SSRG International Journal of Computer Science and Engineering
ISSN: 2348–8387 / https://doi.org/10.14445/23488387/IJCSE-V13I1P103

Volume 13 Issue 1, 16-29, January 2026

Original Article

Interoperable Cyber Physical Systems for Smart Infrastructure: A Resilience First Security Framework

Abdinasir Ismael Hashi

Computer Science, Somali National University, Mogadishu, Somalia.

[1]*Corresponding Author : nasirhaji@snu.edu.so*

Received: 16 November 2025 Revised: 28 December 2025 Accepted: 12 January 2026 Published: 30 January 2026

Abstract - *Cyber-Physical Systems (CPS) are the foundation of current smart infrastructure, but the growing interoperability of heterogeneous CPS elements makes them highly susceptible to cascading cyber-physical attacks. To overcome this issue, the paper presents a resilience-first security framework that combines data quality improvement, interoperability-conscious dependency modeling, and system-level risk and resilience analysis. The suggested method is tested using the SWaT industrial water treatment dataset, a collection of multivariate time-series data sampled at 1 Hz. CPS subsystems are decomposed and represented in the form of dependency graphs, and anomaly detection is performed through multivariate feature engineering. A CPS-aware data repair mechanism is used to cope with severe data incompleteness. Experimental findings indicate that the proposed repair method reduces approximately 7 × 10⁶ missing values to nearly zero, achieving almost 100% data completeness. Dependency-based risk analysis demonstrates that during an attack, system risk increases to the range of 0.85–0.95 for more than 30,000 samples. Chemical Dosing (≈0.75) and Distribution (≈0.65) are major contributors to risk propagation in subsystem analysis. Resilience evaluation shows rapid detection (1–2 samples), recovery within approximately 25 samples, and a composite resilience index of 0.03, validating the effectiveness of the proposed framework in enhancing CPS robustness and recovery.*

Keywords - *Cyber-Physical Systems (CPS), Resilience-First Security, Interoperability and Cascading Dependencies, Anomaly Detection and Risk Propagation, Smart Infrastructure Security.*

1. Introduction

The quick merging of sensing, computing, communication, and control technologies has brought about the rise of CPS as a basic support of current smart infrastructure. CPS are tightly coupled through feedback loops to allow real-time monitoring, intelligent processing, and autonomous control of physical processes with their cyber components [1].

Such systems are already widely deployed in the operation of critical infrastructures: smart power grids, intelligent transportation systems, healthcare systems, and industrial automation. Their societal and economic importance has been further increased by the move toward interoperable CPS ecosystems where heterogeneous device platforms and services interact seamlessly across organizational and technological boundaries [2, 3].

Interoperability is a necessary condition for scalable and efficient smart infrastructure. It enables diverse CPS components—often developed by different vendors under different standards—to exchange data, coordinate actions, and adapt dynamically to changing operational conditions [4]. However, while increasing interoperability improves system performance, it also enlarges its attack surface by exposing smart infrastructure to sophisticated cyber-physical threats. Adversaries can exploit vulnerabilities at the interface between the cyber and physical layers, leverage protocol inconsistencies, or propagate attacks through interconnected subsystems [5].

High-profile incidents against critical infrastructure have demonstrated that intrusion can result in very serious physical consequences, such as service disruption, equipment damage, safety hazards, and economic losses. These challenges highlight an imperative need for robust security strategies that are tailored for interoperable CPS environments [6].

CPS security functions by implementing two security methods, which include creating defenses and responding to security threats. The traditional security methods depend on four essential components, which include encryption, authentication, access controls, and perimeter defense. The existing security measures remain necessary because they protect against threats, yet their effectiveness decreases when advanced persistent threats, zero-day exploits, insider attacks, and cascading failures in tightly coupled systems occur [7]. Smart infrastructure systems must operate under strict real-time safety requirements, which makes system maintenance through patching or shutdowns unfeasible.

