Proc. of the European Safety and Reliability Conference (ESREL 2026)
Edited by José C. Matos, Paulo B. Lourenço, Michael Beer, Daniel Oliveira,
Edoardo Patelli, Hélder S. Sousa, Rui A. Silva and Monica Santamaria
 Published by Research Publishing, Singapore.
doi: 10.3850/ESREL2026061419_esrel26-p27684-cd

Towards Harmonizing Models and Metrics in Physical Security and Cybersecurity Risk Assessment: An Approach for Cross-Domain Risk Alignment

Dustin Witte

Institute for Security Systems, University of Wuppertal, Germany. E-mail: witte@uni-wuppertal.de

Thomas Termin

Institute for Security Systems, University of Wuppertal, Germany. E-mail: thomas.termin@witte-automotive.de

Daniel Lichte

Institute for the Protection of Terrestrial Infrastructures, German Aerospace Center (DLR), Germany. E-mail: daniel.lichte@dlr.de

Kai-Dietrich Wolf

Institute for Security Systems, University of Wuppertal, Germany. E-mail: wolf@iss.uni-wuppertal.de

Systematic risk assessment is an essential tool to design appropriate protection for critical systems against malicious attacks, both physical and cyber. Although the assessment of physical security and cybersecurity risk both rely on attacker-centered models for analyzing threats and vulnerabilities, the methodologies and standards of these two fields have evolved largely in isolation from each other. This separation complicates the determination of comparable risk levels, which is however becoming increasingly important as systems become more interconnected. Aiming for a unified perspective on security risk, this paper takes up representative standards and methods – namely MITRE ATT&CK and CVSS in cybersecurity, and ASD and EASI in physical security – highlighting structural analogies and domain-specific divergences in vulnerability analysis. Particular focus is given to the consideration of uncertainties arising from adversarial behavior, scenario assumptions and model limitations. Based on the identified analogies, we show how vulnerability could be consistently represented across both domains, and propose a unified model regarding three aspects of physical security and cybersecurity: intrusion paths, protection functions and assessment metrics. We apply our proposal to an illustrative example and discuss its potential to support coherent cross-domain risk assessment for balanced decisions on physical security and cybersecurity measures in a security-critical environment.

Keywords: Physical Security, Cybersecurity, Vulnerability Assessment, Security Convergence, Decision Support.

1. Introduction

Modern critical systems are increasingly exposed to malicious attacks that span both the physical and the cyber domain (Yu et al., 2023). While physical intrusions threaten systems through direct access and sabotage, cyberattacks can compromise the same systems remotely, often with cascading consequences (Sinha et al., 2015). As digitalization and connectivity continue to blur the boundaries between cyber and physical infrastructures, security can no longer be assessed in isolated domains (Bakov, 2024). Although the concept of risk in both domains is based on threat, vulnerability, and consequences, risk assessment in the field of physical security and cybersecurity have evolved largely independently (Mccreight and Leece, 2016). Each domain relies on attacker-centered models and well-established standards, such as ASD or EASI in physical security (Garcia, 2008) and CVSS or MITRE ATT&CK in cybersecurity (Al-Sada et al., 2024; Jiang et al., 2025). However, these approaches differ substantially in their assumptions, metrics, and treatment of uncertainty (Depoy et al., 2005).

As a result, risk levels derived from physical and cybersecurity assessments are typically not comparable, complicating balanced security design and informed decision-making in integrated systems. This lack of comparability becomes critical whenever resources must be allocated across domains

or when combined attack scenarios are considered (Brandstatter and Brunlechner, 2024). Without a harmonized perspective, security measures may be overemphasized in one domain while critical vulnerabilities persist in the other.

Against this background, this paper addresses the need for a consistent cross-domain representation of security risk with a focus on vulnerability. By taking up representative models and metrics from physical security and cybersecurity, we identify structural analogies and domain-specific differences in vulnerability analysis. Based on these analogies, we propose a unified model that aligns intrusion paths, protection functions, and assessment metrics, thereby enabling coherent and transparent vulnerability assessment across both domains.

