Proceedings of the 33rd European Safety and Reliability Conference (ESREL 2023)
Edited by Mário P. Brito, Terje Aven, Piero Baraldi, Marko Čepin and Enrico Zio
©2023 ESREL2023 Organizers. *Published by* Research Publishing, Singapore.
doi: 10.3850/978-981-18-8071-1_P564-cd

Cyber Security Anomaly Detection In An Industry 4.0 Testbed – Results and Experiences

Stine Aurora Mikkelsplass

Risk & Security Department, Institute for Energy Technology / Østfold University College, Norway. E-mail: stine.mikkelsplass@ife.no

Per-Arne Jørgensen

Risk & Security Department, Institute for Energy Technology / Østfold University College, Norway. E-mail: per.arne.jorgensen@ife.no

This study investigates Industry 4.0 cybersecurity challenges and how the interconnection of information technology (IT) and operational technology (OT) impacts industrial control systems (ICS) vulnerability to cyber-attacks. An ICS testbed, connected to an IT system for data processing and anomaly detection, was designed to examine monitoring and detecting cybersecurity threats using the Elastic Stack. The testbed comprises an OT environment featuring a FischerTechnik Industry 4.0 Training Factory controlled by a Siemens S7-1500 programmable logic controller (PLC). It also employs Elastic, a search-powered solution, for data collection and processing. Elastic "beats" (agents) were used for data collection, including Heartbeat, Machinebeat, Filebeat, and Packetbeat. The research employed the Microsoft Threat Modelling Tool to identify threats and vulnerabilities, generating a prioritised threat list. Based on this list, a security event was developed. We found that Elastic Beats and Security Information Event Management (SIEM) struggled to operate effectively in an ICS environment, with issues reading OT data protocols, such as OPC-UA and Siemens S7. In this paper, we examine the significance of choosing appropriate OT data to establish a baseline for cybersecurity and its potential impact. Additionally, we discuss challenges related to competence building in ICS security, TIA Portal functionality, PLC functionality, and OT data handling.

Keywords: Industrial control systems, cybersecurity, anomaly detection, IT-OT systems, Industry 4.0, IoT

1. Introduction

The fourth industrial revolution, also known as Industry 4.0, is characterised by the interconnection of physical and digital systems, resulting in increased computerisation of manufacturing industries (Smit et al. 2016). This digital transformation has led to the connection of information technology (IT) and operational technology (OT). Today, data is one of the world's most valuable resources (Bhageshpur 2019), and connecting IT and OT enables industries to collect, analyse, and make business decisions based on these data. Equally important, connecting IT and OT allows for centralised monitoring and control of industrial environments (Cisco 2022).

While IT-OT interconnection allows companies to leverage new technologies in their operational environment, it also exposes the ICS to additional vulnerabilities. The connection of OT devices to the Internet enables threat actors to attack the ICS remotely, creating the need for new tools and methods to address these challenges (Pereira, Barreto, and Amaral 2017). This paper presents results from an experiment performed on an ICS Testbed to investigate cybersecurity challenges associated with Industry 4.0. The testbed was developed at the Institute for Energy Technology's (IFE) Cybersecurity Centre and is a high-fidelity testbed consisting of IT and OT components, as well as the Industrial Internet of Things (IIoT) *(Jørgensen and Mikkelsplass 2023)*. The testbed provides real-time monitoring of data and processes, a key point of Industry 4.0. Data from the testbed were monitored, collected, and analysed using the Elastic Stack[i]. The Elastic Stack is a software tool for storing and analysing various types of data, including OT data, and integrates machine learning capabilities for cybersecurity management and operational cybersecurity detection. As part of our research, we focused on challenges related to monitoring and detecting cybersecurity threats in an Industrial Automation and Control System (IACS) environment, specifically within the context of Industry 4.0. The term IACS is defined by ISA/IEC 62443 as *"includes control systems used in manufacturing and processing plants and facilities, building environmental control systems, geographically dispersed operations such as utilities (i.e., electricity, gas, and water), pipelines and petroleum production and distribution facilities"* (IEC 2009). Our research aimed to answer the following research question (RQ): *how to monitor and detect cybersecurity threats within an IACS environment using the Elastic Stack?*

In this paper, three cyber security attacks were conducted within the ICS testbed environment. The findings demonstrate the capabilities of the Elastic Stack for managing and detecting cybersecurity threats in an IT-OT environment. This study discusses the importance of identifying relevant OT data as a baseline for threat detection and how this relates to ICS cybersecurity. Furthermore, it discusses the challenges associated with competence development in IT-OT environments with respect to cybersecurity issues.

