ISBN: 978-81-972400-5-8

7. A Study of Cybersecurity Applications with Reference to Industrial Framework

Nishant Kumar

Assistant Professor,
Arka Jain University,
Jamshedpur.

Abstract:

The Cybersecurity poses a multifaceted challenge for companies embracing the industry 4.0 paradigm, where the interconnection of physical systems through the Internet amplifies vulnerabilities. Recently, scholarly attention has turned toward understanding how cybersecurity is conceptualized within the context of Industry 4.0. This paper aims to conduct a systematic literature review to explore how existing research addresses cybersecurity concerns within Industry 4.0 environments. Specifically, we examine key elements such as assets susceptible to cyber-attacks, system vulnerabilities, cyber threats, risks, and countermeasures in industrial settings where physical systems are interconnected. Our analysis is structured into four main areas: defining cybersecurity and Industry 4.0, the industrial sectors examined in the literature, the characterization of cybersecurity, and management strategies for addressing cybersecurity challenges. By scrutinizing the literature, we identify recurring themes and nuances in each area, contributing to the development of a comprehensive framework. This framework not only sheds light on current understanding but also paves the way for future research endeavors and practical applications.

7.1 Introduction:

An increasing number of companies are embracing the industry 4.0 paradigm, also referred to as the Industrial Internet of Things (IIoT) or Industrial Internet, by integrating factories and plants with the Internet to enhance efficiency and effectiveness. However, within these interconnected industrial environments, cybersecurity emerges as a critical challenge.

McKinsey & Company, a management consulting firm, suggests that Industry 4.0 transformations have the potential to generate significant value, equating to efficiency improvements of 15 to 20 percent. This value manifests in various ways, including reduced machine downtime through predictive maintenance or remote monitoring and enhanced labor productivity via the automation of manual tasks. Additionally, the ability to analyze vast amounts of data from industrial processes, such as data from sensors and actuators linking machines and products to computing systems, yields benefits such as inventory reduction, improved service levels (e.g., shorter time-to-market, delivery times, and freight costs), and enhanced product quality meeting customer expectations. However, cybersecurity is paramount in Industry 4.0 contexts to safeguard companies' competitiveness.

According to the Cisco 2018 Annual Cybersecurity Report, critical industrial equipment is vulnerable to cyber-attacks, with 31% of organizations experiencing attacks on Operational Technology (OT), and 38% expecting attacks to transition from Information Technology (IT) to OT. Despite cybersecurity being a priority for 75% of experts, only 16% claim their companies are well-prepared to address cybersecurity challenges, primarily due to the absence of precise standards and the lack of managerial and technical expertise required for implementation.

European and international organizations are taking steps in this direction. For instance, the European Cyber Security Organization (ESCO) compiled existing standards and specifications related to cybersecurity in the European Digital Single Market. This document aids companies in understanding applicable schemes for addressing cybersecurity challenges. Moreover, the International Electrotechnical Commission (IEC) issued a guide on information security and data privacy, outlining guidelines for inclusion in IEC publications and their implementation. IEC publications serve as internationally accepted recommendations.

Given the rapidly evolving landscape, cybersecurity is expected to become an integral aspect of the strategy, design, and operations of companies adopting the industry 4.0 paradigm. This paper aims to investigate cybersecurity within Industry 4.0 contexts through a systematic literature review, intending to establish a reference framework for future research and applications in cybersecurity management within Internet-connected industrial environments.

7.2 Research Method:

This study employs a systematic literature review approach to characterize the concept of cybersecurity within Industry 4.0 contexts. This involves examining the industries targeted by cybersecurity, the industrial assets at risk, the types of cyber threats, resulting risks, countermeasures against cyber-attacks, and guidelines and solutions for managing cybersecurity issues.

Following a systematic approach, the literature review process relied on keywords and search terms with a replicable and defined search strategy. While not exhaustive, this approach provides a substantial overview of the current role of cybersecurity within Industry 4.0, highlighting its emergence as a significant research field at the international level.

