Journal of Transactions in Systems Engineering
https://journals.tultech.eu/index.php/jtse.
ISSN: 2806-2973
Volume 4, Issue 2
DOI: https://doi.org/10.15157/JTSE.2026.4.2.667-679
Received: 07.01.2026; Revised: 30.06.2026; Accepted: 03.08.2026

*Research Article*

# Vulnerability Assessment of Operational Technology Systems in Industry 4.0 Manufacturing Environments

**John Hughes, Carlene Campbell*, Simon Thomas**

Wales Institute of Science and Art, University of Wales Trinity Saint David, Swansea, UK

***carlene.campbell@uwtsd.ac.uk**

**Abstract**

The increasing convergence of Information Technology (IT) and Operational Technology (OT) under the Industry 4.0 paradigm has significantly expanded the cyberattack surface of industrial environments, making the manufacturing sector one of the most frequently targeted industries. This study investigates cybersecurity vulnerabilities in a brownfield OT environment that integrates legacy industrial assets with modern connected technologies. A vulnerability assessment was conducted using a grey-box testing methodology, which provides partial knowledge of the target infrastructure while accurately reflecting the security perspective of an internal assessment. Automated reconnaissance and vulnerability scanning were performed using tools available in the Kali Linux distribution, including Nmap, Nikto, and Wifite, to identify security weaknesses and potential attack paths across the OT network. The assessment revealed multiple vulnerabilities that could be exploited to compromise the confidentiality, integrity, and availability of industrial systems, highlighting the need for systematic security evaluation and risk-based remediation. Although individual vulnerability assessment tools have been widely studied, limited research has examined their integrated application in contemporary brownfield OT environments that combine legacy operational infrastructure with Industry 4.0 technologies. The principal contribution of this work is the adaptation and validation of an established vulnerability assessment methodology in a real-world industrial production environment. Additionally, the study demonstrates a transparent approach for quantifying cyber risk and prioritizing remediation actions, providing practical guidance for strengthening the cybersecurity posture of manufacturing organizations undergoing digital transformation.

**Keywords:** Operational Technology; Cybersecurity; Industry 4.0; Industrial Control Systems; Vulnerability Assessment; Penetration Testing.

## INTRODUCTION

Cybersecurity encompasses the technologies, processes, and organizational practices used to protect systems, networks, and data from cyber threats. Within operational technology (OT) environments, cybersecurity extends beyond conventional information systems to include industrial control systems (ICS), physical processes, and safety-critical operations that support essential manufacturing activities.

The convergence of information technology (IT) and OT, driven by the adoption of Industry 4.0 technologies, has significantly increased the cybersecurity risks faced by industrial organizations. Modern manufacturing environments increasingly rely on interconnected devices, Industrial Internet of Things (IIoT) platforms, cloud services, and remote access technologies, expanding the attack surface beyond the traditional factory boundary. Consequently, cyberattacks targeting OT systems can result in production downtime, safety incidents, financial losses, and reputational damage. Cybersecurity has therefore become a fundamental requirement for ensuring operational resilience and business continuity rather than merely an IT concern.

Despite the benefits of digital transformation, the manufacturing sector continues to face significant challenges in modernizing legacy infrastructure. Many industrial facilities operate brownfield environments where aging control systems must coexist with modern digital technologies. The integration of legacy assets with Industry 4.0 technologies has improved operational efficiency, productivity, product quality, and machine-to-machine communication while simultaneously introducing new cybersecurity vulnerabilities [1].

Historically, OT systems were deployed as isolated environments protected by physical air gaps. However, the convergence of IT and OT has transformed these isolated programmable logic controllers (PLCs), distributed control systems (DCSs), and supervisory control and data acquisition (SCADA) systems into highly interconnected cyber-physical networks. As a result, the traditional air gap has largely disappeared, exposing industrial control systems to many of the same cyber threats that affect conventional IT infrastructures [2].

## CYBERSECURITY AND ITS SIGNIFICANCE TO MODERN SOCIETY

With the growing reliance on technology, security in cyberspace has been a growing concern. The extensive deployment of devices and systems in cyberspace has resulted in an ever-expanding flow of data. According to the statistic provided by the International Telecommunication Union (ITU) the United Nation's agency for information and Communication Technology [3], in 2022 there are a total of 5.3 billion (66%) active users (out of the world's population) on the internet, representing an increase of 24% increase from 2019. Figure 1 illustrates the growth of global internet users over time from 2005 to 2022.

