Incidents of Industrial Systems – Part 2: Incident Categories

P. Ungvári

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

T. 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 [1]. 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 [2], [3]. 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 introduced the topics of industrial security risk management and incident management. This is the second part, which delves into the categorization of incidents in more detail. Our goal 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—hold exceptional significance. Economic competitiveness within an ageing society, where workforce availability is limited and competition intensifies, can only be maintained through highly automated cyber-physical systems [4], [5]. However, maintaining industrial information systems involves numerous threats and hazards [6], [7]. Security incidents—events resulting in damage—can cause extremely high-value losses.

The magnitude of such losses varies widely, from life-threatening mass disasters to material damages comparable to the GDP of a small country, or even merely a slight decline in the competitive market position of a manufacturing company [3]. To establish and preserve protection against these losses, risk assessment is indispensable, as required and regulated by numerous industrial and information security standards [1], [8], [9], [10].

However, it is not always evident how to characterise incidents—or, within them, the attackers causing incidents—and how such incidents should be managed. The foundation of incident handling is categorisation. Based on well-defined categories, clear procedures and processes may be formulated to mitigate, eliminate, and prevent the recurrence of incident-related damages.

1 Research for Loss-Based Classification

Based on the experiences and research of the past decade, incidents that appear similar in nature may result in significantly different levels of loss. When designing protection for industrial information systems and when handling incidents, the experiences of past incidents may be used as a foundation. By performing cluster analysis on datasets of globally observed incidents, it is possible to identify dimensions that have a decisive impact on the magnitude of loss. In this way, incidents may be classified according to experienced loss. These categories may then be used as a basis for the risk assessment of new systems [3].

The referenced study describes a concrete procedure that makes the research reproducible and provides a foundation for new investigations. For its practical utilisation, further questions may be formulated:

- Is it worthwhile to perform internal research within the organisation?
- Does the organisation have access to a historical database of incidents?
- Does the database contain relevant incidents with adequate detail?
- Can distortions caused by undisclosed or concealed incidents be handled?
- Can the organisation rely on similar research—that is, conduct secondary research alone?

2 CISA NCISS Categories

The aim of the Cybersecurity and Infrastructure Security Agency (CISA) in developing the National Cyber Incident Scoring System (NCISS) was to elevate

incident handling to the level of national defence, providing a framework for assessing the national-security impact of incidents affecting various organisations.

NCISS assigns a score from 0 to 100 to incidents using weightings across eight categories. Based on this score, it determines a priority level [11].

NCISS Categories (simplified descriptions):

- **Functional impact**: the business/operational impact on the organisation
- **Observed activity**: the activity of the threat actor
- **Location of observed activity**: the network segment where the activity took place
    - Level 1: unsuccessful activity, no network access
    - Level 2: business demilitarised zone (DMZ)
    - Level 3: business network
    - Level 4: critical system DMZ
    - Level 5: critical system management
    - Level 6: critical system processes
    - Level 7: security systems
    - Unknown: the location cannot be identified, only the activity observed
- **Actor characteristics**: the attacker's capabilities and intent
- **Information impact**: the IT security impact
- **Recoverability**: the organisational authority and resources needed for restoration
- **Cross-sector dependencies**: the extent to which the incident affects other sectors
- **Potential impact**: the possible national-security impact of the incident

NCISS Colour-coded Priority Levels (simplified):

- **Emergency** (black): imminent threat to governmental stability or human life
- **Severe** (red): major threat to healthcare, personal safety, national security, economic security, civil liberties, or international relations
- **High** (orange): the incident is likely to affect the above areas
- **Medium** (yellow): consequences may affect the areas listed above

- **Low** (green): consequences do not affect the above areas
- **Baseline**: easily remediable minor incidents, subdivided into minor (blue) and negligible (white). Their function is primarily to raise awareness, even if they do not cause significant damage.

CISA is responsible for cyber defence within the United States [12]. In the European Union, equivalent responsibilities fall to ENISA and the national Computer Security Incident Response Teams (CSIRTs) [18], [19], [20]. In Hungary, this role is fulfilled by the National Cybersecurity Centre [16].

3 Vulnerability and Weakness Categories

The Common Vulnerability Scoring System (CVSS) is currently in its fourth version. CVSS evaluates vulnerabilities based on attacks that have already occurred and are thoroughly understood. Using its predefined categories, the severity of an experienced vulnerability can be clearly determined. The categories, levels, and weights are unambiguously defined within CVSS [16].

