Industry 4.0: An Evaluation of Industrial IoT Vulnerabilities and the Impact of Cyber-Attacks on the Manufacturing Industry

Marc Geggan
School of Design and Informatics
Abertay University
DUNDEE, DD1 1HG, UK

ABSTRACT

Context: The fourth industrial revolution, Industry 4.0, focuses heavily on automation, big data, interconnectivity, and cloud computing. A vastly increasing number of companies are now turning their plants and factories into 'smart factories' by utilizing Industrial Internet of Things (IIoT) devices and Cyber-Physical Systems (CPS). Connecting Operational Technology (OT) to the internet, although having greatly positive business impact such as smart analytics and remote monitoring, introduces new communication models and technologies, thus drastically widening the attack surface of modern industrial control systems (ICS) and cyber-physical systems.

Aim: This paper aims to evaluate the implementation of IoT devices that define 'smart factories' and critically analyse the attack surface of these new technologies, and the impact these threats will have on the manufacturing industry. Furthermore, this research will aid in the development of a proof-of-concept kit that will demonstrate the procedure and result of a cyber-attack against a misconfigured industrial programmable logic controller (PLC).

Method: Research will be conducted to establish the current IIoT technologies implemented within the manufacturing industry. A literature review of existing research will be critically analysed to evaluate the common vulnerabilities found with Industry IoT devices. Lastly, using development kits, a hardware device artifact will be created for live proof-of-concept demonstration of specific vulnerabilities discovered through research.

Results: The literature review and research carried out will be collated to produce a paper on the current cyber threats within Industry IoT**,** and an artefact that will be used to bring awareness of these vulnerabilities to the manufacturing industry.

Conclusion: This project will be used as an educational piece that demonstrates the importance of securing misconfigured devices and highlights current vulnerabilities within the manufacturing industry. The proof-of-concept hardware kit will be used to consult businesses on the importance of security implementation.

Keywords
Industry 4.0, IIoT, Smart Factories, Cyber-Physical Systems, Vulnerabilities, Programmable Logic Controller

1. INTRODUCTION

The modern world is at the brink of a fourth industrial revolution, dubbed Industry 4.0. Since the 1800's, we have witnessed three industrial revolutions. The first saw humans move away from manual labour, to utilizing mechanised steam engines and waterpower. The second introduced electricity and saw the rise of production lines and mass production. The third revolution introduced computing technology, programmable logic controllers, digitization, and automation. Each revolution introducing greater and more efficient technologies than the last.

The fourth industrial revolution combines traditional industrial manufacturing with advanced technologies, such as large-scale machine-to-machine communication, industrial IoT devices, and cyber-physical systems (Georgios et al, 2019). The convergence of industrial operational technology and information technology, and the advances in IIoT capabilities, allow physical assets to communicate live analytical data over the internet to other devices. Thus, evolving automated 'smart factories,' and blurring the lines between physical assets and digital processes.

Although Industry 4.0 brings promising innovation to the manufacturing industry, the cyber-security threat landscape has not yet fully been realized. As advanced devices are connected and physical infrastructure is adapted, a new and more complex attack surface is created (Creese, 2020). As this is a new and developing area, there is a lack of research and understanding of the vulnerabilities that will arise from internet connected assets and it is vital that academic and professional research is carried out to better inform the industry. The overall implementation and success of Industry 4.0 and IIoT technology will be heavily contingent on how businesses, leaders, and managers handle the cyber-security issues (Sony and Naik, 2019).

This paper aims to evaluate the implementation of IoT devices that define 'smart factories' and critically analyse the attack surface of these new technologies, and the impact these threats will have on the manufacturing industry. Furthermore, this research will aid in the development of a proof-of-concept kit that will demonstrate the procedure and result of a cyber-attack against a misconfigured industrial programmable logic controller (PLC). This aim can be deconstructed into four research questions:

1. Does the implementation of Industrial IoT devices and IT/OT convergence generate more complex vulnerabilities?
2. To what extent can an OT network be compromised through a misconfigured Programmable Logic Controller?
3. What impact would a cyber-attack have on the Industry 4.0 'smart factory' supply chain?
4. What current mitigations are available to protect industrial manufacturing companies from cyber-attacks?

This dissertation will be in partnership with Mazars UK – an international audit, tax, and advisory firm that wishes to use this project for employee training, client consulting, and further industry research.

2. BACKGROUND

2.1 Cyber Physical Systems Architecture

The convergence of traditional IT and Operational Technology (OT) allows the manufacturing industry to improve efficiency and speed of production to compete with today's market demand. The interconnection of these devices has been made possible with the introduction of Cyber-Physical Systems. These new technologies are defined as distributed systems that converge physical assets and digital processes through the means of networks and computing infrastructure (Pivoto et al., 2021).

To recognize the threat landscape and vulnerabilities of Industry 4.0 technologies, it is imperative that professionals, businesses, and academics have a strong understanding of the new architecture that will be deployed. Although there have been multiple proposed structures, a paper titled 'A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems' (Lee et al., 2015) has defined a popular architecture labelled the 'CPS 5C level architecture'. Below in *Figure 1* the paper includes a graphical image of the proposed 5C architecture implementation of a CPS, and in *Figure 2*, a more detailed application associated to each level of the 5C architecture.

