures must be tailored to each device type-what works for a cobot may not apply to an CNC machine or solar panel system.

From a sustainability perspective, the case study highlights the potential for environmentally targeted cyberattacks. The CNC machine's emissions are monitored, and a threat actor could manipulate its operation to exceed regulatory limits. The EDR system must be equipped to detect such anomalies, correlating telemetry data with operational thresholds. Failure to do so could result in fines and reputational damage. While the EDR solution may already support such detection, its effectiveness depends on integration with environmental monitoring systems and contextual awareness of industrial processes.

Human-centricity adds another layer of complexity. The EDR system must anonymise or encrypt PII data before transmission to the cloud, ensuring privacy and regulatory alignment. In the case study, the cobot gets some PII from the human operator, such as fingerprint and facial recognition, in order to unlock. This type of information could be important for the EDR to detect and identify the non-authorised operator trying to access the machine. However, this type of information is still PII and needs to be secured. Moreover, aggressive threat mitigation-such as terminating a cobot process during a suspected attack-could disrupt operations and endanger human safety.

The case study organisation's use of a cloud-based SIEM solution, at Level 5, provides centralised visibility across its diverse industrial ecosystem. However, the proliferation of heterogeneous devices-including cobots, CNC machines, and solar panel systems-introduces significant complexity in both detection and response. Each device generates distinct log formats and telemetry, complicating ingestion, normalisation, and correlation within the SIEM. For example, the CNC machine may emit logs related to the mechanical position of the blade and emissions, while the cobot logs be-

havioural patterns and biometric access events. This diversity increases operational noise and difficulty in filtering and may lead to delayed or missed detections. Another problem is the increase in the number of devices, which leads to increased prices in the log ingestion, especially when log ingestion is priced per gigabyte. In the case study, the new CNC machine that will soon arrive at the plant, not only will have the increased costs of the EDR agent but also of the additional logs that it will generate and ingest into the SIEM.

The solar panel system, integrated into the network for energy optimisation, introduces new attack vectors that must be accounted for in detection rules. A threat actor could manipulate its output or telemetry to disrupt energy balance or mask malicious activity. Similarly, the cobot's interaction with human operators introduces novel risks-such as physical or mental harm-that require specialised alerting mechanisms. The SIEM must be configured to detect anomalies across these varied endpoints, necessitating new tailored rules and countermeasures for each device type.

Sustainability-related threats are particularly relevant in this case study. The CNC machine's CO2 emissions are monitored, and a cyberattack could deliberately increase output to trigger environmental penalties. The SIEM system must ingest real-time telemetry from the machine and correlate it with operational baselines to detect such sabotage. For instance, a sudden spike in emissions outside of scheduled cutting operations could indicate a compromise. These alerts must be context-aware, distinguishing between mechanical faults and malicious intent. The integration of environmental data into the SIEM reflects the organisation's commitment to cyber-eco resilience, where digital security supports ecological integrity.

Responding to sustainability incidents requires coordination across multiple departments. In the case study, if the SIEM flags excessive emissions in the CNC machine, cybersecurity teams must collaborate with environmental compliance officers to validate the alert, initiate forensic analysis, and report findings to regulatory bodies. Automated workflows within the SIEM can streamline this process, triggering escalation protocols and generating audit trails.

Human-centricity introduces additional challenges. In the case study, logs from the cobot's facial recognition system must be anonymised and secured to comply with privacy regulations. Furthermore, the SIEM must generate alerts when technologies that interact with humans exhibit abnormal behaviour, such as erratic cobot movements or unauthorised access attempts. These alerts must be handled with sensitivity, ensuring that incident response protocols respect privacy and human safety.

5.2.4 HLFI 5.0 Applied to the Stone Cutting Industry

This subsection will apply HLFI 5.0, which can be seen in Figure 5.3, to some problems of cybersecurity in the context of Industry 5.0, and to one of Industry 5.0's technologies that was applied in the case study. The previously identified problems in Chapter 4 were applied to the case study of a natural stone cutting organisation. These prob-

lems and challenges could be categorised into multiple categories: cybersecurity and resilience, sustainability and human-centric ethics, heterogeneity and an increase in the number of devices. The Industry 5.0 technology, which will be tested, is the cobot.

The cybersecurity context, natural environment context and social context are needed for cybersecurity and resilience, sustainability and human-centric ethics, respectively. The organisational and economic context ties all these other contexts together. For example, sustainability problems will mainly be about the natural environment context; however, it can also affect the economic context and organisational context because of the regulations and fines associated with it.

The sustainability problems of Industry 5.0 also require a lifecycle tracking of assets in order to allow for better resource usage tracking and to align with a circular economy. The framework provides an axis dedicated to the asset lifecycle. The properties axis defines the properties of an asset. In Industry 5.0, the properties of Privacy & Security, Sustainability and Resilience are important, and match the problems related to Sustainability, Cybersecurity and Resilience.

In order to better understand how HLFI 5.0 facilitates the integration and explanation of Industry 5.0 through a structured approach, it will be applied to one practical example: a cobot from the case study. However, first there is a need to do the same practical example but for RAMI 4.0, in order to test the framework and see if it's capable of handling Industry 5.0's demands.

Implementation of Cobot in RAMI 4.0

In order to further prove the contribution of HLFI 5.0. A cobot will be implemented while using RAMI 4.0. The point is to highlight the areas which are lacking with a practical example. RAMI 4.0 was chosen over the IIRA framework because the IIRA was geared specifically towards IIoT, which organisations are not solely build upon.

Starting from RAMI 4.0, in the Layers axis, resilience and sustainability are not present. Using RAMI 4.0 into the cobot, organisations lack visibility into two main aspects of Industry 5.0. If RAMI 4.0, the organisation's lack of visibility into these problems could lead to buying a cobot that lacks resilience and sustainability practices. No resilience means that a cyberattack or any disruption in the cobot could cause harm to both the human operator and the environment. No sustainability could mean a bigger consumption of energy by the cobot, which means bigger electrical bills. Furthermore, the Layer axis lacks privacy and security of the asset. The implementation, in Industry 5.0, of the cobot should have privacy and security aspects in mind, which is not possible by following the RAMI 4.0 structured approach. Otherwise, if the cobot that uses facial recognition and fingerprint to be unlocked is not safe, then this PII could be breached. All these aspects talked about, resilience, sustainability, privacy, and security are present in HLFI 5.0.

The Life Cycle Value Stream axis does not consider Industry 5.0's sustainability goals and circular economy. Despite saying Life cycle, this axis does not seem to have a

cycle. If the cobot reaches its end-of-life, nothing happens to it. When a cobot reaches end-of-life, it needs to be recycled or repurposed, which RAMI 4.0 does not mention. This makes organisations blind to Industry 5.0's sustainability goals, which the HLFI 5.0 does not.

The Hierarchy Levels axis represents the communication hierarchy that the asset has with the different levels in a factory. The cobot could only be applied to the product, field device and control device. The cobot does not participate in the rest of the hierarchy, leaving empty levels in this axis. RAMI 4.0 only looks at the communication aspects in the hierarchy, but a cobot in Industry 5.0 is much than just a device. It needs to have a cybersecurity context where its safety, security and privacy are talked about. Furthermore, a natural environment and social context need to be present if sustainability issues and human-centric ideas are to be discussed. Organisational and economic context will tie the other contexts together by representing the cobot's production levels, costs, organisational workflow and compliance requirements. In RAMI 4.0, if only the communication with the other devices is taken into account, the bigger picture of Industry 5.0 is lost. If cybersecurity is not mentioned, then this could put the cobot in a position of danger to the organisation. Furthermore, it could affect the economic context by increasing costs, and the social context if it puts the human operator in danger. Also, a cyberattack, if it causes the energy consumption of the cobot to go up, then it also affects the natural environment context. This could cause problems in the organisational context if the cyberattack goes out to the public and the ESG score goes down. The Context axis of our developed high-level framework provides a broader view of Industry 5.0's aspects over the Hierarchy Levels axis. Organisations that choose to adopt RAMI 4.0 will be blinded and not have any idea of Industry 5.0's new demands.

