IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received 27 January 2025, accepted 12 March 2025, date of publication 20 March 2025, date of current version 28 March 2025.

Digital Object Identifier 10.1109/ACCESS.2025.3553011

APPLIED RESEARCH

Why to Fail Fast and Often: A Strategy for OT Safety and Security Evaluation

MUKUND BHOLE[1], THILO SAUTER[2,3], (Fellow, IEEE), SABRINA SEMPER[4], AND WOLFGANG KASTNER[1], (Senior Member, IEEE)

[1]Institute of Computer Engineering, TU Wien, 1040 Vienna, Austria
[2]Institute of Computer Technology, TU Wien, 1040 Vienna, Austria
[3]Department for Integrated Sensor Systems, University for Continuing Education Krems, 3500 Wiener Neustadt, Austria
[4]TÜV Austria Services GmbH, 1230 Vienna, Austria

Corresponding author: Mukund Bhole (mukund.bhole@tuwien.ac.at)

This work was supported in part by the TÜV AUSTRIA's #SafeSecLab Research Lab for Safety and Security in Industry, a research collaboration between Technische Universität Wien (TU Wien) and TÜV AUSTRIA; and in part by the TU Wien Bibliothek through its Open Access Funding Program.

ABSTRACT As the Operational Technology (OT) environment becomes increasingly interconnected and integrates diverse technologies, traditional models often struggle to accurately represent the complex interactions and dependencies of the underlying systems. Factors like changes in operational conditions, software updates, and the introduction of new devices can significantly impact the system's risk profile. This paper presents a methodology to bridge the gap between manual and automated safety and security requirements in Industry 4.0 OT environments. First, a meta-model is developed to capture OT infrastructure components and relationships. This is then transformed into a C#-based GUI, enabling tasks like network scanning, application and interface identification, and AI-powered data extraction. Next, compliance checks and risk assessments are conducted using standards such as IEC 62443-3-3 and methods like LOPA, SEFR (HAZID), STRIDE, and DREAD. Finally, the data is converted into system models (e.g., OWL, AutomationML) for visualization. This approach reduces complexity and time by 83.72%, though it faces challenges like platform dependency and resource constraints.

INDEX TERMS OT safety and security, standard compliance, risk evaluation, system modeling, data visualization.

I. INTRODUCTION

The increasing complexity of modern systems and the growing sophistication of threats underscore the urgent need for practical tools to enhance safety and security evaluation. As industries become increasingly reliant on interconnected digital and physical infrastructures, particularly in Operational Technology (OT) environments, the risks of failures, cyberattacks, and operational disruptions have multiplied. Traditional and manual methods often fall short in detecting emerging vulnerabilities, improperly configured systems, or responding swiftly to threats [1].

Security breaches in critical sectors such as energy, manufacturing, and oil & gas have resulted in financial losses, service disruptions, and significant erosion of trust [2].

The associate editor coordinating the review of this manuscript and approving it for publication was Alessandra De Benedictis.

In industrial settings, safety protocols are essential for preventing accidents that could harm workers or the environment, while security measures safeguard systems from cyberattacks that could cause equipment failures, spills, or outages. With the increasing integration of Information Technology (IT) and OT systems, a combined approach to safety and security is crucial to ensure that security vulnerabilities do not compromise safety in today's fast-paced industrial environments. Any lapse in these areas can lead to severe, far-reaching consequences, making their proactive management a top priority [3], [4].

Following this motivation, the philosophy of **"Fail Fast, Fail Often"** is widely embraced in the fields of innovation and agile development [5]. This approach promotes experimentation, learning from failures, and rapid adaptation. By failing quickly and frequently, valuable insights are gained, enabling mistakes to be identified and corrected early in the process. This principle aligns with methodologies such as design thinking, where rapid prototyping and early failures in controlled environments help minimize costly issues later [6], [7]. While system failures in operational settings are often ridiculed due to their impact on downtime and financial loss, adapting this philosophy in a sandbox environment may prove beneficial.

The core idea of this paper is to fail, learn, and improve, thereby accelerating progress in safety and security evaluations. Consequently, practical tools for real-time monitoring, rapid detection, standards compliance management, and risk evaluation are crucial for preventing safety and security risks in OT from escalating into serious incidents. Addressing these safety and security failures in a timely manner—by learning from them, resolving issues, and enhancing processes with these tools—can help avoid costly downtime, protect sensitive data, ensure regulatory compliance, and, most importantly, safeguard human lives and critical assets. Without advanced safety and security solutions, organizations remain vulnerable to increasingly complex risks that could lead to catastrophic and far-reaching consequences.

The motivation to adopt the changing landscape of safety and security is related to EU Regulation 2023/1230 [8], passed on 29 June 2023, on machinery and the repeal of previous legislation, the legislative procedure (Articles 25 and 51) along with Sections 1.1.9 and 1.2.1-1.2.6, addresses risks arising from malicious third-party actions that can impact the safety of products and their surrounding environment as covered by this regulation. It establishes essential health and safety requirements, and compliance with these can be presumed when a certificate or conformity statement is issued under a relevant cybersecurity certification scheme adopted by Regulation (EU) 2019/881 of the European Parliament and the Council.

In recent years, model-based evaluation tools have been widely used to assess safety and security across industrial operations, cybersecurity, and complex system management. These tools rely on static data models, simulations, and algorithms to analyze, predict, and optimize performance, reliability, and risks, particularly in complex environments. However, several factors suggest the need to shift toward more sophisticated approaches. As systems in industries like OT become increasingly complex with technological advancements, traditional models often need help to capture interconnected environments' dynamic and unpredictable nature, requiring frequent updates and refinements. The rapidly evolving cybersecurity landscape also introduces new threats and vulnerabilities, making static models inadequate for addressing emerging risks. Another challenge is integrating real-world data, as theoretical models may only partially reflect actual operational conditions, highlighting the need for runtime data to improve accuracy. Scalability further complicates traditional approaches, which may become inefficient as OT environments expand, calling for methods that can scale while maintaining precision. Additionally, model-based evaluations need more adaptability, making it difficult to respond to unexpected system changes and often overlook human factors, such as operator errors or decision-making under pressure. A more holistic approach is required to address these limitations—one that incorporates human and environmental constraints and the unique context of OT systems.

Since risk scores generated by existing standard solutions do not consider contextual factors such as asset criticality, exploitability, and real-time threat intelligence, a proper contextualized risk assessment approach is needed. This approach should prioritize vulnerabilities based on their exploitability, potential impact, and relevance to the specific system environment. Unlike existing standard solutions, it should integrate dynamic system intelligence, asset criticality, and financial business impact analysis to generate more accurate and actionable risk scores.

In this paper, we adopt the **"Fail Fast, Fail Often"** philosophy to guide the development and use of our tool, addressing the limitations of model-based evaluation as a motivating factor for tackling safety and security challenges in the OT environment. Our goal is to implement a design-thinking approach by utilizing a system meta-model, derived from model-based evaluation, that incorporates all essential components of the OT infrastructure. This meta-model is subsequently transformed into a C#-based GUI application to facilitate more accessible real-time information gathering and enable subsequent evaluation using a four-step methodology. C# is our preferred choice for modern software development due to its active support from Microsoft, cross-platform capabilities enabled by.NET, a large developer community, and robust integration with cloud and AI technologies. These features ensure C# remains relevant, adaptable, and viable for long-term software investments. Guided by the "Fail Fast, Fail Often" philosophy, we aim to quickly adapt to changes and failures, refining the process continuously to improve outcomes. While the proposed methodology may not yet represent a fully sustainable solution, it marks a significant step toward achieving one. The target group for an OT safety and security evaluation tool includes:

- OT professionals: engineers, technicians, safety and security experts
- Facility management: managers, plant operators
- Compliance officers and regulatory authorities
- Executive leadership: CIOs, COSOs, CISOs
- Risk management teams
- Vendors and third-party service providers
- Government bodies
- R&D teams focused on innovation
- End users: operators and supervisors

These stakeholders require up-to-date knowledge of safety and security protocols to effectively manage risks in OT environments. The remainder of the article is organized as follows: Section II reviews the relevant literature and existing work related to the topic; Section III outlines the four-step methodology for assessing safety and security in the OT environment, which includes standard compliance and risk evaluation; Section IV illustrates the application of the methodology using a case study; Section V discusses the results obtained from the study's findings; and Section VI provides concluding remarks.

II. RELATED WORK AND BACKGROUND

Table 1 provides an overview of various integrated safety and security evaluation projects, frameworks, and methods, highlighting their limitations in relation to the scope of this paper. It also summarizes selected security-focused threat modeling frameworks and safety methodologies, whose foundational principles align with those of the proposed methodology, though their implementations differ, as elaborated later in the paper.

A. SECURITY RELATED THREAT MODELING FRAMEWORKS FOR RISK EVALUATION

In this section, we discuss STRIDE to identify potential threats and prioritize them with DREAD based on severity and likelihood. Next. PASTA is introduced to assess the impact on business objectives, and expand to an enterprise level using OCTAVE to address organizational vulnerabilities. Finally, we present VAST to leverage visualization and communication and incorporate TRIKE to evaluate risks from stakeholder-specific perspectives.

1) STRIDE

STRIDE [62], developed by Microsoft, is a threat categorization model designed to identify potential security threats across various aspects of a system. It is widely used for threat modeling in software and system architectures. The acronym STRIDE stands for Spoofing (impersonating another entity), Tampering (unauthorized alteration of data), Repudiation (a user denying they acted), Information Disclosure (unauthorized access to information), Denial of Service (disruptions to services or unavailability of resources), and Elevation of Privilege (gaining unauthorized higher access levels). Applying the STRIDE model involves identifying the components of the system—such as data flows, data stores, and processes—applying the STRIDE framework to each component to uncover potential threats and prioritizing these threats for appropriate mitigation. Critical use cases for STRIDE include threat modeling during the design phase, focusing on addressing technical threats that may impact system components.

2) DREAD

DREAD [63], initially developed by Microsoft and once used alongside the STRIDE model, has become less popular. It is a risk assessment model that prioritizes identified threats based on their potential impact. The acronym DREAD stands for Damage Potential (the extent of damage that could occur if the threat materializes), Reproducibility (how easily the attack can be replicated), Exploitability (the simplicity of exploiting the vulnerability), Affected Users (the number of users that would be impacted), and Discoverability (how easily an attacker can find the vulnerability). Each component of DREAD is scored on a scale from 1 to 10 (in this paper, we use a scale from 1 to 5), and the total score ranks threats according to their risk level. Critical use cases for DREAD include risk-based prioritization of threats during threat modeling and assessing the potential dangers posed by specific vulnerabilities or attacks.

3) PASTA

PASTA [64], developed by Tony UcedaVélez and Marco M. Morana, is a risk-centric threat modeling methodology that emphasizes simulating attacks to analyze potential risks to applications or systems. This approach aligns business objectives with technical security needs. The PASTA methodology consists of several phases:

1) Definition of Objectives: Establishing business goals and security requirements.
2) Definition of the Technical Scope: Identifying system components.
3) Application Decomposition: Breaking down the application to understand its functionality.
4) Threat Analysis: Identifying potential threats using STRIDE or other frameworks.
5) Weakness and Vulnerability Analysis: Pinpointing existing vulnerabilities.
6) Attack Modeling & Simulation: Simulating attack scenarios based on real-world tactics.
7) Risk Analysis and Mitigation: Assessing risks and applying countermeasures.

Critical use cases for PASTA include risk-based threat modeling for complex applications, with a strong focus on attack simulations and real-world applicability.

4) VAST

VAST [65], developed by ThreatModeler, is a threat modeling methodology designed for seamless integration into DevOps and Agile environments. While these methodologies are primarily associated with software development, they can also be effectively adapted to other industries. VAST focuses on scalability, enabling application, and operational threat modeling while maintaining simplicity for team adoption. It consists of two main components: the **Application Threat Model**, which addresses threats at the application level (such as web applications and microservices), and the **Operational Threat Model**, which targets threats at the infrastructure level (including networks, data centers, and cloud environments). Fundamental principles of VAST emphasize automation and scalability, continuous threat modeling within Agile and DevOps workflows, and visual representation of threats and their mitigations. This methodology is particularly beneficial for large-scale enterprises that require comprehensive threat modeling across multiple applications.

TABLE 1. Current literature on few integrated safety and security projects, frameworks, and methods.

