From Manual to Semi-Automated Safety and Security Requirements Engineering: Ensuring Compliance in Industry 4.0

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

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

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

***Abstract*—In response to the growing need for compliance with diverse safety and security regulations, crucial for safeguarding both humans and machines in the era of Industry 4.0 (I4.0), it has also become increasingly crucial for industries to ensure adherence to safety and security standards. However, navigating the complexities of regulations and standards can be daunting, often leading to inefficiencies in compliance processes. Our goal is to foster a comprehensive understanding of an effective approach to meeting compliance requirements in these related fields. Therefore, this paper introduces a semi-automated method for ensuring compliance with unified safety and security standards within the context of I4.0. This approach empowers management teams to thoroughly analyze the specific requirements necessary to maintain a protected environment. Compliance can be achieved at both the asset component and system levels, aligning with the relevant standards. Additionally, we present a detailed analysis of a use case and its output, demonstrating the practical application and efficacy of our approach.**

***Index Terms*—Safety and Security, Standard requirements compliance, Industry 4.0, Automation**

I. INTRODUCTION

Ensuring the safety and security of a complex system's design is crucial, as there is little margin for error in identifying threats—from low-level vulnerabilities that can escalate into high-level risks. Neglecting these risks can have profound consequences, impacting the safety, security, and economic stability of industries

A survey conducted by the Ponemon Institute on cybersecurity incidents within Industrial Control Systems (ICSs) reveals that, on average, it takes 361 days to detect, investigate, and mitigate threats in this domain. The cost of mitigation averages around $936,168 for companies, with additional expenses such as equipment replacement, downtime, and legal-regulatory fines, which can amount to an average of $2,989,550 [1]. To safeguard the industrial environment, it is essential to develop, plan, and implement requirements and recommendations, with industrial standards playing a pivotal role. However, the challenges in maintaining standardized procedures within the industry are notable [2]–[4]:

- Outdated standard documents
- Difficulty in locating standard documents
- Complexity in understanding standards
- Vagueness in standards

In the realm of safety and security, key standardization committees such as CEN-CENELEC[1], ISO[2], IEC[3], DIN[4], IEEE[5], BSI[6], and ETSI[7] cover various domains. These committees bear a social responsibility to ensure the efficacy of the standardization procedure. However, navigating through these committees can be challenging due to the unique architectural complexities present in each industry.

The need for semi-automated compliance in Industry 4.0 is driven by factors such as increased regulatory complexity, massive data volumes, faster pace of change, cyber risks, and the desire for greater operational efficiency and cost savings. Semi-automated tools can compress months of compliance work into weeks, reduce human error, and provide better visibility and control. While achieving 100% compliance may pose challenges, it is crucial to establish a solid foundation to effectively meet the needs of consumers and industries. Ensuring compliance with safety and security regulations not only protects employees from workplace hazards but also prevents accidents, injuries, and fatalities. Beyond fulfilling legal requirements, organizations have an ethical imperative to prioritize the safety of their employees, customers, and the surrounding community, as well as safeguarding the security of their system infrastructure. In this paper, we propose a five-stage methodology to automate compliance with unified safety and security standards in Industry 4.0. Our goal is to address the aforementioned challenges and highlight the benefits of this approach. We aim to answer the following research questions using this methodology:

Q1 How can asset information be mined and maintained?
Q2 How does the proposed approach integrate diverse safety and security regulations in Industry 4.0 into a unified framework?
Q3 What are the advantages and limitations of using semi-automated approaches compared to traditional manual methods?

[1]https://www.cencenelec.eu/
[2]https://www.iso.org/home.html
[3]https://iec.ch/homepage
[4]https://www.din.de/en
[5]https://standards.ieee.org/
[6]https://tinyurl.com/bdhfxhzs
[7]https://www.etsi.org/

Q4 How does the proposed approach facilitate compliance assurance at both the asset component and system levels?

The paper is structured as follows: Section II discusses related works on compliance with safety and security in industrial applications. Section III introduces a five-stage methodology for semi-automated compliance assessment of safety and security requirements. Section IV presents a use case demonstration of the proposed methodology. Finally, Section V concludes the paper by addressing the research questions, highlighting the advantages and limitations of the proposed methodology, and providing an outlook on future work.