Implementation of Cobot in HLFI 5.0

At the Physical Asset property, we encounter the cobot itself: a collaborative robot equipped with sensors, actuators, and grippers, designed to safely share a workspace with human operators. This is the tangible machine that moves stones to the CNC machine.

The Resilience property ensures that the cobot can safely adapt to disruptions. If a human unexpectedly enters its workspace, it slows down or pauses safely. Furthermore, if a cyberattack takes place and the cobot is compromised, then a safe mechanism would prevent harm to the human operator or the environment. This property contributes both to resilience and human-centric ethics.

At the Sustainability property, the organisations ensure that the cobot aligns with sustainability best practices. For example, the energy efficiency rating of this case study's cobot is a B, meaning that the machine does not cause unnecessary energy consumption. The energy efficiency rating also connects with the Economic Context, in a way that more energy consumption means bigger energy bills. Also, the cobot does

not emit any pollutants. These sustainability properties are important for ESG scores and key for Industry 5.0's environmental concerns.

The Integration property connects the cobot into the factory ecosystem. The cobot is directly connected with the PLC. The PLC controls the physical process of the cobot through the use of sensors and actuators. The Communication property guarantees that the cobot speaks the same "language" as its direct links. In this case, the direct link is the PLC. As discussed previously, the industrial communication protocol used by the cobot is OPC UA.

At the Information property, there is the information communicated with the direct links. What type of information is sent and/or received? In the case of the cobot, the communication is with the PLC. The sensors on the cobot send data such as operational status, position, motion data and safety information. While the PLC send to the actuators: start/stop commands, speed and position setpoints and safety commands. The Functional property is where the organisations define the functions and services of an asset. In this case, the cobot's functions are to pick up a heavy stone and place it into the CNC machine. This function will be controlled by a human operator.

At the Privacy & Security property, organisations must evaluate the privacy and security of an asset. Security and privacy include both physical and digital. In terms of physical security and privacy, the cobot is present on the factory floor. The factory floor has cameras and the only entry is through an Radio-Frequency Identification (RFID) door. Furthermore, access and control of the actual cobot is done through facial recognition and fingerprint. Now on the digital side of security and privacy, the cobot has an EDR agent that can detect security anomalies. If an anomaly is detected, an alert is generated for the engineers to take a look and act accordingly. It was agreed between the security team, risk team and managers that the EDR would not have the response capability turned on. The response of the EDR could interfere with the operation of the cobot, which could lead to danger. Furthermore, the communication protocol used is OPC UA, which has security features such as confidentiality, integrity, authentication and authorisation.

Finally, at the Business property, the cobot's role is aligned with strategic goals. ERP and Manufacturing Execution System (MES) systems use their data to optimise scheduling, track KPI, and ensure that the cobot's collaboration with human workers enhances productivity, quality, and competitiveness. At this level, the cobot is no longer just a machine—it is a business asset contributing to the organisation.

Moving to the Asset Life Cycle axis, it describes the journey of an industrial asset from the moment it enters the organisation until its end of life, ensuring that every stage is managed in a structured and value-driven way. The journey of a cobot begins in the Acquisition phase, where the company selects and purchases the robot and defines its intended tasks. Once deployed, it enters the In Use phase, where the cobot actively collaborates with human operators on the factory floor, to pick up and move stones into the CNC machine. Eventually, the cobot reaches the Decommissioning phase, when it is removed from production, disconnected from the PLC, and its operational

history archived for compliance and traceability. Finally, in the Recycling phase, the cobot or its components—such as motors, sensors, or control units—are repurposed, recycled, or disposed of responsibly, with lessons from its performance feeding back into future acquisition decisions to improve sustainability and efficiency. This axis is key to Industry 5.0's sustainability goals.

Finally, the Context axis situates an asset within the broader conditions that shape its operation and value. When viewed through the Cybersecurity Context, the cobot must operate with secure communication protocols and encrypted data flows to protect sensitive production information and prevent unauthorised access. In the Economic Context, the cobot's value is measured by cost, how it improves productivity, reduces labour costs, and enhances competitiveness through flexible automation. The Natural Environment Context highlights the cobot's contribution to sustainability. This context is directly linked with the asset's Sustainability property. In this case, the fact that the cobot has a good energy efficiency rating, B, and that it doesn't emit pollution. Within the Social Context, the relationship between the cobot and the human operator is important. The cobot is there not only to improve productivity, but also to improve the operator's overall work satisfaction. This is done through improving ergonomics and reducing fatigue and overall injury rates, especially when working with the transport of heavy stones. This context is key for Industry 5.0's human-centric viewpoint. Finally, in the Organisational Context, the cobot is integrated into company workflows and governance structures, aligning with strategic goals, compliance requirements, and workforce training programs. Together, these contexts ensure the cobot is not just a machine on the factory floor but a responsible, secure, and socially integrated element of Industry 5.0.

Table 5.1 was created to summarise all the differences talked about in this section between RAMI 4.0 and HLFI 5.0. It can be seen that RAMI 4.0 lacks the majority of Industry 5.0's demands, such as resilience, sustainability, cybersecurity and human-centric ethics.

Table 5.1: *Differences between RAMI 4.0 vs HLFI 5.0*

Characteristics	RAMI 4.0	HLFI 5.0
Resilience	-	✓
Sustainability	-	✓
Cybersecurity	-	✓
Communication	✓	✓
Human-Centric	-	✓
Organisational	-	✓
Business	✓	✓
Economic	-	✓
Functionality	✓	✓
Information	✓	✓
Integration	✓	✓

6
Conclusion

This document was intended to give a better understanding of the implications of Industry 5.0 and the future of cybersecurity. Furthermore, it establishes HLFI 5.0, a novel high-level framework that serves as a common language and structured approach to implement Industry 5.0. These important steps allow organisations to prepare in advance for a possible transition to Industry 5.0. Preparation is the key to a strong cybersecurity posture.

Throughout the document, this objective was achieved, starting from the Background chapter, where a foundation of the key concepts explored in this document is established. In the same chapter, studying the related work helped find opportunities in developing a high-level framework to define Industry 5.0 and help in the implementation. In the next chapter, further background information is given about different cybersecurity domains. This information becomes key in the next chapter, where an analysis of these domains is done in the context of Industry 5.0. The objective was to gather information about the implications of Industry 5.0 in cybersecurity. These implications were then tested, in the next chapter, with a case study. The case study simulated the stone cutting industry. In the same chapter, industrial frameworks are analysed in the context of Industry 5.0. These frameworks fall short in some aspects, and HLFI 5.0 is created. The current industrial frameworks are tested against the case study, which demonstrated their incapacity. HLFI 5.0 is also tested, which demonstrated its compatibility with Industry 5.0. The result is a solid, structured approach to Industry 5.0 and all its different aspects.

Through assessment of the different cybersecurity dimensions in contrast with Industry 5.0, important conclusions were reached, of which we highlight the following:

- Existing industrial protocols will probably be enough for Industry 5.0 enabling technologies.
- Industry 5.0 concepts and technologies will have a meaningful impact on all the investigated cybersecurity concepts. The impacts range from increased costs in cybersecurity to human-centric ethics.

This work completed all the initially proposed objectives, which were to understand the implications that Industry 5.0 has in cybersecurity and to assess the current industrial frameworks against Industry 5.0. The current frameworks failed, and a new framework was developed with the objective of giving a structured approach to implementing Industry 5.0. Future work could expand this work by:

- Conducting a practical test with HLFI 5.0.
- Studying a broader range of cybersecurity concepts in Industry 5.0, such as penetration testing and workforce training.

Throughout the course of this work, some challenges were found, such as a lack of consensus on what Industry 5.0 is and the lack of information on cybersecurity in Industry 5.0.

This page intentionally left blank.

Bibliography

A10 Networks (2025). *What is the Zero Trust Model? | Glossary*. en. URL: https://www.a10networks.com/glossary/what-is-the-zero-trust-model/ (visited on 2025-08-17).

Abdelsattar, Ahmad (Mar. 2023). *An OPC UA client/gateway-based architecture for SCADA systems with automatic mental fatigue detection application*. eng. URL: https://summit.sfu.ca/item/36074 (visited on 2025-08-02).