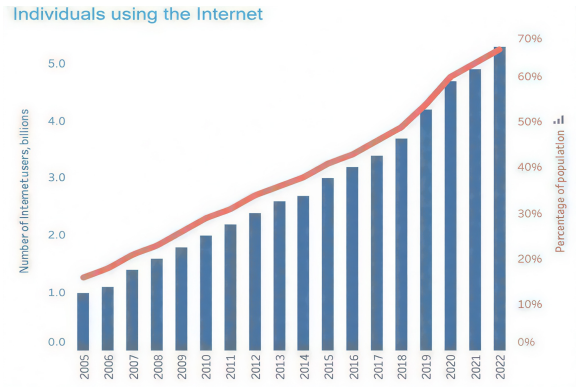


**Figure 1.** Internet Usage Statistics - Adapted from [3]

Though the data does not include the special situation caused by Covid related lockdowns in the period, the data shows that the number is increasing over time consistently since 2005, when there were only one billion users and only 15% of the world population. The burgeoning of global connectivity emphasizes the prominent necessity of global cybersecurity.

## *Cybersecurity in Operational Technology Environments*

In the journal 'The Importance of Cyber Security' written by the author Rajesh Goutam, demonstrates that the ever-increasing reliance on technology is directly proportional to the increased levels of vulnerability to cyber-crimes and as a result this has made cybercrime an issue for every individual, and business or government. The journal lists some types of cybercrime including DoS attacks that aim to overwhelm a computer target by sending it more traffic than it can handle, or a number of different types of malware, trojans, worms, or viruses that infect a computer target [4].

Goutam describes cybersecurity as the way and tools to protect system infrastructure, software and data from hackers, terrorist groups, cybercriminals and other unauthorised users accessing and tampering them through internet to consume the weaknesses in security [4].

While it can be accepted that the first part of Goutam's definition is more or less correct about the attack vectors, the second part about digital attacks through internet exposure ignores physical cyber-threats that can attack the system without going through a network, e.g. social engineering attacks.

The paper by authors in [5], entitled Social Engineering Attacks: A Survey, shows several examples of social engineering as weakening of the cybersecurity chain. Attacks resulting from human based social engineering such as pretexting, impersonation or tailgating allowing physical breach of a system, this poses a separate threat from exposure through the internet. Components of cybersecurity security such as firewalls, cryptography and anti-virus software are all susceptible to attack by this human element. In terms of social engineering, this human element is regarded as the weakest link in the cybersecurity chain [5].

According to the authors, even though social engineering can exist in many ways, they all have a common scheme for implementation which is carried out in four stages. The first stage is the reconnaissance of the target. Once sufficient information is collected, the second phase catches the target by creating a human liaison. The third phase runs the play/exploitation and the last phase exits the attack before getting detected [5].

## *Attack Vectors in Operational Technology*

The 2023 Threat Intelligence report by IBM identified that 3 of the top 10 most attacked industries in the last year utilized OT based systems, with manufacturing emerging as the most attacked sector. Vulnerability exploitation was the most prevalent attack vector, representing 47% of all attacks. Phishing attacks ranked second (40%), with removable media (7%), stolen credentials (3%) and brute force (3%) following [6].

Other organizations that used OT were also frequently targeted and energy organizations was ranked fourth in the top 10 attacked industries. Once again vulnerability exploits and Phishing were the leading attack vectors and DDoS, remote access Trojan (RAT) and business email compromise (BEC) were being heavily used. Moving onto the seventh industry in the top 10 attacked industries, the transport industry, server access attacks, 'credentials harvesting', and RATs were most frequently attacks [6].

## THE CONVERGENCE OF OT-IT SYSTEMS

In order to understand the effect of cyber threats to industry 4.0, the following research covers the emerging technologies that enabled the evolution of OT systems and its convergence with IT.

### *Traditional OT Systems*

Industrial Control Systems are part of the OT environment. As it relates to security, the network architecture of ICS is characterized by the Purdue reference model, known as the Purdue Enterprise Reference Architecture (PERA). As shown in the Figure 2, the model splits the network into 6 levels, level 0-5, with a hierarchical flow of data between them following the structure depicted in Microsoft documentation [7].

