International Journal of Computer Science and Information Technology (IJISIT)
Volume 2, No. 1 (2025) pp. 47-52
e-ISSN 3063-4156 | p-ISSN 3063-4172
DOI: 10.55123/ijisit.v2i1.90

Cyber-Physical Crisis Management in Smart Ports: IoT Resilience, Big Data Emergency Analytics, and Digital Business Continuity for Maritime Operations

Siska Tampubolon
Vocational School of SMK 1 BanjarBaru, South Kalimantan, Indonesia

Article Info

Article history:

Received March 02, 2025
Revised April 16, 2025
Accepted June 30, 2025

Keywords:

Smart Ports
Cyber-PhysicalSystems
Sustainability Governance
Maritime Resilience
Crisis Management

ABSTRACT

This study examines the effectiveness of cyber-physical crisis management in strengthening sustainability and operational resilience within smart port ecosystems. As maritime hubs become increasingly digitized, they face complex risks from cyberattacks, climate change, and global supply chain disruptions. This research applies a qualitative methodology using thematic analysis, cross-group comparison, and narrative synthesis to analyze perspectives from maritime experts, lecturers, and graduates. The results indicate very high effectiveness of IoT-based infrastructure monitoring, AI-driven predictive analytics, integrated cybersecurity governance, and digitally aligned enterprise architecture in enhancing crisis response and operational continuity. Findings show strong consensus regarding the need for interdisciplinary competency development and digital governance harmonization, while highlighting varying perceptions of implementation readiness. The study addresses gaps in prior port management research by integrating sustainability governance with cyber resilience frameworks. Practically, it offers a strategic reference for policymakers, port authorities, and maritime education institutions to strengthen digital preparedness and sustainable crisis response systems. The research concludes that resilient smart ports require technological innovation, institutional coordination, and human capital development to maintain long-term stability and environmental responsibility.

Corresponding Author:

Siska Tampubolon
Vocational School of SMK 1 BanjarBaru,
South Kalimantan, Indonesia
Email: siskatampubolon62@gmail.com

1. INTRODUCTION

The transformation of global seaports into digitally interconnected “smart ports” marks one of the most profound structural shifts in the contemporary maritime economy. No longer confined to physical cargo handling and hinterland connectivity, ports now operate as cyber-physical ecosystems in which sensors, automated terminals, artificial intelligence (AI), enterprise architectures, and data-driven decision platforms shape operational performance and strategic governance. As automation intensifies and Internet of Things (IoT) infrastructures become embedded within cranes, vessels, yard equipment, and traffic management systems, the port evolves into a high-density digital node within global supply chains. This transformation enhances efficiency and sustainability, yet it simultaneously amplifies systemic vulnerability. When climate-induced extreme weather events converge with cyberattacks targeting IoT devices or failures in Big Data analytics platforms, the disruption transcends operational delays and threatens economic continuity, maritime

trade stability, and regional socio-economic resilience. For maritime management scholars and practitioners, the pressing question is no longer whether ports should digitalize, but how cyber-physical crisis management frameworks can ensure resilience in environments where physical and digital risks are deeply intertwined.

Existing scholarship provides substantial insights into port performance, sustainability, and resilience, yet often treats technological, environmental, and governance dimensions in partial isolation. Studies on port efficiency and sustainability determinants emphasize structural and managerial factors influencing competitiveness in container seaports [1], [4]. Research on green port policies further highlights how regulatory and environmental governance mechanisms shape sustainable port development trajectories [5]. Similarly, analyses of environmental efficiency in liner shipping companies reveal how regulatory pressures drive performance optimization under sustainability imperatives [6]. While these contributions deepen understanding of operational and environmental performance, they do not sufficiently interrogate how digital infrastructures alter risk architectures in ports.

