Secure Systems Design and Technology Development. Veliko Tarnovo, Bulgaria
Proceedings of the International Scientific Conference, 2026. Volume I, 351-355

Physical Vulnerability of Cyber Systems: Analysis of Incidents, Risk Factors and Security Strategies

Nikolay Penev
University of Library Studies and Information Technologies
Sofia, Bulgaria
4623496-2@unibit.bg

Daniela Pavlova
Faculty of Information Sciences, Computer Sciences Department
University of Library Studies and Information Technologies
Sofia, Bulgaria
d.pavlova@unibit.bg

Jasen Tanev
University of Library Studies and Information Technologies
Sofia, Bulgaria
q.tanev@unibit.bg

Nikolay Koev
University of Library Studies and Information Technologies
Sofia, Bulgaria
4623497-2@unibit.bg

Andrian Stoilov
University of Library Studies and Information Technologies
Sofia, Bulgaria
a.stoilov@unibit.bg

Kiril Nikolov
University of Library Studies and Information Technologies
Sofia, Bulgaria
k.nikolov@unibit.bg

***Abstract*—Physical security is an essential component of cybersecurity risk management because many cyber and operational technology systems depend on protected facilities, equipment, power supply, communication links and environmental conditions. This paper revises the analysis of physical vulnerability in cyber systems by distinguishing direct physical compromise from cyber incidents that produce physical consequences. A qualitative incident-based methodology is applied to selected cases from 2020 to 2024 and to recent cyber-physical security literature. The method includes source screening, inclusion and exclusion criteria, incident coding by physical vector, affected asset, impact and dependency, and a reproducible ordinal risk score. The results systematize incidents into five categories: direct physical attacks on infrastructure, environmental disruption, compromise of physical-security platforms, compromise of operational technology with physical consequences, and hybrid cyber-physical scenarios. The paper proposes a methodological framework for assessing such incidents and maps the main risk factors to practical security strategies. The findings show that physical vulnerability should not be reduced to facility protection alone; it should be treated as a combined governance, engineering and incident-response problem linking physical access, operational technology, cyber monitoring and business continuity.**

***Keywords*—Critical Infrastructure Protection, Cyber-Physical Systems, Physical Vulnerability, Risk Assessment.**

I. INTRODUCTION

The increasing integration of physical security systems, cyber infrastructure and operational technology (OT) has created a class of risks that cannot be assessed only through conventional information-security controls. Facilities, sensors, actuators, cameras, access-control systems, building automation platforms and industrial control systems are now connected to networks and cloud services, while their failure can affect physical processes and public services. The World Security Report 2023 shows that many security executives already perceive cyber threats against physical security systems as a major organizational challenge [1].

In this paper, a physical vulnerability of a cyber system is defined as a weakness related to physical access, physical protection, equipment location, environmental dependency, power supply, communication infrastructure, or cyber-physical interface that can affect the confidentiality, integrity, availability, safety, or continuity of a digital, OT, or cyber-physical system. This definition is consistent with the NIST view of OT as systems and devices that interact with, monitor, or control the physical environment [2].

Recent scientific literature also emphasizes that cyber-physical system (CPS) security requires threat and risk assessment approaches that connect the cyber domain with the physical domain. Systematic reviews and surveys highlight the importance of defense mechanisms,

Online ISSN 3044-7771
https://doi.org/10.68302/std2026.vol1.58

dependency modelling, safety-security integration and risk prioritization in industrial CPS and OT environments [3]-[6]. However, many incident-based discussions still mix direct physical vulnerabilities with general cyberattacks, ransomware, social engineering and insider threats. This weakens the analytical value of the categorization.

The aim of this study is to provide an incident-based assessment of physical vulnerabilities in cyber systems and to propose a reproducible methodological framework for classifying incidents, evaluating risk factors and selecting mitigation strategies. The contribution of the paper is threefold. First, it clarifies the difference between direct physical compromise and cyber incidents with physical consequences. Second, it systematizes selected incidents according to year, target, vector, impact and risk score. Third, it proposes a methodological framework that can support future assessent of physical security breaches affecting cyber, OT and cyber-physical systems.

II. Materials and Methods

A. Research Scope and Definitions

The study applies a qualitative incident-based research design. It does not claim to be a full statistical survey of all physical-security incidents. Instead, it uses selected documented incidents and authoritative reports to develop a structured assessment framework. The analysis covers incidents and cyber-physical scenarios from 2020 to 2024, while the supporting literature includes peer-reviewed and institutional sources relevant to CPS, OT and critical infrastructure security.

