International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(RESEARCH ARTICLE)

Check for updates

A UNIFIED CYBER-PHYSICAL INCIDENT RESPONSE AND BUSINESS CONTINUITY ARCHITECTURE FOR MANAGING HYBRID, SYSTEMIC, AND CASCADING RISKS ACROSS IT, OT, AND PHYSICAL SECURITY DOMAINS

Vladimir Bunic *

Converged Security Institute (CSI), Barcelona, Spain.
* Corresponding Author

ORCID Details
Vladimir Bunic: https://orcid.org/0009-0006-6209-629X

International Journal of Science and Research Archive, 2026, 20(03), 032–043

Publication history: Received on 17 July 2026; revised on 30 August 2026; accepted on 02 September 2026

Article DOI: https://doi.org/10.30574/ijsra.2026.20.3.1674

Copyright © 2026 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution License 4.0

ABSTRACT

Cyber-physical ecosystems now operate as hyper converged environments in which information technology (IT), operational technology (OT), and physical security systems interact continuously. But this convergence has increased the scale of the risk and impact of hybrid attack, system failures, and cascading risk effects that spread across domains. The way traditional Incident Response and Business Continuity (IRBC) methods work is still somewhat siloed, as they don't contribute to the cross-domain risk management and improve resilience in converged environments. But there are gaps that need to be filled, and this study suggests a single architecture for Incident Response and Business Continuity (IRBC) that unifies cross-domain response policies, applies the Zero Trust approach, implements AI empowering analytics, and integrates recovery plans across cyber-physical systems.

The research utilizes a conceptual methodology which involves mapping the standards, building cross domain dependency models and using the synthesis of architectures. Cyber–physical resilience requirements were extracted from various existing international standards (ISO/IEC 27001:2022, ISO 22301:2019, ISO 31000:2018, NIST SP 800-61, NIST SP 800-34, NFPA 1600, etc. and other European standards. A dependency modelling diagram shows how hybrid, systemic, and cascading risks move across IT, OT, and physical domains, highlighting the need for IT, OT, and physical space collaboration and co-ordinated operational processes across physical and IT systems.

The proposed IRBC architecture will help improve organisational resilience by consolidating incident response and continuity functions, share a common situational awareness based on integrated monitoring, limit lateral movement through the enforcement of Zero Trust and enrich recovery goals across the different domains. The framework is relevant to today's critical infrastructure operators, financial institutions, manufacturing settings and public sector organisations looking to build a more cyber-physical resilient organisation and reduce risk of cascading failure in converged environments.

Keywords: Incident Response; Business Continuity; Cyber-Physical Security; Hybrid Risks; IT/OT Convergence; Zero Trust

1 INTRODUCTION

The convergence of digital and physical infrastructures has fundamentally reshaped organisational risk landscapes. Smaller businesses work under tightly coupled cyber-physical systems (CPS), in which information technology (IT), operational technology (OT) and physical security platforms are constantly and rapidly interacting with each other [1,2]. This integration has introduced a new class of threats that go beyond security concept definitions such as "cyber" or "physical" threats, "national security" threats, "operational" threats, and operational support. This integration has given rise to new classes of threats that go beyond cyber and physical threats, national security threats, operational threats, and operational support threats, such as hybrid threats that combine cyber and physical vulnerabilities, systemic failures resulting from inter-dependent cyber and physical subsystems, and cascading disruptions that can stem from an initial event and spread across multiple domains [1,3].

Silo mentality for security/continuity can no longer be ignored in the academic world. Studies on CPS security highlight the importance of a coordinated response and integrated governance across the IT, OT and physical boundaries of the system [1,2]. Research on critical infrastructure and industrial control systems reveal common vulnerabilities, interdependency across domains and failure paths that exacerbate risk in operation of critical infrastructure [3,4]. Similarly, business continuity research emphasises the need for synchronisation of recovery methods and resilience across the domains in highly interconnected environments [5].

These observations are supported by international standards. The ISO/IEC 27001:2022 delivers governance foundations for information security management system (ISMS) and ISO 22301:2019 lays out requirements for business continuity management system (BCMS). The enterprise risk management principles in ISO 31000:2018 are applicable to the cyber-physical domains. Detailed advice for incident handling and contingency planning in IT environments can be found in NIST SP 800-61 and NIST SP 800-34 [9,10] while comprehensive requirements for emergency and crisis management are available in the NFPA 1600 [11].

Technical needs for physical security systems including requirements for physical security in relation to integration with digital security systems are set by standards such as EN 50131 and EN 62676 in Europe [12,13]. Coordinated incident response, resilience obligations and reporting are also part of the requirements of other regulatory frameworks like NIS2, DORA, and GDPR across sectors [14-16].

Despite all of this work in standards and research, there is still a lack of cohesion: few systems bring together incident response and business continuity functionality for IT, OT, and physical security in a single architecture. These domains are generally considered in isolation with a tiered approach to organisation and governance that fails to align the governance structure, the escalation process, and the recovery goals. This fragmentation breeds exposure to three types of failures: hybrid, systemic and cascading failures in converged environments.