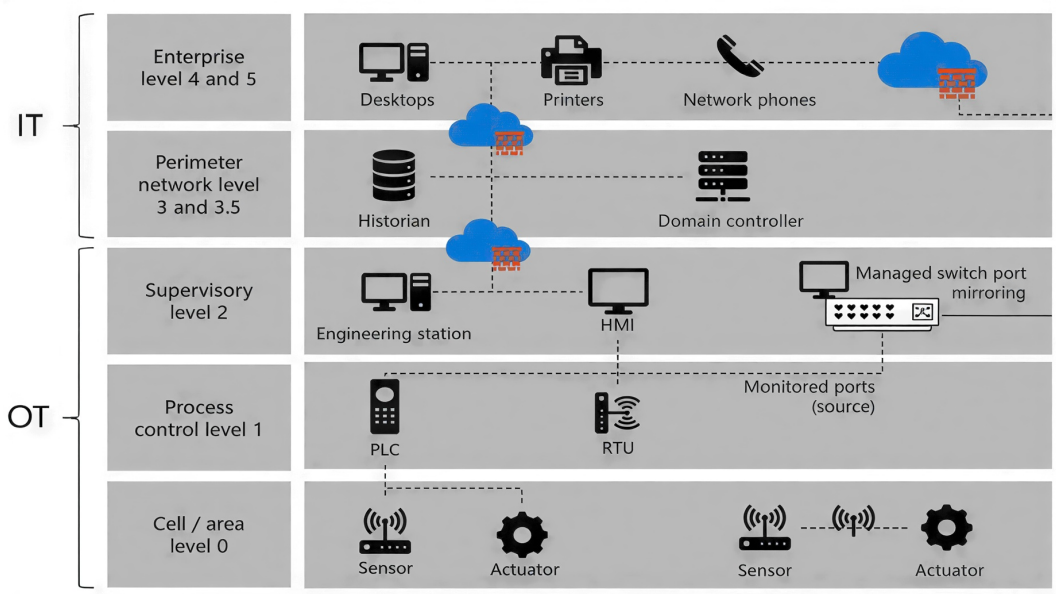


**Figure 2**. Purdue Reference Model - Adapted from [7]

Figure 2 refers to the Purdue reference model, illustrating how operational technology environments are often mapped onto a hierarchical framework. By illustrating the differences between the enterprise systems (top) and the industrial control levels (bottom), this model underpins the significance of network segmentation (curbing lateral movement) in minimising cyber risk. However, in reality, operational obstacles and older legacy systems frequently lead to compromise of this segmented architecture, therefore giving advantages to cyberattacks.

The following is used to describe the PERA taken from [8]:

- *Level 0* represents the physical nature of the system, the actuators, sensors, valves and motors involved in controlling mechanical systems.
- *Level 1* assimilates the physical and cyber nature of the plant through the industrial computers, for example Programmable Logic Controllers (PLC), Remote Terminal Units (RTU), specialized industrial computers used for optimizing the cyber network to process data from robotic devices.
- *Level 2* SCADA Supervisory Control and Data Acquisition (SCADA) overviews the industrial computers higher-level management and provides human interface over the processes of the plant in real time.
- *Level 3/3.5* is structured into two sub levels, the 3-level itself is comprised of domain and software controllers used for production control, the 3.5 is the manufacturing operations management which incorporates data historians for storing data to enable enterprise level analysis.
- *Level 4/5* is where the system integrates with the business with the enterprise itself, otherwise known as Business Planning and Logistics Domain

The Purdue model is an example of how to apply air-gap security controls to prevent cyber-attack on valuable OT equipment. This can be applied at any level of the hierarchy along with segmentation of the network and access controls [8]

## *Industrial Internet of Things*

The Industrial Internet of Things (IIoT) is often used to describe the use of IoT technology in industrial settings. Authors in [9] discusses a number of upgrades to OT enabled by IIoT. For instance, enhanced effectiveness and decision-making can be achieved using instantaneous performance evaluation of tools and machines. An example of which could be, detecting performance problems and correcting faults as soon as possible, thus pre-empting failure and minimising down time. Additionally, in [9] it has been explained how the most ethical of business models could be created by optimizing resources by using data to reduce energy or material waste.

Authors in [10] mention that additional computers can be placed near the data sources, to send the information to remote systems in the cloud in order to stabilize the IIoT scenario.

