IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 3 March 2026, accepted 28 March 2026. Date of publication 00 xxxx 0000, date of current version 00 xxxx 0000.

Digital Object Identifier 10.1109/ACCESS.2026.3682366

PURITY: An Industry-Standard-Based Security Framework for IT-OT Convergence

FRANZ-KARL SCHACHINGER[1], THOMAS ROSENSTATTER[1,2], AND ULRICH PACHE[1]

[1]Department of Information Technologies and Digitalization, Salzburg University of Applied Sciences, 5412 Salzburg, Austria
[2]Josef Ressel Centre for Intelligent and Secure Industrial Automation, Salzburg University of Applied Sciences, 5412 Salzburg, Austria

Corresponding author: Thomas Rosenstatter (thomas.rosenstatter@fh-salzburg.ac.at)

This work was supported by the Austrian Federal Ministry of Economy, Energy and Tourism, the National Foundation for Research, Technology, and Development and the Christian Doppler Research Association.

ABSTRACT The convergence of Information Technology (IT) and Operational Technology (OT) introduces complex cybersecurity challenges, particularly for industrial control systems. This paper presents a security framework that integrates industry security standards into the Purdue model, offering a structured approach to safeguarding IT-OT networks. By mapping security controls from various security standards like ISO 27001, IEC 62443, NIST SP 800-82, and ISO 27033 to the individual Purdue model levels, this framework establishes a security baseline which focuses on small and medium-sized enterprises (SMEs) to enhance their network resilience. The proposed approach emphasizes layered security mechanisms, including network segmentation, access control, encryption, and incident response. In addition, risk assessment methodologies are applied to prioritize security measures, optimizing protection strategies against emerging threats. The implementation guidelines are tailored to address practical constraints in SMEs, ensuring accessibility and effectiveness. The findings underscore the importance of adopting a structured security framework to mitigate cybersecurity threats in industrial environments, aligning IT and OT security postures.

INDEX TERMS Industrial cybersecurity, IT-OT convergence, network segmentation, Purdue model, security framework.

I. INTRODUCTION

The rapid development of digital transformation has accelerated the integration of Information Technology (IT) into Operational Technology (OT), driven by the need for operational efficiency and real-time data analysis [1]. However, OT systems, originally designed for reliability, availability, and safety rather than cybersecurity, face increasing external threats as they become more interconnected. Similarly, IT systems that are interconnected with OT environments inherit additional risks and vulnerabilities stemming from its constraints, differences in requirements, and legacy aspects of OT. These challenges include outdated software, limited patching capabilities, and a lack of built-in security controls, making the IT-OT integration a critical attack vector that requires targeted protective measures.

The associate editor coordinating the review of this manuscript and approving it for publication was Amjad Mehmood.

A. MOTIVATION

Cyberattacks on Industrial Control Systems (ICSs) have become more sophisticated, targeting increasingly critical infrastructure and manufacturing sectors [2]. Small and Medium-sized Enterprises (SMEs) face additional challenges due to limited cybersecurity resources. IBM's Cost of Data Breach Report 2025 [3] found that the average cost of a data breach was 4.44 million USD in the period between March 2024 and February 2025. The report also highlights that the average cost of a data breach has risen for IoT and OT by 175, 010 USD compared to the previous year. The financial impact extends beyond direct expenses, affecting customer trust, reputation, and competitive advantage. As cybercrime continues to escalate, organizations must adopt structured security approaches to protect their IT-OT environments [4].

A widely adopted architectural baseline is the Purdue reference model [5], which segments industrial networks into distinct functional levels. The lowest levels describe the

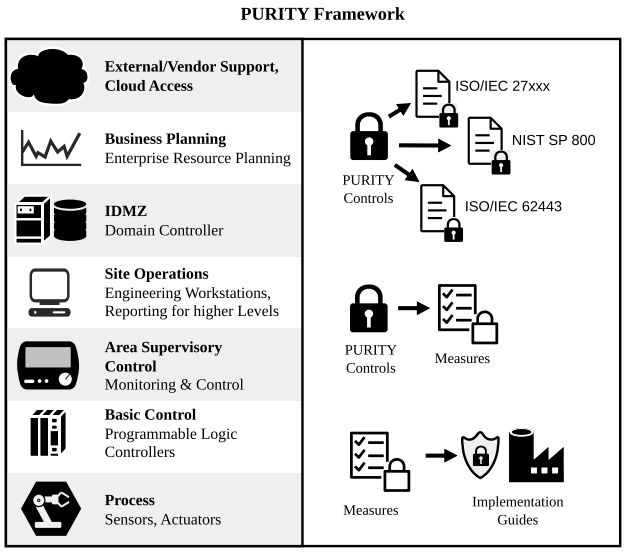

FIGURE 1. The PURITY framework mapped onto the Purdue model, demonstrating how security controls derived from ISO 27000 series, IEC 62443, and NIST SP 800-82 are systematically translated into level-specific measures and implementation guides. This three-layer mapping is the core mechanism by which PURITY bridges the gap between abstract standard requirements and actionable, SME-accessible guidance across all industrial network zones.

physical processes and basic control (Levels 0-1), progressing through supervisory control and site operations (Levels 2–3), and ultimately reaching with enterprise IT and external access (Levels 4–5). The model is commonly extended to also include an Industrial Demilitarized Zone (IDMZ) which acts as a buffer zone between OT and IT systems [6] and is added between Level 3 and Level 4. Securing both domains is essential, as OT systems increasingly interconnect with IT infrastructure, meaning that a compromise in either domain can propagate laterally and disrupt operations, endanger physical processes, or result in significant financial damage [7].

While contemporary standards such as IEC 62443, and NIST SP 800-82 include this model, existing work has not fully translated these controls into level-specific, SME-accessible guidance. This gap motivates PURITY.

B. CONTRIBUTIONS

PURITY addresses this critical gap by investigating established technical and organizational cybersecurity standards across all Purdue levels, guided by the following research questions (RQs).

- **RQ.1** *How can SMEs connect their current IT and OT infrastructure, while implementing safeguards and following security best practices?*
  Our developed framework, *PURITY*, provides SMEs with a structured list of security controls per level of the Purdue model. These security controls are further referenced to the controls mentioned in the analyzed standards to provide traceability.
- **RQ.2** *How can these measures be grouped, and prioritized based on (cost-)effectiveness?*
  We group security controls of various standards and further discuss their prioritization in the form of enhancements similar to IEC 62443.
- **RQ.3** *How can companies having IT and OT infrastructure, where cybersecurity is not the main focus area of operation, attain secure information flow with minimal resources?*
  We provide best practices and configuration guidelines for common IT and OT hardware. These tools demonstrate how to effectively elevate system security.

We contribute to the general understanding of the necessity of cybersecurity in a heterogeneous digital infrastructure. The following list summarizes the key contributions of this article:

- **Development of the PURITY framework**: Establishing a structured, layered security model that integrates heterogeneous industry standards (ISO 27001, IEC 62443, NIST SP 800-82) into the classic Purdue hierarchy (see Figure 1).
- **Mapping of security controls to Purdue levels**: Providing a comprehensive cross-reference that assigns specific technical and organizational controls from multiple standards to each functional layer of the OT system.
- **Actionable implementation guidelines**: Translating abstract security requirements into practical implementation measures tailored for SMEs.
- **Definition of an IT-OT security baseline**: Identifies a converged network security foundation to mitigate the risks of lateral threat movement between enterprise and production zones.
- **Traceability and compliance facilitation**: Enables practitioners to trace recommended measures back to authoritative international standards, simplifying the auditing and compliance processes for industrial cybersecurity.

There are works which cover the bridge between IT and OT like the Cisco and Rockwell's Converged Plantwide Ethernet (CPwE) architectures [8], standards for OT security and architecture like NIST SP800-82r3 [6] or IEC 62443 [9], and various standards for information security either technical or organizational like ISO 27001 [10] or NIST SP 800-53 [11]. However, there is, to the best of our knowledge, no comparable work which maps these security controls to the individual levels of the Purdue model and further discusses how the identified measures can be implemented.

C. ORGANIZATION

This article is organized as follows: Section II provides background on cybersecurity concepts, risk management, and related work, including the Purdue model and relevant security standards. The methodology that is used to identify common security controls from the selected security

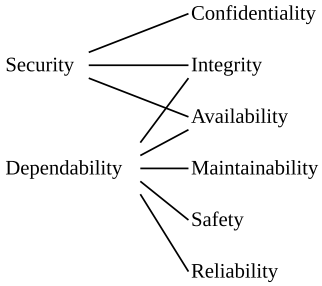

FIGURE 2. Relationship between Security (CIA triad) and Dependability attributes (reliability, safety, maintainability) in cyber-physical systems [12, p. 4]. Understanding this interdependence is foundational to PURITY, which must balance traditional IT security priorities against the availability- and safety-first constraints characteristic of OT environments at the lower Purdue levels.

standards and the development of security guidelines in form of security measures is described in Section III. Section IV presents the *PURITY* framework which examines each level of the Purdue model, describes typical systems, devices, and risks. The core contribution of the framework is presented in form of tables, which systematically map security controls from various standards to the control groups identified in our work, giving practitioners actionable guidance for each system level. Thereafter, Section V introduces a converged network security baseline, which we recommend practitioners to adopt as a minimum foundation for securing modern industrial environments. Finally, Section VI summarizes the key findings and concludes this work.

II. BACKGROUND AND RELATED WORK

To provide a better understanding of the challenges for integrating security controls in IT-OT systems, we first introduce the fundamentals of security and compare it to the system requirements of OT systems followed by the introduction of the Purdue model. Thereafter, we cover risk management essentials and end this section with related work.

A. FUNDAMENTALS OF SECURITY

Security aims to protect an organization's ability to continue its business activities, operations, and existence despite cyberattacks, data theft, compromised assets or manipulation of logical elements. It encompasses technical, organizational, and procedural measures to ensure *confidentiality*, *integrity*, and *availability* (CIA), forming the foundation of cybersecurity principles (see Figure 2). Confidentiality ensures information is accessible only to authorized entities through measures like encryption, secure storage, and access controls. Integrity guarantees data accuracy and prevents unauthorized modifications, incorporating accountability and non-repudiation. Availability ensures timely, uninterrupted resource access through, for instance, redundancy, bandwidth management, and access control [13].

In practice, the CIA properties are interdependent, for instance, a compromise of integrity (e.g., corrupted data) can indirectly affect availability. Moreover, IT security traditionally prioritizes the CIA triad, whereas OT prioritizes availability and integrity (also called the AIC triad) to ensure operational continuity and safety, as recommended by NIST SP 800-82 [6]. The PURITY framework accommodates this by explicitly addressing availability constraints in its lower OT levels while maintaining comprehensive coverage across all Purdue levels.

The key goals of security in an enterprise include:

- **Business Continuity**, which ensures the organization maintains critical business operations during reduced infrastructure capabilities caused by cyberattacks, natural disasters, or other disruptive events [13].
- **Disaster Recovery**, aiming at complementing business continuity, focuses on specific tactical strategies such as system recovery procedures, data backups, and fault tolerance mechanisms aimed at quickly restoring operational capabilities after disruptive events [13, p.115].
- **Operational and Cost Effectiveness**, evaluating the security strategy's performance both in operational terms and in terms of cost-benefit. Operational effectiveness assesses how well security measures support organizational objectives, whereas cost-effectiveness ensures security investments are justified proportionally to its benefits. Organizations must continuously plan, measure, review, and refine security measures according to ISO 27001 [10, pp. 7-10].
- **Security Posture**, encompassing risk management, governance and compliance, incident response, and vulnerability management, provides a comprehensive view of an organization's cybersecurity strategy and its ability to withstand and respond effectively to cyber threats. It evolves dynamically with changes in the organizational environment [14].