Name	Description	Limitations
	Model-Based Safety and Security Risk Evaluation	
FAHP-Based Integrated Assessment [9]–[11]	Integrates safety and security evaluations using fuzzy and probabilistic methods	Complexity of integrating both domains, data uncertainty, and subjectivity in fuzzy evaluation
SSI Architecture [9]	Combines safety failure modes and security measures for holistic risk analysis	Difficulty in aligning safety-security interaction across diverse systems
Fault Tree Analysis (FTA) [10]	Common tool for security risk assessment, but with fuzziness and data precision issues	Data dependency and difficulty in capturing complex, dynamic system behaviors
Bayesian Networks [11], [12]	Handles ambiguity, complex conditional probability for risk evaluation	Requires high-quality data and expert input, computational complexity
Fuzzy and Probabilistic Methods [13], [14]	Includes attack trees and fuzzy-enhanced FMEA for dynamic analysis	Subjectivity in fuzzification, potential for misinterpretation of risk levels
Fuzzy-AHP Integration [15]	Combines AHP with fuzzy evaluations for process failure analysis	Complexity in integrating fuzzy evaluations with AHP; uncertainty in criteria comparison
	Taxonomies and Classifications in Information Security Risk Management (ISRM)	
Campbell and Stamp Classification [16]	3x3 classification for skill requirements and intrusiveness in ISRM methods	Inability to capture the complexity of modern ISRM tools and the evolving nature of threats
Snekkenes Activity-Based Taxonomy [17]	Aids in comparing ISRM methods and identifying research gaps	Difficulty in identifying clear research gaps due to rapid tool and technique evolution
ISRM Challenges [18]–[20]	Lack of independent testing and rigorous analysis in ISRM methods	Insufficient validation of methods, lack of real-world testing environments
	Risk Measurement and Management for ICS	
ICS-Specific Tools [21]–[23]	Tools like CSET, RiskMAP, and VSAT for ICS risk evaluation	ICS-specific metrics are often underdeveloped, limited applicability to diverse ICS environments
	European Union Framework Initiatives	
FP6 and FP7 Contributions [24], [25]	Architectural solutions for ICS resilience (EMILI, CRUTIAL)	Lack of standardization, difficulty in scaling solutions across industries
Other Projects [26]–[29]	VIKING (Resilience and contingency planning innovations) COCKPITCI (autonomous defense), CRISALIS (power grids security)	Difficulty in correlating project outcomes with broader security improvements; Complexity in integrating autonomous defense into existing systems
	Automated Frameworks for Safety and Security	
Automation in ISRM [30]	Automated ISRM process integrating safety-informed approaches	High complexity in system automation, need for real-time adaptability
	Risk-Driven Security Decision Making	
Risk-Based Approaches [31]–[33]	Critique of cost-benefit analysis methods, focusing on evolution and fragmentation	Risk-based approaches may overlook emerging threats, need for more dynamic methodologies
Safety-Security Integration [34]	Aligning safety and security processes using fuzzy-AHP and model-based evaluations	Integration challenges, especially in diverse organizational cultures
	Dynamic Security Analysis	
BDMP (BDM-Processes) [35], [36]	Dynamic, scalable security risk assessments using attack trees and Markov processes	Complexity in integrating multiple models, data inconsistency issues
Markov Chains & CVSS Data [36]	Models security threats and progression over time	Requires accurate data and clear understanding of threat progression
Hybrid Approaches [37], [38]	Combines BDMP with FTA and Bayesian networks for robust analysis	High computational cost, complexity of model integration
	Security and Risk Assessment	
Security vs Risk Assessment [39]–[41]	Security evaluates system defenses, risk assesses threats and consequences	Difficulty in bridging the gap between the two disciplines, evolving nature of threats
Cybersecurity Threat Modeling [42], [43]	Enhances Meta Attack Language (MAL) using MITRE ATT&CK for attack simulations	Data gaps, complexity in real-time attack modeling
	Attack Tree Modeling for Risk Evaluation	
SecurITree & AttackTree+ [44], [45]	Commercial tools for extensive attack tree modeling	Complexity in customizing attack trees for specific environments, limited flexibility
SeaMonster [46], [47]	Visualizes attack trees and integrates security requirement methodologies	Difficulties in visualizing large, complex attack trees
AttackDog [48]	Extends attack tree modeling with collaborative features	High collaboration overhead, limited integration with other tools
	Model-Based Approaches in Security Engineering	
SysML and AML [49]–[51]	Automates security assessments through system modeling	Complex modeling languages, high learning curve for adoption
OWL and SWRL [52]	Knowledge-driven approaches for vulnerability identification	Requires detailed ontologies, integration issues
	Integration of Safety and Security	
Convergence of Safety-Security Standards [53]	Risk analysis approach to tackle malicious attacks and system failure.	Difficulty assessing emerging threats, subjective risk assessment, balancing safety-security.
SafSec: Commonalities [54], [55]	Combines safety and security argumentation to identify risks and control measures.	Separation of disciplines, goal conflicts, evolving threats, human factors.
	Safety and Security Projects	
SAFURE [56]	Cyber-physical systems with integrated safety and security design	Lack of standardization, difficulty in understanding the full attack surface
D-MILS [57]	Ensures system safety with MILS security platform-based modeling	Complexity in modeling, verification issues
SESAMO [58]	Component-based design for safety-security in networked embedded systems	Environmental uncertainties, cost and time constraints
SAFESEC Lifecycle Management [59], [60]	Integrates safety and security through the development process	Organizational challenges, lack of expertise
Cross-Fertilization of Safety and Security [61]	Methodologies for transposing approaches between safety and security	Cultural barriers, conflicting goals

5) OCTAVE

OCTAVE [66], developed by Carnegie Mellon University, is a risk-based information security assessment framework that focuses on identifying critical assets and their associated risks, enabling organizations to formulate security strategies grounded in risk management. The framework consists of several phases, starting with the creation of asset-based threat profiles to pinpoint critical assets and associated threats. The second phase involves identifying infrastructure vulnerabilities by analyzing the security weaknesses of the organization's infrastructure. Finally, the framework guides organizations in developing security strategies and mitigation plans to reduce risks and enhance overall security. Critical characteristics of OCTAVE include its business-centric approach, which aligns security initiatives with business objectives; a focus on assets and vulnerabilities rather than individual technical components; and a self-directed model that empowers organizations to manage their threat assessments. This framework benefits information security risk assessment in large enterprises and supports strategic decision-making based on thorough risk analysis.

6) TRIKE

Trike [67], developed by the open-source community, is a threat modeling framework designed to enhance system security through a risk management approach that emphasizes the risks associated with individual actions or behaviors within the system. The framework comprises three main types of models: the **Requirement Model**, which converts security requirements into acceptable and unacceptable behaviors to assess whether the system meets its security objectives; the **Implementation Model**, which examines the system architecture to identify threats in its current state; and the **Attack Model**, which evaluates potential attack vectors and the likelihood of an attacker exploiting vulnerabilities. The process involves creating a system diagram to represent components and their interactions, assigning actors and roles, identifying risks associated with each action and actor, and assigning risk values for analysis. Trike is beneficial for systems that focus on user roles and permissions and for conducting behavioral analysis in security contexts.

B. SAFETY RELATED METHODOLOGIES

In this section, methods form a hierarchical and iterative process. HAZID and ENVID identify hazards, HAZOP and Bowtie analyze them in detail, LOPA and SIL quantify protective layers, QRA assesses risk probabilistically, and RAMS ensures system reliability aligns with safety goals. Together, they form a comprehensive framework for evaluating and managing safety risks.

1) HAZID (HAZARD IDENTIFICATION)

HAZID [68] is a structured and systematic process designed to identify hazards in operations, processes, or projects early, aiming to assess potential risks and mitigate them before they escalate. This methodology typically involves brainstorming sessions with multidisciplinary teams to generate a comprehensive list of possible hazards, rank them based on severity, and develop action plans for mitigation. HAZID is often conducted early in project planning or during the design phases to ensure safety and efficiency. Critical features of HAZID include its qualitative nature, the involvement of both operational and design teams, and its effectiveness in identifying safety, environmental, and technical risks early. Additionally, HAZID is a foundational basis for further risk assessment techniques, enhancing overall project safety and risk management.

TABLE 2. Overview of security related threat modelling frameworks for risk evaluation.

Framework	Key Focus	Methodology Type	Primary Use Case
STRIDE	Threat categorization	Technical	Software design and architecture threats
DREAD	Risk assessment	Scoring-based	Risk prioritization of threats
PASTA	Risk-based attack simulation	Process-driven	Real-world attack simulation and risk assessment
VAST	Agile and scalable modeling	Visual and scalable	Large-scale enterprises and Agile/DevOps
OCTAVE	Risk-based assessment	Business-centric	Information security strategy and risk management
Trike	Risk and behavioral analysis	Role-based	Systems with role-based access and action analysis

2) ENVID (ENVIRONMENTAL IDENTIFICATION)

ENVID [69] is a tool similar to HAZID but specifically focuses on identifying environmental risks and impacts. Utilized during project planning or design, ENVID ensures that environmental considerations are adequately addressed throughout the project lifecycle. This methodology examines various factors, including pollution, emissions, waste management, and ecosystem impacts. The critical features of ENVID include its focus on environmental issues such as emissions, spills, and waste and its alignment with environmental regulations, making it a critical component in securing environmental permits. By addressing these concerns early in the planning process, ENVID helps organizations effectively mitigate potential environmental risks.

3) HAZOP (HAZARD AND OPERABILITY STUDY)

HAZOP [70] is a structured technique for identifying and evaluating potential operational risks associated with complex processes. It systematically reviews a process's design, operation, and maintenance aspects to identify deviations from normal operations and analyze their causes and consequences. Conducted by a multidisciplinary team, HAZOP focuses specifically on process hazards. Key features of this methodology include its systematic and highly structured analysis, an emphasis on deviations from design or operational intent, and its widespread application in industries such as chemicals, oil and gas, and manufacturing. During the HAZOP analysis, specific parts of the process, known as nodes, are examined alongside potential deviations to assess what could go wrong, enabling organizations to manage risks and enhance safety proactively.

4) BOWTIE ANALYSIS

Bowtie analysis [71] is a graphical risk assessment tool that effectively visualizes the pathway from potential causes of a hazard to their possible consequences. This method maps out preventive and mitigative controls surrounding a central event, or "knot," representing the hazard. Bowtie diagrams facilitate a clearer understanding of the barriers that can either prevent hazards from occurring or mitigate their consequences if they materialize. Critical features of Bowtie analysis include its integration of qualitative and semi-quantitative analysis, which illustrates the causal relationships between hazards, top events, threats, and consequences. Additionally, it helps identify gaps in risk management and safety barriers, making it a valuable tool in major hazard industries such as oil and gas and aviation. By providing a comprehensive overview of risk scenarios, Bowtie analysis aids organizations in enhancing their safety and risk management strategies.

5) SIL ASSESSMENTS (SAFETY INTEGRITY LEVEL ASSESSMENTS)

SIL [72], [73] assessments evaluate the level of risk reduction required by a Safety Instrumented Function (SIF) and assign a Safety Integrity Level (SIL) based on that evaluation. The SIL serves as a measure of the reliability and risk-reducing capacity of the system, playing a crucial role in the functional safety assessment process. This assessment ensures that systems meet the necessary performance standards to prevent failures that could lead to accidents. Critical features of SIL assessments include the quantification of risks and system reliability and the definition of the required risk reduction. These assessments are integral to the IEC 61508 and IEC 61511 industrial-process safety standards. SIL levels range from 1 to 4, with level 4 representing the highest degree of safety integrity, thereby providing a framework for evaluating and enhancing the safety of industrial operations.

6) LOPA (LAYERS OF PROTECTION ANALYSIS)

LOPA [74] is a semi-quantitative risk assessment tool designed to evaluate the adequacy of existing protection layers in mitigating specific hazards. This methodology identifies and assesses multiple Independent Protection Layers (IPLs), such as alarms, safety shutdown systems, and operator responses, to determine whether sufficient safety barriers are in place to reduce risk to an acceptable level. LOPA is often used with HAZOP findings to analyze safety measures comprehensively. It examines the effectiveness and independence of each protection layer, helping organizations ascertain whether additional safety measures are necessary. The semi-quantitative nature of LOPA allows it to assign values to each protection layer, facilitating a clearer understanding of their contributions to overall risk reduction and supporting informed decision-making in safety management.

7) QRA (QUANTITATIVE RISK ASSESSMENT)

QRA [75] is a comprehensive risk analysis method that quantifies risks numerically, often employing probabilistic models to estimate the likelihood of hazardous events and their potential consequences. QRAs are particularly valuable in industries where catastrophic accidents may occur, such as explosions, fires, or toxic releases. Critical features of QRA include the calculation of accident frequencies and their potential impacts, making it essential for applications like land-use planning, facility siting, and regulatory compliance. Depending on the context, QRAs can involve both onshore and offshore models, providing critical data for decision-making in high-risk industries. By systematically evaluating risks, QRA aids organizations in implementing effective safety measures and enhancing overall operational safety.

8) RAMS (RELIABILITY, AVAILABILITY, MAINTAINABILITY, AND SAFETY)

RAMS [76] analysis is a comprehensive approach to assess systems or processes' reliability, availability, maintainability, and safety. It is widely applied in industries such as railways, aviation, and oil and gas to ensure systems operate effectively and safely throughout their lifecycle. RAMS analysis integrates performance and safety evaluations, focusing on operational efficiency while addressing potential risks. Key features of this methodology include an emphasis on lifecycle performance and maintenance, making it relevant during both the design and operational phases. Additionally, RAMS analysis incorporates risk and reliability models, providing organizations with a robust framework for enhancing system performance and ensuring safety.

III. METHODOLOGY

Figure 1 gives an overview of the proposed methodology process, which outlines the four-step process we followed in the overall evaluation of the OT environment.

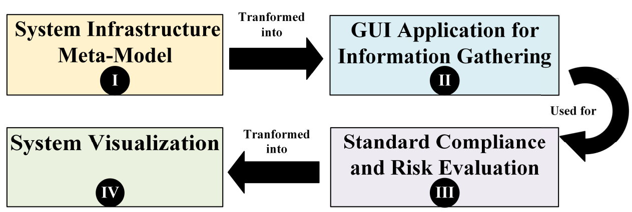

FIGURE 1. Step-wise illustration of proposed methodology for safety and security evaluation of OT environment.

A. SYSTEM INFRASTRUCTURE META-MODEL

In this step, we enhance the granularity of asset information. Figure 2 illustrates the entities, attributes, relationships, and

TABLE 3. Overview of safety related risk evaluation methodologies.

Method/Process	Description	Key Features	Application
HAZID (Hazard Identification)	Early-stage process to identify potential hazards in operations or designs.	• Qualitative • Multidisciplinary team-based • Forms basis for further risk assessment	Project planning, design, operations
ENVID (Environmental Identification)	Identifies environmental risks and impacts in projects or operations.	• Focuses on environmental factors • Ensures compliance with environmental regulations	Environmental impact assessment
HAZOP (Hazard and Operability Study)	Structured review to identify potential operational risks and deviations.	• Systematic • Focuses on deviations • Team-based • Process hazards	Chemical, oil & gas, and manufacturing industries
Bowtie Analysis	Visual tool to map risk pathways from hazards to consequences.	• Combines qualitative and semi-quantitative • Highlights barriers • Visual representation	Major hazard industries (oil & gas, aviation)
SIL Assessment (Safety Integrity Level)	Evaluates and assigns safety levels for safety instrumented systems.	• Quantifies risk reduction • Based on IEC 61508/61511 • SIL levels 0-4	Process safety, system reliability
LOPA (Layers of Protection Analysis)	Semi-quantitative analysis of protection layers to mitigate risks.	• Evaluates multiple safety layers • Identifies need for additional protections	Process industries, HAZOP follow-up
QRA (Quantitative Risk Assessment)	Quantifies risks using probabilistic models for high-hazard industries.	• Estimates frequencies and consequences • Often required for regulatory compliance	Onshore/offshore facilities, catastrophic event modeling
RAMS (Reliability, Availability, Maintainability, Safety)	Comprehensive assessment of system performance and safety over lifecycle.	• Ensures system efficiency • Combines performance and safety metrics	Railways, aviation, oil & gas