2. Background

Physical security has historically focused on preventing unauthorized access through spatially bound protective measures (Perdikaris, 2014). From early fortifications such as castles to modern building protection systems, security effectiveness has been determined by the ability of barriers – walls, fences, gates, doors, or locks – to delay an attacker long enough for detection and intervention to occur (Baker and Benny, 2016). The resistance of these measures, and thus the time required to overcome them, is primarily defined by their physical properties, such as height, thickness, or material strength, and by assumptions about the attacker's tools and capabilities (Crowe and Fennelly, 2013). Consequently, attack paths in the physical domain are largely dictated by the topology of the protected infrastructure and the configuration of its protection system (Garcia, 2008).

Approaches such as the Adversary Sequence Diagram (ASD) and the Estimate of Adversary Sequence Interruption (EASI) method represent attacks as ordered sequences of barrier crossings, each associated with a probability of detection and a characteristic delay (Sandia National Laboratories, 1989; Bennett, 1977), and are still incorporated in current approaches (e.g. Čakija et al., 2020; Lichte et al., 2021; Zou et al., 2021). Physical vulnerability is therefore not a static property of individual measures, but an emergent result of the temporal interaction between protection, observation, and response along an attack path, i.e. combination of barriers in series.

In contrast, cybersecurity has evolved under different conditions. Although cyber systems also employ barriers, such as authentication mechanisms or network segmentation, attacker movement is not strictly bound to physical space (Mallick and Nath, 2024). Attack paths may traverse logical layers, software components, and trust boundaries in ways that are less constrained by system topology and more difficult to predict (Ocaka et al., 2022). Architectural models like the Purdue reference model and attacker-centered knowledge bases like MITRE ATT&CK can structure topology and adversarial behavior and possible attack sequences across technical layers (Al-Sada et al., 2024).

As a result, cybersecurity risk assessment has shifted its focus toward the identification, characterization, and mitigation of exploitable vulnerabilities (Hu et al., 2021). This perspective is reflected in widely used cybersecurity frameworks. For instance, the Common Vulnerability Scoring System (CVSS) provides standardized semiquantitative metrics that describe vulnerabilities in terms of attack context, required capabilities, and potential impact (Aggarwal, 2023). Total scores are calculated from these metrics.

Nevertheless, there are quantitative, time based concepts such as time-to-compromise (Jonsson and Olovsson, 1997; McQueen et al., 2006; Leversage and Byres, 2008) or time-to-respond (Zewail et al., 2025). The concept can be be formulated either as an observable variable (Jonsson and Olovsson, 1997; Zewail et al., 2025) or as a relative indicator (McQueen et al., 2006; Leversage and Byres, 2008). In the latter case, these indicators may be derived from other scales, such as CVSS (Rencelj Ling and Ekstedt, 2023). While these approaches enable systematic threat modeling and vulnerability prioritization, the explicit quantification of temporal aspects – such as time to overcome barriers, detection latency, or response effectiveness – remains challenging. Cybersecurity assessments therefore tend to rely on severity scores or qualitative likelihood estimates rather than on interruption-based metrics

comparable to those used in physical security.

As systems increasingly integrate physical and cyber components, these methodological differences become problematic (Lee, 2020). Hybrid systems give rise to attack scenarios that span multiple system layers, allowing adversaries to exploit whichever path offers the least resistance at a given stage (Sweijs et al., 2021).

However, a common modeling perspective and aligned metrics are difficult to find. This gap makes it difficult to compare physical and cyber risks or to justify balanced security decisions across domains. Although initial efforts exist to link cyber threats to physical consequences or to extend attack modeling to cyber-physical systems (e.g. Prasat et al., 2022), a harmonized framework for comparable cross-domain risk assessment is still missing. This need motivates the approach presented in this paper.

