Human Factors in Cybersecurity, Vol. 168, 2025, 70–81
https://doi.org/10.54941/ahfe1006144

Resolving Conflicts Between PSIRT and Safety Teams: A Collaborative Approach

Jumpei Tahara[1,2], Kenji Watanabe[1], Ichiro Koshijima[2], and Ryushun Oka[1]

[1]Nagoya Institute of Technology, Gokiso-cho, Showa-Ku, Nagoya, Aichi, 466–8555, Japan
[2]Manufacturing and Innovation DX Laboratory, Nagoya Institute of Technology, Gokiso-cho, Showa-Ku, Nagoya, Japan

ABSTRACT

The need to meet safety and security simultaneously is increasing in industrial control systems (ICS) and industrial robots, where network connectivity is rapidly expanding. However, the "safety first" culture that has taken root in many companies has put security requirements on the back burner, and there is a structure prone to conflicts between the two domains. In this study, the authors elucidate the conflict factors in the safety and security life cycle and propose a new collaborative framework based on the knowledge creation theory (SECI model, Ba, knowledge assets) of Nonaka et al. We conducted semi-structured interviews and qualitative analysis of five Japanese Industrial product suppliers. In the interview, we highlighted potential and actual conflicts between the product safety and security teams (e.g., PSIRT: Product Security Incident Response Team). In this paper, we proposed a resolution model for conflicts by dealing with cultural and cognitive gaps among experts from the perspective of human factors. We hope this model improves risk management in various industries and under cybersecurity laws and regulations amid tight regulations worldwide, such as the EU Cyber Resilience Act.

Keywords: Industrial cybersecurity, Safety and security integration, PSIRT, EU cyber resilience act, Cross-functional collaboration

INTRODUCTION

In today's society, where control systems and industrial robots are networked, the threat from cyberspace to the physical world is becoming more serious. For example, there have been many reports of cases where cyber attacks on the Port of Nagoya have caused a three-day work stoppage, forcing Toyota and other factories to suspend operations, and cases where medical institutions have been forced to suspend medical services due to ransomware. As concerns grow over the direct and indirect impact on people and social infrastructure, the balance between safety and security is becoming increasingly important.

In industrial automation, IEC TR 63069 recommends a coordinated and integrated approach to safety and security but does not adequately indicate specific ways of coordination. As a result, it is not easy for product safety

© 2025. Published by AHFE Open Access. All rights reserved.

teams (responsible for functional safety within supplier organizations) and security teams (e.g., PSIRT: Product Security Incident Response Team) to work together with different priorities, terminology, and cultures.

Therefore, in this study, we propose a new coordination framework to embody further the "coordination of safety and security" indicated by the IEC TR63069 and verify the framework's effectiveness through interviews with five large industrial product suppliers in Japan.

BACKGROUND OF THIS WORK AND PROBLEM STATEMENT

As a background, we summarize IEC TR63069 and its issues. Figure 1 shows the "cooperative domain," where the safety and security domains partially overlap in industrial automation and control systems.

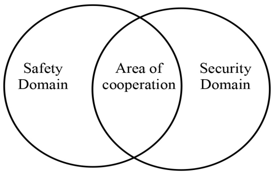


Figure 1: Safety domain and security domain (adapted from IEC TR 63069, Figure 2, 2019).

Furthermore, Figure 2 shows how the safety domain (the area of functional safety based on IEC61508) and the security domain (the area of security based on IEC62443) cooperate and interfere with each other throughout the life cycle.

In the safety domain, functional safety is designed and evaluated. In the security domain, risk assessments are conducted assuming unauthorized access, etc., but depending on the countermeasures, they affect each other. For example, communication restrictions to improve security may adversely affect the response time of safety functions. On the other hand, additional safety designs can create new security vulnerabilities. IEC TR 63069 recommends that experts continuously share and review these conflicts at each life cycle stage (planning, development, operation, and maintenance).