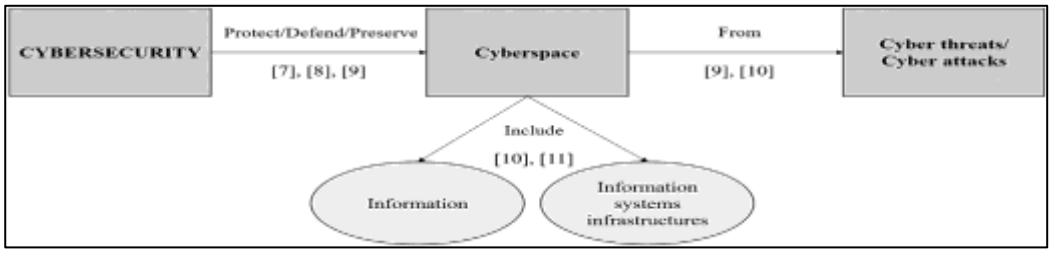

Figure.7.1: Cyber Security Definition

"Prevention of damage to, protection of, and restoration of computers electronic communications systems, electronic communication services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation"; "The protection of information assets by addressing threats to information processed, stored, and transported by internet-worked information systems".

In Figure. 7.1, A schematic representation of the cybersecurity concept integrates insights from the aforementioned definitions. It can be posited that cybersecurity aims to safeguard the cyberspace, encompassing both information and infrastructures, from cyber threats or attacks. Hence, terms such as "cyberspace," "cyber threats," and "cyber-attacks" are integral to the paper selection criteria.

Based on this initial analysis, the first set of papers was identified using the following search queries:

("Cybersecurity" OR "cyber security") AND ("Industry 4.0"):

("Cyber-attack*" OR "cyber threat*" OR "cyberspace") AND ("security") AND "Industry 4.0".

Regarding the term Industry 4.0, variants such as "Industrial Internet of Things" (also referred to as "IIoT" or "Industrial IoT") and "Industrial Internet" (coined by General Electric) from the United States were considered. Consequently, the second set of papers was characterized by the following search queries:

("Cybersecurity" OR "cyber security") AND ("Industrial Internet of Things" OR "IIoT" OR "Industrial IoT" OR "Industrial Internet");

("Cyber-attack*" OR "cyber threat*" OR "cyberspace") AND ("security") AND ("Industrial Internet of Things" OR "IIoT" OR "Industrial IoT" OR "Industrial Internet").

Subsequently, the analysis will focus on the findings derived from these two sets of papers, as defined by the aforementioned search queries.

Definitions:

Following the analysis of the initial set of papers, several definitions highlighted the key elements of Industry 4.0; nevertheless, cybersecurity was only defined in one study as "the protection of theft or damage to IT hardware, software, and the data stored on the systems."

A comparative analysis across the definitions of Industry 4.0 in reference to cyber security, allowed us to notice that some.

1. Definitions	Industry 4.0
	Industrial Internet of Thing or Industrial Internet
	Cybersecurity
2. Industrial focus	Industry types
	Industrial assets
3. Cybersecurity characterization	System security vulnerabilities
	Cyber threats
	Risks
	Countermeasures
4. Managing of cybersecurity risks	Guidelines
	Solutions

Figure 7.2: Areas of Analysis

keywords (such as, Internet of Things, Cyber- Physical Systems, manufacturing and data networking) are very common in the selected papers (see figure 7.3). These words highlight that Industry.

Industry 4.0 is characterized by two pivotal technological conditions, namely the Internet of Things (IoT) and Cyber-Physical Systems (CPS), within the manufacturing industrial context, alongside an enabled condition of data networking. Combining these definitions, Industry 4.0 primarily revolves around the concepts of IoT and CPS in manufacturing settings, involving the networking of data sourced from machines, products, individuals, and the broader interconnection of smart devices across various plants and factories.