3. Approach

This paper presents an analogy-driven approach to establish a quantitative basis for prioritizing security risks across physical and cyber domains. This work consciously excludes threat probabilities due to the epistemic uncertainty inherent in malicious adversary behavior, and instead focuses on models and metrics for vulnerability. The key contribution lies in aligning selected models and metrics from both domains by applying a uniform terminology and structure representation that is consistent across both domains. The aim is to enable scenario-based prioritization and the systematic mapping of attack scenarios to vulnerabilities across both domains.

In contrast to widely used metrics, in particular CVSS that combines ordinal scales through arithmetic operations and produces scores that are neither ratio-scaled nor normalized to a common cross-domain metric, we propose to describe physical and cyber attacks as structurally and functionally similar adversary sequences based on MITRE ATT&CK, ASD, and EASI to enable joint vulnerability prioritization despite domain-specific security measures.

The following description of the approach is structured as follows: first, important assumptions are made that define the conditions for the cross-domain analogy under consideration. Second, the aforementioned physical and cybersecurity models are decomposed into their model elements of intrusion paths, protection functions, and metrics. A comparison highlights structural analogies between the domains. Third, based on these analogies, we synthesize an aligned representation of cybersecurity metrics, that is conceptually equivalent to quantitative physical security metrics, and demonstrate the resulting alignment using a notional example, that illustrates how the proposed approach enables quantitative comparison and prioritization of risks across physical and cybersecurity.

3.1. *Assumptions*

We base the approach on the following assumptions:

(i) *Adversarial intent is the same:* Physical and cyber attacks are assumed to be goal-oriented processes in which an adversary seeks to reach a defined asset by progressing through a sequence of actions.

(ii) *Attack paths are structurally similar:* Attack scenarios in both domains can be abstracted into a common structure consisting of an attack surface, a target asset, intermediate barriers, and a number of possible adversary actions.

(iii) *The barrier concept is domain-independent:* Barriers and their functions are assumed to be conceptually comparable across domains, even though their technical realization differs.

(iv) *Vulnerability is defined by scenarios:* Vulnerability is considered a property of a scenario, determined by the interplay of attacker capabilities, infrastructure topology, protected assets, and the effectiveness of implemented security measures.

3.2. *Intrusion paths*

3.2.1. *MITRE ATT&CK*

To ensure a consistent view on intrusion paths, the concept of adversary sequences needs to be converged for both cybersecurity and physical security. We suggest MITRE ATT&CK as a basis,

since it offers a structured knowledge base of adversarial techniques, categorized to tactics relevant for cybersecurity. For physical security, we propose to represent movement and access to physical areas as tactics. Table 1 lists identified analogies.

Table 1. Analogies based on ATT&CK.

Element	Representation	
	Cyber	Physical
Tactic	One of several types of adversary actions to proceed with an attack (e.g., initial access, privilege escalation, lateral movement, execution)	Movement and access to physical areas (e.g., entering the site, moving inside, accessing restricted areas)
Initial access	First access to a system or network	Physical access to a site or building
Lateral movement	Movement between systems within a network	Movement between physical areas
Technique	Method used to achieve a tactic (e.g., spearphishing attachment for initial access, exploitation for privilege escalation)	Method of gaining physical access (e.g., break through, dig under, climb over)

3.2.2. *Adversary Sequence Diagram (ASD)*

In physical security, an ASD provides a model of system topology and intrusion paths by describing the connection of physical areas separated by protective elements. We propose to extend this concept to the separation of IT interfaces and outline the relevant analogies in Table 2. We suggest to combine the separation of IT interfaces with ATT&CK tactics to describe intrusion paths systematically based on the structure of the IT system in an ASD.

Table 2. Analogies based on ASD.