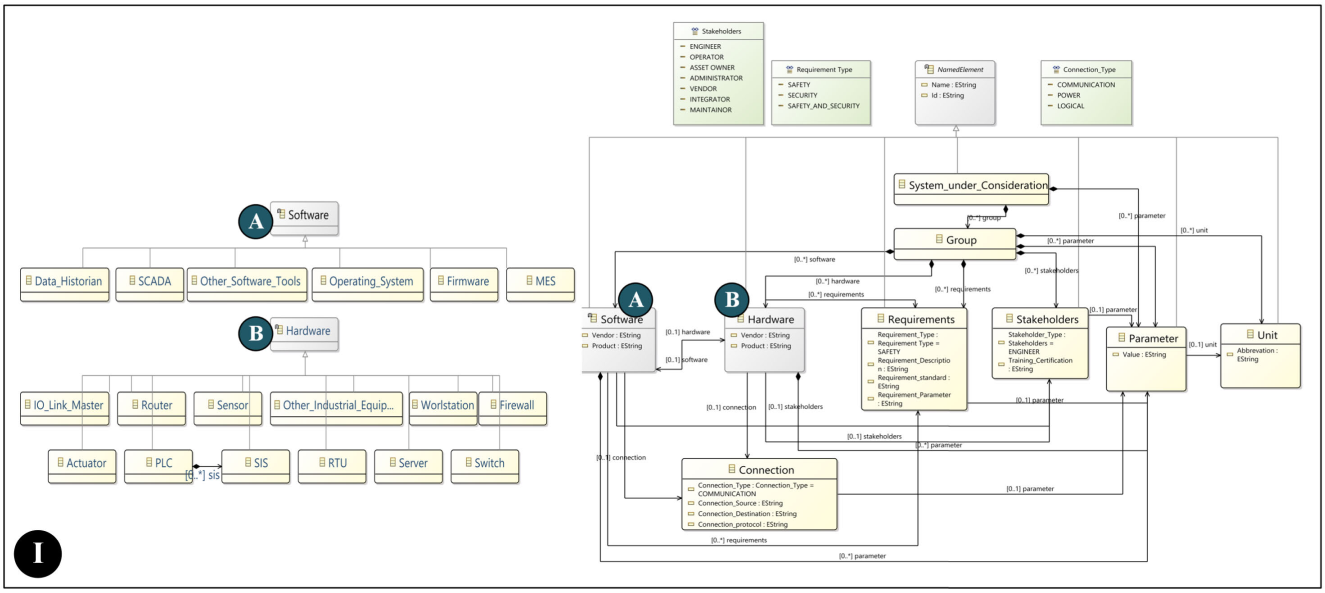

FIGURE 2. Meta-Model for OT system Infrastructure (on right), the extended view of software and hardware components class (on the left side) based on [77].

constraints that reflect the OT infrastructure, as outlined in the meta-model we have developed (see [77]). The process begins with defining the System under Consideration (SuC) and its associated groups (including zones, conduits, DMZs, etc.). Within each group, we can specify various software and hardware components, requirements, stakeholders, parameters, units, and the connections between different software and hardware components.

B. C# BASED GUI APPLICATION

Based on the OT infrastructure meta-model developed in the earlier stage, we transformed the model into a C#-based GUI application by leveraging our earlier work [77]; the application is crucial for improving user accessibility and interaction. Unfortunately, we cannot present or publish the code base due to the sponsoring industry's proprietary rights. However, we have provided sufficient information about the libraries used to replicate the work. The graphical user interface (GUI) enables users to visualize and manipulate the model, regardless of familiarity with the underlying complexities. This transformation reduces errors through intuitive controls, facilitates real-time data manipulation, and allows customization to meet specific user needs, addressing the challenges outlined in the introduction (Section I) for model-based evaluation. Additionally, the GUI supports integration with other tools, streamlining workflows and enhancing overall functionality. Ultimately, this conversion improves usability and promotes better decision-making based on insights from the meta-model. In this C#-based GUI application, we identify and catalog all assets within the OT system infrastructure, gathering detailed information on the system's components, connections, and configurations, as shown in Figure 3.

1) ACTIVE SCAN

We conduct active scans on existing IP addresses within the system, while users can manually enter target IP addresses for scanning. We utilize NMAP in the backend to retrieve information such as open ports, running services, operating systems, and MAC addresses. This real-time information aids in making informed decisions regarding whether security and safety requirements are met. If not, appropriate actions can be taken to address any issues. Additionally, the output data from the scan can be saved as parameters, allowing users to select the components to which these parameters will be assigned. These parameters can then be used to substantiate claims about fulfilled requirements. The technologies used include ***NMAP***, an external tool for network scanning, and ***System.Diagnostics***, a library that manages process execution and captures output.

2) PASSIVE SCAN

Users can select the network interface for passive scanning. During this process, we capture communication between components, including MAC addresses, IP addresses, and product and vendor names. This information serves two primary purposes: it allows users to identify communicating devices within the network and detect unauthenticated and unidentified connections. In the background, we utilize WinPcap as a third-party application for packet capturing. Additionally, we have implemented functionality to import PCAP files for comprehensive network traffic analysis. The technologies used include ***WinPcap***, a third-party library for capturing network packets, and ***PCAP files***, which are utilized for importing and analyzing network traffic.

3) INSTALLED APPLICATIONS

The primary objective of obtaining information about installed applications and their version numbers is to monitor potential attack points. Given the history of attacks exploiting installed applications, prioritizing this task is essential. Additionally, these installed applications can be queried for existing vulnerabilities. The technologies used include ***System.Management***, a package that interacts with system management and retrieves information about installed applications.

4) USB DEVICE SCAN

We aim to identify all potential USB ports on the system to gain insight into possible attack entry points. This awareness enables users to take preventive measures, such as disabling unused USB ports, thereby enhancing overall security. The technologies used include ***System.Management***, a package utilized to interact with system management and retrieve information about USB ports.

5) SIMCARD SCAN

We have explored the potential for analyzing SIM card connections within the network. However, we currently lack a practical use case to test this capability effectively. The technologies used include ***System.Management***, a package utilized for querying system information related to modems.

6) WIRELESS DEVICE SCAN

We aimed to identify wireless devices present in the network, including Bluetooth, ZigBee, WirelessHART, and others. This process requires an appropriate adapter, such as an IEEE 802.15.4 sniffer, to capture devices in the vicinity. The technologies used include ***TheHand.Net.Bluetooth***, a package for querying Bluetooth radio hardware properties; ***XBeeLibrary.Core***, a package for querying system information related to Zigbee devices; and ***System.Management and Network Management Libraries***, the package for obtaining information related to WirelessHART and other devices.

7) VPN CONNECTION

We aim to gather information about the VPN connections established on the system. This allows users to identify unauthenticated external communications and take proactive mitigation measures based on the insights obtained. The technologies used include ***Network Management Libraries***, which are utilized for querying and managing VPN connection information.

8) JTAG DEVICES

We aimed to gather information on JTAG devices, which typically require third-party libraries or SDKs provided by hardware manufacturers and open-source tools like OpenOCD. Some popular JTAG devices include Xilinx, Altera/Intel, FTDI, and OpenOCD. The technologies used include ***OpenOCD***[1], an open-source tool utilized for JTAG device interaction.

9) DATASHEET SCAN

To enhance data extraction and analysis processes as shown in Figure 4, we leverage AI-based solutions such as Google

[1] https://github.com/openocd-org/openocd

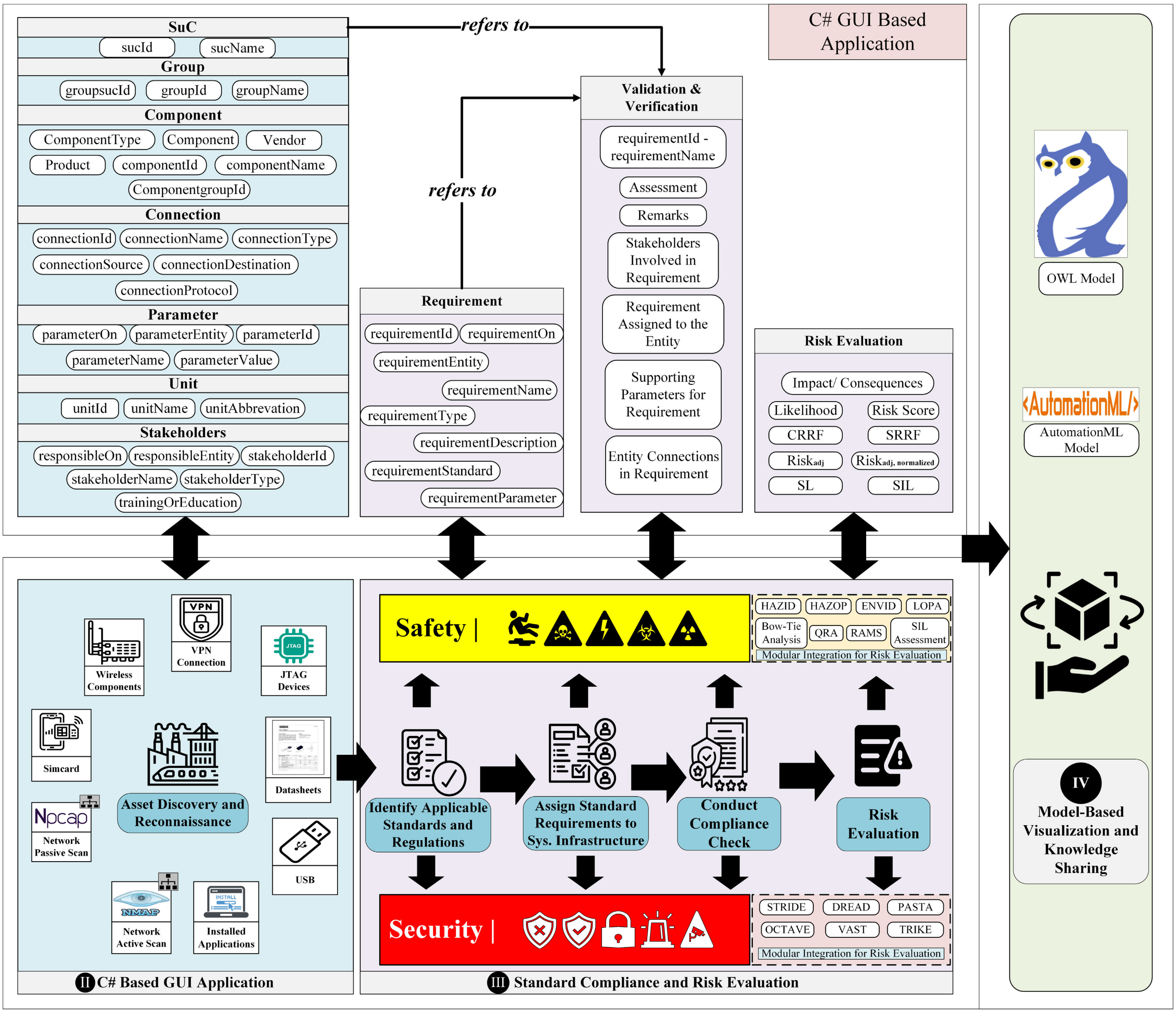

FIGURE 3. Detailed Illustration of Methodology from Step II to Step IV derived from [77], [78], and [79].

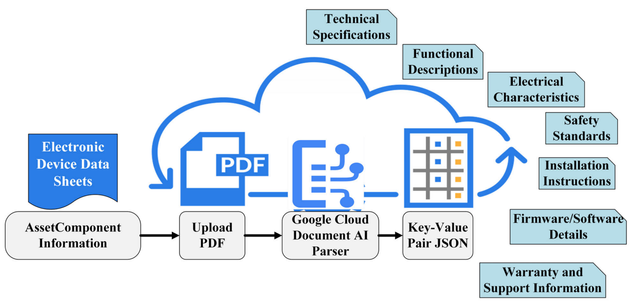

FIGURE 4. Extraction of key-value pair from datasheets based on [79].

Cloud Document AI.[2] This tool efficiently handles various document types, including electronic data sheets, EDDL files, and PDFs containing data historian information. We can extract key-value pairs by uploading these documents to Google Cloud Document AI, facilitating structured data retrieval and analysis [79]. This process enables quick access to non-critical information such as technical specifications, functional descriptions, electrical characteristics, safety standards, installation instructions, firmware/software details, and warranty and support information. Document AI excels at identifying key data points and their corresponding values, regardless of the document's format or complexity.

[2]https://cloud.google.com/document-ai?hl=en

C. STANDARD COMPLIANCE AND RISK EVALUATION

This section is built upon the previous work [77] to implement a standard compliance methodology, which is described in subsubsections III-C1 through III-C3. and for the risk evaluation III-C4 we use [80], [81]

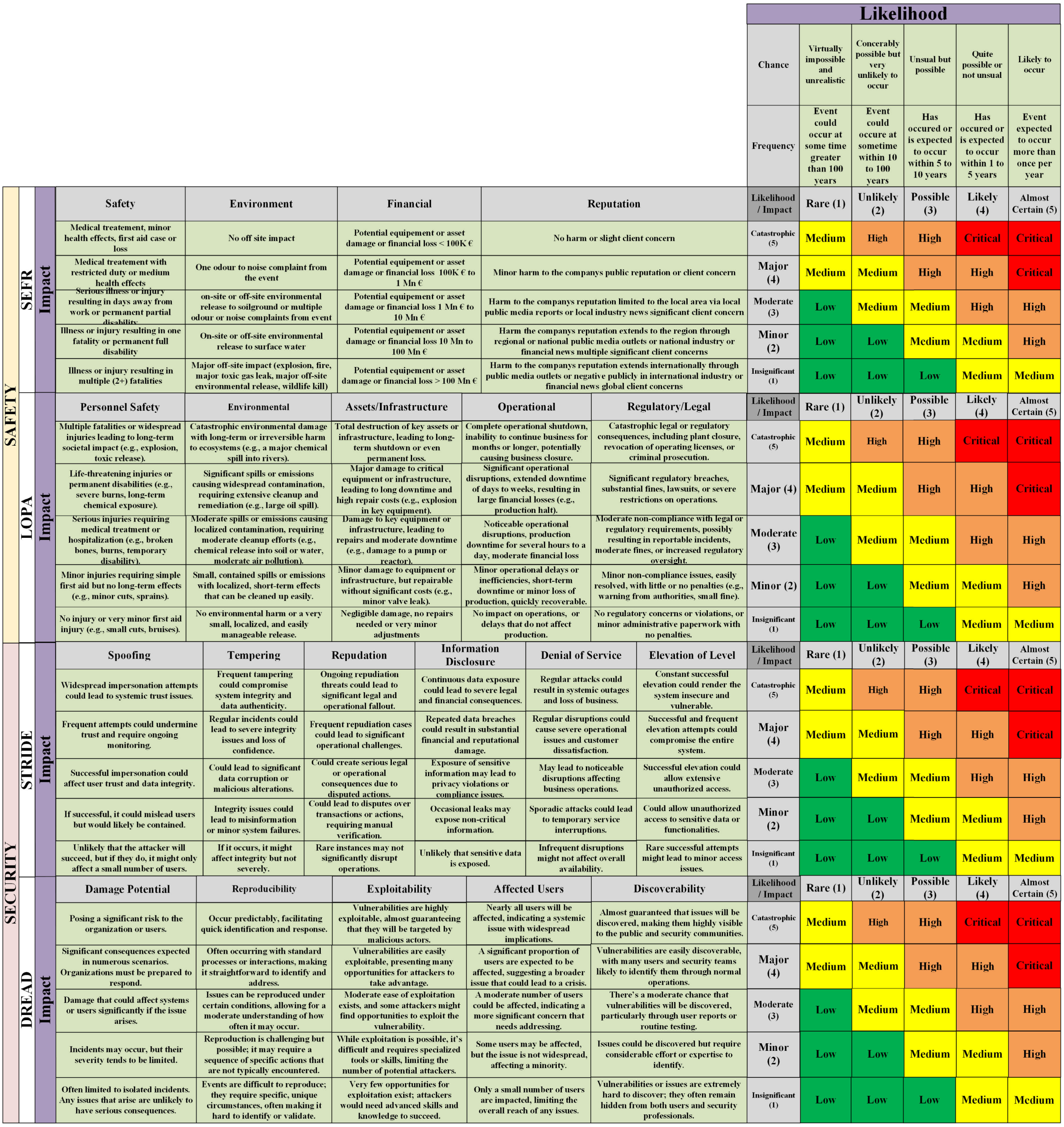

FIGURE 5. Illustration of Risk matrix for likelihood and impact with corresponding scores for safety methodologies and security threat modeling frameworks for risk evaluation.