The goal of this research is to suggest a single Incident Response and Business Continuity (IRBC) architecture for cyber-physical environments where:

- incorporates governance, operational processes, technology platforms and recovery practices;
- repeats words or phrases in context, such as by repeating a question;
- addresses risks from hybrid, systemic and cascading across IT, OT and physical world.

The materials and methods are described in section 2; implications and limitations are discussed in section 3; conclusions are presented in section 4; and future research directions are presented in section 5.

2 MATERIAL AND METHODS

2.1 Research Design

The study follows a conceptual research design, which is commonly featured in the study of cyber-physical security architecture and study of resilience in the literature of cyber security. It utilizes a conceptual research design commonly used in the literature of cyber-physical security architecture and the field of study of resilience in cyber security. For research issues that fall across several interconnected aspects - IT, OT, and physical security, where issues can't be unambiguously captured through empirical measurement, and where issues of interdependencies and cascading pathways are at play, conceptual architecture is appropriate. The research design has four steps, which are literature review, standards mapping and regulatory mapping, cross domain dependency modelling, and unified architecture development.

2.2 Literature Review

A thorough literature study was carried out to set the foundation for the theoretical and operational aspect of cyber-physical incident response and business continuity. Peer-reviewed publications from IEEE, ACM, Springer, Elsevier, and ASIS International were examined. There were seminal contributions by Humayed et al. [1], Cardenas et al. [2], Krotofil and Cárdenas [3] and Herbane [5] that established key perspectives and ideas about CPS vulnerabilities, the convergence of IT and OT, hybrid threat propagation and organisational resilience. Search terms included:

- “cyber-physical systems security”,
- “IT/OT convergence”,
- “industrial control system resilience”,
- “business continuity”,
- “incident response architecture”.

The articles were chosen to have methodological qualities, relevance of the subject for converged environments, and citation impact. Indeed, the existing research has validated the domain interdependencies but has failed to provide consistent models of architecture that integrate domain interdependencies between incident response and continuity roles in IT, OT and physical security.

Standards and Regulatory Mapping

To identify structural complementarities, overlaps, and gaps of incident response and business continuity requirements in international standards and regulatory frameworks, a comparative analysis was carried out based on existing literature [6-16]. The mapping included:

- ISO/IEC 27001:2022 - ISMS governance and incident management [6]
- ISO 22301:2019 - BCMS requirements and recovery objectives [7]
- ISO 31000:2018 - enterprise risk management principles [8]
- NIST SP 800-61 - incident handling guidance [9]
- NIST SP 800-34 - contingency planning for IT systems [10]
- NFPA 1600 - continuity, emergency, and crisis management [11]
- EN 50131, EN 62676, EN 60839 - physical security system specifications [12,13,18]
- NIS2, DORA, GDPR - EU regulatory obligations for resilience, reporting, and ICT governance [14–16]

Requirements were coded into thematic categories as follows: Detection, classification, escalation, recovery goals, governance structure, reporting requirements, technology integration and risk assessment.

Table 1: Standards Mapping Matrix

Standard / Regulation	Domain	Key Contribution	Identified Gap
ISO/IEC 27001 [6]	Cyber	ISMS, incident mgmt.	Limited OT/physical integration
ISO 22301 [7]	BC	RTO/RPO, BCMS	No explicit cyber-physical linkage
ISO 31000 [8]	Risk	Risk principles	No hybrid risk taxonomy
NIST SP 800-61 [9]	Cyber	Incident handling	No physical domain coverage
NIST SP 800-34 [10]	IT	Contingency planning	Limited cross-domain recovery
NFPA 1600 [11]	Emergency	Crisis mgmt.	Minimal digital integration
EN 50131 [12]	Physical	Intrusion systems	No cyber linkage
EN 62676 [13]	Physical	Video surveillance	Integration not fully defined
NIS2 [14]	Regulatory	Cybersecurity	Focused on essential entities
DORA [15]	Regulatory	ICT resilience	Financial sector specific

2.3 Cross-Domain Dependency Modelling

Cyber-physical risk propagation techniques were used to model cross-domain dependencies [1-4]. There are four types of dependency that were identified:

- **Cyber → OT:** IT systems influencing OT processes (e.g., malware affecting PLC logic).
- **OT → Cyber:** OT disruptions impacting IT systems (e.g., SCADA outages affecting telemetry).
- **Physical → Cyber:** Physical events affecting digital systems (e.g., power failure disabling servers).
- **Cyber → Physical:** Digital compromise affecting physical assets (e.g., access-control manipulation).

That's represented in the diagram in Figure 1 - Cyber-Physical Dependency Model that highlights bidirectional dependency and influence between IT, OT, physical systems, business processes, and external stakeholders.

