7th European Conference on Industrial Engineering and Operations Management
Augsburg, Germany, July 16-18, 2024
Publisher: IEOM Society International, USA DOI: 10.46254/EU07.20240093
Published: July 16, 2024

A Systematic Review of the Implementation of IT and OT Cybersecurity Standards in an IT/OT Converged Environment

Thobeka Sishuba
Ph.D. student in Quality & Operations Management
University of Johannesburg, South Africa

Dr Emmanuel Innocents Edoun and Professor Anup Pradhan
Quality & Operations Management
Engineering and the Built Environment
University of Johannesburg, South Africa
anupp@uj.ac.za ; eiedoun@uj.ac.za

Abstract

Digital transformation stems from Industry 4.0 and has introduced innovation across various industries and businesses. Digital transformation requires the integration of Operational Technology (OT) and Information Technology (IT) company departments (Hicking et al. 2021). IT/OT integration results include increased productivity, reduced waste, decreased labour and energy expenditures, and improved maintenance. Traditionally, IT is about data creation, storage, and security within an organization, while OT is about the physical world processes, such as overseeing productivity, personnel, and machinery. With the integration of IT and OT, the boundaries between the two have become blurred. (Kuppusammy and Mariappan 2021). However, because of this connectivity, the once-isolated systems are now vulnerable to various new threats (Cook et al. 2017). Individuals and industries are adapting to internet connectivity for nearly all devices. Recent forecasts indicate that 70 billion devices will be connected to the Internet by 2025. OT devices and systems utilized in critical infrastructures, such as energy distribution, water management, nuclear facilities, and manufacturing, also embrace this connectivity trend (Alrumaih et al. 2023). An increase in IT/OT integration has led to a rise in cybercrimes in OT systems. Cybersecurity standards are created to assist organisations in meeting cybersecurity goals and preventing cybercrimes (Taherdoost 2022). With the integration of IT and OT, organisations need to protect both IT and OT networks by implementing the correct standards. This paper will highlight the security requirements for IT and OT and the most appropriate standards to use for an IT/OT converged environment

Keywords
Operational Technology (OT), Information Technology (IT), Purdue Model, Cyber Security, Standards.

1. Introduction
OT oversees and regulates physical processes, equipment, and industrial operations. It includes hardware and software technologies utilized for monitoring and controlling machinery in real-time. OT is dedicated to the practical management and control of physical assets (Bwatiramba 2023). OT networks and systems include Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) (Murray et al. 2017). OT systems are found in various industrial sectors such as manufacturing, energy, mining, water, pharmaceutical, and transportation. Examples of OT tasks include regulating temperature in power plants, controlling robots on manufacturing lines, and managing controllers at mining sites (Bwatiramba 2023). IT is the resources utilized by a firm for data processing and management, including hardware, Software, communications (voice, data, video), and associated personnel. Information Technology includes the capabilities of computers, software applications, and telecommunications (Victoria 2020). Hiroo Kanamaru (2021) came up with Table 1 to differentiate IT and OT characteristics.

Table 1. Characteristics of IT VS OT (Kanamaru 2021)

IT	Feature	OT
Support Organisation's personnel, implementation, and support of processes provide information.	Main function	Controlling and monitoring of physical processes and equipment
Network and information security	Focus	Continuous and precise production, including the safety of personnel
personal computers, printers, web interfaces, apps, emails, servers and ethernet network	Systems Examples	Industrial Control Systems, which include SCADA, PLC, HIMs, and industrial networks, including other communication protocols such as Modbus, Profibus, etc
Phones, tablets, etc	Example of Devices	Sensors, robots, analysers, etc
High bandwidth, rebooting allowed, redundancy not required as backup retrieval is used.	Performance Requirements	Low bandwidth, production interruptions not allowed, and redundancy is required.

1.1 Objectives

Although different industries experience significant impacts on the integration of IT and OT, this also comes with a major cyber security challenge due to the integration of OT networks with the IT company network and the Internet. These cyber security challenges impose different threats on the OT network (Berardi et al. 2023). OT data and its related control mechanisms are at an increased risk of cyber-attacks. Integrating IT and OT has led to systems previously closed off being interconnected and susceptible to all the risks that have long existed in the IT realm. As a result of this exposure, individuals or groups seeking to exploit these newfound vulnerabilities have emerged and are attacking the OT network (Murray et al. 2017). It is critical for organizations to reduce the risk associated with cyber-attacks by implementing the correct security standards based on risk assessment on the organisation. This study aims to allocate the best cyber security requirement for an IT/OT organisation based on risk assessments.