The concept of CIA has become widely recognized and established in IT security, while OT security, though increasingly recognized, remains less standardized and more operationally constrained than its IT counterpart. Unlike IT systems, OT security must also factor in reliability, physical safety, maintainability in addition to high availability and integrity. These attributes, commonly referred to as *dependability*, are illustrated in Figure 2. Reliability refers to the system's ability to perform its intended function without failure for a defined period. Safety focuses on preventing failures that could impact life or property and minimizing catastrophic consequences. Maintainability ensures that maintenance or service actions can be conducted efficiently within a specified time frame [15], [16].

IT security strategies can be adapted to industrial settings, however, their application must account for OT constraints like real-time and availability requirements and the use of legacy infrastructure. OT environments have evolved from isolated, proprietary systems to interconnected networks incorporating Commercial Off-The-Shelf (COTS)

TABLE 1. Functional and logical partitioning of the industrial network according to the Purdue model, serving as the architectural baseline for subsequent PURITY [17, pp. 3-7], [6, p. 85], [18, p. 92], [19, pp. 17-23].

Type	Purdue Level	Logical Layer	Description	Functional Layer
IT	Level 5	External / Vendor Support, Cloud Access	This level is close to the internet and is partially accessible through the Internet Demilitarized Zone. It includes assets like web servers, remote access, guest Wi-Fi or vendor login portals.	Business / Enterprise Network Zone
	Level 4	Business Planning and Logistics	This level is the IT intranet. It comprises application servers, email servers, databases, internal network access points, workstations, and IT authentication servers.	Business / Enterprise Network Zone
	IDMZ	Industrial Demilitarized Zone	The IDMZ allows to securely connect networks with different security requirements and prevents lower level systems from direct exposure.	Security perimeter
OT	Level 3	Site Operations	This level manages site-level operational control of machines and data is gathered for reporting to higher levels. Systems in this level include database/application/file servers, and engineering workstations.	Manufacturing Operations and Control Zone
	Level 2	Area Supervisory Control	In this level control or supervising systems are located. These systems are responsible for organizing machine operations. Examples are Human-Machine-Interfaces (HMIs) or Supervisory and Data Acquisition (SCADA) systems.	Operational Technology / Machines
	Level 1	Basic Control	Level 1 consists of machine control devices like Programmable Logic Controllers (PLCs), Variable Frequency Drives (VFDs), and other controllers.	Operational Technology / Machines
	Level 0	Processes	Level 0 devices include physical hardware, such as motors, pumps, valves, and sensors.	Operational Technology / Machines

technology [9]. This integration of COTS enhances business operations but also introduces new vulnerabilities, requiring tailored security strategies.

Another critical aspect of OT systems is time sensitivity. OT systems control physical processes where real-time responsiveness is essential. Synchronized operations must be maintained, as security controls like firewalls, access restrictions, or encryption may introduce latency. Therefore, security measures must be carefully tested to prevent operational disruptions.

B. PURDUE MODEL

The Purdue reference model [5] provides a structured approach for designing industrial networks by segmenting them logically into different zones. Its practical proposals and level of detail not only provide a structured approach for designing and securing industrial networks but also integrating information and management systems of classical IT [17]. The *SANS Institute* describes the Purdue model to provide a solid foundation for secure ICS architectures but highlights that it requires the integration of additional controls to meet current standards [20]. A modified Purdue model which already includes an IDMZ is described in Table 1. The table highlights the boundary between IT and OT which lies between Purdue Levels 3 and 4. In this representation the IDMZ forms the zone separating the two technologies by providing access for IT systems to data historians and engineering workstations. Conversely, systems below the IDMZ, OT systems, feed the data historian with data and can be accessed through engineering workstations.

Contemporary frameworks such as *IEC 62443*, *NIST SP 800-82*, and *ISO/IEC 27033* build on this foundation by introducing detailed, risk-based controls [20], [21]. When used alongside the Purdue model, they enable the development of robust and adaptive security architectures.

C. RISK MANAGEMENT

Security controls should be selected and applied based on their potential to deliver the highest risk reduction relative to effort and cost, thereby optimizing the organization's security posture. To ensure that security measures are both effective and resource-efficient, their selection should be grounded in a structured risk management process that aligns with the organization's specific threat landscape and operational priorities.

Risk management is the process of identifying, assessing, and analyzing factors that could negatively impact an organization's ability to generate revenue or achieve its (business) objectives. It enables organizations to prioritize and implement security measures that reduce operating risk to an acceptable level. This threshold varies by organization, depending on factors such as maturity, criticality of assets, and risk appetite. The latter is defined as the level of risk an entity is willing to accept, whether risk-seeking, neutral, or averse [13]. Risk is, for instance, defined by Chapple et al. [13] in the formulas

$$risk = threat \cdot vulnerability$$

or

$$risk = probability\ of\ harm \cdot severity\ of\ harm,$$

where risk is the probability that a threat or harm will exploit a vulnerability to cause damage to a physical, informational, or financial asset.

In general, the risk evaluation process can be divided into a qualitative or quantitative approach. Qualitative techniques rely on descriptive terms to characterize the likelihood of an event and its consequences. The resulting risk is commonly expressed in terms of high, medium and low, however, the qualitative approach is subjective and can be influenced by the person(s) evaluating the risk and their knowledge about either the asset, the threat or the environment.

Quantitative risk assessment, on the other hand, uses numerical values to represent the likelihood of an event and its consequences which would allow for a more precise measurement of risk than qualitative analysis. Nevertheless it depends on the accuracy and availability of data. The quantitative approach is more complex and requires more data to conduct the evaluation. It is carried out using formulas and statistical methods to calculate the risk. Quantitative risk assessment requires also more time and does not factor in non-quantifiable factors [22].

While there are modern quantitative frameworks such as FAIR [23] which can handle uncertainty through probabilistic modelling, their data requirements and complexity make them less accessible for SMEs. Therefore, this work adopts a qualitative approach as a practical compromise.

1) RISK MANAGEMENT METHODS–EXAMPLES

A typical qualitative approach is to utilize a risk matrix based on likelihood and impact. A risk level is determined based on the impact and likelihood. This risk level is then used to determine the priority respectively urgency of mitigating the threat. Figure 3 highlights how the priorities should be chosen, giving higher priorities to threats having a high risk level followed by medium risk to low. In addition, the blue dashed line separates low risk levels from the higher ones highlighting that some of these threats may be accepted.

The quantitative method to risk management is detailing the impact of risks based on probabilities and effects on the company. Following Chapple et al. [13], so-called Annualized Loss Expectancies (ALEs) are calculated. This requires the company to determine the Asset Values (AVs) and the Exposure Factors (EFs) of an asset. The EF determines the percentage of the asset's value lost if an incident occurs. By multiplying the AV with the EF the Single Loss Expectancies (SLEs) can be derived. To scale the SLE for one year and to determine the ALE, it must be multiplied with the Annual Rate of Occurrences (AROs). The ARO is the likelihood of an incident occurring in a year, which can be based on statistical and historical data or be assumed by experience [13].

D. RELATED WORK

Several standards and norms exist for IT security where technical and procedural measures are listed, as well as holistic approaches are made. Industry standards like the ISO/IEC 27000 series define information security management systems and detailed technical controls, while NIST SP 800 series offers an extensive catalog of security and privacy safeguards as well as deeper dives into specific IT security topics like network or application security or patch management. For OT security, Cisco and Rockwell's Converged Plantwide Ethernet (CPwE) architectures [8] and the IEC 62443 series offer guidance while the Purdue model (see Table 1) provides an architectural approach to connect IT and OT. Additionally, the CIS Controls [25] provide a prioritized set of practical security actions widely adopted across both IT and OT environments, and are referenced in this work complementarily.

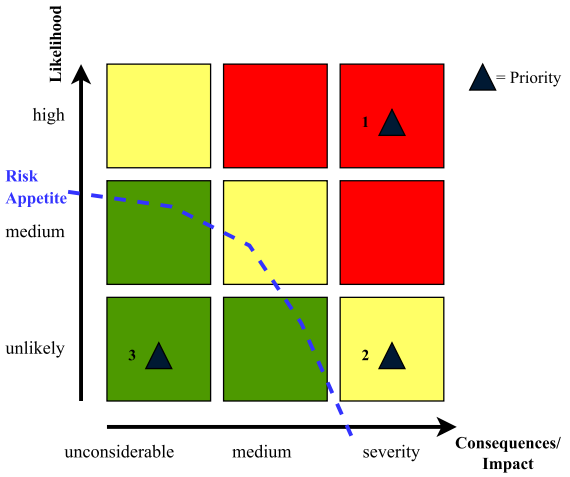

FIGURE 3. Qualitative risk prioritization matrix used within the PURITY methodology to rank threats by likelihood and consequence, adapted from [24, p. 146]. By distinguishing three priority tiers and explicitly marking the risk-appetite boundary (dashed line), this matrix guides SMEs in allocating limited security resources to the controls where risk reduction is greatest, thereby guiding the prioritization of PURITY controls across the full Purdue hierarchy.

Notably, the core CPwE Design and Implementation Guide, last updated in 2011 [8], predates many contemporary OT threats and standards revisions, further motivating the need for an up-to-date, standards-aligned security framework such as PURITY. The IEC 62443 addresses the security of OT systems holistically and defines requirements derived from its risk-based methodology, but it provides limited guidance on the concrete realization of these requirements. Furthermore, it does not cross-reference or map to complementary standards that SMEs are commonly required to comply with, such as ISO 27001 or NIST SP 800-82. Similarly, the ISA Global Cybersecurity Alliance white paper [26] describes the relationship between IEC 62443 and ISO 27001 and ISO 27002, demonstrating how both standards can be applied complementarily within a single organization. While this work provides valuable conceptual alignment, it does not associate security controls with specific Purdue levels nor provides actionable implementation guidance tailored to SMEs.

Comparative research studies [27], [28] explore the relationship between standards highlighting overlaps and differences. While useful, these mappings are on a high level. For instance, Djebbar and Nordström [27] map various industrial cyber security standards to ISO/IEC 27001 and 27002. Voicu [28] follows a similar approach and aims to combine ISO/IEC 27001 and 27002 with IEC 62443. In contrast, we further advance such a mapping by directly associating the requirements, respectively controls with the specific levels of the Purdue model where they are needed. Furthermore, we provide detailed implementation guidance through security measures mapped to relevant controls.

III. METHODOLOGY

The PURITY framework aims to provide a holistic security approach for Information Technology-Operational Technology (IT-OT) convergence through a structured, standards-based methodology. The methodology leverages the ISO/IEC 27000 series, NIST SP 800 series, and IEC 62443 as its primary reference standards. The rationale for their selection is detailed in Section III-A.

A. CONTROL SELECTION CRITERIA

The inclusion, applicability mapping, and prioritization of security controls in PURITY are governed by the following criteria.