Element	Representation	
	Physical	Cyber
Zone	Area without spatial access restrictions (e.g., outdoor area, hallway, room)	Area without access restrictions on IT interfaces (e.g., privilege ring, network segment)
Barrier	Physical obstacle that hinders movement between zones (e.g., fences, walls, doors)	Separation of IT interfaces that restricts access (e.g., firewalls, user roles, ACL)

3.3. *Protection functions and metrics based on Estimate of Adversary Sequence Interruption (EASI)*

In physical security, EASI describes the effectiveness of security measures along an intrusion path by the probability of detection P_{D} and a time game of delay time t_{D} and response time t_{R} in which both types of times are represented by random variables with assumed probability distributions. EASI utilizes the ASD by considering a detection event and a delay at each barrier. For the remaining path, the delay times add up to a residual delay time t_{RD}. For a path with n barriers, the probability of interruption P_{I} is calculated by Eq. (1) and Eq. (2):

$$P_{\mathrm{I}} = P_{\mathrm{D},1} \cdot P(t_{\mathrm{R}} < t_{\mathrm{RD},1}) + \sum_{i=1}^{n} (P_{\mathrm{D},i} \cdot P(t_{\mathrm{R}} < t_{\mathrm{RD},i})) \cdot \prod_{j=1}^{i-1} (1 - P_{\mathrm{D},j}) \tag{1}$$

$$t_{\mathrm{RD},i} = \sum_{j=i}^{n} t_{\mathrm{D},j} \tag{2}$$

We propose to apply this concept of events and times to cybersecurity as well, since time-based metrics provides objective and transparent model behavior, separating metric validity from parameter uncertainty. This separation is essential for cross-domain comparability. Table 3 points out analogies of detection, delay and response in physical security and cybersecurity.

Table 3. Analogies based on EASI.

Element	Representation	
	Physical	Cyber
Detection	Event of detecting the overcoming of barriers or unauthorized movements in zones through surveillance and alarms (e.g., via video cameras, alarm systems)	Event of detecting malicious activity (e.g., intrusion, misuse, exploitation via logging, SIEM, IDS/IPS)
Delay	Time required for an intruder to penetrate or bypass a physical barrier (e.g., breakthrough, open, climb over)	Time required for an attacker to compromise, corrupt, or progress through a cyber barrier (e.g., exploit execution, lateral movement)
Response	Time required for security personnel to react after detection (e.g., via security staff, lockdown, evacuation)	Time required for technical or organizational response after detection (e.g., containment, isolation, account suspension, remediation)

4. Illustrative example

In the following, we illustrate the approach using a notional simplified case study of an aligned assessment of physical security and cybersecurity. For this purpose, we consider the protection of an asset that can be sabotaged by a physical or a cyber-attack.

For the physical domain, we consider a simple layout of an operating site that includes two layers of protection: perimeter (fence and gate) and building (door and window). The physical ASD in Fig. 1 shows the corresponding zones and barriers relevant for access escalation. For illustration purpose, we assume $t_{\mathrm{R}} \sim \mathrm{Normal}(600\,\mathrm{s}, 100^2\,\mathrm{s}^2)$ along with the values in Table 4 to describe the parameters according to EASI given different adversarial techniques. It is assumed that the distribution of t_{D} follows a normal distribution here and in the following.

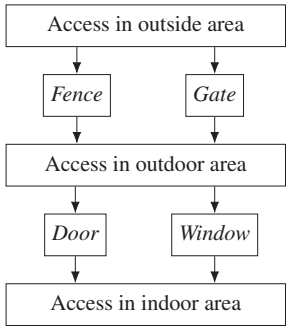

Fig. 1. Physical ASD of illustrative example.

For the cyber domain, we consider an ASD inspired by the Purdue model that describes the progress of intrusion by privilege escalation and lateral movement inside and between enterprise network and ICS network (Jafari et al., 2025). The cyber ASD in Fig. 2 shows exemplary sequences of initial access, privilege escalation, lateral movement, and execution. Table 5 shows an assumed representation of the intrusion steps in EASI. We also assume $t_{\mathrm{R}} \sim \mathrm{Normal}(1200\,\mathrm{s}, 200^2\,\mathrm{s}^2)$.