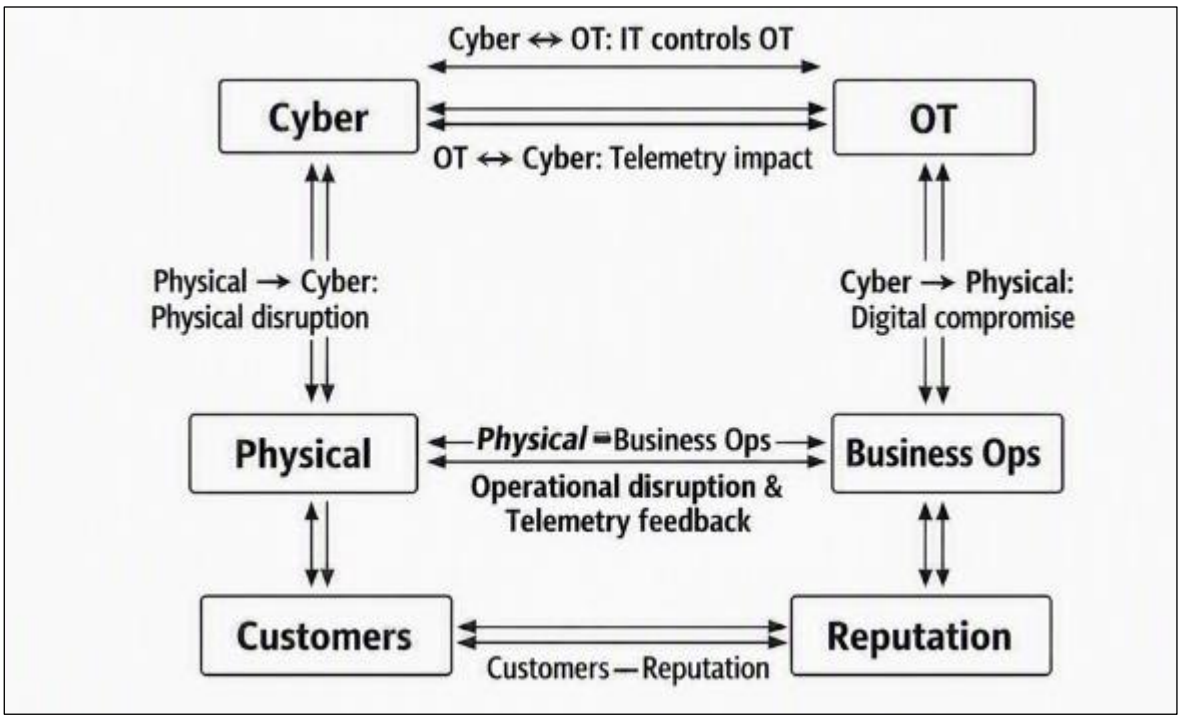

Figure 1: Cyber-Physical Dependency Model

2.4 Architecture Development

The unified IRBC architecture has been created by a structured synthesis process, which integrates the conceptual modelling with the operational requirements that are derived from internationally recognised standards. Governance, incident response, technology integration and business continuity principles were moulded to architectural layers for holistic application across IT, OT and physical security.

The guidance on cyber-physical telemetry correlation [1,19] was implemented for cross-domain situational awareness using unified monitoring concepts, mostly through the SIEM and PSIM platforms. To achieve this validation, NIST SP 800-207 [20] stipulated that zero trust principles be applied to an environment where integration of identities, devices, and connections are expected to be persistent.

To leverage predictive threat detection, anomaly identification and enable automation for incident response activities, a feature implemented was AI/machine-learning based analytics in tune with CPS resilience research on anomaly detection and predictive modelling [2,3].

Standards integration was done by using standards relating to information security governance ISO/IEC 27001:2022 [6], continuity planning ISO 22301:2019 [7], risk management ISO 31000:2018 [8], incident handling NIST SP 800-61 [9] and contingency planning NIST SP 800-34 [10] were used, in addition to those in the physical security standards: NFPA 1600 (Emergency and Crisis Management) [11] and EN 50131, EN 62676, EN 60839 (Physical security system interoperability) [12,13,18]. These frameworks informed architecture governance, operation, technology and recovery aspects, providing the structure or requirements. To promote regulatory convergence between NIS2, DORA and GDPR [14-16] the IRBC model is conceptually coherent and practically deployable in cyber-physical systems.

2.5 Ethical Approval

This study uses only publicly available secondary sources and does not involve human participants or other subjects. Ethical approval and informed consent were therefore not required.

3 RESULTS

3.1 Architectural Components of Unified IRBC Model

The analysis resulted in an Integrated Incident Response and Business Continuity (IRBC) architecture of four layers: ***Governance, Operational, Technology integration, and Recovery*** which are all interlinked. These layers when combined are a single cyber-physical resilience construct that can coordinate incident response and continuity functions between the IT, OT, and physical security domains. The findings show that resilience in converged environments is not the result of an individual capability, but rather, the synergy of multiple capabilities.