1) INCLUSION CRITERIA

A control was included if it satisfied at least one of the following conditions: (i) it is mandated or recommended by one of the four reference standards, i.e., ISO/IEC 27001, ISO/IEC 27033, IEC 62443, and NIST SP 800-82; (ii) it directly mitigates a threat vector identified during the level-specific risk analysis described in Step 2 of the methodology (see Section III-B and Figure 4); or (iii) it is technically feasible within the resource and operational constraints typical of SMEs.

Controls were excluded if they required infrastructure or expertise that is unrealistic for the target organizations, or if an equivalent control already present in the set rendered them redundant.

2) APPLICABILITY TO PURDUE LEVELS

Each candidate control was evaluated against the asset types, and threat vectors documented for each Purdue level (Step 2 of the methodology). A control was assigned to a level if the assets (or processes) at that level are directly exposed to the threat the control mitigates. Controls whose scope spans multiple levels, for instance, asset inventory or incident response, were assigned to all relevant Purdue levels, with level-specific implementation measures providing the contextual differentiation (see Step 7).

3) PRIORITIZATION

Controls were prioritized using the qualitative risk matrix introduced in Section II-C (see Figure 3). A control received *Priority 1* if the residual risk without it was rated high; *Priority 2* for medium residual risk; and *Priority 3* for low residual risk. Where two controls addressed the same threat, the one with the lower implementation effort for SMEs was assigned the higher priority. The final set of 99 mappings are the result of a review by a co-author with ten years of OT cybersecurity research experience, whose feedback led to the addition of nine controls and the removal of five from the initial set of 93 controls.

B. CONTROL IDENTIFICATION AND MAPPING PROCEDURE

Building on the selection criteria defined in Section III-A, the following seven steps operationalize the development of PURITY by systematically extracting, evaluating, and mapping security controls to the individual levels of the Purdue model, as illustrated in Figure 4.

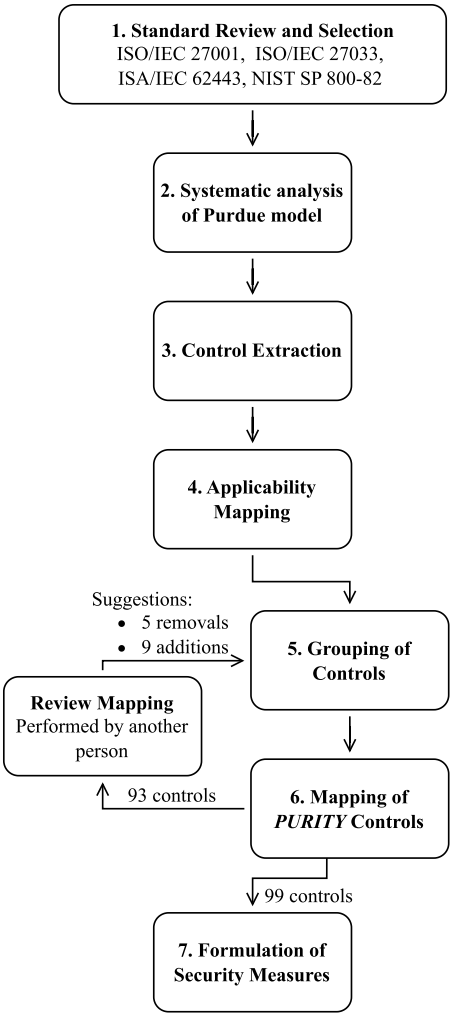

FIGURE 4. Flowchart illustrating the seven steps methodology applied in PURITY. Starting with an initial review and selection of standards and ending with the creation of the PURITY framework linking to grouped controls and measures applicable for SMEs.

1) **Review and selection of internationally recognized security standards**
The standards are selected based on their international recognition, relevance, and practical guidance. Note that further standards and guidelines are added as a reference, e.g., NIST SP 800-167 [29] due to its relevance as a guide to application whitelisting.

2) **Analysis of each Purdue level**
For each Purdue level, the OT and IT characteristics, constraints, and risks are documented. Furthermore, the typical assets, systems, and devices found at each level are identified. Based on the gathered information, the level-specific security risks and threat vectors are analyzed. Finally, the differing requirements between IT and OT environments are explicitly considered.

3) **Extraction of security controls in a unified structure**
For each standard, the security requirements and their applicability to a given Purdue level are reviewed, the corresponding control identifiers, descriptions, and objectives are documented, and the relevant technical as well as organizational measures are extracted.

4) **Risk evaluation of each Purdue level based on expert expertise**
Controls are matched to level-specific threats to achieve risk mitigation, their technical feasibility is reviewed with particular attention to OT constraints, and their implementation effort and tooling needs are evaluated to understand resource requirements.

5) **Grouping of security controls into five distinct categories**
The identified security controls are organized into five categories, namely *Network Security* (segmentation, firewalling, encryption), *Access Control* (authentication, authorization, privilege management), *System Hardening* (configuration, patching, vulnerability management), *Monitoring and Detection* (logging, SIEM, incident response), and *Physical Security* (access control, environmental protection).

6) **Establishment of PURITY controls and links to security controls by standards**
Cross-reference tables are created that (i) map PURITY security controls to the corresponding standard controls, and (ii) document the associated control IDs and standard sections. These tables enable practitioners to trace requirements back to authoritative sources and to support compliance verification and audit processes.

7) **Development of security measures for SMEs**
In this last step, the measures are developed and mapped to the corresponding security controls, completing the framework by grouping multiple controls that can be addressed simultaneously by a single measure to increase resource efficiency, providing complementary measures where appropriate, and conducting a feasibility review of all measures with a particular focus on SME constraints.

The assessments are based on the authors' professional experience in cybersecurity working in the field as security consultant for 5 years as well as suggestions and recommendations by cybersecurity studies and reports referenced in this work. For evaluating the mappings of controls to referenced standards, one of the co-authors, a researcher working in OT cybersecurity research for 10 years reviewed the references. Out of the initial set of 93 mappings the researcher suggested adding 9 more controls and removing 5 from the initial set. The authors then discussed the changes and agreed on a final set of 99 mappings to relevant standards.

It should also be noted that certain security controls intentionally span multiple Purdue levels, as the underlying security requirements they address are architectural in nature and cannot be meaningfully confined to a single level. The level-specific realization of such controls is addressed through the corresponding implementation measures, which provide concrete, context-sensitive guidance for each layer of the industrial network.

C. APPLICATION EXAMPLE OF THE PURITY FRAMEWORK IN SMALL AND MEDIUM-SIZED ENTERPRISES

To illustrate the practical implementation of the PURITY framework in SMEs, this section considers a small metal-working company. During the application of the framework, the analyst identifies that, according to IM1.1 (see Table 5), Layer 1 network components should be separated from devices not belonging to this category. It is recommended to apply logical segmentation for example with Virtual Local Area Networks (VLANs). Given that the company's network architecture is flat and its two only PLCs currently reside in the same network segment as other IT components, a dedicated VLAN is established for the PLCs, and the devices are migrated into this segment. The firewall separating the VLANs is subsequently configured to permit only the strictly necessary traffic required for PLC configuration from the designated management workstation. These measures, which require little effort given the size of the enterprise, ensure compliance with Security Controls C1.1.0 and C1.1.1 (see Table 4), thereby satisfying the corresponding requirements derived from the underlying security standards. It is self-evident that the effort required to implement such measures depends on the size and complexity of the underlying infrastructure and organizational structure.

IV. PURITY FRAMEWORK

The *PURITY* framework follows the structure of the Purdue model (see Section II-B). PURITY identifies for each Purdue level security controls and their corresponding security mechanisms needed to cover basic security demands to assure

TABLE 2. Security baseline for Level 0 (Processes), focusing on asset visibility and environmental protection to mitigate physical tampering and local denial-of-service risks.

Control ID	Control Name	Description	Reference Standards
C0.1.0	Asset Inventory	The organization must establish and maintain a system or information database where all relevant assets are listed. In the network context these assets may be network devices, such as switches, routers, access points, or simple ports distributed in production premises.	ISO 27001 [10] Ctrl. 5.9, NIST SP 800-53r5 [11] CM-8, NIST SP 800-82r3 [6, sec. 6.1.1]
C0.1.1	Asset Ownership	For the identified assets, an owner should be assigned and a use case context established. Implementing these measures ensures that there is information for critical assets and appropriate measures can be planned accordingly with the asset owner.	ISO 27002 [30] Ctrl. 5.9
C0.2.0	Prevent Physical DoS	The organization must take measures to prevent a Denial-of-Service (DoS) attacks by physical means.	IEC 62443-3-3 [31] RA SR 7.1
C0.2.1	Secure Areas	The organization must ensure that access to sensitive areas is only allowed to authorized persons. These sensitive areas may be server rooms, machine control interfaces, or offices.	ISO 27002 [30] Ctrl. 7.1
C0.2.2	Physical Access Control	The organization should implement a physical security system which controls access to sensitive areas. This may include access control systems, video surveillance, or security personnel.	NIST SP 800-82r3 [6, sec. 5.2.2, 6.2.1.2], NIST SP 800-53r5 [11] PE-3, PE-6
C0.2.3	Equipment Security	The organization must ensure that relevant network equipment is sited securely and protected. This includes the physical separation from equipment managed by partners and not by the organization.	ISO 27002 [30] Ctrl. 7.8
C0.2.4	Power Equipment and Cabling	Cabling and power equipment must be installed in a secure and safe way. The organization must ensure that redundancy is implemented to ensure reaching the availability target for critical and high-value assets.	NIST SP 800-53r5 [11] PE-9, PE-11, IEC 62443-3-3 [31] RA SR 7.5

TABLE 3. Practical implementation measures for Level 0 (Processes) to provide physical asset tracking and perimeter reinforcement, and to ensure hardware integrity.

ID	Security Measure	Description	Covered Controls
IM0.1	Implement an Asset Management System	The organization should implement a central asset management system to track all assets. This may be done manually; however, modern asset management solutions offer advanced features. Each asset should have an assigned owner - either a person or department – and its physical location recorded. Optionally, a network sniffer may be used to automatically detect assets via network traffic [32], [11, pp. CM–8], [30, p. 5.9].	C0.1.0 C0.1.1
IM0.1.1	Hardware and Physical Layout	To complement measure IM 0.1, the organization should maintain a detailed inventory of all hardware, including floor plans and cabinet layouts. Items should be clearly labeled and follow a standardized labeling scheme. A reference example is provided in [33, Annex B.1.5].	C0.1.0 C0.1.1
IM0.2	Implement Physical Access Control	Access should require identification-based authentication. Physical perimeter defenses such as a Physical Access Control System (PACS), which restricts entry to sensitive areas by authenticating users through credentials such as smart cards or biometrics, should be implemented to limit access to secure areas [6]. Further guidance can be found in IEC 62443-3-2 [34, ZCR3, 1–3.6]. It is also recommended that sensitive equipment and cabling is physically protected, for instance by limiting accessibility through building infrastructure [11, PE-4].	C0.2.0 C0.2.1 C0.2.2 C0.2.3 C0.2.4

a security baseline for SMEs. The presented security controls are an aggregation of security controls identified by various standards and transparently mapped in the respective tables.

A. LEVEL 0-THE PHYSICAL PROCESS

At Level 0 of the Purdue model, the focus lies on the physical process, which includes sensors, actuators, and safety-critical devices that directly interact with industrial operations. Due to the variability in processes, this section concentrates on security measures concerning the devices that execute the process, emphasizing their physical protection and the environmental context in which they operate. Risks in Level 0 primarily arise from unauthorized physical access or manipulation of devices. These include threats that can directly compromise safety and operational integrity, like tampering, destruction, or DoS [35].