2. Literature Review

Joe Wiess (2024) states that security can be compared to a three-legged stool comprising physical, IT, and OT security. While the law addresses physical security, IT security primarily deals with standard commercial hardware and Software and internet connections managed by IT and military professionals. OT security, the third leg, lacks understanding and expertise and is often deemed non-critical. Professionals in this field typically come from the IT security domain with limited knowledge of ICSs or ICS experts who focus on system operation rather than security (Wiess 2024). IT security focuses on protecting information assets to prevent leaks, as restoring reputation and trust is challenging once information is compromised. Operational Technology (OT) security aims to avoid personal harm, equipment damage, operational disruptions, and service outages. Therefore, security risk assessments for OT should prioritize safety and IT security measures to reduce the likelihood of incidents (Kanamaru 2021). Weis (2024) elaborates on this topic by stating that OT security protects physical processes from unintentional incidents and deliberate attacks. Technologically, OT security differs from IT security due to the unique devices and diverse communication protocols (Weiss 2024). Apart from Ethernet and IP protocols, which are common to IT, OT also has other industrial protocols that pose challenges to consistent security implementation. Common Industrial Protocol (CIP), Modbus, MTConnect, DNP3, Profinet, and EtherCAT are more susceptible to cyber-attacks than IP-based protocols. The fundamental difference between IT and OT security management is the different industrial processes and operational priorities. OT operational challenges differ from IT operational challenges and, therefore, have different attackers targeting them (Maleh 2021). On the other hand, one cannot mention IT security and OT security without mentioning cyber security. Cybersecurity extends beyond safeguarding information; it includes OT and IT security to protect digital assets (Uddin 2023).
The Purdue model offers a standard framework for defining OT and IT levels in an organisation with a control system. It features featuring six levels of hierarchy. Levels 4 and 5 comprise the IT level, and Levels 0 to 3 are the OT level. Level 5 handles corporate networks, Level 4 oversees planning and logistics, Level 3 manages daily operations, Level 2 supervises equipment, Level 1 controls devices, and Level 0 consists of sensors and devices. The Purdue model is essential in understanding the layered approach for IT and OT security (Cook et al. 2016).

When it comes to addressing security in the OT environment, the priorities of OT (Safety and continuous production) limit security measures that are put in place. OT environments often include unpatched and outdated systems, limited visibility, and various other challenges (Maleh 2021). On the other hand, the main priority for IT is data protection. This has led to developing various tools, practices, and procedures to protect IT systems from cyber threats. Unlike IT security, minimal effort or changes have been made in the OT security domain, as

implementing security measures could require an interruption in production. The potential loss of production and revenue and the expenses associated with designing and implementing necessary security solutions have led to OT systems significantly trailing behind IT systems in addressing security threats (Murray et al. 2017). However, Sekonya and Sithunga (2023) also noted that IT/OT integration has heightened the susceptibility of OT to cyberattacks. Given these systems' critical role in managing infrastructure, such attacks can lead to significant downtime in critical infrastructure, placing a risk on the nation's welfare and economy (Sekonya and Sithunga,2023). OT security is becoming a priority due to the potential impact of cyber-attacks on the OT system, and avoiding the implementation of security measures poses a significant risk for continuous production.

Numerous case studies have shown that various types of attacks can target OT systems. Many of these attacks include the introduction of malware or ransomware into the OT system, exploiting legacy networks and systems, and capitalizing on their weaknesses. Typically, the malware enters the OT network through methods such as phishing emails, insecure internet connections, or USB drives (Alladi et al. 2020).

When addressing threats in the OT network, directly applying IT security practices to the OT network or system can result in availability and timing complications. Adding resources, computing power, or functionalities to meet IT security standards in the OT network may only sometimes be feasible (Hollere et al. 2023). As OT networks integrate with IT networks, conventional IT security measures like firewalls, penetration tests, and antivirus software prove inadequate or impractical to implement due to their potential adverse effects on system availability. Any delay in the OT network can directly affect the timely operation of the physical system, unlike in IT, where a delay only affects performance (Taylor and Sharid 2017).

