IT Security Solutions for IT/OT Integration: Identifying Gaps and Opportunities

Mukund Bhole
Institute of Computer Engineering
TU Wien
Vienna, Austria
mukund.bhole@tuwien.ac.at

Wolfgang Kastner
Institute of Computer Engineering
TU Wien
Vienna, Austria
wolfgang.kastner@tuwien.ac.at

Thilo Sauter
Institute of Computer Technology, TU Wien
Dep. of Integrated Sensor Systems
Danube University Krems, Austria
thilo.sauter@tuwien.ac.at

***Abstract*—In the contemporary landscape of convergence between Information Technology (IT) and Operational Technology (OT), maintaining asset visibility within the Industrial Control Systems (ICS) infrastructure is paramount. Yet, the escalating targeting of legacy systems and air-gapped networks by cyber threats underscores the need for robust security measures and solutions to counter unauthorized access and malicious activities. This paper presents an analysis aimed at identifying gaps and opportunities in integrating IT Security Solutions with OT environments. These solutions offer comprehensive features such as real-time threat detection, asset identification, network monitoring, and incident response capabilities tailored specifically for the unique challenges posed by industrial control networks. Leveraging the Festo MPS 403-1 system as a case study, we delve into the intricacies of IT/OT integration and highlight areas necessitating improvement to achieve seamless convergence and harness the advantages of unified systems across industries.**

***Index Terms*—IT/OT Integration, Operation Technology, IT Security Solutions, Data acquisition, Industry 4.0**

I. Introduction

The convergence of OT and IT has indeed become increasingly common in various industries. IT and OT convergence refers to the merging of OT, which involves specialized hardware and software used for monitoring and controlling physical processes in industrial environments, with IT, encompassing computing technology, data storage, networking, and software applications for administrative purposes. This integration aims to drive operational efficiency, productivity, and innovation by combining the capabilities of both domains.

However, in many industries, the development of OT and IT infrastructure has led to the emergence of two distinct domains, each managed separately on its own technologies, standards, and governance methods [1]. This division has created a notable gap between IT and OT, necessitating manual and limited data exchange between their respective systems [2].

Several factors contribute to this gap, including technical disparities, differences in equipment life cycles, and organizational cultures between production-oriented OT and business-oriented IT. Additionally, inadequate central governance covering enterprise-wide OT safety and security strategies, harmonized with IT responsibilities, further compounds the challenge [3], [4]. Fundamental differences in orientation between product/control-oriented OT and business/information-oriented IT, coupled with security and safety concerns, further underscore the gap between the two domains.

Moreover, IT-based information systems and OT-based control systems differ in lifecycle, operation, monitoring, and maintenance. Basic technologies such as programming languages and communication protocols also vary [5]. Achieving the fusion of OT and IT environments requires a comprehensive evaluation framework to navigate the integration landscape effectively. This entails not only identifying existing solutions but also assessing their suitability, interoperability, and alignment with industrial objectives.

This paper addresses the critical task of assessing IT security solutions for OT integration, highlighting gaps and opportunities for improvement. The paper is structured as follows: Section II presents the related work on the gaps in the convergence of IT and OT, while Section III provides a brief overview of the solutions used in the IT environment for asset identification, network monitoring and threat detection in OT. In Section IV, we present the analysis and results of gaps in IT solutions used in the OT environment. Section V delves into the discussion regarding the imperative to bridge the gap in the IT/OT environment. Finally, Section VI offers concluding remarks and future work on the paper.

II. Related work

In the domain of IT, paramount importance is accorded to safeguarding data integrity, confidentiality, and availability through rigorous security protocols. Conversely, OT focuses primarily on ensuring functional safety and resilience to preempt operational hazards. Although these objectives are inherently complementary, the contrasting architectures and protocols utilized in IT and OT environments frequently engender discordance and vulnerability [6].

A notable gap exists in the informal nature of data exchange between OT devices and IT back-end servers. Unlike the structured and controlled systems typical in OT environments, these exchanges lack standardized protocols, leaving systems exposed to cyber threats. As OT networks become more dynamic, the risk of security breaches and operational disruptions increases [1].

Furthermore, the differing priorities of IT and OT exacerbate the divide. While IT focuses on agility, cost reduction, and

business insight, OT prioritizes efficiency, consistency, and safety. Bridging these objectives requires overcoming organizational silos and fostering collaboration between IT and OT teams [7].