II. Related Work

In the context of Industry 4.0, where smart manufacturing and interconnected systems present new safety and security requirements, various standards and best practices have been proposed. These advancements highlight the importance of achieving compliance and maintaining robust safety and security measures. Here, we evaluate the existing literature on standard compliance verification. Misra et al. [5] offered practical recommendations for Industrial IoT (IIoT) safety, discussing various hazard types, potential sources of hazards, and the potential for automating the detection of safety incidents. However, their work does not present an integrated approach that combines both safety and security perspectives. Sicari et al. [6] surveyed three security requirements—authentication, confidentiality, and access control—on Internet of Things (IoT) systems, addressing IoT security and open issues. However, their work does not encompass the full spectrum of technologies and standards in IIoT environments, nor does it guarantee adaptation to evolving security threats. Sauter et al. [7] examined the current security posture in industrial environments, emphasizing the rapid evolution of the IIoT landscape. As IIoT is increasingly integrated into safety-critical systems, ensuring security has become more crucial than ever. Julisch et al. [8] explored bridging the gap between academic research and practical industry needs, but its effectiveness remains uncertain. Schneider et al. [9] analyzed safety properties and their enforcement using formal logic to derive consequences from formalization. However, applying a formalized approach to real-world applications presents significant challenges. Ziegler et al. [10] proposed a robust, autonomic security framework with integrated trust and security, optimizing all phases and including asset components that meet security and privacy standards with real-time monitoring. However, it lacks technical applicability and representative metrics for industrial applications. Choi et al. [11] proposed a system hardening and security monitoring scheme for IoT systems, addressing vulnerabilities with appropriate technology, including a practical prototype for malware detection. However, it follows a RedHat checklist instead of relevant IoT standards. Matheu et al. [12] presented an architectural framework for security assessment and testing methodologies, aiming to certify IoT security through risk assessment, testing, and labeling. However, it lacks actions to monitor environments for standard-based security compliance. The IoT Security Foundation [13] introduced an IoT security compliance framework with a checklist and questionnaire for stakeholders to assess and categorize security processes, including the supply chain. However, it lacks guidance on implementing security properties and real-time compliance monitoring. Bicaku et al. [14] presented an automated, continuous compliance verification framework for devices, systems, and services during secure onboarding and runtime. This approach involves selecting relevant standards with implementable metrics and applying them across device, system, and service layers. However, existing standards provide requirements and metrics, but the approach lacks implementation guidelines. Peldszus et al. [15] proposed an approach that checks the compliance of design-level models with implementation-level models, revealing relations between asset components. However, it relies on manually defined or accepted mappings to determine compliance. Bicaku et al. [16] introduced Measurable Indicator Points (MIPs) classified into Measurable Security Indicators (MSIs), Measurable Safety Indicators (MSFIs), and Measurable Organizational Indicators (MOIs), which serve as inputs for the compliance verification framework, showing compliance based on evaluated standards. However, the effectiveness depends on the accuracy and relevance of the selected standards and extracted MIPs. Anwar et al. [17] presented a toolchain utilizing formal methods to create a detailed network dependency graph, incorporating physical (e.g., links) and logical connections (e.g., service dependencies) extracted from SCADA specification languages like Common Information Model (CIM). However, the effectiveness of the security assessment hinges on the accuracy and completeness of the initial specifications and defined best practices.

III. Methodology

We leverage our previous works [18], [19] to integrate and manage data at each stage of the proposed methodology. This data management approach supports various types of Database Management System (DBMS). Here, we utilize the system database described in [18] in Relational DBMS form, as shown in Fig. 1, which illustrates the constituent parts of the database, including its tables, relations, and descriptions of each entity that can be used in the compliance process. The tables are designed for reusability in various settings, incorporating the some entities to minimize data redundancy.

Stage I: Asset Information

In the first stage, we adopt an asset-centric approach commonly found in asset-intensive industries such as manufacturing or critical infrastructure. This approach prioritizes gathering asset information before assessing specific regulatory requirements. Therefore, we initially focus on collecting asset information, followed by evaluating requirements, especially for already commissioned brownfield systems undergoing compliance checks.

During this stage, we utilize our work from [19] to gather asset information semi-automatically using Asset Information

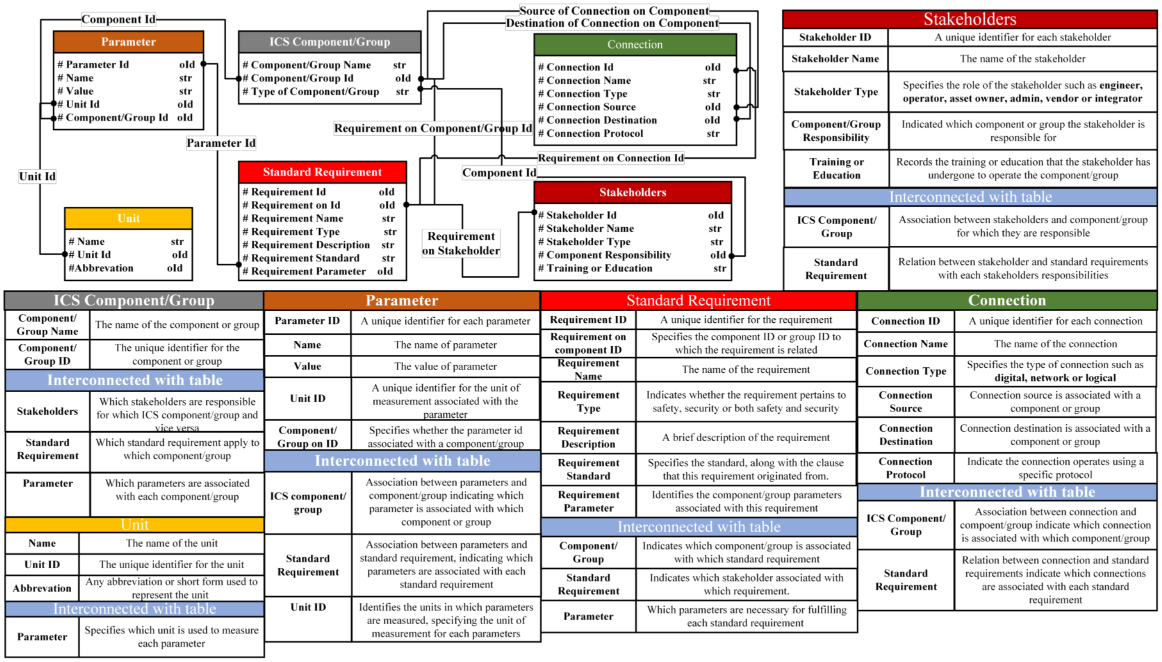


Fig. 1. Constituent parts of the database, including its tables, relationships, and descriptions of each entity, which can be used in the compliance methodology based on [18].