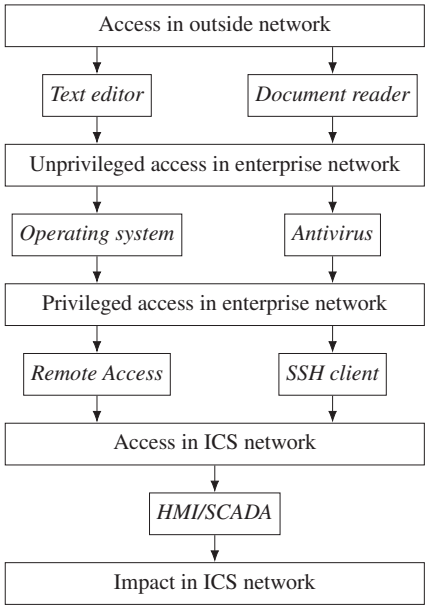

Fig. 2. Cyber ASD of illustrative example.

Table 4. Parameters of physical security model.

Barrier	Technique	P_{D}	t_{D}	
			μ (s)	σ (s)
Fence	Break through	0.95	440	100
	Climb over	0.95	360	160
Gate	Open	0.95	400	120
	Break through	0.95	600	180
Door	Open	0.9	400	120
	Break through	0.8	600	180
Window	Open	0.9	460	138
	Break through	0.95	300	90

Table 5. Parameters of cybersecurity model.

Tactic	Barrier	Technique	P_{D}	t_{D}	
				μ (s)	σ (s)
Initial Access	Text editor	Spearphishing attachment	0.65	420	90
	Document Reader	Spearphishing attachment	0.8	300	60
Privilege Escalation	Operating System	Exploitation for privilege escalation	0.9	240	40
	Antivirus	Exploitation for privilege escalation	0.85	180	30
Lateral Movement	Remote Access	Remote service session hijack	0.75	360	70
	SSH Client	Remote Services: SSH	0.7	400	80
Execution	HMI/SCADA	Exploitation for client execution	0.6	480	100
		DLL search order hijacking	0.55	540	120

Table 6. Some intrusion paths for physical security and cybersecurity, ranked by the aligned metric of effectiveness.

Rank	Domain	P_{I}	Path
1	Physical	0.58	1) Fence: Climb over, 2) Window: Break through
2	Cyber	0.59	1) Document Reader: Spearphishing attachment, 2) Antivirus: Exploitation for privilege escalation, 3) Remote Access: Remote service session hijack, 4) HMI/SCADA: Exploitation for client execution
⋮	⋮	⋮	⋮
9	Cyber	0.67	1) Document Reader: Spearphishing attachment, 2) Operating System: Exploitation for privilege escalation, 3) Remote Access: Remote service session hijack, 4) HMI/SCADA: Exploitation for client execution
10	Physical	0.68	1) Gate: Open, 2) Window: Break through
11	Cyber	0.7	1) Text editor: Spearphishing attachment, 2) Antivirus: Exploitation for privilege escalation, 3) SSH Client: Remote Services: SSH, 4) HMI/SCADA: DLL search order hijacking
⋮	⋮	⋮	⋮
31	Physical	0.94	1) Fence: Break through, 2) Door: Break through
32	Physical	0.96	1) Gate: Break through, 2) Door: Break through

Parameters of both domains are intentionally simplified to isolate the methodological effects of the proposed alignment rather than to represent realistic system configurations.

The notional case study yields a list of paths in both domains, 16 in each domain, where the effectiveness of physical and cybersecurity measures is measured in the aligned metric P_1. By sorting the paths of both domains by P_1, we achieve a ranking that spans both domains. Table 6 illustrates how physical and cyber intrusion paths alternate in this ranking.

