INTERNATIONAL JOURNAL OF PUBLIC ADMINISTRATION,
MANAGEMENT AND ECONOMIC DEVELOPMENT

Risk Convergence in Critical Infrastructure Governance in the European Union: A Qualitative Framework for Integrated Multi Domain Risk Oversight

Dr. Vladimir Bunic

Converged Security Institute (CSI), Barcelona, Spain, E-mail: vladimir.bunic@convergedsecurity.es, ORCID: 0009-0006-6209-629X

Abstract

The critical infrastructure sectors of the European Union (EU) face growing cross-functional cyber, physical, operational, and human-factor threats. With the increased pace of digitalisation, the effects of such risks spread across organisations, creating systemic vulnerabilities that challenge conventional governance models. This paper analyses the causes and effects of risk convergence and proposes an organised governance model to support integrated multi-domain control. The study adopts a qualitative conceptual methodology based on academic literature, EU regulatory frameworks, industry reports, and documented incidents. Thematic analysis was used to identify recurring themes of risk convergence, supported by cross-document comparison. Regulatory triangulation ensured alignment with NIS2, CER, GDPR, DORA, and the Cyber Resilience Act. Five patterns of risk convergence were identified: cyber-physical interdependencies, operational-cyber propagation, human-factor amplification, regulatory-risk misalignment, and organisational fragmentation. These patterns reveal governance vulnerabilities that undermine resilience and complicate compliance. The paper proposes a hybrid governance system comprising structural, operational, and assurance layers. This study presents one of the earliest governances-focused models tailored to converged risk environments in EU critical infrastructure. It incorporates recent academic insights (2022–2024), sector-specific examples, and regulatory expectations, offering practical guidance for policymakers and operators seeking to enhance resilience in complex socio-technical systems.

Keywords: risk convergence; critical infrastructure; cyber physical systems; EU governance; organisational resilience

JEL classification: H12; H56; L94; O33; K23

1. Introduction

There is growing interconnected socio technical environments in the critical infrastructure sectors of the European Union (EU), such as energy, healthcare, transportation, water, and telecommunications. The digital transformation, automation, and IT OT integration have significantly removed the distinction between the sphere of cyber, physical, operational and human factor. Consequently, risks do not happen in a

vacuum and spread across systems, causing cascading effect and putting pressure on traditional systems of governance (Cherdantseva et al., 2016; Alderson and Doyle, 2023).

This convergence has been experienced in recent incidences.

- Physical interference of grid functions in the energy industry has occurred due to cyberattacks of SCADA systems (ENISA, 2024).
- Criminal activities related to ransomware have led to a stagnation of the clinical flow in the health sector, impacting patient safety and the flow of operations (Wang and Patel, 2022).
- GPS spoofing and sensor manipulation in the transport sector has caused interruptions in the navigation and signal systems (Khan and McLaughlin, 2023).
- Cyber intrusions in the water sector have distorted the chemical dose systems posing physical and population health risks (OECD, 2023).

In spite of these facts, a lot of organisations still handle risks in siloed architecture and have isolated teams in cybersecurity, physical security, operational risk, and safety (Boin, A. and Lodge, M. 2016). This disaggregation inhibits situational knowledge, slows down the process of responding to incidents, and resilience.

European regulation also makes government difficult. Converged risk reality is typically not necessarily in line with domain specific obligations stipulated in directives like NIS2, CER, GDPR, DORA, and the Cyber Resilience Act (European Parliament and Council, 2022; 2023). Organisations are thus faced with conflicting needs and are forced to deal with more hybrid threats.

This paper looks at the corporative aspect of the problem of convergence of risk and suggests an integrated multi domain regulation model.

1.1 Background of the Study

There is an increase in the interdependence of digital, physical, operational, and human factor system, which is manifested by risk convergence. Even a single incident like a cyber-attack, a technical issue, or an insider mistake can cause a subsequent crash in several spheres (Kott and Linkov, 2021). For example:

- Disruption of a pipeline work control via a cyberattack can lead to physical destruction and closure.

- Cyber intrusions into core networks may occur through a physical attack on a telecommunications hub.

- Hospital IT systems may suffer a human factor error that will interfere with digital and clinical operations.

