ICS Network Security in the Rise of IIoT technology

Anh Dao
anh.d.dao@aalto.fi

Tutor: Mohit Sethi

Abstract

This paper examines how Industrial Control Systems network security has been designed and implemented, alongside potential future implementations in the face of modern technological developments. It starts by providing an overview of the Purdue model and how the model has been used to implement zone-based network segmentation. The paper then looks at the new security paradigm called Zero-trust in the context of Operational Technology. It then describes how industrial systems can utilize a combination of segmentation methods to achieve Zero-trust security. Finally, the paper analyzes the current landscape of Industrial Control Systems network security and the way forward for enterprises.

KEYWORDS: IoT, Industrial networks, Zero-trust, Network Segmentation

1 Introduction

Industrial Control Systems (ICS) security frameworks might undergo a paradigm change as we know it within the next decade. ICS, as defined by the National Institute of Standards and Technology (NIST), is a general term for several types of control systems that are used to achieve an industrial objective such as manufacturing or transportation [1]. ICS

is considered part of Operational Technology (OT) architecture and often contrasts with Information Technology (IT) architecture.

This OT/IT contrast stems from differing priorities. Traditionally, IT departments maintain internal network security and critical enterprise data, while OT departments make sure physical processes and related equipment operate smoothly without physical failure. Due to this, ICS network security focuses on isolating OT devices from the network. Models like the Purdue model and other related ICS network security models provide a traditional perimeter defense which has become the industry standard since their conception.

However, with the rapid improvement and integration of Internet of Things (IoT) devices into the enterprise framework, dubbed Industrial Internet of Things (IIot) or Industry 4.0, the boundaries between IT and OT have blurred, exposing traditional models to new attack vectors. Current research trends aim to rectify these vulnerabilities with many calling for a gradual transition towards Zero-trust as a paradigm.

This paper reviews the Purdue model's method of network segmentation as the current standard for ICS networks. Various implementations of network segmentation that aim to achieve Zero-trust principles are also reviewed.

This paper is organized as follows. Section 2 explains the design behind the Purdue model and how it has been adapted for network security. Section 3 examines the principles of zero trust and how different aspects of it can be implemented in an industrial setting. Section 4 analyzes the current state of ICS networks and whether a fully Zero-trust solution is viable.

2 Purdue and Zone-based network segmentation

Before being used as the reference for security implementations, the Purdue Model was part of the Purdue Enterprise Reference Architecture (PERA)[2]. PERA abstracts a Computer-integrated Manufacturing (CIM) system into separate elements (Information System, Human and Organizational, and Manufacturing Equipment Architectures). Because of this, it quickly becomes the standard for ICS network security. This results in a hierarchical model in which an ICS is separated between layers [3].

Level 0 contains machinery and other devices that are directly responsible for the manufacturing process. Level 1 has the sensors and con-

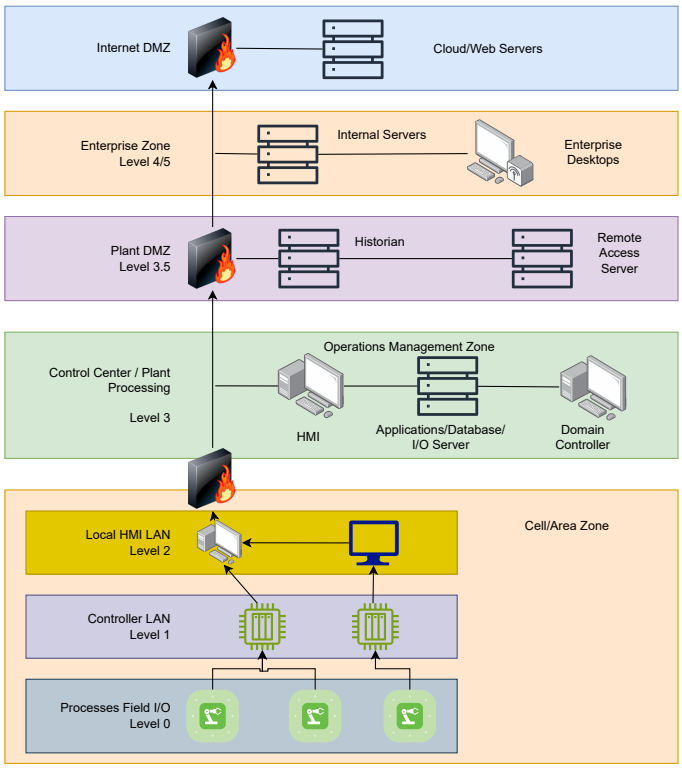

Figure 1. Standard Purdue model with DMZ [3]