Similarly, the analysis of the second group of papers delved into the concept of the Industrial Internet of Things (IIoT), also known as the Industrial Internet, as introduced by General Electric in 2014. Numerous definitions of IIoT were gathered, although only one paper among the selected ones explicitly linked cybersecurity to the condition where "a system does what it is supposed to do and no more." As with the first group of papers, a comparative analysis across IIoT definitions associated with cybersecurity issues revealed common keywords such as sensors, cloud technologies, manufacturing, and IoT device networking, enabling the characterization of the IIoT concept. Three key elements emerged:

The utilization of enabling technologies like wireless sensor networks and cloud technologies, which, supported by advanced industrial analytics and intelligent machine applications, increasingly control and monitor facility functionalities.

The application of these technologies within manufacturing industrial contexts, particularly emphasizing Industrial Control Systems.

The networking of IoT devices associated with machines, computers, and individuals. Combining these concepts, it can be asserted that the Industrial Internet of Things pertains to the utilization of wireless sensor networks, cloud technologies, and advanced analytics within manufacturing contexts, with a focus on controlling and monitoring industrial processes and the networking of IoT devices.

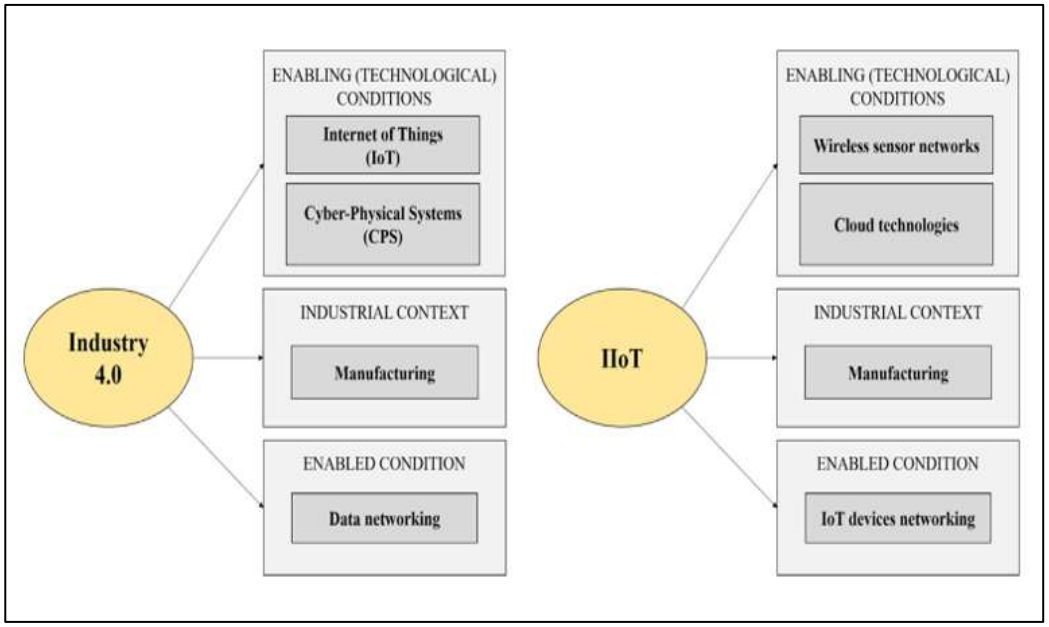

Figure 7.3: Comparison between Industry4.0 and Industrial Internet of Things.

networks(tomonitorfunctionalitiesoffacilities)andcloudtechnologies(tomanagedata producedbysensors)withinmanufacturing industrial contexts. The Internet of Things (IoT) refers to a collection of networked, interconnected gadgets that are connected to computers, machines, and humans.

The terms related to Industry 4.0 and the Industrial Internet of Things in respect to cybersecurity concerns are represented graphically in Figure 7.3

7.3 Industrial Focus:

This section aims to analyze the industries and related assets susceptible to cybersecurity issues within the contexts of Industry 4.0 and the Industrial Internet of Things (IIoT), with a focus on industrial assets directly affected by cyber-attacks.

Upon reviewing the literature from the two groups of papers, it is evident that the manufacturing industry is the primary sector addressed in studies concerning cybersecurity issues. Specifically, out of 26 papers in the first group, 15 explicitly mention the manufacturing industry, while six papers mention Critical Infrastructures (CI) without specifying further. It's worth noting that CI encompasses various sectors, including manufacturing, chemical, commercial facilities, communications, and more. Conversely, only one paper explicitly discusses the healthcare industry, while three papers do not specify any particular industry.