This paper is organised as follows: Section 2 presents an overview of cybersecurity challenges within the ICS and provides a context for the testbed environment. In Section 3, the research methodology used in this study is described. Section 4 describes the laboratory setup and ICS testbed infrastructure, while section 5 describes the anomaly detection process. Section 6 presents the threat scenarios selected for the experiment and the experiment results. Section 7 discusses results and challenges, and conclusions and future directions are presented in Section 8.

2. Background

In Industry 4.0, combining IT and OT enables the integration of digital and physical technologies, such as artificial intelligence, the Internet of Things, robotics, and cloud computing (Deloitte Insight 2018). Analytical tools that utilise machine learning, artificial intelligence, and big data make it possible to gain insights into data and make informed decisions. However, the increasing adoption of IIoT devices in manufacturing networks has increased the risk of cyber-attacks (Munirathinam 2020; Yu and Guo 2019). Malicious actors can exploit these systems for industrial espionage, intellectual property theft, information leakage, or production sabotage. As such, resilient network architectures and methods are needed for detecting and responding to cyber threats.

The primary difference between IT and OT systems is that the former focuses on managing information and data, while the latter manages physical operations, such as controlling and monitoring physical assets. IT systems are built to be adaptable and easy to modify, while OT systems are usually built for a specific purpose or task and are designed for continuous operations in harsh environments. Therefore, ICS security requires a holistic approach, and best practices based on standards for design and protection are needed to defend against modern threats (Malatra, Skouloudi, and Koukounas 2019; Knowles et al. 2015).

Testbeds provide a controllable cyber environment for experimentation, prototype testing, and product development across various scientific fields (Edgar and Manz 2017b). In cybersecurity research, testbeds are particularly useful for examining aspects of large and complex systems that cannot be tested at full scale (Arntzen et al. 2019).

3. Research Methodology

To answer the RQ: *how can we effectively monitor and detect cybersecurity threats in an IACS environment using the Elastic Stack?*, we adopted an exploratory research approach to investigate the integration of IT and OT systems in an Industry 4.0 testbed environment (Edgar and Manz 2017a). Our primary objective was to evaluate the effectiveness of the Elastic stack as a tool for cybersecurity management and monitoring.

Using the Elastic Stack for cybersecurity management and detection requires insight into the unique challenges associated with using the Elastic Stack for OT data. In order to address this challenge, we examined the complexities associated with integrating OT data with IT data within an IACS environment. Our research began with a study of the challenges faced by the industry in integrating IT and OT systems. A literature review, interviews with subject matter experts, and experiments with the testbed environment were performed as part of the data collection process. Elastic Stack was evaluated from both the IT and operational perspectives to gain further insight into its potential as a cybersecurity management and monitoring tool. Qualitative as well as quantitative approaches were employed to gain insight into the research problem.

We designed and implemented a testbed environment representing an Industry 4.0 setting to evaluate the Elastic Stack's capabilities. The testbed includes various devices, systems, and applications that generate diverse data types, which are detailed in section 4. This allowed for a comprehensive exploration of the Elastic Stack's capabilities for managing and monitoring IT and OT data. Three cyber-attacks were selected using the STRIDE methodology and Microsoft Threat Modelling Tool[ii].

4. Laboratory Setup

This section introduces the laboratory setup, i.e., the testbed and the surrounding network infrastructure, as well as threat scenarios used in identifying potential threats and vulnerabilities in the ICS testbed. The objective is to gain an in-depth understanding of the security risks that attackers could exploit to compromise the system's security and develop a realistic anomaly detection approach.