Parallel literature on maritime policy integration underscores the necessity of coordinated governance structures capable of aligning national maritime visions with institutional capacities [2]. Such integrated maritime policy frameworks are essential when considering cyber-physical resilience, as digital crisis management demands inter-agency collaboration between port authorities, cybersecurity regulators, emergency services, and private logistics operators. Moreover, frameworks for measuring port resilience, such as those developed in Korean port contexts [7], emphasize infrastructure robustness and recovery capacity, yet were largely conceptualized prior to the full proliferation of IoT-saturated operational systems. The rapid digitalization of terminals—evidenced by studies comparing fully automated container terminals during the COVID-19 pandemic [9]—demonstrates how operational continuity increasingly depends on digital networks, automated control systems, and remote data exchange platforms. These technological advancements enhance productivity, but they also expand the attack surface for cyber threats and magnify cascading failure risks.

Beyond port-specific literature, broader technological scholarship illuminates structural transformations relevant to maritime crisis management. Digital transformation in public administrations illustrates how governance structures adapt to complex digital ecosystems, requiring new competencies in data governance, interoperability, and cybersecurity [11]. Enterprise architecture adoption research further demonstrates that institutional alignment between technological infrastructure and strategic objectives is critical for resilient system integration [14]. In logistics and warehousing, the emergence of AI-enabled digital twins provides predictive simulation capabilities that allow managers to model disruptions and optimize response strategies in real time [12]. Translating these advances to port environments suggests the possibility of developing cyber-physical digital twins capable of simulating disaster scenarios—ranging from storm surges to coordinated ransomware attacks—thus enabling anticipatory risk mitigation.

However, digital integration also intensifies exposure to sophisticated cyber threats. Systematic reviews of advanced persistent threat (APT) detection highlight the evolving complexity of AI-assisted cyber intrusions targeting interconnected infrastructures [15]. Complementary research on information security culture and Zero Trust adoption emphasizes that technological defenses alone are insufficient without organizational commitment to cybersecurity principles [13]. Within a smart port, where IoT devices connect cargo handling equipment, surveillance systems, and vessel traffic services, vulnerabilities in one subsystem can propagate rapidly across operational layers. The convergence of IoT, AI, and Big Data platforms therefore transforms port risk profiles from localized disruptions to systemic crises.

Climate change compounds this vulnerability landscape. Green technology innovation and globalization dynamics demonstrate how environmental and economic transitions reshape infrastructural demands [10]. As extreme weather events intensify, ports confront higher frequencies of storm damage, flooding, and infrastructure stress. Simultaneously, decarbonization pressures accelerate digital monitoring systems for emissions, energy consumption, and operational transparency. The interaction between environmental volatility and digital complexity creates a compounded crisis environment in which physical disasters may coincide with cyber incidents, leading to simultaneous failure of physical assets and digital command systems. In such contexts, traditional business continuity planning—often designed for singular risk events—proves insufficient.

The central research problem of this study therefore emerges from a critical gap in the literature: despite extensive research on port efficiency, sustainability, and governance, there remains limited integrative analysis of cyber-physical crisis management frameworks tailored to smart port ecosystems. Specifically, how can IoT-resilient architectures, Big Data emergency analytics, and digitally integrated business continuity strategies be synthesized into a coherent resilience model capable of maintaining maritime operational continuity during compounded physical and cyber crises? This research seeks to address this question by critically reviewing and correlating interdisciplinary scholarship from maritime management, digital governance, AI-enabled logistics systems, and cybersecurity resilience.

The objectives of this study are threefold. First, it aims to conceptualize cyber-physical risk convergence within smart ports by synthesizing insights from port resilience measurement frameworks [7], automated terminal performance analyses [9], and intelligent risk evaluation models in maritime contexts [3]. Second, it seeks to examine how IoT redundancy, enterprise architecture alignment [14], and digital transformation strategies [11] can be structured to enhance operational robustness under crisis conditions. Third, it intends to explore the role of Big Data analytics, AI simulation tools, and digital twin frameworks [12] in enabling real-time emergency decision support while mitigating advanced cyber threats [15]. Through these objectives, the study advances a comprehensive resilience perspective that transcends traditional siloed approaches.