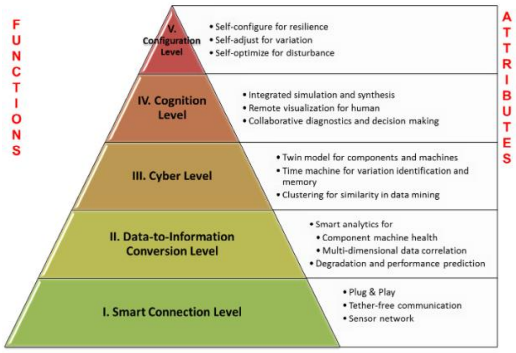

Figure 1 – 5C architecture for implementation of Cyber-Physical System. (adapted from Lee et al., 2015).

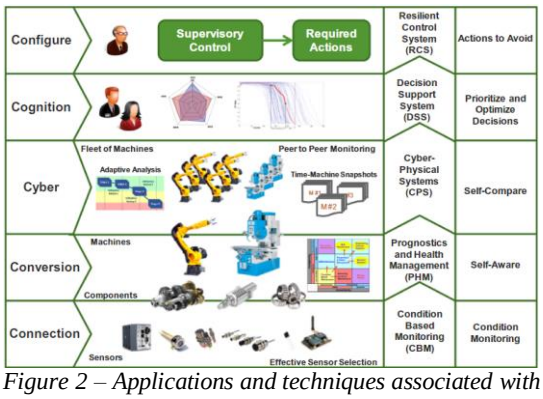

Figure 2 – Applications and techniques associated with each level of the 5C architecture. (adapted from Lee et al., 2015).

2.2 Vulnerabilities in CPS

In a paper titled 'Cyber-physical systems security: Limitations, issues, and future trends' (Yaacoub et al., 2020), the authors provide research of CPS vulnerabilities, threats, and attacks. The paper explains the major issues that the technology comprising cyber-physical systems have. Firstly, they were not built with secure by design methods. This in turn means that connecting previously unsecure devices to the internet has widened the attack surface that can be leveraged by threat actors. CPS systems are almost always comprised of multi-vendor third-party components. Many systems use outdated legacy technology that no longer receive security updates from their manufacturers, thus enabling attackers to use publicly available exploits to gain unauthorised access to networks. Other vulnerabilities arise from the use of standard protocols that lack basic security measures, such as encryption and authentication. As this is a new and evolving industry, there is minimal awareness, research and education in the securing of these devices, meaning many internet facing systems are misconfigured.

Considering the afore mentioned issues within cyber-physical system technology, many common exploits and vulnerabilities can be applied by threat actors. Unsecure internet facing devices can be scanned for and through brute-force attacks, unauthorised access to systems can be gained. Unencrypted protocols and open wireless networks allow for packet sniffing, spoofing, relay, and man-in-the-middle (MITM) attacks. This would enable an attacker to modify packets being sent between ICSs, PLCs, and other OT, which could seriously affect production operations and equipment. Outdated legacy systems are still vulnerable to malicious software (malware). This software is used to infect CPS devices to steal data, manipulate processes, and in some cases demand ransom from businesses. Furthermore, the dependency on multiple third-party vendors introduces a much more complex attack surface to the industry. With security researchers constantly reporting new critical vulnerabilities, threat actors can use compromised third-party software to send malicious files in the form of repositories and updates to infect target CPSs, as seen in the Georgia Nuclear Power Plant shutdown of 2008.

From a cyber-security aspect, the convergence of IT and OT environments cannot be addressed by simply 'bolting on' intrusion detection systems and firewalls. Addressing the security of Industry 4.0 this way is counterintuitive and presents unclear outcomes. It is imperative that businesses build security into their cyber-physical system architecture through a layered approach, and not just as an afterthought (Peters., 2018).

2.3 Related work

A research paper by Team82, a Claroty research team, titled 'Evil PLC Attack: Weaponizing PLCs' (Sapir et al., 2022), has been released documenting a recently discovered method to essentially weaponize a programmable logic controller with the end goal of executing arbitrary code on an engineer's workstation.

Firstly, the paper explains how engineers interact with PLCs through various workstation software. Next, it goes into detail about the compiling of bytecode that is handled by the PLC, its programming code transformation, and upload/download procedures. Lastly, the paper introduces the method used to 'weaponize' PLCs and gain access to the engineer workstation. The method is as follows:

1. Attacker scans for internet-facing PLCs.
2. Attacker infects the PLC with malicious download procedure and causes malfunction.
3. Engineer workstation connects to PLC to address malfunction.
4. Malicious code uploaded to engineering workstation.

This method of attack was tested on multiple leading companies that produce ICS workstation software, and it was discovered that seven companies including Rockwell Automation and Emerson were vulnerable. Unlike previous PLC attacks such as the Stuxnet malware that effected PLC logic, this attack aims at using the PLC as a foothold and pivot point for attackers to gain deeper access to the OT network through vulnerable third-party software.