OT operations face challenges when implementing IT security practices into the OT network. Unlike IT networks, OT networks are not uniform, have diverse devices, have limited encryption, and are air-gapped, which limits cybersecurity implementation. Some OT systems cannot be offline, raising safety concerns (Pulsipher et al. 2024).

Maleh (2021) listed the below vulnerabilities for the OT network due to their different proprieties with the IT network:

1. Outdated software needs robust authentication and data integrity features.
2. Simple or default passwords.
3. Lack of encryption due to legacy products needing more encryption capabilities.
4. Insecure remote access methods provide entry points for attackers.

(Maleh 2021)

Standards are optional directives or specifications for organisations to improve efficiency or obtain objectives (Agarwal 2022). International organizations play a crucial role in their development. Standards, as defined by www.standards.org.au, cyber security standards ensure the safety, consistency, and reliability of products, services, and systems (Taherdoost 2022).

Frameworks resemble standards but are more general and may include a series of standards, guidelines, and resources that organizations can utilize to obtain specific objectives and goals. A simple example is that a cybersecurity framework may include different standards aimed at safeguarding networks and data, along with tools and guidelines for implementing these standards (Agarwal 2022).

The Table 2 below lists the differences between cybersecurity standards and frameworks.

Table 2. The difference between standards and Frameworks (Taherdoost,2022)

Standards	Framework
Standards consist of documents that detail procedures, specifications, and guidelines.	Frameworks are general and not specific; they guide the selection of the correct standards.
Standards are guidelines used to meet regulations.	Frameworks determine the basics of meeting regulations and require standards to define steps to meet objectives.
Standards can be combined with other standards to strengthen regulatory requirements.	Frameworks are used to determine which standards can be used and the right combination of standards.
Some standards are open for all industries, and some are for specific industries.	Frameworks are for meeting Governance and risk management objectives. They are not necessarily industry-based.

Regarding the implementation of standards, IT security standards implemented in the OT network may disturb operations and endanger individuals. Failing to understand the OT environment and the best security measures for OT can lead to conflicts among administrators, resulting in compromised security (Pulsipher et al. 2024). Network security organizations have crafted cybersecurity policies for IT and OT, with limited input from engineering entities responsible for the hardware and control systems (Weiss 2024).

Standards and regulations are essential in ensuring the security of Industrial Control Systems (ICSs) and critical infrastructure (Maesschalck 2022). International cybersecurity standards offer tools, policies, and risk management approaches to reduce cyber security risk and protect users and organizations from cyber-attacks. The most popular standards include the ISO 27000 as well as the IEC62443. The ISO/IEC 27000 series focuses on IT security. The ISA/IEC 62443 standards address security vulnerabilities in industrial automation and control systems (IACSs) or OT networks (IAIANI et al., 2021). Djebbar and Nordstrom (2023) conducted a comparative analysis of standards and found that cybersecurity includes diverse and generic standards. They compared ISA/IEC 62443-3-3, ISO/IEC 27001, and ETSI EN 303 645 standards and found overlaps among these standards. ISO/IEC 27001 notably covers ETSI provisions and partially ISA/IEC 62443-3-3, with ETSI focusing on organization and technology and ISA/IEC 62443 on physical and technology security. ISO/IEC 27001 uniquely emphasizes cyber resilience (Djebbar and Nordstrom 2023). Dihiran et al. (2021) findings also agree with Djebbar and Nordstrrom (2023) by stating that different sectors implement different standards and unique cybersecurity models through a combination of security standards (Dihiran et al. 2021). Taherdoost, 2024 also states that selecting a standard should be based on the organisation's requirements; in some instances, a single standard is not enough, and a combination of standards is the best practice (Taherdoost 2024). It is important to consider laws and regulations when selecting standards; if an organization is subject to EU regulations, then the IEC 62243 is better. If the organisation is subject to the United States of America, then NIST cyber security standards are likely a better choice. Based on these findings, when it comes to security standards, no security standard meets all organisation, but security standards are based on the uniqueness and requirements of each organisation (Brooks 2022).

3. Methodology

Utilizing the information obtained from the literature review, the research in this paper will identify the best standards for the security requirements in an IT/OT converged environment. The study consisted of three parts: literature analysis, selection of standards, and allocating the best standards for the requirements.