5. Discussion

With this contribution, we show that physical security models (ASD, EASI) and cybersecurity models (MITRE ATT&CK) have strong analogies and these can be used to base the assessment of both domains on a unified model of adversary sequences with aligned metrics.

In light of divergent and incomparable metrics for physical security and cybersecurity, this paper provides a transparent, scenario-based approach to align them without claiming unrealistic probabilistic accuracy. However, some limitations must be taken into account:

(i) Empirical data, particularly for time-based parameters, is often limited in both domains. In cybersecurity, detection and time-to-compromise are highly context-dependent, while physical security testing is costly and operationally demanding. As a result, parameter estimation frequently relies on expert judgment, requiring careful alignment of assumptions to maintain comparability.

(ii) Effectiveness of cybersecurity measures may change more rapidly over time than effectiveness of physical security measures. The approach presented therefore treats variations in attacker capabilities or security measures as distinct scenarios rather than modeling adaptive behavior within a single scenario. This abstraction limits applicability in highly dynamic environments and confines results to scenario-specific interpretations for decision-making.

(iii) The analysis is limited to time-based metrics to support comparison and prioritization in cybersecurity and physical security under uncertainty. Therefore, it does not provide encompassing risk values. The validity of the analysis thus depends on transparent assumptions and awareness of the methodological boundaries introduced by such a simplification.

6. Conclusion

The presented approach demonstrates that aligning cybersecurity intrusion models with models and metrics from physical security can enhance cross-domain comparability. Despite inherent limitations related to data availability, dynamic threat evolution, and methodological simplification, the contribution provides a structured basis for consistent interpretation and prioritization of vulnerability under uncertainty. When applied with transparent assumptions and scenario awareness in an integrated security risk assessment, it offers value for balanced decision support, and is a first step towards harmonized risk assessment for physical security and cybersecurity.

References

Aggarwal, M. (2023, September). A study of cvss v4.0: A cve scoring system. In *2023 6th International Conference on Contemporary Computing and Informatics (IC3I)*, pp. 1180–1186. IEEE.

Al-Sada, B., A. Sadighian, and G. Oligeri (2024, October). Mitre att&ck: State of the art and way forward. *ACM Computing Surveys 57*(1), 1–37.

Baker, P. R. and D. J. Benny (2016, April). *The Complete Guide to Physical Security*. Auerbach Publications.

Bakov, K. (2024, June). The new realities in synchronizing physical security and cybersecurity in digital societies.

Bennett, H. A. (1977). EASI (estimate of adversary sequence interruption) - an evaluation method for physical security systems. *Nuclear Materials Management 6*, 371–379.

Brandstatter, C. and D. Brunlechner (2024, May). A cost-benefit model for the evaluation of cyber physical production systems. In *Proceedings of the 2024 10th International Conference on Computer Technology Applications*, ICCTA 2024, pp. 255–263. ACM.

Crowe, T. D. and L. J. Fennelly (2013). *Crime Prevention Through Environmental Design* (Third ed.). Elsevier.

Depoy, J., J. Phelan, P. Sholander, B. Smith, G. B. Varnado, and G. Wyss (2005). Risk assessment for physical and cyber attacks on critical infrastructures. In *IEEE Military Communications Conference*, pp. 1961–1969. IEEE.

Garcia, M. L. (2008). *The Design and Evaluation of Physical Protection Systems* (Second ed.). Burlington: Butterworth-Heinemann.

Hu, W., C.-H. Chang, A. Sengupta, S. Bhunia, R. Kastner, and H. Li (2021, June). An overview of hardware security and trust: Threats, countermeasures, and design tools. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 40*(6), 1010–1038.

Jafari, A., C. Özkan, H. Ergun, D. Van Hertem, and D. Singelee (2025, September). An advanced cybersecurity risk assessment framework: Integrating vulnerabilities and exploitation techniques for systematic attack path analysis in multilayered power system networks. *Sustainable Energy, Grids and Networks 43*, 101876.