Adriano, José D., Elcio Carlos do Rosario, and Joel J.P.C. Rodrigues (Nov. 2018). "Wireless Sensor Networks in Industry 4.0: WirelessHART and ISA100.11a". In: pp. 924–929. URL: https://ieeexplore.ieee.org/document/8627177 (visited on 2025-08-02).

Alto, Palo (2025). *What Is the Principle of Least Privilege?* en-US. URL: https://www.paloaltonetworks.com/cyberpedia/what-is-the-principle-of-least-privilege (visited on 2025-06-30).

Alvey, Elan (Dec. 2024). *OT Cybersecurity Best Practices for SMBs: Identity and Access Management in OT | Dragos*. en-US. URL: https://www.dragos.com/blog/ot-cybersecurity-best-practices-for-smbs-identity-and-access-management-in-ot/ (visited on 2025-03-02).

Asghar, Muhammad Rizwan, Qinwen Hu, and Sherali Zeadally (Dec. 2019). "Cybersecurity in industrial control systems: Issues, technologies, and challenges". In: *Computer Networks* 165, p. 106946. ISSN: 1389-1286. URL: https://www.sciencedirect.com/science/article/pii/S1389128619306292 (visited on 2024-04-04).

Atar, Bentsi Ben (2025). *Asset Inventory: A Key to ESG Excellence!* en-US. URL: https://sepiocyber.com/blog/asset-inventory/ (visited on 2025-09-20).

Attaxion (2025). *Active and Passive Vulnerability Scanning: What Is the Difference?* en. URL: https://attaxion.com/blog/active-and-passive-vulnerability-scanning-what-is-the-difference/ (visited on 2025-03-16).

Automation, B&R Industrial (2024). *OPC UA over TSN – Unified standard for the IIoT | B&R Industrial Automation*. en. URL: https://www.br-automation.com/en/about-us/customer-magazine/2020/20204/opc-ua-over-tsn-unified-standard-for-the-iiot/ (visited on 2024-07-29).

Automation, Beckhoff (2024). *EtherCAT – the Ethernet Fieldbus*. en. URL: https://www.beckhoff.com/en-en/products/i-o/ethercat/ (visited on 2024-07-29).

Automation, Rockwell (2025). *The Value of OT Endpoint Security | Rockwell Automation | Rockwell Automation | US*. en-US. URL: https://www.rockwellautomation.com/en-us/company/news/blogs/ot-endpoint-security.html (visited on 2025-06-28).

Aveva (2025). *Cybersecurity Deployment Guide - Security Concepts*. en. URL: https://docs.aveva.com/bundle/cybersecurity-deployment-security-concepts/page/1510579.html (visited on 2025-06-14).

Avigdor Book (June 2023). *Zero Trust vs Least Privilege: The Battle of Cybersecurity Giants*. en-US. URL: https://www.tufin.com/blog/zero-trust-vs-least-privilege-battle-cybersecurity-giants (visited on 2025-06-30).

Bances, Enrique et al. (Jan. 2020). "Exoskeletons Towards Industrie 4.0: Benefits and Challenges of the IoT Communication Architecture". In: *Procedia Manufacturing*. International Conference on Industry 4.0 and Smart Manufacturing (ISM 2019) 42, pp. 49–56. ISSN: 2351-9789. URL: https://www.sciencedirect.com/science/article/pii/S2351978920306521 (visited on 2025-08-02).

Bécue, Adrien, Isabel Praça, and João Gama (June 2021). "Artificial intelligence, cyber-threats and Industry 4.0: challenges and opportunities". en. In: *Artificial Intelligence Review* 54.5, pp. 3849–3886. ISSN: 1573-7462. URL: https://doi.org/10.1007/s10462-020-09942-2 (visited on 2024-04-07).

Belal, Syed M. (2025). *The Top 7 Operational Technology Patch Management Best Practices*. en. URL: https://gca.isa.org/blog/the-top-7-operational-technology-patch-management-best-practices (visited on 2025-09-28).

Berrick, Daniel (2025). *Brain-Computer Interfaces and Data Protection: Understanding the Technology and Data Flows*. URL: https://fpf.org/blog/brain-computer-interfaces-data-protection-understanding-the-technology-and-data-flows/ (visited on 2025-09-20).

Bhamare, Deval et al. (Feb. 2020). "Cybersecurity for industrial control systems: A survey". In: *Computers & Security* 89, p. 101677. ISSN: 0167-4048. URL: https://www.sciencedirect.com/science/article/pii/S0167404819302172 (visited on 2024-03-27).

Bidwai, Amit (2025). *6 important Pillars of Information Security*. en-US. URL: https://www.linkedin.com/pulse/6-important-pillars-information-security-amit-bidwai/ (visited on 2025-09-22).

BlastWave (2025a). *Authentication | BlastWave Glossary | Leading OT Cybersecurity Solution for ICS and SCADA Protection*. en. URL: https://glossary.blastwave.com/entry/authentication (visited on 2025-06-14).

BlastWave (2025b). *Authorization | BlastWave Glossary | Leading OT Cybersecurity Solution for ICS and SCADA Protection*. en. URL: https://glossary.blastwave.com/entry/authorization (visited on 2025-06-14).

BlastWave (2025c). *Data Integrity | BlastWave Glossary | Leading OT Cybersecurity Solution for ICS and SCADA Protection*. en. URL: https://glossary.blastwave.com/entry/data-integrity (visited on 2025-06-14).

BlastWave (2025d). *Detect and Respond | BlastWave Glossary | Leading OT Cybersecurity Solution for ICS and SCADA Protection*. en. URL: https://glossary.blastwave.com/entry/detect-and-respond (visited on 2025-07-15).

BlastWave (2025e). *Endpoint Detection and Response (EDR) | BlastWave Glossary | Leading OT Cybersecurity Solution for ICS and SCADA Protection*. en. URL: https://glossary.blastwave.com/entry/endpoint-detection-and-response-edr (visited on 2025-06-28).

BlastWave (2025f). *Functional Safety | BlastWave Glossary | Leading OT Cybersecurity Solution for ICS and SCADA Protection*. en. URL: https://glossary.blastwave.com/entry/functional-safety (visited on 2025-06-14).

BlastWave (2025g). *High Availability (HA) | BlastWave Glossary | Leading OT Cybersecurity Solution for ICS and SCADA Protection*. en. URL: https://glossary.blastwave.com/entry/high-availability-ha (visited on 2025-06-14).

BlastWave (2025h). *Incident Response | BlastWave Glossary | Leading OT Cybersecurity Solution for ICS and SCADA Protection*. en. URL: https://glossary.blastwave.com/entry/incident-response (visited on 2025-07-14).

BlastWaveConfidentiality (2025). *Encryption | BlastWave Glossary | Leading OT Cybersecurity Solution for ICS and SCADA Protection*. en. URL: https://glossary.blastwave.com/entry/encryption (visited on 2025-06-14).

Breen, Jon (July 2019). *How to Upgrade an Obsolete PLC*. en-US. URL: https://www.breen-machine.com/how-to-upgrade-an-obsolete-plc/ (visited on 2025-06-28).

Business, Verizon (2024). *2024 Data Breach Investigations Report*. en. URL: https://www.verizon.com/business/resources/reports/dbir/ (visited on 2024-05-12).

Bütün, İsmail (Mar. 2022). "Security Implications of Underlying Network Technologies on Industrial Internet of Things". en. In: *Politeknik Dergisi* 25.1, pp. 223–229. ISSN: 2147-9429. URL: https://dergipark.org.tr/en/pub/politeknik/issue/68943/724656 (visited on 2024-07-29).

Caltagirone, Sergio (Jan. 2018). *Industrial Control Threat Intelligence Whitepaper | Dragos*. en-US. URL: https://www.dragos.com/resources/whitepaper/industrial-control-threat-intelligence-whitepaper/ (visited on 2025-04-27).

Cavalcanti, Dave et al. (Dec. 2022). "WiFi TSN: Enabling Deterministic Wireless Connectivity over 802.11". In: *IEEE Communications Standards Magazine* 6.4, pp. 22–29. ISSN: 2471-2833. DOI: 10.1109/MCOMSTD.0002.2200039. URL: https://ieeexplore.ieee.org/document/10034532 (visited on 2025-09-28).