1) IDENTIFY APPLICABLE STANDARDS AND REGULATIONS

At this stage, we conduct a thorough review of relevant regulations, standards, and guidelines to determine the specific requirements that components or systems must meet. Industry experts identify applicable regulatory mandates, industry standards, internal policies, and contractual obligations. Safety and security requirements include safety regulations, quality criteria, and security protocols as part of this methodology. We adopt a modular integration approach to incorporate safety and security standards based on specific needs, allowing for the consolidation of various standards.

2) ASSIGN STANDARD REQUIREMENTS TO SYSTEM INFRASTRUCTURE

After identifying the standard requirements, a compliance committee—typically comprising asset owners, vendors, system integrators, and other stakeholders—allocates these requirements to the corresponding asset components or systems. This stage involves mapping each requirement to a specific component or system (or group of components) and assigning parameters that ensure the concrete fulfillment of the requirement criteria.

3) CONDUCT COMPLIANCE CHECK

This stage involves assessing the compliance of asset components or systems with the identified requirements. Various methods, including inspections, audits, tests, and reviews, ensure adherence to regulatory standards and internal policies. We conduct a preliminary assessment in this stage, emphasizing that human involvement must be noticed. Third-party audit and certification bodies may perform the actual safety and security compliance assessment. The assessment results determine whether the asset component or system meets the specified compliance criteria or if further actions are required to address non-compliance issues.

4) RISK EVALUATION

At this stage, we integrate risk evaluation by aligning safety methodologies (e.g., LOPA and SEFR/HAZID) with security threat modeling frameworks (e.g., STRIDE and DREAD). For demonstration purposes, STRIDE is employed to identify potential threats and prioritize them based on their severity and likelihood. DREAD is then applied to further assess these threats, focusing on their severity and likelihood. Concurrently, SEFR/HAZID is utilized to identify and analyze potential hazards, while LOPA quantifies the effectiveness of protective layers specific to the use case. Other methods (refer to Sections II-A and II-B) can be incorporated following a similar structure to address additional applications as shown in the proposed risk matrix, illustrated in Figure 5, demonstrates the integration of safety methodologies and security threat modeling frameworks for comprehensive risk assessment. The following equations assist in evaluating control measures:

$$R = I \times L \tag{1}$$

where R is the risk score, I is the impact score, and L is the likelihood score.

For Security Risk Evaluation, the Cyber Risk Reduction Factor (CRRF) represents the proportion of cyber risk that has been mitigated through the implementation of security controls.

For Safety Risk Evaluation, the Safety Risk Reduction Factor (SRRF) is a quantitative measure used to assess the extent to which the risk of a hazardous event or safety issue has been reduced through safety controls or mitigation strategies. It is calculated as follows:

$$\begin{aligned} &CRRF/SRRF \\ &= \frac{\text{Risk Before Controls} - \text{Risk After Controls}}{\text{Risk Before Controls}} \end{aligned} \tag{2}$$

where $0 \leq CRRF/SRRF \leq 1$.

TABLE 4. Component/System assessment of safety and security based on SIL, SL.

System Assessment	Condition
Safe & Secure	• High (SIL 3-4) • High (SL 3-4)
Safe but Partly Secure	• High (SIL 3-4) • Medium (SL 2)
Secure but Partly Safe	• Medium (SIL 2) • High (SL 3-4)
Partly Safe & Partly Secure	• Medium (SIL 2) • Medium (SL 1-2)
Insecure but Safe	• High (SIL 3-4) • Low (SL 1)
Insecure & Unsafe	• Low (SIL 1) • Low (SL 1)
Unsafe but Secure	• Low (SIL 1) • High (SL 3-4)
Unsafe but Partly Secure	• Low (SIL 1) • Medium (SL 2)

For the individual component,

$$R_{\text{adj}} = \text{Initial Risk of Component} \times (1 - CRRF/SRRF) \tag{3}$$

where R_{adj} represents Adjust for CRRF/SRRF

For the whole system,

$$CRRF_{\text{total}}/SRRF_{\text{total}} = 1 - \prod (1 - CRRF_i/SRRF_i) \tag{4}$$

where $CRRF_i/SRRF_i$ represents max. and min. individual control's CRRF/SRRF.

$$\begin{aligned} R_{\text{adj}} = &\text{ Maximum Initial Risk in System} \\ &\times (1 - CRRF_{\text{total}}/SRRF_{\text{total}}) \end{aligned} \tag{5}$$

For an individual or whole system,

$$R_{\text{adj, normalized}} = \frac{R_{\text{adj}}}{5} \tag{6}$$

where $R_{\text{adj, normalized}}$ represents Normalized Adjusted Risk[3]

Compare to SL-T or SIL to determine acceptability:

$$\text{Status} = \begin{cases} \text{Acceptable} & \text{if } R_{\text{adj, normalized}} \leq SL/SIL \\ \text{Unacceptable} & \text{if } R_{\text{adj, normalized}} > SL/SIL \end{cases} \tag{7}$$

Following Equation 7, if the risk is deemed unacceptable the following decisions could be made:

- **Additional Countermeasures:** Reduce the risk by implementing more controls or improving existing ones.
- **Accept Risk:** Acknowledge and tolerate the risk if mitigation is too costly or the impact is minimal.
- **Discard Risk:** Avoid the activity or process causing the risk.
- **Transfer Risk:** Shift the risk to a third party, such as through insurance or outsourcing.

Based on the assessed risk and the corresponding SIL and SL values, we can identify the safety and security assessment of the system, as shown in Table 4.

[3]Normalized Adjusted Risk ranges from 1 to 25, while SIL/SL ranges from 0 to 4. To normalize, Adjusted Risk is divided by 5.

D. SYSTEM VISUALIZATION: MODEL-BASED VISUALIZATION AND KNOWLEDGE SHARING

This step transforms all the information, from asset components to risk evaluation, collected via the C# GUI-based application into a system model for visual representation. This model is utilized for knowledge sharing, decision-making, and further analysis. The following strategy outlines the conversion of JSON data from the application to OWL and AutomationML. Transforming from a JSON-based repository to OWL and AutomationML is advantageous for industrial applications with large datasets and frequent queries. While JSON is lightweight and efficient for basic data exchange, it becomes less scalable due to its redundancy and slower query performance as data grows. In contrast, OWL offers faster querying with optimized indexing and reasoning, making it ideal for complex relationships. AutomationML excels with hierarchical data and efficient tree traversal. Both OWL and AutomationML are more space-efficient due to normalized structures, offering better scalability for large datasets. Thus, for long-term efficiency and performance, OWL and AutomationML outperform JSON in data-intensive scenarios. The technologies used for OWL include the ***dotNetRdf.Ontology*** libraries, which provide an API for creating and manipulating OWL ontologies, For AutomationML, we used the ***Aml.Engine*** libraries, which offer methods for creating and processing AutomationML documents.

Mapping and Assertions from JSON to OWL [82]:

- JSON Objects → OWL Classes.
- JSON Properties/Attributes → OWL Data Properties or Object Properties.
- JSON Arrays → OWL Individuals.

Mapping and Assertions from JSON to AutomationML [83]:

- Classes and Instances: Map JSON objects to AutomationML elements like `InstanceHierarchy` or `InternalElement`.
- Attributes: Map JSON properties to `Attribute` elements in AutomationML.
- Relations: Model JSON object relationships using `InternalLink` for associations and `RoleClass` for classification.

IV. DEMONSTRATION

We demonstrate the proposed methodology process with a use case illustrated in Figure 6, which shows the deployment of an automated smart factory setup. This setup includes an ABB collaborative robotic arm and critical components, including the SINUMERIK PCU and NCU controllers, which manage the EMCO MAXXTURN 45 CNC milling machine. The network is secured through MGUARD routers, enterprise security gateways, and managed switches for handling data traffic. A remote maintenance server is enabled via secure connections, and remote communication is facilitated by an OPC UA server connected to multiple hosts. The robotic arm has appropriate tools and end-effectors in the CNC machine's workspace. The completed workpiece from the CNC machine is picked up by the robotic arm and placed in a nearby tray for further processing. This integrated approach enables real-time monitoring, predictive maintenance, and efficient handling of maintenance tasks, thereby optimizing production processes in the CNC machining environment. Additionally, it helps identify potential security vulnerabilities. Unfortunately, we only had one use case available for demonstration: a non-critical smart factory setup. However, the approach can also be implemented in critical infrastructure sectors such as energy grids, communication networks, health, water supply, or transportation systems.

A. C# BASED USER APPLICATION FOR INFORMATION GATHERING

As shown in Figure 3, in Step II, we gather the system infrastructure information (c.f. Subsection III-B). The collected information is then used for further processing, as outlined in [78], [79], [81].

B. STANDARD COMPLIANCE AND RISK EVALUATION

In Table 6, we combine two evaluation aspects: the standard compliance check and risk evaluation. Together, these aspects provide a comprehensive overview of the risk controls that can be implemented, based on standards, to mitigate safety and security risks. Using the use case illustrated in Figure 6, the following evaluation is presented in the subsections:

1) STANDARD COMPLIANCE:

We adopt IEC 62443 to address security requirements and IEC 61508 to ensure compliance with safety requirements. Table 6 outlines the safety and security requirements for each component of the use case system, along with the relevant clauses where applicable. In the context of IEC 62443, the Security Level for Target (SL-T) defines the security objectives based on a risk assessment process (as described in IEC 62443-3-2). The Security Level for Capability (SL-C) ensures that the product or system has the potential to meet these objectives (as specified in IEC 62443-4-1 and IEC 62443-4-2). Finally, the Security Level for Achievement (SL-A) evaluates whether the implemented security measures meet the SL-T objectives in practice (as defined in IEC 62443-3-3 and IEC 62443-2-4). For simplicity, we focus on SL-A, as specified in IEC 62443-3-3, and refer to it as "SL" in our analysis. Similarly, in IEC 61508, Part 2 specifies the hardware design and system architecture required for risk mitigation, while Part 3 outlines the software requirements for achieving SIL compliance, if applicable. In our approach, we focus exclusively on "SIL" for the assessment. Typically, SIL is assigned to safety-critical components that perform safety instrumented functions (SIF). In this analysis, we have considered all components embedded with safety instrumented functions (as defined in IEC 61508-4 §3), which is why all components are assigned a SIL.

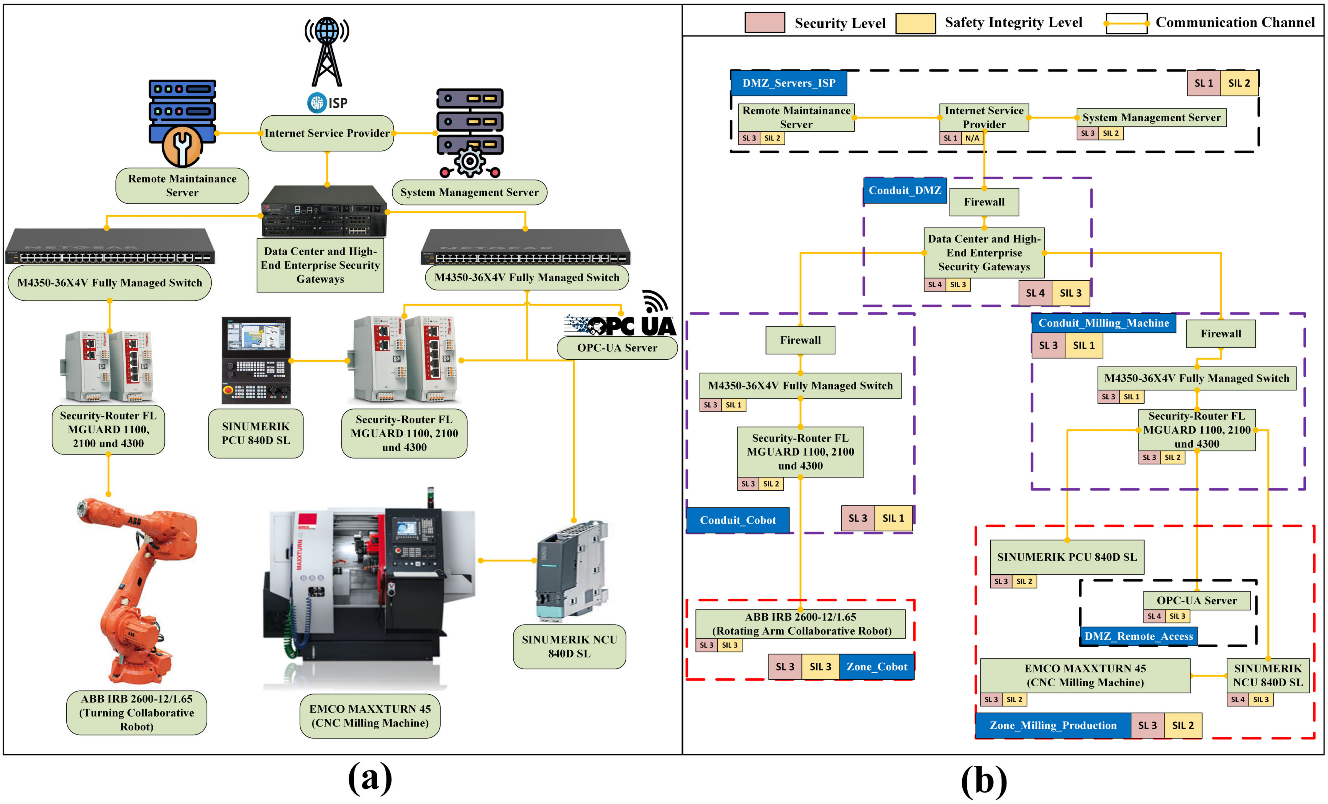

FIGURE 6. (a). Milling and Cobot Use Case: Pilot Factory Architecture, (b). Block design of Pilot Factory Architecture in Compliance.

