
Proceedings Paper:
Comert, M., Ahmed, A. and Ahmed, H. (2025) Identifying security challenges in the transition from traditional to smart manufacturing through IIoT retrofitting. In: Peltonen, E., Hyrynsalmi, S., Wagner, I., Rellermeyer, J. and Mohan, N., (eds.) IoT '24: Proceedings of the 14th International Conference on the Internet of Things. IoT 2024: 14th International Conference on the Internet of Things, 19-22 Nov 2024, Oulu, Finland. ACM, pp. 285-289. ISBN: 9798400712852.

https://doi.org/10.1145/3703790.3703824

Identifying Security Challenges in the Transition from Traditional to Smart Manufacturing Through IIoT Retrofitting

Mert Comert
Nuclear AMRC
The University of Sheffield
Sheffield, United Kingdom
m.comert@sheffield.ac.uk

Arslan Ahmed
Nuclear AMRC
The University of Sheffield
Derby, United Kingdom
arslan.ahmed90@gmail.com

Hafiz Ahmed
Nuclear AMRC
The University of Sheffield
Derby, United Kingdom
hafiz.ahmed@sheffield.ac.uk

Abstract

The integration of Industrial Internet of Things (IIoT) sensors and devices into traditional manufacturing environments offers significant benefits in terms of efficiency, adaptability, and data-driven decision-making. However, the transition from traditional manufacturing systems to smart manufacturing systems, often achieved through retrofitting legacy systems, introduces new security risks that must be carefully addressed to ensure operational resilience. This paper explores the vulnerabilities and threats associated with retrofitting legacy systems with modern Industrial IoT technologies. By examining recent case studies and industry incidents, critical security gaps that emerge from the coexistence of legacy systems and contemporary IoT solutions are identified. These gaps include unauthorized access, data breaches, system manipulation. The research emphasizes the necessity of adopting a proactive cybersecurity approach that is well-suited to the specific vulnerabilities and risks associated with retrofitting traditional manufacturing systems. These measures include updated security protocols, enhanced device management practices, secure software updates, and ongoing system monitoring. By implementing these strategies, manufacturers can mitigate risks, protect their intellectual property, and maintain operational continuity. Outcome of the paper provide manufacturers with strategic insights and practical recommendations to safeguard the integrity and reliability of their smart manufacturing environments against evolving cyber threats. By addressing these security challenges proactively, organizations can realize the full potential of IIoT technologies while minimizing risks to their operations.

Keywords

Industry 4.0, Digital Manufacturing, Information Technology, Data, Industrial IoT, Sensors, Network, Threat, Vulnerability, Countermeasure ,Operational Technology

ACM Reference Format:
Mert Comert, Arslan Ahmed, and Hafiz Ahmed. 2024. Identifying Security Challenges in the Transition from Traditional to Smart Manufacturing Through IIoT Retrofitting. In *14th International Conference on the Internet of Things (IoT 2024), November 19–22, 2024, Oulu, Finland*. ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3703790.3703824

IoT 2024, November 19–22, 2024, Oulu, Finland

ACM ISBN 979-8-4007-1285-2/24/11
https://doi.org/10.1145/3703790.3703824

1 Introduction

Manufacturing serves as a key pillar of the economy, with over 230,000 companies employing more than 27 million individuals. These industries collectively contribute around €1.3 trillion in added value across Europe [20]. Prior to the rise of digital manufacturing, traditional manufacturing systems were predominantly driven by manual labour and mechanical operations. These systems depended significantly on human involvement for both production tasks and decision-making processes. Factories followed a linear workflow, with machines operating independently, while data collection was carried out manually or with minimal automation. Digital manufacturing is a modern approach that integrates advanced technologies such as the Industrial Internet of Things (IIoT), cloud computing, artificial intelligence, machine learning, and robotics. Its primary goal is to boost productivity and reduce costs by automating processes and enhancing data-driven decision-making throughout the production cycle [6, 15, 21]. Digital manufacturing is a key component of Industry 4.0, which enables the establishment of smart factories characterized by the seamless collaboration of machines, systems, and humans. The Internet of Things (IoT) plays a crucial role in enhancing the value of digital manufacturing. The primary function of IoT devices is to provide accurate, real-time information from various machines, equipment, and processes. This capability facilitates new analytical opportunities and enables rapid dissemination of results, thereby supporting decision-making processes effectively [8]. In contrast to large corporations that have made significant progress in adopting smart manufacturing practices, small and medium-sized enterprises (SMEs) face challenges in embracing these advancements [16]. Many SMEs struggle with limited budgets, expertise, and access to necessary tools to effectively implement such technologies [23].