Similarly, among the 14 papers in the second group, six explicitly mention the manufacturing industry, while the others are distributed as follows: one paper focuses on Critical Infrastructures, three on the energy industry, one on telecommunications, and three do not specify any industry. Regarding the industrial assets involved in cyber-attack events, all papers from both groups highlight Industrial Control Systems (ICS) and Cyber-Physical Systems (CPS) as vulnerable systems requiring protection.

Industrial Control Systems (ICS) are management and control systems that automate industrial technical facilities while monitoring business processes. They encompass various control components such as electrical, mechanical, hydraulic, and pneumatic systems, commonly used in critical infrastructures and industries including electrical, water and wastewater, oil and gas, transportation, pharmaceuticals, and manufacturing. ICSs include Supervisory Control and Data Acquisition (SCADA) systems and Distributed Control Systems (DCS), with core components like Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), and Intelligent Electronic Devices (IEDs).

7.4 Cyber Security Characterization:

After determining which industrial assets, or what has to be secured, are primarily involved in cybersecurity challenges in Industry 4.0 contexts, this section makes use of the identification of the systems' inherent weaknesses that compromise their security the dangers posed by cyberspace to the systems. The threats posed by cyberattacks, The defenses against cybersecurity vulnerabilities. All of these components are related to the idea of cybersecurity. Specifically, (1) and (2) respond to the questions "what is to be protected against?"; (3) identifies the possible risks that the business may face as a result of cyberattacks taking advantage of system vulnerabilities (i.e., "what are the impacts?"); and (4), finally, responds to the question "how should you protect yourself?"

7.5 Systems Vulnerability:

Vulnerabilities, as defined by Jansen and Jeschke, are weaknesses in IT or automation systems that could be exploited by hackers to compromise cyber-physical systems. In a broader sense, the NIST glossary defines vulnerabilities as weaknesses in information systems, security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. These vulnerabilities can be categorized based on remote access, software, and Local Area Network (LAN), and they may affect virtual machines within cloud resources and IT systems. Among various types of vulnerabilities affecting CPSs or ICSs, zero-day vulnerabilities are particularly common and exist in interfaces

where information exchange occurs. Notably, SCADA systems exhibit numerous vulnerabilities across different components, including communication infrastructure, network protocols, application servers, database servers, human-machine interfaces, program logic controllers, and remote terminal units.

IoT devices are often targets for botnets due to manufacturers' lack of prioritization of security. Common security lapses include the use of default passwords and open ports, absence of mechanisms for automatic firmware updates, and neglect of firmware updates after installation. Jansen identifies several reasons why most industry devices are vulnerable to hacking: devices often run without security updates or antivirus tools for extended periods; many controllers in ICS networks can be disrupted by malformed or high-volume network traffic, as they were designed without cybersecurity considerations; multiple entry points allow cyber threats to bypass existing security measures; and many ICS networks lack isolation between unrelated networks, enabling malware spread even to remote plant sites.

To address these issues, companies should conduct vulnerability assessments to identify and assess potential system vulnerabilities. NIST defines vulnerability assessment as a systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, predict the effectiveness of proposed security measures, and confirm their adequacy post-implementation.

Cyber threats, according to the NIST glossary, are circumstances or events with the potential to adversely impact organizational operations or assets through unauthorized access, destruction, disclosure, modification of information, or denial of service. Attacks on interconnected physical systems can be characterized by the type of attacker (insider or outsider), aims and objectives (e.g., destruction, specific targeting), and attack mode (active or passive). Active attacks aim to make changes to system resources or operations, while passive attacks aim to learn or use information from a system without making changes. Cybersecurity threats can act on three main layers: the aware execution layer (e.g., sensors, actuators), the data transport layer (e.g., network architecture), and the application control layer (e.g., user data storage). Each layer is susceptible to different types of attacks, such as physical attacks, denial of service attacks, routing attacks, unauthorized accesses, and malicious code dispatching.

