Incidents of Industrial Systems Part 1: Industrial Cybersecurity

Péter Ungvári

Doctoral School on Safety and Security Sciences, Óbuda University, Budapest
ungvari.peter@kvk.uni-obuda.hu
ORCID: 0009-0004-9068-6081

Tibor Wührl

Kandó Kálmán Faculty of Electrical Engineering, Óbuda University, Budapest
wuhrl.tibor@kvk.uni-obuda.hu
ORCID: 0000-0002-7522-3511

Abstract: In the study, design, and maintenance of information system security, knowledge of relevant standards is fundamental. These standards require risk analysis. During risk analysis, incidents are assessed, and attackers are identified. It is useful to categorize incidents when assessing the likelihood of their occurrence and their impact, which facilitates the transparency and management of incidents. Our premise is that there is currently no universally accepted and applied classification system for industrial system incidents and attacks. The first part of our two-part study introduces the topics of industrial security risk management and incident management, laying the foundation for the second part, which delves into the categorization of incidents in more detail. Our goal by the end of the second part is to substantiate the hypothesis with literature sources and explore related causes and possibilities.

Keywords: incident, risk analysis, cybersecurity, safety, industrial automation

Introduction

During the fourth industrial revolution and at the threshold of the fifth, industrial automation systems—as information systems—play a crucial role. Economic competitiveness within an ageing society, under the constraints of a limited workforce and increasing competition, can only be maintained through the use of highly automated cyber-physical systems [1], [2]. Maintaining industrial information systems, however, involves numerous threats and hazards [3], [4].

Security incidents—events causing damage—may result in substantial losses. Such losses range widely: from life-threatening mass disasters, through material damage comparable to the GDP of smaller countries, to slight reductions in the competitive market position of a manufacturing company [5]. To establish and maintain protection against such losses, risk assessment is indispensable, and its application is defined and required by numerous industrial and IT standards [6], [7], [8], [9]. However, it is not always evident how incidents—and, within them, incidents caused by intentional attacks—may be described or handled. The foundation of incident management is categorisation. Based on category definitions, clear procedures and processes can be formulated to mitigate, prevent, or avoid recurrence of incident-related damage.

Introduction to Part 1: Industrial Cybersecurity

Due to digitalisation, an industrial system can only be considered secure if both physical safety and cyber security requirements are met. In cyber-physical systems, data processing and hardware operation are strongly interlinked; consequently, physical safety heavily depends on cyber security. Information security is dynamic, relative, and represents a momentary state. As a result of the activity of threat agents, new hazards and threats appear daily. Exploiting system vulnerabilities, these threats lead to risk, which—acting on assets—results in system exposure [5], [10].

1 Standards of Industrial Security

Physical safety in industrial process control is covered by the IEC 61511 functional safety standard series (Functional safety – Safety instrumented systems for the process industry sector). We refer to this standard series for completeness and due to its fundamental risk-related terminology that also appears in other standards. Such foundational terms include Safety Instrumented System (SIS), Safety Instrumented Function (SIF), and Safety Integrity Level (SIL), representing the degree of risk reduction achieved by a SIF. Implementing a safety instrumented system and achieving certification in accordance with the standard are costly and may not always be feasible for smaller enterprises. Nevertheless, from an educational perspective and for identifying hidden risks, familiarity with the standard is highly beneficial [3].

The general standard for industrial cyber security is ISA / IEC 62443 [11].

2 Acceptable Security Level

IEC 62443-3-2 specifies that the acceptable level of risk, i.e. the Target Security Level (SL-T), must be defined and regularly compared to the Available Security Level (SL-A) and the Current Security Level (SL-C). Determining these security levels requires risk assessment. It is important to assign numerical values to the levels for normative comparison. Table 1 illustrates the individual security levels.

Table 1: Security Levels According to IEC 62443

Security Level	Description
SL4	Protection against sophisticated attacks by groups with extensive resources and strong motivation. These include international criminal organisations, cyber-warfare actors, and the tools and defences associated with them.
SL3	Protection against intentional, targeted attacks. Attackers possess significant resources and motivation.
SL2	Protection against simple, intentional attacks carried out by less motivated attackers with limited knowledge and resources.
SL1	Protection against unintentional damage, such as accidental errors, improper use, configuration mistakes, or unintended information disclosure.
SL0	No protection required or provided. The security of the system is not evaluated. This represents the baseline state and is extremely rare as an acceptable level. Therefore, some sources consider only SL1–SL4.

Based on these descriptions, it becomes straightforward to determine the current level of protection of the examined system (System Under Consideration, SuC) or its components.

The standard provides guidance for assessing these levels through seven Foundational Requirements (FR1–FR7). Through detailed technical analysis of technologies, components, and their documentation, as well as information obtained from vendors and integrators, it becomes possible to evaluate the achievable security level for individual components and the integrated system as a whole under proper operation.

Risk assessment helps identify what risks a system or component may be exposed to. Based on this assessment, the acceptable security level can be defined, in accordance with the given relationships [11].

3 Risk Assessment

To avoid incidents and mitigate damage, security measures must be implemented whose cost (C) is substantially lower than the risk value (R), defined as the cost of damage (D) weighted by the probability of incident occurrence (P). Effective protection reduces risk by an amount greater than the cost of implementing the protection (see Figure 1).

$$R = P * D$$

$$C \ll R$$

$$R - R' > C$$

Figure 1: Inequalities in Risk Assessment

However, risk analysis and risk management must also consider that the organisation must be able to finance the maintenance of protection, and severe consequences—such as threats to human life or significant environmental damage—must be excluded.