The industrial edge technology generated by the coming solution has forced the Purdue Reference Model to be questioned, whether data for a given hierarchical level mentioned in the PERA either can be sent to the cloud directly resulting in drastically threat to cyber security, see Figure 3.

Authors in [12] identified the various security weaknesses of IoT nodes such as edge devices, sensors and actuators and SCADA systems that oversee their operation, are susceptible to multiple forms of cyber-attack. The main problems are as follows:

- Wireless device encryption issues, can compromise data communications which can be intercepted and thus put the integrity of data at risk.

- Older devices that have been upgraded with sensors may find themselves obsolete in regards to security. This can lead to the inability for port security to be properly applied due to the use of the devices.
- Unpatched, known vulnerabilities can be present if the firmware isn't updated.
- Insecure default settings, possibly leading to easy-to-guess passwords and default users that might be vulnerable to brute force or other password related attacks.
- Services that are easy to compromise such as HTTP, TELNET and SSH.
- Human error that results in networks being exposed to malicious links & downloads and social engineering attacks that undermine the security of the network.

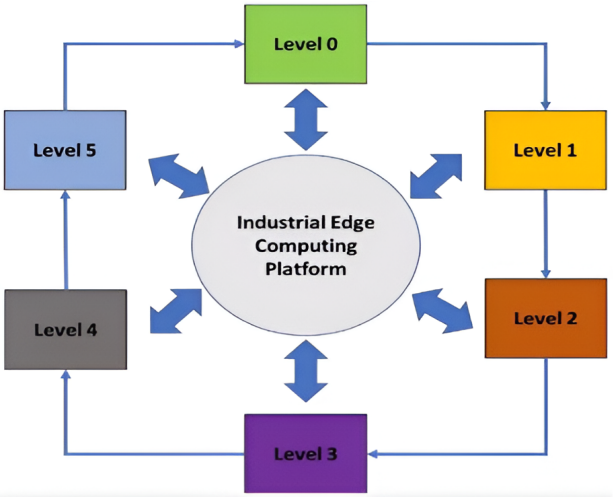


**Figure 3.** Industrial Edge Technology Data Flow - Adapted from [11]

## VULNERABILITY ASSESSMENT PROCESS

In contrast to existing literature that offers established procedures and tools for undertaking vulnerability assessment, these are more described as universal processes, suitable for use on both Information Technology (IT) as well as Operational Technology (OT), with less focus on real OT environments that have legacy IT systems as well as new Industry 4.0 capabilities. This study fills that gap by using existing vulnerability assessment procedures in a real OT environment and testing the findings on those vulnerabilities according to the context of industrial cybersecurity.

The work of authors in [3] propose a four-step process to vulnerability assessments.

- *Target Discovery* - the initial stage of the vulnerability assessment process creates an image of the target infrastructure by estimating a topology based on the assets discovered, resulting in improved decision making.
- *Scanning* - With an estimated image of the network infrastructure, system scanning can be refined to a target area.
- *Result Analysis* - This step analyses the results based on their impact & severity.

- *Reporting* – This documents the entire process, including an executive summary, results & findings, risk assessment & recommendations.

## VULNERABILITY ASSESSMENT TOOLS

The tools displayed below are those present on the version of Kali Linux distribution used for the experiment.

### *Wifite*

Wifite is a python script that simplifies and automates the process of auditing Wi-Fi security. The attack on Wi-Fi networks encrypted with WEP, WPA, and WPA2-PSK encryption keys. It is compatible with most wireless network adapters, Wifite automates WEP cracking, WPA handshake capturing, password brute-force guessing, and attacks on WPS networks.

### *Nmap/Zenmap*

In asset discovery, there are a number of completely automated utilities which can determine network topology. In Penetration Tester's Open-Source Toolkit, author Jeremy Faircloth described Nmap as being used in Asset Discovery with many different methods. The author notes that a ping sweep will find any asset that is listening for ICMP messages by sending out echo requests over a group of IP's within a subnet. Nmap then produces a list of hosts that are currently active to the user [2].

### *Nikto*

Nikto is an open-source application that enables the user to perform various tests to identify vulnerabilities. It is claimed by the developers that it has a database which can detect in excess of 1250 server versions and specific issues relating to 250 types of servers in addition to checking for outdated software/ plug-ins, application misconfigurations and default files and directories [14].