A systematic literature review was conducted based on peer-reviewed journals. The key focus of the evaluation was on security standards and Frameworks. The search occurred in the database of recognised publishers and aggregative databases, which includes ResearchGate, IEEE Xplora, Springer, ScienceDirect, MDPI, EBSCOhost, and the Association for Computing Machinery (ACM).

An internet search was conducted using the primary key works, which included IT/OT convergent/ IT/OT integration, cyber security, IT, and OT security standards. The search looked at publications that included the keywords mentioned above. This resulted in seventy-four publications analysed manually by reading abstracts and conclusions. Sixty-one publications that included IT security and OT security standards were studied. Thirty-two publications addressing IT and OT security standards were used for this literature analysis. Table 3 gives the numerical summary of key words on articles selected for the study.

Table 3. Table showing the number of articles containing keywords

Keyword /words	Number of articles
Security standards	67
Cyber security	65
IT/OT convergent or IT/OT integration	30
IT security standards	62
OT security Standards	66
IT security standard and OT security standard	61

3. Literature analysis

A comparative analysis approach was used to find the different standards applied in the IT and OT environments. Comparative analysis was based on the standards' objectives and implementation guidelines. This approach led to eight security standards detected for both the IT and OT environments. Not all standards could be used for this literature analysis, and the standards used in this study had to be narrowed. The publications used during the comparative analysis were analysed to identify common standards for the study. The selection of standards to use was quantitative, based on keywords and the number of occurrences of keywords. Out of the seventy-four

publications studied, ten publications referred to ISO27000 standards, ten publications referred to CIS Controls, 33 publications referred to IEC 62443 standards, and 25 publications referred to NIST SP 800-82.Table 4 below lists the standards identified.

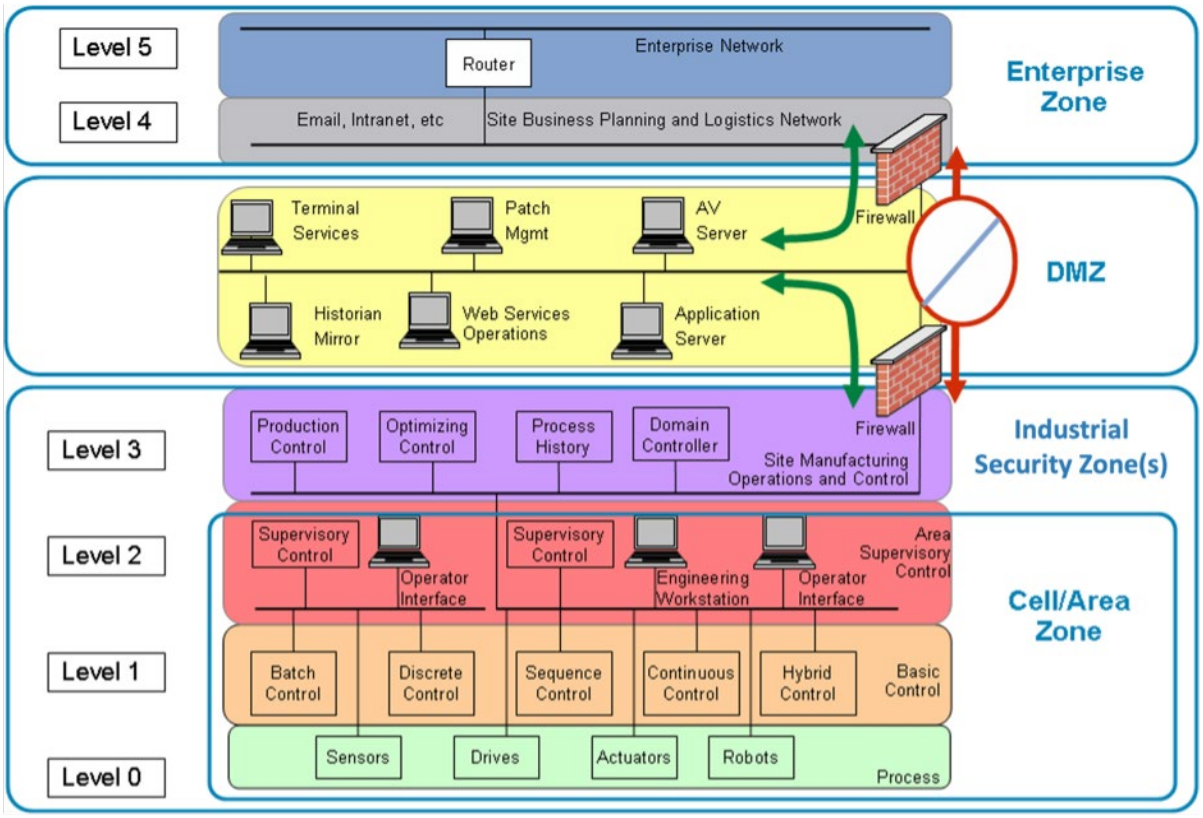
Table 4. List of IT and OT Standards (CIS,2024) (Niemann,2021) (Djebbar and Nordstroom ,2023)