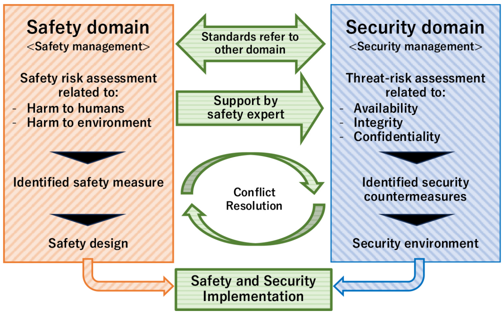


Figure 2: Safety and security interaction (adapted from IEC TR 63069, Figure 4, 2019).

Other Concurrent Approaches

In recent years, examples of the V-model, which simultaneously designs and implements safety and security, have been proposed, using the development of automated wheelchairs as an example (Sasaki et al., 2022). In addition, in industrial control systems (ICS/OT), examples of how system integrators and asset owners can manage both areas in an integrated manner have been reported (IPA, 2018; Ehrlich et al., 2021). However, there is still a shortage of specialists who are familiar with both safety and security in practice (IPA, 2018), and security and evidence management in safety-critical areas (e.g., automotive, medical) continue to be challenged by the lack of cross-organizational processes and the shortage of specialized human resources, as shown by Mohamad et al. (2024).

Based on the above, although a framework that simultaneously deals with security and safety requirements is being proposed, there are still many difficulties in applying it to practice. How safety and security teams (e.g., PSIRT) work together is not well examined, and further research is needed, especially at supplier companies.

Problem Setting to Focus on in This Study

This study focuses on the conflict factors and coordination processes between safety teams (responsible for functional safety at supplier organizations) and security teams (e.g., PSIRT) in product suppliers. The following issues must be solved when applying the coordination outlined in IEC TR 63069 to practice.

1. **Lack of concrete measures to "bridge the gap" between the two experts**

There is no concrete way to reconcile the two areas, which differ in terminology and organizational culture.

2. **Lack of concrete measures to resolve conflicts in the life cycle**

The circulation of knowledge, operating models, and guidelines at each stage are insufficient. From the perspective of human factors, differences in recognition and culture among specialists, as well as a lack of cross-organizational management, are significant factors that hinder cooperation between the two fields.

RESOLUTION MODEL FOR SAFETY VS SECURITY CONFLICT

To ensure safety and security throughout the product life cycle - from planning and development to operation and maintenance - we propose a new framework (Figure 3) based on the knowledge creation theory (SECI model, Ba, knowledge assets) of Nonaka et al. (2000) as a mechanism to shift from domain-specific activities to cooperative processes when conflicts arise.