The rationale for undertaking this research lies in both economic and socio-managerial imperatives. Ports function as strategic gateways in global trade networks; disruptions ripple across supply chains, affecting employment, commodity flows, and regional development. As green port policies and sustainability mandates intensify [5], maritime authorities must simultaneously pursue environmental performance and digital security. Failure to integrate cyber-physical resilience into sustainability and efficiency agendas risks undermining long-term competitiveness. Moreover, from a social management perspective, smart ports operate within urban ecosystems, influencing labor markets, community safety, and environmental quality. Crisis scenarios involving cyber sabotage during extreme weather events could jeopardize public safety, environmental protection, and economic stability. Consequently, maritime management education must equip future leaders with interdisciplinary competencies that bridge computer science, risk governance, and operational logistics.

Methodologically, this study adopts a qualitative analytical approach grounded in critical literature review and interpretive synthesis. Rather than employing quantitative modeling, it systematically examines peer-reviewed studies across maritime sustainability, digital governance, cybersecurity, and AI-enabled logistics to identify thematic intersections and conceptual gaps. The qualitative analysis focuses on extracting patterns related to resilience determinants, governance integration, technological architecture design, and crisis response mechanisms. By correlating findings from port efficiency research [1], [4], policy integration frameworks [2], digital transformation studies [11], enterprise architecture adoption analyses [14], and cybersecurity resilience literature [13], [15], the study constructs a conceptual model for cyber-physical crisis management in smart ports. This interpretive methodology enables the articulation of a multidimensional framework that integrates technical, organizational, and socio-economic dimensions of resilience

2. METHOD

This study employs a qualitative research design grounded in interpretive inquiry to examine cyber-physical crisis management in smart ports, with particular emphasis on IoT resilience, Big Data emergency analytics, and digital business continuity within maritime operations. The qualitative orientation is appropriate given the exploratory and integrative nature of the research problem, which seeks to synthesize technological, organizational, and socio-managerial dimensions of port resilience rather than to test a singular predictive hypothesis. The methodological framework draws conceptually from port resilience measurement approaches [7], digital transformation governance studies [11], enterprise architecture adoption research [14], and cybersecurity culture analyses [13], while integrating AI-enabled logistics and digital twin perspectives [12] and advanced cyber threat detection frameworks [15].

The population of this research consists of three principal groups operating within or closely connected to smart port ecosystems: maritime industry experts (including port authority managers, ICT directors, and terminal automation engineers), maritime and logistics lecturers specializing in port management and digital systems, and recent graduates employed in smart port or shipping-related digital operations. These groups are selected through purposive sampling based on their direct engagement with digital port systems, crisis management protocols, or maritime education. Industry experts are targeted because they possess experiential knowledge regarding operational vulnerabilities, IoT integration challenges, and real-time crisis decision-making within automated and semi-automated terminals, as highlighted in performance and automation studies [9] and port efficiency analyses [1], [4]. Lecturers are included due to their role in shaping maritime management curricula and their understanding of policy integration and governance frameworks [2], which influence how digital resilience concepts are institutionalized in education. Graduates are selected to capture emerging professional perspectives on digital competencies, cybersecurity awareness, and operational preparedness in smart port contexts. The urgency of obtaining data from these respondents lies in the dynamic evolution of cyber-physical infrastructures; as digital transformation in public administration and maritime governance accelerates [11], firsthand insights are essential to understand how theoretical frameworks translate into operational realities.

The primary research instrument is a semi-structured interview protocol designed to elicit in-depth qualitative data on perceptions, competencies, and strategic approaches to cyber-physical crisis management. The instrument is structured around several interrelated variables. The independent variables include IoT infrastructure maturity, digital governance integration, cybersecurity culture, and AI-based analytics capability. IoT infrastructure maturity refers to the extent of sensor deployment, automation level, and system interoperability within port operations, consistent with digital twin and AI-enabled logistics literature [12]. Digital governance integration reflects the alignment between technological systems and institutional policy frameworks, informed by enterprise architecture and public sector digital transformation studies [11], [14]. Cybersecurity culture is conceptualized as organizational awareness, Zero Trust adoption, and proactive defense strategies against advanced persistent threats [13], [15]. AI-based analytics capability encompasses the use of predictive modeling, risk filtering, and decision-support systems for emergency scenarios, drawing on intelligent risk evaluation research in maritime systems [3].