trollers that instruct the processes in level 0. Level 2 contains supervisory systems that oversee the Level 0/1 processes and ensure things run smoothly at a Cell/area level. Level 3 coordinates the production within the plant. Level 4/5 houses the enterprise systems responsible for administrative operations and the company's internal servers. Traditionally, this level has always been associated with IT infrastructure. Firewalls are placed between different Zones for IT and OT, preventing unrestricted traversal.

Although PERA originally did not have the concept of a demilitarized zone (DMZ), the DMZs are introduced into the security model with the goal of further separation between the levels of IT and OT. Network movement between IT zones and OT zones is under the supervision of a firewall, virtual or physical, with clearly defined rules that allow for exceptions only in the most critical circumstances. The result is a perimeter defense with "air gaps" that block the connection between devices of different zones but allow devices in each zone to communicate with one another.

3 Zero-trust Architecture

Zone-based segmentation satisfies the need of the enterprise to separate IT and OT. However, it is exactly because of this property that the threat of IIoT devices becomes a real issue. A connected IIoT device that periodically sends data to a server is a critical vulnerability that can be breached for lateral movement throughout the affected zone [4]. The blurring of the "air gaps" essentially erases the key security element of the zone-based segmentation method.

This rising threat results in the rise of a new paradigm called Zero-trust. Zero-trust Architecture (ZTA), as described by NIST [5], has the following view of a network:

- There are no implicit trust zones inside the network
- Enterprise network may include devices non-configurable by the enterprise
- Resource access needs to always be evaluated and authorized
- Certain resources might not be on the enterprise infrastructures
- Remote subjects and assets must not trust the local network connection
- Assets moving between enterprise and non-enterprise infrastructure should be under a strict and consistent access control policy

To successfully implement ZTA, there are three core logical components: the Policy Engine (PE), the Policy Administrator (PA), and the Policy Enforcement Point (PEP). Figure 2 showcases the core design of a Zero-trust system by NIST [5]. The PE decides on devices' access to a network based on the enterprise's security policy. The PA executes the decision of the PE and sends the command to the relevant PEP. The PA and PE are sometimes implemented as a single component called the Policy Decision Point (PDP). PEPs enable, monitor and ultimately terminate the relevant connections between devices and the network according to the instructions of the PA. Other components within the architecture assist in the operations of these core logical components.

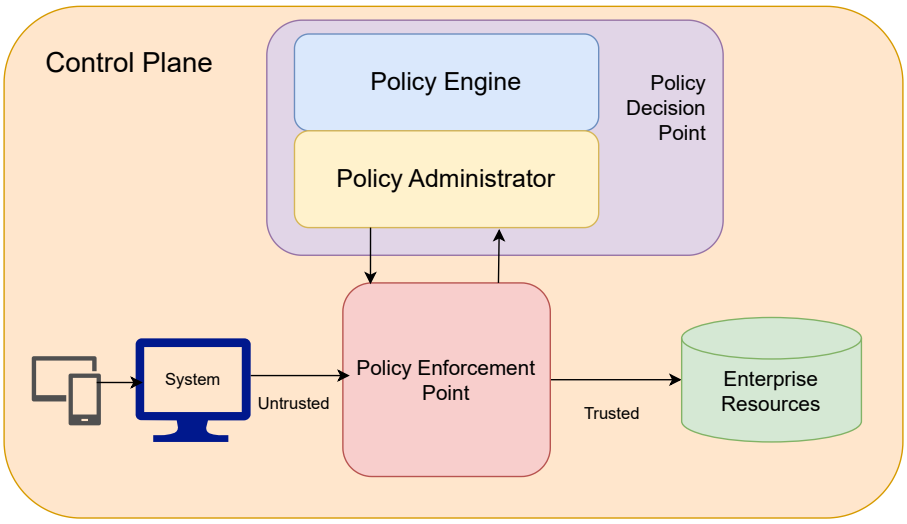

Figure 2. Zero-trust Core Logical Component[5]

Implementing Zero-trust in a factory setting is challenging and oftentimes not feasible at the current moment. Such extensive policy controls take time and resources to implement, sometimes resulting in the halting of critical processes of a facility. In these cases, the enterprise might not be able to take the financial damage related to the stoppage of operation. On the other hand, traditional OT devices are updated slowly with costs amortized over many years which means in most factories with IIoT, there are legacy machinery and systems in place that do not have IoT capabilities at all. These devices are still connected to the internal network without a fine-tuned policy for network communication because previously, the device relied on the inherent zones of trust provided by the Purdue model.