Mining Sources (AIMSs), along with expert knowledge and contributions from the management team. This process involves identifying and cataloging all relevant assets, including equipment, asset components, connections, and stakeholders. Asset information may encompass details such as asset type, location, specification parameters, operational status, maintenance history, and associated risks. The gathered information populates the constituent tables (**'ICS component/group, Parameters, Unit, Connection, Stakeholder'**) shown in Fig. 1.

Stage II: Requirement Identification

In this stage, a thorough review of relevant regulations, standards, and guidelines is conducted to determine specific requirements that components or systems must adhere to. Industry experts identify applicable regulatory requirements, industry standards, internal policies, and contractual obligations. Safety and security requirements encompass safety regulations, quality criteria, and security protocols in this methodology.

Several safety and security standards and technical reports are recommended by industry partners working in safety and security certifications, as they cover the most crucial aspects of industrial infrastructure. These include, but are not limited to, IEC 61508 [20], CEN ISO/TR 22100-4 [21], OVE IEC TR 63069 [22], IEC TR 63074 [23], BSI [24], NIST SP 800-82 Revision 2 [25], and IEC 62443 [26]–[29].

Here, we adopt a modular integration approach for incorporating safety and security standard requirements based on specific needs, allowing various standards to be consolidated into a unified requirements table. This table undergoes independent verification for each asset component or system. The identified requirements are then integrated into the constituent table (**'Standard Requirement'**), depicted in Fig. 1.

Stage III: Requirement Allocation

After identifying the standard requirements, a compliance experts committee—typically consisting of asset owners, vendors, system integrators, and other stakeholders—proceeds to allocate or assign them to the corresponding asset components or systems. This stage involves matching each requirement to the specific asset component or system (or group of components) and assigning parameters that support the concrete fulfillment of the requirement criteria.

Requirement allocation ensures that each asset component or system is linked with the appropriate compliance obligations and parameters, facilitating targeted assessment and monitoring efforts. During this process, the (*'component id/group id' and 'parameter id'*) are assigned to the respective requirement for effective tracking and management within the constituent table (**'Standard Requirement'**), as depicted in Fig. 1.

Stage IV: Gap Analysis

Gap analysis involves assessing the current state of compliance against the established requirements and parameters that support the fulfillment of those requirements. This stage aims to identify discrepancies or gaps between the existing condition of the system and the desired compliance level. Typically, a dedicated internal audit officer, Chief Information Security Officer (CISO), or safety-security consultant oversees this stage. Gap analysis helps pinpoint areas where corrective actions or improvements are needed to enhance compliance.

During this process, corrective changes are made not only to current systems but also to the data populated in constituent tables to ensure alignment with compliance requirements, both digitally and in real-world system operations.

Stage V: Compliance Assessment

The final stage involves assessing the compliance of asset components or systems with the identified requirements. Compliance assessment employs various methods, including inspections, audits, tests, and reviews, to ensure adherence to regulatory standards and internal policies. Here, we conduct a preliminary assessment, emphasizing that human involvement in the assessment is **"must"** and should not be overlooked.

The actual safety and security compliance assessment can be carried out by various third-party audit certification bodies. The assessment results determine whether the asset component or system meets the specified compliance criteria or if further actions are necessary to address any non-compliance issues. During this stage, queries can be submitted to the constituent tables shown in Fig. 1 using a (*'requirement id'*) as an input to retrieve associated information supporting the system's compliance with the requirement. We use the process shown in Fig. 2 data flow diagram to retrieve this information from the tables, where the input is the (*'requirement id'*). The output includes the compliance (*'requirement name,' 'component id,' 'component name,' 'stakeholder name,' 'stakeholder type,' 'connection id,' 'connection source,' 'connection destination,' 'parameter id,' 'parameter name,' and 'parameter value'*). The auditor can then determine, based on the retrieved information, whether the requirement is fulfilled.