1) THE RISK OF SAFETY SYSTEMS

Industrial machines are often required to implement some sort of safety system to protect human operators from harm. These safety systems may be implemented in form of Emergency Shutdown (ESD) systems, which are designed to stop machines in case of an emergency. If these systems are not secure, they can be exploited to shut down machines

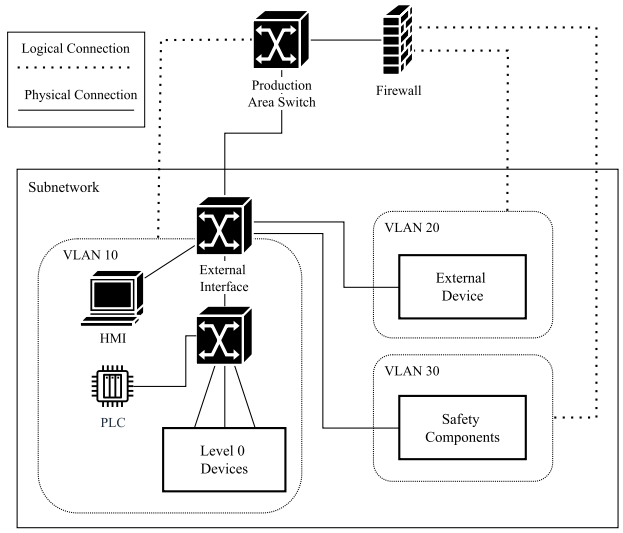

FIGURE 5. Practical application of VLAN-based segmentation at Level 1, demonstrating the isolation of safety-critical components from external interfaces via firewall policy enforcement.

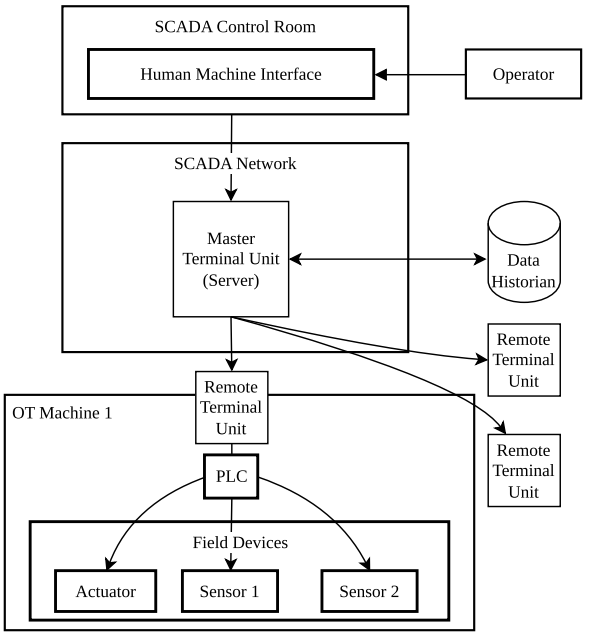

FIGURE 6. Typical SCADA architecture implementation at Level 2, illustrating the logical hierarchy of main and remote terminal units required to establish centralized monitoring and data acquisition [41].

in non-emergency situations, causing a DoS attack. Another attack scenario is that the safety system is disabled, resulting in machines not shutting down when required, or in the intended way, causing a safety risk for the operators and potential danger to humans [36].

The controls outlined in Table 2 define foundational security requirements for Level 0 devices and infrastructure. To support the practical implementation of these controls, Table 3 presents corresponding technical and organizational measures that organizations can adopt to mitigate identified risks and improve the overall security posture at the physical layer.

B. LEVEL 1-BASIC CONTROL

Basic control systems are located in Purdue Level 1. These systems, for example, PLCs, are responsible for the direct perception via sensors and control of actuators to manipulate the physical processes. The PLCs get their input from Level 2 and translate it downwards, e.g., through I/O (Input and Output) channels. The control devices may also be called *Equipment Under Control (EUC)*. It is of critical importance that no disruption, disturbance, or noise affects these devices, as it can impact production and escalate to disrupt all operations [36, p. 21].

1) LEVEL 1 RISKS

Some risks associated with this level are [35], [37], [38]:

- Manipulation of PLCs
- Software/Firmware vulnerabilities
- Lack of encryption in communication
- Exposure of network interfaces

At Level 1 security focuses on protecting core automation components responsible for direct process control, such as PLCs and I/O devices. The controls listed in Table 4 address critical aspects like secure communication, firmware integrity, and hardware life-cycle management. To translate these requirements into actionable steps, Table 5 provides implementation-oriented measures designed to help organizations reduce risk exposure at the control layer. These measures take into account both the technical limitations and operational constraints of industrial control systems.

2) IM 1.1 NETWORK SEGMENTATION

The security measure IM1.1 (see Table 5) is applied on an OT-system housing different components as shown in Figure 5. The components are segmented into different VLANs, logical network partitions that group devices independently of their physical location and restrict communication to authorized paths, to ensure that the communication between them is separated [6]. The VLANs are connected through a firewall which ensures that only the necessary communication is allowed. For example, external devices from VLAN 20 should not communicate with the safety components in VLAN 30 in order to not interfere with their operation. Similarly, devices in VLAN 10 are responsible for the correct functioning of the production but may need some information from external devices in VLAN 20. By using the firewall, this communication can be controlled and monitored. Security policies can be applied and traffic which does not comply with the policies or has malicious attributes can be blocked and an alert created.

C. LEVEL 2-AREA SUPERVISORY CONTROL

The area supervisory control level contains systems that are responsible for organizing machine operations and

TABLE 4. Security baseline for Level 1 (Basic Control), emphasizing firmware integrity and secure communication to protect Level 1 PLC operations.

Control ID	Control Name	Description	Reference Standards
C1.1.0	Segmentation of Communication	The organization must ensure that the communication of Level 1 devices is reasonably segmented from other network components. Segmentation measures must be implemented until an acceptable cost-to-risk balance is reached. OT focused guidance is provided in NIST SP 800-82r3 [6].	NIST SP 800-53r5 [11] SC-7, IEC 62443-3-2 [34] ZCR 3.2, IEC 62443-3-3 [31] RDF SR 5.1
C1.1.1	Control Communication to External Networks	If external network communication is required at this level, appropriate controls must be implemented. The organization should also evaluate whether such communication can be shifted to a higher network level.	ISO 27002 [30] Ctrl. 5.14, IEC 62443-3-3 [31] IAC SR 1.13
C1.2.0	Encrypted Communication	Encrypted communication measures should be implemented to protect data in transit at Level 1.	IEC 62443-3-3 [31] DC SR 4.1, ISO 27002 [30] Ctrl. 8.24
C1.2.1	Firmware Updates	Devices at Level 1 should undergo regular checks for firmware vulnerabilities and be updated accordingly.	ISO 27002 [30] Ctrl. 8.8
C1.2.2	Firmware Update Verification	Firmware updates must be verified for authenticity to ensure they have not been tampered with prior to deployment.	NIST SP 800-53r5 [11] SI-7
C1.2.3	Secure Firmware Configuration	Many Level 1 devices have insecure factory default settings. These should be reviewed and secured, including changing default credentials.	IEC 62443-3-3 [31] IAC SR 1.2 RE 1, ISO 27002 [30] Ctrl. 8.9(f), NIST SP 800-82r3 [6] AC-3, NIST SP 800-53r5 [11] CM-9
C1.2.4	Hardware Upgrades	When hardware becomes unsupported, fails, or lacks firmware updates, organizations must assess whether the risk of continued use is acceptable or whether hardware upgrades are necessary. It must be reviewed if the continued use may evolve in a dependency bottleneck.	NIST SP 800-53r5 [11] SA-3

TABLE 5. Actionable security measures for Level 1 (Basic Control) devices, detailing VLAN-based segmentation, and firmware verification processes to maintain real-time automation stability.

ID	Security Measure	Description	Covered Controls
IM1.1	Network Segmentation	The organization should segment Level 1 network components from other systems or external entities. Logical segmentation (e.g., VLANs) is recommended. As network traffic in OT can be difficult to classify, temporarily allowing and logging all communication may help establish approved rulesets, however it must be taken into account that an active infection may be missed [6, p. 102]. Guidance: CIS Control 3.12 [39, p. 3.12]. See also Figure 5.	C1.1.0 C1.1.1
IM1.2	Encryption for External Traffic	Encryption should be applied to outbound traffic from the OT system. VPN technologies using TLS or IPsec are suitable for securing Level 1 communications [6].	C1.2.0
IM1.3	Evaluate Encryption Constraints	Encryption should be used when confidentiality or integrity is required, but limitations must be considered: *(1)* Time sensitivity: encryption latency may disrupt OT systems; *(2)* Processing power: embedded devices may lack resources; *(3)* Protocol limitations: common OT protocols like PROFIBUS, Modbus and CAN may not support encryption; *(4)* Impact on monitoring tools: encryption may reduce the effectiveness of anomaly detection [6], [40].	C1.2.0
IM1.4	Use Supported Hardware	Organizations should plan regular hardware refresh cycles to replace unsupported legacy equipment. If replacement is not possible, compensating controls at higher Purdue levels must be enforced [6].	C1.2.4
IM1.5	Secure Firmware Update Process	A process for verifying and applying firmware updates must be in place. This can be done via OEM tools, third-party patching platforms, or manually. Verification ensures integrity of the update[6].	C1.2.1 C1.2.2

data acquisition. Common examples are HMIs or SCADA systems. HMIs are visualizing data and allowing control of a single work cell or machine, as they are the interface through which an operator interacts. A SCADA system of an ICS is commonly linked to an HMI. It monitors, coordinates and controls entire processes or plants, rather than controlling a single machine [42]. Both systems can be based on general purpose operating systems like Windows or Linux, or standalone systems with proprietary software. Manufacturers, however, increasingly rely on COTS products [43]. While both proprietary and non-proprietary systems face the risk of software vulnerabilities, this risk is often less visible in proprietary systems, where vulnerability disclosure is typically more restricted.

An example architecture of a SCADA system in which the SCADA server is located in Level 2 is shown in Figure 6. These systems may also be found in Level 3, but in Level 2 they are targeted and scoped to a single area or machine [42]. Tables 6 and 7 summarize the

TABLE 6. Security baseline for Level 2 (Area Supervisory Control), highlighting the necessity of system hardening and wireless monitoring.

Control ID	Control Name	Description	Reference Standards
C2.1.0	Secure and Harden Control Systems	The organization must take measures to harden SCADA, HMI, and other control systems, as well as regularly update operating systems and networking devices.	NIST SP 800-82r3 [6, sec. 5.2.4]
C2.1.1	Whitelisting of Applications and Services	The organization must implement application whitelisting to prevent unauthorized software from running.	NIST SP 800-82r3 [6, sec. 5.2.5], NIST SP 800-167 [29][a]
C2.2.0	Network Segmentation	The organization must implement network segmentation to separate single-machine zones from other zones.	NIST SP 800-82r3 [6, sec. 5.2.3.1], ISO 27033-3 [44, chap. 11]
C2.3.0	Secure Wireless Network Access	The organization must secure wireless networks by enforcing authentication policies, encrypting traffic, and monitoring for unauthorized access. These controls ensure confidentiality and integrity across wireless communication channels.	ISO 27033-6 [45], IEC 62443-3-3 [31] UC SR2.2, IAC SR1.2, DC SR4.1

[a]The *National Institute of Standards and Technology* has published a specialized guide for *Application Whitelisting*, applicable to OT and IT environments [29].