Wifite was chosen to discover wireless networks and automate the capture of the 802.11 wireless encryption standards WEP, WPA and WPA2. Zenmap was then chosen to map the network by locating hosts, services and operating systems and showing the network topology graphically. Nikto was then used to scan the services that had been discovered for insecure software versions and known vulnerabilities. This sequence of tools enabled each phase of the vulnerability assessment to integrate further information gathered in the previous phase.

## VULNERABILITY ASSESSMENT STAGES AND RESULTS

### *Approval*

Preparation is the essential stage in the design of the vulnerability assessment; it involves gaining the official endorsement of the target organization in order to access the correct tools that will be used during the vulnerability assessment and to determine the parameters with

which the vulnerability assessment will be conducted within. Once approval has been gained the process can proceed to the first stage.

Due to the sensitive nature of the network, access was limited to only the 172.21.0.0 network and only for non-destructive identification of vulnerabilities. No Security information was kept back from the networks administration, and all vulnerabilities were fed back to the customer in confidential business data.

## *Approach*

The physical network infrastructure that was used during grey-box conditions remained in the university robotics laboratory, and target information was supplied by the network administrator as:

- Target SSID: CP-S-UniversityofWales-5GHz
- Subnet mask: 255.255.192.0.
- Gateway address: 172.21.0.200

According to the literature review, there is a degree of variation in the steps taken in a vulnerability assessment, with differing variations on the process being implemented by various information security organisations. In converting what had been learned from the literature into the needs of a target Operating Technology environment, a structured assessment was performed based upon target identification, scanning, analysis of results and reporting, with each stage relying on the successful completion of the previous stage, providing a repeatable process for performing the assessment.

## *Process*

The procedure in figure 4 has been identified and implemented as follows to comply with the network condition:

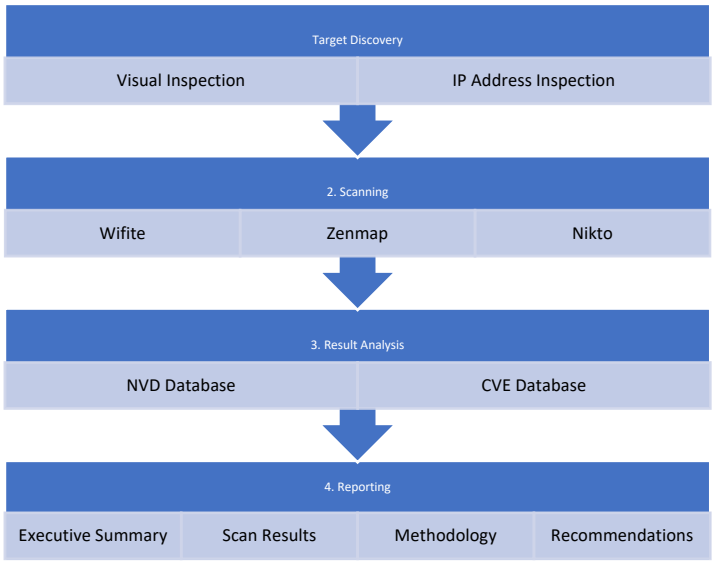


**Figure 4.** Vulnerability Assessment Process

***Target discovery*** - The following steps were performed:

- Physically investigate the infrastructure.
- Create an image of the network topology.
- Investigate the system information.

***Scanning*** - Investigated the SSID and Wireless security. Wifite used to identify several WLANs. Using an automated process of copying packets and cracking the 802.11 wireless encryptions standards such as WEP, WPA and WPA2. As shown in Figure 5 the wireless adapter will discover a large number of WLANs in the UWTSD campus building and outputs the list numerically, which includes the target SSID CP-S-UniversityofWales-5GHz.