Standard	Description	Selected in Study?
ISO 27000	Information Security standards	Yes
NIST SP 800-53	United States of America (USA) security and privacy controls for classified information	No
NIST SP 800-171	USA Security and Privacy Controls for none classified information	No
CIS Controls	Critical security controls for cyber security	Yes
IEC 62443	Standards focused on cyber security of industrial control systems	Yes
NIST SP 800-82	USA Standards focused on cyber security of industrial control systems for critical infrastructure	Yes
NERC CIP	Cyber security standards for the electric utility industry in North America	No
ETSI EN 303 645	European Standard for Internet of Things (IoT) devices	No

4. Results

Before defining which standard to use in an IT/OT converged environment, one needs to understand the structural framework of industrial control systems using a Purdue Model. As mentioned in the literature review, the Purdue Model is a structural framework for industrial control systems and visual segments traditionally known as the IT Zone and the OT Zone (Ribeiro,2023). The Two zones are divided further into six zones. Please refer to Table 5 , taken from the Cisco Website, for a visual view of the zones.

Table 5. Purdue model for ICS security(Cisco,2024)



Based on the literature analysed, the Table 6 summarises the Purdue Model. The summary includes the type of devices at each level, the risk level, and the focus areas for security implementation.

Table 6. Description of Purdue Model (Hodes 2021) (Cisco 2020) (Garton 2019) (Dave 2023)

Level	IT or OT	Type of Devices	Type of Risk	Key Security Focus
0	OT	Process Level includes physical devices for operation	High-risk rating as Safety is a major risk.	Physical security, access controls, and device hardening.
1	OT	The Controller Level includes controlling devices to control level 0 devices.	High-risk rating as Safety is a significant risk.	Physical security, access controls, and device hardening.
2	OT	Area Supervisory Control –devices for supervising and controlling multiple processes.	High-risk rating due to access to the SCADA system, which controls process levels.	network segmentation, secure remote access, control threat detection
3	OT	Manufacturing Operations - Manages the flow of production and data historian	Medium risk rating due to low risk to personnel production impact is medium due to possible data breaches.	Role-based access control
DMZ	OT	Demilitarized Zone (DMZ)	Penetration of cyber attacks from IT level to OT level	Controlling communication between IT and OT and protecting the OT environment
4	IT	Business Operations - Business management processes include internet Emails, Enterprise resource planning systems, etc	The low-risk rating is due to the well-established IT controls in place.	Implementation of IT security controls, antiviruses, patch management, and security monitoring
5	IT	enterprise network – supports broader business functions and is not directly linked to OT systems.	The low-risk rating is due to the well-established IT controls in place.	Implementation of IT security controls, antiviruses, patch management, and security monitoring

The Canter of Internet Security (CIS) Critical Security Controls is a list of technical security and operational controls. Asset management is the foundation of CIS Critical Security Controls. These controls can be applied in any environment, including the public and private sectors (Roy 2023). The findings reveal that CIS Critical Security Controls were adapted for information security, but these controls can expand to the OT environment (Knowles et al. 2025).

The CIS Critical Security Controls consists of 18 best practices meant to protect organizations from cyber-attacks. The controls are placed into three categories. The basic controls focus on critical cyber security measures such as regular patches and antivirus. Foundational controls include advanced techniques such as log file monitoring and two-factor authentication. Organisational controls are tailored controls for the organisation based on their requirements (CIS 2024).

The International Organisation develops the ISO 27000 standards for Standardization. These standards can be applied to organisations of various sizes (Roy 2023).

ISO 27000 standards are more focused on IT security management systems (ISMS). They generally address information security. These standards define the essential requirements for IT security in an organisation. The ISO 27000 Series consists of 60 standards covering information security issues; therefore, the standards focus more on the organisation's IT-related processes (Niemann,2021). Even though the standards can be used in an OT environment, one needs to be careful of the challenges of implementing some of the measures as previously discussed in the literature review.