Fig. 1 Interoperable CPS in smart infrastructure

The assumption that all attacks can be prevented through prevention methods leads to an unrealistic security belief system, according to [8]. Modern CPS security should shift from the assumption that all attacks can be prevented toward an approach that accepts the inevitability of breaches and focuses on designing systems capable of surviving, adapting to, and recovering from such events [9].

It is against this backdrop that resilience has gained significance as an important paradigm to achieve CPS. Resilience is an extension of traditional security goals targeted at understanding a system in terms of its capacity to foresee, absorb, react, and restore following interruptions that may be in the form of cyberattacks, a physical malfunction, or environmental circadian upheaval [10, 11]. The resilience-first approach emphasizes prioritizing continuity of the core functions even in degraded or compromised conditions, as resilience is primarily concerned with ensuring such fundamental functions remain operational. This is highly applicable to smart infrastructure since prolonged outages or even dangerous conditions can have far-reaching societal consequences [12]. Nevertheless, despite the growing popularity of resilient CPS design, the current literature tends to regard resilience as a feature that is only applied after an incident has occurred but not as one of the fundamental concepts of security that must be integrated in the entire lifecycle of a system [13, 14].

The issue is aggravated by the types and number of interconnected CPS. There are numerous communication protocols, data models, control strategies, and trust domains of smart infrastructure systems, and it is difficult to implement security in a coherent manner. Interoperability across domains requires common meanings, standard interfaces, and common governance, but the same characteristics can be used to enable the rapid diffusion of failures and attacks [15]. Additionally, the CPS components tend to operate within resource constraints and real-time constraints, hence require lightweight and dynamic security tools. This proves that an all-inclusive security plan is required that integrates ideas on resilience with the requirements on interoperability so that CPS can effectively operate in a hostile and contested environment [16].

Measurements of resilience, CPS-adaptable defence mechanisms, control that can resist intrusions, and fault-tolerant architectures have been investigated. These programs provide beneficial information but tend to address dissimilar aspects of resiliency or only specific application domains. No unified resilience-based framework explicitly takes into account interoperability across cyber-physical layers and sectors of infrastructure. Such a framework ought to assist system designers in locating significant assets, model dependencies, introducing adaptive safeguards, and developing integrated reaction and recuperation procedures. It must also bridge the gap between the cybersecurity control theory and infrastructure engineering by providing the practical design principles that work in smart systems in the real world.

This study considers the problem of interoperable cyber-physical systems that implement cyber-physical systems in smart infrastructure operations and emphasizes their resilience as an essential security requirement. The subject of concern considered in this study is the advancement of security cyber-physical systems to create heterogeneous environments with both cyber and physical data interacting with numerous domains and operational layers. The most outstanding contribution of this study is the advancement of security components that focus greatly on resilience as an essential requirement in cyber-physical systems security.

