The Role of Network Segmentation and Micro-segmentation in Operational Technology Security

Ziad Tariq Almulla
College of Computer Sciences and Information Technology
King Faisal University
Al-Ahsa, 31982, Saudi Arabia
Email: 225000830@student.kfu.edu.sa

Hafizur Rahman
College of Computer Sciences and Information Technology
King Faisal University
Al-Ahsa, 31982, Saudi Arabia
Email: mhrahman@kfu.edu.sa

***Abstract*—Within critical sectors like manufacturing, electricity grids, and water treatment, cybersecurity in operational technology (OT) systems is highly important to managed industrial operations. With the increasing convergence between operational technology (OT) and information technology (IT) networks, they are now more vulnerable to cyber threats and thus require sophisticated security controls.This paper presents, we have presented a systematic literature review (SLR) in respect of network segmentation and micro-segmentation in improving OT security. These are barriers against the traffic of a network, reduce lateral movement of the attackers, and ensure secure perimeters for the protection of the critical infrastructure. The system incompatibility challenge of the legacy systems and the need to maintain high availability in the OT environment are highlighted as key challenges. Furthermore, it assesses existing best practices and identifies open research questions. This review offers practical steps to OT systems in the face of continually increasing OT cyber risks.**

***Index Terms*—Operational Technology,Network Segmentation, Micro-Segmentation, Software-Defined Networking, AI-driven Security**

I. Introduction

Operational Technology (OT) systems are the most widely used and have continued to remain the main systems used throughout the industrial process due to OT systems' ability to manage and control equipment such as sensors and actuators that are found in factories, energy grids, and water treatment plants, as well as other critical infrastructure. For security reasons, historically OT networks could not be connected with IT networks; however, OT proliferation and the necessity to perform operational analytics are changing this paradigm. While this intertwining has provided new efficiencies, it has also made OT networks susceptible to increasing vulnerabilities to cybersecurity threats [1].

A. Background

OT systems being of a sensitive nature, the security of such systems requires special attention as the OT systems operate within the boundaries of the critical infrastructure, affecting the safety of society and the sovereignty of a nation is directly concerned. Failure on the part of OT networks as a target from cyber-attacks can result in physical destruction, disruption in systems operations, and even loss of lives. For example, in 2015, a cyber-attack targeting Ukraine's power grid illustrated the destructive prospects that targeting the OT network can essence because such an attack brought millions without electricity [2].

B. Motivation

This research paper is motivated to study the OT Systems risks from various threats, and to counteract it, two strategies that stand out include network segmentation and micro-segmentation [3]. Network segmentation describes dividing the network into multiple security zones that can reduce the offense axiom of the attacker or his/her movement in the network, and minimize damage spread for incidents when they occur. Micro-segmentation builds on this logic by allowing control over individual workloads or devices, which comes in handy in OT environments where devices have differing security statistics [4].

C. Problem Statement

Most OT systems are composed of older technologies that never had cybersecurity considerations hence complexity in incorporating contemporary security measures like segmentation of networks [5]. Also, OT environments operate automatically, and constant downtime, however brief, may cause both economic and perennial adverse effects or threats to safety. These factors, among others, are hindrances to the deployment and effective maintenance of segmentation strategies in OT environments [6].

Additionally, the shortage of cybersecurity professionals knowledgeable in OT and IT is equally a bar to the security of these networks. Designing networks that use segmentation also requires knowledge of the typical performance of OT systems because the deployable segmented networks need configuration and monitoring in real-time. This paper would like to look into the possibilities of carrying out network

segmentation and micro-segmentation in OT environments while accommodating the constraints of legacy systems and the demand for high availability [7].

D. Scope

Through a systematic literature review, this study seeks to look into the significance of The Role of Network Segmentation in OT.
The key objectives of this review are: By understanding the current state-of-the-art network segmentation and micro-segmentation strategies for OT security [8]. To identify the challenges and limitations in applying these strategies in the OT environment.