TABLE 5. Illustration of risk evaluation, the safety and security assessment for each component, and the overall pilot factory use case.

Component/System	$CRRF$	Security R_{adj}	Security $R_{\text{adj, norma}}$	Security Status (In SL)	$SRRF$	Safety R_{adj}	Safety $R_{\text{adj, norma}}$	Safety Status (In SIL)	Assessment
Remote Maintenance Server	0.34	5.94	1.18	$1.18 \leq 3$	0.5	4	0.8	$0.8 \leq 2$	Secure but Partly Safe
Internet Service Provider (ISP)	0	0	0	$0 \leq 1$	N/A	N/A	N/A	N/A	Insecure
System Management Server	0.5	6	1.2	$1.2 \leq 3$	0.5	4	0.8	$0.8 \leq 2$	Secure but Partly Safe
Data Center and High-End Security Gateways	0.5	8	1.6	$1.6 \leq 4$	0.5	6	1.2	$1.2 \leq 3$	Safe and Secure
Fully Managed Switch 1	0.5	8	1.6	$1.6 \leq 3$	0.5	4	0.8	$0.8 \leq 1$	Unsafe but Secure
Fully Managed Switch 2	0.5	8	1.6	$1.6 \leq 3$	0.5	4	0.8	$0.8 \leq 1$	Unsafe but Secure
Security-Router FL MGUARD 1	0.5	8	1.6	$1.6 \leq 3$	0.5	4	0.8	$0.8 \leq 2$	Secure but Partly Safe
Security-Router FL MGUARD 2	0.5	8	1.6	$1.6 \leq 3$	0.5	4	0.8	$0.8 \leq 2$	Secure but Partly Safe
SINUMERIK PCU	0.5	8	1.6	$1.6 \leq 3$	0.5	6	1.2	$1.2 \leq 2$	Secure but Partly Safe
OPC UA Server	0.5	8	1.6	$1.6 \leq 4$	0.5	4	0.8	$0.8 \leq 3$	Safe and Secure
Turning Collaborative Robot	0.5	10	2	$2 \leq 3$	0.5	6	1.2	$1.2 \leq 3$	Safe and Secure
CNC Milling Machine	0.5	10	2	$2 > 1$	0.5	6	1.2	$1.2 \leq 2$	Partly Safe and Insecure
SINUMERIK NCU	0.5	8	1.6	$1.6 \leq 4$	0.5	6	1.2	$1.2 \leq 3$	Safe and Secure
Overall System	**0.5**	**10**	**2**	$\mathbf{2 \leq 2}$	**0.75**	**3**	**0.6**	$\mathbf{0.6 \leq 1}$	**Unsafe but Partly Secure**

2) RISK EVALUATION:

In this analysis, we utilize Subsections II-A and II-B to devise a risk matrix. This matrix considers the likelihood of an incident occurring (ranging from Rare to Almost Certain) and its impact or consequence on the system (ranging from Insignificant to Catastrophic), along with an associated scoring system. We also experimented with two safety methods (LOPA and SEFR/HAZID) and two security methods (STRIDE and DREAD), as illustrated in Figure 5. The methods from Section II can be selected and adjusted as needed to refine the matrix. Using this matrix, as detailed in Table 6, the **likelihood (L)** and **impact (I)** for each

TABLE 6. Illustration of use case components: security requirements in light red, safety requirements in light yellow, ✔ for acceptable risks, and ✖ for unacceptable risks.

Group	Component	Compliance Requirement	Process/ Method Likelihood	Max. Likeli-hood (L)	Conseq./ Impact (I)	Risk (R) (IxL)	SL/ SIL	Risk Control	Rev. Like-lihood (RL)	Rev. Risk (RR) (RLxI)
DMZ Servers ISP	Remote Maintainance Server ✔	Ensure secure access, data encryption in transit, authentication, and access control. Key requirements include boundary protection, secure remote access, and activity logging (IEC 62443-3-3 §SR 1.1, 1.2, 3.1, 7.8).	Spoofing: **Unlikely (2)**, Tampering: **Possible (3)**, Elevation of Privilege: **Possible (3)**	Possible (3)	Moderate (3)	9	SL 3	Multi-factor authentication, VPN encrypted tunnels, role-based access control, log monitoring, intrusion detection.	Unlikely (2)	6
	Remote Maintainance Server✔	Data integrity checks, backups, and redundancy minimize downtime from data corruption (IEC 61508-2 §7.4.8, IEC 61508-3 §7.4.4.1).	Personal Safety: **Possible (3)**, Environmental: **Rare (1)**, Asset/Infrastructure: **Possible (3)**, Operational: **Likely (4)**, Regulatory/Legal: **Possible (3)**	Likely (4)	Minor (2)	8	SIL 2	Continuous security monitoring, SIEM integration, access time restrictions.	Unlikely (2)	4
	Internet Service Provider✔	Secure external connections, boundary protection through firewalls, and secure communication protocols. Monitor for attacks like DDoS or man-in-the-middle (IEC 62443-3-3 §SR 5.1, 5.2, 4.1, 3.3).	Denial of Service: **Unlikely (2)**, Information Disclosure: **Unlikely (2)**, Tampering: **Rare (1)**	Unlikely (2)	Major (4)	8	SL 1	DDoS mitigation tools, redundant connections	Unlikely (2)	8
	Internet Service Provider✔	Emergency shutdown and automated restart systems prevent extended shutdowns and production losses (IEC 61508-2 §7.5.2).	Personal Safety: **Rare (1)**, Environmental: **Rare (1)**, Asset/Infrastructure: **Unlikely (2)**, Operational: **Likely (4)**, Regulatory/Legal: **Unlikely (2)**	Likely (4)	Minor (2)	8	N/A	SLAs, geo-redundancy	Unlikely (2)	4
	System Management Server✔	Identity and access management, secure logging, and system integrity checking. Ensure all updates are verified, and control over permissions and authorizations is maintained (IEC 62443-3-3 §SR 1.2, 6.2, 3.2, 7.7).	Elevation of Privilege: **Likely (4)**, Repudiation: **Likely (4)**	Likely (4)	Moderate (3)	12	SL 3	Privileged access management, encryption, endpoint detection and response, security audits	Unlikely (2)	6
	System Management Server✔	SIS and alarms prevent disruptions from escalating into safety risks (IEC 61508-2 §7.4.7, IEC 61508-3 §7.5.2.2).	Personal Safety: **Unlikely (2)**, Environmental: **Rare (1)**, Asset/Infrastructure: **Likely (4)**, Operational: **Likely (4)**, Regulatory/Legal: **Possible (3)**	Likely (4)	Minor (2)	8	SIL 2	Automated configuration management, network segmentation, vulnerability scanning.	Unlikely (2)	4
Conduit DMZ	Data Center and High-End Enterprise Security Gateways✔	Encryption, integrity protection, firewall configurations, and intrusion detection systems. Regular security audits and patch management (IEC 62443-3-3 §SR 4.1, 3.1, 5.2, 3.4, 7.2)	Denial of Service: **Likely (4)**, Tampering: **Possible (3)**, Information Disclosure: **Likely (4)**	Likely (4)	Major (4)	16	SL 4	Firewalls, IDS/IPS, security zoning, strong encryption protocols, physical security controls, vulnerability scanning and penetration testing	Unlikely (2)	8
	Data Center and High-End Enterprise Security Gateways✔	Cybersecurity and backups protect against data loss and integrity issues (IEC 61508-2 §7.4.11).	Personal Safety: **Rare (1)**, Environmental: **Rare (1)**, Asset/Infrastructure: **Likely (4)**, Operational: **Likely (4)**, Regulatory/Legal: **Possible (3)**	Likely (4)	Moderate (3)	12	SIL 3	Data Loss Prevention, Zero Trust Architecture, continuous penetration testing.	Unlikely (2)	6
Conduit Cobot	Fully Managed Switch 1✔	Ensure network segmentation, monitor for unauthorized access, enforce secure configurations (disable unused ports). (IEC 62443-3-3 §SR 5.1, 2.1, 3.3, 7.3)	Spoofing: **Likely (4)**, Tampering: **Likely (4)**, Denial of Service: **Possible (3)**	Likely (4)	Major (4)	16	SL 3	Port security, Network Access Control, firmware updates	Unlikely (2)	8
	Fully Managed Switch 1✔	Network segmentation and firewalls prevent unauthorized lateral movement (IEC 61508-2 §7.4.11).	Personal Safety: **Rare (1)**, Environmental: **Rare (1)**, Asset/Infrastructure: **Likely (4)**, Operational: **Likely (4)**, Regulatory/Legal: **Unlikely (2)**	Likely (4)	Minor (2)	8	SIL 1	Network behavior analysis, automatic port lockdown.	Unlikely (2)	4
	Security-Router FL MGUARD1✔	Firewalls and VPN tunnels must be configured, regular firmware updates and IDS/IPS (IEC 62443-3-3 §SR 5.2, 7.7, 3.4)	Denial of Service: **Likely (4)**, Spoofing: **Likely (4)**, Information Disclosure: **Possible (3)**	Likely (4)	Major (4)	16	SL 3	Secure routing protocols, VPN tunnels, firewall rules, IDS/IPS, regular firmware updates.	Unlikely (2)	8
	Security-Router FL MGUARD1✔	Encryption and access controls protect data confidentiality and integrity (IEC 61508-2 §7.4.11).	Personal Safety: **Unlikely (2)**, Environmental: **Rare (1)**, Asset/Infrastructure: **Likely (4)**, Operational: **Likely (4)**, Regulatory/Legal: **Possible (3)**	Likely (4)	Minor (2)	8	SIL 2	Encrypted traffic analytics, redundancy, automatic firmware updates	Unlikely (2)	4
Conduit Milling Machine	Fully Managed Switch 2✔	Ensure network segmentation, monitor for unauthorized access, enforce secure configurations (disable unused ports) (IEC 62443-3-3 §SR 5.1, 2.1, 3.3, 7.3)	Spoofing: **Likely (4)**, Tampering: **Likely (4)**, Denial of Service: **Possible (3)**	Likely (4)	Major (4)	16	SL 3	Port security, Network Access Control, firmware updates	Unlikely (2)	8
	Fully Managed Switch 2✔	Network segmentation and firewalls prevent unauthorized lateral movement (IEC 61508-2 §7.4.11).	Personal Safety: **Rare (1)**, Environmental: **Rare (1)**, Asset/Infrastructure: **Likely (4)**, Operational: **Likely (4)**, Regulatory/Legal: **Unlikely (2)**	Likely (4)	Minor (2)	8	SIL 1	Network behavior analysis, automatic port lockdown.	Unlikely (2)	4
	Security-Router FL MGUARD2✔	Firewalls and VPN tunnels must be configured, regular firmware updates and IDS/IPS. (IEC 62443-3-3 §SR 5.2, 7.7, 3.4)	Denial of Service: **Possible (3)**, Spoofing: **Likely (4)**, Information Disclosure: **Likely (4)**	Likely (4)	Major (4)	16	SL 3	Secure routing protocols, VPN tunnels, firewall rules,IDS/IPS, regular firmware updates.	Unlikely (2)	8
	Security-Router FL MGUARD2✔	Loss of confidentiality and integrity of data. Redundancies prevent operational failures from miscommunication (IEC 61508-2 §7.4.8, IEC 61508-3 §7.4.4.2).	Personal Safety: **Unlikely (2)**, Environmental: **Rare (1)**, Asset/Infrastructure: **Likely (4)**, Operational: **Likely (4)**, Regulatory/Legal: **Possible (3)**	Likely (4)	Minor (2)	8	SIL 2	Encrypted traffic analytics, redundancy, automatic firmware updates	Unlikely (2)	4
Zone Cobot	Turning Collaborative Robot✔	Control network access, ensure secure communication between the robot and central controller, restrict physical access (IEC 62443-3-3 §SR 1.2, 3.1, 2.1)	Spoofing: **Likely (4)**, Tampering: **Likely (4)**	Likely (4)	Catastrophic (5)	20	SL 3	Physical safety measures, secure communication protocols, regular software updates, and integrity, robot behavior monitoring	Unlikely (2)	10
	Turning Collaborative Robot✔	Injury to operators, damage to property. PPE and safeguards protect operators and property(IEC 61508-2 §7.5.2, IEC 61508-3 §7.5.2.2).	Personal Safety: **Possible (3)**, Environmental: **Rare (1)**, Asset/Infrastructure: **Rare (1)**, Operational: **Possible (3)**, Regulatory/Legal: **Likely (4)**	Likely (4)	Moderate (3)	12	SIL 3	Advanced proximity sensors, redundant safety systems, periodic safety drills.	Unlikely (2)	6
Zone Milling Machine & DMZ Remote Access	SINUMERIK PCU✔	Ensure secure software environments, access control for operators, and protection of critical settings (IEC 62443-3-3 §SR 1.2, 7.3, 7.1)	Elevation of Privilege: **Possible (3)**, Tampering: **Likely (4)**	Likely (4)	Major (4)	16	SL 3	Whitelisting, input validation, strong authentication, secure boot mechanisms.	Unlikely (2)	8
	SINUMERIK PCU✔	Physical damage to equipment or injury to operators. Pressure relief valves (PRV), fail-safe systems (IEC 61508-2 §7.4.7, IEC 61508-3 §7.5.2.2).	Personal Safety: **Possible (3)**, Environmental: **Rare (1)**, Asset/Infrastructure: **Likely (4)**, Operational: **Likely (4)**, Regulatory/Legal: **Possible (3)**	Likely (4)	Moderate (3)	12	SIL 2	Secure boot, behavioral monitoring	Unlikely (2)	6
	OPC UA Server✔	Secure communication protocols, identity and access control, and system monitoring. (IEC 62443-3-3 §SR 3.1, 1.1, 6.1)	Tampering: **Likely (4)**, Spoofing: **Likely (4)**, Information Disclosure: **Possible (3)**	Likely (4)	Major (4)	16	SL 4	Encryption, authentication and authorization, anomaly detection systems, Regular patching of OPC UA server software.	Unlikely (2)	8
	OPC UA Server✔	Miscommunication between components, operational failure. Safety interlocks and emergency stops protect personnel and equipment (IEC 61508-2 §7.4.8, IEC 61508-3 §7.4.4.2).	Personal Safety: **Rare (1)**, Environmental: **Likely (4)**, Asset/Infrastructure: **Likely (4)**, Operational: **Likely (4)**, Regulatory/Legal: **Possible (3)**	Likely (4)	Minor (2)	8	SIL 3	Intrusion detection for industrial protocols, role-based authorization, detailed auditing.	Unlikely (2)	4
	CNC Milling Machine✖	Secure configuration settings, monitor communications, and implement authentication for operators (IEC 62443-3-3 §SR 7.3, 3.3, 1.1)	Tampering: **Likely (4)**, Denial of Service: **Likely (4)**	Likely (4)	Catastrophic (5)	20	SL 1	Whitelisting of commands and authentication for users, use encrypted communication, safety checks, redundant safety systems	Unlikely (2)	10
	CNC Milling Machine✔	Injury to personnel or equipment damage. Maintenance and hazard detection prevent equipment damage or injury (IEC 61508-2 §7.4.6, IEC 61508-3 §7.4.5.2).	Personal Safety: **Possible (3)**, Environmental: **Rare (1)**, Asset/Infrastructure: **Possible (3)**, Operational: **Likely (4)**, Regulatory/Legal: **Possible (3)**	Likely (4)	Moderate (3)	12	SIL 2	SIL-rated components, periodic maintenance, emergency power cut-off.	Unlikely (2)	6
	SINUMERIK NCU✔	Protect the network control unit with secure access controls and monitoring for abnormal activity (IEC 62443-3-3 §SR 1.1, 3.3)	Elevation of Privilege: **Possible (3)**, Tampering: **Likely (4)**	Likely (4)	Major (4)	16	SL 4	Strong authentication, encryption and secure communication channels, anomaly detection, system health checks and updates.	Unlikely (2)	8
	SINUMERIK NCU✔	Equipment damage, operator injury (IEC 61508-2 §7.4.7, IEC 61508-3 §7.5.2.2).	Personal Safety: **Possible (3)**, Environmental: **Unlikely (2)**, Asset/Infrastructure: **Likely (4)**, Operational: **Likely (4)**, Regulatory/Legal: **Possible (3)**	Likely (4)	Moderate (3)	12	SIL 3	Real-time monitoring, secure firmware updates.	Unlikely (2)	6