When cyber threats succeed, unauthorized access to information systems, including confidential data, can occur, leading to various impacts such as unauthorized use, disclosure, disruption, modification, or destruction of critical data or interfaces; denial of service of networks and computers; and risks to the confidentiality, integrity, and availability of information systems. These impacts can result in reduced company productivity and competitiveness, increased costs, and loss of profitability.

Countermeasures refer to actions, devices, procedures, or techniques that oppose threats, vulnerabilities, or attacks by eliminating or preventing them, minimizing harm, or facilitating corrective action. Jansen suggests three high-level approaches to secure Industrial Control Systems: hardening the perimeter using firewalls and demilitarized zones, implementing defense in depth with multiple layers of defense throughout the network, and securing remote access with Virtual Private Networks.

Continuous updating of security controls at the device, network, and plant/factory levels is crucial to maintaining protection. Cheminod et al. emphasize the role of countermeasures in protecting against unwanted accesses and separating critical services within the plant, between different areas, subsystems, and production cells. Encryption is a commonly adopted countermeasure, offering various levels of protection such as encrypting communication between entities, stored data, and data streams to mitigate tampering, information disclosure, repudiation, and denial of service threats.

7.6 Managing of cyber security issues:

In this section, we present an overview of the recommendations and solutions put forward in the selected papers to address cybersecurity challenges within Industry 4.0 settings. These recommendations and solutions reflect the presence of several security standards and guidance documents, which establish a shared understanding of industry-specific security measures and methods for evaluating their effectiveness. Specifically, the papers primarily cite:

NIST 800-53, which outlines various security control categories and families covering aspects such as access control, awareness and training, audit and accountability, security assessment and authorization, configuration management, contingency planning, identification and authentication, incident response, maintenance, media protection, physical and environmental protection, planning, personnel security, risk assessment, system and services acquisition, system and communications protection, system and information integrity, and program management.

Guidelines: The following provides an overview of the key guidelines in the cybersecurity field gathered from the literature, particularly focusing on the manufacturing industry. Huxtablea and Schaefera propose that companies should support their connected products, particularly in:

- Providing cybersecurity consulting to offer advice and guidance on cybersecurity strategy at a high level.
- Implementing risk management strategies to prevent cyber-attacks.
- Establishing threat monitoring and detection mechanisms through software and hardware to identify cyber threats.
- Implementing cyber incident response measures to limit damage and prevent further cyber-attacks.
- Offering training programs to reduce the likelihood of successful cyber-attacks.
- Providing cybersecurity packages tailored to the products being sold, which may include basic subscriptions offering anti-malware software as a service, along with monitoring, detection, and training.

Generally, any security strategy should focus on network, transport, and application levels. Specifically, attention to the network level aims to ensure a secure and reliable connection; the transport level aims to prevent unauthorized access and authenticate both parties; and the application level aims to ensure information security even without encryption at the transport level.

To ensure information security at each level, Sergey and Nikolay recommend a series of actions, including:

- Identifying information sources.
- Classifying objects requiring protection.
- Describing potential threats from unauthorized access and malicious changes to information.
- Implementing measures to prevent unauthorized access and changes to information, as well as corrective measures in case of unauthorized access or changes.
- Regarding the implementation of industrial security services, Jansen outlines four steps:
- Designing the service based on knowledge of automation systems and their operational environment.
- Defining operations for managed security services to address customer needs.
- Implementing the DevOps approach to integrate operational experience into the development process.
- Introducing control loops to socio-technical and economic systems of industrial companies to restore system stability in case of disturbances.

7.6.1 Solutions:

Solutions: In addition to the previously mentioned guidelines, various cybersecurity solutions are proposed in the analyzed papers to address cybersecurity challenges within Industry 4.0 contexts. These solutions are described using a variety of terms, such as framework, approach, method, model, methodology, and architecture.