To address these challenges, organizations should establish cross-functional teams dedicated to IT-OT convergence, implement interoperable technologies and standards, and invest in training to enhance interdisciplinary skills. Additionally, adopting holistic cybersecurity strategies that encompass both IT and OT security needs is essential [8]. By addressing these disparities pragmatically, organizations can leverage the potential of IT-OT convergence for enhanced industrial efficiency and innovation.

Stergiopoulos et al. [9] emphasized the pivotal role of the ICS security community as a central reference point and the exploration of potential modeling combinations, which can facilitate the identification and development of complex integrated solutions. The work also highlighted a prioritization of risk mitigation through qualitative analyses over quantitative approaches, although it fell short in addressing specific IT/OT integration challenges.

The Suricata, Snort, and Bro (Zeek) tools are utilized for analysis in ICS due to their notable advantages. For example, they provide a modular and extensible framework for generating and analyzing security-related events. However, it should be noted that these solutions have limited visibility into OT-specific threats or anomalies [10].

Hurd et al. [11] not only scrutinized existing security solutions for an ICS environment but also delved into the availability of solutions in specific domains. The investigation proceeded under the assumption that enterprise zone security solutions are readily accessible and well-supported. The authors also outlined the landscape of available solutions and their limitations in detecting malware or malicious anomalies. Additionally, they conducted a gap analysis to identify areas within ICS environments lacking adequate solutions for specific security purposes and proposed desired attributes of future technologies to address these gaps. However, the feasibility of integrating these solutions into legacy systems was not addressed.

Knapp et al. [12] discuss the aspects of ICS to monitor, what information to collect, and how to utilize it effectively. Monitoring priorities primarily concentrate on logs due to their capability to offer detailed accounts of past activities, widespread availability, and familiarity. However, it's important to acknowledge that log files may not always be accessible and could lack sufficient detail in certain scenarios. Moreover, this could lead to compatibility issues or challenges in integrating these solutions with existing OT infrastructure.

Coletta et al. [13] and González-Granadillo et al. [14] have highlighted that SIEM systems not only incorporate log data aggregation and event correlation, providing valuable assistance in forensic analysis of cyber incidents and aiding in attack prevention through real-time alerting, but they also need to enhance features such as behavioral analysis, risk assessment and deployment, visualization, data storage, and response capabilities to remain competitive in the market.

Bhosale et al. [15] investigated various IDS methodologies commonly utilized in ICS and presented NIDS solutions that can aid in network protection. However, the study fell short in addressing specific IT/OT integration challenges.

III. IT-Based Security Solutions

Network monitoring and asset identification solutions in IT for OT environments serve crucial roles in identifying, mapping, and understanding the layout and connectivity of OT networks. These solutions help OT professionals gain visibility into their network infrastructure, which is essential for effective management, monitoring, and security. Here, we present IT-based security solutions along with their main features that make them helpful for deployment in the OT domain:

A. OTORIO Industrial Risk Monitoring & Management Platform (RAM^2)

The RAM^2[1] platform aims to provide comprehensive risk monitoring and management capabilities for industrial environments. It typically offers features such as real-time threat detection, asset inventory and management, vulnerability assessment, anomaly detection, and compliance monitoring. By analyzing data from various sources within an industrial network, RAM^2 helps organizations identify and respond to potential security threats and operational risks effectively.

Overall, RAM^2 serves as a centralized platform for monitoring, analyzing, and managing cybersecurity risks within industrial environments, helping organizations enhance their security posture and maintain operational resilience.

B. Nozomi Networks OT and IoT Security Tool

The Nozomi Networks tool[2] addresses this common challenge by automatically creating and maintaining an IoT/OT asset inventory, ensuring it remains current. It identifies network devices, verifies details, and provides precise descriptions. Additionally, it continuously monitors each asset's metadata in real-time, capturing attributes such as:

- Device name, type, serial number, firmware version, and components
- Asset and subpart properties: site, name, IP address, MAC address, and state
- Embedded devices like controllers or Programmable Logic Controllers (PLCs) and their internal components
- Logical node subsystems such as circuit breakers, switches, and measurement points
- PC operating system and installed software applications with version numbers

Dedicated asset views facilitate easy visualization, search, and detailed exploration of device information. Furthermore, operators have the flexibility to include additional details such as location and site.