Charbonneau, Vincent (Oct. 2018). *Latest Production Tech: FANUC Cobot, Honeywell Pressure Transmitter & More*. en-US. URL: https://www.engineering.com/latest-production-tech-fanuc-cobot-honeywell-pressure-transmitter-more/ (visited on 2025-08-02).

CheckPoint (2025). *O que é Shadow IT? - Software Check Point*. pt-BR. URL: https://www.checkpoint.com/pt/cyber-hub/cyber-security/what-is-cybersecurity/what-is-shadow-it/ (visited on 2025-03-16).

Chennupati, Silpa (Apr. 2020). *Advanced Threat Detection With Modern SIEM Solutions*. en-us. URL: https://www.innominds.com/blog/advanced-threat-detection-with-modern-siem-solutions (visited on 2025-09-28).

CIP Security™ | Common Industrial Protocol | ODVA Technologies (2024). en-US. URL: https://www.odva.org/technology-standards/distinct-cip-services/cip-security/ (visited on 2024-07-29).

Cisco (2025). *802.11 Network Security Fundamentals Cisco Secure Services Client*. en. URL: http://www.cisco.com/en/US/docs/wireless/wlan_adapter/secure_client/5.1.0/administration/guide/C1_Network_Security.html (visited on 2025-07-27).

Community, Automation (Dec. 2023). *EtherCAT Questions - Ethernet for Control Automation Technology*. en-US. URL: https://automationcommunity.com/ethercat-questions/ (visited on 2024-07-29).

CompareSoft (2025). *What Is Asset Lifecycle Management & Why Tracking ALM Is Important*. en-US. URL: https://comparesoft.com/asset-management-software/asset-life-cycle/ (visited on 2025-08-02).

Consortium, Industry IoT (2022). *The Industrial Internet Reference Architecture*. en-US. URL: https://www.iiconsortium.org/iira/ (visited on 2024-05-09).

Conti, Mauro, Denis Donadel, and Federico Turrin (2021). "A Survey on Industrial Control System Testbeds and Datasets for Security Research". In: *IEEE Communications Surveys & Tutorials* 23.4, pp. 2248–2294. ISSN: 1553-877X. URL: https://ieeexplore.ieee.org/abstract/document/9471765 (visited on 2024-04-03).

CoreTigo (2025). *Deterministic Industrial Communication Protocol*. en-US. URL: https://www.coretigo.com/glossary/deterministic-industrial-communication-protocol/ (visited on 2025-03-02).

Cyberdefense, Orange (Oct. 2021). *Case study: Technical benchmarking of EDR solutions in an OT environment*. en-US. URL: https://www.orangecyberdefense.com/global/

blog/managed-detection-response/case-study-technical-benchmarking-of-edr-solutions-in-an-ot-environment (visited on 2025-06-28).

CyberOne (2025). *Endpoint Protection vs EDR: What's the Difference?* en. URL: https://cyberone.security/blog/endpoint-protection-epp-vs-edr-whats-the-difference (visited on 2025-06-28).

Cybersecurity & Infrastructure Security Agency (Feb. 2025). *Layering Network Security Through Segmentation Infographic | CISA*. en. URL: https://www.cisa.gov/resources-tools/resources/layering-network-security-through-segmentation-infographic (visited on 2025-03-31).

Cybiant (2018). *Difference in CIA Triad (Security) in IT and Operational Technology*. en-US. URL: https://www.cybiant.com/knowledge/difference-in-cia-triad-security-in-information-technology-and-operational-technology/ (visited on 2025-03-02).

Datadog (2025). *Log Collection and Integrations*. en-US. URL: https://docs.datadoghq.com/logs/log_collection/ (visited on 2025-09-29).

Directorate-General for Research and Innovation (European Commission) and Julian Müller (2020). *Enabling Technologies for Industry 5.0: results of a workshop with Europe's technology leaders*. eng. Publications Office of the European Union. ISBN: 9789276220480. URL: https://data.europa.eu/doi/10.2777/082634 (visited on 2024-04-17).

Directorate-General for Research and Innovation (European Commission) et al. (2021). *Industry 5.0: towards a sustainable, human centric and resilient European industry*. eng. Publications Office of the European Union. ISBN: 9789276253082. URL: https://data.europa.eu/doi/10.2777/308407 (visited on 2024-07-04).

Doebbert, Thomas R., Christoph Cammin, and Gerd Scholl (2022). "Safety Architecture Proposal for Low-Latency Sensor/Actuator Networks using IO-Link Wireless". In: *IEEE Access* 10, pp. 3030–3044. ISSN: 2169-3536. URL: https://ieeexplore.ieee.org/document/9617589 (visited on 2025-08-02).

doronbasson (Jan. 2025). *Access Control and Authorization in OT Environments*. en-US. URL: https://www.coraltechteam.com/access-control-and-authorization-in-ot-environments/ (visited on 2025-06-14).

Dragos (June 2024). *Implementing Zero Trust in Operational Technology (OT) Environments | Dragos*. en-US. URL: https://www.dragos.com/blog/implementing-zero-trust-in-operational-technology-ot-environments/ (visited on 2025-06-30).

Dragos Inc. (Dec. 2024a). *Risk-Based Vulnerability Management for OT Systems | Dragos*. en-US. URL: https://www.dragos.com/blog/how-to-prioritize-vulnerabilities-with-risk-based-vulnerability-management-in-ot/ (visited on 2025-04-26).

Dragos Inc. (June 2024b). *Understanding OT Cyber Threat Intelligence | Dragos*. en-US. URL: https://www.dragos.com/blog/what-is-ot-cyber-threat-intelligence/ (visited on 2025-04-27).

EdB-MSFT (2025). *Plan costs and understand pricing and billing - Microsoft Sentinel*. en-us. URL: https://learn.microsoft.com/en-us/azure/sentinel/billing (visited on 2025-09-21).

Ellis, Larry (Mar. 2023). *On-Prem vs. Cloud Mail Server: Key Differences and Benefits for Network Security*. en-US. URL: https://abusix.com/blog/on-prem-vs-cloud-mail-server/ (visited on 2025-09-28).

Etela, Noora (2021). *Coping with personal data breaches in healthcare*. URL: https://jyx.jyu.fi/handle/123456789/78245.

Eureka (2025). *How to Use SCADA + OPC UA in Renewable Energy Control Applications*. en-US. URL: https://eureka.patsnap.com/article/how-to-use-scada--opc-ua-in-renewable-energy-control-applications (visited on 2025-08-02).

European Comission (Jan. 2022). *Industry 5.0 - European Commission*. en. URL: https://research-and-innovation.ec.europa.eu/research-area/industrial-research-and-innovation/industry-50_en (visited on 2024-04-17).

Faisal, Muhammad Yousuf (2025a). *Endpoint Detection and Response (EDR) Solutions for IT and OT/ICS*. en. URL: https://gca.isa.org/blog/endpoint-detection-and-response-edr-solutions-for-it-and-ot/ics (visited on 2025-06-28).

Faisal, Muhammad Yousuf (2025b). *OT Security Dozen Part 3: Network Security Architecture & Segmentation*. en. URL: https://gca.isa.org/blog/ot-security-dozen-part-3-network-security-architecture-segmentation (visited on 2025-08-17).

FANUC (2025). *CR-35iB*. en. URL: https://www.fanuc.eu/eu-en/product/robot/cr-35ib (visited on 2025-09-21).

Farsi, Maryam and John Ahmet Erkoyuncu (Oct. 2021). *Industry 5.0 Transition for an Advanced Service Provision*. en. Tech. rep. 3944547. Rochester, NY. URL: https://papers.ssrn.com/abstract=3944547 (visited on 2024-04-29).

Firch, Jason (Mar. 2024). *How To Centralize Your Patch Management*. en-US. URL: https://purplesec.us/learn/centralize-patch-management/ (visited on 2025-09-28).