For example, Babycino and Seker propose Software-Defined Networks (SDN)-based cybersecurity resilience mechanisms for manufacturing applications. They suggest a framework that encompasses system identification, setting resilience objectives, vulnerability analysis, and stakeholder engagement. Similarly, NIST proposes a framework to address and manage cybersecurity risks associated with Industrial Control Systems, consisting of five core functions: identification, protection, detection, response, and recovery, each implemented through a set of security controls.

The DevOps approach is highlighted as enabling new industrial security business, where log sources for security monitoring of comparable asset classes are identified. To visually represent security risks, Kobara introduces an improved attack tree approach, depicting the problem as the root and its sources as leaves, along with the severity level of each stage, transferability between stages, and the effects of countermeasures.

Ren et al. discuss various risk evaluation methods, including quantitative and qualitative approaches, developed for manufacturing systems. For instance, they mention the hierarchical model, which identifies potential vulnerabilities of a system across six layers: control, communication, network, supervisory, and management.

Quantitative methods like Bayesian probability and Leontief-based models are also mentioned, along with qualitative methods providing a holistic view of risks through conceptual diagrams and graphs.

Preuveneers and Ilie-Zudor, as well as Preuveneers et al., model the networked production workflow as a data flow diagram to conduct STRIDE security analysis, a threat modeling method developed by Microsoft focusing on Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege.

Furthermore, Flatt et al. adopt the process model of VDI/VDE guideline 2182 to consider IT security across the entire lifecycle of industrial systems, encompassing eight iterative steps: identifying assets, determining relevant security objectives, analyzing threats, assessing risks, identifying measures and assessing effectiveness, selecting an overall solution, implementing and using the overall solution, and performing audits.

Januario et al. propose a methodology for assessing vulnerabilities in Industrial Control Systems, which involves creating a complete network representation for each component, defining the functionalities of each subsystem, and listing the resources and operations used for each operation.

Lastly, Bordel et al. describe a functional architecture supporting a protection system for Industry 4.0 applications, consisting of five elements: a predictive model representing the system's state at a certain moment and in the future, an analysis module comparing data to the real state of components in the system, a template repository describing different cyber-physical attacks and associated security policies, a distance function determining the closest templates to system observations, and a decision-making module selecting the appropriate protection method.

7.7 A Framework for Cyber Security In I-4.0:

The intersection of cybersecurity and Industry 4.0 began to gain significant attention around 2015, as evidenced by searches in electronic scientific databases. While the term "Industry 4.0" was first introduced in Germany in 2011, awareness of cybersecurity issues concerning industrial systems connected to networks developed gradually afterward. There remains a need for further investigation to systematically understand the key elements and support industrial management in addressing cybersecurity challenges effectively.

The findings of this study are categorized into four main areas: analysis of cybersecurity and Industry 4.0/IIoT definitions, examination of the industrial context, characterization of cybersecurity within Industry 4.0 scenarios, and identification of management strategies for addressing cybersecurity issues. These areas provided insights and considerations for future research.

Initially, analyzing representative definitions of "cybersecurity" facilitated the creation of a taxonomy for the study. This involved incorporating terms such as "cyberspace," "cyber threats," and "cyber-attacks" into the search criteria. Additionally, identifying keywords associated with Industry 4.0 and IIoT allowed for pinpointing technological conditions, target industries (particularly manufacturing), and specific conditions enabled by these technologies, such as data networking for Industry 4.0 and IoT devices networking for IIoT. A comprehensive definition for both concepts was formulated by combining the identified keywords.

Furthermore, the analysis highlighted the centrality of the manufacturing industry in cybersecurity issues, with Industrial Control Systems and Cyber-Physical Systems being identified as primary vulnerable systems requiring protection from cyber-attacks.

A significant aspect of the study involved characterizing cybersecurity within the context of Industry 4.0/IIoT, focusing on system vulnerabilities, potential cyber threats, associated risks, and countermeasures. It was found that security is not always a priority for many manufacturers, leading to common vulnerabilities such as weak passwords, open ports, neglecting firmware updates, and inadequate monitoring of installed firmware. Unknown vulnerabilities, including zero-day vulnerabilities, pose significant risks, emphasizing the importance of vulnerability assessment processes to identify and address security deficiencies effectively.