[1]https://www.otorio.com/ram2-ot-security-solution/

[2]https://www.nozominetworks.com/

C. Security Onion

Security Onion[3] is a widely used open-source platform designed for network security monitoring and threat detection. It provides a comprehensive suite of tools and capabilities to help organizations detect and respond to security threats effectively. Security Onion is built on top of the Linux operating system and integrates various security solutions and technologies into a single platform. Some of the key features and components of Security Onion include:

- Network Security Monitoring (NSM): Security Onion includes tools like Suricata and Zeek (formerly known as Bro) for network traffic analysis, intrusion detection, and protocol analysis.
- Host-based Intrusion Detection System (HIDS): It utilizes tools like Wazuh and osquery for host-based intrusion detection and monitoring on individual devices within a network.
- Log Management and Analysis: Security Onion leverages Elasticsearch, Logstash, and Kibana (ELK stack) for centralized log management, storage, and analysis. This allows security analysts to correlate events across different sources and identify potential security incidents.
- Packet Capture (PCAP) Analysis: The platform supports the collection and analysis of network packet captures using tools like tcpdump and Wireshark, enabling deep packet inspection and forensic analysis.
- Threat Intelligence Integration: Security Onion can integrate with various threat intelligence feeds to enhance its detection capabilities and provide context for identified security events.

D. Sofia Community Tool by Dragos

Sofia[4] is an intrusion detection and network asset discovery tool that offers Deep Packet Inspection (DPI) capabilities for industrial protocols such as Modbus/TCP, DNP3, Ethernet/IP, BACnet, and OPC UA. This functionality enables users to gain deeper insights into their OT assets. Additionally, Sofia allows users to passively capture network traffic, providing valuable data for security analysis and monitoring.

E. ForeScout

ForeScout[5] is a robust commercial tool developed by ForeScout to discover, classify, and manage network OT assets. Utilizing both passive and active methods, this tool effectively identifies assets across the network, eliminating blind spots and streamlining the collection of asset intelligence. ForeScout's functionality extends to maintaining inventories for various device types within the network, ensuring comprehensive coverage.

In addition to asset discovery, ForeScout provides real-time device context sharing, enabling swift decision-making and action implementation. Furthermore, it automates policy enforcement based on predefined rules and executes response actions, enhancing overall security posture and operational efficiency in OT environments.

IV. Analysis of gaps in IT-based security solutions used in OT environment

A. Testing Lab Setup

Fig. 1 illustrates the lab infrastructure, the IT/OT environment extends across two locations interconnected via a VPN tunnel facilitated by OpenVPN. Our attention now turns towards assessing the suitability and resilience of market-available solutions for integration within the OT environment using the Festo MPS 403-1 system use case[6]. The principal goal is to evaluate the necessary adjustments to the current infrastructure before deploying IT-based security solution aimed at monitoring the OT environment.

1) OT Environment: In an OT environment, the Festo MPS 403-1 System by Festo Didactic comprises three stations: Distribute Pro, Join, and Sort Inline. The distribution station manages tasks such as holding, sorting, and feeding workpieces. It is equipped with several RFID read and write heads and intelligent sensors based on IO-Link, forming an autonomous system. The join station is responsible for combining multiple workpieces into one and facilitating their feeding. The sorting station categorizes workpieces based on different configurations and sorts them accordingly. Typical components of such a system include:

- PLC: A ruggedized computer for automating electromechanical processes, such as controlling conveyor systems. It executes control logic, interfaces with sensors and actuators, and exchanges data with other systems.
- Sensors: Devices detecting physical parameters like position, speed, temperature, or pressure in the conveyor system. Examples include proximity sensors, photoelectric sensors, and encoders, providing input for the PLC to monitor and respond to system changes.
- Actuators: Convert electrical signals from the PLC into mechanical motion to control the conveyor system's operation. Examples include motors, pneumatic cylinders, and solenoid valves, with the PLC commanding them based on sensor input and programmed logic.
- Human Machine Interface (HMI): Allows operators and engineers to interact with the conveyor system, monitor its status, and adjust parameters. Typically a touchscreen display or software interface providing real-time visualization of process data, alarms, and control options.
- Control Software: Specialized software for programming the PLC, configuring system parameters, and simulating conveyor operations. Enables users to develop control algorithms, simulate scenarios, and troubleshoot issues before real-world implementation.
- Networking and Communication: Interconnects OT components using industrial communication protocols like Ethernet/IP, Profinet, or Modbus TCP/IP. Facilitates data