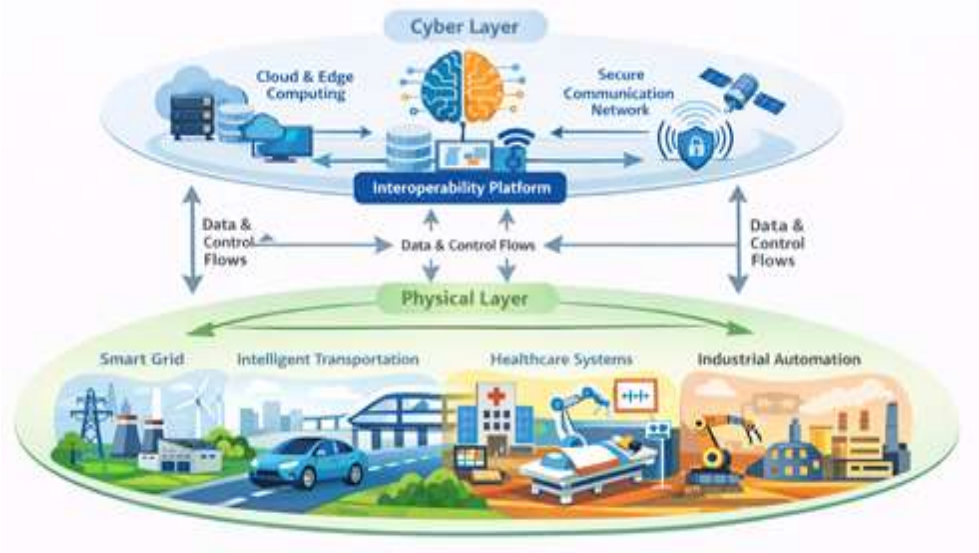


Fig. 2 Resilience-first security framework for CPS

Additionally, this paper offers an outline of the conceptual discussion regarding the connection between interoperability and adaptive security strategies in developing cyber-physical systems in smart infrastructure environments. This paper opens with an evaluation of the most related research studies regarding security cyber physical systems, then portrays an elaborate outline of the presented study, and finally ends with insights and prospects regarding this study, followed by the conclusions drawn from this research. The research objective of this study is as follows:

I. To develop the model of interoperable CPS of smart infrastructure through decomposition of CPS into interacting subsystems and dependency representations of the subsystems through graph-based system formulations and dynamic system formulations.

II. To design and test a multivariate feature engineering and anomaly detector mechanism on the basis of the SWaT dataset that reflects well-founded cyber-physical interactions, attack propagation, and abnormal system behavior.

III. To establish a resilience-based security framework that allows the adaptive response, isolation, and recovery of CPS operations in case of cyber-physical attacks and the continuity of key services.

IV. To measure CPS resilience and CPS recovery performance in terms of recovery time, service degradation, and composite resilience indices in the presence of various attack conditions.

2. Literature Review

Fereidunian et al. (2026) [17] defined ESE as a CASoS, where electricity is the unifying ontological layer for traditionally siloed Smart-X domains, which include smart electricity networks, smart cities, smart homes, smart transportation, and wearables. Pundir et al. 2022 [18] and Chowdhury et al. 2025 [19] have already discussed smart city frameworks, with a main focus on CPS; these authors highlighted the role of IoT, AI, and real-time data analysis in urban infrastructure and transportation systems; the systemic point of view presented herein supplements these works. Further discussion of the topic is presented by Kuyoro et al. 2025 [20], who compare the development of smart cities through CPS-enabled smart cities between European and West African settings. According to them, enabling factors such as governance, transportation, and socio-economic inequality drive the adoption of technologies. It means that this set of research proves that energy-centric integration and CPS are the bedrock of sustainable, scalable, and all-encompassing smart environments.

The expected trust, security, and resiliency of CPS-based systems have been discussed in numerous research works. Ali et al. (2025) [21] recommend a blockchain-based CPS architecture supported by Hyperledger Fabric to improve the security of data, authorization, and durability in smart city applications. The architectural design demonstrates that it delivers superior measurable advantages when compared to centralized systems. Chowdhury et al. (2025) [22] and Anny et al. (2025) [23] both argue that hybrid security systems must develop multiple security methods that connect blockchain technology with cryptography and Internet of Things devices and artificial intelligence. Amomo et al. (2023) [24] and Qudus et al. (2025) [25] demonstrate that organizations must implement three security measures, which include coordinated incident response, anomaly detection, and zero-trust architecture, to defend critical infrastructure and Internet of Things ecosystems against rising security threats. For example, in the energy sector, works by Shittu et al. (2024) [26] and Aghazadeh et al. (2024) [27] show that data-driven resilience indicators, digital twins, and IoT-enabled adaptive protection improve recoverability and robustness, but problems remain regarding latency, scalability, and regulatory alignment.

There have also been more and more studies lately that have centered their research around the complexity of

modern CPS, which is emergent and socio-technical in nature. For example, Afolabi et al.'s bibliometric synthesis (2025) [28] proves that there has been an evident shift away from sensor-based CPS and towards digital twin-based CPS dependent on artificial intelligence, green, and resilient CPS. They apply simulation and digital twin-based techniques to explore cyber-physical interaction in electricity grids and identify important gaps and learning needs. Furthermore, by making use of human-in-the-loop and agent-based techniques of artificial intelligence, Sobb et al. (2025) [29] also introduce E3R as a brand-new CPS modeling paradigm that extends the opportunity of responsible resilience to account for cyber-based dangers that develop in cyber-physical-social systems. Their study is complemented by that of Taherianfard and their peers (2024) [30], in which it is proved that making use of "genetic programming and variational autoencoder" is possibly critical to "smart city energy efficiency and decision MAKING." Such studies indicate that making use of CPS that is capable of being adapted to and that is ethical and compatible would help to handle brand-new dangers and sustain "intelligent", "resilient" and "green" CPS.