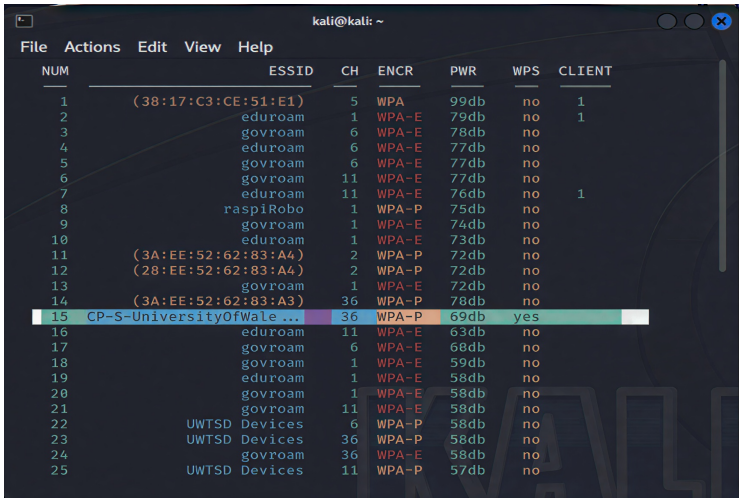


**Figure 5.** Wifite Target Selection

The Zenmap network scanner was chosen in order to locate open ports, services & operating systems using an intuitive, visual interface, see Figure 6. This tool was used primarily due to the visual depiction of data, and because scanning options could be selected from drop down menus that would provide the appropriate Nmap command line. The information acquired using Zenmap was then fed into the Nikto scanner to probe the open ports for outdated versions of programs and incorrectly configured options, thus adding another layer of detail to the vulnerability scan

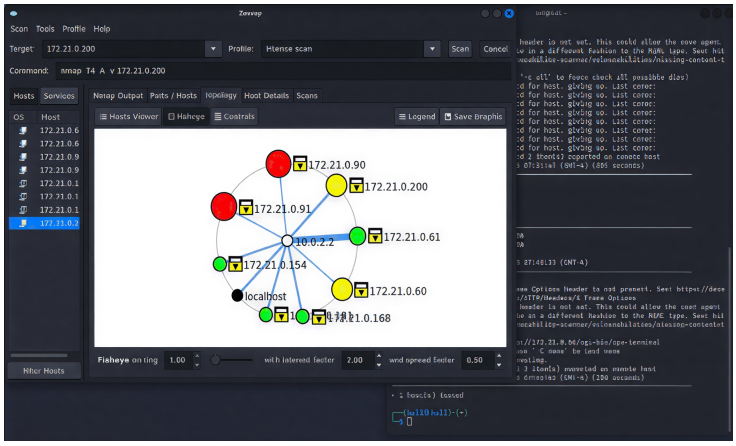


**Figure 6.** Zenmap Router Topology

Sequentially, the data gathered from the Zenmap scan, illustrated in figure 7 was used in conjunction with the Nikto http probe, to look for open ports with known vulnerabilities such as misconfiguration or insecure versions. This was done to provide a higher level of sophistication to the vulnerability identification process.

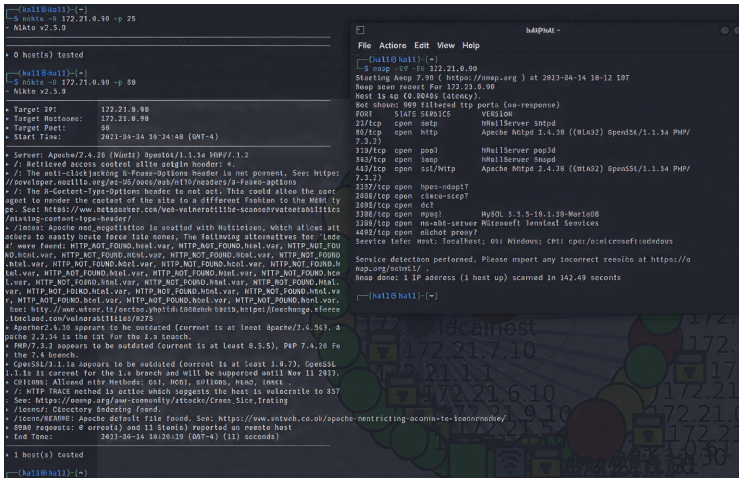

**Figure 7.** Nikto Port Scanning Results

***Result Analysis*** – Severity of the vulnerabilities discovered was assessed using the NVD (National Vulnerability Database) along with the CVE (Common Vulnerability Exposure) database.

The consolidated vulnerabilities were evaluated by means of the Common Vulnerability Scoring System (CVSS). Three of the found vulnerabilities had a CVSS value in the High Severity range, these were weak password security, wireless WPA2 encryption and the MyHelpDesk cross-site scripting vulnerability. Four vulnerabilities fell into the Common Vulnerability Scoring System Medium Severity range with a single High Severity finding. Despite the individual vulnerabilities being of generally moderate severity the total effect added multiple factors to an already vulnerable operational technology platform.