A common challenge faced by many manufacturing companies is their reliance on legacy machines and equipment that are not equipped for digital manufacturing. As these companies seek to enhance digital connectivity within their production lines, they must decide whether to substitute their outdated machinery with new models or retrofit their existing assets to meet modern requirements [3, 17]. While modernizing machinery can offer immediate digital advantages, the financial burden and potential conflict with sustainable production are significant considerations [11, 14]. By utilizing low-cost industrial IoT sensors and devices, manufacturers, particularly small and medium-sized enterprises (SMEs), can transform their legacy machinery into monitored and manageable assets. This integration allows for enhanced visibility and control over operations, improving overall efficiency and decision-making.

Cybersecurity focuses on protecting the availability, privacy, confidentiality, and integrity of digital information, whether it is stored or transmitted in various formats. With the rise of sophisticated cyberattacks, individuals, businesses, and governments must prioritize protection measures such as firewalls and intrusion detection systems (IDS) [4]. However, as technology advances and becomes more interconnected, the risk of security vulnerabilities also increases [9].

In digital manufacturing, cybersecurity ensures that product information, manufacturing processes, and resource data are protected from unauthorized access or tampering. This safeguards the integrity and confidentiality of operations, building trust and collaboration among stakeholders [22]. The Industrial Internet of Things presents distinct security challenges, particularly in safeguarding critical industry control systems [1, 5], due to its differences from the Internet of Things. While IIoT enhances traditional industrial systems with improved connectivity, scalability, and real-time intelligence, it simultaneously introduces new vulnerabilities. For instance, traditional Operational Technology (OT) systems were initially designed to be isolated from enterprise IT networks and were not built with cybersecurity in mind. The growing interconnectivity among networks and devices significantly increases the number of entry points into OT systems, heightening their susceptibility to cyber threats. This evolving landscape necessitates the implementation of new security designs and practices to effectively mitigate these risks [24]. In this research paper, we examine the security vulnerabilities, threats, and corresponding countermeasures related to retrofitted legacy machines integrated with Industrial IoT and devices that inherently possess Industrial IoT technology.

2 Traditional Security Outlook

Research done by Kolla et al. in [12] focuses on retrofitting legacy machines in SMEs to enable data gathering capacity, thereby facilitating their transition to Industry 4.0 (I 4.0). A highlevel overview of this can be seen in Figure 1. Through a structured literature survey, the study identified retrofitting technology as a crucial initial step. This involves analysing various variables for measurement, such as sensor types, manufacturers, communication interfaces, and mounting points, while leveraging existing electronics to minimize costs. A general architecture for integrating legacy machines with reporting and analytical systems, categorized into physical and cyber layers, was developed. The process involves retrofitting intelligent sensors, actuators, and IoT devices onto existing machinery to establish connectivity with digital networks. Incorporating IoT nodes such as microcontrollers or PLCs facilitates the extraction of data from sensors and enables internet connectivity, thereby setting the groundwork for subsequent stages of the project.

The implementation of an IIoT gateway serves as an intermediary layer to guarantee secure communication between the physical and cyber elements. Utilizing standardized communication protocols facilitates efficient and precise data transmission to IIoT middleware, thereby improving interoperability and maintaining data integrity. The gathered data is stored within databases and then forwarded for analysis through either web-based applications or local edge computing devices. This crucial step enables SMEs to engage in real-time monitoring, analysis, and decision-making processes, all

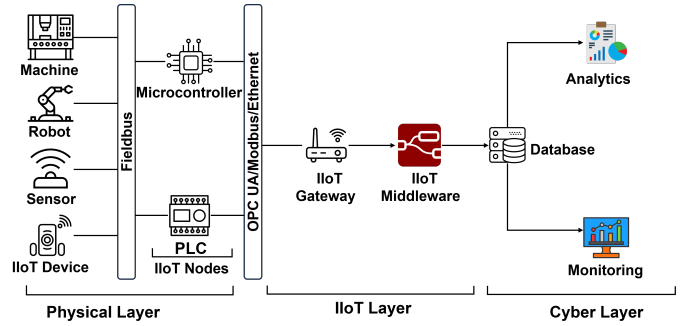

Figure 1: General architecture of IIoT in the context of retrofitting [12].