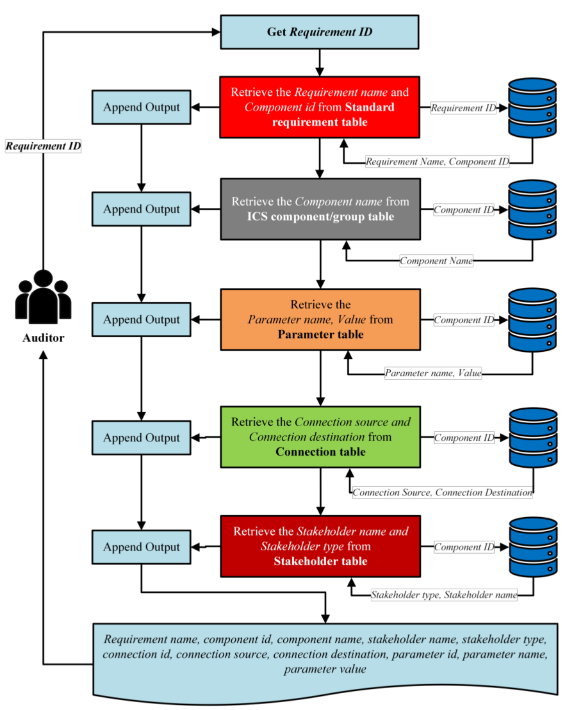


Fig. 2. Data Flow Diagram Illustrating the Retrieval of Requirement Information from the Database

TABLE I
GATHERED INFORMATION IN MPS 403-1

A. Component/Group		
Component Id/ Group Id	**Component/ Group Name**	**Type of Component/ Group**
G01	Distribution Group	Both
C01	Emergency Button	Hardware
C02	PLC	Hardware
C03	Mini IO Terminal	Hardware
C04	Switch	Hardware
C05	Workstation (Manufacturing Execution System (MES))	Hardware
C06	Human-Machine Interaction (HMI)	Hardware
C07	IO Gateway	Hardware
C08	Radio-Frequency Identification (RFID) Gateway	Hardware
C09	RFID	Hardware
C10	PLC Firmware	Software
C11	Operating System	Software
C12	Server 1	Software
C13	Server 2	Software
C14	Database 1	Software
C15	Database 2	Software
C16	Router (Access Point)	Hardware

B. Unit		
Unit Id	**Name**	**Abbreviation**
U01	Year	Yr

C. Parameter				
Parameter Id	**Name**	**Value**	**Unit Id**	**Component Id**
P01	Patch Management Capabilities	Available	-	C05, C10, C11
P02	Access Control Mechanisms	ACL's, and VPN Control	-	C04, C06, C08, C16
P03	Audit trail completeness	YES	-	C06, C12, C13
P04	Authentication logs	Available	-	C06
P05	Compliance with safety lifecycle stages	Not Available	-	G01
P06	Continuous operation logs	Available	-	C08, C16
P07	Data integrity checks	MACsec (802.1AE), IPsec and SSL	-	C08
P08	Encryption protocols used	PROFINET	-	C01, C02, C03, C04, C05, C06, C07, C16
P09	FMEA reports	Not Available	-	G01, C02
P10	Frequency of security assessments	Each Quarter	-	G01
P11	Log retention policies Period	2	U01	C06, C12, C13
P12	Log review and analysis procedures	Not Available	-	C06, C12, C13
P13	Safety function test results	Available	-	G01, C01, C02
P14	Security Level-2	Not Available	-	C04, C08
P15	Security Level-3	Not Available	-	C02, C05, C06, C16
P16	SIL rating documentation	Not Available	-	C01, C02

TABLE II
GATHERED INFORMATION IN MPS 403-1

A. Connection					
Conn. Id	**Conn. Name**	**Conn. Type**	**Conn. Source**	**Conn. Destination**	**Conn. Protocol**
CN01	Connection 1	Digital Signal	C07	C08	-
CN02	Connection 2	Digital Signal	C08	C09	-
CN03	Connection 3	Network Connection	C01	C02	PROFINET
CN04	Connection 4	Network Connection	C02	C04	PROFINET
CN05	Connection 5	Network Connection	C03	C04	PROFINET
CN06	Connection 6	Network Connection	C04	C07	PROFINET
CN07	Connection 7	Network Connection	C04	C16	TCP/IP
CN08	Connection 8	Network Connection	C04	C06	PROFINET
CN09	Connection 9	Logical	C02	C10	-
CN10	Connection 10	Logical	C05	C11	-
CN11	Connection 11	Logical	C05	C12	-
CN12	Connection 12	Logical	C05	C13	-
CN13	Connection 13	Logical	C05	C14	-
CN14	Connection 14	Logical	C05	C15	-

B. Stakeholder				
Stakeholder Id	**Stakeholder Name**	**Stakeholder Type**	**Component Responsibility**	**Training or Education**
S01	John Doe 1	ENGINEER	C15, C03, C06, C07, C02, C04, C05, C01	TÜV Certified Functional Safety Expert
S02	John Doe 3	OPERATOR	C04, C05, C08, C10	On-board training
S03	John Doe 4	ASSET OWNER	C04, C05, C08, C10	ICS410: ICS/SCADA Security Essentials
S04	Jane Doe 1	ADMIN	C15, C03, C06, C07, C02, C9	SANS Security Essentials for IT Administrators
S05	Jane Doe 3	VENDOR	C15, C03, C06, C07, C02, C04, C05	BSI Vendor management
S06	Jane Doe 5	INTEGRATOR	C15, C03, C06, C07, C02, C04, C05, C01, C08	CISA NCCIC ICS TRAINING

IV. USE CASE DEMONSTRATION

The use case shown in Fig. 3 demonstrates a Festo MPS 403-1 didactic plant system. The distribution group is responsible for handling, sorting, and supplying workpieces within the production system. The MES initiates workpiece orders, the HMI specifies workpiece colors, and RFID technology records data on completed workpieces. The entire process revolves around these operations. We acknowledge that the study is being conducted on a small quantitative basis but is complex enough to reflect the Industry 4.0 landscape, demonstrating proof of concept for the proposed methodology.