E. Research Questions

This paper addresses the following research questions:

- What is the efficiency of network segmentation and micro-segmentation in the improvement of OT security?
- What difficulties may be faced during the segmentation strategies in OT environments?
- Which procedures may be followed while implementing network segmentation and micro-segmentation in OT systems?
- How may new technologies such as SDN and AI enhance the segmentation strategies in OT environments?

II. Literature Review

A. Network Segmentation: Definition and Use Cases

Network segmentation refers to creating zones over a network where these zones are more secure and self contained while allowing communication between these zones in a controlled manner. In IT networks this has been the common approach for a long time because it reduces the risks of malware and avoids unauthorized access to some parts of the network. Segmentation becomes important to improving the security of critical infrastructure by limiting a cyberattack to a small part of the network, it can confine an attacker to a small segment. If the OT network is properly segmented, then, for example, an attacker who has compromised his way through the corporate IT network will not be able to reach the sensitive OT system, such as the industrial control system (ICS). Most discussions about OT security include firewalls and VLANs as a means of segmenting communication zones. Then, inter zone communication is access-controlled so that approved devices and users can communicate between the network segments. This also reduces the risk of an attack, or about the impact an attack may have. An example of the figure 1 shows the mechanism of segmenting networks into OT boundaries to prevent a cyberattack [4].

B. Micro-Segmentation

Historically, micro-segmentation is a granular-type control that takes the concept of network segmentation even further in that instead of segments, individual devices or workloads are being isolated within the network. In the OT environment, the situation is even worse, because we need to increase

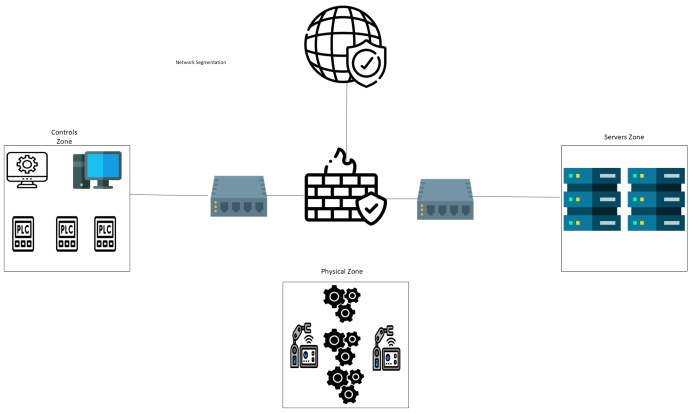

Fig. 1. OT network structure segmentation

the security of individual devices or systems, and this is especially beneficial. An instance is the programmable logic controller (PLC) used in a factory, which will require more security than the sensor controlling environmental conditions. Micro-segmentation ensures a tool to manage traffic on the network in a manner that, once a host is breached, lateral movement within other hosts in the network is impossible. Such approaches are not only theoretical; current analysis has brought out that indeed micro-segmentation limits the attack surface in OT networks. As an illustration, Basta et al. [9] practically illustrated how the zero-trust micro-segmentation framework reduced the network exposure to vulnerabilities within the network with the time of up to 90 percent and therefore makes it more challenging for attackers to take any advantage of the vulnerabilities present in the network [10].

C. Security Threats in OT Networks

Such networks are subjected to a great number of cyber threats, for example, including but not limited to malware, ransomware, APTs, and insiders. The existence of the Stuxnet malware, which targeted Iranian nuclear facilities and the capacity of lacking facilities, is still remembered, further demonstrating the vulnerability of OT cyber systems. In this regard, the damage incurred by a cyberattack on Iran's nuclear capabilities also reverberated in other aspects of warfare where cybernetic capability was useful in inflicting physical deterrence on OT environments [11].

To cut through the risk factors, there is evidence to suggest that OT networks face insider threats as a more significant concern. [12] IT personnel or employees with access to OT assets can create opportunities for abuse and thereafter insert these risks into the network. To reduce these challenges even further, segmentation would be used to restrict employee and contractor access to sections of a network based on what they need to do.