The most common vulnerabilities were identified from the result established from the scan, as shown in Figure 8. The result identifies the percentage occurrences of the vulnerabilities, where Cross Site Scripting was the highest. Password encryption and mis configuration were also one of the most common vulnerabilities.

The analysis showed that the highest percentage of identified issues were web application vulnerabilities, with Cross Site Scripting (XSS) being the most prevalent type. The two following highest percentages of detected issues were related to exploitable passwords and weak encryption algorithms; this suggests that the issue of authentication & access control is a significant security consideration for converged OT environments. The final three category of security issues (such as legacy software, exposed services and default configurations) were however primarily with respect to legacy equipment being used in combination with Industry 4.0 technologies.

Severity analysis was conducted using the Common Vulnerability Scoring System (CVSS) where published scores could be retrieved from the National Vulnerability Database. Three vulnerabilities; Weak wireless authentication, WPA2 encryption and the MyHelpDesk Cross Site Scripting vulnerability were therefore shown to be of High severity on the CVSS scale (≥7.5). Of the other discovered vulnerabilities, the majority were of a medium severity while there was only one Low severity issue. This suggests that the combined effect of the multiple Medium to Low vulnerabilities would considerably increase the attack surface of the network, even if one individual device wasn't a critical weakness.

The evidence gathered during this assessment aligns well with the literature study conducted earlier in this report, finding exploitation of known vulnerabilities as the most popular attack method used on manufacturing organisations. The discovered presence of outdated software and unsecure configuration and web application deficiencies reinforce earlier research demonstrating that legacy systems and poor patching practices remain prominent Cyber security concerns for Operational Technology systems.

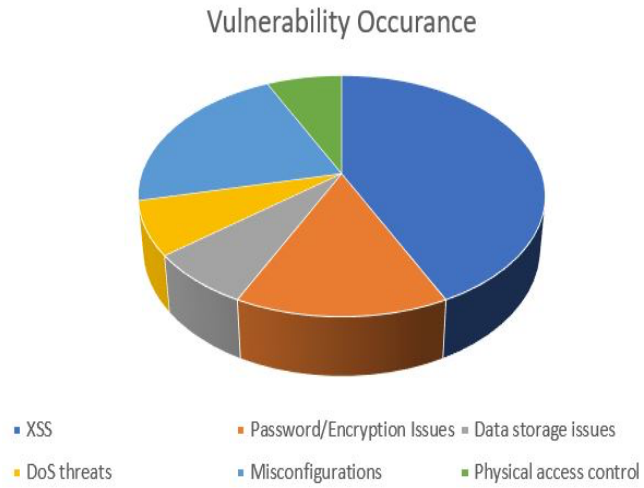


**Figure 8.** Most Common Vulnerabilities

***Reporting*** – The final report of vulnerability assessment. It involved details of software used, steps taken & results of the scans. It also provides an executive summary which offers an overview of the assessment's objective, results & recommendations.

The findings suggest a high incidence of vulnerabilities within legacy platforms, systems running outdated versions and with known exposure. Several of those classified as compromising the system was noted, with these vulnerabilities appearing on a large number of hosts, indicating the increased risk to security that these threats pose through the incremented risk of compromised systems in IT/OT convergence. The recurrence of configuration related deficiencies, unsupported software and web application flaws increases the likelihood of initial compromise and lateral Movement through connected Industrial Network architectures.

This seems to be in line with the typical challenges faced by OT security items, with availability and longevity generally being far more important than green security updates.

These issues are, therefore, evidence of some of the systemic vulnerabilities present in industrial environments, especially when coupled with the excessive connectivity now inherent in many of these systems. The compromise of such security flaws could allow an attacker to access, interfere with or even bring down the system services. This underpins the importance of a risk-based approach to vulnerability management within an OT context rather than a straight implementation of an IT-centric model.

The research shows that vulnerabilities of OT environments are typically not just a technical matter but are generally embedded in architectural design, legacy dependency, and operational focus. The integration of digital is to enhance operational efficiency but at the same time the pathways for cyber-attack are created and need to be addressed by coordinated technical, organisational and people controls. This reaffirms the need for cybersecurity strategy that are specifically designed for OT environments as opposed to traditional IT oriented security technology.