TABLE 7. Technical hardening and monitoring measures for Level 2 (Area Supervisory Control), focusing on mitigating COTS-related vulnerabilities within HMI and SCADA environments.

ID	Security Measure	Description	Covered Controls
IM2.1.0	Hardening of Operating System and Applications	The organization must establish device-level and computer security controls. This includes regular patching of operating systems and applications. Where patching is not feasible, compensating controls must be used. System hardening includes disabling unused services, closing unnecessary ports, and applying least privilege principles. CIS benchmarks are recommended[a].	C2.1.0
IM2.1.1	Network Device Maintenance	Ensure regular patching and secure configuration of network devices. Use CIS Benchmarks as a reference. Major deviations from benchmarks should trigger architectural reviews. Document and validate configurations against the security policy.	C2.1.0
IM2.1.2	Whitelisting and Blacklisting	OT systems allow static configurations, enabling strict application/service whitelisting. Use host-based controls (e.g., Windows AppLocker[b]), EDR, or firewalls. Combine multiple approaches for effective coverage.	C2.1.1
IM2.2.0	Network Segmentation	Implement segmentation between Level 2 and Level 3 systems to prevent unauthorized lateral movement.	C2.2.0
IM2.3.0	Wireless Network Security and Monitoring	Define and enforce wireless access policies. Apply measures such as WPA3, MAC filtering, captive portals, EAP-TLS, and disabling WPS. Separate guest/internal networks. Additionally, monitor wireless traffic via SPAN or other tools.	C2.3.0

[a]CIS Security Benchmarks: https://www.cisecurity.org/cis-benchmarks.
[b]AppLocker overview: https://learn.microsoft.com/en-us/windows/security/application-security/application-control/windows-defender-application-control/applocker/applocker-overview.

identified security controls and security measures for this level respectively.

1) LEVEL 2 RISKS

At Purdue Level 2 control software is introduced, requiring high availability and near-zero latency. As a result, the following risks to the Level 2 systems emerge [42, pp. 81-82], [41]:

- DoS attacks that overwhelm the network and consume most of the bandwidth
- Malicious software
- Improper application of software patches
- Interdependence with other networks
- Insecure network access
- Weak authentication
- Operating system vulnerabilities

2) LEVEL 2 NETWORK SECURITY IMPLEMENTATIONS

Networking devices found in Level 2 are mostly industrial switches, OT firewalls and remote terminal units.

a: REMOTE TERMINAL UNITS (RTUs)

RTUs are microprocessor-based devices that interface between SCADA systems and field equipment such as sensors and actuators. They include digital/analog I/O and communication modules [46]. RTUs often communicate via TCP/IP-based protocols like Modbus TCP/IP, which improves interoperability but introduces additional protocol vulnerabilities [47].

b: INDUSTRIAL SWITCHES

Industrial switches operate at OSI Layer 2 and enable LAN segmentation using VLANs. Compared to standard

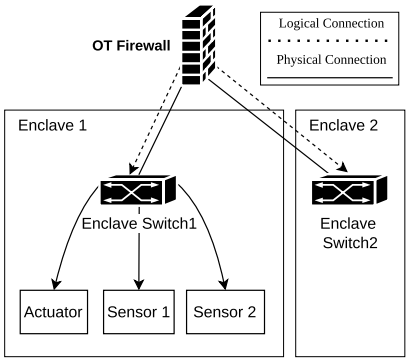

FIGURE 7. OT firewall architecture for enclave-based network security, demonstrating the logical isolation of automation equipment into secure subnets to control lateral traffic and minimize the impact of localized breaches [36, p. 136].

IT network switches, industrial variants are ruggedized, featuring metal housings, and resistance to dust, moisture, vibration, and extreme temperatures, meeting environmental standards such as IEC 61850-3 [48] for power plant and substation-grade deployments. IEEE 1613-2023 further explicitly mandates fanless cooling to ensure reliable operation without moving parts [49]. This makes them well-suited for deployment in factory floors, utility plants, and other demanding OT environments.

c: OT FIREWALLS

OT firewalls are built to support industrial protocols and meet the performance demands of OT systems. While they may lack the advanced features of next-generation IT firewalls, they offer reliable traffic filtering and basic policy enforcement suitable for harsh environments [50]. They are commonly used to segment networks through approaches like *network enclaving*, isolating critical assets to reduce exposure and enhance security [36].

> *Enclaves are logical subsections within the industrial network typically created by grouping related automation equipment into a subnet (VLAN) or a physically separate network connected via a firewall.* [36, p. 49]

d: ESTABLISHING ENCLAVES

Enclave formation involves grouping assets that share similar functional and logical requirements. Grouping should prioritize the most critical common characteristic, such as protocol, application, or service, even if devices support multiple. A clear understanding of asset functionality is essential, and simplifications may be necessary to identify a unifying trait. The rationale for each enclave must be documented, including the shared functionality and security needs, relevant threats, and justification for grouping. This serves as the foundation for subsequent risk assessments, defining security requirements, accepted risks, and control measures [51].

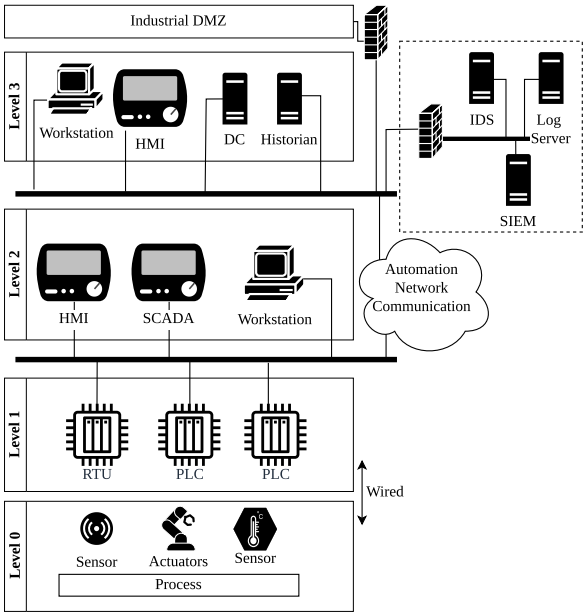

FIGURE 8. Integrated industrial zone layout demonstrating the centralized convergence of Level 0–2 automation data into Level 3 monitoring systems, facilitated by a secure, wired communication backbone for enhanced operational visibility [54, p. 335].

IEC 62443-3-2 defines the concept of *Zones and Conduits* as the primary mechanism for network segmentation in industrial environments. A zone groups assets with similar security requirements, while conduits define the controlled communication paths between zones [34]. The term enclave, as used in [36] defines enclaves as logical subsections of functionally related assets. Both concepts isolate assets based on shared assets and requirements.

The use case of OT firewalls is not limited to Purdue Level 2, but can also be found in Level 3. An exemplary architecture implementing an OT firewall is shown in Figure 7.

D. LEVEL 3-SITE OPERATIONS

Level 3 represents the central control layer of an industrial environment, where data from lower levels is aggregated for supervisory monitoring. It typically includes HMIs and terminals in a control room setup, enabling operators to oversee production status, quality metrics, and performance. Only systems essential to production should reside in this level; non-critical systems belong to enterprise IT.

Level 3 key components include domain controllers, directories, and data historians, which are logically and often physically separated from enterprise networks to maintain authentication integrity and limit access risks [36, p. 20]. The data exchange with higher levels typically occurs via push or pull methods through the IDMZ. Figure 8 further illustrates key elements in OT systems up to Level 3.

The identified security controls from standards are further grouped and referenced in Table 8. The security measures, addressing the risks in this level can be found in Table 9.

TABLE 8. Security baseline for Level 3 (Site Operations), aiming to prevent lateral movement and securing data-driven decision-making through API and integrity controls.

Control ID	Control Name	Description	Reference Standards
C3.1.0	API Security	All application interfaces must enforce strict authentication and authorization for users and software.	IEC 62443 3-3 [31] IAC SR1.1, SR1.2, NIST SP 800-53r5 [11] IA-2, IA-9
C3.1.1	Secure Coding Practices	Software must be developed following secure coding standards, such as NIST SSDF[a].	NIST SP 800-218 [52], ISO 27002 [30] Ctrl. 8.28
C3.2.0	Lateral Movement Prevention	Apply Defense-in-Depth (DiD) with segmentation, access controls, Intrusion Detection and Prevention System (IDPS), and logging to prevent internal propagation.	NIST SP 800-53r5 [11] AC-3, IR-4, SI-4, ISO 27002 [30] Ctrl. 5.15
C3.3.0	Data Integrity Controls	Ensure the correctness of live data used for operational decisions through integrity checks and validation.	IEC 62443 3-3 [31] SI SR 3.4, NIST SP 800-53r5 [11] SI-7
C3.4.0	Emergency Access to Control Systems	Provide rapid access to critical systems in emergencies without compromising baseline security.	IEC 62443 3-3 [31] IAC SR 1.1

[a]Secure Software Development Framework: https://csrc.nist.gov/Projects/ssdf.

TABLE 9. Level 3 (Site Operations) security measures, emphasizing API access strategies, emergency access protocols, and the detection lateral movement.

ID	Security Measure	Description	Covered Controls
IM3.1.0	API Secure Access (User)	Secure API access for users should include Multi-Factor Authentication (MFA) using FIDO2 tokens or Time-based One-Time Password (TOTP), with contextual checks like location, device, or login time.	C3.1.0
IM3.1.1	API Secure Access (M2M)	For machine-to-machine access, use secure mechanisms like OAuth 2.0, JWT, or Mutual TLS with short-lived, rotating certificates [53].	C3.1.1
IM3.2.0	Prevent Lateral Movement	Implement defense-in-depth (DiD) measures such as segmentation, access control, IDPS, and monitoring as outlined in control C3.2.0.	C3.2.0
IM3.3.0	Data Integrity Controls	Use encryption, hashing, and secure protocols (e.g., TLS, IPsec) to protect data. If unavailable, implement hash validation with alerting [31], [11].	C3.3.0
IM3.4.0	Emergency Access	For critical systems, implement access mechanisms in physically restricted areas to allow secure emergency access [31, p. 23].	C3.4.0

1) LEVEL 3 RISKS

Level 3 systems, such as Active Directory (AD) domain controllers [36], are often similar to those found in enterprise networks but focus on production operations. While this allows administrators to use familiar IT tools, it also exposes Level 3 to enterprise-level threats such as ransomware and advanced exploitation techniques.

Unlike purely IT environments, system compromises at this level can have a direct impact on production. The following risks are specific to Level 3; risks applicable to lower levels are not repeated here:

- Exploitation of Application Programming Interfaces (APIs)[1]
- Lateral movement through SCADA systems
- Data manipulation in HMIs or data historians
- Unauthorized access to critical control systems
- Network address spoofing

a: THE RISKS OF DIRECTORY SERVICES IN OT

While directory services offer centralized management, they also become high-value targets in OT environments, enabling privilege escalation and lateral movement if compromised. Their integration adds complexity, requires continuous maintenance, and may disrupt production [55]. A hybrid approach, in which only selected OT assets are managed via directory services and critical systems are isolated, can help balance control and security [54].