The IEC 62443 standards are more focused on the protection of industrial control systems or OT environment; this includes Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS),

and Other Control System Configurations such as Programmable Logic Controllers (PLC). The IEC 62443 standards can be utilized for information systems management, but their key focus is on the OT environment (Niemann, 2021). The IEC standards include ISMS, risk assessment, technical requirements, and management of components for the OT environment. People working in the OT environment better understand the IEC 62443 standards due to the terminology used in these standards (Niemann 2021). The IEC 62443 standards address the roles of users, product suppliers, and system integrators in cyber security protection (Hao et al. 2016).

NIST SP 800-82r3 Guide to Operational Technology (OT) Security is a special publication published by NIST to assist those owning and working in the OT environment (Stouffer et al. 2024). The NIST SP 800-82r3 addresses the safety requirements, required performance, and reliability of the OT environment. This standard mainly addresses confidently and availability of the OT systems and includes topics such as security assessments, authorisation, and implementation of security controls (Rafal 2018). In summary, NIST 800-82 detects security gaps and threats in the OT environment and advises on security applications and management to address these security gaps (Hao et al. 2016).

Based on the literature analysis, the Purdue model, devices installed, risk, and critical security focus can be used as a base to define which cybersecurity standards to apply. Table 7 is a modification of Table 6, which defines which cyber security standards to apply and where to apply them.

Table 7. standards for IT/OT integrated environment (Hodes 2021) (Cisco 2020) (Garton 2019) (Dave 2023)

Level	IT or OT	Type of Devices	Type of Risk	Key Security Focus	Standards
0	OT	Process Level includes physical devices for operation	High-risk rating as Safety is a significant risk.	Physical security, access controls, and device hardening.	IEC 62443
1	OT	The Controller Level includes controlling devices to control level 0 devices.	High-risk rating as Safety is a significant risk.	Physical security, access controls, and device hardening.	IEC 62443/ NIST 800-82
2	OT	Area Supervisory Control –devices for supervising and controlling multiple processes.	High-risk rating due to access to the SCADA system, which controls process levels.	network segmentation, secure remote access, control threat detection	IEC 62443/ NIST 800-82
3	OT	Manufacturing Operations - Manages the flow of production and data historian.	Medium risk rating due to low risk to personnel production impact is medium due to possible data breaches.	Role-based access control	IEC 62443/ NIST 800-82/ CIS Control
DMZ	OT	Demilitarized Zone (DMZ)	Penetration of cyber attacks from IT level to OT level	Controlling communication between IT and OT and protecting the OT environment	CIS Control/ NIST 800-82/ IEC 62443
4	IT	Business Operations - Business management processes include internet Emails, Enterprise resource planning systems, etc	The low-risk rating is due to the well-established IT controls in place.	Implementation of IT security controls, antiviruses, patch management, and security monitoring	ISO 27000/ CIS Control
5	IT	enterprise network – supports broader business functions and is not directly linked to OT systems.	The low-risk rating is due to the well-established IT controls in place.	Implementation of IT security controls, antiviruses, patch management, and security monitoring	ISO 27000/ CIS Control

Based on Table 7, it is clear that no one standard can apply both to the IT and OT environment, and a combination of standards needs to be used to secure an integrated environment.

5. Discussions

An IT/OT integrated environment does not necessarily mean one set of standards for cyber security implementation. Industries need to assess risk in their organisations and select standards based on risk evaluations. Table 7 is a good starting point for industries with industrial control systems that need to be protected, as it simplifies which standards to use and where. Where there is an option of using more than one standard, the organisation can choose standards based on regulations that apply to the organisation. It is also advised that during the initial phase of the implementation of standards, not more than two standards are used. This will simplify the implementation phase for IT and OT departments.

The terminologies used in the standards can create a gap for employees unfamiliar with the environments. For example, IT people working in the OT environment may not be familiar with the OT terminology and vice versa. As mentioned in the literature review, IT and OT have different priorities; by understanding the priorities and cyber risks of the different levels in an IT/OT environment, the necessary and required security measures are put in place. The understanding and implementing Table 7 can have a positive cultural and security outcome for the organisation.