D. Existing Studies to Segment OT and Research Gaps

Existing Studies to Segment OT and Research Gaps A thorough investigation has also been carried out with regard to the deployment of network segmentation in OT environments as numerous studies identified a positive correlation between network segmentation and increased security. For instance, [9] created a model designed for assessing packet forwarding and filtering policies on industrial networks with an emphasis on administratively correct configurations as critical for the success of segmentation strategies In the same manner Wagner et al [12] modeled a continuous-time in order to examine network security against segmentation architecture comprising segments and demonstrated that correlated architectures reduced the success of cyber wars attacks. These findings indicate this however that segmentation thought to enhance OT systems security significantly, the effectiveness will be reliant on design and ongoing management [12].

III. Methodology

A. Search Strategy

The systematic literature review (SLR) technique has been applied in this study to thoroughly cover all the available literature on network segmentation and micro-segmentation as they are applied in OT environments for protection purposes. The databases employed during this search include:IEEE Xplore Google Scholar The following keywords were applied in the search:

”Network Segmentation, Micro-segmentation, ”OT Security, Industrial Control Systems, Critical Infrastructure Cybersecurity,Operational Technology,Software Defined Networking.

In other words, as shown in Figure 2 only peer-reviewed published articles conducted between the years of 2014 and 2024 are included in order to guarantee the authenticity and then recency of the work.

IV. Findings / Analysis

As shown in table 1, the key findings from the review studies on network segmentation and micro-segmentation in OT environments are presented in this section. The analysis is divided into three main categories: We discuss the effectiveness of segmentation, challenges in implementation, and best practices.

A. Effectiveness of Network Segmentation in OT Security

Lateral Movement Reduction: It has been ascertained that the lateral movement potential of attackers in OT environments is greatly reduced due to network segmentation. A great lateral movement is a movement within the networks of a network breach; in this perspective, it would be the movement of threat actors through the network once the first foothold has been established. In traditional OT networks, which are characterized by a flat network structure and interconnections, this flaw or weakness can be utilized by attackers to traverse between systems, resulting in uncontrollable havoc. In contrast,

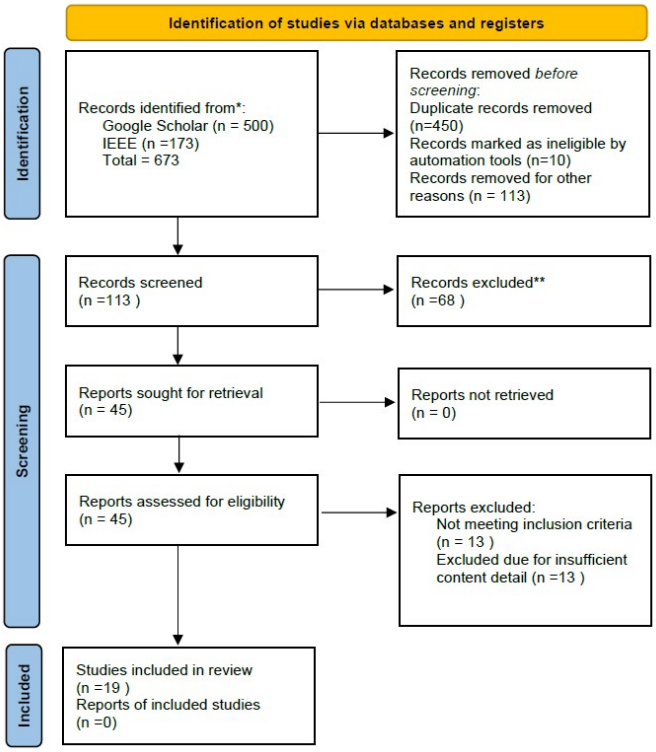

Fig. 2. PRISMA 2020 flow diagram

TABLE I
Key findings of segmentation in OT security

Study	Key Finding	Impact on OT Security
Basta et al.	Micro-segmentation reduces network exposure by 90%	Significant reduction in lateral movement.
Rajashekar et al.	Automation of micro-segmentation improves operational efficiency	Improved accuracy and scalability.
Cheminod et al.	Filtering and packet forwarding reduce unauthorized access	Enhanced network resilience.
Wagner et al.	Segmentation models reduce attack probability in OT networks	Better threat mitigation in segmented OT.