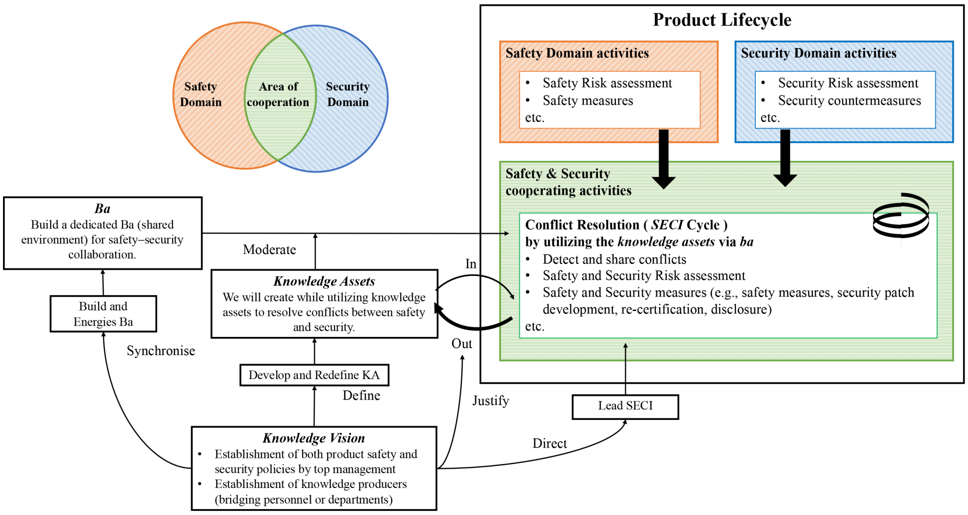

Safety Domain
Area of cooperation
Security Domain
Product Lifecycle
Safety Domain activities
• Safety Risk assessment
• Safety measures
etc.
Security Domain activities
• Security Risk assessment
• Security countermeasures
etc.
Safety & Security cooperating activities
Conflict Resolution (SECI Cycle)
by utilizing the knowledge assets via ba
• Detect and share conflicts
• Safety and Security Risk assessment
• Safety and Security measures (e.g., safety measures, security patch development, re-certification, disclosure)
etc.
Ba
Build a dedicated Ba (shared environment) for safety–security collaboration.
Moderate
In
Knowledge Assets
We will create while utilizing knowledge assets to resolve conflicts between safety and security.
Out
Build and Energies Ba
Synchronise
Develop and Redefine KA
Define
Justify
Lead SECI
Direct
Knowledge Vision
• Establishment of both product safety and security policies by top management
• Establishment of knowledge producers (bridging personnel or departments)

Figure 3: Safety-security cooperation based on knowledge creation theory of Nonaka et al. (2000).

Knowledge Vision

Knowledge Vision is the starting point for top management to set out a policy that equally emphasizes product safety and security and to build cooperative relationships that transcend the boundaries of specialized fields. This will encourage the creation and activation of Ba, and the people in charge of both domains will be able to interact and create knowledge with the same sense of purpose. Furthermore, it will be possible to continuously operate new knowledge and guidelines in the latest form by defining and redefining the scope of knowledge assets and providing standards that justify the results of these assets as an organization. By leading and directing the SECI process, it is possible to effectively utilize tacit and explicit knowledge, turning the conflict between safety and security into a creative learning opportunity. In order to facilitate this process, it is essential that management clearly states a policy that treats both safety and security equally and that middle management and specific departments are formally positioned as “knowledge producers” and appointed as coordinators and facilitators of decision-making to connect the two teams.

Parallel Domain Activities

- The safety domain (e.g., functional safety teams) and the security domain (e.g., PSIRT) continue their respective activities, adhering to specialized standards (e.g., IEC 61508 for safety, IEC 62443 for security).
- Each domain conducts risk assessments, designs, and validation steps, preserving domain-specific expertise and autonomy.

Detection and Escalation of Conflicts

Whenever a conflict or trade-off emerges (e.g., performance degradation caused by encryption or required re-certification due to post-shipment updates), it is immediately escalated to a dedicated Ba – a shared environment for dialogue and knowledge exchange.

Knowledge Assets and Ba

- The organization maintains a library of knowledge assets relevant to safety and security (e.g., risk assessment templates, threat models, past incident reports, and design guidelines).
- These assets are the foundation for an interactive, constructive debate within the Ba. Both teams can articulate tacit knowledge, exchange perspectives, and converge on solutions through face-to-face or virtual sessions.

SECI Cycle for Conflict Resolution

The SECI (Socialization–Externalization–Combination–Internalization) cycle provides a systematic approach to harness both tacit and explicit knowledge in conflict resolution:

- **Socialization:** Team members share real-world concerns, experiences, and intuitions face-to-face in Ba, identifying the root causes behind the conflict.
- **Externalization:** Using metaphors or diagrams, tacit insights become explicit proposals and risk models that both domains can understand.
- **Combination:** These explicit proposals are synthesized with existing organizational assets (e.g., incident databases) to generate actionable measures for mitigating the conflict.
- **Internalization:** The solutions (e.g., updated design requirements, security patches, or revised safety protocols) are tested or implemented, allowing teams to refine their tacit knowledge through real-world application.