These challenges alter the direction of ZTA research for ICS security. A popular direction has been to take existing segmentation methods and use them to achieve certain security aspects of a Zero-trust model, such as no implicit trust zones or resource access authorization, instead of a fully Zero-trust model seen in IT infrastructure. This paper looks at widely used methods that have been suggested in contemporary research.

3.1 Identity-based segmentation

Identity Management and Access Controls (sometimes referred to as PR.AC) is a known method of protection for traditional ICS systems in both IT and OT networks, with guidelines and suggestions across numerous standards [1]. However, traditionally, due to the separation between

IT and OT, a single device would have a set of identifications for use in different zones or levels. This makes it challenging to scale up a factory PR.AC system in an IIoT environment as more and more devices are connected to the network that needs some form of authentication and authorization. Recommendations suggest centralizing the identity management process. However, once attackers gain access to an identity in either the OT or IT network, they can potentially traverse the network bypassing our intended zone-based isolation. Other issues involve the time needed for authentication and authorization which might not satisfy the stringent requirement of OT systems. An example would be in the case of an emergency, an operator should be able to instantly access a supervisory system to shut down the processes before immediate risks to safety or potential damages.

A possible solution suggests using blockchain to create a proof of identity that can provide fast authentication[6]. The concept essentially establishes edge computing centers near where the IIoT devices are located on the network. These edge centers set up the blockchain network that acts as the local hub where devices can connect and gain access to enterprise network resources like the cloud. The identity certificates are authenticated through a public key-based system with both the certificates and the authentication themselves being appended as a transaction on the blockchain, ensuring integrity over a pre-determined period. While the scalability of this method remains to be seen in real scenarios, this solution shows that emerging technology can also help ICS designers in creating secure systems.

3.2 Micro-segmentation

An alternative way of describing network traffic comes from cardinal direction terminology. If zone-based network segmentation focuses on north-south traffic (moving between the levels and the external network), what is a segmentation method that can monitor east-west traffic? The solution comes from micro-segmentation, a segmentation method that enforces security policies between workloads in the same area, furthering the control a system has between its devices [7]. In an IIoT environment where most devices are integrated into the network, this method is suitable for isolating critical devices for an enterprise operation from vulnerable terminals in a manufacturing process.

However, implementing micro-segmentation remains a consistent chal-

lenge for enterprises. Flow-based firewalls in small to medium-sized enterprises were optimized for environments that do not scale well to a micro-segmentation implementation [8]. While in an IT environment, it is possible to implement micro-segmentation using different strategies, such as agentless, hypervisor-based, or agent-based, in an ICS setting this is not a realistic solution. As described above, this is primarily due to the lack of network security capabilities of the IIoT devices or legacy OT devices that do not have any network security considerations in their design. Therefore, the main approach that an ICS network can have when it comes to network segmentation comes from a network-based micro-segmentation, where the network itself is the one enforcing traffic through the use of a third-party controller. The main issue with this approach comes from the risk of latency increase as the network needs to handle increasing traffic loads as the enterprise infrastructure integrates more and more IIoT devices.

Future research direction for micro-segmentation therefore aims to smoothly integrate micro-segmentation through the usage of tools like machine learning or automated threat detection [7]. Conceptually, this approach creates a dynamic protection system where access policies are dynamic and constantly changing according to the current state of the network. Irregular traffic would be quickly detected and blocked without the need for a defined rule set such as an access control list. This prevents potential loopholes from being discovered by attackers even as the list of potential connections grows as an enterprise scales up. The goal is to develop an implementation that can be smoothly integrated over existing macro-segmentation implementations, such as a Purdue model-based network, to make it suitable for deployment in a large-scale enterprise.