in networks that are segmented, traffic and communication with zones are controlled and conducted via firewalls, access control lists (ACLs), or any such mechanisms that are meant to enhance security. This strategy allows the attacker to only be able to access the first breached segment and not move away from this segment, therefore reducing the amount of damage that the attackers can cause. Basta et al. [9] and Wagner et al. [12] in their research on segmentation in their cyberattack chains, showed that segmented architectures can reduce the ratio of successful cyberattacks to greater than seventy percent.

Containment of Malware and Ransomware: Malware attacks have been on the rise in the past couple of years, with notable cases such as the WannaCry ransomware case in 2017 or the attack on Ukraine’s power grid in 2015 that

were able to demonstrate the amount of damage that a lack of segmentation can cause [7]. Segmenting the network into different independent zones will ensure that malware does not spread throughout the network too easily. Micro-segmentation, for instance, makes sure that communication can be enforced at a more restrictive level so that only trusted devices on the same segment can communicate. Research shows that segmented OT networks were able to significantly curb the spread of malware as compared to non-segmented networks [3] [13].

Enhanced Protection of Critical Infrastructure: Other forms of cyber warfare in the more recent years have proven to be a major threat to critical infrastructural sectors such as the energy, water, and manufacturing sectors. With both OT systems controlling the physical processes and cyber-targeted attacks, if one is successful, the impact could be catastrophic [4].

In these environments, segmentation proves to be useful in safeguarding the most sensitive of the systems. Managed segmented zones allow for the identification of the most essential systems and physical separation from risks. As is the case in energy grids, there is no need to allow corporate IT networks access to SCADA system operations, as it will make the control systems out of reach of the adversaries even if the IT network is breached.

B. Issues in the Adoption of Segmentation in OT

The design architecture brings about potential benefits but on the other hand the segmentation of a network in OT settings has several potential obstacles (shown in table 2).
These barriers pertain to both the technical intricacies in OT architectures as well as operational considerations of the systems which require low downtime [7].

TABLE II
CHALLENGES OF SEGMENTATION IN OT ENVIRONMENTS

Challenge	Description	Example
Legacy System	Incompatible with modern segmentation techniques.	Power plants with outdated SCADA systems
High Availability	Downtime caused by reconfiguration interrupts operational processes.	Energy and manufacturing environments
Lack of Skilled Personnel	Shortage of staff experienced in OT cybersecurity and segmentation management.	Heavy reliance on third-party vendors
Monitoring and Maintenance	Difficulty in continuously monitoring and updating segmented OT environments. Frequent changes in OT network devices.	Heavy reliance on third-party vendors

1) Legacy Systems: Legacy systems apply to the majority of OT systems used in industries, which were created several decades ago and do not take into account modern threats regarding cybersecurity. Such systems, as a rule, do not have the required hardware or software capabilities necessary for implementing network segmentation. Furthermore, the process of changing or replacing these legacy systems to create ways for segmentation is both expensive and slow. Operators of such systems in some instances may also be resistant to making changes that may interfere with existing operations or introduce new risks. For instance, in the case of the energy industry, SCADA legacy systems are much more complicated to upgrade, making micro-segmentation very difficult to put in place [14].

2) High-Availability Requirements: OT environments, particularly those that comprise critical infrastructure, should have continuous as well as high availability. Any downtime or any disconnection due to the restructuring of the network can lead to dreadful impacts like financial loss, production stoppages, and even death. This availability high complicates the edges of the network implementation, which involves segmentation since any expected change in the network has to be done as the operations are running. However, different segmentation strategies should be explored to thoroughly ensure that issues do not arise during the deployment of the OT networks. In some situations, operators may specifically look for maintenance windows outside peak hours to carry out segmentation of policies, which sometimes causes lag in deployment. High availability is a critical target in operations such as that of manufacturing, where the production lines are steady and there is zero possibility for downtime losses [5].