Fluke (2025). *4 Things You Need to Know About Industrial Ethernet*. en. URL: https://www.fluke.com/en/learn/blog/electrical/industrial-ethernet (visited on 2025-03-02).

forense.io (2025). *O que é: Jump Server - Entenda sua Importância*. pt-BR. URL: https://forense.io/glossario/o-que-e-jump-server-importancia-seguranca/ (visited on 2025-09-28).

Fortinet (2025a). *Information Technology (IT) vs. Operational Technology (OT) Cybersecurity*. en. URL: https://www.fortinet.com/resources/cyberglossary/it-vs-ot-cybersecurity (visited on 2025-08-30).

Fortinet (2025b). *OT Network Segmentation and Microsegmentation Guide*. en. URL: https://www.fortinet.com/resources/cyberglossary/ot-network-segmentation-and-microsegmentation (visited on 2025-03-31).

Fortinet (2025c). *What is Air Gap? Essential Guide to Air Gap Security*. en. URL: https://www.fortinet.com/resources/cyberglossary/what-is-air-gap (visited on 2025-03-31).

Fortinet (2025d). *What Is SOAR? Security Orchestration, Automation, and Response*. en. URL: https://www.fortinet.com/resources/cyberglossary/what-is-soar (visited on 2025-07-15).

Foundation, OPC (2024a). *Exploring OPC UA Security Concepts*. en. URL: https://opcconnect.opcfoundation.org/2020/06/exploring-opc-ua-security-concepts/ (visited on 2024-07-29).

Foundation, OPC (2024b). *UA Part 1: Overview and Concepts - 6.4 Redundancy*. en. URL: https://reference.opcfoundation.org/Core/Part1/v104/docs/6.4 (visited on 2024-07-29).

Foundation, OPC (2024c). *UA Part 2: Security - 4.9 User Authentication*. en. URL: https://reference.opcfoundation.org/Core/Part2/v104/docs/4.9 (visited on 2024-07-29).

Gartner (2025). *Best Vulnerability Assessment Reviews 2025 Gartner Peer Insights*. en. URL: https://www.gartner.com/reviews/market/vulnerability-assessment (visited on 2025-04-27).

Goetzman, Amy (Sept. 2023). *What is the fieldbus protocol?* en-US. URL: https://connectorsupplier.com/what-is-the-fieldbus-protocol/ (visited on 2025-03-02).

Grance, Tim, Karen Kent, and Brian Kim (Jan. 2004). *Computer Security Incident Handling Guide*. en. Tech. rep. URL: https://csrc.nist.gov/pubs/sp/800/61/final (visited on 2025-07-14).

Great (June 2024). *The Environmental Impact of CNC Machining*. en-US. URL: https://mfg-solution.com/the-environmental-impact-of-cnc-machining/ (visited on 2025-09-21).

Green, Benjamin et al. (Aug. 2017). "Pains, Gains and PLCs: Ten Lessons from Building an Industrial Control Systems Testbed for Security Research". In: *10th USENIX Workshop on Cyber Security Experimentation and Test (CSET 17)*. Vancouver, BC: USENIX Association. URL: https://www.usenix.org/conference/cset17/workshop-program/presentation/green.

Hartrup, Alastair (2025). *IT vs OT Networks: Key Differences in Modern Industrial Systems*. en. URL: https://www.networkcritical.com/blogs/it-vs-ot-networks (visited on 2025-06-14).

Hassan, Muhammad Ali et al. (Jan. 2024). "Systematic Analysis of Risks in Industry 5.0 Architecture". en. In: *Applied Sciences* 14.4, p. 1466. URL: https://www.mdpi.com/2076-3417/14/4/1466 (visited on 2024-04-29).

HMS (2025). *Industrial Ethernet is now bigger than fieldbuses*. en. URL: https://www.hms-networks.com/news/news-details/16-07-2018-industrial-ethernet-is-now-bigger-than-fieldbuses (visited on 2025-03-02).

Hollerer, Siegfried et al. (Jan. 2021). "Cobot attack: a security assessment exemplified by a specific collaborative robot". In: *Procedia Manufacturing*. 10th CIRP Sponsored Conference on Digital Enterprise Technologies (DET 2020) Digital Technologies as Enablers of Industrial Competitiveness and Sustainability 54, pp. 191–196. URL: https://www.sciencedirect.com/science/article/pii/S2351978921001657 (visited on 2024-04-30).

HostSailor (Apr. 2024). *Advanced Firewall Rules: Secure Your Dedicated Server - Hostsailor: Domains, Web Hosting & more| Explore A New World*. en-US. URL: https://web.hostsailor.com/blog/advanced-firewall-rules-secure-your-dedicated-server/ (visited on 2025-09-28).

Huawei (2025). *Understanding Solar Power Systems: A Deep Dive into Photovoltaic Energy | HUAWEI Smart PV Global*. en. URL: //solar.huawei.com/en/blog/2024/solar-power-system (visited on 2025-09-28).

Ibrahim, Rosdiazli et al. (Jan. 2017). "Solar Energy Harvester for Industrial Wireless Sensor Nodes". In: *Procedia Computer Science*. 2016 IEEE International Symposium on Robotics and Intelligent Sensors, IRIS 2016, 17-20 December 2016, Tokyo, Japan 105, pp. 111–118. ISSN: 1877-0509. URL: https://www.sciencedirect.com/science/article/pii/S1877050917302028 (visited on 2025-08-02).

Ijemaru, Gerald et al. (Apr. 2018). "Security Challenges of Wireless Communications Networks: A Survey". In: *International Journal of Applied Engineering Research* 13. URL: https://www.researchgate.net/publication/324979423_Security_Challenges_of_Wireless_Communications_Networks_A_Survey.

Illinois, University of (2025). *EWS Windows Lab Software*. en-US. URL: https://answers.uillinois.edu/illinois.engineering/84701 (visited on 2025-09-21).

Inductive Automation (2025a). *HMI: Human-Machine Interface*. en-US. URL: https://inductiveautomation.com/resources/article/what-is-hmi (visited on 2025-09-28).

Inductive Automation (2025b). *PLC: Programmable Logic Controller*. en-US. URL: https://inductiveautomation.com/resources/article/what-is-a-PLC (visited on 2025-08-30).

Industrial Defender (2025a). *How to Centralize OT Security Data in a SIEM*. en. URL: https://www.industrialdefender.com/blog/how-to-centralize-ot-security-data-in-siem (visited on 2025-09-29).

Industrial Defender (2025b). *How to Create an EDR/MDR Alternative for OT Systems*. en. URL: https://www.industrialdefender.com/blog/how-to-create-edr-mdr-alternative-for-ot-systems (visited on 2025-09-29).

Industrial Shields (2025). *The Power of Cobots with ESP32PLC*. en-US. URL: https://www.industrialshields.com/case-study-robotisation-with-esp32-plc (visited on 2025-09-28).

Industries, American Micro (May 2024). *Demystifying the Use of CAD in CNC Machining | AMI*. en-US. URL: https://www.americanmicroinc.com/resources/use-cad-cnc-machining/ (visited on 2025-09-21).

influxdata (June 2023). *Data Historians Explained*. URL: https://www.influxdata.com/glossary/data-historian/ (visited on 2025-09-28).

Jansson, Magnus (2025). *Annual Analysis Reveals Steady Growth in Industrial Network Market*. en. URL: https://www.hms-networks.com/news/news-details/17-06-2024-annual-analysis-reveals-steady-growth-in-industrial-network-market (visited on 2025-03-02).

Jia, Yifan et al. (Oct. 2022). "Physical Adversarial Attack on a Robotic Arm". In: *IEEE Robotics and Automation Letters* 7.4, pp. 9334–9341. ISSN: 2377-3766. URL: https://ieeexplore.ieee.org/abstract/document/9826387 (visited on 2024-05-01).

Jiang, Xue et al. (July 2023). "Active poisoning: efficient backdoor attacks on transfer learning-based brain-computer interfaces". en. In: *Science China Information Sciences* 66.8, p. 182402. ISSN: 1869-1919. DOI: 10.1007/s11432-022-3548-2. URL: https://doi.org/10.1007/s11432-022-3548-2 (visited on 2024-05-02).