4.1. *ICS Testbed*

The ICS testbed consists of both an OT and an IT environment. The OT environment contains a FischerTechnik Industry 4.0 Training Factory controlled by a Siemens S7-1500 programmable logic controller (PLC), a TXT controller, an engineering workstation (EW) and an IoT Gateway. The Industry 4.0 Training factory replicates a manufacturing line, with a vacuum gripper robot (VGR) transporting workpieces from one station to another. Workpieces are available in three colours: red, blue, or white. "Customers" can order workpieces by logging onto Fischertechnik's cloud interface. Once a workpiece is delivered to the "receiving" zone, it is taken up by the VGR and stored in a warehouse. When an order for a workpiece comes in, the VGR picks up the workpiece from the warehouse, transporting it to a processing station. From the processing station it is moved to a conveyor belt which sorts the workpieces by colour. After moving the workpieces to the "shipping" zone, they must be physically picked up. The testbed utilised communication protocols such as TCP/IP, OPC-US, MQTT and Profibus (figure 1).

Data from this ICS testbed is then connected to the IT environment using Elastic, a search-powered solution for data collection, processing, and anomaly detection. The Elastic Stack is built on Elasticsearch, Logstash and Kibana, known as the ELK Stack. These open-source projects are used to search and analyse data (Elasticsearch), process and transform data (Logstash), and visualise data (Kibana). Elastic integrates with various agents called "Beats". This open-source software platform gathers data and metrics across diverse environments. Beats can be installed on servers and containers, or deployed as functions, forwarding data to Elasticsearch or Logstash. A GitHub community is dedicated to developing custom Beats based on the libbeat framework[i] for specific data retrieval and shipping needs. These lightweight data shippers allow users to collect various data from different devices. Some agents are proprietary to Elastic, while others are open source. The beats used in this experiment are Heartbeat, Machinebeat, Filebeat, Packetbeat and Winlogbeat.

Heartbeat periodically checks the status and availability of services (uptime) from the EW, monitoring the host via ICMP, TCP and HTTP(S).

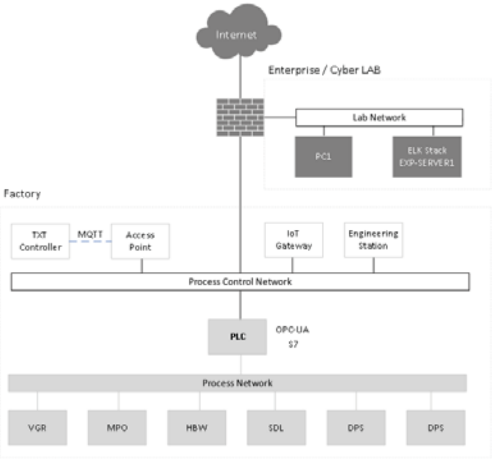

Figure 1: Testbed Network Infrastructure

Filebeat ships collected log data by monitoring specified locations. Once installed and configured, the Filebeat application creates inputs that search for matching log data at specified locations. As soon as a log is located, Filebeat launches a harvester process that opens, reads, and sends data from the log to the output for indexing. Filebeat is installed on the EW and the IoT Gateway.

Packetbeat captures network traffic between application servers and parses application layer protocols into JSON transactions ready for output using Packetbeat's real-time network packet analysis and flow data.

Machinebeat was still in the early stages of development at the time of our experiment. Machine metrics and other related information can be obtained from a PLC through OPC-UA and MQTT interfaces in this experimental version. It is specifically designed for industrial environments and pulls data in real-time.

Winlogbeat sends Windows application-, hardware-, security-, and system events to Elasticsearch or Logstash. Winlogbeat reads event logs from Windows APIs, filters them according to the user's preferences, and sends the results to the desired location.

All beats are installed on the EW, except for Filebeat, which is installed on both the EW and IoT Gateway.

4.2. Identifying Threats and Vulnerabilities

To implement effective security measures, understanding asset and system risk and vulnerability is essential. In our assessment of system threats and vulnerabilities, we employed three methods for identifying threats and vulnerabilities, primarily the Microsoft Threat Modeling Tool. It is a software tool developed to analyse network designs for potential security issues and suggest and manage mitigations. The modelling tool creates an infrastructure model containing objects, services, and protective barriers (figure 2). This tool provides a framework for identifying, communicating, and understanding threats and mitigations, emphasising security and privacy-related threats. Microsoft's STRIDE (Kohnfelder and Garg 1999), a threat modelling methodology, was also used to identify potential threats. STRIDE is a mnemonic and refers to six types of attack: *Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service DoS,* and *Elevation of privilege.* As part of the threat modelling landscape, the STRIDE method is widely used, which assists developers in considering threats when designing systems. Lastly, we used the Common Attack Pattern Enumeration and Classification (CAPEC)[iii] dictionary provided by the MITRE attack framework to identify vulnerabilities and weaknesses within the testbed.