Risk assessment and its methodologies are covered in ISO/IEC 27005 and IEC 31010, among others [9], [12].

4 Incident Management

IEC 62443-2-1 addresses planning and procedures for responding to incidents as part of the security lifecycle requirements. The main objectives of incident management are personal safety, protection of physical assets, and maintaining business continuity [11].

Incident management is also addressed independently in ISO/IEC 27035, NIST SP 800-61, and NIST SP 800-171, Section 3.6 [13], [14], [15]. Incident handling in the IEC 62443 industrial cyber security standard does not differ significantly from general cyber security standards. A common feature is that none define incident categories.

Table 2 lists the key steps of incident management according to IEC 62443 [11].

Table 2: Key Steps of Incident Management

Step	Description
Incident Detection	Identification of malicious or operationally harmful security events.
Incident Containment	Actions taken to isolate the incident or limit its propagation.
Incident Analysis	Investigating the cause and extent of the incident to understand how it occurred.
Incident Recovery	Restoring affected systems and processes to normal operation.
Post-Incident Review	Evaluation, lessons learned, and development of additional security measures.

Summary

This article has organised and presented the principal standards and concepts of industrial security, based on scientific sources and the texts of the standards. The individual scholarly contribution lies in highlighting relevant details and drawing new conclusions. We discussed risk assessment and incident management in general terms, identifying the objectives and steps of incident handling, which demonstrated why incident categorisation is valuable. The IEC 62443 standard defines security levels referencing the intent, motivation, and available resources of the threat actor (e.g. attacker). The standard focuses primarily on designing and maintaining secure systems through assessments and protective measures, with less emphasis on incident handling. Thus, it approaches incident-related topics from the direction of risk assessment. Categorising potential incidents can be performed during the assessment of a specific system (SuC), through risk analysis and continuous review. This requires predefined category classes.

References

[1] M. A. Bär and A. W. Colombo, “Engineering ICPS for Small and Medium Enterprises: A Novel DIN SPEC 91345 Compliant Digitalization Approach,” *IEEE Trans. Ind. Cyber-Phys. Syst.*, vol. 1, pp. 307–321, 2023, doi: 10.1109/TICPS.2023.3328840.

[2] J. Shi, J. Wan, H. Yan, and H. Suo, “A survey of Cyber-Physical Systems,” in *2011 International Conference on Wireless Communications and Signal Processing (WCSP)*, 2011, pp. 1–6. doi: 10.1109/WCSP.2011.6096958.

[3] A. Bicaku, C. Schmittner, P. Rottmann, M. Tauber, and J. Delsing, “Security Safety and Organizational Standard Compliance in Cyber Physical Systems,” *Infocommunications J.*, vol. XI, no. 1, pp. 2–9, 2019.

[4] A. Corallo, M. Lazoi, and M. Lezzi, “Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts,” *Comput. Ind.*, vol. 114, p. 103165, Jan. 2020, doi: 10.1016/j.compind.2019.103165.

[5] J. P. Kesan and L. Zhang, “Analysis of Cyber Incident Categories Based on Losses,” *ACM Trans Manage Inf Syst*, vol. 11, no. 4, p. 25:1-25:28, 0 2020, doi: 10.1145/3418288.

[6] F. Brancati, D. Mongelli, F. Mariotti, and P. Lollini, “A cybersecurity risk assessment methodology for industrial automation control systems,” *Int. J. Inf. Secur.*, vol. 24, no. 2, 2025, doi: 10.1007/s10207-025-00990-9.

[7] H. L. Hassani, A. Bahnasse, E. Martin, C. Roland, O. Bouattane, and M. E. Mehdi Diouri, “Vulnerability and security risk assessment in a IIoT environment in compliance with standard IEC 62443,” *Procedia Comput. Sci.*, vol. 191, pp. 33–40, 2021, doi: 10.1016/j.procs.2021.07.008.

[8] S. Hollerer, T. Sauter, and W. Kastner, “Risk Assessments Considering Safety, Security, and Their Interdependencies in OT Environments,” in *Proceedings of the 17th International Conference on Availability, Reliability and Security*, in ARES ’22. New York, NY, USA: Association for Computing Machinery, 0 2022, pp. 1–8. doi: 10.1145/3538969.3543814.

[9] “Risk assessment standards,” IEC TC 56. Accessed: Dec. 05, 2023. [Online]. Available: https://tc56.iec.ch/risk-assessment-standards/

[10] “Risk Management Standards,” ENISA. Accessed: Dec. 10, 2023. [Online]. Available: https://www.enisa.europa.eu/publications/risk-management-standards

[11] “ISA/IEC 62443 Series of Standards - ISA,” isa.org. Accessed: June 01, 2025. [Online]. Available: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

[12] “ISO/IEC 27005:2022,” ISO. Accessed: June 01, 2025. [Online]. Available: https://www.iso.org/standard/80585.html

[13] “ISO/IEC 27035-2:2023,” ISO. Accessed: June 01, 2025. [Online]. Available: https://www.iso.org/standard/78974.html

[14] R. Ross and V. Pillitteri, “Protecting controlled unclassified information in nonfederal systems and organizations,” National Institute of Standards and Technology (U.S.), Gaithersburg, MD, NIST SP 800-171r3, May 2024. doi: 10.6028/NIST.SP.800-171r3.

[15] A. Nelson, S. Rekhi, M. Souppaya, and K. Scarfone, “Incident response recommendations and considerations for cybersecurity risk management : a CSF 2.0 community profile,” National Institute of Standards and Technology (U.S.), Gaithersburg, MD, NIST SP 800-61r3, Apr. 2025. doi: 10.6028/NIST.SP.800-61r3.