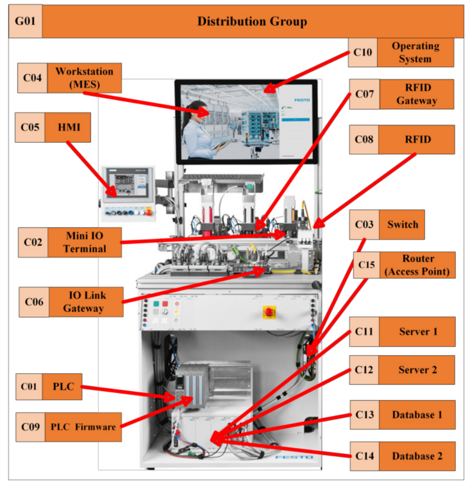


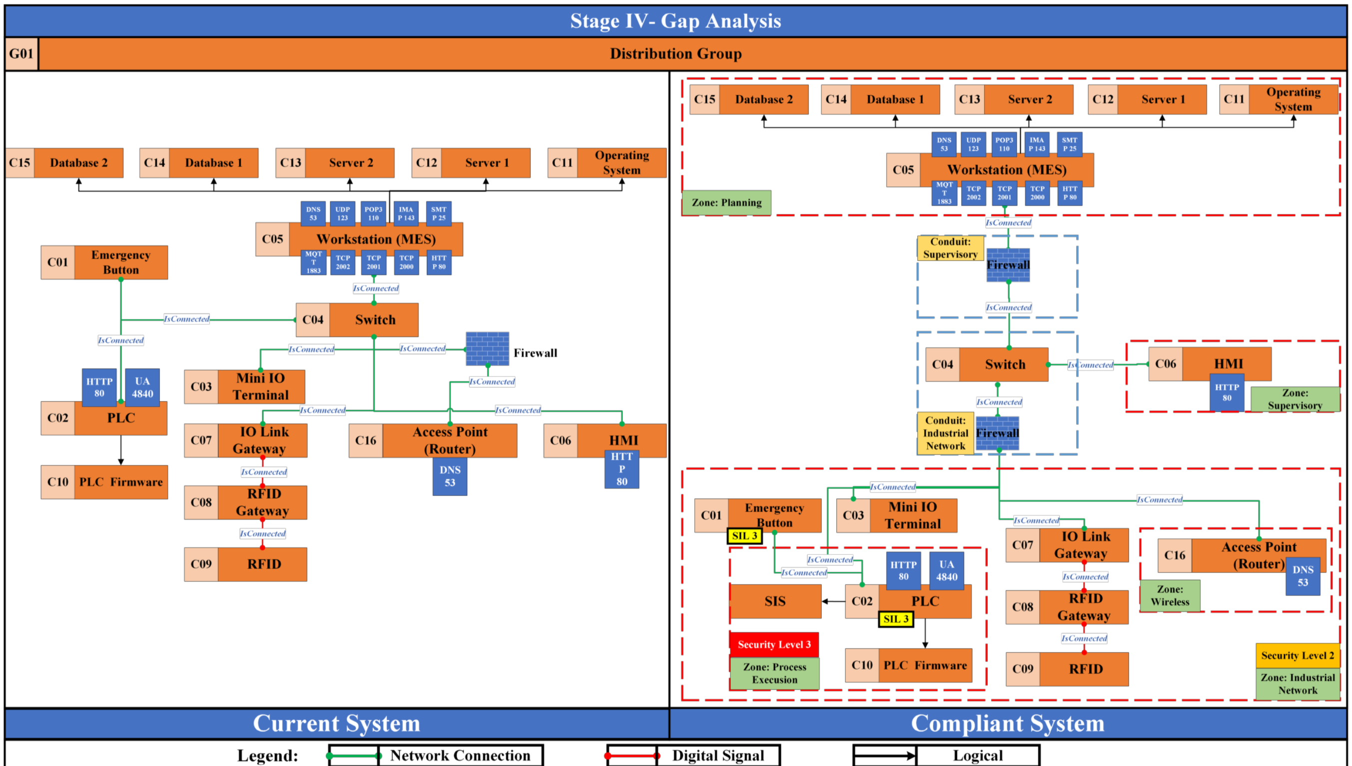
Fig. 3. Distribution Group in Modular Production System (MPS) 403-1

Stage I: In this stage, we have collected the following information: Component/group information (G01, C01-C16) in Table I-A, Unit (U01) for those component/group parameter values in Table I-B, Parameters (P01-P16) related to those components/groups in Table I-C, Connections (CN01-CN14) of those components/groups in Table II-A, and Stakeholders (S01-S06) related to the components/groups in Table II-B.

Stage II: In this stage, we exclusively focus on the identified IEC 62443 standard for security and IEC 61508 standard for safety to conduct a compliance check based on a modular integration approach. The related requirements **(RQ1-RQ10)**, with five requirements for each standard for demonstration, are depicted in Table III.