The analysis distinguishes three related but different cases. Direct physical vulnerability refers to physical access, sabotage, theft, environmental damage, or failure of physical protection that directly affects cyber or OT assets. Cyber compromise with physical consequences refers to a cyber intrusion into OT or control systems that can affect physical processes, even when the initial intrusion is not physical. Human-factor incidents such as social engineering are not treated as physical vulnerabilities unless they are directly connected to physical access control, facility security or device compromise.

B. Source Selection and Screening

Sources were selected from four groups: peer-reviewed literature on CPS and OT security, institutional guidance from NIST and CISA, public incident reports, and official or organization-level incident descriptions. Selected sectoral and incident sources were used to document cases relevant to energy infrastructure, environmental disruption, security platforms, building automation, water treatment, and ICS/OT attacks [9]-[14].

Incidents were included when at least one of the following conditions was met: a direct physical act affected a cyber or OT asset; an environmental event disrupted the physical dependencies of cyber infrastructure; a physical-security platform was compromised; an OT or ICS system was compromised with potential physical consequences; or a controlled cyber-physical test demonstrated a combined attack path. Incidents were excluded from the core sample when no physical component or physical consequence could be identified from public evidence. For this reason, general ransomware or social-engineering cases were not used as core examples unless they were connected to physical access or OT operation.

C. Incident Coding and Risk Scoring

Each incident was coded according to the following variables: year, sector, target, physical or cyber-physical vector, affected cyber/OT asset, operational impact, evidence type and mitigation focus. To make the comparison reproducible, a simple ordinal risk score was used:

$$R = E \times I \times D \qquad (1)$$

where E is exposure, I is impact and D is dependency. Each variable is scored from 1 to 5 and the risk score is calculated according to (1). Exposure reflects how reachable or weakly protected the relevant physical or OT asset is. Impact reflects the potential operational, safety, continuity, or data-security effect. Dependency reflects the degree to which other services depend on the affected asset. For transparency, the ordinal scale is interpreted as follows: 1 = low, isolated, or minimal effect; 3 = moderate exposure, sector-level disruption potential, or medium dependency; 5 = high exposure, severe operational/safety effect, or strong dependency of critical services on the affected asset. Scores 2 and 4 represent intermediate levels between the defined low, moderate and high categories.

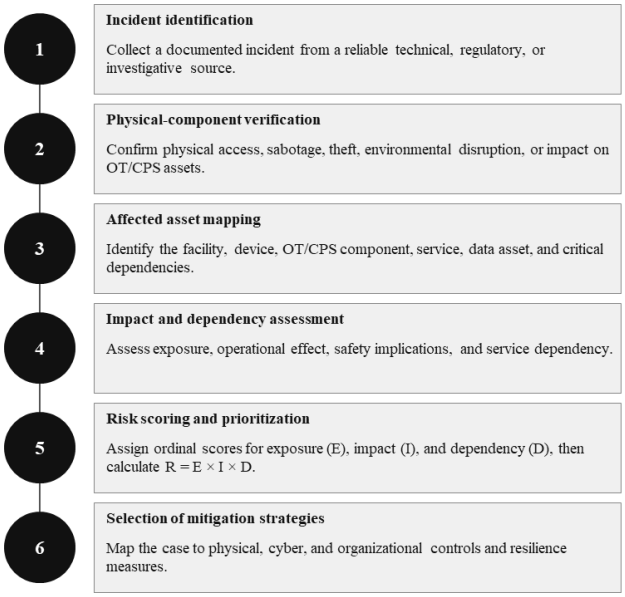

Fig. 1. Methodological framework for assessing incidents caused by physical vulnerabilities of cyber systems.

The framework in Fig. 1 starts with the identification of an incident and then verifies whether a physical component is present. If the case is only a cyber incident without a physical element, it is excluded from the physical-vulnerability category or treated as a related cyber-to-physical case. The next step maps the affected asset and its dependencies, followed by risk scoring. The final steps map the incident to security strategies and use the lessons

learned to improve response, recovery and governance processes. The framework is aligned with the logic of the NIST Cybersecurity Framework 2.0 functions - Govern, Identify, Protect, Detect, Respond and Recover [7] - and with CISA cross-sector goals for prioritized practices in IT and OT environments [8].