6. Future Directions and Conclusion

Based on the Literature findings, we can conclude that the IT and OT environments are different regarding priorities, infrastructure, and culture; however, threats occurring in the OT environments have made it essential for IT and OT to work together to reduce cybercrimes. The selection and implementation of standards phase is the best phase to start from.

Cybersecurity standards assist organisations in meeting cybersecurity requirements and reducing cyber-attacks. Cyber security standards have their own goals, whether it's for data protection, system architecture protection, equipment protection, or the protection of personnel (Taherdoost 2022). Cybersecurity standards are selected based on the purpose and the environment. This paper was meant to highlight the differences Between IT Security and OT Security standards and illustrate the approaches to securing IT and OT systems using the best-fit standards. It is important to note that some of the standards and best practices implemented in the IT domain can benefit the OT environment; however, this must be done with caution, as some IT practices can cause production issues in the OT environment. Understanding and implementing Table 7 can have a positive outcome for the organisation. Apart from increasing cyber security, it can potentially lead to an improved culture between IT and OT departments and accelerate digital transformation or IT/OT convergence. It is proposed that further studies be carried out to prove the positive benefits of using the best cyber security standards based on the environment of implementation.

References

Alrumaih, T. N., Alenazi, M. J., AlSowaygh, N. A., Humayed, A. A., & Alablani, I. A. Cyber resilience in industrial networks: A state of the art, challenges, and future directions. *Journal of King Saud University - Computer and Information Sciences*, 35(9), 101781, 2023.

Alladi, T., Chamola, V., & Zeadally, S. Industrial Control Systems: Cyberattack trends and countermeasures. Computer Communications, 155, 1–8, 2020.

Bonnie, E. Essential Guide to Security Frameworks & 14 Examples. Secureframe. Retrieved from https://secureframe.com/blog/security-frameworks, 2024.

Cabaj, K., Kotulski, Z., Księżopolski, B., & Mazurczyk, W. Cybersecurity: trends, issues, and challenges. *EURASIP Journal on Information Security*, 2018(1), 2018.

Conklin, W. A. IT vs. OT Security: A Time to Consider a Change in CIA to Include Resilience. 2016 49th *Hawaii International Conference on System Sciences (HICSS)*, 2016.

Cook, A., Janicke, H., Maglaras, L., & Smith, R. An assessment of the application of IT security mechanisms to industrial control systems. *International Journal of Internet Technology and Secured Transactions*, 7(2), 144, 2017.

Dely, J. SANS ICS/OT Cybersecurity Survey: 2023's Challenges and Tomorrow's Defenses. Retrieved from https://www.sans.org/white-papers/ics-ot-cybersecurity-survey-2023s-challenges-tomorrows-defenses/ , 2024.

Dhirani, L. L., Armstrong, E., & Newe, T. Industrial IoT, Cyber Threats, and Standards Landscape: Evaluation and Roadmap. Sensors, 21(11), 3901, 2021.

Djebbar, F., & Nordström, K. A Comparative Analysis of Industrial Cybersecurity Standards. *IEEE Access*, 11, 85315–85332, 2023.

Future Trends in Cybersecurity: Exploring Emerging Technologies and Strategies. *International Research Journal of Modernization in Engineering Technology and Science*, 2024.

Hao, X., Zhou, F., & Chen, X. Analysis of security standards for industrial control system and enlightenment on relevant Chinese standards. *2016 IEEE 11th Conference on Industrial Electronics and Applications* (ICIEA), 2016.

Hicking, J., Stroh, M. F., & Kremer, S. Collaboration Through Digital Integration – An Overview of IT-OT-Integration Use-Cases and Requirements. *IFIP Advances in Information and Communication Technology,* 403–410, 2021.

Iaiani, M., Tugnoli, A., Bonvicini, S., & Cozzani, V. Analysis of Cybersecurity-related Incidents in the Process Industry. *Reliability Engineering & System Safety*, 209, 107485, 2021.

Janakiraman, S. Cyber security for industrial automation & control systems. *Oil And Gas Business*, 1, 176–194, 2024.

Kuppusamy, E., & Mariappan, K. Integration of Operation Technology (OT) and Information Technology (IT) Through Intelligent Automation in Manufacturing Industries. *Advances in Transdisciplinary Engineering*, 2021.

Laydon, B. Automation IT: Cybersecurity at the edge - ISA. *isa.org*. Retrieved from https://www.isa.org/intech-home/2018/may-june/features/cybersecurity-at-the-edge, 2022.