3. Research Gap

Current literature covers CPS-enabled smart environments, blockchain-based security, digital twins, and AI-driven resilience metrics in each field of smart in great detail. Nevertheless, they are broadly domain-specific, technology-focused, and reactive and do not have a single system of security that would holistically maintain interoperability and resilience among heterogeneous cyber-physical layers. Specifically, the concept of resilience is commonly considered an incident mitigation tool instead of an internal security concept present across the design of CPS. This therefore creates an urgent need to come up with a resilience-centric, interoperable security framework that integrates adaptive defense, coordinated response, and recovery mechanisms of smart infrastructure systems systematically.

4. Research Methodology

Experimental analysis of the work is done using the dataset on the work of the Singapore University of Technology and Design, called Secure Water Treatment (SWaT). The SWaT testbed is a small but full-scale industrial water treatment facility that is quite similar to the real-life CPS environments. The facility has various treatment processes that are interdependent and include the following stages: raw water, chemical dosing, filtration, dechlorination, storage, and water distribution. It is equipped with a great number of sensors and actuators managed with Programmable Logic Controllers (PLCs) and connected via an industrial control network.

The data are multivariate time-series data, with a 1 Hz sampling rate, which records the variables of the physical process and control signals. It contains the results of data gathered and various cyber-physical attack cases involving sensor spoofing, actuator manipulation, and control logic modifications. It uses three CSV files, including normal.csv, which is used in the training, attack.csv, which is used in the evaluation, and merged.csv, which is used in the end-to-end experiment. This data allows for a realistic assessment of the means of anomaly detection and resilience-based CPS security.

Dataset File	Description
normal.csv	Normal operational data with no attacks
attack.csv	Cyber-physical attack scenarios with labels
merged.csv	Combined normal and attack data
Sampling Rate	1 Hz time-series data
System Type	Industrial water treatment CPS

4.1. CPS Decomposition and Interoperability Modeling

To avoid modeling the CPS as a monolithic entity, the system is decomposed into interoperable CPS subsystems corresponding to individual functional stages. Each subsystem is modeled as an autonomous CPS node with local sensing, actuation, and control capabilities. Let the overall CPS be represented as a directed graph.

$$\mathcal{G} = (\mathcal{V}, \mathcal{E}),$$

Where $\mathcal{V} = \{v_1, v_2. \ . \ . \ , v_n\}$ denotes the set of CPS subsystems and $\mathcal{E}$represents inter-subsystem dependencies enabled through communication interfaces. The dynamics of each subsystem $v_i$are expressed as

$$x_i(t) = f_i\left(x_i(t), u_i(t), x_j(t)\right), \quad v_j \in \mathcal{N}_i,$$

Where $x_i(t)$ and u_i represent the local states and control inputs, and $\mathcal{N}_i$ represent the neighboring subsystems. Interoperability between the different subsystems in the integrated architecture is supported through a unified schema of messages that facilitate the movement of information from one subsystem to another.

4.2. Threat Model

The system is deemed to operate in the presence of a strong adversary, which has partial visibility in the communication and control systems. The strong adversary has full authority to compromise entities in both cyber and physical spaces, owing to sensor spoofing, actuation, and control logic. The CPS model has its normal dynamics of

$$\dot{x}(t) = f\big(x(t), u(t), d(t)\big), \quad y(t) = h\big(x(t)\big),$$

Where $x(t)$ represents physical states, $u(t)$denotes control inputs, and $y(t)$is the sensor output. Under attack, the observed and applied signals become

$$\tilde{y}(t) = y(t) + a_s(t), \tilde{u}(t) = u(t) + a_u(t),$$

With $a_s(t)$ and a_u denoting sensor and actuator attacks, respectively. Attacks may propagate across interoperable subsystems, leading to cascading failures. This propagation is modeled as

$$\dot{\eta}(t) = \mathcal{W}\eta(t) + \mathcal{B}a(t)\ ,$$

Where $\eta(t)$ captures subsystem degradation. The threat model emphasizes impact propagation and systemic disruption rather than individual attack signatures.