Jim Cobb Eric Rotvold, Jeff Potter (2024). *WirelessHART Security Overview*. en-US. URL: https://www.emerson.com/documents/automation/white-paper-wirelesshart-security-overview-by-hcf-en-42578.pdf (visited on 2024-07-29).

Katie Bykowski (July 2025). *How to Build an Incident Response Playbook in 9 Steps*. en-US. URL: https://swimlane.com/blog/incident-response-playbook/ (visited on 2025-08-16).

Kidd, Chrissy (2025). *Vulnerabilities, Threats & Risk Explained*. en. URL: https://www.splunk.com/en_us/blog/learn/vulnerability-vs-threat-vs-risk.html (visited on 2025-08-09).

Klingenberg, Cristina Orsolin, Marco Antônio Viana Borges, and José Antônio do Vale Antunes (Aug. 2022). "Industry 4.0: What makes it a revolution? A historical framework to understand the phenomenon". In: *Technology in Society* 70, p. 102009. ISSN: 0160-791X. URL: https://www.sciencedirect.com/science/article/pii/S0160791X22001506 (visited on 2024-03-26).

Knowles, William et al. (June 2015). "A survey of cyber security management in industrial control systems". In: *International Journal of Critical Infrastructure Protection* 9, pp. 52–80. ISSN: 1874-5482. URL: https://www.sciencedirect.com/science/article/pii/S1874548215000207 (visited on 2024-04-03).

Koelemij, Sinclair (Oct. 2023). *Rethinking the Relevance of the Security Triad*. en-US. URL: https://industrialcyber.co/expert/rethinking-the-relevance-of-the-security-triad/ (visited on 2025-03-02).

Kon, Maximillian (2025). *How to Define Zones and Conduits*. en. URL: https://gca.isa.org/blog/how-to-define-zones-and-conduits (visited on 2025-03-31).

Lee, Changdae and Young Il Lee (Oct. 2023). "Smart Energy Town: Constructing OPC UA-Based Network Architecture". In: ISSN: 2642-3901, pp. 1105–1107. URL: https://ieeexplore.ieee.org/document/10316871 (visited on 2025-08-02).

Leng, Jiewu et al. (Oct. 2022). "Industry 5.0: Prospect and retrospect". In: *Journal of Manufacturing Systems* 65, pp. 279–295. ISSN: 0278-6125. URL: https://www.sciencedirect.com/science/article/pii/S0278612522001662 (visited on 2024-03-26).

LetsDefend (2025). *NIST Incident Response: Detection and Analysis*. en. URL: https://letsdefend.io/blog/nist-incident-response-detection-and-analysis (visited on 2025-07-15).

Li, Jun et al. (2020). "Study on the Reference Architecture and Assessment Framework of Industrial Internet Platform". In: *IEEE Access* 8, pp. 164950–164971. ISSN: 2169-3536. URL: https://ieeexplore.ieee.org/abstract/document/9186625 (visited on 2024-04-07).

Libeer, Laura (Aug. 2024). *Security Incident Response with Asset Discovery*. en-US. URL: https://www.lansweeper.com/blog/cybersecurity/how-asset-discovery-enhances-security-incident-response/ (visited on 2025-03-16).

Liu, Chengyin, Jun Teng, and Ning Wu (May 2015). "A Wireless Strain Sensor Network for Structural Health Monitoring". In: *Shock and Vibration* 2015, pp. 1–13.

Liu, Jiajia and Wen Sun (Dec. 2016). "Smart Attacks against Intelligent Wearables in People-Centric Internet of Things". In: *IEEE Communications Magazine* 54.12, pp. 44–49. ISSN: 1558-1896. DOI: 10.1109/MCOM.2016.1600553CM. URL: https://ieeexplore.ieee.org/abstract/document/7786109 (visited on 2024-05-02).

Livingston, John (Mar. 2022). *OT Patch Management: A Step-by-Step Guide*. en-US. URL: http://verveindustrial.com/resources/blog/6-steps-to-patch-management/ (visited on 2025-04-27).

Logpoint (Nov. 2023). *The ultimate SIEM pricing guide*. en. URL: https://www.logpoint.com/en/blog/the-ultimate-siem-pricing-guide/ (visited on 2025-07-15).

Lund, Peter (2025). *How to Create an EDR/MDR Alternative for OT Systems*. en. URL: https://www.industrialdefender.com/blog/how-to-create-edr-mdr-alternative-for-ot-systems (visited on 2025-06-28).

Maddikunta, Praveen Kumar Reddy et al. (Mar. 2022). "Industry 5.0: A survey on enabling technologies and potential applications". In: *Journal of Industrial Information Integration* 26, p. 100257. ISSN: 2452-414X. URL: https://www.sciencedirect.com/science/article/pii/S2452414X21000558 (visited on 2024-03-26).

Martina Vass (Feb. 2024). *Environmental crimes: MEPs adopt extended list of offences and sanctions | News | European Parliament*. en. URL: https://www.europarl.europa.eu/news/en/press-room/20240223IPR18075/environmental-crimes-meps-adopt-extended-list-of-offences-and-sanctions (visited on 2025-08-02).

Martinez, Juan (2025). *User Authentication in Manufacturing PLC Cybersecurity | rf IDEAS*. en. URL: https://www.rfideas.com/about-us/blog/understanding-manufacturing-plc-cybersecurity-why-user-authentication-critical (visited on 2025-06-30).

Martinovic, Ivan et al. (2012). "On the Feasibility of {Side-Channel} Attacks with {Brain-Computer} Interfaces". en. In: pp. 143–158. URL: https://www.usenix.org/conference/usenixsecurity12/technical-sessions/presentation/martinovic (visited on 2024-05-02).

Martins, Tiago and Sergio Vidal Garcia Oliveira (Jan. 2022). "Enhanced Modbus/TCP Security Protocol: Authentication and Authorization Functions Supported". en. In: *Sensors* 22.20, p. 8024. ISSN: 1424-8220. URL: https://www.mdpi.com/1424-8220/22/20/8024 (visited on 2025-09-29).

MATICS (2025). *Shop Floor Management*. en-US. URL: https://matics.live/glossary/shop-floor-management/ (visited on 2025-09-28).

McMaster University (2025). *Vulnerability Management*. en-US. URL: https://informationsecurity.mcmaster.ca/procedures/vulnerability-management/ (visited on 2025-09-21).

MDCplus (Mar. 2025). *Direct Connection with MTConnect & Modbus TCP/RTU to Industrial Equipment*. en. URL: https://mdcplus.fi/blog/mtcconnect-modbus-tcp-rtu-connectivity/ (visited on 2025-09-28).

Mehta, Urvi (2025). *Asset Inventory Management: Key to Effective Vulnerability Management*. en-US. URL: https://www.armorcode.com/blog/asset-inventory-management-key-to-effective-vulnerability-management (visited on 2025-03-16).

Meng, Lubin et al. (2023). "EEG-Based Brain–Computer Interfaces are Vulnerable to Backdoor Attacks". In: *IEEE Transactions on Neural Systems and Rehabilitation Engineering* 31, pp. 2224–2234. ISSN: 1558-0210. DOI: 10.1109/TNSRE.2023.3273214. URL: https://ieeexplore.ieee.org/abstract/document/10119172 (visited on 2024-05-02).

Microminder (2025). *What Is OT/ICS Asset Inventory and Why Is It the Foundation of a Cybersecurity Program? | Microminder Cybersecurity | Holistic Cybersecurity Services*. en. URL: https://www.micromindercs.com/blog/what-is-ot-ics-asset-inventory (visited on 2025-03-16).

Microsoft (2025). *Defending operational technology (OT) environments with Microsoft Defender XDR*. en. URL: https://techcommunity.microsoft.com/t5/s/gxcuf89792/attachments/gxcuf89792/MicrosoftThreatProtectionBlog/632/3/Whitepaper%2520-%2520Defending%2520OT%2520environments%2520with%2520Defender%2520XDR%2520(Nov%25202024).pdf (visited on 2025-06-28).

Miller, Thomas et al. (Dec. 2021). "Looking back to look forward: Lessons learnt from cyber-attacks on Industrial Control Systems". In: *International Journal of Critical Infrastructure Protection* 35, p. 100464. ISSN: 1874-5482. URL: https://www.sciencedirect.com/science/article/pii/S1874548221000524 (visited on 2024-04-03).