[1]MITRE Technique: https://attack.mitre.org/techniques/T0871/

E. LEVEL 3.5-INDUSTRIAL DEMILITARIZED ZONE

The Industrial Demilitarized Zone (IDMZ) was introduced as an additional segregation layer in the Purdue model to separate industrial networks from enterprise IT. It uses firewalls at both boundaries to enforce controlled data exchange, acting more as an information-sharing buffer than a direct communication path. This prevents direct exposure of OT systems to external threats. Typical services hosted include Windows Server Update Services (WSUS), proxy, and file transfer services, often deployed virtually for scalability and redundancy [36].

Designing the IDMZ must follow the specific requirements of the organization and any regulatory or legislative obligations the organization may be subject to. A well-designed IDMZ functions as a strong barrier for attackers and minimizes the attack surface of the industrial equipment. Some guidelines are:

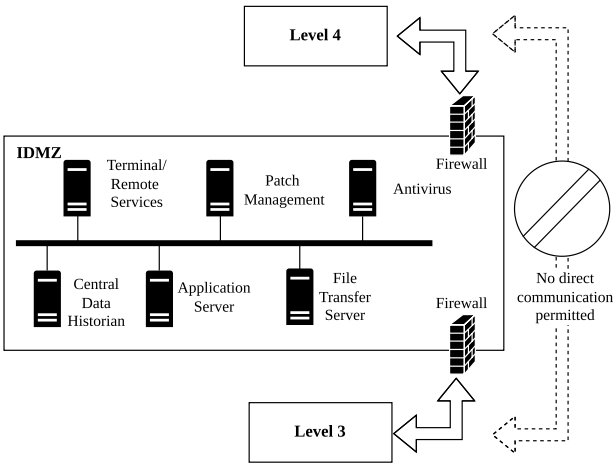

FIGURE 9. IDMZ architectural design illustrating the termination of direct logical paths between IT and OT networks to enforce a security boundary that protects production-critical assets [36].

- All traffic must terminate in the IDMZ; no direct IT–OT communication should bypass it.
- OT-specific protocols must remain confined to the OT network.
- Broker services (e.g., proxy, WSUS, file transfer) should be isolated in separate segments for containment.
- Critical OT services and data at rest (e.g., databases) must not reside in the IDMZ.
- Components should be virtualized, redundant, and capable of isolation or rebuilding in the event of compromise.

As the IDMZ primarily serves as a security buffer between zones (see Figure 9) to protect them from one another, proper and secure configuration is essential to ensure the correct functionality of this zone. The IDMZ typically hosts system and security components of different kinds. The extra time necessary to properly configure these services, assess vulnerabilities by penetration testing and ensuring correct operation and integrity of the zone may protect the OT environment in the long run. While IDMZ components may vary significantly between organizations, the controls listed in Table 10 should serve as a baseline security target.

The main goal of the IDMZ is to separate and control traffic between IT and OT environments while allowing data flows that serve business processes [6]. The security measures in Table 11 contribute to facilitate this goal.

F. LEVEL 4-BUSINESS PLANNING AND LOGISTICS

Level 4 represents the enterprise IT environment according the Purdue model. It hosts systems such as databases, email services, workstations, and authentication infrastructure. Data gathered from lower levels is processed here to support business operations including planning, logistics, finance, and management functions [36, p. 17]. Core enterprise systems at this level include Enterprise Resource Planning (ERP), Human Resources (HR), and other critical business services. As the main interface for users across the organization, this level must ensure secure and reliable IT operations while maintaining a strong separation from the industrial network. Tables 12 and 13 provide the identified controls and measures for Level 4.

G. LEVEL 5-THE ENTERPRISE ZONE/EXTERNAL ACCESS LEVEL

Level 5 represents the enterprise and external access zone of the Purdue model. It is closest to the internet and, thus, may be partially reachable from external networks. Users in this level interact with corporate applications such as ERP, email, and cloud services across multiple sites. While Levels 4 and 5 may be merged in smaller organizations, a separate abstraction is useful to distinguish between internally isolated systems and those exposed to external networks [36, p. 17].

The security measures in Level 5 are largely organization-specific and depend on the tools and technologies in use. However, remote access has been identified as a central focus as it inherits a high risk when not configured properly. The security controls for this zone can be found in Table 14 and the corresponding measures are listed in Table 15.

H. CYBERSECURITY ADDITIONS

The measures detailed in this article provide a structured approach to securing interconnected IT and OT environments. By establishing the controls presented in this work, implementing and expanding on the suggested measures, organizations can establish a security baseline for their interconnected networks. By building cyber-resilient systems that not only defend against threats but also recover and adapt in the face of disruption, organizations can ensure the continued operation of their critical systems and protect against the evolving threat landscape. Cybersecurity is a complex and evolving field, with new threats and vulnerabilities emerging constantly. To keep up with these challenges, organizations not only need to invest in technical security but organizational measures as well. The first step in the security process should be risk management. With a risk analysis and evaluation, measures can be prioritized and weighted, therefore creating a security strategy for the company.

V. DISCUSSION

A structured approach to securing interconnected IT and OT environments by establishing a unified security baseline is presented. By applying the recommended controls, organizations can build resilient systems that defend against threats, recover from incidents, and adapt to evolving risks.

A secure baseline begins with strong network segmentation using VLANs, firewalls, access control lists, and Intrusion Detection System (IDS) to limit lateral movement and separate IT, OT, and IDMZ environments. Centralized access management enforces least privilege and prevents unauthorized access through MFA, which requires users to verify their identity via two or more independent factors, and Role-Based Access Control (RBAC), whereby system

TABLE 10. Security baseline controls for the IDMZ, detailing role-based access control and flow-control mechanisms required to shield the OT environment from enterprise-level threats.

Control ID	Control Name	Description	Reference Standards
C3.5.1	Controlled Data Flow	Enforce strict traffic filtering and monitoring between IT and OT through the IDMZ.	IEC 62443-3-3 RDF SR 5.2 [31], NIST SP 800-53 [11] SC-7, AC-4, ISO 27002 [30] Ctrl. 5.14
C3.5.2	Role-Based Access Control (RBAC)	Ensure only authorized personnel access IDMZ systems through RBAC.	IEC 62443-3-3 [31] IAC SR 1.3, NIST SP 800-53 [11] AC-5, CM-5, ISO/IEC 27002 [30] Ctrl. 8.2
C3.5.3	Secure Configuration Management	Systems must be securely configured and reviewed regularly by trained staff.	NIST SP 800-53 [11] AT-3, IEC 62443-3-3 [31] SI SR 3.3, ISO 27002 [30] Ctrl. 8.9
C3.5.4	Vulnerability Management	Regularly scan IDMZ systems and apply patches using a defined mitigation process.	ISO 27002 [30] Ctrl. 8.8, NIST SP 800-53 [11] RA-5
C3.5.6	Virtualization Security	Secure virtual infrastructure with hardened hypervisors and updates.	ISO 27033-7 [56], NIST SP 800-125 [57]

TABLE 11. Security measures for the IDMZ, highlighting the deployment of specialized servers to facilitate secure IT-OT data mirroring and patch distribution.

ID	Security Measure	Description	Covered Controls
IM3.5.1	Firewalling	Firewalls must be implemented between IT, OT, and the IDMZ. Rules should restrict traffic to only explicitly permitted flows and be reviewed regularly.	C3.5.1
IM3.5.2	Secure Privileged Access	Implement RBAC and Just-in-Time (JIT) access to protect critical IDMZ systems.	C3.5.2
IM3.5.3	Hardening and Configuration Management	Systems should be configured to secure standards (e.g., CIS Benchmarks) and validated via automated/manual checks.[a]	C3.5.3, C3.5.6
IM3.5.4	Vulnerability Management	Use automated tools and threat intelligence to detect, prioritize, and remediate vulnerabilities.	C3.5.4, C3.5.6

[a]CIS-CAT: https://www.cisecurity.org/cybersecurity-tools/cis-cat-pro.

TABLE 12. Security controls for Level 4 (Business Planning and Logistics), focusing on sustaining the enterprise-wide security posture.

Control ID	Control Name	Description	Reference Standards
C4.1.0	Establish an ISMS	Define and maintain an Information Security Management System (ISMS) aligned with business needs. In addition, a comprehensive collection can be found in NIST SP 800-53r5 [11].	ISO 27001 [10], ISO 27002 [30], IEC 62443-3-2 [31]
C4.2.0	Internal Network Security Policy	Enforce rules for safe and compliant network use within the organization.	ISO 27033-1 [58], ISO 27033-2 [33]
C4.3.0	Workstation Security	Secure employee workstations and raise awareness of safe handling and usage.	NIST SP 800-70 [59]
C4.4.0	SIEM and SOC	Establish logging and monitoring to gather relevant events in a Security Information and Event Management (SIEM). A Security Operations Center (SOC) should be operated to react to incidents.	NIST SP 800-92 [60], ISO 27002 [30] Ctrl. 8.15, Ctrl. 8.16, ISO 27033-6 [45], ISO 27035-1 [61], ISO 27035-2 [62]
C4.5.0	Network Segmentation	Segment enterprise services logically to reduce exposure and limit access.	NIST SP 800-82r3 [6, sec. 5.2.3.1], ISO 27033-3 [44, chap. 11], ISO 27002 [30] Ctrl. 8.22
C4.6.0	Patch Management	Regularly patch IT assets to mitigate vulnerabilities.	NIST SP 800-40 [63]
C4.7.0	Administrative Tiering Model	Implement tiered access to protect high-privilege assets.	NIST SP 800-207 [64]

permissions are assigned according to a user's organisational role rather than on an individual basis [6]. Hardened jump servers further reduce exposure.

Patch management and system hardening reduce attack surfaces and address vulnerabilities. For unpatchable OT assets, compensating controls and a defense-in-depth strategy

TABLE 13. Level 4 (Business Planning and Logistics) security measures, outlining the administrative tiering and governance procedures required to protect business planning data and IT authentication services.

ID	Security Measure	Description	Covered Controls
IM4.1.1	Establish an ISMS	Define security policies, processes, and responsibilities within a formal ISMS. Ensure documentation and training for responsible staff.	C4.1.0
IM4.1.2	Risk Management Process	Implement a documented process to identify, assess, and treat information security risks.	C4.1.0
IM4.2.1	Network Usage Policy	Define acceptable use of network resources, including personal internet access and GDPR compliance [33], [58].	C4.2.0
IM4.3.0	Workstation Security	Configure workstations to secure baselines and raise user awareness. For sensitive and critical tasks, use Privileged Access Workstations (PAWs).	C4.3.0
IM4.3.1	Server Security	Secure servers by hardening, patching, access control, and monitoring. Perform backups, vulnerability scans, and log security events [65].	C4.3.1, C4.6.0
IM4.4.0	Security Operation and Monitoring	Logs and Events should be aggregated to security use cases which trigger automatic alerts for deviation from standard system behavior to detect malicious actors.	C4.4.0
IM4.5.0	Segmentation for Enterprise Services	As described in previous controls and measures, the enterprise services must as well be segmented by functionality and criticality. The goal must be that an infection can be contained easily in a network segment with as little as possible impact to services in other segments and business operation.	C4.5.0, C.4.7.0

TABLE 14. Boundary protection controls for Level 5 (Enterprise Zone), illustrating the defensive mechanisms required to regulate information flow between the internet and the internal business-OT ecosystem.