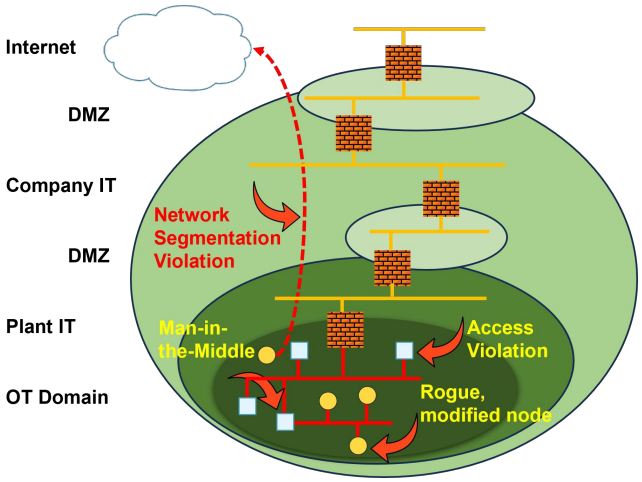

Figure 2: The traditional defense-in-depth strategy is based on the structure of the automation pyramid, where distinct zones are created, each with specific access control points at their intersections [19], including considerations for possible attack vectors (in red) [18].

of which are essential for a successful transition into the Industry 4.0 [12]. Security in retrofitted automation systems is often implemented through multiple layers to address vulnerabilities inherent in older technologies [10]. This strategy, originally proposed in the early 2000s, has since evolved into the best standard for modern security architectures [19].

The traditional approach to securing industrial control systems (ICS) has recognized the inherent limitations of OT systems, such as their lack of built-in security and limited computing resources. To address security risks, a layered security architecture is utilized, which divides the system into zones with different security levels, ensuring rigorous access controls at the boundaries to prevent unauthorized access. The upper layers of the ICS architecture in Figure 2, referred to as IT systems, implement standard IT security practices to manage tasks like data storage and analysis. The lower layers, referred to as the OT domain, are dedicated to field-level devices and their related technologies. The Purdue model has recently evolved to enhance the layered security approach by introducing

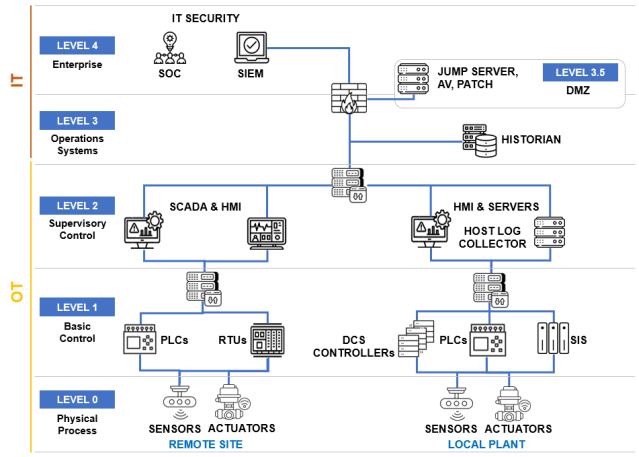

Figure 3: Purdue model of OT and IT system by Dragos ™.

a Demilitarized Zone (DMZ) at the top, which serves to protect systems that require external accessibility while maintaining a separation from the core network. The Purdue model has also served as the foundation for the IEC 62443 standard, which is a comprehensive set of international standards designed to secure industrial automation systems [13]. As shown in Figure 3, the Purdue Model for ICS (Industrial Control Systems) security architecture consists of six layers [18, 19].