III. RESULTS AND DISCUSSION

A. Incident Categorization

The incident analysis shows that physical vulnerability in cyber systems is not a single category. Five analytical categories were identified: direct physical attacks on infrastructure; environmental hazards affecting cyber or OT dependencies; unauthorized access or compromise of physical-security platforms; OT or building automation compromise; and cyber-to-physical boundary cases. The summarized incident coding is presented in Table 1. The cases also show that physical and cyber impacts often interact. A substation shooting can cause digital service disruption because communication, control and business operations depend on power. A compromised cloud-based camera platform may expose physical-security data even though the intrusion path is digital. A water-treatment attack may begin remotely but create potential physical process effects. Therefore, the analytical distinction between vector and consequence is essential.

TABLE 1 SUMMARY OF SELECTED INCIDENTS AND ORDINAL RISK CODING.

Year	Incident / sector	Target / affected asset	Method / vector	Impact / consequence	Risk R (E/I/D)
2020	Glass Fire, California / infrastructure dependencies [10]	Power, facility and communication dependencies	Environmental physical disruption	Availability and continuity risk for dependent systems	32 (2/4/4)
2021	Verkada platform compromise / physical-security systems [11]	Video surveillance and access-control platform	Compromise of a physical-security platform	Camera-feed exposure and facility-related information risk	36 (4/3/3)
2021	Building automation attack, Germany / BMS [12]	Building automation and facility-control devices	Compromise of automation devices	Loss of contact with devices and operational disruption	48 (4/3/4)
2021	Oldsmar water treatment / water sector [13]	Water-treatment process control interface	Unauthorized remote access; cyber-to-physical case	Potential manipulation of water-treatment process	75 (5/5/3)
2022	Moore County substations / energy sector [9]	Electrical substations and dependent services	Firearms attack against substations	Power outage and disruption of dependent digital services	60 (3/5/4)
2023-2024	Cyber Av3ngers and pro-Russia ICS attacks / water, food, healthcare [14]	Internet-facing PLC/HMI and OT assets	PLC/HMI compromise affecting physical processes	Manual operations, HMI manipulation and service-continuity risk	80 (5/4/4)

Note: E - exposure; I - impact; D - dependency; R - ordinal risk score. The notation R (E/I/D) reports the final risk score and the three component scores. Scores are used for transparent prioritization, not for statistical probability estimation.

The evolution of selected incidents and developments is summarized in Fig. 2.

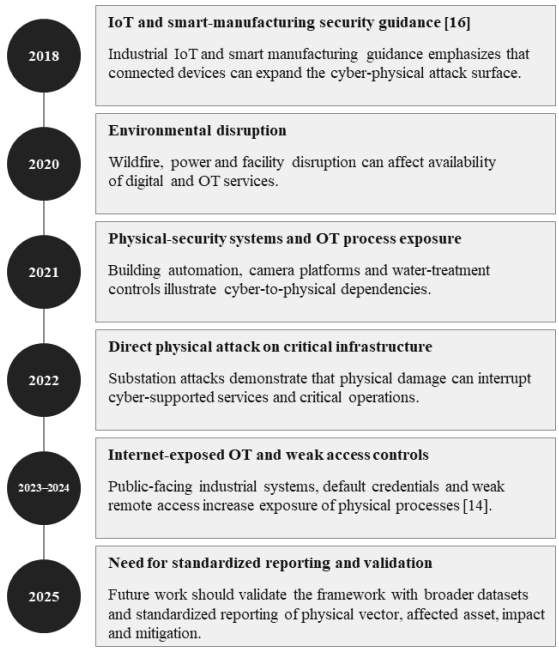

Fig. 2. Timeline of selected physical-security-related and cyber-physical incidents and developments, 2018-2025.

B. Interpretation of the Incident Evidence

The highest risk scores in Table 1 are associated with OT and ICS exposure because the affected systems can interact directly with physical processes. The ODNI/CTIIC dataset from November 2023 to April 2024 reports that Iran-affiliated and pro-Russia actors gained access to or manipulated U.S. ICS in several sectors, including water and wastewater, food and agriculture, healthcare and state/local government. The same report identifies poor password security, default credentials, outdated software and public-facing interfaces as important weaknesses [14].

Direct physical attacks remain highly relevant. The Moore County substation attack illustrates how physical damage to electrical infrastructure can disrupt services for a large population and affect dependent communications, business processes and digital systems. The NCSL report notes that physical security incidents against U.S. electricity infrastructure increased in 2022 compared with prior years and that reported incidents include vandalism, theft, suspicious activity, threats and trespassing [9].

Environmental hazards represent a different mechanism. They do not involve a malicious actor, but they can affect the physical dependencies of cyber systems: power supply, cooling, connectivity and facility availability. The Glass Fire is therefore treated not as a

cyberattack but as an example of environmental disruption that can undermine the operational continuity of dependent digital and cyber-physical services [10].