Nevertheless, governance systems have not been properly integrated in spite of these interdependencies. There are various taxonomies, evaluation approaches, and reporting lines that risk functions tend to apply (Mazieri, Conti and De Gaspari, 2022). This disconnection restricts the capacity of the organisation to predict, evaluate and address converged risks.

1.2 Research Objectives

This study aims to:

1. Examine risk convergence in terms of nature and drivers in the sectors of critical infrastructure in the EU.
2. Determine governance issues with multi domain dependencies.
3. Establish a qualitative model of combined risk management.
4. Present workable suggestions that concern the strengthening of organisational resilience.

1.3 Significance of the Study

One aspect of cyber physical resilience that is under-researched is the aspect of risk convergence. Current studies tend to view cybersecurity, physical security, and operational risk, and human factor risk as discontinuities. There are minimal studies that observe the interaction between these risks and what governance structures are needed to handle them in an integrated manner (Alderson and Doyle, 2023; Khan and McLaughlin, 2023). This study contributes by:

- combining multi domain risk insight to single governance viewpoint.
- fitting the risk convergence analysis to EU expectations of regulation
- suggesting a hierarchical system of combined supervision.
- including the latest specific examples in the sector (2022-2024)

The results have practical implications to policymakers, risk managers, and operators to reinforce resilience in systems with integrated environments.

1.4 Research Questions

The study addresses the following research questions:

1. How do cyber, physical, operational, and human-factor risks converge in EU critical infrastructure sectors?
2. What governance issues arise from multi-domain risk interdependencies?
3. Which mechanisms can support integrated risk oversight?
4. How can a hybrid governance structure improve organisational resilience?

2. Literature Review

Risk convergence is an intersecting multidimensional phenomenon that touches on cybersecurity, physical security, organisational governance, resilience studies, and critical infrastructure protection. The literature shows that converged risks are the product of the synergy of technological, organisational and human factor factors and need combined ways of governance, which goes beyond the conventional security boundaries (Alderson and Doyle, 2023; Mazieri, Conti and De Gaspari, 2022). This part will be a synthesis of theoretical background as well as empirical evidence that can be added to the topic of multi domain risk governance in EU critical infrastructure sectors.

2.1 Theoretical Foundations

Risk convergence is being studied in terms of several theoretical perspectives.

Cyber-Physical Systems (CPS) Theory

The CPS theory focuses on bringing together both computational and physical processes, generating interdependence that increases hazards spread (Lin, Zhao and Chen, 2024). CPS architectures are interconnected in critical infrastructure, between IT networks, OT systems, sensors, and actuators and physical processes, becoming susceptible to hybrid attacks.

Socio-Technical Systems Theory

Socio technical theory is focused on the interactions between human, organisational, and technological elements (Smith and Brooks, 2013). Convergence on risk is created by socio technicality whereby the vulnerability is not always caused by technical aspects alone but also through human behaviour, organisational structure and process design.

Organisational Risk Governance Theory

Risk governance systems are characterised by accountability, transparency and integrated decision making (Briggs, Brooks and Nelson, 2020). The converged risks do not lend themselves to the governance model whereby they necessitate convergence of overarching forms of oversight that aid in integrating risk ownership, reporting and decision making across domains.

Resilience Theory

The theory of resilience dwells on adaptability, learning, and shock absorption ability (Duchek, 2020). Converged risk management needs to have dynamic governance systems that are able to react to the changing threat and promote continuous improvement.

2.2 Risk Convergence in Critical Infrastructure

Recent literature reveals that there are a number of risk convergence drivers in critical infrastructure sectors. These include:

- IT OT integration
- IoT proliferation
- Cloud dependency
- Robotisation and remote operations
- Vulnerabilities of the human factor.

The systemic vulnerabilities are formed by cyber physical interdependencies. when failures in one domain will spread into others (Cherdantseva et al., 2016). This can be best exemplified in sector specific situations:

- Power: SCADA systems have been attacked, leading to physical disruption of the grid (ENISA, 2024).
- Healthcare: Ransomware has interrupted clinical processes and put patients at risk (Wang and Patel, 2022).
- Transportation: GPS spoofing has interfered with the navigation and signalling systems (Khan and McLaughlin, 2023).
- Water: Cyber-attacks have modified chemical dosing mechanisms, posing health risks to the population (OECD, 2023).