Iterative Learning and Continuous Improvement

- The outcomes of each conflict-resolution cycle are fed back into the organization's knowledge assets, thus enriching future safety–security cooperation.
- Over time, the organization cultivates a more robust, adaptive process that balances safety imperatives and security demands throughout the product life cycle.

This integrated model ensures that safety and security teams can carry out their specialized work while having a well-defined, knowledge-driven mechanism for constructive cooperation whenever trade-offs or conflicts arise. By iterating the SECI cycle within Ba and leveraging shared knowledge assets, an organization can transform potential friction points into opportunities for collective learning and innovation.

EVALUATION AND METHODOLOGY OF THE PROPOSED MODEL

Study Design

In this study, we adopted a case study method centered on qualitative interviews to explore the practical realities of safety and security coordination and the usefulness and challenges of the proposed framework. Specifically, we will collect and analyze the roles of security and safety managers at Industrial product supplier companies, collision cases, and the current state of knowledge sharing through semi-structured interviews.

Target Companies and Interview Participants

We asked five large companies that develop and provide products that can be connected to networks, such as industrial control systems and industrial robots, to cooperate with them and conducted semi-structured interviews with seven people involved in safety and security practices (Table 1).

Table 1: List of interviewees (P# = Participant ID, "Case" indicates different companies A to E).

P#	Case	Role	Experience (Total/ Security/ Safety)
1	A	PSIRT Leader	>20 / >20 / 2–5
2	B	Safety Leader	>20 / >20 / 0–2
3	C	PSIRT Operations	15–20 / 5–10 / -
4	C	Product Security Specialist	10–15 / 10–15 / -
5	D	PSIRT Member	10–15 / 2–5 / 10–15
6	E	Security Promotion Manager	10–15 / 5–10 / -
7	E	Developer (Control Division)	>20 / 5–10 / 10–15

Interview Guide & Conduct

The interviews covered topics such as (1) organizational background and division of roles, (2) timing of consideration in the life cycle, (3) collision cases and decision-making flow, (4) information sharing and incident response, (5) compliance with management policies and laws and regulations, and (6) educational programs and bridging human resources. Depending on the interviewee, there were cases where more than one person was present (Case C) or only a preliminary questionnaire response (P#7).

Implementation Period and Method

From January 6 to 31, 2025, one of the authors conducted 1~1.5 hours of online interviews with each company, and the interview took notes without recording. At a later date, the interviewee confirms and supplements the content and adjusts the scope of disclosure.

Data Analytics

The interview records were first divided into questions, labeled (open-coded) into characteristic phrases, and keywords such as "resistance to post-shipment updates" and "encryption and availability" were extracted. Next, the extracted codes were organized by commonality and relevance and categorized from the viewpoint of safety and security considerations, organizational culture, and educational system. In addition, referring to SECI and Ba indicated by the Proposed Model, we organized "what works and does not work in conflict resolution" on a case-by-case basis, based on the points that have already been practiced, the deficiencies, and the management policy and leadership situation.

Ethical Considerations

Participants were explained in advance about the purpose of the study, the time required, and the handling of data, and their cooperation was obtained based on their free will. The names of companies and individuals will not be disclosed, and the analysis results will be anonymized and reported.

RESULTS

In this study, we interviewed seven people in charge of five large companies to investigate the actual situation regarding safety and security coordination. In this section, we present findings on (1) the timing of consideration in the life cycle, (2) examples of collisions between the two, (3) organizational culture and leadership, (4) the shortage of education systems and bridging human resources, and (5) future issues.

Timing of Consideration in the Life Cycle

In many companies, safety is analyzed using FMEA and other methods from the early planning stages, while security tends to be considered just after the functional requirements are determined.