The analysis of cyber threats identified various attacks affecting Industrial Control Systems and Cyber-Physical Systems, with Denial-of-Service attacks being among the most prevalent. These threats can target different layers of interconnected physical systems, highlighting the need for detailed characterization specifying the type of attacker, objectives, and attack mode. Countermeasures such as network isolation, defense in depth strategies, and the use of Virtual Private Networks were identified to prevent or mitigate cyber threats, with encryption being a commonly mentioned measure.

Finally, the study examined guidelines and solutions in the literature for managing cybersecurity issues, noting the existence of security standards and guidance documents providing industry-specific security controls and assessment methods. While some solutions offer high-level guidance for management, others propose more structured approaches tailored to specific industrial scenarios.

In conclusion, this study provided a structured analysis of cybersecurity issues in Industry 4.0 contexts, offering insights for future research and managerial decision-making. Future research can use this study as a reference framework to advance investigations in the industrial field, while managerial stakeholders can leverage it to gain a comprehensive understanding of cybersecurity in Industry 4.0 and inform decision-making processes and training initiatives within IT departments.

7.8 References:

1. Behrendt, N. Müller, P. Od enwälder, C. Schmitz, Industry4.0 Demystified—Lean's Next Level [Online].
2. Cisco, Cisco2018Annual Cyber security Report, (2018).
3. Bauer, G. Scherf, V. vonder Tann, Six Ways CEOs Can Promote Cyber security in the IoT Age [Online]. Available, Mc Kinsey &Company, 2017
4. E.C.S. Organisation, StateoftheArt Syllabus Overview of Existing Cybersecurity Standards and Certification Schemes,ECSO,2017.
5. C. o. N. S. S. CNSS, Committee on National Security Systems (CNSS) Glossary,(2015).
6. J. Huxtablea, D. Schaefera, On servitization of the manufacturing industry in the UK, Procedia CIRP52(2016)46–51.

7. He, C. Maple, T. Watson, A. Tiwari, J. Mehnen, Y. Jin, B. Gabrys, The security challenges in the IoTenabled cyber-physical systems and opportunities for evolutionary computing & other computation a lintel ligence, 2016 IEEE Congress on Evolutionary Computation,(2016).
8. E. P on tarollo, Industry 4.0: a new approach to industrial policy, L'industria37(3) (2016)375–381.
9. Daniels, B. Amaba, A. Sargolzaei, Industrial control system applications go mobile in the cloud, IAMOT2016-25th International Association for Management of Technology Conference, Proceedings: Technology- Future Thinking, (2016).
10. Jansen, A review on the read inesslevel and cyber-security challenges in Industry4.0, ACMSEEDA-CECNSMConference2017, (2017).
11. Bordel, R. Alcarria, D. Sánchez-de-Rivera, T. Robles, Protecting Industry4.0 systems against the malicious effects of cyber-physical attacks, Computer Science Book Series, Springer, Cham,2017,pp.161–171.
12. H. Gao, Y. Peng, Z. Wen, K. Jia, H. Li, Cyber-physical systems test bed based on cloud computing and software defined, Proceedings-2015 International Conference on Intelligent Information Hid ingand Multimedia Signal Processing,(2015).
13. Mugarza, J. Parra, E. Jacob, Software updates in safety and security co-engineering, Computer Safety, Reliability, and Security, Springer, Cham, 2017, pp. 199–210.
14. H. Flatt, S. Schriegel, J. Jasperneite, H. Trsek, H. Adamczyk, Analysis of the cyber-security of industry 4.0 technologies based on RAMI4.0 and identification of requirements, IEEE International Conference on Emerging Technologies and Factory Automation(2016).
15. C. J. Smith, The industrial internet of things and cyber security. Anecological and system icperspective on security indigital industrial eco systems, Petroleum and Chemical Industry Conference Europe Conference,(2017).
16. L. Urquhart, D. McAuley, Avoid ingthe Internet of insecure industrial things, Comput. Law Secur. Rev.: Int. J. Technol. Law Pract. 34(3) (2018)450–466.
17. G.J. Palavicini, J. Bryan, E. Sheets, M. Kline, J. San Miguel, Towards firm ware analysis of Industrial Internet of Things (IIoT)-applying symbolic analysis to IIoT firm ware vetting, 2nd International Conference on Internet of Things, Big Data and Security,(2017).
18. B. VanLier, The Industrial Internet of Things and Cyber Security. An ecological and systemic perspective on security in digital industrial ecosystems,201721st International Conference on System Theory, Control and Computing,(2017).
19. NIST-National Institute of Standards and Technology. Cybersecurity framework-CriticalInfrastructureResources,13February2018.[Online].[Accessed22March 2018]Available: NIST https://www.nist.gov/cyberframework/critical-infrastructure-resources
20. X. Fan, K. Fan, Y. Wang, R. Zhou, Overview of cyber-security of industrial control system, 2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), (2015).
21. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, A. Hahn, Guide to Industrial Control Systems (ICS) Security, NIST-NationalInstituteofStandardsandTechnology,2015.
22. Cyber-security of SCADA and Other Industrial Control Systems, Springer, Cham, 2016, pp.15–28.