Stage III: In this stage, as illustrated in Table III, attributes (*'Req. on Component/Group Id'*) and (*'Req. Parameter'*) are allocated to support the requirements. To optimize, we assigned the same requirement to multiple components/groups and parameters.

Stage IV: Using the information gathered and shown in Table I and II, we visualize the exact architecture of the actual system. A security or safety expert, such as a CISO or Operational Technology (OT) security consultant, will then analyze the actual system shown in Fig. 4 (top left). The experts identify gaps in the current system as part of internal audits, ensuring compliance with the IEC 62443 standard for security and the IEC 61508 standard for safety. These audits reveal where the plant's security and safety practices and controls fall short. These gaps can include issues such as open ports, running services in the network, boundary protection, allocation of conduits and zones, evaluation of SIL levels, identification of safety hazards, and safety requirements specifications—all of which are critical aspects evaluated against the standards'



Stage V- Compliance Assessment

SECURITY REQUIREMENT

Input: RQ2
Output:
Requirement Name: SR 5.1 – Network Segmentation
Component/Group Id-Name: Switch (C04), Router Access Point (C16)
Connections:
PLC (C02) --> (C04)
Mini IO Terminal (C03) --> Switch (C04)
Switch (C04) --> IO Gateway (C07)
Switch (C04) --> Router Access Point (C16)
Switch (C04) --> HMI (C06)
Parameter-Value:
Access Control Mechanisms (P02)= ACL's and VPN Control
Continuous Operation Logs (P06)= Not Available
Encryption Protocols Used (P08)= PROFINET
Security Level-3 (P15)= Not Available
Stakeholder Name-Type:
John Doe 1 - ENGINEER, John Doe 2 - OPERATOR, John Doe 4 - ASSET OWNER, Jane Doe 3 - VENDOR, Jane Doe 5 - INTEGRATOR

SAFETY REQUIREMENT

Input: RQ7
Output:
Requirement Name: Clause 7 – Safety requirements specification
Component/Group Id-Name: Emergency Button (C01), PLC (C02)
Connections:
Emergency Button (C01) --> PLC (C02)
PLC (C02) --> Switch (C04)
PLC (C02) --> PLC Firmware (C10)
Parameter-Value:
SIL Rating Documentation (P16)= Not Available
Stakeholder Name-Type:
John Doe 1 - ENGINEER, Jane Doe 1 - ADMIN, Jane Doe 3 - VENDOR, Jane Doe 5 - INTEGRATOR

SECURITY REQUIREMENT

Input: RQ2
Output:
Requirement Name: SR 5.1 – Network Segmentation
Component/Group Id-Name: Switch (C04), Router Access Point (C16)
Connections:
PLC (C02) --> (C04)
Mini IO Terminal (C03) --> Switch (C04)
Switch (C04) --> IO Gateway (C07)
Switch (C04) --> Router Access Point (C16)
Switch (C04) --> HMI (C06)
Parameter-Value:
Access Control Mechanisms (P02)= ACL's and VPN Control
Continuous Operation Logs (P06)= Available
Encryption Protocols Used (P08)= PROFINET
Security Level-3 (P15)= Available
Security Level-2 = Available
Zones and Conduits = Available
Stakeholder Name-Type:
John Doe 1 - ENGINEER, John Doe 2 - OPERATOR, John Doe 4 - ASSET OWNER, Jane Doe 3 - VENDOR, Jane Doe 5 - INTEGRATOR

SAFETY REQUIREMENT

Input: RQ7
Output:
Requirement Name: Clause 7 – Safety requirements specification
Component/Group Id-Name: Emergency Button (C01), PLC (C02)
Connections:
Emergency Button (C01) --> PLC (C02)
PLC (C02) --> Switch (C04)
PLC (C02) --> PLC Firmware (C10)
PLC (C02) --> Safety Instrumented System (SIS)
Parameter-Value:
SIL Rating Documentation (P16)= Available
Stakeholder Name-Type:
John Doe 1 - ENGINEER, Jane Doe 1 - ADMIN, Jane Doe 3 - VENDOR, Jane Doe 5 - INTEGRATOR

Fig. 4. Demonstration of Stage IV and V of the Methodology (Top left: Visualization of the Current System, Top right: Compliant System, Bottom left: Compliance Assessment of the Current System, Bottom right: Compliance Assessment of the Compliant System)