- `Level 0: Process Level`: This is the lowest level, directly interacting with physical processes (e.g., sensors, actuators).
- `Level 1: Basic Process Control`: This level includes devices like programmable logic controllers (PLCs) that control individual processes.
- `Level 2: Supervisory Control`: This level oversees multiple processes and provides a centralized view of operations.
- `Level 3: Plant/Unit Management`: This level manages entire plants or units, including production planning and scheduling.
- `Level 4: Enterprise Management`: This level integrates plant-level data with corporate-wide information systems for business decision-making.

This model covers a wide range of cybersecurity aspects, including asset ownership, system integration, component supply, communication networks, management systems, and the overall security lifecycle. By adhering to IEC 62443, organizations can significantly enhance their security posture, reduce risks, comply with regulations, and improve their resilience against cyber threats in industrial environments.

3 Security Challenges of IIoT Sensors and Devices

With the advent of Industry 4.0, the Internet of Things has evolved beyond consumer devices to encompass Industrial IoT, which connects advanced embedded hardware in industrial environments. This shift, leading to the concept of smart factories, optimizes complex production processes, enhancing productivity while reducing costs. Unlike IoT, IIoT focuses on more secure, large-scale data processing and industrial applications. Despite its advanced nature, IIoT shares common security challenges with IoT but IIoT security challenges are generally not as relevant or critical in IoT [24]. In digital manufacturing, devices integrated with IIoT technology are now sold as ready-to-use systems, while companies with legacy machines aim to make cost-effective use of digital retrofitting. This process involves equipping older, non-connected devices with IoT sensors and IIoT capabilities to match the functionality of modern IIoT-enabled machines. Data-driven decision-making has accelerated production processes through this approach. However, retrofitted systems face security challenges due to the lack of embedded security features in older machines. Designed without modern security concerns, these legacy devices lack built-in security protocols and network segmentation, making them more vulnerable to cyber threats. Adapting them to incorporate secure communication protocols, access control, and network isolation is a major challenge. Conversely, systems built with integrated IIoT technology have inherent security features like encrypted communication and authentication measures. Despite this, scaling security for vast networks of connected devices, ensuring data integrity, and addressing new threats like advanced persistent attacks remain challenging. Both approaches demand robust defense strategies, but retrofitted systems often face more foundational challenges, while integrated IIoT systems require maintaining advanced protections against evolving cyber threats. The security challenges with built-in IIoT-enabled devices and digital retrofitting with IIoT devices are as follows:

3.1 Default/Inadequate Security Configurations

- `Built-in IIoT Devices`: Default credentials, poor access control mechanisms, and outdated protocols make these devices vulnerable.
- `Digital Retrofitting`: Incompatible security standards and failure to apply strong security measures during integration can lead to similar vulnerabilities.

3.2 Vulnerabilities Due to Lack of Updates

- `Built-in IIoT Devices`: Firmware vulnerabilities that are not patched or updated can expose devices to attacks.
- `Digital Retrofitting`: Legacy systems often lack the ability to receive updates or don't adhere to modern security practices, creating security gaps.

3.3 Increased Attack Surface

- `Built-in IIoT Devices`: Insufficient encryption and insecure communication protocols make these devices easier targets for attackers.
- `Digital Retrofitting`: Adding new devices to legacy systems increases the attack surface, providing more entry points for cyber threats.

3.4 Data Security and Privacy

- `Built-in IIoT Devices`: Lack of encryption for data in transit and at rest can lead to data interception.

- `Digital Retrofitting`: Retrofitting systems without properly managing data flows increases the risk of data leakage.

3.5 Inadequate Monitoring

- `Built-in IIoT Devices`: Poor user access controls may result in unnoticed changes to device settings or security breaches.
- `Digital Retrofitting`: Legacy systems often lack robust monitoring, making it hard to detect anomalies or breaches.

3.6 Insufficient Pyhsical Access

- `Built-in IIoT Devices & Digital Retrofitting`: Lack of proper protective measures to physically secure IIoT devices and infrastructure from unauthorized access, tampering, theft, or damage. IIoT devices are often deployed in remote or industrial locations where physical security can be overlooked. When devices are left exposed, attackers can gain direct access to hardware, bypass software security controls, alter configurations, or install malicious software, posing significant risks to the overall system.