- *"Security cannot be considered unless functional requirements are determined, and risk assessments are conducted separately" (Case A)*
- *"We do not do it together, and we do not think about safety in terms of probability and bad faith" (Case B)*

In addition, there are concerns about retesting and additional costs when corrections are made on the safety side after shipment.

- *"It is hard to fix it on the safety side after shipment, and it requires retesting for standard certification, which is expensive" (Case B)*

Some companies (e.g., Case C) reported a policy incorporating threat analysis from the planning stage. However, there were reports that cooperation at the practical level was insufficient, and the business unit and product category pointed out variations.

Examples of Safety and Security Conflicts

In the process industry and control system fields, where availability and response are important, there are concerns about performance degradation due to communication encryption and cases where security measures are postponed.

- *"We want to encrypt it, but it will be damaged if it stops even for a moment because availability is our priority. At the very least, we will seek a compromise by ensuring completeness through hashing" (CaseA)*

On the other hand, some companies responded that there were few cases where the two persons in charge clashed or were confronted at the design stage, but this was because "it is difficult for the security side to refute safety risks" and "risk assessments are conducted separately in the first place, and conflicts do not surface."

- *"I do not think there was a confrontation in the first place, but I think it is difficult to argue when safety risks are raised" (Case B)*

As a result, security issues are put on the back burner due to corporate culture and organizational power relations. However, the structure makes it difficult for conflicts to surface.

Organizational Culture and Leadership

While the safety field has a long history and a culture of "safety first" has taken root, security seems to be treated as an "afterthought."

- *"Safety and security are different religions, and safety has been around for 100 years" (Case A)*

There is also an example of a move by the quality department to include security (Case C), but it has not yet reached explicit coordination across the organization. In addition, in Case E, *there is an opinion that "the protection of human life (safety) is prioritized, and the protection of assets (security) is treated as a derivative,"* and the imbalance of priorities has become apparent. In addition, it was pointed out that there was a lack of policies and resources at the management level and a tendency for "budgets to fall after an incident occurs."

- *"We do not have the money to investigate vulnerabilities, and if there is damage, the budget will be dropped" (Case A)*
- *"It is more of a bottom-up, top-down is weak" (Case E)*

As a result, it is left to the response of each business unit, and it is challenging to recognize conflicts and issues as management issues.

Shortage of Education and Bridging Personnel

Although there are safety and security experts in each, most respondents said there are "almost no" "bridging personnel" or cross-training personnel who can understand both and mediate in the event of conflict.

- *"Safety: Security is 100:0 or 0:100 experts, not 60:40" (Case A)*
- *"There are no bridging personnel, there is no cross-training" (Case B)*
- *"We provide product security-related training for the quality department, but rarely the other way around (safety training)" (Case C)*
- *"There is no program that can learn about safety and security from each other, and it should be introduced, but it is difficult to set the scope" (Case D)*

Some companies have expressed their desire to introduce cross-training in the future, but it is not easy to set the scope of what exactly will be taught at what stage and to what extent, and discussions have only just begun. The absence of such bridging personnel and a proper education system are obstacles to coordinating the organization.

Expectations and Challenges for the Future

Regulations such as the EU CRA are being strengthened, and international standards are being developed; there is a growing need to balance safety and security throughout the supply chain.

- *"In order to comply with new laws and regulations such as the EU CRA, it is necessary to have human resources with legal skills, and there is no staff who can interpret the law in both areas" (Case C)*
- *"It is difficult to comply with the EU CRA, there are many supply chains, and 24-hour operation is expensive" (CaseA)*

Under these circumstances, there was a desire for top-down leadership and a restructuring of the organizational structure. Case E emphasizes that *"safety education is individualized, security education is only partial, and it is necessary to encourage decision-making from the top management to move things forward across the organization."* On the other hand, Case C states, *"It is effective to separate operations while maintaining 'connections' that can be consulted with each other, rather than forcibly promoting integration, but in the end, it is necessary to have human resources with diverse expertise, including legal affairs, and a clear organizational structure."* Furthermore, as Case A says, *"It is difficult to change awareness without external enforcement, such as laws and standards,"* it can be seen that the government is trying to solve problems by conforming to laws and regulations.