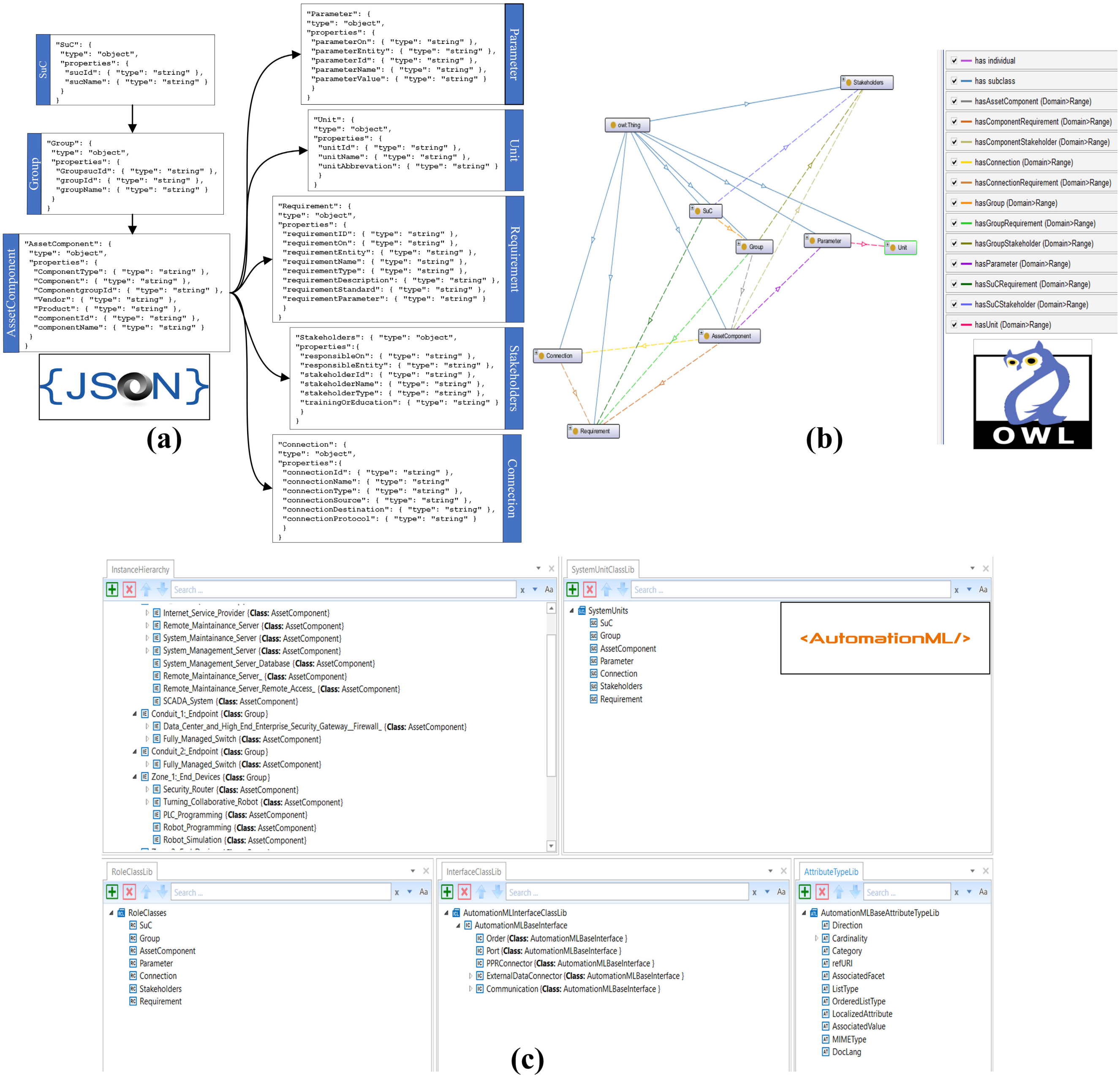

FIGURE 7. (a). JSON Schema of Database, (b).Graphical Illustration of Relationships in (OWL) Ontological Classes, (c). Illustration of AutomationML Class Libraries.

component were estimated based on the expertise of the risk assessor and feedback from stakeholders. The **risk (R)** of each component was then calculated using Equation 1. SL/SIL were determined through a standard compliance process. Risk controls were applied to components to adjust the **revised likelihood (RL)** and recalculate the **revised risk (RR)**. To assess the acceptability of the revised safety and security risks, Equations 2 through 7 were used. If the risk remains unacceptable, further decisions and mitigation measures can be applied. Based on these assessments, the overall level of safety and security in the system can be determined, as shown in Table 4. The illustration of usecase on individual components and the overall system for safety and security requirement compliance and risk evaluation is shown in Table 6 and the detailed risk evaluation and assessment follows in Table 5.

C. SYSTEM VISUALIZATION

Figure 7 illustrates the transformation of system information from the C# GUI application's JSON file to OWL and AutomationML formats. These files can then be utilized for knowledge sharing and further decision-making, such as

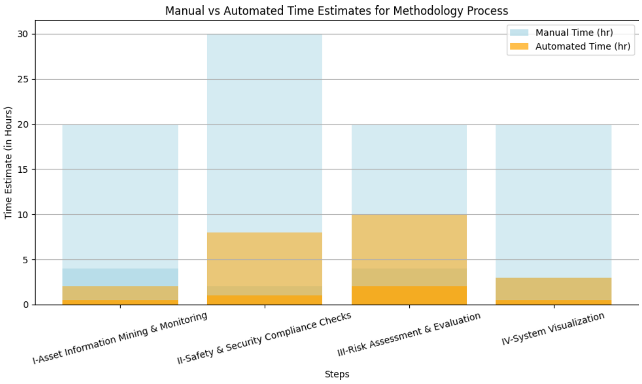

FIGURE 8. Time comparison between manual and automated methodology steps in the pilot factory use case.

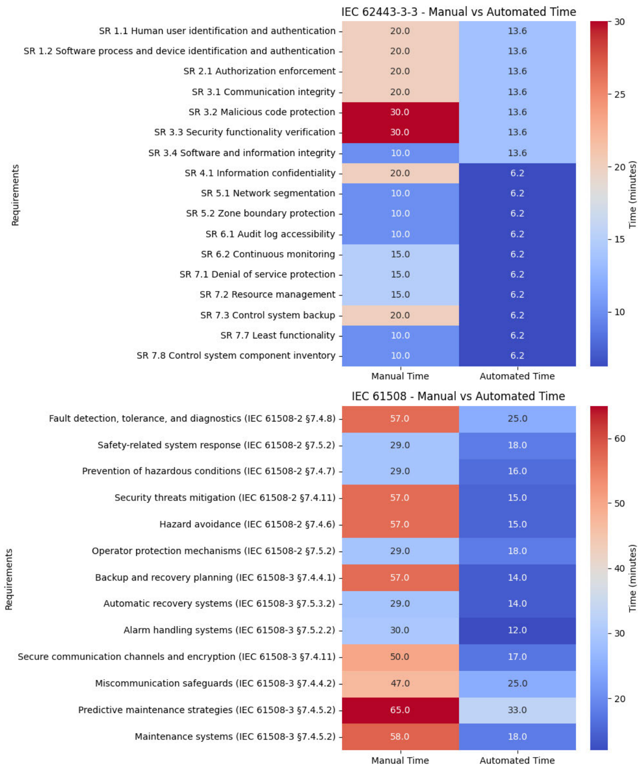

FIGURE 9. Time Comparison for Manual vs. Automated Safety (IEC 61508) and Security (IEC 62443) Compliance Checks in the Pilot Factory Use Case.

applying OWL and AutomationML in the safety and security domain. Examples include Threat Modeling [84], [85], [86], ICS infrastructure design and validation of requirements [6], and risk assessment [12], [81], [87], [88], [89].

V. RESULTS AND ANALYSIS

To evaluate the reliability of the process, we consulted safety and security certification expert to gather their opinions on manual compliance with safety and security standards as well as risk evaluation. Using the same pilot factory as a use case, the estimated time for manual compliance included conducting interviews with responsible stakeholders, reviewing documentation, analyzing incident logs and reports, and completing checklists. In contrast, while automated

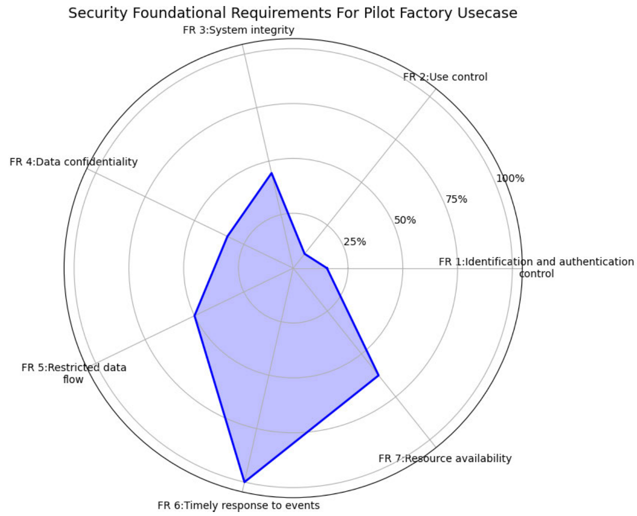

FIGURE 10. IEC 62443-3-3 Fulfilled System Requirements (SR) Across Foundational Requirements (FR) in Security Compliance for the Pilot Factory Use Case.

compliance and evaluation also require a significant initial effort to collect data and resources, these efforts are primarily one-time investments. Once the necessary resources are gathered and prepared, they become readily available for subsequent analysis and assessment, significantly reducing the overall evaluation time in future iterations.

A. OVERALL METHODOLOGY

We categorized two types of timings in the proposed methodology: estimated time and the actual time required to complete each step. The estimated time for each step varies depending on whether the process is manual or automated. For **Asset Information Mining & Monitoring**, the time required ranges from 4 to 20 hours for manual processing and 0.5 to 2 hours for automated processing. Similarly, **Safety and Security Compliance Checks** take 2 to 30 hours manually but only 1 to 8 hours when automated. For **Risk Assessment and Evaluation**, manual processing requires 4 to 20 hours, while automation reduces this to 2 to 10 hours. Finally, **System Visualization** takes 3 to 20 hours manually, compared to just 0.5 to 3 hours with automation. Figure 8 illustrates the average actual time for the entire process, highlighting the efficiency of automation in reducing both complexity and processing time. On average, manual processing takes **32.25 hours**, whereas automated processing requires only **5.25 hours**, representing a substantial **time reduction of 83.72%** when transitioning from manual to automated methods.

B. SAFETY AND SECURITY COMPLIANCE CHECK AND RISK EVALUATION

1) COMPLIANCE

Based on the IEC 62443-3-3 security requirements, we analyzed which system requirements (SRs) are applicable to the demonstrated use case using the Table 6. We then assessed the time required to check compliance both manually and automatically. Similarly, for IEC 61508-2 and 61508-3 safety requirements, we identified the applicable clauses and subclauses for the use case and evaluated the time needed for compliance checks in both manual and automated methods.

The data shown in Figure 9 presents the individual times required for each safety and security compliance requirement. In conclusion, for safety compliance, the manual process required **9.9 hours**, while the automated process took **4 hours**. For security compliance, the manual process took **4.75 hours**, and the automated process required **2.62 hours**.

2) RISK EVALUATION

Based on the Table 6, Before the risk controls, likelihood of security issues reveals that **Tampering** and **Spoofing** have a high chance of occurring, with **Tampering** likely in 8 instances and **Spoofing** in 6, indicating that these should be key areas for mitigation efforts. **Denial of Service (DoS)** and **Information Disclosure** also present high likelihoods, highlighting the need for their inclusion in security planning. For safety, the **Operational** category emerges as a primary concern, marked likely in 15 cases, emphasizing its high priority. **Asset/Infrastructure** is similarly significant, with 12 occurrences marked as likely, underscoring the importance of protecting infrastructure and critical assets. **Regulatory/Legal** and **Personal Safety** concerns also show balanced potential risks. Regarding consequences, the majority of security issues fall under **Major (4)** severity, pointing to the need for urgent attention and mitigation, with some **Catastrophic (5)** incidents requiring immediate response. While **Moderate (3)** security concerns are fewer, they should still not be ignored. In terms of safety, **Minor (2)** issues are most frequent and typically have limited consequences but should still be addressed to prevent escalation. **Moderate (3)** safety concerns are more serious and require prompt intervention to mitigate risks to personnel or operations.