4 Protective Approaches to IIoT Device Security

Security challenges for IoT sensors and devices result in the following common attack scenarios [18]:

- breach of the legitimate access (Secs. 3.1,3.5) and confidentiality of data (Sec. 3.4)
- man-in-the-middle attacks (Scs. 3.2 and 3.3)
- network segmentation violation attacks (Secs. 3.1 and 3.3)
- insertion of rogue nodes or modification of node functionality (Secs. 3.1 and 3.5)

These attack scenarios are depicted in Figure 2. The following sections will discuss countermeasures with examples [18].

4.1 Breach of the Legitimate Access and Confidentiality of Data

The integration of Industrial Internet of Things systems in manufacturing and industrial sectors has greatly enhanced operational efficiency but also revealed key vulnerabilities, particularly regarding breaches of legitimate access and data confidentiality. Attackers often exploit weak security mechanisms, gaining unauthorized access to control systems and confidential information, potentially compromising operational integrity. One of the key vulnerabilities is the absence of robust authentication mechanisms, which can allow unauthorized users to manipulate system parameters or steal critical data.

Encryption plays a crucial role in addressing these vulnerabilities by protecting data confidentiality. Through encrypting data both in transit and at rest, organizations can ensure that even if data is intercepted, it remains unreadable without the proper decryption keys. For example, encrypted communications between IIoT devices and servers can protect sensitive production data, making it significantly harder for attackers to exploit any intercepted information. In 2017, the Triton malware attack targeted industrial safety systems, allowing hackers to compromise safety protocols and highlighting the need for stronger security measures [7]. One effective defense is the Multi-Factor Authentication (MFA), which requires additional verification beyond passwords to access critical systems, significantly reducing the risk of unauthorized access.

4.2 Man-in-the-Middle Attacks

Man-in-the-Middle (MitM) attacks present considerable security risks to Industrial Internet of Things systems by intercepting and manipulating data exchanged between devices and control systems [2]. This attack enables adversaries to eavesdrop on sensitive communications, inject malicious content, or alter data, causing disruptions that could severely impact industrial operations. For example, in a manufacturing plant, a MitM attack could intercept commands between robotic arms and control systems, leading to malfunctions or even physical damage. To defend against cyber threats, encryption protocols like Transport Layer Security (TLS) are critical in safeguarding IIoT communications by encrypting data exchanges, making intercepted information unreadable without the proper decryption keys. Intrusion Detection Systems complement encryption by monitoring network traffic for unusual activity that may indicate a man-in-the-middle attack, enabling quick intervention. By implementing both encryption and IDS, industries can significantly enhance the security of IIoT systems, protecting critical operations from unauthorized access or tampering.

4.3 Network Segmentation Violation Attacks

Network segmentation violations can seriously threaten the security of IIoT systems by enabling unauthorized access to sensitive data and critical assets. Segmentation helps isolate different parts of the network, limiting the potential damage from a breach. However, if attackers bypass segmentation, they can move laterally through the system, potentially accessing the OT network from the IT network, which could disrupt industrial processes. To mitigate this risk, strong firewall policies can enforce communication controls, restricting traffic between IT and OT networks. Virtual Local Area Networks (VLANs) add another layer of protection by isolating different sections of the network into separate domains. Furthermore, Access Control Lists (ACLs) can regulate inter-VLAN traffic, preventing attackers from easily moving across the network. Continuous monitoring with intrusion detection systems is essential for detecting abnormal behaviors that may signal network segmentation violations. These systems can identify unauthorized access attempts and unusual traffic patterns, enabling security teams to react swiftly, especially in industrial environments where communication between IT systems and OT devices may indicate a potential breach. To prevent such violations in IIoT settings, organizations should implement robust firewall rules, utilize VLAN-based segmentation, and maintain ongoing monitoring to protect sensitive operations and ensure network integrity.