[3]https://securityonionsolutions.com/

[4]https://www.dragos.com/

[5]https://www.forescout.com/solutions/ot-security/

[6]https://ip.festo-didactic.com/Infoportal/MPS/MPS403I4.0/EN/index.html

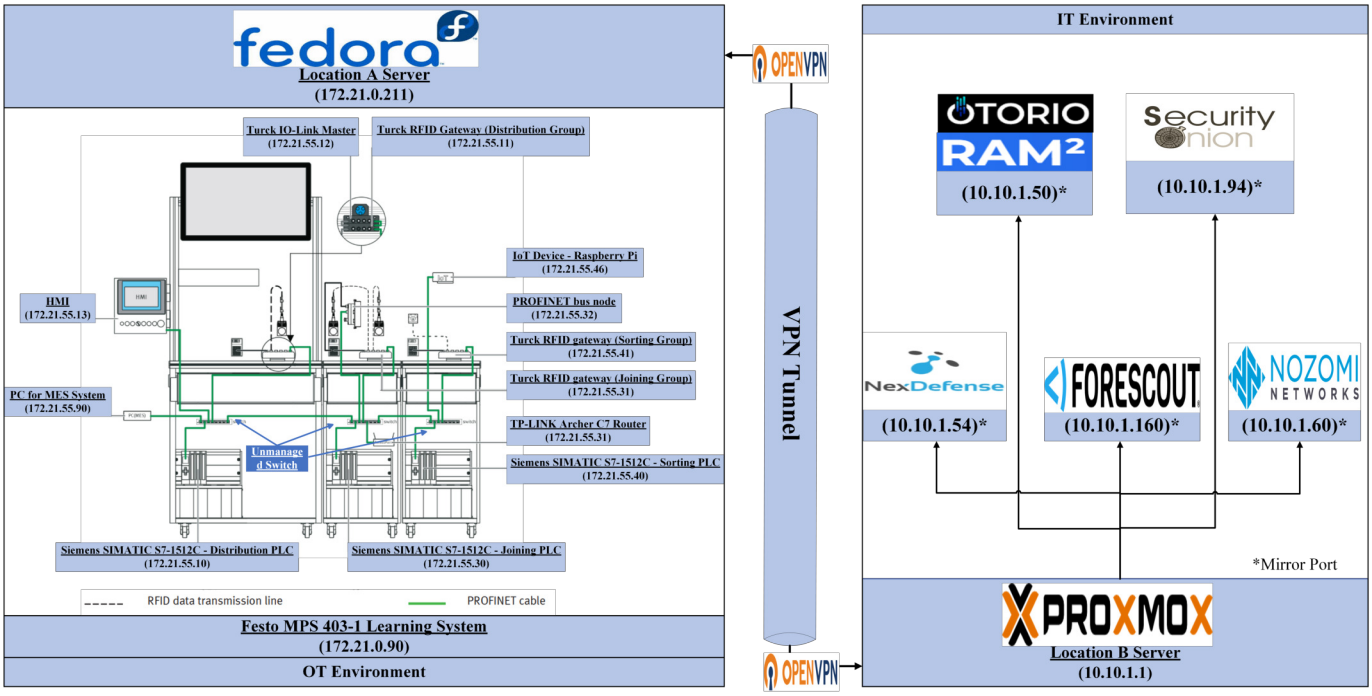

Fig. 1. Testing Lab Setup: Festo MPS 403-1 system in OT environment on the left, IT security solutions monitoring OT environment on the right, interconnected via VPN tunnel.

exchange between devices and integration with higher-level control systems or enterprise networks.

2) IT Environment: A Virtual Machine (VM) environment hosted on a Proxmox server is equipped with several cybersecurity solutions tailored for network monitoring and defense. Among these solutions are Otorio RAM^2, offering real-time asset visibility and threat detection specifically for OT environments, and Forescout, providing extensive network visibility and device identification capabilities. Complementing these are Security Onion, an open-source platform for network security monitoring and log analysis, and Nozomi Networks, specializing in OT and IoT security solutions with advanced threat detection capabilities. Additionally, Sofia by Dragos, a threat intelligence platform focused on ICSs and OT environments, enhances cybersecurity resilience through actionable insights and context-aware alerts. Leveraging a mirror port configuration on the Proxmox server, these solutions collectively empower organizations to bolster their OT network security, proactively identify threats, and maintain operational integrity.