The Common Security Advisory Framework (CSAF) Version 2.0—maintained by the OASIS CSAF Technical Committee—specifies the global reporting and management of vulnerabilities in detail. Using this framework, the CVE (Common Vulnerabilities and Exposures) online catalogue—maintained jointly by MITRE, CISA, and the DHS—provides globally accessible information on identified vulnerabilities with detailed CVSS scoring and categorisation [17], [18]. Consequently, for most globally known vulnerabilities, there exists a database entry affecting the software components used in industrial systems.

However, further challenges may arise:

- Industrial systems may include closed, custom-developed, or restricted-licence software components.
- Even components that are secure and free of major vulnerabilities may form a vulnerable system when poorly integrated or misconfigured.
- New and previously unknown vulnerabilities emerge daily.

Therefore, while CVE and CVSS are necessary for establishing industrial system security, they are not sufficient on their own. Nevertheless, they offer useful guidance for analysing a system and determining IEC 62443 SL-A, SL-C, and SL-T security levels.

MITRE's Common Weakness Scoring System (CWSS) resembles CVSS and uses similar category classes but serves a different purpose: it focuses specifically on preparing for potential incidents that have not yet occurred [19]. It can further

refine and validate the security levels defined for industrial systems in accordance with the IEC 62443 standard.

Summary of Incident Categories

Risk levels and security levels can be established for known, widely used system components based on databases of published vulnerabilities. The CSAF and CWSS frameworks provide ready-made incident category classes and calculation methods for this.

Security Operations Centres (SOCs) within industrial organisations are responsible for defining security levels that apply both to individual components and to integrated systems as a whole, as well as for conducting full-scope risk analyses and security assessments [6]. General and industrial security standards offer methodologies for performing such analyses. Methods such as CWSS or cluster-analysis-based calculations—like those presented in Section 1.1—may also be applied or further extended.

Organisational incident management can be extended to the national-security level, as demonstrated by CISA, ENISA, and related CSIRT organisations. The NCISS provides the most comprehensive incident category and priority classification, as it considers both the operational impact on a given organisation and national-security implications, including cross-sector dependencies.

The scientific contribution of this chapter lies in interpreting and discussing the various frameworks within a complementary, standards-aligned context.

Conclusion

Incident category classes may be defined in similar, but not uniform, ways when examining vulnerabilities of software components, integrated systems within industrial enterprises, or national-security-level impacts. Although the IEC 62443 industrial cyber-security standard does not define incident categories, it addresses incident response and provides procedures and methods, alongside additional general cyber-security standards.

The referenced sources support the original hypothesis and describe incident category classes in detail. The scoring frameworks discussed not only categorise incidents but also calculate key parameters: prioritisation (NCISS), severity (CWSS), and risk level (CVSS). The cited cluster-analysis approach enables the determination of unique incident categories as well.

Therefore, the hypothesis is confirmed: no unified incident categorisation system exists, despite the necessity of such categorisation and the existence of multiple frameworks that define fixed classes applicable at different levels. Moreover, incident categories may also be determined algorithmically, for example through cluster analysis.

References

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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)*, IEEE, 2011, pp. 1–6.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

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

[11] ‘CISA National Cyber Incident Scoring System (NCISS) | CISA’. Accessed: June 01, 2025. [Online]. Available: https://www.cisa.gov/news-events/news/cisa-national-cyber-incident-scoring-system-nciss

[12] ‘Home Page | CISA’. Accessed: June 01, 2025. [Online]. Available: https://www.cisa.gov/

[13] ‘ENISA’, ENISA. Accessed: Dec. 10, 2023. [Online]. Available: https://www.enisa.europa.eu

[14] ‘EU incident response and cyber crisis management | ENISA’. Accessed: June 01, 2025. [Online]. Available: https://www.enisa.europa.eu/topics/eu-incident-response-and-cyber-crisis-management

[15] ‘CSIRT, Computer Security Incident Response Team’. Accessed: June 01, 2025. [Online]. Available: https://www.csirt.org/

[16] ‘Magunkról’, Nemzeti Kibervédelmi Intézet. Accessed: June 01, 2025. [Online]. Available: https://nki.gov.hu/intezet/tartalom/magunkrol/

[17] ‘Common Security Advisory Framework Version 2.0’.

[18] ‘CVE: Common Vulnerabilities and Exposures’. Accessed: June 01, 2025. [Online]. Available: https://www.cve.org/

[19] ‘CWE - Common Weakness Scoring System (CWSS)’. Accessed: Dec. 02, 2024. [Online]. Available: https://cwe.mitre.org/cwss/cwss_v1.0.1.html