By utilising these methods, we identified the various threats to the testbed and got a deeper understanding of the security vulnerabilities that attackers might exploit to compromise the system's security. Further, we determined which data are required to establish a realistic baseline in this particular environment, which is necessary for developing an effective method of detecting anomalies. The information gained from these methods was the basis for designing the threat scenarios described in section 6. In addition to identifying a DoS vulnerability, we discovered several potential vulnerabilities, including information disclosure and tampering. These vulnerabilities cannot be publicly disclosed.

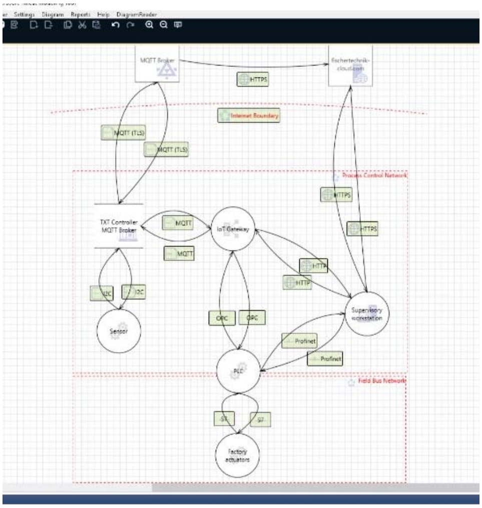

Figure 2: Microsoft Threat Modeling Tool

5. Anomaly Detection

Anomaly detection is crucial to protecting Industry 4.0 against cyber threats. In this section, we discuss the monitoring process, challenges faced with unstable TXT controllers and OT data, baseline challenges, and results of the anomaly detection process.

5.1. Establishing a Baseline

According to NIST, a baseline is defined as *"Hardware, software, databases, and relevant documentation for an information system at a given point in time"* (NIST n.d.). Establishing a baseline for normal operations requires gathering data on the factory while it operates as usual, or functions as intended for the Industry 4.0 testbed. Under these conditions, it is possible to establish a baseline for normal operations, which can be used to identify abnormal behaviour. Based on the previous analysis, we created two baselines: one for network performance and one for producing workpieces.

Establishing a baseline for normal manufacturing process operations is challenging, as the baseline did not account for normal operations of the PLC system without information from the PLC system log (syslog). The authors established two baselines: one for production and shipping time and one for network performance.

5.2. Monitoring

The authors monitored the testbed using the Heartbeat agent to ensure all services were available. The monitoring process, however, helped identify the issue as an unstable TXT controller causing us to have to do a cold restart of the controller every morning to publish messages to the cloud service provider.

We collected data from the testbed using the UAExpert tool[iv], a cross-platform OPC UA test client program, which allowed us insight into the OPC UA data sent to and from the testbed. Using Machinebeat and Filebeat agent configuration files, it retrieved data points from OPC-UA and MQTT interfaces. However, there were challenges associated with data not already available through these interfaces. We lacked the necessary skills to alter the Siemens Control Language (SCL) program to accomplish this task within the project timeframe. Additionally, the Packetbeat agent could not customise and define protocols, limiting their data collection ability.

5.3. Anomaly Detection with Elastic Stack

Elastic licensing is required to unlock SIEM functionality with machine learning capabilities. With Elastic's SIEM, threats can be detected, compliance can be managed, and security incidents can be handled. The detection of threats is done using both supervised and unsupervised machine learning.

6. Threat Scenarios and Results

This section presents the threat scenarios chosen for the experiment and the result of the cyber-attacks.

6.1. Threat Scenario

Security issues can be classified as targeted (tailored) or generic (broad spectrum) attacks. Several types of security events can induce particular behaviours within a system's IT or OT components. It is harder to predict and protect against tailored malicious attacks. Furthermore, safety events may trigger certain behaviours within the system due to security events. However, there are also security events that may lead to safety events. Consequently, system behaviour during security events may be misinterpreted as safety events. It is necessary to understand other possible events within the system to determine the type of security event. For the purpose of this experiment, we presume an attacker is already inside the network. Based on information from the threat modelling tools, we selected three attacks for the experiment, each described below:

1a: A DoS attack on PLC inside the testbed network can reduce factory availability to test Elastics' capability to detect a malicious event by collecting data network data through Packetbeat or log files through Filebeat running on the EW.