Mirmex Motor (2025). *Micromotors for Cobots | Collaborative Robotics*. en-GB. URL: https://www.mirmexmotor.com/application/robotics/motors-for-cobots (visited on 2025-09-28).

MITRE (2025). *ICS Matrix*. en-US. URL: https://attack.mitre.org/matrices/ics/ (visited on 2025-09-20).

Modbus Organization (n.d.). *MODBUS Application Protocol*. URL: https://modbus.org/docs/Modbus_Application_Protocol_V1_1b3.pdf.

Morningstar (2025). *How Does a Solar Charge Controller Work?* en-US. URL: https://www.morningstarcorp.com/faq/how-does-solar-charge-controller-work/ (visited on 2025-09-28).

Mozilla (Apr. 2025). *What is a web server? - Learn web development | MDN*. en-US. URL: https://developer.mozilla.org/en-US/docs/Learn_web_development/Howto/Web_mechanics/What_is_a_web_server (visited on 2025-09-28).

Murad, Jousef (Mar. 2023). *Comparing and Contrasting MATLAB vs. Python*. en. URL: https://www.engineered-mind.com/coding/python-vs-matlab/ (visited on 2025-09-28).

Nakagawa, Elisa Yumi et al. (June 2021). "Industry 4.0 reference architectures: State of the art and future trends". In: *Computers & Industrial Engineering* 156, p. 107241. ISSN: 0360-8352. URL: https://www.sciencedirect.com/science/article/pii/S0360835221001455 (visited on 2024-04-06).

Nardone, Roberto, Ricardo J. Rodríguez, and Stefano Marrone (Dec. 2016). "Formal security assessment of Modbus protocol". In: *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*, pp. 142–147. URL: https://ieeexplore.ieee.org/document/7856685 (visited on 2024-07-29).

Nelson, Alexander et al. (Apr. 2025). *Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile*. en. Tech. rep. URL: https://csrc.nist.gov/pubs/sp/800/61/r3/final (visited on 2025-07-14).

NIST (2025). *security incident*. EN-US. URL: https://csrc.nist.gov/glossary/term/security_incident (visited on 2025-07-14).

OPC Foundation (2025a). *UA Part 1: Overview and Concepts - 5.7.5 Authorization services*. en. URL: https://reference.opcfoundation.org/Core/Part1/v105/docs/5.7.5 (visited on 2025-07-27).

OPC Foundation (2025b). *UA Part 4: Services - 6.2 Authorization Services*. en. URL: https://reference.opcfoundation.org/Core/Part4/v105/docs/6.2 (visited on 2025-07-27).

Organization, Modbus (2024). *MODBUS Security Protocol*. en. URL: https://modbus.org/specs.php (visited on 2024-07-29).

OT Security Glossary (2025). *What is Confidentiality in OT systems? - OT Security Glossary & Guide*. en-US. URL: https://www.otsecurityglossary.com/what-is-confidentiality-in-ot-systems/ (visited on 2025-05-28).

OTBase (Mar. 2020). *A comprehensive guide to OT/ICS asset management*. en-US. URL: https://www.langner.com/2020/03/a-comprehensive-guide-to-ot-ics-asset-management/ (visited on 2025-03-16).

Palo Alto (2025a). *What is an Incident Response Playbook?* en-US. URL: https://www2.paloaltonetworks.com/cyberpedia/what-is-an-incident-response-playbook (visited on 2025-07-15).

Palo Alto (2025b). *What Is SOAR?* en-US. URL: https://www.paloaltonetworks.com/cyberpedia/what-is-soar (visited on 2025-07-15).

Palo Alto (2025c). *What Is the Difference Between IT and OT? | IT vs. OT*. en-US. URL: https://www.paloaltonetworks.com/cyberpedia/it-vs-ot (visited on 2025-08-30).

Panchal, Abhijeet C., Vijay M. Khadse, and Parikshit N. Mahalle (Nov. 2018). "Security Issues in IIoT: A Comprehensive Survey of Attacks on IIoT and Its Countermeasures". In: *2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN)*, pp. 124–130. URL: https://ieeexplore.ieee.org/abstract/document/8668630 (visited on 2024-04-03).

Plattform Industrie 4.0 (Aug. 2018). *Reference Architectural Model Industrie 4.0 (RAMI4.0) - An Introduction*. en. URL: https://www.plattform-i40.de/IP/Redaktion/EN/Downloads/Publikation/rami40-an-introduction.html (visited on 2024-04-07).

Podzins, Oskars and Andrejs Romanovs (Apr. 2019). "Why SIEM is Irreplaceable in a Secure IT Environment?" In: *2019 Open Conference of Electrical, Electronic and Information Sciences (eStream)*, pp. 1–5. URL: https://ieeexplore.ieee.org/abstract/document/8732173 (visited on 2024-04-24).

Portnox (2025). *What is WPA3 vs. WPA2?* en-US. URL: https://www.portnox.com/cybersecurity-102/wpa3/ (visited on 2025-09-28).

Proctor, Gordon, Shobna Varma, and Steve Varnedoe (2025). *Asset Sustainability Index: A Proposed Measure for Long-Term Performance*. en-US. URL: https://www.planning.dot.gov/documents/ASI_report/asi-00.htm (visited on 2025-09-20).

Radonix (Mar. 2025). *What Does a CNC Controller Do? Functions & Types*. en-US. URL: https://radonix.com/what-does-cnc-controller-do/ (visited on 2025-09-28).

Rhim, Hana and Milos Simic (Dec. 2023). *What Is Endpoint Detection and Response? | Baeldung on Computer Science*. en-US. URL: https://www.baeldung.com/cs/edr (visited on 2025-08-12).

Ribeiro, Anna et al. (Sept. 2024). *Addressing OT cyber risk management threats and attacks with risk registers and tabletop exercises*. en-US. URL: https://industrialcyber.co/features/addressing-ot-cyber-risk-management-threats-and-attacks-with-risk-registers-and-tabletop-exercises/ (visited on 2025-04-26).

Robotics, IFR International Federation of (2025). *Collaborative Robots - How Robots Work alongside Humans*. en. URL: https://ifr.org/ifr-press-releases/news/how-robots-work-alongside-humans (visited on 2025-08-24).

Rommer, Simon (2025). *Which Logs to Collect in a Power Grid OT Environment?* en. URL: https://www.omicroncybersecurity.com/en/resources/which-logs-to-collect-in-a-power-grid-ot-environment (visited on 2025-07-15).

Ruan, Jiaqi et al. (Mar. 2024). "On Vulnerability of Renewable Energy Forecasting: Adversarial Learning Attacks". In: *IEEE Transactions on Industrial Informatics* 20.3, pp. 3650–3663. ISSN: 1941-0050. DOI: 10.1109/TII.2023.3313526. URL: https://ieeexplore.ieee.org/document/10255313 (visited on 2024-05-02).

Sangfor Technologies (2025). *Understanding the Purdue Model for ICS & OT Security*. en. URL: https://www.sangfor.com/glossary/cybersecurity/what-is-purdue-model-ics-security (visited on 2025-09-29).

SANS (2025). *Incident Response*. EN-US. URL: https://www.sans.org/security-resources/glossary-of-terms/incident-response/ (visited on 2025-07-14).

SANS (2024). *Industrial Protocols Cheat Sheet*. en. URL: https://www.sans.org/posters/industrial-protocols-cheat-sheet/ (visited on 2024-07-29).

Santos, Bruno, Rogério Luís C. Costa, and Leonel Santos (Aug. 2024). "Cybersecurity in Industry 5.0: Open Challenges and Future Directions". In: ISSN: 2643-4202, pp. 1–6. URL: https://ieeexplore.ieee.org/document/10788065 (visited on 2025-08-24).

Sarangan, Srikrishna, Vivek Kumar Singh, and Manimaran Govindarasu (Sept. 2018). "Cyber Attack-Defense Analysis for Automatic Generation Control with Renewable Energy Sources". In: *2018 North American Power Symposium (NAPS)*, pp. 1–6. DOI: 10.1109/NAPS.2018.8600589. URL: https://ieeexplore.ieee.org/abstract/document/8600589 (visited on 2024-05-02).