B. Analysis and Results

1) Gap Analysis of IT-based security solutions against requirements: Table I presents the analysis results of the IT solutions with respect to the specified requirements. By assessing IT solutions against these criteria, organizations can make informed decisions regarding which tool best aligns with their specific needs and objectives for OT integration and network management. Additionally, conducting hands-on trials or proofs of concept can further validate the tool's capabilities and suitability for the organization's environment. The requirements are as follows:

RQ1: Network Clustering: A network cluster refers to a densely connected group of nodes within a network, which may represent standard devices interconnected with other clusters in the graph.
RQ2: Visualization: Visualization entails representing the network's nodes and links visually, providing a graphical depiction of the system's architecture and connectivity.
RQ3: Automated Networked OT Asset Discovery: This process involves cataloging and monitoring OT assets automatically, facilitating efficient asset management and security monitoring.
RQ4: Plugin Support: Plugins enable additional functionalities within the system, eliminating the need for a dedicated platform environment to incorporate new features.
RQ5: Security Alerts & Patch Management: This feature detects security vulnerabilities in assets and provides alerts, along with suggesting available patches to mitigate identified risks.
RQ6: User Interface (Dashboard): The dashboard serves as an interface presenting progress reports and real-time data representation through infographics, enhancing user interaction and insight into system performance.
RQ7: Licensing: Integrated tools ensure consumer and producer rights protection through proper licensing, mitigating risks associated with unauthorized software usage. Licensing options can include commercial or open-source, each with

distinct implications.

RQ8: Packet Capturing and Analysis: Packet capturing, which involves intercepting and analyzing IP packets between source and destination, aids in detecting and analyzing network security threats.

RQ9: Multi-Vendor Support: The tool is designed to support assets from multiple vendors, facilitating comprehensive monitoring and management capabilities across diverse environments.

RQ10: Deployment: Deployment, whether on-premise or in the cloud, involves running tools in either a System Under Test (SUT) or a production environment, utilizing servers or applications.

RQ11: Scanning: Network scanning using tools encompasses two approaches: active and passive scanning.

RQ12: Export File: This feature enables the tool to convert asset information into different formats, facilitating compatibility with various systems and applications.

2) Discovery of Networked OT Assets: The total number of networked assets typically encompasses all devices connected to the network, including workstations, servers, networking equipment, Internet of Things (IoT) devices, and potentially OT devices. Conversely, the total number of discovered OT assets specifically refers to OT devices such as industrial controllers, sensors, actuators, and other equipment used in the OT lab infrastructure of the Festo MPS 403-1 learning system. The findings' results are depicted in Fig. 2, which also includes the total number of networked assets, discovered OT and IT assets, along with any unknown assets.

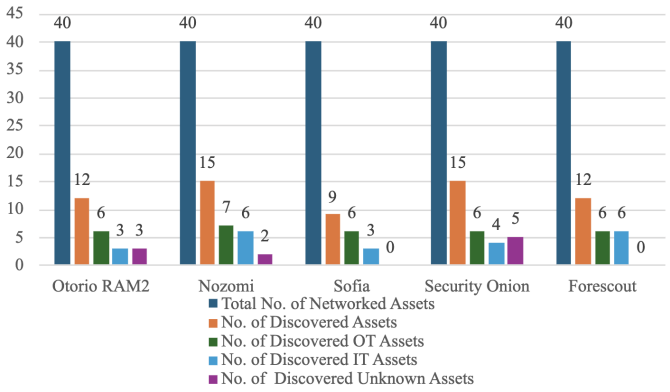

Fig. 2. Asset Discovery with IT security solutions

3) Discovery of used Network Protocols: Discovering the network protocols used in the Festo MPS 403-1 OT environment is crucial for understanding communication patterns and ensuring interoperability and security, as depicted in Table II.

4) Analysis of IT Security solutions based on Gap Categories: Analyzing IT solutions based on gap categories such as monitoring, hardware & software, safety, and security benefits can provide valuable insights into the effectiveness and limitations of these solutions in Festo MPS 403-1 OT environments, as illustrated in Table III.