Table 2: Mapping IRBC Architectural Components to Cyber Physical Domains

IRBC Component	IT Domain Functions	OT Domain Functions	Physical Security Functions	Cross-Domain Contribution
Governance & Oversight	Policy enforcement, digital governance, SOC oversight	OT governance, process safety oversight	Physical security governance, access policy enforcement	Establishes unified authority and cross-domain decision-making
Operational Coordination	Incident response workflows, digital DPIAs	OT incident handling, safe-state activation	Physical incident response, perimeter control	Enables coordinated multi-domain response and escalation
Technology & Monitoring	SIEM, IAM, encryption, endpoint telemetry	SCADA/ICS monitoring, anomaly detection	PSIM, access control telemetry, sensor data	Provides unified monitoring and detection of hybrid/systemic risks
Assurance & Continuity - Recovery	Digital continuity, backup systems, audit trails	OT redundancy, manual override, process continuity	Physical redundancy, emergency access, facility continuity	Maintains resilience during cascading disruptions

The architecture is based on the international norms and cyber-physical resilience studies, not only to detect, contain, and recover from hybrid, systemic and cascading disruptions in converged environments, but also to serve as a general vector of effective and efficient resilience.

3.1.1 Governance Layer

The governance layer sets the organizational authority needed to manage incidents involving cyber-physical in a coherent manner. It brings together the three areas of leadership, regulatory requirements, and cross-domain oversight in one governance framework. There is a shared leadership role that offers strategic leadership and multi-functional committees that include the IT, OT, physical security, risk, compliance, and operations functions. Incident response, business continuity and emergency management policies are aligned to ensure a seamless response to disruptions across the domains. The journey to regulatory reporting is aligned with NIS2, DORA and GDPR [14-16] which ensure the cyber-physical incidents are handled in a compliant and accountable governance journey. For resilience, this layer focuses on it being an organisational capability, in line with the governance principles in ISO/IEC 27001 [6] and ISO 31000 [8].

3.1.2 Operational Layer

The operational layer outlines processes needed for interdomain coordination of incident response and continuity activities. Provides a consistent, standardised classification of incidents, that allows organisations to with clarity and consistency recognise a hybrid incident, a systemic incident and a cascading incident [1, 2, 3]. Escalation paths have been built-in enabling cyber, OT, and physical response teams to respond as one, helping to minimize delays and stop disjointed response. Communication paths are coordinated between domains, ensuring there are no delays or disruption between domains during high velocity incidents. Domain's silos are broken down, and responsibilities are given transparently enough that they promote coordinated action.

Operational readiness and preparedness through training programmes and simulation exercises [5,11]. This layer takes governance intent and helps to convert the intent into operational capability and corresponds to the incident handling guidance provided by NIST SP 800-61 [9] and emergency management requirements contained in NFPA 1600 [11].

3.1.3 Technology Integration Layer

The situational awareness and ability to analyse threats come from technology integration, which is essential for cyber-physical response. Integrated monitoring systems facilitate the integration of cyber telemetry with physical security signals, assisting organisations to identify and comprehend incidents with utmost precision [1,19]. The enforcement of Zero Trust in IT and OT and physical systems limits the movement of people laterally and decreases the potential for misuse of privileges in accordance with the principles of "continuous check and never assume". Using AI and machine-learning analytics, the system not only performs behavioural anomaly detection but also allows for a new standard of predictive threat modelling and automated correlation of cyber-physical events [2,3], enhancing the organization's potential to automate potential hybrid threats and limit their impact. The EN50131, EN62676 and EN60839 interoperability standards provide reliable interworking of security systems among domains, including the coordination of responses and unified monitoring. Use secure communication channels to facilitate cross-domain coordination. The layer guarantees that technology becomes an enabler for convergence and not an impediment, paying heed to research on cyber- physical systems which focus on integrated telemetry and cross-domain analytics [1-3].

3.1.4 Recovery Layer

The recovery layer harmonizes business continuity and disaster recovery strategies on domains. The recovery goals fulfil the requirements of ISO 22301 [7] and are connected to the IT, OT and physical recovery goals. Alternative operating sites are designed to allow for cyber-physical operations while reducing downtime in the event that there is a severe disruption, and the continuous operation of critical processes is important. Continuity of the supply chain is arranged so as to reduce vulnerabilities in the supply chain and eliminate instability in the operation due to dependence on external resources. Cascading failure containment strategies are informed by CPS risk propagation research [3], ensuring that secondary and tertiary disruptions are anticipated and controlled.

Post incident: Organisation learning through the analysis of incidents, continuous learning through post incident learning, and building long-term resilience by these analysis cycles [5,11]. This layer is related to the principles of continuity and recovery in ISO 22301 [7] and NFPA 1600 [11] and ensures recovery is coordinated, comprehensive and is sensitive to the reality of the organisation.

The unified IRBC architecture is described in figure 2, which shows how the IRBC layers are related to each other.