3) Lack of Skilled Personnel: One more serious problem comes along with the lack of specially trained personnel to plan, launch, and carry out the management of segmented OT networks. Such specialists do not usually exist in IT environments to such an extent that segmentation operates regularly, while OT environments require craftsmanship of industrial systems and of cybersecurity knitted together. This fusion of skills is rare, making many organizations depend on third-party providers for segmentation.

Based on dependence on external vendors, it may introduce extra risks to the organization. It may be the case that a vendor does not comprehend the operational context of OT enough to implement effective perimeter security controls, and thus the network remains susceptible to attacks. In addition, the practice of outsourcing security management can lead to communication problems between OT stakeholders and facility security teams, which further aggravate the implementation stage [1].

4) Challenges in Monitoring and Maintenance: Once segmentation is done in an OT network, all network segments have to be managed and maintained to keep the segmented environment from being compromised. In OT, networks are dynamic because they are always incorporating new devices and systems. Such activities might necessitate re-segmentation or adjustments to the rules that govern segmentation. Poor maintenance practices tend to allow segmented networks to assume other vulnerabilities with time, since power loss, for instance, may make old rules that govern the segregation networks, which were authoritative, irrelevant with replacement

devices and new incorporation into the topology [6].

Because of the inherent complexity of OT, monitoring is very difficult. The OT systems work with different types of devices that implement different communication protocols that complicate the overview of network traffic and detection of potential threats. Support of monitoring capabilities for segmented OT networks requires more complex solutions than conventional instruments such as IDS or even real-time analytics with their level of detail.

C. OT Segmentation Considerations and Policies

To address the above mentioned challenges, several issues have been stipulated for the effective deployment of network segmentation in OT environments. These concerns revolve around deploying the best suitable technologies, their configuration, and management, along with periodic reviews of security policies and control [13].

1) Firewalls and Intrusion Detection Systems (IDS): Firewalls are among the most essential elements of a network segmentation practice. Firewalls keep unwanted devices from connecting to key systems by regulating how traffic between segments occurs. In most OT areas, firewalls are used to protect SCADA and PLC systems by creating zones of segmentation from the nonsecure areas [15]. Firewalls can be complemented by deploying intrusion detection systems that are capable of detecting abnormal behavior in network flows. IDS is also capable of detecting boundary breaches and attempts to use segmentation undermining weaknesses [16].

Best practices for firewalls and IDS deployment in OT segmentation are given in Table 3.

D. Firewalls and IDS Deployment in OT Segmentation

Firewalls are essential in OT environments to monitor traffic between segmented zones.

TABLE III
FIREWALLS AND IDS DEPLOYMENT IN OT SEGMENTATION

Best Practice	Description	Example
Use of Firewalls and IDS	Monitor traffic between segmented zones.	Implemented in the critical sectors for isolation
Software-Defined Networking (SDN)	Dynamic segmentation based on centralized control and automation	Used in M. Ma, Z. Yu, and B. Liu study on cloud OT systems
Layered Defense with Segmentation	Multi-layer approach by combining segmentation, IDS, and encryption	Applied in manufacturing OT systems
Regular Security Audits	Conducting periodic audits with verified segmentation configurations	Standard in OT environments with critical infrastructure

Software-Defined Networking (SDN) as a Tool for Micro-Segmentation: Software-defined networking (SDN) [17] has developed into a solution for the challenge of network segmentation in dynamic OT environments. Instead of physically going to every piece of equipment and trying to configure it, SDN empowers administrators to design, create, and alter segmentation policies from a central control plane [18]. This is a streamlined process to change segmentation policies and assures that the network can accept shifted traffic flow or device architecture. Micro-segmentation can also significantly benefit from SDN capacity to isolate inter-device or workload communications. According to Basta et al. [9] micro-segmentation which was automated using recognition of workload in this case SDN was able to realize serious improvements in network security while virtually having no impact on operations in a cloud-based OT environment.