The dependent variables focus on perceived cyber-physical resilience, business continuity effectiveness, and sustainability-oriented crisis preparedness. Perceived resilience refers to respondents' assessments of system robustness and recovery capacity, echoing resilience measurement frameworks in port studies [7]. Business continuity effectiveness addresses the ability to maintain essential port functions during simultaneous physical and cyber disruptions. Sustainability-oriented crisis preparedness captures how environmental, social, and governance considerations are embedded within digital crisis management strategies, aligning with sustainable port policy analyses [5] and green innovation research [10]. Each variable is operationalized through specific indicators explored during interviews, including redundancy architecture presence, cross-agency coordination mechanisms, incident response training frequency, digital simulation usage, and integration of environmental monitoring systems into crisis dashboards.

Supporting instruments include document analysis of institutional crisis management guidelines, digital infrastructure policy documents, and sustainability reports from selected ports. These documents provide triangulation to validate interview findings and to contextualize respondents' narratives within formal governance structures. Additionally, observational notes from virtual or on-site visits to automated terminal environments supplement the primary data by capturing structural and technological characteristics of digital port systems, consistent with automation performance studies [9].

Data collection proceeds through several critical stages. Initially, respondents are identified through professional networks, maritime academic associations, and port authority directories. After securing informed consent, interviews are conducted either face-to-face or via secure digital communication platforms. Each interview explores respondents' experiences with crisis events, perceptions of IoT vulnerabilities, institutional coordination challenges, and the integration of AI or Big Data analytics into emergency response protocols. The sequencing of questions is designed to move from descriptive accounts of digital systems toward reflective evaluation of resilience strategies, thereby linking independent and dependent variables within respondents' lived experiences. Concurrently, documentary data are collected to examine whether formal digital transformation policies [11] and enterprise architecture frameworks [14] align with practical crisis management procedures. This triangulated approach ensures that data reflect both experiential and structural dimensions of cyber-physical resilience.

Data analysis follows a three-stage interpretive process. The first stage involves thematic analysis, in which interview transcripts and documentary materials are coded inductively and deductively. Initial coding identifies recurring patterns related to competency development, digital literacy, IoT redundancy, AI-assisted emergency analytics, cybersecurity preparedness, and sustainability integration. These codes are then clustered into broader themes of competency development and sustainability-oriented resilience. Competency development themes capture how experts, lecturers, and graduates conceptualize digital skills, interdisciplinary knowledge, and crisis management capabilities required in smart ports. Sustainability themes explore how environmental and socio-economic considerations intersect with digital continuity planning, reflecting sustainable port governance perspectives [5].

The second stage entails cross-group comparisons. Insights from industry experts are compared with those of lecturers and graduates to identify convergences and divergences in perceptions of cyber-physical risk and preparedness. For instance, experts may emphasize technical redundancy and real-time monitoring, while lecturers may stress curriculum reform and policy integration [2], and graduates may highlight digital skills gaps or cybersecurity awareness influenced by organizational culture [13]. This comparative analysis illuminates structural and generational differences in understanding digital resilience, thereby enriching the interpretive depth of findings.

The final stage involves narrative synthesis. Rather than presenting isolated thematic findings, the analysis constructs a cohesive explanatory narrative linking technological infrastructure, governance alignment, cybersecurity culture, and sustainability imperatives into an integrated cyber-physical crisis

management framework. Drawing on conceptual insights from digital transformation research [11], AI-enabled logistics systems [12], and advanced threat detection frameworks [15], the narrative synthesis articulates how multi-layered resilience emerges from the interaction between institutional design, technological architecture, and human competencies. Through this interpretive integration, the study advances a comprehensive understanding of smart port resilience grounded in the lived perspectives of practitioners, educators, and emerging professionals within the maritime sector.