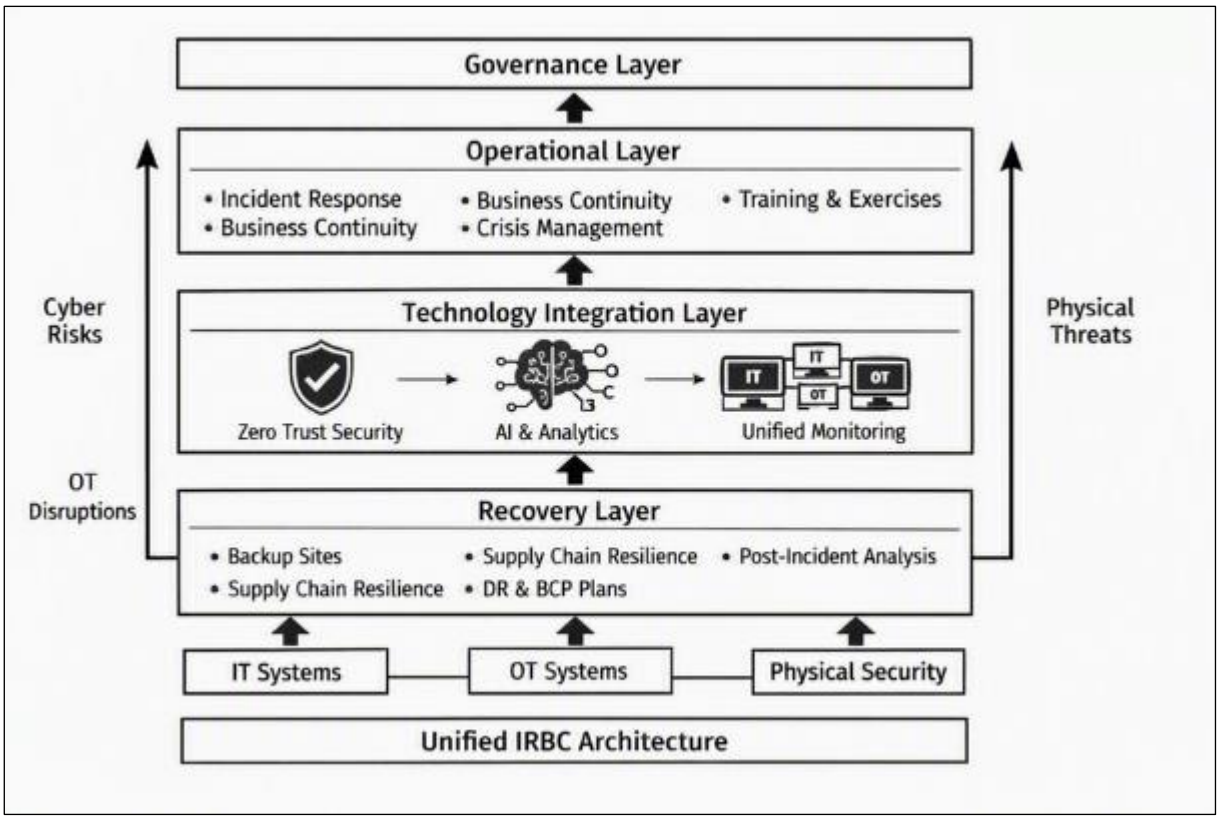

Figure 2: Unified IRBC Architecture

3.2 Technology Integration Findings

The results of the technology integration analysis were consistent with the results that unified monitoring platforms can significantly improve situational awareness, by being able to correlate cyber events with physical security signals [1,19]. The Zero Trust architecture minimizes the lateral movement across domains taking into account continuously ongoing verification and the principle of granting only the minimum access needed (least privilege) [20].

Behavioural anomaly detection, predictive threat modelling, and automated correlation of cyber-physical events are supported by AI and machine-learning models [2,3]. These results illustrate, on a structural level, that technology convergence is essential to risk management of hybrid and systemic threats and not just an operational addition. Table 3 provides a cross-domain mapping of IRBC capabilities, showing how each function behaves across IT, OT, and physical security, and how it contributes to hybrid, systemic, and cascading risk mitigation.

Table 3: Mapping Incident Response & Business Continuity Capabilities to Cyber-Physical Domains

IRBC Capability	IT Domain	Operational Technology (OT)	Physical Security Domain	Hybrid / Systemic / Cascading Risk Contribution
Unified Detection & Monitoring	SIEM correlation, endpoint telemetry	SCADA/ICS anomaly detection	PSIM events, access control logs	Enables early identification of hybrid attacks across domains
Cross-Domain Incident Classification	Digital incident taxonomy	OT-specific failure modes	Physical breach categories	Prevents misclassification that leads to systemic escalation
Coordinated Containment Procedures	Network segmentation, identity isolation	Process isolation, safe-state activation	Physical lockdown, perimeter control	Limits cascading propagation across interconnected systems
Integrated Communication Protocols	IT incident channels, SOC workflows	OT operator alerts, control room escalation	Security operations notifications	Ensures unified situational awareness during multi-domain crises

Business Continuity Activation	Digital service failover, backup systems	Redundant control systems, manual override	Physical redundancy, emergency access	Maintains operational continuity during systemic disruptions
Cross-Domain Forensics & Recovery	Log analysis, malware forensics	Root-cause analysis of OT failures	Physical breach reconstruction	Supports full reconstruction of hybrid and cascading incidents
Regulatory & Reporting Alignment	GDPR, NIS2, DORA reporting	NIS2 OT-specific obligations	EN physical security compliance	Ensures unified regulatory fulfilment across all domains

3.3 Risk Propagation Analysis

The risk propagation analysis reveals that hybrid, systemic and cascading risks flow through cyber-physical environments. Hybrid risks involve an attack via both cyber and physical paths, for example by asking to access via a cyber path while simultaneously attempting a physical attack through a security system whose authentication is disabled by malware [1,2].