DISCUSSION

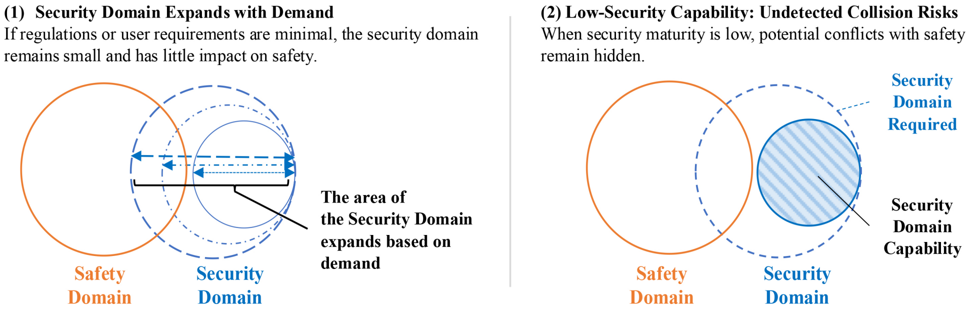
The interview results revealed the following insights.

Coordination Throughout the Lifecycle

In this study, we combined the life cycle concept of IEC TR 63069 with the knowledge creation theory of Nonaka et al. to analyze the gap between the safety department and the PSIRT (security department). As a result of the interviews, it is recognized that it is necessary to deal with both areas simultaneously throughout the life cycle, but in practice, there is a noticeable lack of coordination, especially in the event of a collision due to a culture that prioritizes safety. Therefore, it is essential to have a system that comprehensively examines security from the early stages of the life cycle and allows for continuous cooperation between the two areas even after shipment.

Factors Behind the Seemingly Low Conflict: Demand and Maturity

Some companies responded that "safety and security rarely collide" because (1) security requirements are limited at the moment, and there is little overlap with safety requirements. (2) The maturity of the security side is low, and the risk has not materialized (Figure 4). However, if security requirements are expanded due to the EU CRA and other measures, the area of cooperation will expand, and the possibility of serious conflicts will increase.



(1) Security Domain Expands with Demand
If regulations or user requirements are minimal, the security domain remains small and has little impact on safety.

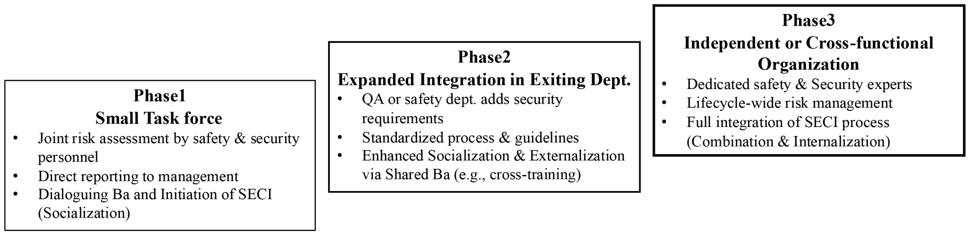
(2) Low-Security Capability: Undetected Collision Risks
When security maturity is low, potential conflicts with safety remain hidden.

The area of the Security Domain expands based on demand
Safety Domain
Security Domain
Security Domain Required
Security Domain Capability
Safety Domain
Security Domain

Figure 4: Two key factors for minimal conflict perception: (1) Limited security demands; (2) Low-security capability.

Organizational Structure and Leadership Roles: An Approach to Incremental Expansion of Collaborative Areas

In some cases, when safety and security are managed simultaneously, the quality department handles both areas. However, concerns such as "security requirements are likely to be buried" and "management support is weak" have been pointed out. Therefore, in this study, we propose a framework that expands the cooperation area in three stages according to the company's maturity level (Figure 5).