SecurityThings (2025). *Whitepaper Endpoint Detection & Response (EDR) Solutions Implementation Best Practices in IT & OT/ICS Environment*. en. URL: https://securingthings.com/resources/ (visited on 2025-06-28).

ServiceNow (2025). *What is a configuration management database (CMDB)?* en. URL: https://www.servicenow.com/products/it-operations-management/what-is-cmdb.html (visited on 2025-03-16).

Smith, Brandon (2025). *A brief introduction to Industrial Control Systems and Security*. en. URL: https://www.bitsight.com/blog/brief-introduction-industrial-control-systems-and-security (visited on 2025-06-28).

Solar Winds (2025). *Log Collector for Servers | SolarWinds*. en-us. URL: https://www.solarwinds.com/log-analyzer/use-cases/log-collector (visited on 2025-09-28).

Splunk (2025). *Top 10 SIEM Use Cases Today: Real Examples and Business Value*. en. URL: https://www.splunk.com/en_us/blog/learn/siem-use-cases.html (visited on 2025-09-29).

Staff, Editorial (2025). *Deterministic System - Glossary*. en-US. URL: https://www.devx.com/terms/deterministic-system/ (visited on 2025-06-14).

Stellar Cyber (2025a). *Common Log Formats*. en-US. URL: https://docs.stellarcyber.ai/5.4.x/Configure/LogParser/common-data-log-formats.htm (visited on 2025-07-15).

Stellar Cyber (2025b). *SIEM Correlation Rules: Enhancing Your Threat Detection*. en-US. URL: https://stellarcyber.ai/learn/siem-correlation-rules/ (visited on 2025-07-15).

Stouffer, Keith et al. (Sept. 2023). *Guide to Operational Technology (OT) Security*. en. Tech. rep. URL: https://csrc.nist.gov/pubs/sp/800/82/r3/final (visited on 2024-03-26).

StrongDM Team (2025). *Zero Trust vs. the Principle of Least Privilege: What's the Differences?* en. URL: https://www.strongdm.com/what-is/zero-trust-vs-principle-of-least-privilege (visited on 2025-06-30).

Sustain, Renew and (July 2024). *Guide to Solar Panels for Businesses | Renew & Sustain*. en-GB. URL: https://renewandsustain.co.uk/guide-to-solar-panels-for-business/ (visited on 2025-09-21).

Tang, Daogui, Yi-Ping Fang, and Enrico Zio (July 2023). "Vulnerability analysis of demand-response with renewable energy integration in smart grids to cyber attacks and online detection methods". In: *Reliability Engineering & System Safety* 235, p. 109212. ISSN: 0951-8320. DOI: 10.1016/j.ress.2023.109212. URL: https://www.sciencedirect.com/science/article/pii/S0951832023001278 (visited on 2024-05-02).

Tedeschi, Pietro, Savio Sciancalepore, and Roberto Di Pietro (2020). "Security in Energy Harvesting Networks: A Survey of Current Solutions and Research Challenges". In: *IEEE Communications Surveys & Tutorials* 22.4, pp. 2658–2693. ISSN: 1553-877X. DOI: 10.1109/COMST.2020.3017665. URL: https://ieeexplore.ieee.org/abstract/document/9170604 (visited on 2024-05-02).

THE RECORDED FUTURE (2025). *6 Phases of the Threat Intelligence Lifecycle*. en. URL: https://www.recordedfuture.com/blog/threat-intelligence-lifecycle-phases (visited on 2025-08-10).

Tile, MATERIAL Bespoke Stone + (2025). *CNC Stone Cutting 101*. en. URL: https://www.exploremateriall.com/blogs/the-trade/cnc-stone-cutting-101 (visited on 2025-09-21).

Tim Mullen (2025). *Understanding CIA in an OT environment*. en. URL: https://www.ace-net.com/blog/confidentiality-integrity-availability (visited on 2025-05-28).

Toker, Firdevs Sevde, Kevser Ovaz Akpinar, and İbrahim ÖZÇELİK (June 2021). "MITRE ICS Attack Simulation and Detection on EtherCAT Based Drinking Water System". In: *2021 9th International Symposium on Digital Forensics and Security (ISDFS)*, pp. 1–6. URL: https://ieeexplore.ieee.org/abstract/document/9486331 (visited on 2024-07-29).

Trend Micro (July 2020). *ICS / OT Security Guideline : IEC62443 System*. en-US. URL: https://www.trendmicro.com/en_us/research/20/g/guidelines-related-to-security-in-smart-factories-part-2-system-design-and-security-level-of-iec62443.html (visited on 2025-03-31).

Tullman-Botzer, Jennifer (2025a). *The Relationship Between Safety, Availability, and Security in Critical Industries*. en. URL: https://cyolo.io/blog/the-relationship-between-security-safety-and-availability-in-critical-industries (visited on 2025-06-14).

Tullman-Botzer, Jennifer (2025b). *Why Perimeter Security Is No Longer Enough*. en. URL: https://cyolo.io/blog/why-perimeter-security-is-no-longer-enough (visited on 2025-06-30).

UK, Profibus & Profinet International (2024). *PROFINET Security Guideline*. en-US. URL: https://www.profibus.com/download/profinet-security-guideline (visited on 2024-07-29).

Universal Robots (2025a). *Communication Protocols*. en-US. URL: https://www.universal-robots.com/developer/communication-protocol/ (visited on 2025-09-22).

Universal Robots (2025b). *OPC UA Client Server*. en-US. URL: https://www.universal-robots.com/marketplace/products/01tP40000071NgaIAE/ (visited on 2025-08-02).

Vaideeswaran, Narendran (2025). *What is Principle of Least Privilege (POLP)? | CrowdStrike*. en-US. URL: https://www.crowdstrike.com/en-us/cybersecurity-101/identity-protection/principle-of-least-privilege-polp/ (visited on 2025-06-30).

Vestal, Maria (May 2022). *What is a Control Room? Types, Design & Solutions for Modern Operations*. en-US. URL: https://www.saravalindustries.com/what-is-a-control-room/ (visited on 2025-09-28).

Vigo, Jesus (2025). *Zero Trust vs. Least Privilege: Modern Cybersecurity Strategies*. en. URL: https://www.jamf.com/blog/zero-trust-vs-least-privilege/ (visited on 2025-06-30).

Watson, Venesa, Xinxin Lou, and Yuan Gao (2017). "A Review of PROFIBUS Protocol Vulnerabilities - Considerations for Implementing Authentication and Authorization Controls:" in: *Proceedings of the 14th International Joint Conference on e-Business and Telecommunications*. Madrid, Spain: SCITEPRESS - Science and Technology Publications, pp. 444–449. ISBN: 9789897582592. URL: http://www.scitepress.org/DigitalLibrary/Link.aspx?doi=10.5220/0006426504440449 (visited on 2024-07-29).

Wei, Huanxia (Sept. 2022). "A Method for Patient Gait Real-time Monitoring based on Powered Exoskeleton and Digital Twin". In.

Williams, T. J. (July 1993). "The Purdue Enterprise Reference Architecture". In: *IFAC Proceedings Volumes*. 12th Triennal Wold Congress of the International Federation of Automatic control. Volume 4 Applications II, Sydney, Australia, 18-23 July 26.2, Part 4, pp. 559–564. ISSN: 1474-6670. URL: https://www.sciencedirect.com/science/article/pii/S1474667017485326 (visited on 2024-04-05).

Yilmaz, Ercan Nurcan and Serkan Gonen (Aug. 2018). "Attack detection/prevention system against cyber attack in industrial control systems". In: *Computers & Security* 77, pp. 94–105. ISSN: 0167-4048. URL: https://www.sciencedirect.com/science/article/pii/S0167404818303316 (visited on 2024-04-04).

Zscaler (2025). *What Is the Purdue Model for ICS Security? | Zscaler*. en. URL: https://www.zscaler.com/resources/security-terms-glossary/what-is-purdue-model-ics-security (visited on 2025-09-28).

This page intentionally left blank.