These illustrations demonstrate that there is a necessity of converged risk management practices that embody converged risk realities.

2.3 Governance Challenges in Multi Domain Risk Environments

According to the literature, a number of governance problems are related to risk convergence:

- Discrete departmental risk ownership.
- Unequal risk evaluation procedures.
- Isolated incident response practices.
- Regulatory misalignment
- Denied cross domain situational awareness.

EU regulatory structures present domain specific requirements which are not always in line with converged risk realities (European Parliament and Council, 2022; 2023). For example:

- NIS2 pays attention to cybersecurity.
- CER focuses on operational and physical strength.
- GDPR deals with protection of data.
- DORA aims at digital operational resiliency.
- CRA pays attention to the security of products.

This fragmentation gives rise to compliance lapses and irregular governance.

2.4 Gaps in Existing Research

Although there is increasing awareness of risk convergence, there are still a number of gaps:

- There are not many converged risk models of governance in the critical infrastructure of the EU.
- Current frameworks have a tendency to concentrate on the separate risk areas instead of their connections.
- Few studies have associated risk convergence with organisational resilience.
- Very little research offers effective governance frameworks to the multidomestic governance.

This research paper fills these gaps by coming up with a hybrid system of governance that incorporates structural, operational, and assurance systems

3. Methodology

The current study will utilize qualitative conceptual approach to explore the implications of risk convergence on governance of critical infrastructure in EU. A qualitative methodology is suitable since converged risks are created through the social technical interaction, complexity in regulation, and organisational dynamism that is not completely measured using quantitative indicators.

3.1 Research Design

The study adheres to a three-stage conceptual design:

1. Academic literature review and EU regulatory materials and industry reports.
2. Thematic analysis to categorize issues of risk in the domains of cyber, physical, operational and human factors.
3. Synthesis of framework using descriptive information along with prescriptive recommendations.

3.2 Data Collection

There were four types of publicly available sources, which provided the data:

- Academic literature (2015-2024)
- EU laws (NIS2, CER, GDPR, DORA, CRA)
- Report in industry (ENISA, ISACA, OECD).
- Reported cases in the areas of energy, health, transportation, and water.

The sources were a wide evidence base to establish the interactions of multi domain risks.

3.3 Data Analysis

Risk convergence patterns were identified through thematic analysis, in order to obtain recurrent patterns. Coding categories included:

- cyber physical interdependencies
- operational cyber propagation.
- vulnerabilities of the human factor.
- regulatory misalignment
- organisational fragmentation

Cross document validation In cross document validation, the themes were checked against a regulating triangulation of documents.

3.4 Validation and Reliability

To improve the rigor of the methodology, the research used:

- analyst triangulation
- regulatory triangulation
- iterative code refinement

To make the findings consistent, they were compared between various sources.

3.5 Ethical Considerations

The paper will be based solely on secondary sources of data. No human subject was used, and no secret and sensitive operation information was consulted.

4. Findings and Discussion

The thematic analysis determined that there are five broad themes of converged risks across the fields of EU critical infrastructure. These trends demonstrate the interaction and domain propagation of cyber, physical, operational, and human factor risks.

4.1 Presentation of Findings

Five thematic areas emerged:

1. Cyber physical interdependencies
2. Operational cyber propagation
3. Human factor amplification

4. Regulatory risk misalignment
5. Organisational fragmentation

Table 1: Patterns of Risk Convergence in EU Critical Infrastructure

Risk Convergence Area	Key Drivers	Implications for Critical Infrastructure
Cyber Physical Interdependencies	IT OT integration; IoT proliferation; SCADA connectivity; cloud linked control systems	Cascading failures across digital and physical domains; systemic vulnerabilities; hybrid attack pathways
Operational Cyber Propagation	Automation; remote operations; digitalised industrial processes; sensor dependencies	Operational disruptions triggering cyber exposure; cyber incidents halting physical processes; amplified downtime
Human Factor Amplification	Misconfigurations; insider threats; procedural errors; inadequate training	Multi domain vulnerabilities; error propagation across systems; compromised safety and continuity
Regulatory Risk Misalignment	Domain specific EU directives (NIS2, CER, GDPR, DORA, CRA); inconsistent compliance expectations	Governance gaps; fragmented controls; conflicting reporting requirements; compliance inefficiencies

Source: Author

4.2 Cyber Physical Interdependencies

The most crucial source of risk convergence came as cyber physical interdependencies. Examples include:

- Physical grid instability resulting in manipulation of the SCADA (ENISA, 2024).
- IoT usage that allows hybrid cyber physical attacks.
- Hardware attack to permitting cyber penetration of main systems.