- **Monitoring Gap**: This gap refers to the capability of IT security solutions to adequately monitor OT systems, encompassing devices, processes, network traffic, heartbeat, status, and bandwidth. Many conventional IT monitoring solutions may lack inherent support for monitoring the industrial protocols commonly utilized in OT environments. Moreover, OT systems often demand real-time monitoring functionalities that might surpass the capabilities offered by standard IT monitoring solutions.
- **Hardware & Software Gap**: This gap pertains to the compatibility and support of IT solutions for the diverse hardware and software utilized in OT environments, including CPU usage, memory usage, disk space, latency, and jitter. OT systems frequently rely on specialized hardware and proprietary software, which might not be entirely compatible with standard IT solutions. Additionally, legacy OT systems may face constraints in terms of hardware capabilities and software versions, presenting challenges for seamless integration with modern IT security solutions.
- **Safety & Security Benefits Gap**: This gap focuses on the ability of IT security solutions to address both safety concerns and security benefits for OT systems, including compliance requirements. This includes capabilities such as threat detection, vulnerability management, access control, and ensuring compliance with relevant regulations and standards. Safety-critical OT systems require robust monitoring and control measures to prevent accidents and ensure compliance with safety standards. However, IT security solutions may lack specialized features for monitoring safety parameters and responding to critical events in real time. Additionally, OT environments are increasingly targeted by cyber threats, necessitating robust security measures to protect against unauthorized access and malicious activities. Many traditional IT security solutions may not adequately address the unique security challenges present in OT environments, such as legacy systems and air-gapped networks. Compliance with industry regulations and standards adds another layer of complexity to the monitoring and security requirements of OT systems.

V. Discussion

Upon analyzing the discovered OT assets in the use case depicted in Fig. 2, it becomes evident that bridging the gap between IT and OT requires several significant steps. Initially, efforts should concentrate on establishing an IoT-based gateway and network infrastructure tailored for industrial automation. This infrastructure should aim to connect OT assets to IT, thereby facilitating the discovery and seamless integration of OT-IT convergence.

Central to this integration are IoT gateways, serving as intelligent system performance indicators operating at the network edge. These gateways can perform diverse functions, including ensuring high scalability for innovative systems by decentralizing data collection and processing, thus alleviating

TABLE I
GAP ANALYSIS OF IT SECURITY SOLUTION AGAINST REQUIREMENTS

Solutions	**RQ1**	**RQ2**	**RQ3**	**RQ4**	**RQ5**	**RQ6**	**RQ7**	**RQ8**	**RQ9**	**RQ10**	**RQ11**	**RQ12**
Security Onion	✓	✓	✓	✓	✓	✓	■	✓	✓	△+⌀	A+P	✗
Sophia	✓	✓	✓	✓	✓	✓	■	✓	✓	△	A+P	✓
ForeScout	✓	✓	✓	✓	✓	✓	☒	✓	✓	△	A+P	✓
OTORIO [RAM^2]	✗	✓	✓	✓	✓	✓	☒	✓	✓	△+⌀	A+P	✓
Nozomi Networks	✓	✓	✓	✓	✓	✓	☒	✓	✓	△+⌀	A+P	✓
Legends: ✓= Fullfilled, ✗= Not Fullfilled, ■ = Open-Source, ☒ = Commercial, △ = On-Premise, ⌀ = Cloud, P = Passive Scan, A = Active Scan												

TABLE II
DISCOVERY OF USED NETWORK PROTOCOLS IN FESTO MPS 403-1

Category	**OTORIO RAM^2**	**Nozomi Networks**	**Security Onion**	**Sofia**	**Forescout**
Protocols in Festo MPS System	HTTPS, HTTP, DNS, UDP, POP3, IMAP, SMTP, MQTT, UA, SSH, PROFINET, QUIC, SMB, SSDP, NetBIOS, LLDP, IGMP, MDNS				
Protocols Detected	ALL	ALL	ALL except UA	ALL except MQTT, UA	ALL except QUIC

the burden on centralized locations. IoT gateways can also streamline industrial networks by providing an abstraction layer between devices and higher-level applications, expediting the introduction of new endpoints while reducing development complexities. Moreover, they contribute to cost efficiency by minimizing Machine-to-Machine (M2M) Wide Area Network (WAN) traffic and latency, ensuring compatibility with legacy devices and protocols, and enhancing security through device isolation and upstream communications protection. This approach can establish a robust foundation for bridging the gap between IT and OT, paving the way for seamless integration and unlocking the full potential of converged systems in industrial environments.