C. IEC 62443-3-3 COMPLIED REQUIREMENTS

In IEC 62443-3-3, SRs define the broad security objectives for the overall system, while FRs specify the detailed technical functionalities required to achieve these objectives. Based on the overall security compliance of each FR, we assessed how many SRs have been fulfilled for each use case. The compliance results are as follows: FR 1 (2 out of 13), FR 2 (1 out of 12), FR 3 (4 out of 9), FR 4 (1 out of 3), FR 5 (2 out of 4), FR 6 (2 out of 2), and FR 7 (5 out of 8), as illustrated in Figure 10. In OT, security is often prioritized based on the AIC (Availability, Integrity, and Confidentiality) triad. This prioritization is reflected in the implementation of security requirements, confirming the importance of the AIC triad in the OT environment, with Availability (FR 7) at **62.5%**, Integrity (FR 3) at **44.4%**, and Confidentiality (FR 4) at **33.3%**.

VI. CONCLUSION

In this work, we proposed and demonstrated a tool-based methodology to ensure compliance in the OT environment and evaluate risks. This process helps to determine whether the proposed SIL and SL levels are sufficient to manage the identified risks and whether proactive SIL/SL levels are necessary to further protect the system. Additionally, the methodology provides clear guidance for decision-making in cases where risks are deemed unacceptable and offers a way to define the overall level of safety and security in the system. Furthermore, we discussed how the application-based approach can be adapted and integrated into existing model-based evaluation frameworks, such as OWL and AutomationML. The study also provides insights into the efficiency gains achieved through methodology, demonstrating a significant reduction in processing time by 83.72%. It highlights the time savings in compliance checks and the identification of critical security and safety risks. The IEC 62443-3-3 Compliance section offers a quantitative assessment of how many SRs are fulfilled by each FR, while also illustrating how the AIC triad (Availability, Integrity, and Confidentiality) guides the prioritization of security measures within the OT environment. While this methodology offers several advantages, it also has some limitations:

- **Platform Dependence:** The application may rely on a Windows-based infrastructure, which could limit its usability. However, we aim to enhance compatibility in future iterations.
- **Complexity Management:** Developing accurate OT infrastructure system models can be challenging, especially for large-scale or highly dynamic systems. Managing this complexity may necessitate simplifications that impact evaluation fidelity.
- **Data Dependency:** System models may depend on data for calibration, validation, or parameter estimation. Limited or biased data can undermine the accuracy and reliability of the model, affecting safety and security evaluation outcomes.
- **Resource Constraints:** Constructing and simulating complex system models often demands substantial computational resources, scalable solutions, specialized third party software, and expertise. Resource limitations can impede the feasibility of model-based evaluations, particularly for small teams or organizations with restricted resources, which might open another security breach point.
- **Human Bias:** Risk evaluation and decision-making processes can be influenced by cognitive biases, subjective judgments, or inconsistencies among evaluators. These biases may affect model interpretation, risk prioritization, and further mitigation strategies, potentially impacting the overall reliability of assessments.

Considering the overall proposed methodology, the "fail fast, fail often" mindset aligns with compliance processes by promoting continuous evaluation and enabling prompt resolution of issues. In case of evaluation of both critical and non-critical infrastructure, the basic methodology remains; however, the system components within the infrastructure may vary. Common asset components (e.g., SCADA, PLCs, and sensors) remain unchanged, while distinct asset components (e.g., transformers and substations in electrical grids, pumps, valves, and filtration systems in water treatment plants) may require modifications. In this context, there is a need for refinement at the OT system meta-model and GUI application level to define new components, along with ensuring standard compliance process specific to that system infrastructure is followed. This approach helps streamline safety and security compliance processes, as failures during evaluations provide actionable insights into areas requiring improvement. In future work, it would be interesting to explore how the presented methodology performs in complex environments with a high number of assets, distributed systems, and real-time infrastructure. Based on the results, refining the methodology to accommodate not only the needs of Small and Medium-sized Enterprises (SMEs) but also large industries would be valuable.

REFERENCES

[1] S. Hollerer, W. Kastner, and T. Sauter, ''Safety and security: A field of tension in industrial practice,'' in *Proc. IEEE 21st Int. Conf. Ind. Informat. (INDIN)*, Jul. 2023, pp. 1–7.

[2] M. Bhole, T. Sauter, and W. Kastner, ''Enhancing industrial cybersecurity: Insights from analyzing threat groups and strategies in operational technology environments,'' *IEEE Open J. Ind. Electron. Soc.*, vol. 6, no. 8, pp. 145–157, Aug. 2025, doi: 10.1109/OJIES.2025.3527585.

[3] T. Sauter and A. Treytl, ''IoT-enabled sensors in automation systems and their security challenges,'' *IEEE Sensors Lett.*, vol. 7, no. 12, pp. 1–4, Dec. 2023.

[4] M. Bhole, W. Kastner, and T. Sauter, ''IT security solutions for IT/OT integration: Identifying gaps and opportunities,'' in *Proc. IEEE 29th Int. Conf. Emerg. Technol. Factory Autom. (ETFA)*, Sep. 2024, pp. 1–8.

[5] N. Koporcic, D. Sjödin, M. Kohtamäki, and V. Parida, ''Embracing the 'fail fast and learn fast' mindset: Conceptualizing learning from failure in knowledge-intensive SMEs,'' *Small Bus. Econ.*, vol. 64, no. 1, pp. 181–202, Feb. 2024, doi: 10.1007/s11187-024-00897-0.

[6] A. M. Hosseini, T. Sauter, and W. Kastner, ''Integrating security into industrial control system architecture based on IEC 42010,'' in *Proc. IEEE 29th Int. Conf. Emerg. Technol. Factory Autom. (ETFA)*, vol. 21, Sep. 2024, pp. 1–8.

[7] A. M. Hosseini, T. Sauter, and W. Kastner, ''Formal verification of safety and security properties in industry 4.0 applications,'' in *Proc. IEEE 28th Int. Conf. Emerg. Technol. Factory Autom. (ETFA)*, Sep. 2023, pp. 1–8.

[8] Council Eur. Union. (2023). *Council Regulation (EU), no. 2023/1230*. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02023R1230-20230629

[9] J. Mi, W. Huang, M. Chen, and W. Zhang, ''A method of entropy weight quantitative risk assessment for the safety and security integration of a typical industrial control system,'' *IEEE Access*, vol. 9, pp. 90919–90932, 2021.

[10] A. Hristova, R. Schlegel, and S. Obermeier, ''Security assessment methodology for industrial control system products,'' in *Proc. 4th Annu. IEEE Int. Conf. Cyber Technol. Autom., Control Intell.*, Jun. 2014, pp. 264–269.

[11] X. Wang, Z. Tang, and S. Xu, ''Information security risk assessment based on fuzzy theory and brbpnn,'' *Comput. Simul.*, vol. 36, no. 11, pp. 184–189, 2019.

[12] P. Bhosale, W. Kastner, and T. Sauter, ''Modeling human error factors with security incidents in industrial control systems: A Bayesian belief network approach,'' in *Proc. 19th Int. Conf. Availability, Rel. Secur.*, Jul. 2024, pp. 1–9.

[13] W. Shang, T. Gong, C. Chen, J. Hou, and P. Zeng, ''Information security risk assessment method for ship control system based on fuzzy sets and attack trees,'' *Secur. Commun. Netw.*, vol. 2019, pp. 1–11, Mar. 2019.

[14] K. Meng Tay and C. Peng Lim, ''Fuzzy FMEA with a guided rules reduction system for prioritization of failures,'' *Int. J. Quality Rel. Manage.*, vol. 23, no. 8, pp. 1047–1066, Oct. 2006.

[15] A. Hassan, M. R. A. Purnomo, and A. R. Anugerah, ''Fuzzy-analytical-hierarchy process in failure mode and effect analysis (FMEA) to identify process failure in the warehouse of a cement industry,'' *J. Eng., Design Technol.*, vol. 18, no. 2, pp. 378–388, Sep. 2019.

[16] P. L. Campbell and J. E. Stamp, ''A classification scheme for risk assessment methods,'' Sandia Nat. Laboratories (SNL), Albuquerque, NM, USA, Tech. Rep. SAND2004-4233; TRN: US200807360, Aug. 2004. [Online]. Available: https://doi.org/10.2172/925643

[17] E. Snekkenes, ''An information security risk management research menu,'' *Norsk informasjonssikkerhetskonferanse (NISK)*, vol. 2012, no. 4, p. 5, 2012.

[18] B. Blakley, E. McDermott, and D. Geer, ''Information security is information risk management,'' in *Proc. Workshop New Security Paradigms*, Sep. 2001, pp. 97–104.

[19] D. W. Hubbard, *The Failure of Risk Management: Why It's Broken and How To Fix It*. Hoboken, NJ, USA: Wiley, 2020.

[20] Y. Zhiwei and J. Zhongyuan, ''A survey on the evolution of risk evaluation for information systems security,'' *Energy Proc.*, vol. 17, pp. 1288–1294, Jan. 2012.

[21] *Cyber Security Evaluation Tool: Performing a Self-assessment*, U.S. Dept. Homeland Secur., Washington, DC, USA, 2012.

[22] J. Watters, S. Morrissey, D. Bodeau, and S. C. Powers, ''The risk-to-mission assessment process (riskmap): a sensitivity analysis and an extension to treat confidentiality issues,'' Inst. Inf. Infrastruct. Protection (I3P), Tech. Rep. AD1107410, Jul. 2009.

[23] T. S. Lowry, V. C. Tidwell, W. J. Peplinski, R. Mitchell, D. Binning, and J. Meszaros, ''Framework for shared drinking water risk assessment,'' Sandia National Lab. (SNL-NM), Albuquerque, NM, USA, Tech. Rep. SAND2017-0241; 650294, Jan. 2017, [Online]. Available: https://doi.org/10.2172/1339494

[24] Community Research and Development Information Service (CORDIS). (2012). *Emergency Management in Large Infrastructures (emili)*. Eur. Commission, Luxembourg. Accessed: Dec. 31, 2024. [Online]. Available: https://cordis.europa.eu/project/rcn/93509_en.html

[25] Community Research and Development Information Service (CORDIS). (2008). *Critical Utility Infrastructural Resilience (crutial)*. Eur. Commission. Accessed: Dec. 31, 2024. [Online]. Available: https://cordis.europa.eu/projects/rcn/79318_en.html

[26] Community Research and Development Information Service (CORDIS). (2011). *Vital Infrastructure, Networks, Information and Control Systems Management (viking)*. Eur. Commission. Accessed: Dec. 31, 2024. [Online]. Available: https://cordis.europa.eu/project/rcn/88625_en.html

[27] Community Research and Development Information Service (CORDIS). Eur. Commission. (2014). *Cybersecurity on Scada: Risk Prediction, Analysis and Reaction Tools for Critical Infrastructures (cockpitci)*. Accessed: Dec. 31, 2024. [Online]. Available: https://cordis.europa.eu/projects/285647

[28] Community Research and Development Information Service (CORDIS). Eur. Commission. (2014). *Critical Infrastructure Security Analysis (crisalis)*. Accessed: Accessed: Dec. 31, 2024. [Online]. Available: https://cordis.europa.eu/projects/rcn/103538_en.html

[29] Community Research and Development Information Service (CORDIS). Eur. Commission, Luxembourg. (2014). *Prevention, Protection and Reaction To Cyber Attacks on Critical Infrastructures (precyse)*. Accessed: Dec. 31, 2024. [Online]. Available: https://cordis.europa.eu/project/rcn/102446_en.html

[30] M. Ehrlich, A. Bröring, C. Diedrich, J. Jasperneite, W. Kastner, and H. Trsek, ''Determining the target security level for automated security risk assessments,'' in *Proc. IEEE 21st Int. Conf. Ind. Informat. (INDIN)*, Jul. 2023, pp. 1–6.

[31] R. Baskerville, ''Information systems security design methods: Implications for information systems development,'' *ACM Comput. Surveys*, vol. 25, no. 4, pp. 375–414, Dec. 1993.

[32] Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby, and K. Stoddart, ''A review of cyber security risk assessment methods for SCADA systems,'' *Comput. Secur.*, vol. 56, pp. 1–27, Feb. 2016.

[33] M. Eckhart, A. Ekelhart, S. Biffl, A. Lüder, and E. Weippl, "QualSec: An automated quality-driven approach for security risk identification in cyber-physical production systems," *IEEE Trans. Ind. Informat.*, vol. 19, no. 4, pp. 5870–5881, Apr. 2023.

[34] M. Ehrlich, A. Bröring, C. Diedrich, and J. Jasperneite, "Towards automated risk assessments for modular manufacturing systems: Process analysis and information model proposal," *at-Automatisierungstechnik*, vol. 71, no. 6, pp. 453–466, Jun. 2023.

[35] L. Piètre-Cambacédès and M. Bouissou, "Beyond attack trees: Dynamic security modeling with Boolean logic driven Markov processes (BDMP)," in *Proc. Eur. Dependable Comput. Conf.*, Apr. 2010, pp. 199–208.

[36] N. T. Le and D. B. Hoang, "Security threat probability computation using Markov chain and common vulnerability scoring system," in *Proc. 28th Int. Telecommun. Netw. Appl. Conf. (ITNAC)*, Nov. 2018, pp. 1–6.

[37] C. Y. T. Ma, N. S. V. Rao, and D. K. Y. Yau, "A game theoretic study of attack and defense in cyber-physical systems," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Apr. 2011, pp. 708–713.

[38] R. Vigo, A. Bruni, and E. Yüksel, "Security games for cyber-physical systems," in *Secure IT Systems* (Lecture notes in computer science). Berlin, Germany: Springer, 2013, pp. 17–32.

[39] J. Großmann and F. Seehusen, "Combining security risk assessment and security testing based on standards," in *Proc. 3rd Int. Workshop Risk Assessment Risk-Driven Testing*, Berlin, Germany. Cham, Switzerland: Springer, Jun. 15, 2015, pp. 18–33.

[40] M. Felderer, P. Zech, R. Breu, M. Büchler, and A. Pretschner, "Model-based security testing: A taxonomy and systematic classification," *Softw. Test., Verification Rel.*, vol. 26, no. 2, pp. 119–148, Mar. 2016.

[41] M. Eckhart, B. Brenner, A. Ekelhart, and E. Weippl, "Quantitative security risk assessment for industrial control systems: Research opportunities and challenges," *J. Internet Serv. Inf. Secur.*, vol. 9, pp. 52–73, 2019.