These dependencies need combined control systems.

4.3 Operational Cyber Risk Propagation

Digital systems are becoming involved in the operational processes. As a result:

- cyber vulnerabilities can be instigated by operational failures.

- cyber-attacks have the potential to interfere with operational continuity.
- automation has the potential to expand cross domain effects.

This brings out the necessity of integrated risk assessment methodologies

4.4 Human Factor Amplification

There are human factors vulnerabilities that enhance converged risks:

- omissions that lead to OT network exposures.
- the rapid spread of effects across digital and physical systems.
- clinical or industrial issues of procedural error.

The human factor governance should be incorporated in risk oversight.

4.5 Regulatory Risk Misalignment

EU directives contain domain specific requirements that are not necessarily in line with converged risk reality. This brings compliance rifts and irregular governance practices.

4.6 Organisational Fragmentation

Separated risk functions lead to:

- inconsistent taxonomies
- weak situational awareness.
- delayed incident response
- conflicting priorities

There is need to have integrated structure of governance to provide coordination of risk management across area.

5. Hybrid Framework for Integrated Risk Governance

The hybrid framework created in the present research will combine descriptive data gathered through risk convergence analysis and prescriptive suggestions on the merit of enhancing multi domain risk management in the EU critical infrastructure sectors. The framework comprises three dependent layers, namely, structural, operational and assurance, and which discuss particular governance issues that were revealed during the findings. This stratified system of governance was in line with the modern models of governance that focus on coherence, accountability, and adaptive capacity (Briggs, Brooks and Nelson, 2020; OECD, 2023).

5.1 Structural Risk Governance Layer

The structural layer is concerned with the organisational design, ownership of risk as well as cross domain accountability. Disjointed risk functions-cybersecurity, physical security, operational risk and safety-may not be fully integrated and this leads to inconsistent risk reporting, situational awareness and lack of alignment of priorities Boin, A. and Lodge, M. 2016). The further issue on governance is regulatory fragmentation across NIS2, CER, GDPR, DORA, and the Cyber Resilience Act.

In order to manage these issues, the structural layer suggests:

- Risk Governance Council of cyber, physical, operational and human factor risks.
- Cross Domain Risk Ownership Model with the assistance of a single risk taxonomy.
- Harmonised Regulatory Interpretation Function so that there is conformity in compliance in multiple fields.
- Determined Governance Policies clearly dealing with cross domain dependencies.

Through these mechanisms, organisational alignment is enhanced and coherent decision making within converged environments facilitated.

5.2 Operational Risk Governance Layer

The operational layer deals with processes and controls as well as incident response mechanisms. The results reported gaps in the reporting of cyber, physical, and operational risks, such as those in incomplete methodologies, poor monitoring instrumentation, and isolation of incident response operations (Khan and McLaughlin, 2023).

In order to solve these problems, the operational layer suggests the following:

- Converged Risk Assessment Methodology that includes cyber, physical, operational and human factor risks.
- Web based Threat Intelligence Infrastructure that allows cross domain analysis.
- Cross Domain Incident Response Teams are operating on similar protocols.
- IT OT Integration Roadmap that places more importance on interoperability and standardised controls.

The measures increase operational coherence and increase the organisational capacity to deal with converged risks.

5.3 Assurance Risk Governance Layer

The assurance layer aims at the audits, metrics and continuous improvement. The process of auditing activities may be siloed where cybersecurity, physical security, and operational audits are performed separately. This precludes the effectiveness of cross domain control evaluation in the organisation (Alderson and Doyle, 2023).

As an assurance enhancement, the framework hypothesizes:

- Cross domain control measuring performance based on Converged Audit Framework.
- Integrated KPIs and Dashboards on risks.
- Cross Domain Maturity Model analysing the organisational capability.
- Continuous Improvement Cycle including the lessons learned in the incident, audits, and regulation changes.