The Verkada case is also not a direct physical intrusion into a facility. Its relevance lies in the fact that the compromised system was a physical-security platform. Exposure of video feeds and facility-related data may support reconnaissance, privacy violations or subsequent physical-security risks [11]. Similarly, building automation incidents demonstrate that connected BMS devices can become an attack surface affecting lighting, access, heating, ventilation and other physical operations [12].

C. Risk Factors and Security Strategies

The analyzed incidents identify recurring risk factors: insufficient protection of remote access, internet-facing OT, weak password practices, default credentials, inadequate segmentation between IT and OT, weak physical perimeter protection, poor asset inventory, insufficient backup power and cooling, and limited joint training between physical security and cybersecurity teams. The main risk categories and corresponding mitigation strategies are mapped in Table 2.

TABLE 2 MAPPING OF RISK CATEGORIES TO MITIGATION STRATEGIES.

Risk category	Typical risk factors	Recommended strategies
Direct physical attack on infrastructure	Unprotected facilities; limited monitoring; slow response	Perimeter hardening; monitoring; patrols; redundancy
Unauthorized physical access and device compromise	Weak access control; poor asset tracking; removable media	MFA for physical access; visitor control; secure storage; asset inventory
Environmental hazard affecting cyber systems	Fire, flood, heat; power/cooling failure; poor siting	Backup power; environmental sensors; redundant links; DR tests
Compromise of physical-security or OT platforms	Internet-facing devices; default passwords; weak segmentation/logging	Segmentation; remove public exposure; MFA; monitoring; patching
Hybrid cyber-physical scenario	Separate teams; weak exercises; poor information sharing	Joint IR; exercises; alarm correlation; threat intelligence; recovery playbooks

The strategies in Table 2 should be mapped to a governance framework instead of being applied as isolated controls. NIST CSF 2.0 can be used to organize the activities into Govern, Identify, Protect, Detect, Respond and Recover functions [7]. For OT environments, NIST SP 800-82 Rev. 3 emphasizes the need to consider reliability, safety and performance requirements when selecting controls [2]. CISA performance goals also stress prioritized practices for reducing the attack surface and improving resilience in critical infrastructure organizations [8].

The 7SHIELD project illustrates why integrated cyber-physical response is necessary. The project was designed to protect space ground segments against physical, cyber and combined threats and includes prevention, detection, response and mitigation mechanisms [15]. ENISA also emphasizes security and privacy challenges in IoT-enabled smart manufacturing environments, which are relevant to the protection of industrial cyber-physical systems [16].

The analysis also requires the reclassification of some widely cited cybersecurity incidents. Cases such as ransomware attacks or social-engineering intrusions should not automatically be categorized as physical vulnerabilities. They may be relevant when they disrupt physical services or reveal weaknesses in access-control procedures, but the initial vector must be clearly distinguished from the operational consequence. This distinction improves the precision of incident analysis and addresses the main weakness of broad descriptive approaches.

D. Limitations and Future Research

The study is limited by the availability and detail of public incident information. Many reports do not disclose technical evidence, intrusion paths, physical access conditions, or full impact data. Therefore, the risk scores in Table 1 should be interpreted as structured qualitative assessments, not as verified statistical measurements. Future work should expand the dataset, include interviews with infrastructure operators, compare multiple sectors and test the framework with real organizational risk-assessment data.

Future research should also examine whether cyber-physical incident reporting can be standardized across sectors. Standardized reporting fields - physical vector, cyber/OT asset, operational impact, evidence confidence and recovery time - would allow stronger comparison and trend analysis over time.

CONCLUSIONS

The revised analysis shows that the physical vulnerability of cyber systems is a multi-dimensional problem involving facilities, devices, environmental dependencies, OT assets, access-control systems and incident-response processes. The article therefore distinguishes direct physical compromise from cyber incidents with physical consequences. This distinction is necessary because not every cyberattack that affects an organization is a physical vulnerability, while not every physical event is a cyberattack.

The proposed methodological framework supports a more precise assessment of incidents by verifying the physical component, mapping the affected asset and dependency, applying an ordinal risk score, assigning the incident to an analytical category and selecting mitigation strategies. The incident summary and timeline provide a clearer overview of how different physical and cyber-physical mechanisms affect critical infrastructure and cyber systems.