## CONCLUSION

This paper investigated cybersecurity vulnerabilities in a brownfield operational technology (OT) environment undergoing digital transformation through Industry 4.0 technologies. Using a grey-box vulnerability assessment methodology and automated security tools available in the Kali Linux platform, the study identified security weaknesses, evaluated potential attack paths, and demonstrated how vulnerabilities can be systematically prioritized for remediation. The findings confirm that although the convergence of information technology (IT) and OT improves operational efficiency and connectivity, it also significantly expands the attack surface of industrial environments, particularly where legacy systems remain in operation.

From a research perspective, this work demonstrates the practical applicability of an integrated vulnerability assessment methodology for evaluating cybersecurity risks in real-world industrial environments. Unlike studies that focus on individual security tools, this research illustrates how multiple automated assessment tools can be combined to provide a comprehensive evaluation of OT network security. From an industrial perspective, the results emphasize the importance of adopting a holistic cybersecurity strategy that incorporates network segmentation, continuous monitoring, vulnerability management, secure remote access, and personnel awareness to improve cyber resilience.

The proposed methodology provides a practical framework that manufacturing organizations can adopt to identify vulnerabilities, quantify cyber risk, and prioritize remediation activities during Industry 4.0 implementation. Future research should investigate predictive threat detection using artificial intelligence and machine learning, continuous vulnerability assessment for industrial control systems, and automated risk prioritization techniques tailored to the operational constraints of critical OT environments.

## ACKNOWLEDGMENT

This research was supported by the University of Wales Trinity St David, The School of Applied Computing and the department of Innovation and Engagement.

## CONFLICT OF INTERESTS

The authors confirm that there is no conflict of interest associated with this publication.

## REFERENCES

1. Nardo, M., Forino, D., Murino, T. The Evolution of Man–Machine Interaction: The Role of Human in Industry 4.0 Paradigm. *Prod. Manuf. Res.* **2020**, *8*(1), 20–34.
2. Murray, G., Johnstone, M.N., Valli, C. The Convergence of IT and OT in Critical Infrastructure. *In Proceedings of the Australian Information Security Management Conference*; **2017**, pp. 149-155.
3. International Telecommunication Union (ITU). *Statistics*. Available from https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx (Accessed date 11 january 2026).
4. Goutam, R.K. Importance of Cyber Security. *Int. J. Comput. Appl.* **2015**, *111*(7), 14-17.
5. Salahdine, F., Kaabouch, N. Social Engineering Attacks: A Survey. *Future Internet* **2019**, *11*(4), 89.
6. IBM. *IBM Security X-Force Threat Intelligence Index 2023*. Available from https://www.ibm.com/reports/threat-intelligence (Accessed date 11 january 2026).
7. Microsoft. *Understand Your OT Network Architecture—Microsoft Defender for IoT*. Available from https://learn.microsoft.com/en-us/azure/defender-for-iot/organizations/best-practices/understand-network-architecture (Accessed date 11 january 2026).
8. Boyes, H., Hallaq, B., Cunningham, J., Watson, T. The Industrial Internet of Things (IIoT): An Analysis Framework. *Comput. Ind.* **2018**, *101*, 1–12.
9. Ying, Z., et al. An Overview of Computational Models for Industrial Internet of Things To Enhance Usability. *Complexity* **2021**, *2021*, 5554685.
10. Li, Z., Fei, F., Zhang, G. Edge-to-Cloud IIoT for Condition Monitoring in Manufacturing Systems with Ubiquitous Smart Sensors. *Sensors* **2022**, *22*(15), 5901.
11. Greenfield, D. Is the Purdue Model Still Relevant? *Automation World*, May 12, 2020. Available from https://www.automationworld.com/factory/iiot/article/21132891/is-the-purdue-model-still-relevant (Accessed date 11 january 2026).
12. Jiang, X., Lora, M., Chattopadhyay, S. An Experimental Analysis of Security Vulnerabilities in Industrial IoT Devices. *ACM Trans. Internet Technol.* **2020**, *20*(2), 1–24.
13. Shah, S., Mehtre, B. M. An Overview of Vulnerability Assessment and Penetration Testing Techniques. *J. Comput. Virol. Hacking Tech.* **2015**, *11*(1), 27–49.
14. CIRT.net. *Nikto2*. Available from https://cirt.net/Nikto2 (Accessed date 11 january 2026).