However, when systems are interconnected, compromising the IT system can impact on OT telemetry systems and cause operational changes to occur, systemic risks [3,4]. The cascading risks follow one another in a cascading order: a disruption in the supply usually results in a production stoppage, a degraded service and a fall of reputation [5]. The classification model to analyse these risk types is shown in table 4. The findings support the hypothesis that cyber-physical ecosystems create a risk propagation effect and conclude that there is a need for an integrated IRBC architecture to prevent the risk from escalating between different domains.

Table 4: Cross-Domain Cyber-Physical Risk Categories and Propagation Characteristics

Risk Category	IT Domain Characteristics	OT Domain Characteristics	Physical Security Characteristics	Propagation Pattern
Hybrid Risks	API failures, identity compromise, digital service disruption	ICS/SCADA anomalies, sensor malfunction	Access control failures, perimeter breaches	Simultaneous multi-domain impact triggered by shared dependencies
Systemic Risks	Platform-wide outages, cloud dependency failures	Automation chain collapse, process-wide disruption	Sensor network collapse, facility-wide failure	Amplified through interconnected systems and organisational dependencies
Cascading Risks	Data correlation leaks, inference-driven exposure	Sequential OT disruptions, control loop failures	Physical-digital chain reactions, multi-stage breach escalation	Sequential propagation across domains driven by interlinked processes

4 DISCUSSION

4.1 Interpretation of Findings

The findings validate the fact that cyber-physical ecosystems will present structural challenges, ones that will not be solved by traditional incident response and business continuity practices, which are largely domain specific. Hybrid, systemic, and cascading risks spread across IT, OT, and physical security permeating and undermining siloed organisational structures. The unified IRBC architecture accounts for this fact by moving past the notion of incident response and continuity as different and, instead, specifying them as a single, converged capability.

Convergence becomes a structural criterion and extends beyond being an optimal option for the provision of services. Cyber - Physical Systems orchestrate operations, share telemetry and have closely converged control flows. If they do happen, it's difficult for them to stay isolated. Difficulty in receiving OT data from the telemetry system from an IT system can cause physical processes to be disturbed and eventually lead to operational instability from a cyber intrusion. On the other hand, during a physical disruption (e.g., loss of power) a digital system may lose functionality, put some monitoring platforms out of service, and undermine incident detection capabilities. These interactions demonstrate that the hybrid and systemic risk are not unusual but rather, part and parcel of the environment in which they are merged.

The IRBC is a single resilient architecture that provides a multi-disciplinary approach to addressing these challenges and presents recovery, governance, and operations in one common package. Governance offers the needed organisational legitimacy to enable cyber-physical response. If there is no unity of leadership, cross-domains committees and harmonised policies, then there is no way to sustain the operational coordination. As governance is separated, response is separated and a risk propagation kicks in as a response. The architecture also frames governance as a pivot that connects the regulatory requirements, organizational structure and cross-domain supervision.

Co-ordinating operations is also essential. The architecture shows the importance of a flow of functions when it comes to incident classification, escalation, communication and response. Cyber Teams, OT Teams, and Physical Teams working in isolation leads to misclassifying incidents, delaying escalations and skewed situational awareness. These problems are solved by the operational layer where unified processes are introduced, reflecting the interconnections of cyber-physical systems.

Technology integration supports the convergence. Benefits of unified monitoring platforms include the ability to tie cyber telemetry with physical security signals and then view or understand the incident with high fidelity. IT, OT and physical system security are treated under Zero Trust, limiting lateral movement and privilege abuse. AI-based analytics deliver predictive analytics on behavioural deviations and new threats. The capabilities highlight that technology is not an add-on but a structural factor of Cyber-Physical Resilience.

Recovery processes conclude the architecture by choosing continuity processes across domains. Inconsistencies in recovery goals foster secondary failures, operational instability and long periods of downtime.

The architecture achieves this through enabling RTO and RPO goals to be aligned, incorporating alternate operating locations, and incorporating cascading failure containment mechanisms based on CPS risk propagation research. Recovery is no longer a silo mentality operation but rather a cross-domain coordinated effort.

4.2 Implications for Industry

The unified IRBC architecture implies significance to sectors of efficient cyber-physical convergence. It is created to help achieve the goals of regulatory alignment, operational coherence, and resilience enhancement in environments with high interdependencies between digital and physical systems.

4.2.1 Critical Infrastructure Operators

Relying on IT/OT integration, whether or not they are connected to the outside world, critical infrastructure operators in energy, transportation and water and healthcare settings are highly susceptible to hybrid and/or systemic disruptions. Enterprise segments are ones that are heavily dependent on interaction with tightly coupled control systems, real-time telemetry and physical processes, which are vulnerable to cyber intrusion or failures during operation.