3.3 Software-Defined Networking Segmentation

As relying on IIoT devices' networking capabilities is oftentimes insufficient in terms of security, a fully software-based approach has been suggested as a potential implementation for ICS models. The approach, appropriately named as Software-Defined Networking (SDN), allows for network designs that bypass the differences in configurations between IIoT devices of different manufacturers and legacy OT systems.

While traditional SDN implementations in an IT network involve 3 layers called application, control, and data, SDN in the context of an ICS network replaces the data layer with the physical layer [9]. Based on Fig-

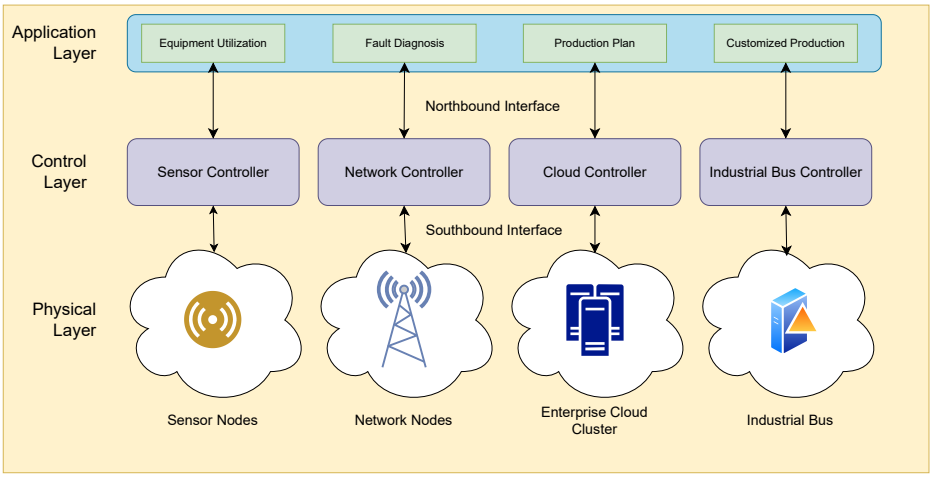

Figure 3. SDN in an Industrial Internet of Things Framework [9]

ure 2, the network is abstracted into several different components. The physical layer includes the sensors and their related processes, the network nodes like routers and switches of the original network, the enterprise's internal and cloud servers, and devices related to manufacturing data transmission (industrial bus). The control layer involves the various controllers that manage and monitor the network traffic and behavior of devices in the physical layer. It is also responsible for the communication between the physical layer and the application layer. The application layer is where the factory supervisory system is located alongside the enterprise's IT network. This design allows for networks that were previously designed under the Purdue model to transition into this network without scalability issues. Furthermore, the preliminary design shown in Figure 3 looks similar to the zone-based segmentation method seen in traditional network segmentation.

However, the similarities end here as SDN segmentation allows for more fine-tuned control as it provides complete visibility to all traffic happening in the network. This ensures that abnormal patterns are properly detected while specific segmentation strategies like micro-segmentation can be deployed without scalability issues [7]. Furthermore, while IIoT devices do not have the necessary capabilities to have defined security controls, manufacturers can implement software components that describe a specific IIoT network configuration during its production. These software components, called Manufacturing Usage Descriptions (MUD), allow for well-defined access-control schemes that ensure protection against volume-based attacks such as Denial-of-Service (DoS) or Transmission Control Protocol (TCP) flooding [10]. Similar to an automated Intrusion

Detection System, an SDN security model can monitor SDN telemetry according to pre-existing MUDs provided by connected IIoT devices. Any anomalous patterns that fall outside of MUD-compliant behavior would then be restricted by an automated system using machine learning or artificial intelligence.

3.4 Example of a Zero-trust implementation

The methods described above all see utilization in proposed Zero-trust models that do not necessarily contradict the Purdue model but rather improve upon it. One suggestion establishes that while inherent trust zones are not removable in ICS models, designers can reduce the zone through micro-segmentation as much as IT and OT can be separated, in essence achieving zero-trust standards [11]. The core ZTA components, the PDP/PEP, exist between the different zones in the Purdue model, replacing the firewalls in the standard implementation. Within the Enterprise Zone is IT identity-based security protection like multi-factor authentication or endpoint security. Security in the Operations Zone focuses on protecting the controls of ICS/SCADA systems. This means a micro-segmentation model that isolates critical infrastructures from one another through the use of fine-tuned and granular firewalls and identity policies. Finally, the Process Zone focuses on data and source system integrity. This is accomplished through the use of Process Variable Detection (PVAD), with a digital twin monitoring and mapping of all communications between devices. Rogue data from processes can then be identified and isolated.