Phase1
Small Task force
- Joint risk assessment by safety & security personnel
- Direct reporting to management
- Dialoguing Ba and Initiation of SECI (Socialization)

Phase2
Expanded Integration in Exiting Dept.
- QA or safety dept. adds security requirements
- Standardized process & guidelines
- Enhanced Socialization & Externalization via Shared Ba (e.g., cross-training)

Phase3
Independent or Cross-functional Organization
- Dedicated safety & Security experts
- Lifecycle-wide risk management
- Full integration of SECI process (Combination & Internalization)

Figure 5: Step by step for area of cooperation.

Phase 1: Set up a small task force, conduct risk assessments with safety and security staff concurrently, and report the results directly to management to create a foothold for the next step.

Phase 2: Expand the safety department (e.g., the quality department) to a framework that integrates security and develops company-wide standards and processes. Integrate safety culture and security knowledge through training and education.

Phase 3: Establish a cross-sectional organization directly under management and strengthen risk response in cooperation with the supply chain and external organizations. With a two-tier structure in which the quality department is responsible for day-to-day operations and the cross-sectional organization is responsible for policy formulation and integrated promotion, it is possible to achieve a balance between the entire life cycle.

This phased approach is expected to change the status quo, where security tends to take a back seat and make safety and security a permanent part of the organizational culture in the long term.

CONCLUSION

In this study, the authors presented a framework that combines the coordination between safety and security indicated by IEC TR 63069 with the knowledge creation theory of Nonaka et al. and examined its effectiveness through a qualitative survey of an Industrial product supplier. As a result of the interviews, issues such as the current situation where security tends to be put off and the lack of bridging human resources and top-down measures were clarified. At the same time, the importance of "visualization of tacit knowledge" and "commitment of management and development of middle managers" indicated by this model was suggested.

This study focused on product supplier internal conflicts. Further study is necessary for post-shipment collaboration between a product supplier and its customer.

ACKNOWLEDGMENT

We would like to express our deepest gratitude to all participants for their openness and cooperation in providing information and interviews on the sensitive topic of safety and security. We would also like to thank all of the business partners who provided coordination and support for this research.

REFERENCES

Ehrlich, M., Bröring, A., Harder, D., Auhagen-Meyer, T., Kleen, P., Wisniewski, L., Trsek, H., and Jasperneite, J. (2021). Alignment of safety and security risk assessments for modular production systems, e & i Elektrotechnik und Informationstechnik, 138, 454–461.

Information-technology Promotion Agency, Japan (IPA). (2018). Control System Safety and Security Requirements Consideration Guide – Basic Edition. IPA Website: https://www.ipa.go.jp/files/000064728.pdf

International Electrotechnical Commission (IEC). (2019). Industrial-process measurement, control and automation – Framework for functional safety and security (IEC TR 63069:2019). International Electrotechnical Commission.

International Electrotechnical Commission (IEC). (n.d.). IEC 61508 series. Functional safety of electrical/electronic/programmable electronic safety-related systems. International Electrotechnical Commission.

International Electrotechnical Commission (IEC). (n.d.). ISA/IEC 62443 series. Industrial communication networks – Network and system security. International Electrotechnical Commission.

Mohamad, M., Steghöfer, J.-P., Knauss, E. and Scandariato, R. (2024). Managing security evidence in safety-critical organizations, Journal of Systems and Software, 214:112082.

Nonaka, I., Toyama, R. and Konno, N. (2000). SECI, Ba and Leadership: A Unified Model of Dynamic Knowledge Creation, Long Range Planning, 33(1), 5–34.

Sasaki, T., Hamaguchi, T., and Hashimoto, Y. (2022). A Collaborative Design Method for Safety and Security Engineers, Proceedings of the European Conference on Cyber Warfare and Security, 21(1), 263–270.