TABLE III
SAFETY AND SECURITY COMPLIANCE REQUIREMENTS

Req. Id	Req. on Component/ Group Id	Req. Name	Req. Type	Req. Description	Req. Standard	Req. Parameter
RQ1	C15	SR 1.1 – Human User Identification and Authentication	Security	Ensure that only authorized personnel can access the control system, with different levels of access based on user roles.	IEC 62443-3-3:2013	P02, P03, P04, P08, P11, P15
RQ2	C04, C16	SR 5.1 – Network Segmentation	Security	Separate the network into distinct zones to limit the spread of potential cyber threats, ensuring critical areas are isolated.	IEC 62443-3-3:2013	P02, P06, P08, P15
RQ3	C05, C08, C09	SR 3.1 – Communication Integrity	Security	Implement measures to protect data from being altered or tampered with during transmission and storage.	IEC 62443-3-3:2013	P01, P02, P06, P07, P08, P14
RQ4	C06, C12, C13	SR 6.1 – Audit Log Accessibility	Security	Maintain detailed logs of all access and operations performed within the system to monitor and trace security incidents.	IEC 62443-3-3:2013	P02, P03, P04, P08, P11, P12, P15
RQ5	G01	4.3.4.5 – Security Assessment and Audit	Security	Conduct regular security assessments and vulnerability scans to identify and address potential weaknesses in the system.	IIEC 62443-2-1:2010	P10
RQ6	G01	Clause 7 – Overall safety lifecycle requirement	Safety	A safety management plan includes hazard analysis, safety requirements specification, design and implementation, operation, and maintenance procedures.	IEC 61508-1:2010	P05, P09, P13
RQ7	C01, C02	Clause 7 – Safety requirements specification	Safety	Define and apply appropriate Safety Integrity Levels (SIL) to various components and processes based on their risk assessment.	IEC 61508-1:2010	P16
RQ8	G01	Clause 7.4.4.3 – FMEA	Safety	Perform FMEA to identify potential failure modes and their effects on the system, ensuring proper mitigation measures are in place.	IEC 61508-2:2010	P05, P09
RQ9	G01	Clause 7.9 – Safety Validation	Safety	Conduct thorough safety validation tests to confirm that the system meets all specified safety requirements and performs as intended under all conditions.	IEC 61508-2:2010	P13
RQ10	C16	Clause 7.4.4 – Fault Tolerance	Safety	Design the system with redundancy and fault tolerance to ensure it remains operational even in the event of component failures.	IEC 61508-2:2010	P06

criteria. After the gap analysis, the necessary changes are implemented in the current system to achieve compliance, as shown in Fig. 4 (top right).

Stage V: This may involve conducting third-party audits or internal inspections of the plant's security and safety controls on a preliminary basis. Using the process shown in Fig. 2, an auditor who wants to check the security requirement **RQ2** and safety requirement **RQ7** can input the respective (*'requirement id.'*) The output mainly consists of details auditors typically look for, such as the requirement's name, the names of the components/groups involved, the connections of these components, the parameter names supporting the requirement, and the stakeholder names and their respective types responsible for the component/group. Based on the output for the current system, as shown in Fig. 4 (bottom left), the auditor can suggest improvements. The auditor can then again follow the process shown in Fig. 2 for the compliant system and view the output, as shown in Fig. 4 (bottom right). We assessed all 10 requirements (5 for safety and 5 for security) using the proposed methodology on the current state of the Festo MPS system. Among these, only three security requirements (RQ1, RQ3, and RQ5) were fulfilled, while none of the safety requirements were followed.

V. CONCLUSION

In this work, we propose a methodology for semi-automated safety and security compliance checks, demonstrated through a Festo MPS 403-1 use case. The methodology leverages the reusability of entities to support the increasing complexity of Industry 4.0 applications. In response to the research questions addressed in this paper: **Q1** delves into methods and techniques for effectively gathering, storing, and managing asset information. This includes discussions on various data sources such as AIMS [19], expert knowledge, and management efforts, which are detailed in Section III-Stage I. **Q2** highlights how the methodology identifies commonalities among requirements, ensures compliance with each requirement, and streamlines the compliance process for organizations operating in multiple regulatory environments. This discussion is covered in Section III-Stage II and Stage III. **Q3** explores the benefits and drawbacks of employing semi-automated approaches for safety and security compliance compared to traditional manual methods. This system can process vast amounts of data much faster than manual checks, leading to quicker compliance verification. It also ensures that compliance processes are consistently applied across all operations, thereby reducing the chances of human error and saving on labor costs. Timely and accurate compliance checks with detailed information can help avoid fines and penalties associated with non-compliance. **Q4** aims to facilitate compliance assurance at both the component and system levels by providing mechanisms for tracking and monitoring compliance requirements throughout the development lifecycle. Sections III-Stage I and Stage IV address these questions, covering the entire system lifecycle from initial asset information gathering to gap analysis at both component and system levels. This methodology serves as a valuable tool for different certification bodies, enabling them to conduct efficient preliminary compliance checks. By employing our methodology, certification bodies can recommend necessary changes to industries before the actual certification process, thereby optimizing and enhancing the overall certification procedure.

While beneficial, this methodology has several limitations and drawbacks that need addressing for improvement. One significant issue is the reliance on data accuracy; if the data used for checks is incomplete or inaccurate, the results will be unreliable. Additionally, the system may struggle with intricate details, exceptions, and overlapping requirements that are challenging to translate into automated rules, leading to potential false positives (flagging compliant as non-compliant) or false negatives (missing non-compliant). The ability to interpret context-specific situations that require human judgment is another limitation, as the system may not always grasp the nuances involved. Furthermore, maintaining and updating the system requires continuous resources, and as automation becomes more sophisticated, the system's complexity can increase, making it harder to manage and troubleshoot.

For future work, we will be developing a software framework for safety and security evaluation and compliance which will be available in upcoming dissemination. Our methodology also offers the potential to analyze the time saved in requirement analysis. Automating this process aims to improve the efficiency of the certification process for both certification bodies and management teams. Furthermore, by providing a centralized repository for all requirements, our methodology facilitates easier management and tracking of compliance efforts, ultimately enhancing safety and security standards across multiple industries.