Unified IRBC will offer a clear framework for handling cyber physical incidents, enhancing native resilience and mitigation of cascading failures, and ensuring conformance with NIS2 and sector-specific regulations [14]. The architecture combines incident response, continuity planning, and cross-domain monitoring, so that response and recovery activities are not conducted in ways that presuppose the digital setting to be independent of the industrial system, but rather dependent upon it. This alignment reflects the resilience needs which have been highlighted in CPS security literature [1-3] and continuity research [5].

4.2.2 Financial Institutions

Financial institutions have online environments that are increasingly reliant on physical infrastructure, distributed data centres and third-party service providers. Through the integrated pathway of incident reporting, the unified IRBC architecture promotes DORA-related resilience, while cross-domain functions and harmonised resiliency continuity plans serve as coherent mechanisms for responding to such incidents. The IRBC architecture is unified so that it promotes the resilience associated with DORA via integrated pathways to reporting incidents, harmonised pathways to continuity and coordinated cross-domain responses. In financial markets, a disruption can cascade quickly and reach many people via digital platforms, payment systems and services that interact with customers. It is the architecture's convergence around unified monitoring, Zero Trust enforcement [20] and predictive analytics [2,3] that pave the way for precise and regulated management of cyber-physical risks. With multi-domain incidents, this allows financial institutions to keep their flow of services intact, safeguard sensitive data transfers and follow rigid report deadlines.

4.2.3 Industrial and Manufacturing Environments

Industrial and manufacturing settings are even more critical and sensitive to OT breaches, where system failures in the control systems can lead to loss of productivity, deterioration of safety, and disruption in supply-chain continuity. They rely on highly integrated industrial control systems, sensors and automation solutions, which can be vulnerable to physical and cyber disruptions. The unified IRBC concept improves resilience through a unified approach to monitor OT and IT systems, the implementation of predictive analytics to identify operational anomalies and integrated recovery processes aiming to guarantee the continuity of production processes [3,4]. With these, manufacturing firms have the ability to plan ahead, manage and get back to business after a cyber physical incident while maintaining operational integrity.

The building code compliance with EN 50131, EN 62676 and EN 60839 [12,13,18] continues to improve interoperability between the physical security system and digital monitoring platform.

4.2.4 Public Sector and Emergency Services

The public sector and crisis organisations, such as emergency services , will benefit from better crisis coordination, a common emergency response procedure and better cross-agency communication [11]. This context often involves handling incidents with digital repercussions and physical repercussions - and involves multiple operating domains which must be interconnected.

The centralized IRBC structure offers an integrated structure for the management of multi-domain incidents and disaster, where classification, escalation, and communication logs are connected for cyber, physical, and operational technology teams. It enhances the readiness of institutions, facilitates interagency collaboration among public safety and critical service agencies and addresses NFPA 1600 [11] emergency management principles. This allows public sector organisations to be effective when dealing with hybrid, systemic and cascading incidents which are beyond the conventional emergency response boundaries.

4.3 Limitations

While the unified IRBC architecture offers a solid conceptual basis for cyber-physical resilience, there are some limitations to be recognized. The architecture has yet to be tested in real organisational settings and its impact might differ in different sectors that have different operating constraints. Legacy systems may involve integration issues, especially within OT systems that often utilize complex, vendor-specific architectures and protocols that prove difficult to connect with new technologies. There may be greater vendor differences that complicate the movement of the monolithically integrated monitoring platform and enforcing Zero Trust.

Another non- technical restriction is the human factor. The ability to work cross-domain, to make decisions collaboratively, and to work under stress during the complex incident requires training, decision making, and interoperability across the domains. Factors such as organisational culture, existing incident response and continuity programmes, and communication may affect uptake. While these restrictions do not negate the concept interest of architecture, they emphasize the need to adapt and validate the architecture empirically in every sector [5,17].

4.4 Future Research Directions

Research efforts should seek to empirically validate unified IRBC architecture through case studies, controlled simulation and cross domain exercises. There is a need for quantitative resilience metrics to monitor the impact of effective cohesive response and continuity strategies, and to enable organisations to benchmark their efforts and target future improvements. AI and machine-learning models need to be further developed and refined to achieve more effective capabilities for hybrid threat detection, predictive analytics, and automated cyber(physical) event correlation.

The architecture should be adapted sector by sector in those sectors that are considered to have different constraints and regulations on operation, such as energy, transportation, healthcare, finance, and manufacturing. Further research is needed around human-machine teaming during incident response, especially in cases where an automated system must interact with human decisionmakers in stressful conditions under uncertainty [2-5,17]. The research developments will help evolve the unified IRBC architecture from a conceptual model to an empirical validated framework that can increase the cyber-physical resilience in sectors.