While this is not the only type of ZTA model suggested, other proposed architectures share the same design principle. The Purdue model is not replaced by Zero-trust, but instead, a Zero-trust model is implemented within the Purdue framework [12]. In this model, the corporate network and the manufacturing network still exist as zones. However, an identity access management system is responsible for controlling access between the operator and the manufacturing system, removing implicit trust between them. Tools like the Enterprise Device Discovery System and the Endpoint Compliance Management System are used to ensure strict monitoring of devices registered to the network, effectively serving as the PE and PA of this model. On the other hand, the manufacturing processes are treated in terms of phases, where the local area is deemed as one unit that is isolated from other units in the network. While the zones of trust still

exist, similar to the previous model it has been reduced to just existing within local areas.

A more abstract implementation of ZTA utilizes a modified version of the logical model provided by NIST [13]. Instead of a central PDP/PEP governing the entire system, this model proposes a micro-segmentation model where a central system determines the policies of individual local zones of trust and securely distributes these policies to local PDP/PEP logical units that are only responsible for their respective areas of controls. Access to resources in these local areas uses IAM controls, requiring mutual authentication with digital certificates and ensuring that the identity of the requested device is authenticated locally by the PEP. The local PDP/PEP pairs periodically get updated to the latest security policy through a central policy server with a backup available for process authorization in the event the network goes down. This ensures that there are no singular points of failure for the entire network. Given the scale of the network model, SDN is required to have a consistent policy enforcement framework that can be easily scaled up as the enterprise network grows larger with further IIoT integration.

4 Analysis

As shown in the sections above, IIoT has resulted in the development of new segmentation methods on top of the original Purdue model to better safeguard against potential critical vulnerabilities. These methods do not necessarily contradict the original Purdue model but instead, supplement it by filling up the supposed security gaps in its designs. However, the security gaps differ between enterprises and how they implement their ICS. It also differs between various industries and their processes. Therefore, in terms of feasibility of implementation for the various segmentation methods, it can be viewed under the following lens:

Segmentation Method	Feasibility of Implementation
SDN segmentation	Feasible and required for Zero-trust
Micro-segmentation	Feasible with potential scalability issue. Requires SDN implementation.
Identity-based segmentation	Conceptual implementation with Blockchain. Requires SDN implementation.

SDN should become the primary transition step for enterprises if the goal is to eventually fully transition to Zero-trust. This is because in terms of scalability and implementation ease, SDN satisfies both aspects given that developers can layer an SDN over the traditionally flat ICS network. Afterwards, the abstraction provided by SDN allows for specific areea isolation, particularly in dangerous IIoT segments or in critical areas of a manufacturing plant, which allows security specialists to implement further segmentation methods, such as micro-segmentation and identity management.

This reflects the trends in ICS network security research in general and ZTA research more specifically. Most proposals don't seek to completely overhaul the entire system, as that would be largely impractical. Instead, suggested models implement what is essentially a pseudo Zero-trust design where at its core, the Purdue model is still there as the PERA model for ICS, and stricter security controls are implemented to reduce the implicit zones of trust. Most models assume a degree of ambiguity regarding the current state of IIoT devices and how they interact with the network with a combination of intermediary control that acts as the equivalent of an IT node. This also demonstrates how Zero-trust is still in its early phase regarding OT systems. The latest NIST standard for OT includes guidelines for Zero-trust for the first time in 2023. Its previous iteration was 8 years ago in 2015. Even the NIST standard for Zero-trust architecture only comes out in 2020. The pace in which IIoT technology is developing might be too fast for standards to properly keep up which reflects the current research focus in finding what might be the Purdue model for Industry 4.0.

Another observation regarding IIoT research showcases the current cultural divide between IT and OT. Because network security was traditionally the concern of the IT side, research regarding network segmentation for ICS is largely a reaction to IT improvement, such as in IoT and

network infrastructure. OT research regarding IIoT security focusing on pre-existing components included by the device manufacturers, such as MUD, which can be used to clearly create control rules without the need of too much IT involvement. However, given that MUD is closely related to SDN segmentation, an OT/IT convergence is a realistic possibility in the near future. Because of this, research should slowly incorporate both IT and OT in its design to better reflect this paradigm change. While this seems like a promising idea, the lack of qualified researchers and experts that are knowledgeable in both fields means it will be several years before complete convergence is possible and a potentially brand new field of research is opened up.