1b: A change in OPC-UA sessions when the factory is in production indicates that a connection to the PLC has been initiated. Such an event can be malicious or malevolent, but from a detection perspective, it is crucial to collect if correlated with other data.

1c: A Slow DoS against the IoT Gateway (SlowITe). A SlowDos targets the MQTT protocol, using a minimum attack bandwidth and resources while executing the attack (Vaccari, Aiello, and Cambiaso 2020). A DoS attack on the IoT gateway or Fischertechnik cloud service through the MQTT protocol can impact the factory's availability.

Based on the nature of the identified threats, it is possible to predict the consequences of cybersecurity threats. The repercussions for a Denial-of-Service (DoS) attack could include disruption of normal operations and potentially debilitating effects. We also use the insights gained from threat modelling to establish a baseline for normal operations. This baseline can then be used to detect anomalies - any deviation from this baseline could be an indication of a cybersecurity threat. Also, identifying the consequences of these cybersecurity threats involved executing threat scenarios and observing the system's response to them.

6.2. Results

Threat scenarios 1a & 1c: A DoS attack launched from the IoT gateway towards the PLC using the hping3 command resulted in a disconnect between the engineering workstation and the PLC. The factory is producing a workpiece, and the attack did not appear to have affected the process. The behaviour of the engineering workstation resulted in a suspension and session timeout, which resulted in an unexpected exit from the TIA portal application. From an OT perspective, operator visuals from the PLC are not available. The following hping32 command is issued from the IoT gateway for this purpose:

hping3 IP−Address−PLC −S −P −U –flood.

Kibana logs indicate that the Filebeat-agent and Packetbeat-agent collected data during the attack, but Kibana cannot detect the DoS attack on the PLC. Using our approach, the Packetbeat agent should have collected network packets for the ICMP protocol. Network statistics have revealed a delay or timing issue for the network packets destined for the EW; however, we cannot detect or see this behaviour inside Kibana. Before the connection was suspended, we observed a significant increase in the PLC cycle time and CPU load. After reconnecting, the diagnostic buffer only reported a lost session.

Threat scenario 1b: As the training factory does not have a continuous ordering process, data generation occurs once a workpiece is ordered. Our baseline for anomaly detection failed to perform as anticipated over time since the factory had a more significant proportion of passive and idle periods than in active production. Data from the baseline found that when the testbed had been idle for some time, the expected number of OPC-UA sessions would be 2.27. In contrast, the number of OPC-UA sessions for the testbed in production was 6. Additional training data will be required to correct this issue.

7. Discussion

As previously stated, the experiment and results presented in this paper are a part of the larger project of setting up the testbed. One of the key findings of this study is that the integration of IT and OT systems presents significant challenges for cybersecurity management and monitoring. The challenges identified in this study include the differences in protocols, competence, and goals between IT and OT systems. These differences contribute to the challenge of integrating IT and OT. Additionally, the lack of cybersecurity expertise in OT cybersecurity, the rise in ransomware attacks, and the exposure of OT networks to the Internet contribute to the growing threat landscape of OT and Industry 4.0 (Chen 2018; CISA 2021; Radiflow 2021). This study focuses on using the Elastic Stack as a cybersecurity management and monitoring tool to address one of these challenges. This was done in an Industry 4.0 testbed environment. This study shows that the Elastic Stack has the potential to address IT and OT integration challenges. The Elastic Stack's detection and anomaly functionality helped detect a security incident, and the monitoring process helped identify an unstable TXT controller. However, challenges faced with OT data, baseline, and the need for customising protocols limited the team's ability to collect data.