ACKNOWLEDGMENT

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

REFERENCES

[1] Dragos, "Ponemon institute: The 2021 state of industrial cybersecurity," 02 2022. [Online]. Available: https://www.dragos.com/resource/2021-state-of-industrial-cybersecurity-ponemon/

[2] D. Goetsch and S. Davis, *Quality Management for Organizational Excellence: Introduction to Total Quality*. Prentice Hall, 2010.

[3] Y. Lu, K. Morris, and S. Frechette, "Current standards landscape for smart manufacturing systems," *Nat. Inst. Stand. Technol.*, 01 2016.

[4] M. Felser, M. Rentschler, and O. Kleineberg, "Coexistence standardization of operation technology and information technology," *Proceedings of the IEEE*, vol. 107, no. 6, pp. 962–976, 2019.

[5] S. Misra, C. Roy, T. Sauter, A. Mukherjee, and J. Maiti, "Industrial internet of things for safety management applications: A survey," *IEEE Access*, vol. 10, pp. 83 415–83 439, 2022.

[6] S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: The road ahead," *Computer Networks*, vol. 76, pp. 146–164, 2015.

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

[8] K. Julisch, "Security compliance: The next frontier in security research," in *Proceedings of the 2008 New Security Paradigms Workshop*, ser. NSPW '08. New York, NY, USA: Association for Computing Machinery, 2008, p. 71–74.

[9] F. B. Schneider, "Enforceable security policies," *ACM Trans. Inf. Syst. Secur.*, vol. 3, no. 1, p. 30–50, feb 2000.

[10] S. Ziegler, A. Skarmeta, J. Bernal, E. E. Kim, and S. Bianchi, "Anastacia: Advanced networked agents for security and trust assessment in CPS IoT architectures," in *2017 Global Internet of Things Summit (GIoTS)*, 2017, pp. 1–6.

[11] S.-K. Choi, C.-H. Yang, and J. K. and, "System hardening and security monitoring for IoT devices to mitigate IoT security vulnerabilities and threats," *KSII Transactions on Internet and Information Systems*, vol. 12, no. 2, pp. 906–918, February 2018.

[12] S. N. Matheu, J. L. Hernandez-Ramos, and A. F. Skarmeta, "Toward a cybersecurity certification framework for the Internet of Things," *IEEE Security & Privacy*, vol. 17, no. 3, pp. 66–76, 2019.

[13] A. Gandhi, A. Suditu, A. Frame, and A. Mison, "IoTSF IoT security assurance framework release 3.0 nov 2021," https://iotsecurityfoundation.org/wp-content/uploads/2021/11/IoTSF-IoT-Security-Assurance-Framework-Release-3.0-Nov-2021-1.pdf, 11 2021.

[14] A. Bicaku, M. Zsilak, P. Theiler, M. Tauber, and J. Delsing, "Security standard compliance verification in system of systems," *IEEE Systems Journal*, vol. 16, no. 2, pp. 2195–2205, 2022.

[15] S. Peldszus, K. Tuma, D. Strüber, J. Jürjens, and R. Scandariato, "Secure data-flow compliance checks between models and code based on automated mappings," in *2019 ACM/IEEE 22nd International Conference on Model Driven Engineering Languages and Systems (MODELS)*, 2019, pp. 23–33.

[16] A. Bicaku, M. Tauber, and J. Delsing, "Security standard compliance and continuous verification for Industrial Internet of Things," *International Journal of Distributed Sensor Networks*, vol. 16, no. 6, p. 1550147720922731, 2020.

[17] Z. Anwar and R. Campbell, "Automated assessment of compliance with security best practices," in *Critical Infrastructure Protection II*. Boston, MA: Springer US, 2008, pp. 173–187.

[18] M. Bhole, W. Kastner, and T. Sauter, "A model based framework for testing safety and security in operational technology environments," in *2022 IEEE 27th International Conference on Emerging Technologies and Factory Automation (ETFA)*, 2022, pp. 1–4.

[19] ——, "Knowledge representation of asset information and performance in OT environments," in *2023 IEEE 28th International Conference on Emerging Technologies and Factory Automation (ETFA)*, 2023, pp. 1–8.

[20] "IEC 61508-1 : Functional safety of electrical/ electronic/programmable electronic safety-related systems," 06 2010.

[21] "CEN ISO/TR 22100-4 : Safety of machinery — Relationship with ISO 12100 guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects," 03 2021.

[22] "OVE IEC TR 63069 : Industrial-process measurement, control and automation - Framework for functional safety and security," 05 2019.

[23] "IEC TR 63074 : Safety of machinery – security aspects related to functional safety of safety related control systems," 05 2019.

[24] "BSI - Industrielle Steuerungs- und Automatisierungssysteme (ICS)."

[25] "NIST Special Publication 800-82 Revision 2 : Guide to Industrial Control Systems (ICS) Security," 04 2022.

[26] "IEC TR 62443-3-3:System security requirements and security levels IEC," 08 2013.

[27] "IEC 62443-3-2: Security risk assessment for system design," 06 2020.

[28] "IEC 62443-4-1: Secure product development lifecycle requirements," 01 2018.

[29] "IEC 62443-4-2: Technical security requirements for IACS components," 02 2019.