[42] W. Xiong, E. Legrand, O. Åberg, and R. Lagerström, "Cyber security threat modeling based on the MITRE enterprise ATT&CK matrix," *Softw. Syst. Model.*, vol. 21, no. 1, pp. 157–177, Feb. 2022.

[43] M. Burmester, E. Magkos, and V. Chrissikopoulos, "Modeling security in cyber–physical systems," *Int. J. Crit. Infrastruct. Protect.*, vol. 5, nos. 3–4, pp. 118–126, 2012.

[44] B. Kordy, P. Kordy, S. Mauw, and P. Schweitzer, "ADTool: Security analysis with attack-defense trees (Extended Version)," 2013, *arXiv:1305.6829*.

[45] G. Petrica, S.-D. Axinte, I. C. Bacivarov, M. Firoiu, and I.-C. Mihai, "Studying cyber security threats to Web platforms using attack tree diagrams," in *Proc. 9th Int. Conf. Electron., Comput. Artif. Intell. (ECAI)*, Jun. 2017, pp. 1–6.

[46] P. H. Meland, D. G. Spampinato, E. Hagen, E. T. Baadshaug, K.-M. Krister, and K. S. Velle, "Seamonster: Providing tool support for security modeling," in *Proc. Norwegian Symp. Inf. Secur.*, Nov. 2008, pp. 59–68.

[47] N. R. Mead and T. Stehney, "Security quality requirements engineering (SQUARE) methodology," *ACM SIGSOFT Softw. Eng. Notes*, vol. 30, no. 4, pp. 1–7, Jul. 2005.

[48] E. Lazarus, D. L. Dill, J. Epstein, and J. L. Hall, "Applying a reusable election threat model at the county level," in *Proc. Electron. Voting Technol. Workshop/Workshop Trustworthy Elections*, Aug. 2011, pp. 1–19.

[49] A. Rashid, A. Moreira, and J. Araájo, "Modularisation and composition of aspectual requirements," in *Proc. 2nd Int. Conf. Aspect-oriented Softw. Develop.*, Mar. 2003, pp. 11–20.

[50] M. Glawe, C. Tebbe, A. Fay, and K.-H. Niemann, "Knowledge-based engineering of automation systems using ontologies and engineering data," in *Proc. 7th Int. Joint Conf. Knowl. Discovery, Knowl. Eng. Knowl. Manage.*, 2015, pp. 1–56.

[51] M. Eckhart, A. Ekelhart, and E. Weippl, "Automated security risk identification using AutomationML-based engineering data," *IEEE Trans. Dependable Secure Comput.*, vol. 19, no. 3, pp. 1655–1672, May 2022.

[52] C. Tebbe, M. Glawe, A. Scholz, K.-H. Niemann, A. Fay, and J. Dittgen, "Wissensbasierte sicherheitsanalyse in der automation," *Atp Magazin*, vol. 57, no. 4, pp. 56–66, Apr. 2015.

[53] A. Derock, P. Hébrard, and F. Vallée, "Convergence of the latest standards addressing safety and security for information technology," in *Proc. Embedded Real Time Softw. Syst.*, 2010, pp. 1–11.

[54] T. J. Cockram and S. R. Lautieri, "Combining security and safety principles in practice," in *Proc. 2nd IET Int. Conf. Syst. Saf.*, vol. 2007, 2007, pp. 159–164.

[55] S. Lautieri, D. Cooper, and D. Jackson, "SafSec: Commonalities between safety and security assurance," in *Constituents of Modern System-safety Thinking*, F. Redmill and T. Anderson, Eds., London, U.K.: Springer, 2005, pp. 65–75.

[56] K. Heckemann, M. Gesell, T. Pfister, K. Berns, K. Schneider, and M. Trapp, "Safe automotive software," in *Knowledge-Based and Intelligent Information and Engineering Systems*, A. König, A. Dengel, K. Hinkelmann, K. Kise, R. J. Howlett, and L. C. Jain, Eds., Berlin, Germany: Springer, 2011, pp. 167–176.

[57] M. Bozzano, H. Bruintjes, A. Cimatti, J.-P. Katoen, T. Noll, and S. Tonetta, "Compass 3.0," in *Tools and Algorithms for the Construction and Analysis of Systems*, T. Vojnar and L. Zhang, Eds., Cham, Switzerland: Springer, 2019, pp. 379–385.

[58] S. Mazzini, J. Favaro, A. Martelli, and L. Baracchi, "Security and safety modelling in embedded systems," in *Proc. Embedded Real Time Softw. Syst.*, Toulouse, France, Feb. 2014, pp. 1–57.

[59] B. Hunter, "Integrating safety and security into the system lifecycle," in *Proc. Improving Syst. Softw. Eng. Conf. (ISSEC)*, 2009, p. 147.

[60] D. P. Eames and J. Moffett, "The integration of safety and security requirements," in *Proc. Comput. Saf., Rel. Secur.*, in Lecture Notes in Computer Science, Berlin, Germany, M. Felici and K. Kanoun, Eds., Cham, Switzerland: Springer, 1999, pp. 468–480.

[61] L. Piètre-Cambacédès and M. Bouissou, "Cross-fertilization between safety and security engineering," *Rel. Eng. Syst. Saf.*, vol. 110, pp. 110–126, Feb. 2013.

[62] S. Hernan, S. Lambert, T. Ostwald, and A. Shostack, "Threat modeling-uncover security design flaws using the stride approach," in *Proc. MSDN Mag.*, 2006, pp. 68–75.

[63] L. Zhang, A. Taal, R. Cushing, C. de Laat, and P. Grosso, "A risk-level assessment system based on the STRIDE/DREAD model for digital data marketplaces," *Int. J. Inf. Secur.*, vol. 21, no. 3, pp. 509–525, Sep. 2021.

[64] A. Wolf, D. Simopoulos, L. D'Avino, and P. Schwaiger, "The PASTA threat model implementation in the IoT development life cycle," in *Proc. INFORMATIK*, 2021, pp. 1195–1204.

[65] N. Mead, F. Shull, K. Vemuru, and O. Villadsen, "A hybrid threat modeling method," Carnegie Mellon Univ., Softw. Eng. Inst., Tech. Rep. CMU/SEI-2018-TN-002, Mar. 2018.

[66] C. Alberts, S. Behrens, R. Pethia, and W. Wilson, "Operationally critical threat, asset, and vulnerability evaluation (octave) framework," Carnegie Mellon Univ., Softw. Eng. Institute's Digit. Library, Pittsburgh, PA, USA, Tech. Rep. CMU/SEI-99-TR-017, Sep. 1999.

[67] D. Chernov, "Application TRIKE methodology when modeling threats to APCs information security," in *Proc. Adv. Autom. III*, A. A. Radionov and V. R. Gasiyarov, Eds., Cham, Switzerland: Springer, Jan. 2022, pp. 452–461.

[68] C. Rivera Domínguez, J. I. Pozos Mares, and R. G. Zambrano Hernández, "Hazard identification and analysis in work areas within the manufacturing sector through the HAZID methodology," *Process Saf. Environ. Protection*, vol. 145, pp. 23–38, Jan. 2021.

[69] Z. Yessekeyeva and V. Vandenbussche, "Performance standards for environmentally critical elements," in *Proc. SPE Int. Conf. Exhib. Health, Safety, Environ., Sustainability*, Mar. 18, 2014, pp. 1–34.

[70] C. Palmer and P. W. H. Chung, "An automated system for batch hazard and operability studies," *Rel. Eng. Syst. Saf.*, vol. 94, no. 6, pp. 1095–1106, Jun. 2009.

[71] A. de Ruijter and F. Guldenmund, "The bowtie method: A review," *Saf. Sci.*, vol. 88, pp. 211–218, Oct. 2016.

[72] *IEC 61511–1 : Functional Safety-Safety Instrumented Systems for the Process Industry Sector-Part 1: Framework, Definitions, System, Hardware and Application Programming Requirements*, Standard IEC 61511–1, 2016.

[73] *IEC 61508–1 : Functional Safety of Electrical/ Electronic/programmable Electronic Safety-related Systems*, Standard IEC 61508–1, 2010.

[74] A. I. Chemical Engineers. Center Chemical Process Safety, *Layer Protection Analysis: Simplified Process Risk Assessment* (CCPS concept book). New York, NY, USA: Center for Chemical Process Safety of the American Institute of Chemical Engineers, 2001.

[75] G. E. Apostolakis, "How useful is quantitative risk assessment?" *Risk Anal.*, vol. 24, no. 3, pp. 515–520, Jun. 2004.

[76] L. Boggero, M. Fioriti, G. Donelli, and P. D. Ciampa, *Model-Based Mission Assurance/Model-Based Reliability, Availability, Maintainability, and Safety (RAMS)*. Cham, Switzerland: Springer, 2020, pp. 1–39.

[77] M. Bhole, W. Kastner, and T. Sauter, "From manual to semi-automated safety and security requirements engineering: Ensuring compliance in industry 4.0," in *Proc. 50th Annu. Conf. IEEE Ind. Electron. Soc.*, Chicago, IL, USA, Nov. 2024, pp. 1–8.

[78] M. Bhole, W. Kastner, and T. Sauter, "A model based framework for testing safety and security in operational technology environments," in *Proc. IEEE 27th Int. Conf. Emerg. Technol. Factory Autom. (ETFA)*, Sep. 2022, pp. 1–4.
[79] M. Bhole, W. Kastner, and T. Sauter, "Knowledge representation of asset information and performance in OT environments," in *Proc. IEEE 28th Int. Conf. Emerg. Technol. Factory Autom. (ETFA)*, Sep. 2023, pp. 1–8.
[80] J. Braband, "Towards an it security risk assessment framework for railway automation," 2017, *arXiv:1704.01212*.
[81] P. Bhosale, W. Kastner, and T. Sauter, "AutomationML meets Bayesian networks: A comprehensive safety-security risk assessment in industrial control systems," *IEEE Open J. Ind. Electron. Soc.*, vol. 5, pp. 823–835, 2024.
[82] H. Cheong, "Translating JSON schema logics into OWL axioms for unified data validation on a digital manufacturing platform," *Proc. Manufacturing*, vol. 28, pp. 183–188, Jan. 2019.
[83] R. Drath, *AutomationML: A Practical Guide*. Walter de Gruyter GmbH & Co KG, 2021, doi: 10.1515/9783110746235.
[84] S. Hollerer, W. Kastner, and T. Sauter, "Towards a comprehensive ontology considering safety, security, and operation requirements in OT," in *Proc. IEEE 28th Int. Conf. Emerg. Technol. Factory Autom. (ETFA)*, Sep. 2023, pp. 1–4.
[85] S. Hollerer, T. Sauter, and W. Kastner, "A survey of ontologies considering general safety, security, and operation aspects in OT," *IEEE Open J. Ind. Electron. Soc.*, vol. 5, pp. 861–885, 2024.
[86] S. Hollerer, W. Kastner, and T. Sauter, "Towards a threat modeling approach addressing security and safety in OT environments," in *Proc. 17th IEEE Int. Conf. Factory Commun. Syst. (WFCS)*, Jun. 2021, pp. 37–40.
[87] P. Bhosale, W. Kastner, and T. Sauter, "Integrated safety-security risk assessment for industrial control system: An ontology-based approach," in *Proc. IEEE 28th Int. Conf. Emerg. Technol. Factory Autom. (ETFA)*, Sep. 2023, pp. 1–8.
[88] P. Bhosale, W. Kastner, and T. Sauter, "AutomationML use for safety and security risk assessment in industrial control systems," in *Proc. IEEE 28th Int. Conf. Emerg. Technol. Factory Autom. (ETFA)*, Sep. 2023, pp. 1–4.
[89] P. Bhosale, W. Kastner, and T. Sauter, "Comparative analysis of AAS and AML as a data source for integrated risk assessment in ICS," in *Proc. IEEE 29th Int. Conf. Emerg. Technol. Factory Autom. (ETFA)*, Sep. 2024, pp. 1–4.

MUKUND BHOLE received the B.Tech. degree in information technology from Shivaji University, Kolhapur, India, in 2019, and the M.Tech. degree in information security from COEP Technological University, Pune, India, in 2021. Currently, he is pursuing the Ph.D. degree with Technische Universität Wien (TU Wien), Vienna, Austria, with a research focus on safety and security in operational technology environments. In addition, he is a Project Assistant with #SafeSecLab. His research interests include information security, penetration testing, intrusion detection, vulnerability assessment, and overall industrial cybersecurity.

THILO SAUTER (Fellow, IEEE) received the Dipl.-Ing. and Ph.D. degrees in electrical engineering from the Technische Universität Wien (TU Wien), Vienna, Austria, in 1992 and 1999, respectively. From 2004 to 2013, he was the Founding Director of the Institute for Integrated Sensor Systems, Austrian Academy of Sciences. He is currently a Professor of automation technology with TU Wien and a Senior Scientist with the University for Continuing Education Krems, Wiener Neustadt, Austria. His expertise and research interests include embedded systems and integrated circuit design, smart sensors, and automation and sensor networks with a focus on real-time, security, interconnection, and integration issues relevant to cyber-physical systems and the Internet of Things in various application domains, such as industrial and building automation, smart manufacturing, or smart grids. He is member of the Board of Austrian Electrotechnical Association and a Senior AdCom Member of the IEEE Industrial Electronics Society (IES). Moreover, he has been involved in the standardization of industrial communication systems, for more than 25 years.

SABRINA SEMPER received the bachelor's degree in information and communication systems and the master's degree in IT security from the University of Applied Sciences Technikum Wien. She is currently a Senior Consultant with TÜV Austria TRUST IT, where she helps clients protect and secure their (critical) infrastructure. She is an accomplished IT professional who has over 20 years of experience in the IT industry. She began her career as an Operations Engineer at a leading provider of government solutions. Eight years ago, she transitioned into IT security, where she became a White Hat Hacker. More recently, her focus has shifted to operational technology (OT) security, where she has developed expert knowledge in IEC 62443 standards.

WOLFGANG KASTNER (Senior Member, IEEE) received the Dipl.-Ing. and Dr.Techn. degrees in computer science from the Technische Universität Wien (TU Wien), Vienna, Austria, in 1992 and 1996, respectively. He is currently a Full Professor of the Industrial Internet of Things with the Faculty of Informatics, TU Wien. His research addresses distributed automation and (industrial) communication systems in various application domains, such as factory automation, building automation, and smart grids. His research topics tackle the safe while secure IT/OT convergence and approaches for the industrial internet based on information modeling and knowledge representation.