Discussing the gaps introduced in this paper, addressing the *monitoring gap* involves developing or integrating monitoring features specifically tailored to industrial protocols and real-time requirements. Collaboration with OT experts can help understand monitoring requirements and refine IT security solutions accordingly.

Addressing the *hardware & software gap* entails developing adapters or gateways that bridge the gap between IT and OT hardware and software. These solutions can offer customization options or APIs for integrating IT security solutions with proprietary OT systems, as well as harmonizing duplicate or overlapping IT/ OT processes, data structures, and strategies.

Addressing the *safety & security gap* involves incorporating safety-specific monitoring features into IT security solutions, such as alarms, shutdown procedures, and safety interlocks. Ensuring integration with safety-certified systems and protocols to comply with industry standards and regulations is essential. Additionally, developing specialized security features for IT security solutions targeting OT environments, such as anomaly detection algorithms tailored to industrial protocols, is crucial. Collaborating with OT security experts can help identify and address specific security risks and requirements within OT systems.

Bridging the gap between IT and OT presents various opportunities for enhancing industrial efficiency and innovation. IT vendors can play a crucial role by developing specialized functionalities tailored to the unique requirements of OT environments, including features like time-sensitive control loops and deterministic communication protocols essential for the smooth operation of industrial processes. However, establishing collaborative frameworks between IT and OT teams is vital. These frameworks foster knowledge sharing, alignment of objectives, and effective communication. By working together, IT and OT professionals can better understand each other's perspectives and requirements, leading to more seamless integration efforts and ultimately unlocking the full potential of converged systems in industrial environments.

VI. CONCLUSION

In this work, we examined several IT-based security solutions—Nozomi, Otorio RAM^2, Forescout, Sofia, and SecurityOnion—for their integration into OT systems. Using the Festo MPS 403-1 as a case study, we conducted an analysis to identify various gaps, including monitoring, hardware and software, and safety and security benefits, as well as opportunities in connecting IT with OT environments. Our findings underscored the need for improvement to achieve seamless integration and capitalize on the advantages of unified systems across industries. Recognizing these gaps and opportunities in current IT-based security solutions empowers industries to make informed decisions, enhancing their IT/OT integration strategies and operational efficiency.

Future research endeavors could focus on developing specialized functionalities within IT-based security solutions tailored to the specific needs of OT environments. These specialized functionalities in IT-security solutions can include:

- IT-based security solutions should be focused to accurately discover and inventory OT assets such as devices, software, and systems. This provides a comprehensive view of the OT environment, crucial for managing vulnerabilities, planning upgrades, and responding effectively to incidents.
- The solutions should recommend integrating Industrial IoT (IIoT) gateways when legacy devices are detected. IIoT gateways serve as intermediaries to enforce security policies, monitor communications, and enhance visibility

TABLE III
ANALYSIS OF IT SECURITY SOLUTIONS BASED ON GAP CATEGORIES IN FESTO MPS 403-1

Gap Analysis Categories	**Otorio RAM**[2]	**Nozomi Networks**	**Security Onion**	**Sofia**	**Forescout**
Scanning Efficiency of OT Asset	15%	17.5%	15%	15%	15%
Monitoring Gap					
Heart Beat	Not Available	Available	Not Available	Available	Available
Nodes status	Not Available	Available	Not Available	Available	Available
Bandwidth (Average.↑↓ in *Mbps*)*	360	348	424	253	369
Hardware & Software Performance Gap					
CPU usage (Mean)*	42.2%	58.6%	74.6%	35.2%	49.1%
Memory usage*	64.8%	54.8%	45.1%	57.5%	61.4%
Disk space*	60.0%	54.3%	78.8%	45.3%	42.2%
Latency(in *ms*)*	101.2	79.3	90.2	89.3	54.7
Jitter (in *ms*)*	17.243	15.642	16.473	20.246	14.243
Safety and Security Benefits Gap					
Compliance	IEC 62443, NIST, and NERC CIP	CMMC compliance, NIST-Cybersecurity Framework (CSF)	N/A	N/A	TSA SD 2021-02, Comply to Connect (C2C), Continuous Diagnistics and Mitigation (CDM), EU NIS, ISA 99/IEC 62443, NERC CIP, TSA pipeline security
*The analysis was done using *Solarwinds VoIP & Network Quality Manager*					

into older systems. This integration allows for unified monitoring across both IT and OT environments, streamlining security management and enabling swift incident responses.