E. Layered Defense Using Micro-Segmentation Techniques

Applying micro-segmentation to critical infrastructure [4] computer networks should adhere to an appropriately layered defense strategy. A breach in one segment should be contained within that segment, allowing organizations to maintain experiential integrity within the entire system. In the approach referred to as defense in depth, segmentation takes part among several strategies including encryption, access control, and monitoring.

V. FUTURE WORK

A. AI-Driven Segmentation

Artificial Intelligence (AI) and Machine Learning (ML) will play an important role in OT environments, especially network segmentation, shortly. Through AI technology, a network administrator can carry out several processes involving segmentation policy management including traffic anomalies detection, modification of segmentation policies, and threat mitigation. AI-powered applications can always track the OT network, and analyze traffic events to learn and modify policies to protect the OT devices.

For example, if a device not known to be authorized tries to connect with a core control network, the segmentation specific to that control network can be modified to prevent such devices. In OT environments such instantaneous action is needed, because the consequences of a threat that remained undetected and unaddressed for any brief period of time would be catastrophic. AI also presents a solution to the problem of the ever-increasing scale of OT networks whereby the number of devices and design of communication protocols make it difficult to define segmentation policies manually.

The emphasis of new initiatives is on seeking tools inspired by AI that are focused on segmentation tasks within OTs while conforming to the requirements of the operational environment and security of these systems. In addition, through the simplification of organizations being able to deploy and manage segmented OT Networks, an AI-based solution can significantly reduce labor burden by performing various necessary tasks of operating and maintaining segmentation policies in design.

B. Real-time Threat Detection and Automation

Focus in OT security research is on the approach of including real time threat detection and automation into the segmentation strategy. The traditional model of network segmentation involves using policies and rules that are static and ordinarily tend to be slow in adapting to new and upcoming threats.

Real-time detection of a threat works the other way around in that sophisticated threat detection systems complemented with analytics and artificial intelligence monitor the network at any time for indications of disparaging activities. If a threat is identified, measures can be taken to ensure that the policy on segmentation is changed automatically to ensure that the threat is confined to a particular location and does not extend to several others.

Network Segmentation is also used as an automation method to enhance the scalability and flexibility of OT networks. In large-scale and complex OT networks, configuring and maintaining the segmentation policies becomes a major challenge if it is to be done manually. Automated solutions, such as SDN, make it possible for administrators to develop advanced segmentation policies that can be elevated in the future without human interaction. This means that policy updates do not risk the overall struggle to maintain security standards as the scope of network changes, new devices, users, and traffic patterns can be added to the segmented hierarchy with ease.

A future in OT security that is dependent on AI, real-time threat detection, and automation will result in a security fabric that is self-evolving and takes machines to a new level. Such technologies will enable organizations to be able to defend their OT systems from both known and unknown threats, thus, critical infrastructure security and reliability will be maintained.

VI. Conclusion

Network segmentation and micro-segmentation techniques are an emerging security focus in the OT environment. The purpose of the techniques is to divide the network inhibit lateral moves for attackers, manage cyber threats, and defend most critical assets. However, some limitations exist regarding the applications of segmentation in OT contexts: legacy systems and high availability. The case for segmentation remains strong. Modern technologies like Software Defined Networking (SDN), as well as Artificial Intelligence (AI) provide excellent means of resolving the impediments. These tools based on Artificial Intelligence particularly can reduce the cyberattack segmentation management practice upon organizations, hence greater flexibility in the security design of the organizations.

In further studies, attention should be directed towards the development of common patterns for OT network segmentation and the use of AI and instant detection of threats in the segmentation strategies. Such advanced technologies would improve the security of OT systems against the upcoming threats and hence the safety and effectiveness of the key infrastructures will be maintained.

References

[1] W. Schwab and M. Poujol, "The state of industrial cybersecurity 2018," 06 2018.