Control ID	Control Name	Description	Reference Standards
C5.1.0	Remote Access Security	Define policies for secure remote work, including internal users and external partners.	ISO 27033-1 [58], ISO 27033-4 [66], ISO 27033-5 [67], NIST SP 800-46 [68], NIST SP 800-53 [11] AC-17, NIST SP 800-41 [69], ISO 27002 [30] Ctrl. 6.7
C5.2.0	Secure VPN or ZTNA	Implement a secure VPN or Zero Trust Network Access (ZTNA) solution.	ISO 27033-5 [67], NIST SP 800-77 [70], NIST SP 800-53 [11] AC-17, IEC 62443-3-3 [31] RDF SR 5.2, IAC SR 1.13
C5.3.0	Secure Cloud Gateway	Regulate and secure access to cloud services such as file sharing, SaaS, and AI tools.	NIST SP 800-144 [71], ISO 27033-4 [66], ISO 27017 [72]
C5.4.0	NAT	Protect internal IPs by applying Network Address Translation (NAT) at the network edge.	NIST SP 800-41 [69, chap. 3.2], NIST SP 800-77 [70]

TABLE 15. Edge defense and remote access measures for Level 5, providing implementation guidelines for remote access and network edge protection to secure the primary external attack vector.

ID	Security Measure	Description	Covered Controls
IM5.1.1	Remote Access Policy for Employees	Define secure use of remote access, including device handling, public network use, and secure connection requirements.	C5.1.0
IM5.1.2	Remote Access Contract for Partners	Formalize network access terms, obligations, and liability with third-party partners.	C5.1.0
IM5.2.1	Secure VPN Implementation	Secure the VPN tunnel, client, and internal endpoint for external access.	C5.2.0
IM5.3.1	NAT	Use NAT on external-facing firewalls to obscure internal IPs.	C5.4.0
IM5.4.1	Secure Cloud Gateway	Implement identity access management, data loss prevention, encryption, logging, and policy enforcement for cloud access. Must comply with legal requirements [71].	C5.3.0

must be applied. Continuous monitoring through Security Information and Event Management (SIEM) enables timely detection and incident response. Prepared response plans help contain attacks and restore operations quickly.

Securing data flows between IT and OT with encryption and secure VPNs protects confidentiality and integrity. Redundancy and backup mechanisms support availability and recovery in the event of failures or attacks.

Finally, continuous improvement must guide implementation. Regular assessments, penetration testing, and audits help adapt the baseline to new threats, strengthening the organization's long-term cybersecurity posture.

Beyond the technical controls, PURITY carries broader managerial and operational implications for organizations adopting the framework:

- **Enhanced SME accessibility:** By mapping security controls to individual Purdue levels and providing actionable implementation measures, PURITY lowers the barrier for organizations with limited cybersecurity expertise and resources to adopt structured security practices.
- **Reduced complexity through IT-OT alignment:** Consolidating controls from multiple standards into a unified framework eliminates the need for organizations to navigate disparate guidelines independently, directly reducing the operational complexity of securing such environments.
- **Compliance facilitation:** The explicit traceability of PURITY controls to ISO 27001, IEC 62443, and NIST SP 800-82 simplifies audit preparation and supports organizations in demonstrating compliance with international cybersecurity standards.

While the current methodology relies on expert assessment and standards mapping, a comprehensive field testing across diverse industrial sectors is essential to verify the framework's effectiveness. Future work will focus on the empirical validation of the PURITY framework through practical deployment in SME OT environments.

VI. CONCLUSION

The convergence of IT and OT environments yields potentials for organizations to streamline their processes, gather and analyze data of production in real time and opportunities for automation. However this convergence also introduces significant security challenges due to the nature of both environments. While established standards provide guidance, SMEs in particular often lack the resources to fully implement comprehensive security frameworks.

In this work, we present *PURITY*, a structured and accessible security framework to improve security in converged environments. First, we create a layered defense strategy by integrating various industrial security standards and referencing them to specific guidance and measures, thereby addressing **RQ.1** (see Sections III and IV). Second, we provide a foundation on risk management techniques and group security measures into the individual levels of the Purdue model, prioritized by risk mitigation level to address high-risk threats first, thereby addressing **RQ.2** (see Sections II-C and IV). Third, *PURITY* leverages security best practices and configuration guidelines for common IT and OT hardware, enabling SMEs to implement a defense-in-depth architecture even with limited resources and without requiring next-generation security appliances, thereby addressing **RQ.3** (see Section IV).

In summary, the proposed framework delivers an accessible security baseline for SMEs, enabling them to strengthen their resilience against cyber threats while maintaining operational efficiency.

A. FUTURE WORK

The *PURITY* framework establishes a structured, standards-based security baseline for IT-OT convergence, with its design rooted in perimeter-oriented and zone-based segmentation principles. A natural and important extension of this work is the advancement to Zero Trust Architectures (ZTAs).

ZTAs fundamentally challenge the implicit trust assumptions of traditional, segmentation-based architecture models by following the principles of continuously enforcing verification of all users, devices and communication flows, regardless of their network location [73]. The applicability of ZTAs to industrial and manufacturing environments has been demonstrated in [74], where the adaption of ZTAs in smart manufacturing can effectively reduce lateral movement risks in environments characterized by deep IT-OT integrations.

Future work will therefore investigate how ZTA principles and standards can be mapped and integrated into *PURITY* across the individual Purdue levels, for instance, by replacing static firewall rulesets at the IDMZ with dynamic, identity-aware policy enforcement. Given the resource constraints of SMEs, a gradual adoption path is envisioned as a sequence of enhancements to the existing *PURITY* baseline, rather than a full replacement. Furthermore, empirical validation of the *PURITY* framework in real-world industrial settings will be pursued to assess its practical effectiveness and SME adoption barriers.

REFERENCES

[1] R. Venanzi, G. D. Modica, L. Foschini, and P. Bellavista, "Towards IT/OT integration in industry digitalization: A comprehensive survey," *J. Netw. Comput. Appl.*, 2025, Art. no. 104373, doi: 10.1016/j.jnca.2025.104373.

[2] M. Schirmbrand and A. Tomek, "Cybersecurity in Österreich," KPMG Security Services, Vienna, Tech. Rep., 2024.

[3] IBM Security and Ponemon Institute. (Mar. 2025). *Cost of a Data Breach Report 2025*. [Online]. Available: https://www.ibm.com/reports/data-breach

[4] M. Schirmbrand, A. Tomek, and G. Weidinger, "Cybersecurity in Österreich," KPMG Security Services GmbH, Vienna, Tech. Rep., 2023, pp. 50–53.

[5] T. J. Williams, "A reference model for computer integrated manufacturing from the viewpoint of industrial automation," *Int. J. Comput. Integr. Manuf.*, vol. 2, no. 2, pp. 114–127, Mar. 1989, doi: 10.1080/09511928908944389.

[6] K. Stouffer, M. Pease, C. Tang, T. Zimmerman, V. Pillitteri, S. Lightman, A. Hahn, S. Saravia, A. Sherule, and M. Thompson, "Guide to operational technology (OT) security," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, NIST SP 800-82, Revision 3, 2023.

[7] G. Murray, M. N. Johnstone, and C. Valli, "The convergence of IT and OT in critical infrastructure," in *Proc. 15th Austral. Inf. Secur. Manage. Conf.*, 2017, pp. 149–155.