- When developing IT-based security for OT, it's essential to consider the specific hardware and software capabilities of industrial systems. This includes understanding processing power, memory usage, and communication protocols. By optimizing solutions within these constraints, organizations can minimize disruptions to critical operations and seamlessly integrate with existing OT infrastructure.
- Development of IT-based security solutions should align closely with safety and security compliance regulations. This involves implementing stringent security controls, conducting regular audits, and maintaining comprehensive documentation to demonstrate adherence to regulatory requirements. Such alignment helps mitigate legal risks, uphold industry standards, and bolster overall cybersecurity resilience.
- IT-based security solutions leverage advanced technologies like behavioral analytics and predictive analysis to detect anomalies and potential threats within OT environments. By analyzing deviations from normal patterns and using machine learning algorithms to forecast potential risks, these solutions enhance proactive threat detection and enable timely responses to security incidents. Initiatives such as the ETHOS [7] open-source platform is one way for sharing anonymous early warning threat information.

Additionally, fostering increased collaboration between IT and OT experts could lead to refining existing solutions and creating new ones better equipped to address the unique challenges associated with OT integration.

[7]https://www.ethos-org.io/

ACKNOWLEDGMENT

This paper was supported by TÜV AUSTRIA #SafeSecLab Research Lab for Safety and Security in Industry, a research cooperation between TU Wien and TÜV AUSTRIA.

REFERENCES

[1] T. Sauter and A. Treytl, "Iot-enabled sensors in automation systems and their security challenges," *IEEE Sensors Letters*, vol. 7, no. 12, pp. 1–4, 2023.

[2] K. Sharma, "20 - information technology–operation technology convergence," in *Overview of Industrial Process Automation (Second Edition)*, second edition ed., K. Sharma, Ed. Elsevier, 2017, pp. 359–375.

[3] *IT and OT Convergence - Opportunities and Challenges*, ser. SPE Intelligent Energy International Conference and Exhibition, vol. All Days, 09 2016.

[4] S. Mantravadi, R. Schnyder, C. Møller, and T. D. Brunoe, "Securing it/ot links for low power iiot devices: Design considerations for industry 4.0," *IEEE Access*, vol. 8, pp. 200 305–200 321, 2020.

[5] H. Kanamaru, "The extended risk assessment form for it/ot convergence in iacs security," in *2021 60th Annual Conference of the Society of Instrument and Control Engineers of Japan (SICE)*, 2021, pp. 1365–1370.

[6] S. Hollerer, T. Sauter, and W. Kastner, "Risk assessments considering safety, security, and their interdependencies in ot environments," in *Proceedings of the 17th International Conference on Availability, Reliability and Security*, ser. ARES '22, 2022.

[7] A. Hahn, *Operational Technology and Information Technology in Industrial Control Systems*. Cham: Springer International Publishing, 2016, pp. 51–68.

[8] N. S. T. A. C. (NSTAC), "NSTAC Report to the President: Information Technology and Operational Technology Convergence," 2022.

[9] G. Stergiopoulos, E. Vasilellis, G. Lykou, P. Kotzanikolaou, and D. Gritzalis, "Classification and comparison of critical infrastructure protection tools," in *Critical Infrastructure Protection X*, 2016, pp. 239–255.

[10] J. E. Rubio, C. Alcaraz, R. Roman, and J. Lopez, "Current cyber-defense trends in industrial control systems," *Computers & Security*, vol. 87, p. 101561, 2019.

[11] C. M. Hurd and M. V. McCarty, "A survey of security tools for the industrial control system environment," United States, Tech. Rep., Jun 2017.

[12] E. D. Knapp and J. T. Langill, "Chapter 12 - security monitoring of industrial control systems," in *Industrial Network Security (Second Edition)*, second edition ed. Boston: Syngress, 2015, pp. 351–386.
[13] A. Coletta and A. Armando, "Security monitoring for industrial control systems," in *Security of Industrial Control Systems and Cyber Physical Systems*. Cham: Springer International Publishing, 2016, pp. 48–62.
[14] G. González-Granadillo, S. González-Zarzosa, and R. Diaz, "Security information and event management (siem): Analysis, trends, and usage in critical infrastructures," *Sensors*, vol. 21, no. 14, 2021.
[15] D. A. Bhosale and V. M. Mane, "Comparative study and analysis of network intrusion detection tools," in *2015 International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT)*, 2015, pp. 312–315.