The main practical implication is that organizations should integrate physical security and cybersecurity governance. Protection should include access control, asset inventory, segmentation, remote-access management, environmental monitoring, independent safety

mechanisms, incident-response exercises and recovery planning. By applying an integrated approach aligned with current OT and cybersecurity frameworks, organizations can reduce exposure, improve resilience and respond more effectively to combined physical and cyber threats.

REFERENCES

[1] Allied Universal, "World Security Report 2023," 2023. [Online]. Available: https://www.worldsecurityreport.com/media/v1ahrj2v/a4_world-security-report_vf_en.pdf. [Accessed: May 4, 2026].

[2] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, A. Hahn, and S. H. Le, "Guide to Operational Technology (OT) Security," NIST Special Publication 800-82 Rev. 3, 2023. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-82r3. [Accessed: May 4, 2026].

[3] H. Harkat, L. M. Camarinha-Matos, J. Goes, and H. F. T. Ahmed, "Cyber-physical systems security: A systematic review," Computers & Industrial Engineering, vol. 188, 109891, Feb. 2024, https://doi.org/10.1016/j.cie.2024.109891.

[4] A. Akbarzadeh and S. K. Katsikas, "Dependency-based security risk assessment for cyber-physical systems," International Journal of Information Security, vol. 22, no. 3, pp. 563-578, 2023, https://doi.org/10.1007/s10207-022-00608-4.

[5] X. Lyu, Y. Ding, and S.-H. Yang, "Safety and security risk assessment in cyber-physical systems," IET Cyber-Physical Systems: Theory & Applications, vol. 4, no. 3, pp. 221-232, 2019, https://doi.org/10.1049/iet-cps.2018.5068.

[6] N. Agrawal and R. Kumar, "Security perspective analysis of industrial cyber physical systems (I-CPS): A decade-wide survey," ISA Transactions, vol. 130, pp. 10-24, 2022, https://doi.org/10.1016/j.isatra.2022.03.018.

[7] National Institute of Standards and Technology, "The NIST Cybersecurity Framework (CSF) 2.0," NIST Cybersecurity White Paper 29, Feb. 2024. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf. [Accessed: May 4, 2026].

[8] Cybersecurity and Infrastructure Security Agency, "Cross-Sector Cybersecurity Performance Goals," 2023. [Online]. Available: https://www.cisa.gov/cybersecurity-performance-goals-cpgs. [Accessed: May 4, 2026].

[9] National Conference of State Legislatures, "Human-Driven Physical Threats to Energy Infrastructure," May 22, 2023. [Online]. Available: https://www.ncsl.org/energy/human-driven-physical-threats-to-energy-infrastructure. [Accessed: May 4, 2026].

[10] NASA Jet Propulsion Laboratory, "Glass Fire, September 27, 2020," Oct. 7, 2021. [Online]. Available: https://www.jpl.nasa.gov/images/pia24209-glass-fire-september-27-2020/. [Accessed: May 4, 2026].

[11] Verkada, "Verkada Security Update - Incident Report," 2021. [Online]. Available: https://www.verkada.com/security-update/report/. [Accessed: May 4, 2026].

[12] Dark Reading, "Lights Out: Cyberattacks Shut Down Building Automation Systems," 2021. [Online]. Available: https://www.darkreading.com/cyberattacks-data-breaches/lights-out-cyberattacks-shut-down-building-automation-systems. [Accessed: May 4, 2026].

[13] BBC News, "Hacker tries to poison water supply of Florida city," Feb. 8, 2021. [Online]. Available: https://www.bbc.com/news/world-us-canada-55989843. [Accessed: May 4, 2026].

[14] Cyber Threat Intelligence Integration Center, "Recent Cyber Attacks on US Infrastructure Underscore Vulnerability of Critical US Systems, November 2023-April 2024," Office of the Director of National Intelligence, June 2024. [Online]. Available: https://www.dni.gov/files/CTIIC/documents/products/Recent_Cyber_Attacks_on_US_Infrastructure_Underscore_Vulnerability_of_Critical_US_Systems-June2024.pdf. [Accessed: May 4, 2026].

[15] European Commission, CORDIS, "Safety and Security Standards of Space Systems, Ground Segments and Satellite Data Assets, via Prevention, Detection, Response and Mitigation of Physical and Cyber Threats (7SHIELD)," Project Fact Sheet, 2023. [Online]. Available: https://cordis.europa.eu/project/id/883284. [Accessed: May 4, 2026].

[16] ENISA, "Good Practices for Security of Internet of Things in the Context of Smart Manufacturing," 2018. [Online]. Available: https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot. [Accessed: May 4, 2026].