[8] P. Didier, F. Macias, J. Harstad, R. Antholine, and S. A. Johnston, "Converged plantwide Ethernet (CPwE) design and implementation guide," Cisco Systems, San Jose, CA, USA, Tech. Rep. ENET-TD001E-EN-P, 2011.
[9] International Electrotechnical Commission (IEC), "Industrial communication networks–network and system security–part 1–1: Terminology, concepts and models," IEC, Geneva, Switzerland, Tech. Specification IEC/TS 62443-1-1, Jul. 2009.
[10] *Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems—Requirements*, International Organization for Standardization International Standard, Standard ISO/IEC 27001:2022, 2022.
[11] V. Pillitteri, E. Olumese, E. Porter, D. Black, E. Takamura, M. Tolboe, L. Humphries, J. N. Snyder, R. Graubart, N. Goren, D. Pappas, D. Faigin, C. Sames, P. Duspiva, A. Regenscheid, K. Dempsey, N. Lefkovitz, C. Enloe, K. Boeckl, and J. Boyens, "Security and privacy controls for information systems and organizations," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. NIST SP 800-53 Revision 5, 2020.
[12] D. Ratasich, F. Khalid, F. Geissler, R. Grosu, M. Shafique, and E. Bartocci, "A roadmap toward the resilient Internet of Things for cyber-physical systems," *IEEE Access*, vol. 7, pp. 13260–13283, 2019.
[13] M. Chapple, J. M. Stewart, and D. Gibson, *CISSP: Certified Information Systems Security Professional Study Guide*, 9th ed., Newark, NJ, USA: Wiley, 2021.
[14] M. P. Barret, "Framework for improving critical infrastructure cybersecurity version 1.1," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. NIST.CSWP.04162018, 2018, doi: 10.6028/NIST.CSWP.04162018.
[15] P. Phister and D. Olwell, "Guide to the systems engineering body of knowledge (SEBoK)–system reliability, availability, and maintainability," Stevens Institute of Technology and INCOSE and IEEE Systems Council, Hoboken, NJ, USA, Tech. Rep. v. 2.9, 2023.
[16] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *IEEE Trans. Dependable Secure Comput.*, vol. 1, no. 1, pp. 11–33, Jan. 2004.
[17] D. Garton, "Purdue model framework for industrial control systems & cybersecurity segmentation," National Petroleum Council, Washington, DC, USA, Tech. Rep. Topic Paper nos. 4–14, Nov. 2019. https://www.energy.gov/sites/default/files/2022-10/InfraTopicPaper4-14FINAL.pdf
[18] International Electrotechnical Commission, "Industrial communication networks–network and system security—Part 2-1: Establishing an industrial automation and control system security program," Int. Electrotechnical Commission, Geneva, Switzerland, Tech. Rep. IEC 62443-2-1:2010, 2010.
[19] P. Ackerman, *Industrial Cybersecurity: Efficiently Secure Critical Infrastructure Systems*. Birmingham, U.K.: Packt, 2017.
[20] S. Mathezer. (2021). *Introduction to ICS Security Part 2—The Purdue Model*. [Online]. Available: https://www.sans.org/blog/introduction-to-ics-security-part-2
[21] G. Murphy, "A reimagined Purdue model for industrial security is possible," Forbes Technology Council, New York, NY, USA, Tech. Rep., Jan. 2022. [Online]. Available: https://www.forbes.com/sites/forbestechcouncil/2022/01/18/a-reimagined-purdue-model-for-industrial-security-is-possible/?sh=37fef1c41162
[22] *Risk Management—Guidelines*, International Standard, International Organization for Standardization, Standard ISO 31000:2018, 2018.
[23] J. Freund and J. Jones, *Measuring and Managing Information Risk: A FAIR Approach*, 1st ed. Oxford, U.K.: Butterworth-Heinemann, 2015.
[24] G. Verteegen, *Risikomanagement in IT-Projekten*. Berlin, Germany: Springer-Verlag, 2003.
[25] Center for Internet Security. (2021). *CIS Critical Security Controls Version 8*. [Online]. Available: https://www.cisecurity.org/controls/v8
[26] ISA Global Cybersecurity Alliance, "Applying ISO/IEC 27001, ISO/IEC 27002 and the ISA/IEC 62443 series for operational technology environments," ISA Global Cybersecurity Alliance (ISAGCA), Durham, NC, USA, White Paper, Tech. Rep., Jun. 2025.
[27] F. Djebbar and K. Nordström, "A comparative analysis of industrial cybersecurity standards," *IEEE Access*, vol. 11, pp. 85315–85332, 2023.
[28] A.-E. Voicu, "Combined approach to information security based on ISO 27001/2 and IEC 62443-2-1," Secura A Bureau Veritas Company, Utrecht, The Netherlands, White Paper, 2017. https://securitydelta.nl/media/comhsd/report/641/document/01-Secura-WP-Combined-Approach-to-Information-Security.pdf
[29] A. Sedgewick, M. Souppaya, and K. Scarfone, "Guide to application whitelisting," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. NIST SP 800-167, 10 2015.
[30] *Information Security, Cybersecurity and Privacy Protection—Information Security Controls*, International Standard, International Organization for Standardization, Standard ISO/IEC27002:2022, 2022.
[31] International Electrotechnical Commission, "Industrial communication networks–network and system security—Part 3–3: System security requirements and security levels," Int. Electrotechnical Commission, Geneva, Switzerland, Tech. Rep. IEC 62443-3-3:2013, Aug. 2013.
[32] A. M. Thomas, M. Marali, and L. Reddy, "Identification of assets in industrial control systems using passive scanning," in *Proc. Comput. Netw.*, 2022, pp. 269–283.
[33] *Information Technology—Security Techniques—Network Security—Part 2: Guidelines for the Design and Implementation of Network Security*, Standard ISO/IEC 27033-2:2012, International Standard, International Organization for Standardization, 2012,
[34] International Electrotechnical Commission, "Industrial communication networks–network and system security—Part 3–2: Security risk assessment and system design," Int. Electrotechnical Commission, Geneva, Switzerland, Tech. Rep. IEC 62443-3-2:2020, Jun. 2020.
[35] G. P. H. Sandaruwan, P. S. Ranaweera, and V. A. Oleshchuk, "PLC security and critical infrastructure protection," in *Proc. IEEE 8th Int. Conf. Ind. Inf. Syst.*, Dec. 2013, pp. 81–85.
[36] P. Ackerman, *Industrial Cybersecurity: Efficiently Monitor the Cybersecurity Posture of Your ICS Environment*, 2 ed., Birmingham, U.K.: Packt, 2021.
[37] A. Ghaleb, S. Zhioua, and A. Almulhem, "On PLC network security," *Int. J. Crit. Infrastruct. Protection*, vol. 22, pp. 62–69, Sep. 2018.
[38] S. A. Milinkovic and L. R. Lazic, "Industrial PLC security issues," in *Proc. 20th Telecommun. Forum (TELFOR)*, Nov. 2012, pp. 1536–1539.
[39] Center for Internet Security. (Nov. 2022). *CIS Controls v8 Internet of Things Companion Guide*. Center for Internet Security Website. [Online]. Available: https://www.cisecurity.org/white-papers/cis-controls-v8-internet-of-things-companion-guide/
[40] S. Dynes, C. Palmer, and S. Shenoi, *IFIP Advances in Information and Communication Technology* (IFIP Advances in Information and Communication Technology), vol. 311. Berlin, Germany: Springer-Verlag, 2009.
[41] G. Yadav and K. Paul, "Architecture and security of SCADA systems: A review," *Int. J. Crit. Infrastructure Protection*, vol. 34, Sep. 2021, Art. no. 100433.
[42] T. Macaulay and B. L. Singer, *Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS, English*, 1st ed. Boca Raton, FL, USA: CRC Press, 2011.
[43] University of Kentucky, "SCADA report appendix B–Survey statistics," Univ. Kentucky, Lexington, KY, USA, Tech. Rep. 01-29-14, Jan. 2014. [Online]. Available: https://www.uky.edu/WDST/PDFs/[27.3]%20SCADA%20Report%20App%20B%20-%20Survey%20Stats%20Revised%2001-29-14.pdf
[44] *Information Technology—Security Techniques—Network Security–Part 3: Reference Networking Scenarios– Threats, Design Techniques and Control Issues*, International Standard, International Organization for Standardization, Standard ISO/IEC 27033-3:2010, 2010.
[45] *Information Technology—Security Techniques—Network Security—Part 6: Securing Wireless IP Network Access*, International Standard, International Organization for Standardization, Standard ISO/IEC 27033-6:2016, 2016.
[46] M. Aamir, J. Poncela, M. A. Uqaili, and B. S. Chowdhry, "Optimal design of remote terminal unit (RTU) for wireless SCADA system for energy management," *Wireless Pers. Commun.*, vol. 84, no. 1, pp. 3–19, 2015.
[47] C. Alcaraz, *Securing Cyber-Physical Systems* (Advanced Sciences and Technologies for Security Applications). Cham, Switzerland: Springer, 2019.
[48] *Communication Networks and Systems for Power Utility Automation—Part 3: General Requirements*, International Standard, International Electrotechnical Commission, Standard IEC 61850-3, 2013.
[49] *IEEE Standard for Environmental and Testing Requirements for Devices With communications functions used With Electric Power Apparatus*, Institute of Electrical and Electronics Engineers, Standard IEEE 1613-2023, 2023.
[50] R. S. Yadav and P. Likhar, "Firewall: A vital constituent of network security," in *Information Technology Security: Modern Trends and Challenges*. Singapore: Springer Nature, 2024, pp. 47–67.

[51] E. D. Knapp and J. T. Langill, *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*. Waltham, MA, USA: Syngress, 2011.

[52] M. Souppaya, K. Scarfone, and D. Dodson, "Secure software development framework (SSDF) version 1.1: Recommendations for mitigating the risk of software vulnerabilities," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. NIST SP 800-218, Feb. 2022.

[53] P. Grassl, J. Fenton, E. Newton, R. Perlner, A. Regenscheld, W. Burr, J. Richer, N. Lefkovitz, J. Danker, Y.-Y. Choong, K. Greene, and M. Theofanos, "Digital identity guidelines: Authentication and lifecycle management," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. NIST SP 800-63B, 2017.

[54] C. J. Brooks and P. A. Craig Jr., *Practical Industrial Cybersecurity: ICS, Industry 4.0, and IIoT*. Hoboken, NJ, USA: Wiley, Jun. 2022.

[55] M. Usman, M. S. Sarfraz, U. Habib, M. U. Aftab, and S. Javed, "Automatic hybrid access control in SCADA-enabled IIoT networks using machine learning," *Sensors*, vol. 23, no. 8, p. 3931, Apr. 2023.

[56] *Information Technology—Network Security—Part 7: Guidelines for Network Virtualization Security*, International Standard, International Organization for Standardization, Standard ISO/IEC 27033-7:2023, 2023.

[57] K. Scarfone, M. Souppaya, and P. Hoffman, "Guide to security for full virtualization technologies," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. NIST SP 800-125, 2011.

[58] *Information Technology—Security Techniques—Network Security—Part 1: Overview and Concepts*, International Standard, International Organization for Standardization, Standard ISO/IEC 27033-1:2015, 2015.

[59] S. Quinn, M. Souppaya, M. Cook, and K. Scarfone, "National checklist program for IT products: Guidelines for checklist users and developers," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. NIST SP 800-70, Revision 4, Feb. Jan. 2018.

[60] K. Kent and M. Souppaya, "Guide to computer security log management," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. NIST SP 800-92, 2006.

[61] *Information Security Incident Management—Part 1: Principles and Process*, International Standard, International Organization for Standardization, Standard ISO/IEC 27035-1:2023, 2023.

[62] *Information Security Incident Management—Part 2: Guidelines to Plan and Prepare for Incident Response*, International Standard, International Organization for Standardization, Standard ISO/IEC 27035-2:2023, 2023.

[63] M. Souppaya and K. Scarfone, "Guide to enterprise patch management planning: Preventive maintenance for technology," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. NIST SP 800-40, Revision 4, Jun. 2022.

[64] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero trust architecture," Nat. Inst. Standards Technol. (NIST), Gaithersburg, MD, Special Publication SP 800-207, Aug. 2020.

[65] K. Scarfone, W. Jansen, and M. Tracy, "Guide to general server security," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. NIST SP 800-123, Jul. 2008.

[66] *Information Technology—Security Techniques—Network Security–Part 4: Securing Communications Between Networks Using Security Gateways*, International Standard, International Organization for Standardization, Standard ISO/IEC 27033-4:2014, 2014.

[67] *Information Technology—Security Techniques—Network Security–Part 5: Securing Communications Across Networks Using Virtual Private Networks (VPNs)*, Standard ISO/IEC 27033-5:2013, International Standard, Geneva, Switzerland: International Organization for Standardization, 2013.

[68] M. Souppaya and K. Scarfone, "Guide to enterprise telework, remote access, and bring your own device (BYOD) security," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. NIST SP 800-46, Revision 2, 2016.

[69] K. Scarfone and P. Hoffman, "Guidelines on firewalls and firewall policy," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. NIST SP 800-41, Revision 1, 2009.

[70] E. Barker, Q. Dang, S. Frankel, K. Scarfone, and P. Wouters, "Guide to IPsec VPNs," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. NIST SP 800-77 Revision 1, 2020.

[71] W. Jansen and T. Grance, "Guidelines on security and privacy in public cloud computing," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. NIST SP 800-144, 2011.

[72] *Information Technology—Security Techniques–Code of Practice for Information Security Controls Based on ISO/IEC 27002 for cloud Service*, International Standard, International Organization for Standardization, Standard ISO/IEC 27017:2015, 2015.

[73] N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig, and R. Doss, "Zero trust architecture (ZTA): A comprehensive survey," *IEEE Access*, vol. 10, pp. 57143–57179, 2022.

[74] B. Paul and M. Rao, "Zero-trust model for smart manufacturing industry," *Appl. Sci.*, vol. 13, no. 1, p. 221, Dec. 2022.

FRANZ-KARL SCHACHINGER received the B.Sc. degree in business informatics and digital transformation and the M.Sc. degree in information technology and systems management with a focus on networking, privacy, and security from Salzburg University of Applied Sciences, Austria, in 2022 and 2025, respectively. He is currently a Security Engineer, focusing on hardening devices, security operations, and network security, and establishing ISMS.

THOMAS ROSENSTATTER received the B.Sc. degree in information technology and systems management from Salzburg University of Applied Sciences, Austria, in 2014, the M.Sc. degree in embedded and intelligent systems from Halmstad University, Sweden, in 2016, and the Ph.D. degree in computer science and engineering with a focus on automotive cybersecurity from the Chalmers University of Technology, Sweden, in 2021. He was a Researcher with the RISE Research Institutes of Sweden, concentrating on cybersecurity in mobility solutions. He is currently a Senior Lecturer and a Researcher with the Josef Ressel Centre for Intelligent and Secure Industrial Automation, Salzburg University of Applied Sciences. His research interests include cybersecurity and resilience in cyber-physical systems, with a focus on the automotive and industrial domains.

ULRICH PACHE received the Mag.iur. degree from the University of Salzburg, in 2001, and the B.Sc. and M.Sc. degrees in information technology and systems management from Salzburg University of Applied Sciences, in 2011 and 2013, respectively. He was a Candidate Lawyer and a Network and Security Engineer. He was a Researcher with the Center for Secure Energy Informatics, Salzburg University of Applied Sciences, with a focus on smart grids and 5G applications for industrial use cases. He is currently a Senior Lecturer with Salzburg University of Applied Sciences, with a focus on network technologies and IT security.