[2] R. Rajashekhar, S. B. Prapulla, and K. Kishore, "Automation of network micro segmentation," vol. 5, no. 3, pp. 6341–6344, 06 2017. [Online]. Available: https://www.ijitr.com/index.php/ojs/article/download/1733/pdf

[3] M. Arifeen, A. Petrovski, and S. Petrovski, "Automated microsegmentation for lateral movement prevention in industrial internet of things (iiot)," vol. undefined, no. undefined, 12 2021. [Online]. Available: https://doi.org/10.1109/sin54109.2021.9699232

[4] H. A. Al-Ofeishat and R. Alshorman, "Build a secure network using segmentation and micro-segmentation techniques," vol. 16, no. 1, pp. 1499–1508, 07 2024. [Online]. Available: https://doi.org/10.12785/ijcds/1601111

[5] T. Kampa, C. K. Müller, and D. Großmann, "Interlocking it/ot security for edge cloud-enabled manufacturing," 01 2023. [Online]. Available: https://doi.org/10.2139/ssrn.4481855

[6] M. Kallatsa, "Strategies for network segmentation: A systematic literature review," 01 2024.

[7] M. Niedermaier, T. Hanka, F. Fischer, and D. Merli, "A secure network scanner architecture for asset management in strongly segmented ics networks," vol. 1, no. 1, pp. 347–355, 01 2021. [Online]. Available: https://doi.org/10.5220/0010191603470355

[8] T. Bashir, "Zero trust architecture: Enhancing cybersecurity in enterprise networks," vol. 6, no. 4, pp. 54–59, 09 2024. [Online]. Available: https://doi.org/10.32996/jcsts.2024.6.4.8

[9] N. Basta, M. Ikram, M. A. Kâafar, and A. Walker, "Towards a zero-trust micro-segmentation network security strategy: An evaluation framework," vol. undefined, no. undefined, pp. 1–7, 04 2022. [Online]. Available: https://doi.org/10.1109/noms54207.2022.9789888

[10] M. Cheminod and L. Seno, "Static analysis of packet forwarding and filtering configurations in industrial networks," vol. undefined, no. undefined, 04 2023. [Online]. Available: https://doi.org/10.1109/wfcs57264.2023.10144115

[11] R. Setola, G. Oliva, G. Assenza, and L. Faramondi, "Cyber threats for operational technologies," *Int. J. Syst. Syst. Eng.*, vol. 10, 2020.

[12] N. Wagner, C. Şahin, M. Winterrose, J. Riordan, J. Peña, D. Hanson, and W. Streilein, "Towards automated cyber decision support: A case study on network segmentation for security," 12 2016. [Online]. Available: https://doi.org/10.1109/ssci.2016.7849908

[13] M. Ma, Z. Yu, and B. Liu, "Automatic generation of network micro-segmentation policies for cloud environments," pp. 1–5, 06 2023. [Online]. Available: https://doi.org/10.1109/ainit59027.2023.10212857

[14] A. Koay, R. K. L. Ko, H. Hettema, and K. Radke, "Machine learning in industrial control system (ics) security: current landscape, opportunities and challenges," *Springer Science+Business Media*, vol. 60, no. 2, pp. 377–405, 10 2022. [Online]. Available: https://doi.org/10.1007/s10844-022-00753-1

[15] W. Shang, Q. Qiao, M. Wan, and P. Zeng, "Design and implementation of industrial firewall for modbus/tcp," *Academy Publisher*, pp. 432–438, 01 2016. [Online]. Available: https://doi.org/10.17706/jcp.11.5.432-438

[16] S. S. Soniya and S. M. C. Vigila, "Intrusion detection system: Classification and techniques," 03 2016. [Online]. Available: https://doi.org/10.1109/iccpct.2016.7530231

[17] N. S. Bülbül, D. Ergenç, and M. Fischer, "Sdn-based self-configuration for time-sensitive iot networks," *2021 IEEE 46th Conference on Local Computer Networks (LCN)*, pp. 73–80, 2021.

[18] D. Kreutz, F. M. V. Ramos, P. Verissimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-defined networking: A comprehensive survey," 2014. [Online]. Available: https://arxiv.org/abs/1406.0440