5 CONCLUSION

Organisations need to respond to incidents and disruptions that transcend boundaries between the physical security, OT and IT spaces and this is where Cyber-physical ecosystems come in. Based on the analysis found in this study, hybrid, systemic and cascading risks extend beyond converged environments and siloed incident response, and business

continuity methods cannot address these risks anymore. The integrated IRBC architecture is addressing this challenge by bringing together governance, operations, technology and recovery into a common "resilience" construct, which is better suited to the challenges faced in modern cyber-physical systems.

The architecture also sets a platform for governance, with a holistic organizational view of leadership, regulatory requirements and cross-domain oversight ensuring coordinated action. Operational processes are re-engineered to better capture the close linkages between the cyber and physical aspects of incidents and support coherent CC classification, escalation, communication and response.

Driven by technology integration, situational awareness and people's ability to analyse and understand events across domains enabled by this technology, their ability to detect and interpret cross domain events with accuracy and insight, and recovery strategies were synchronized across IT, OT and physical systems to prevent secondary failures and expedite recovery.

While conceptual, the unified IRBC architecture provides a strong basis for organisations wanting to increase the cyber-physical resilience of their organisation.

It conforms to international standards and regulatory requirements, and builds on lessons learned from the CPS security and resilience research and offers a framework for converged threats management. The model underlines the importance of coordinated governance, integrated monitoring, enforced Zero Trust measures, AI-driven analyses and harmonized recovery opportunities as characteristics of cyber-physical resilience.

Further research is needed in the areas of empirical testing, sector-specific adaptation and quantification of metrics of resilience to measure unified response and continuity. The importance of integrated architectural approaches will grow as the cyber-physical ecosystems evolve. The model of unified IRBC described in this research provides a roadmap for attaining resilience amidst the interdependence, convergence and increasing complexity of hybrid threats in the conditions of such an environment.

STATEMENTS ON COMPLIANCE WITH ETHICAL STANDARDS

Acknowledgments

The author acknowledges the institutional support provided by the Converged Security Institute, whose commitment to advancing cyber-physical resilience research created the conditions necessary for the development of this unified IRBC architecture. The intellectual environment, access to multidisciplinary expertise, and organisational encouragement contributed significantly to the conceptual refinement and structural coherence of the work.

Funding Source

The author declares that no financial support, funding, sponsorship, or monetary compensation was received from any organization, institution, or commercial entity for the conduct of this research. The author has no financial relationships that could be perceived to influence the results or interpretation of this study.

Disclosure of conflict of interest

The study was conducted independently, without external influence on its design, analysis, interpretation, or conclusions. All assessments and architectural formulations reflect the author's professional judgement and adherence to academic integrity. The author declares that there are no financial or non-financial conflicts of interest related to this research

REFERENCES

[1] Humayed A, Lin J, Li F, Luo B. Cyber-physical systems security: A survey. IEEE Internet Things J. 2017;4(6):1802–1831.

[2] Cardenas A, Amin S, Sastry S. Research challenges for the security of control systems. Proc 3rd USENIX HotSec. 2008.

[3] Krotofil M, Cárdenas A. Resilience of cyber-physical systems: The role of detection. In: Proceedings of the 10th International Conference on Critical Information Infrastructures Security (CRITIS 2015). Springer, 2016. pp. 3–17.

[4] Cárdenas A, Manadhata PK, Rajan S. Big data analytics for security. IEEE Secur Priv. 2013;11(6):74–76.

[5] Herbane B. Rethinking organizational resilience and business continuity management. Journal of Contingencies and Crisis Management. 2019; 27(2): 123–133.

[6] ISO/IEC 27001:2022. Information Security Management Systems - Requirements. International Organization for Standardization; 2022.

[7] ISO 22301:2019. Security and resilience -Business continuity management systems -Requirements. International Organization for Standardization; 2019.

[8] ISO 31000:2018. Risk Management -Guidelines. International Organization for Standardization; 2018.

[9] NIST SP 800-61 Rev.2. Computer Security Incident Handling Guide. National Institute of Standards and Technology; 2012.

[10] NIST SP 800-34 Rev.1. Contingency Planning Guide for Federal Information Systems. National Institute of Standards and Technology; 2010.

[11] NFPA 1600:2019. Standard on Continuity, Emergency, and Crisis Management. National Fire Protection Association; 2019.

[12] EN 50131-1:2006. Alarm systems -Intrusion and hold-up systems. European Committee for Standardization; 2006.

[13] EN 62676-1:2014. Video surveillance systems for use in security applications. European Committee for Electrotechnical Standardization; 2014.

[14] European Union. Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive).

[15] European Union. Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector (DORA).

[16] European Union. Regulation (EU) 2016/679 (General Data Protection Regulation -GDPR).

[17] Linkov I, Trump BD. The science and practice of resilience. Springer; 2019.

[18] EN 60839-11-1:2013. Electronic access control systems. European Committee for Electrotechnical Standardization; 2013.

[19] CISA. Security Information and Event Management (SIEM) best practices. Cybersecurity and Infrastructure Security Agency.

[20] NIST SP 800-207. Zero Trust Architecture. National Institute of Standards and Technology; 2020.