23. T. Lu, X. Guo, Y. Li, Y. Peng, X. Zhang, F. Xie, Y. Gao, Cyber physical security for industrial control systems based on wireless sensor networks, Int. J. Distrib.Sens.Netw.10(6)(2014)p.17.
24. Preuveneers, W. Joosen, E. Ilie-Zudor, Trustworthy data-driven net worked production for customer-centric plants, Ind. Manag. Data Syst. 117 (10) (2017)2305–2324.
25. M.Cheminod,L.Durante,L.Seno,F.Valenza,A.Valenzano,C.Zunino,Leveraging SDN to improve security in industrial networks, IEEE International Workshop on Factory Communication Systems-Proceedings,(2017).
26. G. Corbò, C. Foglietta, C. Palazzo, S. Panzieri, Smart behavioral filter for industrial internet of things, Mobile Networks and Application, Springer, 2017,pp.1–8.
27. Preuveneers, E. Ilie-Zudor, Identity management for cyber-physical production work flows and individualized manufacturing inindustry4.0, Proceedings of the ACM Symposium on Applied Computing PartF128005,(2017).
28. R. Roy, R. Stark, K. Tracht, S. Takata, M. Mori, Continuous maintenance and the future–foundations and technological challenges, CIRP Ann. Manuf. Technol.65(2)(2016)667–688.
29. Yang, Y. Chen, W. Huang, Y. Li, Survey on artificial intelligence for additive manufacturing, ICAC2017-201723rdIEEE International Conference on Automation and Computing, (2017).
30. S. Tedeschi, D. Rodrigues, C. Emmanouilidis, J. Erkoyuncu, R. Roy, A. Starr, A cost estimation approach for IoT modular architectures implementation in legacy systems, Procedia Manuf. 19(2017)103–110.
31. S. Lee, S. Lee, H. Yoo, S. Kwon, T. Shon, Design and implementation of cyber security test bed for industrial IoT systems, J. Super comput. (2017)1–15.
32. Kobara, Cyber physical security for industrial control systems and IoT, IEICE Trans. Inf. Syst.E99D (4) (2016)787–795.
33. Januario, C. Carvalho, A. Cardoso, P. Gil, Security challenges in SCADA systems Ultra-Modern(2016).
34. C. Jansen, Stabilizing the industrial system: managed security services' contribution to cyber-peace, IFAC-Papers on Line 50 (1) (2017) 5155–5160.
35. T. Ahram, A. Sargolzaei, S. Sargolzaei, J. Daniels, B. Amaba, Block chain technology innovations, 2017 IEEE Technology & Engineering Management Conference(TEMSCON),(2017).
36. B. Diebera, B. Breilinga, S. Taurera, S. Kaciankab, S. Rass, P. Schartner, Security for the robot operating system, Rob. Auton. Syst. 98(2017)192–203.
37. C. Jansen, S. Jeschke, Mitigating risks of digitalization through managed industrial security services, AI Soc. J. (2018)1–11.