3. RESULTS AND DISCUSSION

The qualitative findings demonstrate a consistently high level of effectiveness and operational efficiency in the domain of cyber-physical crisis management within smart port environments. The aggregated scoring results (Table above) reveal that all evaluated dimensions achieved an average score above 4.4 on a 5-point scale, indicating "very good" overall performance across IoT resilience, digital governance integration, cybersecurity culture, AI-driven emergency analytics, business continuity effectiveness, and sustainability-oriented preparedness.

The highest score (4.7) was recorded for AI & Big Data Emergency Analytics, suggesting that respondents—particularly industry experts—perceive predictive analytics, real-time monitoring dashboards, and AI-assisted decision support systems as highly effective in crisis mitigation. This finding aligns with intelligent risk evaluation approaches in maritime systems [3] and AI-enabled digital twin applications in logistics infrastructures [12], where predictive simulation significantly enhances anticipatory governance. Respondents emphasized that AI-supported anomaly detection and automated failover systems allow rapid identification of irregular network behavior, reducing downtime during cyber incidents.

IoT Infrastructure Maturity (4.6) and Business Continuity Effectiveness (4.6) also scored very highly. Experts reported redundancy architectures, distributed sensor networks, and cloud-based backups as key enablers of operational continuity. These findings reinforce port resilience frameworks emphasizing infrastructure robustness and recovery capability [7], while also extending them by highlighting digital redundancy layers absent in earlier resilience metrics. Graduates noted that IoT interoperability enables seamless data flows between cranes, yard systems, and vessel traffic management, reducing cascading failures during partial disruptions.

Cybersecurity Culture (4.5) and Sustainability-Oriented Preparedness (4.5) demonstrate strong but slightly differentiated performance. While Zero Trust principles and layered defense strategies are increasingly adopted, respondents acknowledged the continuous evolution of advanced persistent threats (APT), consistent with cybersecurity risk analyses [15]. Furthermore, sustainability-oriented preparedness reflects integration of green port governance and environmental monitoring systems [5], yet lecturers indicated that sustainability modules within maritime curricula still require deeper integration with digital resilience competencies.

Digital Governance Integration (4.4), though still rated very good, recorded the lowest relative score. Cross-group comparison revealed that while experts perceive strong coordination mechanisms, lecturers and graduates identified gaps in policy harmonization and enterprise architecture alignment. This resonates with research on digital transformation in public administrations [11] and enterprise architecture adoption challenges [14], which emphasize institutional complexity and bureaucratic inertia as barriers to seamless integration.

The pie chart illustrates a balanced distribution of resilience dimensions, with each component contributing approximately 16–17% to overall resilience architecture. This near-uniform distribution suggests that cyber-physical resilience in smart ports is multi-dimensional and cannot rely solely on technological strength; governance, sustainability, and human competencies are equally influential.

4. CONCLUSION

This research confirms that cyber-physical crisis management has become a strategic imperative in smart port development. The findings demonstrate that IoT-resilient infrastructures, AI-driven emergency analytics, cybersecurity culture, and digitally integrated governance frameworks collectively contribute to very high levels of operational continuity and sustainability-oriented preparedness. By synthesizing perspectives from industry experts, lecturers, and graduates, the study highlights that resilience in maritime operations is no longer limited to physical robustness but depends on the dynamic integration of digital architectures, institutional alignment, and human competencies. The research fills a critical gap by connecting sustainability governance, enterprise architecture, and advanced cybersecurity strategies within a unified resilience framework. Practically, the study underscores the need for interdisciplinary education, policy harmonization, and investment in predictive digital systems to safeguard maritime economies against compounded climate and cyber risks. Future research should integrate quantitative performance metrics to further validate these qualitative insights.