As this study progressed, it became clear that its primary concern would be getting the testbed to function appropriately for monitoring. Our priority was to ensure that the testbed behaved as intended to detect anomalies, which is a crucial aspect of this study as it provides us with a clear indication of the testbed's capabilities at the time of the study. As a result of the DoS attack command, the Packetbeat-agent should have gathered enough information and network packets and found that there was a delay or timing issue. This behaviour is not detected or shown in Kibana logs. The reason is unknown at this stage; however, the attack affected the engineering workstation, which could lead to an inability to control the system. The methodologies employed suggest that it should be possible to identify and analyse multiple concurrent threats. The Elastic Stack, with its diverse data collection and visualisation tools, allows for real-time monitoring and analysis of several system parameters. This makes it possible to detect and study the effects of multiple threats at the same time. Furthermore, constructing multiple baselines for different threat scenarios would allow the detection and monitoring of multiple threats simultaneously. However, the results and experiences highlight some limitations of their current approach. Elastic's machine learning tool seems user-friendly at first glance. However, using machine learning in an anomaly detection scenario requires knowledge of the data and a basic understanding of machine learning. Pre-built detection rules are available only on the IT side to help define a baseline for such environments. It is necessary to develop and customise detection rules for OT environments. Out-of-the-box detection rules do not apply to OT environments.

Moreover, we recognised that effective cybersecurity measures require a deep understanding of system data and behaviour. Therefore, we also considered the importance of system data knowledge for effective cybersecurity management and detection. As a result of this study, relevant research questions related to cybersecurity anomaly detection in an IACS environment were addressed. Unique challenges have been identified in integrating IT and OT data. As a result of this study, we have provided insight into the use of the Elastic Stack in managing and detecting cybersecurity threats and demonstrating the importance of system data knowledge for implementing effective cybersecurity measures in Industry 4.0.

8. Conclusions and Furter Work Directions

An exploratory research approach is presented in this paper to investigate how IT and OT systems can be interconnected in the context of an Industry 4.0 testbed environment, focusing on cybersecurity management and monitoring.

This experiment is intended to provide information on Elastic Stack's potential to be used to manage and monitor complex IT/OT security systems. Despite identifying one of the attacks, Elastic SIEM does not seem mature enough to cope with the full complexity of an IT-OT environment. Several challenges, including unstable TXT controllers, OT data, baselines, and customised protocols, limited the amount of data available for analysis.

This study highlights the importance of a holistic cybersecurity management and monitoring approach in IACS. This is done by considering the unique challenges IT and OT integration poses. This study also emphasises the need for organisations to invest in cybersecurity measures and adopt best practices to protect their assets and systems from cyber threats.

8.1. Limitations

It is worth noting that this study focused on a specific Industry 4.0 testbed environment, and the findings may not be directly applicable to other contexts. Nevertheless, the study provides valuable insights into the challenges and potential cybersecurity management and monitoring solutions in Industry 4.0. As a result of this study, future research can explore cybersecurity management and monitoring using other tools and techniques. In addition, research can identify more effective ways to collect and analyse OT data to improve anomaly detection capabilities.

8.2. Acknowledgement

We thank our supervisor at Østfold University College, professor Øystein Haugen, for his support and constructive feedback throughout this project. We would also like to thank senior researchers John Eidar Simensen and Dr Bjørn Axel Gran, our internal supervisors at the Institute for Energy Technology. We appreciate their advice and the opportunity to invest in the factory testbed.

References

Arntzen, Siri, Zach Wilcox, Neil Lee, Catherine Hadfield, and Jen Rae. 2019. 'Testing Innovation in the Real World'. NESTA.

Bhageshpur, Kiran. 2019. 'Council Post: Data Is The New Oil - And That's A Good Thing'. *Forbes Technology Council* (blog). 15 November 2019. https://www.forbes.com/sites/forbestechcouncil/2019/11/15/data-is-the-new-oil-and-thats-a-good-thing/.

Chen, M. 2018. '3 Key Challenges to OT Cybersecurity and How to Overcome Them'. *Splunk Blogs* (blog). 2018. https://www.splunk.com/en_ us/blog/industries/3-key-challenges-to-ot-cybersecurity-and-how-to-overcomethem. html.

CISA. 2021. 'Significant Historical Cyber-Intrusion Campaigns Targeting ICS | CISA'. 20 July

2021. https://www.cisa.gov/news-events/alerts/2021/07/20/significant-historical-cyber-intrusion-campaigns-targeting-ics.

Cisco. 2022. 'Solutions - IT/OT Convergence in Critical Infrastructure and Industrials White Paper'. *Cisco*, 30 September 2022. https://www.cisco.com/c/en/us/solutions/collateral/industries/manufacturing/itot-convergence-wp.html.