Leszczyna, R. Standards on the cyber security assessment of smart grid. *International Journal of Critical Infrastructure Protection*, 22, 70–89, 2018.

Maesschalck, S., Giotsas, V., Green, B., & Race, N. Do not get stung, cover your ICS in honey: How do honeypots fit within industrial control system security. *Computers & Security*, 114, 102598, 2022.

Maleh, Y. IT/OT convergence and cyber security. *Computer Fraud & Security*, 2021(12), 13–16, 2021.

Moutairou, S. Standard vs. Framework vs. Laws vs. Regulations. TrustCommunity. Retrieved from https://community.trustcloud.ai/docs/grc-launchpad/grc-101/compliance/standard-vs-framework-vs-laws-vs-regulations, 2023.

Niemann, K. Differentiation of the IT security standard series ISO 27000 and IEC 62443 A view of automation systems in the manufacturing and process industries. *ABB*. Retrieved from https://library.e.abb.com/public/fc76636ebed845b88c640a613f0c95a0/3ADR010839_Differentiation_ISO_27001_IEC_62443_REV_C_en_US.pdf, 2021.

Parsons, D. SANS ICS/OT Cybersecurity Survey: 2023's Challenges and Tomorrow's Defenses. Retrieved from https://www.sans.org/white-papers/ics-ot-cybersecurity-survey-2023s-challenges-tomorrows-defenses, 2024.

Pulsipher, W., Scott, A., & Reeb, F. An Argument for a Holistic Approach to Critical Infrastructure Security. *Intel*.

Roy, N. Top 10 IT security frameworks and standards explained. Retrieved from https://www.linkedin.com/pulse/top-10-security-frameworks-standards-explained-nilesh, 2023.

Sekonya, N., & Sithungu, S. An Analysis of Critical Cybersecurity Controls for Industrial Control Systems. *European Conference on Cyber Warfare and Security*, 22(1), 410–419, 2023.

Stouffer, K. Guide to Operational Technology (OT) Security. [2023]

Taherdoost, H. Understanding Cybersecurity Frameworks, and Information Security Standards—A Review and Comprehensive Overview. *Electronics*, 11(14), 2181. [July 12, 2022]

"The NIST Cybersecurity Framework (CSF) 2.0." *The National Institute of Standards and Technology*. Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf , 2024.

"The State of OT/ICS Cybersecurity in 2022 and Beyond." Retrieved from https://www.sans.org/white-papers/state-ics-ot-cybersecurity-2022-beyond, 2023.

"Topic Paper #4-14 PURDUE MODEL FRAMEWORK FOR INDUSTRIAL CONTROL SYSTEMS & CYBERSECURITY SEGMENT." *America's Evolving Oil and Natural Gas Transportation Infrastructure*. Retrieved from https://www.energy.gov/sites/default/files/2022-10/Infra_Topic_Paper_4-14_FINAL.pdf, 2019

Biographies

Thobeka Sishuba is a PhD student at the University of Johannesburg. Her PhD thesis is focused on creating a framework for integrating IT and OT departments. Thobeka Sishuba currently works at Rockwell Automation as an account manager and has previous experience as a technology consultant. Thobeka Obtained her master's in business administration from the Tshwane University of Technology (2021), her Bachelor of Technology in Electrical Engineering from the Tshwane University of Technology (2014), and her Electrical engineering diploma from the Durban University of Technology (2009).

Dr Emmanuel Innocents Edoun, a lecturer specializing in Management Economics and Public Management, holds a doctoral degree from the University of the Witwatersrand. He has worked in the economic and business sectors, public administration, development studies, and socio-economic projects in both rural and urban

landscapes; Dr. Edoun has played pivotal roles in consulting and has led projects in institutions such as the African Union (2008), NEPAD (2003-2008), the Pan-African Parliament (2004-2011), and AFRODAD (2014).

Prof. Anup Pradhan has a PhD in Biological and Agricultural Engineering from the University of Idaho, United States. He holds a Master of Engineering degree in Agricultural Systems and Engineering from the Asian Institute of Technology, Thailand. He also has a Bachelor of Science degree in Agricultural Engineering from Bangladesh Agricultural University, Bangladesh. Prof Anup is a senior lecturer at the University of Johannesburg in South Africa.