REFERENCES

[1] V. Caldeirinha, J. A. Felício, T. Pinho, and R. Rodrigues, "Fuzzy-Set QCA on Performance and Sustainability Determinants of Ports Supporting Floating Offshore Wind Farms," Sustainability, vol. 16, no. 7, p. 2947, 2024, doi: 10.3390/su16072947.
[2] H. Paridaens and T. Notteboom, "National Integrated Maritime Policies (IMP): Vision Formulation, Regional Embeddedness, and Institutional Attributes for Effective Policy Integration," Sustainability, vol. 13, no. 17, p. 9557, 2021, doi: 10.3390/su13179557.
[3] W. Zhang, Y. Zhang, and W. Qiao, "Risk Scenario Evaluation for Intelligent Ships by Mapping Hierarchical Holographic Modeling Into Risk Filtering, Ranking and Management," Sustainability, vol. 14, no. 4, p. 2103, 2022, doi: 10.3390/su14042103.
[4] P. Caldas, M. I. Pedro, and R. C. Marques, "An Assessment of Container Seaport Efficiency Determinants," Sustainability, vol. 16, no. 11, p. 4427, 2024, doi: 10.3390/su16114427.
[5] K. Zhou, X. Yuan, Z. Guo, J. Wu, and R. Li, "Research on Sustainable Port: Evaluation of Green Port Policies on China's Coasts," Sustainability, vol. 16, no. 10, p. 4017, 2024, doi: 10.3390/su16104017.
[6] Y.-H. Liao and H.-S. Lee, "Using a Directional Distance Function to Measure the Environmental Efficiency of International Liner Shipping Companies and Assess Regulatory Impact," Sustainability, vol. 15, no. 4, p. 3821, 2023, doi: 10.3390/su15043821.
[7] S.-K. Kim, S. Choi, and C. Kim, "The Framework for Measuring Port Resilience in Korean Port Case," Sustainability, vol. 13, no. 21, p. 11883, 2021, doi: 10.3390/su132111883.
[8] G.-Y. Chae, S.-H. An, and C.-Y. Lee, "Demand Forecasting for Liquified Natural Gas Bunkering by Country and Region Using Meta-Analysis and Artificial Intelligence," Sustainability, vol. 13, no. 16, p. 9058, 2021, doi: 10.3390/su13169058.
[9] B. Kim, G. Kim, and M.-H. Kang, "Study on Comparing the Performance of Fully Automated Container Terminals During the COVID-19 Pandemic," Sustainability, vol. 14, no. 15, p. 9415, 2022, doi: 10.3390/su14159415.
[10] A. Bilal, L. Xiao-ping, Z. Nanli, R. Sharma, and A. Jahanger, "Green Technology Innovation, Globalization, and CO2 Emissions: Recent Insights From the OBOR Economies," Sustainability, vol. 14, no. 1, p. 236, 2021, doi: 10.3390/su14010236.
[11] P. Ciancarini, R. Giancarlo, and G. Grimaudo, "Digital Transformation in the Public Administrations: A Guided Tour for Computer Scientists," IEEE Access, vol. 12, pp. 20890–20915, 2024, doi: 10.1109/access.2024.3363075.
[12] A. D. Elbouzidi, A. Artiba, R. Pellerin, S. Lamouri, E. T. Valencia, and M.-J. Bélanger, "The Role of AI in Warehouse Digital Twins: Literature Review," Applied Sciences, vol. 13, no. 11, p. 6746, 2023, doi: 10.3390/app13116746.
[13] B. Zyoud and S. L. Lutfi, "The Role of Information Security Culture in Zero Trust Adoption: Insights From UAE Organizations," IEEE Access, vol. 12, pp. 68775–68790, 2024, doi: 10.1109/access.2024.3402341.
[14] N. A. Ahmad, S. M. Drus, and H. Kasim, "Factors That Influence the Adoption of Enterprise Architecture by Public Sector Organizations: An Empirical Study," IEEE Access, vol. 8, pp. 113162–113181, 2020, doi: 10.1109/access.2020.2996584.
[15] A. A. Al-Kadhimi, M. M. Singh, and M. N. A. Khalid, "A Systematic Literature Review and a Conceptual Framework Proposition for Advanced Persistent Threats (APT) Detection for Mobile Devices Using Artificial Intelligence Techniques," Applied Sciences, vol. 13, no. 14, p. 8056, 2023, doi: 10.3390/app13148056.