Combined, the mechanisms contribute to a more robust and flexible model of governance.

6. Limitations and Future Research

The paper is theoretical and it is based on the secondary data sources such as academic sources, regulations, and market reports. Although this method offers overall understanding of risk convergence, it lacks the organisation peculiarities or operational real time data. The ever-changing regulatory environment in the EU can also pose new challenges of governance which have not been fully captured by the analysis.

Empirical case studies should be studied in the future to prove and improve the suggested framework. The application of sector specific studies: especially in energy, healthcare, transportation, and water would give a more in-depth understanding of the peculiar patterns of risk convergence encountered by various critical infrastructure sectors. The field of being an established part of integrated risk governance could also be investigated through the role of the technologies emerging, including AI driven analytics, digital twins, and predictive modelling.

7. Conclusion

Risk convergence is the emergence of a paradigm shift in the area of security of the EU critical infrastructure segments. There is an increased dependency between cyber, physical, operational and human factor risks, and therefore, old siloed governance models can no longer operate. The results of this paper indicate that cyber physical interdependencies, operational cyber propagation, amplification by the human factors, regulatory risk misalignment, and organisational fragmentation prevail to weaken the success of risk governance.

A hybrid governance model that has been presented in this paper offers a systematic solution to these issues where structural, operational as well as assurance mechanisms are combined to tackle these problems. Incorporation of the organisational alignment, solution of operational processes, and heightening of assurance procedures allow critical infrastructure enterprises to shift to a more consistent and robust risk governance framework. This is especially true in the context of EU where regulatory complexity and industry dependencies require single approaches to multi domain risk management.

After all, converged risks cannot be ruled without technical integration as well as organisational coordination in effective governance, a regulative clarity and the continuing improvement pledge. The demand of integrated risk governance will expand as the critical infrastructure environments become more and more connected. The framework in this article provides a frontier to the scholarly study and practical use to enhance more adaptive and robust risk management frameworks throughout the EU.

References

- Alderson, D. and Doyle, J. (2023) 'Systemic risk in cyber physical infrastructure networks', Risk Analysis, 43(7), pp. 1298–1314.
- Boin, A. and Lodge, M. (2016) 'Designing resilient institutions', Public Administration Review, 76(2), pp. 292–302.
- Briggs, R., Brooks, D. and Nelson, J. (2020) 'Security governance in critical infrastructure', International Journal of Critical Infrastructure Protection, 29, p. 100–112.
- Cherdantseva, Y. et al. (2016) 'A review of cybersecurity risk assessment methods for SCADA systems', Computers & Security, 56, pp. 1–27.
- Duchek, S. (2020) 'Organizational resilience: A capability based conceptualization', Business Research, 13, pp. 215–246.
- ENISA (2024) Threat Landscape for Critical Infrastructure 2024.
- European Parliament and Council (2022) Directive (EU) 2022/2555 (NIS2).
- European Parliament and Council (2022) Directive (EU) 2022/2557 (CER).
- European Parliament and Council (2022) Regulation (EU) 2022/2554 (DORA).
- European Parliament and Council (2023) Cyber Resilience Act (CRA).

- Khan, R. and McLaughlin, K. (2023) 'Integrated governance for cyber physical resilience in critical infrastructure', International Journal of Critical Infrastructure Protection, 42, p. 100–125.
- Kott, A. and Linkov, I. (2021) Cyber physical security: Protecting critical infrastructure. Springer.
- Lin, Y., Zhao, H. and Chen, X. (2024) 'Governance challenges in cyber physical systems', Journal of Cybersecurity Studies, 12(1), pp. 44–59.
- Mazieri, M., Conti, M. and De Gaspari, F. (2022) 'Converged security governance in the EU', European Security Journal, 31(4), pp. 512–530.
- OECD (2023) Good Governance for Critical Infrastructure Resilience.
- Smith, R. and Brooks, D. (2013) Security science: The theory and practice of security. Butterworth Heinemann.
- Wang, L. and Patel, S. (2022) 'Human factor vulnerabilities in cyber physical systems', Computers & Security, 120, p. 102–118.