4.4 Insertion of Rogue Nodes or Modification of Node Functionality

The use of digital certificates and Public Key Infrastructure (PKI) is essential for authenticating devices within IIoT systems, as it prevents unauthorized devices from entering the network and compromising security. Rogue nodes, which are unauthorized devices that can disrupt operations or steal data, pose significant threats,

especially when they alter the functionality of legitimate nodes. Countermeasures such as strong device authentication through PKI and continuous monitoring with intrusion detection systems are crucial to detecting and mitigating these risks. By ensuring that only verified devices can communicate and continuously monitoring network activity, organizations can significantly enhance the security of their IIoT networks and protect their industrial operations.

5 Conclusion

The transition from traditional manufacturing systems to digital manufacturing environments presents both significant opportunities and formidable security challenges. Industries are stepping into the smart manufacturing process by integrating various IIoT sensors and devices into outdated machinery, thereby enabling these machines to utilize IIoT technology while adopting a cost-focused approach. Although machines that inherently incorporate IIoT technology and those retrofitted to gain certain IIoT capabilities possess specific security vulnerabilities and countermeasures, it should not be overlooked that devices designed with integrated IIoT technology by manufacturers contain advanced security systems. However, IIoT sensors and devices used in outdated machinery, where digital modernization has been applied, are easily accessible in the market and consist of components that lack basic security measures and users can customize.

This research highlights critical security challenges and vulnerabilities in both retrofitted and advanced systems, recommending countermeasures such as robust encryption, continuous network monitoring, and improved network segmentation. It also reviews the IEC 62443 standardś "defense-in-depth" strategy and emphasizes the need for developing standardized security frameworks tailored to IIoT-enabled digital manufacturing systems that account for the unique characteristics of OT networks rather than relying solely on IT frameworks. Research into advanced threat detection mechanisms, machine learning-based anomaly detection, and resilient design strategies for retrofitted systems will be crucial in beforehand addressing emerging security threats. By proactively engaging with these challenges, the manufacturing sector can leverage the benefits of digital technologies while securing itself against the inherent risks of digital transformation.

Acknowledgments

This work is supported by the CHIST-ERA funded TROCI Project (CHIST-ERA-22-SPiDDS-07) through the UK's Engineering and Physical Sciences Research Council (EPSRC) under grant EP/Y036344/1.

References

[1] Brian Aamoth, William E. Lee, and Hafiz Ahmed. 2022. Net-Zero Through Small Modular Reactors - Cybersecurity Considerations. In *IECON 2022 – 48th Annual Conference of the IEEE Industrial Electronics Society*. 1–5.

[2] Saif Ahmad and Hafiz Ahmed. 2023. Robust Intrusion Detection for Resilience Enhancement of Industrial Control Systems: An Extended State Observer Approach. *IEEE Transactions on Industry Applications* 59, 6 (2023), 7735–7743.

[3] Diego Hernandez Arjoni, Fernando Silveira Madani, Guilherme Ikeda, Gustavo de M Carvalho, Loredana B Cobianchi, Luiz FLR Ferreira, and Emília Villani. 2017. Manufacture equipment retrofit to allow usage in the industry 4.0. In *2017 2nd international conference on Cybernetics, Robotics and Control (CRC)*. IEEE, 155–161.

[4] Abiodun Ayodeji, Antonio Di Buono, Iestyn Pierce, and Hafiz Ahmed. 2024. Wavy-attention network for real-time cyber-attack detection in a small modular pressurized water reactor digital control system. *Nuclear Engineering and Design* 424 (2024), 113277.

[5] Abiodun Ayodeji, Mokhtar Mohamed, Li Li, Antonio Di Buono, Iestyn Pierce, and Hafiz Ahmed. 2023. Cyber security in the nuclear industry: A closer look at digital control systems, networks and human factors. *Progress in Nuclear Energy* 161 (2023), 104738.

[6] Jim Davis, Thomas Edgar, James Porter, John Bernaden, and Michael Sarli. 2012. Smart manufacturing, manufacturing intelligence and demand-dynamic performance. *Computers & Chemical Engineering* 47 (2012), 145–156.

[7] Alessandro Di Pinto, Younes Dragoni, and Andrea Carcano. 2018. TRITON: The first ICS cyber attack on safety instrument systems. *Proc. Black Hat USA* 2018 (2018), 1–26.