5 Conclusion

Overall, while the rise of IIoT has created new security risks and concerns, there are multiple ways of mitigating these issues without compromising on existing system infrastructure. However, given the contrasting nature of IT/IoT advancement cycles versus OT advancement cycles, it might not be possible for enterprises to change to the latest security standards. Instead, a more gradual approach, dependent on the ICS implementation, is needed for safe and smooth integration of IIoT systems to

References

[1] National Institute of Standards and Technology. Guide to operational technology (ot) security. Technical Report National Institute of Standards and Technology Special Publication (NIST SP) 800-82, Revision 3, September, 2023, U.S. Department of Commerce, Washington, D.C., 2023. doi: 10.6028/NIST.SP.800-82r3.

[2] T.J. Williams. The purdue enterprise reference architecture. *Computers in Industry*, 24(2):141–158, 1994. doi: 10.1016/0166-3615(94)90017-5.

[3] Blagovest Chanev Belev. Purdue model implementation in the shipping control systems. In *2022 10th International Scientific Conference on Computer Science (COMSCI)*, pages 1–4, 2022. doi: 10.1109/COMSCI55378.2022.9912594.

[4] Murshedul Arifeen, Andrei Petrovski, and Sergei Petrovski. Automated microsegmentation for lateral movement prevention in industrial internet of things (iiot). In *2021 14th International Conference on Security of Information and Networks (SIN)*, volume 1, pages 1–6, 2021. doi: 10.1109/SIN54109.2021.9699232.

[5] National Institute of Standards and Technology. Zero trust architecture. Technical Report National Institute of Standards and Technology Special Publication (NIST SP) 800-207, August, 2020, U.S. Department of Commerce, Washington, D.C., 2023. doi: 10.6028/NIST.SP.800-82r3.

[6] Yongjun Ren, Fujian Zhu, Jian Qi, Jin Wang, and Arun Kumar Sangaiah. Identity management and access control based on blockchain under edge computing for the industrial internet of things. *Applied Sciences*, 9(10), 2019. doi: 10.3390/app9102058.

[7] Ziad Tariq Almulla and Hafizur Rahman. The role of network segmentation and micro-segmentation in operational technology security. In *2025 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*, pages 0342–0347, 2025. doi: 10.1109/ICAIIC64266.2025.10920695.

[8] Kemal Šanjta and Elmir Babović. Are firewalls limiting scaling factor to small to medium-sized enterprises in the wake of micro-segmentation? In *2021 20th International Symposium INFOTEH-JAHORINA (INFOTEH)*, pages 1–6, 2021. doi:10.1109/INFOTEH51037.2021.9400651.

[9] Jiafu Wan, Shenglong Tang, Zhaogang Shu, Di Li, Shiyong Wang, Muhammad Imran, and Athanasios V. Vasilakos. Software-defined industrial internet of things in the context of industry 4.0. *IEEE Sensors Journal*, 16(20):7373–7380, 2016. doi: 10.1109/JSEN.2016.2565621.

[10] Ayyoob Hamza, Hassan Habibi Gharakheili, Theophilus A. Benson, and Vijay Sivaraman. Detecting volumetric attacks on lot devices via sdn-based monitoring of mud activity. In *Proceedings of the 2019 ACM Symposium on SDN Research*, SOSR '19, page 36–48, New York, NY, USA, 2019. Association for Computing Machinery. doi: 10.1145/3314148.3314352.

[11] Raven Sims. *Implementing a Zero Trust Architecture for ICS/SCADA Systems*. Phd thesis, Dakota State University, 2024. url: https://scholar.dsu.edu/theses/445.

[12] Biplob Paul and Muzaffar Rao. Zero-trust model for smart manufacturing industry. *Applied Sciences*, 13(1):221, 2023. doi: 10.3390/app13010221.

[13] Claudio Zanasi, Silvio Russo, and Michele Colajanni. Flexible zero trust architecture for the cybersecurity of industrial iot infrastructures. *Ad Hoc Networks*, 156:103414, 2024. doi: 10.1016/j.adhoc.2024.103414.