Jiang, Y., Q. Meng, F. Shang, N. Oo, L. T. H. Minh, H. W. Lim, and B. Sikdar (2025, February). Mitre att&ck applications in cybersecurity and the way forward.

Jonsson, E. and T. Olovsson (1997, April). A quantitative model of the security intrusion process based on attacker behavior. *IEEE Transactions on Software Engineering 23*(4), 235–245.

Lee, S. (2020). A basic principle of physical security and its link to cybersecurity. *International Journal of Cyber Criminology 14*(1), 203–219.

Leversage, D. J. and E. J. Byres (2008, January). Estimating a system's mean time-to-compromise. *IEEE Security & Privacy 6*(1), 52–60.

Lichte, D., D. Witte, T. Termin, and K.-D. Wolf (2021, December). Representing uncertainty in physical security risk assessment. *European Journal for Security Research 6*(2), 189–209.

Mallick, M. A. I. and R. Nath (2024). Navigating the cyber security landscape: A comprehensive review of cyber-attacks, emerging trends, and recent developments. *World Scientific News 190*(1), 1–69.

Mccreight, T. and D. Leece (2016, September). Physical security and it convergence: Managing the cyber-related risks. *Journal of Business Continuity & Emergency Planning 10*(1), 18.

McQueen, M. A., W. F. Boyer, M. A. Flynn, and G. A. Beitel (2006). Time-to-compromise model for cyber risk reduction estimation. In D. Gollmann, F. Massacci, and A. Yautsiukhin (Eds.), *Quality of Protection*, Advances in Information Security, pp. 49–64. Springer.

Ocaka, A., D. O. Briain, S. Davy, and K. Barrett (2022, April). Cybersecurity threats, vulnerabilities, mitigation measures in industrial control and automation systems: A technical review. In *2022 Cyber Research Conference - Ireland (Cyber-RCI)*, pp. 1–8. IEEE.

Perdikaris, J. (2014, April). *Physical Security and Environmental Protection*. CRC Press.

Prasat, K., S. Sanjay, V. Ananya, R. Kannadasan, S. Rajkumar, R. Raut, and R. Selvanambi (2022, July). Analysis of cross-domain security and privacy aspects of cyber-physical systems. *International Journal of Wireless Information Networks 29*(4), 454–479.

Rencelj Ling, E. and M. Ekstedt (2023, April). Estimating time-to-compromise for industrial control system attack techniques through vulnerability data. *SN Computer Science 4*(3).

Sandia National Laboratories (1989, December). SAVI: Systematic analysis of vulnerability to intrusion. Technical Report SAND89-0926/1, United States.

Sinha, A., T. H. Nguyen, D. Kar, M. Brown, M. Tambe, and A. X. Jiang (2015, November). From physical security to cybersecurity. *Journal of Cybersecurity 1*(1), 19–35.

Sweijs, T., S. Zilincik, F. Bekkers, and R. Meessen (2021). *A framework for cross-domain strategies against hybrid threats. Den Haag, NL: Hague Centre for Strategic Studies*. Hague Centre for Strategic Studies.

Čakija, D., v. Ban, M. Golub, and D. Čakija (2020). Optimizing physical protection system using domain experienced exploration method. *Automatika 61*(2), 207–218.

Yu, Z., H. Gao, X. Cong, N. Wu, and H. H. Song (2023, December). A survey on cyber–physical systems security. *IEEE Internet of Things Journal 10*(24), 21670–21686.

Zewail, A., Y. Abdulghany, and M. Samy (2025, July). Reducing mean time to respond using large language model-driven incident response with the aid of reactively retrieved threat intelligence. In *2025 Intelligent Methods, Systems, and Applications (IMSA)*, pp. 322–327. IEEE.

Zou, B., M. Li, and M. Yang (2021, April). Vulnerability learning of adversary paths in physical protection systems using AMC/EASI. *Progress in Nuclear Energy 134*, 103666.