3. METHOD

3.1 Research

The first stage of this project will consist of a comprehensive literature review of papers related to the technological advances within the manufacturing industry, more specifically Industrial Control Systems (ICS), Cyber-Physical Systems (CPS) and the current state of Industrial IoT technology. Research will also be conducted to examine common vulnerabilities within Industrial IoT devices, potential ICS penetration testing methodologies such as infosecinstitutes methodology, and possible mitigations that can be implemented within industry.

The information collated on current IIoT technologies, vulnerabilities, and attack surfaces, and mitigations will be evaluated to establish the current state of cyber-security within the manufacturing industry. This information will be documented in the form of a dissertation paper with the aims of consulting businesses on the current threat landscape of Industry 4.0 IT/OT convergence.

Finally, research will be carried out on the most suitable devices to aid in the development of a proof-of-concept artefact. This will be in the form of a hardware kit and will be used to demonstrate cyber-physical system exploits and educate businesses on the importance of cyber resilience and threat mitigation.

3.2 Development

This section covers the practical aspect of the dissertation. The information collated from the research phase, more specifically into PLC vulnerabilities, will be used to design and develop a proof-of-concept hardware kit for vulnerability demonstration. The requirements for this design will be researched and analysed to ensure the project is feasible in terms of timeframe and skillset.

The developed kit will be based on a Programmable Logic Controller (PLC), an industrial controller that can be programmed to control manufacturing processes. Using information gathered from the research phase on common PLC vulnerabilities, a scenario will be created in which a PLC has been misconfigured. This will be developed into an interactive hardware kit with the purpose of demonstrating how a threat actor would gain access to an exposed network through the PLC. This practical side of the project will be utilized to bring awareness to the new vulnerabilities that rise from IT/OT convergence and cyber-physical systems within the new industry 4.0 smart factory.

3.3 Evaluation

A qualitive method will be used to critically evaluate the findings from the research stage to achieve four main aims: Firstly, to determine the current state of technologies used in the ‘smart factory’ landscape. Secondly, to document the vulnerabilities and attack-surface of these new converged technologies. Thirdly, to analyse the impact these often-ignored vulnerabilities may have on the manufacturing industry if exploited by threat actors and possible mitigations that may be implemented to prevent these attacks. Lastly, to bring awareness to the niche area of Industrial IoT security with the aim of improving the cyber-security of the manufacturing industry.

4. Summary

In summary, the ultimate outcome of this project is to provide a qualitive evaluation of the current threats that face Industry 4.0 businesses. A dissertation paper will document current technologies, vulnerabilities, and mitigations, and an artefact will be developed to demonstrate the importance of securing devices.

As this is a new and developing niche area, this dissertation work aims to highlight the particular importance of implementing secure devices, protocols, and practices, thus providing professionals and businesses a solid base of knowledge for which to inspire further research, discussion, and development.

5. REFERENCES

Creese, S., 2020. Foresight review of cyber security for the Industrial IoT 68. 1st ed. [eBook]. Available at: https://ocsiiot.web.ox.ac.uk/files/lrfforesightreviewofcybersecurityfortheiiotjuly2020pdf-0

Georgios, L., Kerstin, S., Theofylaktos, A., 2019. Internet of Things in the Context of Industry 4.0: An Overview. Available at: http://dspace.vsp.cz/handle/ijek/103

Lee, J., Bagheri, B., Kao, H.-A., 2015. A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems. Manufacturing Letters 3, 18–23. Available at: https://www.sciencedirect.com/science/article/pii/S221384631400025X?via%3Dihub

Peters, R., 2018. Securing the Industrial Internet of Things in OT Networks [WWW Document]. Fortinet Blog. Available at: https://www.fortinet.com/blog/industry-trends/securing-the-industrial-internet-of-things-in-ot-networks

Pivoto, D.G.S., de Almeida, L.F.F., da Rosa Righi, R., Rodrigues, J.J.P.C., Lugli, A.B., Alberti, A.M., 2021. Cyber-physical systems architectures for industrial internet of things applications in Industry 4.0: A literature review. Journal of Manufacturing Systems 58, 176–192. Available at: https://doi.org/10.1016/j.jmsy.2020.11.017

Sapir, M., Katz, U., Moshe, N., Brizinov, S., Preminger, A., 2022. EVIL PLC ATTACK: WEAPONIZING PLCS 60. Available at: https://claroty.com/team82/research/white-papers/evil-plc-attack-weaponizing-plcs

Sony, M., Naik, S.S., 2019. Ten Lessons for Managers While Implementing Industry 4.0. IEEE Engineering Management Review 47, 45–52. Available at: https://ieeexplore.ieee.org/document/8704884

Yaacoub, J.-P.A., Salman, O., Noura, H.N., Kaaniche, N., Chehab, A. and Malli, M. (2020). Cyber-physical systems security: Limitations, issues, and future trends. *Microprocessors and Microsystems*, 77, p.103201. doi:10.1016/j.micpro.2020.103201.