[8] Brian Hartmann, William P King, and Subu Narayanan. 2015. Digital manufacturing: The revolution will be virtualized. *McKinsey & Company* (2015).

[9] Christoph Jansen. 2016. Developing and operating industrial security services to mitigate risks of digitalization. *IFAC-PapersOnLine* 49, 29 (2016), 133–137.

[10] Juergen Jasperneite, Thilo Sauter, and Martin Wollschlaeger. 2020. Why we need automation models: handling complexity in industry 4.0 and the internet of things. *IEEE Industrial Electronics Magazine* 14, 1 (2020), 29–40.

[11] Muztoba Ahmad Khan, Sameer Mittal, Shaun West, and Thorsten Wuest. 2018. Review on upgradability–A product lifetime extension strategy in the context of product service systems. *Journal of cleaner production* 204 (2018), 1154–1168.

[12] Sri Sudha Vijay Keshav Kolla, Diogo Machado Lourenço, Atal Anil Kumar, and Peter Plapper. 2022. Retrofitting of legacy machines in the context of Industrial Internet of Things (IIoT). *Procedia Computer Science* 200 (2022), 62–70.

[13] Björn Leander, Aida Čaušević, and Hans Hansson. 2019. Applicability of the IEC 62443 standard in Industry 4.0/IIoT. In *Proceedings of the 14th International Conference on Availability, Reliability and Security*. 1–8.

[14] Xinyu Li, Zuoxu Wang, Chun-Hsien Chen, and Pai Zheng. 2021. A data-driven reversible framework for achieving Sustainable Smart product-service systems. *Journal of Cleaner Production* 279 (2021), 123618.

[15] Yan Lu, Katherine C Morris, Simon Frechette, et al. 2016. Current standards landscape for smart manufacturing systems. *National Institute of Standards and Technology, NISTIR* 8107, 3 (2016), 1–39.

[16] Sameer Mittal, Muztoba Ahmad Khan, Jayant Kishor Purohit, Karan Menon, David Romero, and Thorsten Wuest. 2020. A smart manufacturing adoption framework for SMEs. *International Journal of Production Research* 58, 5 (2020), 1555–1573.

[17] Kofi Atta Nsiah, Manuel Schappacher, Christoph Rathfelder, Axel Sikora, and Voicu Groza. 2018. An open-source toolkit for retrofit industry 4.0 sensing and monitoring applications. In *2018 IEEE International Instrumentation and Measurement Technology Conference (I2MTC)*. IEEE, 1–6.

[18] Thilo Sauter and Albert Treytl. 2023. IoT-Enabled Sensors in Automation Systems and Their Security Challenges. *IEEE Sensors Letters* 7, 12 (2023), 1–4.

[19] Albert Treytl, Thilo Sauter, and Christian Schwaiger. 2005. Security measures in automation systems-a practice-oriented approach. In *2005 IEEE Conference on Emerging Technologies and Factory Automation*, Vol. 2. IEEE, 9–pp.

[20] Engelbert Westkämper. 2007. Digital Manufacturing in the global Era. In *Digital enterprise technology: Perspectives and future challenges*. Springer, 3–14.

[21] Dazhong Wu, Shaopeng Liu, Li Zhang, Janis Terpenny, Robert X Gao, Thomas Kurfess, and Judith A Guzzo. 2017. A fog computing-based framework for process monitoring and prognosis in cyber-manufacturing. *Journal of Manufacturing Systems* 43 (2017), 25–34.

[22] Dazhong Wu, Anqi Ren, Wenhui Zhang, Feifei Fan, Peng Liu, Xinwen Fu, and Janis Terpenny. 2018. Cybersecurity for digital manufacturing. *Journal of manufacturing systems* 48 (2018), 3–12.

[23] Thorsten Wuest and Klaus-Dieter Thoben. 2012. Information management for manufacturing SMEs. In *Advances in Production Management Systems. Value Networks: Innovation, Technologies, and Management: IFIP WG 5.7 International Conference, APMS 2011, Stavanger, Norway, September 26-28, 2011, Revised Selected Papers*. Springer, 488–495.

[24] Xingjie Yu and Huaqun Guo. 2019. A survey on IIoT security. In *2019 IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS)*. IEEE, 1–5.