Deloitte Insight. 2018. 'The Industry 4.0 Paradox'. Deloitte Development LLC. https://www2.deloitte.com/global/en/insights/focus/industry-4-0/challenges-on-path-to-digital-transformation.html.

Edgar, Thomas W., and David O. Manz. 2017a. *Research Methods for Cyber Security*. Cambridge, MA: Syngress, an imprint of Elsevier.

———. 2017b. 'Chapter 13 - Instrumentation'. In *Research Methods for Cyber Security*, edited by Thomas W. Edgar and David O. Manz, 321–44. Syngress. https://doi.org/10.1016/B978-0-12-805349-2.00013-3.

IEC. 2009. 'NEK IEC TS 62443-1-1:2009 Industrial Communication Networks'. TS 62443-1-1. ISA/IEC 62443 Security for Industrial Automation and Control Systems. Geneva, Switzerland: International Electrotechnical Commission. https://standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=396212.

Jørgensen, Per-Arne, and Stine Aurora Mikkelsplass. 'Creating a Testbed for Cyber Security Assessment of Industrial 4.0 Factory Infrastructure'. Preprint, submitted in 2023.

Knowles, William, Daniel Prince, David Hutchison, Jules Ferdinand Pagna Disso, and Kevin Jones. 2015. 'A Survey of Cyber Security Management in Industrial Control Systems'. *International Journal of Critical Infrastructure Protection* 9 (June): 52–80. https://doi.org/10.1016/j.ijcip.2015.02.002.

Kohnfelder, L., and P. Garg. 1999. 'The Threats To Our Products'. Microsoft.

Malatra, Dr. Apostolos, Christina Skouloudi, and Aggelos Koukounas. 2019. 'Industry 4.0 - Cybersecurity Challenges and Recommendations'. Attiki, Greece: European Union Agency for Network and Information Security (ENISA). https://www.enisa.europa.eu/publications/industry-4-0-cybersecurity-challenges-and-recommendations.

Microsoft. 2022. 'Microsoft Threat Modeling Tool Overview - Azure'. 25 August 2022. https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool.

MITRE Corporation. n.d. 'MITRE ATT&CK®'. Accessed 30 April 2023. https://attack.mitre.org/.

Munirathinam, Sathyan. 2020. 'Chapter Six - Industry 4.0: Industrial Internet of Things (IIOT)'. In *Advances in Computers*, edited by Pethuru Raj and Preetha Evangeline, 117:129–64. Elsevier. https://doi.org/10.1016/bs.adcom.2019.10.010.

NIST. n.d.' Baseline - Glossary | CSRC'. In *Computer Security Resource Center*. NIST Computer Security Resource Center. NIST. Accessed 10 August 2021. https://csrc.nist.gov/glossary/term/baseline.

Pereira, T., L. Barreto, and A. Amaral. 2017. 'Network and Information Security Challenges within Industry 4.0 Paradigm'. *Procedia Manufacturing* 13: 1253–60. https://doi.org/10.1016/j.promfg.2017.09.047.

Radiflow. 2021. 'OT Cyber Security: What Are the Common Challenges?' *Radiflow* (blog). 26 April 2021. https://www.radiflow.com/blog/ot-cyber-security-what-are-the-common-challenges/.

Smit, Jan, Stephan Kreutzer, Carolin Moeller, and Malin Carlberg. 2016. 'Industry 4.0 Analytical Study'. Study PE 570.007. European Union: Policy Department A: Economic and Scientific Policy. https://www.europarl.europa.eu/RegData/etudes/STUD/2016/570007/IPOL_STU(2016)570007_EN.pdf.

Vaccari, Ivan, Maurizio Aiello, and Enrico Cambiaso. 2020. 'SlowITe, a Novel Denial of Service Attack Affecting MQTT'. *Sensors* 20 (10): 2932. https://doi.org/10.3390/s20102932.

Yu, Xingjie, and Huaqun Guo. 2019. 'A Survey on IIoT Security'. In *2019 IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS)*, 1–5. https://doi.org/10.1109/VTS-APWCS.2019.8851679.

[i] Elastic Stack: Elasticsearch, Kibana, Beats & Logstash | Elastic

[ii] Microsoft Threat Modeling Tool overview - Azure | Microsoft Learn

[iii] CAPEC - New to CAPEC? (mitre.org)

[iv] UaExpert "UA Reference Client" - Unified Automation (unified-automation.com)