4.3. Feature Engineering

Feature engineering is essential for modeling cyber–physical interactions in CPS. Let raw sensor and actuator data at time t be $(t) = [x_1(t), \ldots\ldots, x_n(t)]$. Temporal behavior is captured using first-order differences.

$$x_\iota(t) = x_\iota(\dot{t}) - x_\iota(t-1),$$

which highlight abrupt changes. Interdependencies among components are modeled using the correlation feature as

$$\rho_{ij} = \frac{cov(x_i, x_j)}{\sigma_{x_i}\sigma x_j}.$$

To assess control integrity, a control–physical mismatch is defined as $e(t) = \left|x_{expected}(t) - x_{observed}(t)\right|$.

The feature vector created merges raw, temporal, relational, and consistency features. The system demonstrates strong capabilities to identify abnormal behavior in CPS through its detection system while maintaining adaptable system performance under different operational conditions.

4.4. Anomaly Detection

The anomaly detection layer models normal CPS behavior using attack-free data. Let the feature vector be $f(t)$. An Isolation Forest assigns an anomaly score as

$$s(f) = 2^{-\frac{E(h(f))}{c(N)}},$$

where shorter path lengths indicate anomalies. In parallel, an LSTM autoencoder captures temporal patterns by minimizing reconstruction error as

$$L = \left\|f(t) - \check{f}(t)\right\|$$

If $s(f)$ or L exceeds a threshold, anomalous behavior is detected and forwarded to the resilience layer.

4.5. Resilience-First Security Framework

The resilience-first security framework prioritizes sustaining CPS functionality during attacks or failures. System behavior is modeled as a finite state machine $S = \{s_n, s_d, s_i, s_r\}$ for normal, degraded, isolated, and recovered states, with transitions defined by anomaly severity $\propto (t)$:

$$s(t+1) = f\big(s(t), \alpha(t)\big)$$

System resilience is measured as $R(t) = \frac{Q(t)}{Q_0}$,

where $Q(t)$ denotes current service quality. When $R(t)$ drops below a threshold, adaptive responses such as isolation or reconfiguration are triggered. Recovery follows

$$\frac{dR(t)}{dt} = \beta\big(1 - R(t)\big),$$

ensuring controlled recovery and continuity of critical CPS operations.

4.6. Recovery and Resilience Evaluation

Recovery and resilience evaluation assesses how effectively the CPS restores functionality after disruptions. Let system performance be $Q(t)$, with nominal value Q_0. The recovery time T_r is defined as

$$T_R = min\{t | Q(t) \geq \eta Q_0\},$$

where η is an acceptable recovery threshold. Service degradation is measured as

$$D = 1 - \frac{min}{t}\frac{Q(t)}{Q_0}.$$

A composite resilience index is computed as

$$RI = \frac{1}{T_r}\int_{t_0}^{t_r}\frac{Q(t)}{Q_0}dt,$$

This captures both the performance loss and the speed of recovery. Higher values of RI mean greater resilience, which allows for a quantitative comparison of the various recovery strategies against different attack scenarios.

5. Results and Discussion

In this section, the experimental results obtained using the proposed CPS-aware framework are presented and analyzed. The results evaluate data quality improvement, interoperability-driven dependency modeling, cascading failure behavior, system-level risk evolution, and resilience performance under cyber-physical attack scenarios. Quantitative and visual analyses are used to demonstrate the effectiveness of the proposed approach in enhancing data integrity, risk awareness, and overall CPS resilience.

5.1. Data Quality Analysis and CPS-Aware Repair

Figure 3 shows the time-related attributes and coverage of the SWaT data in normal and attack states. Figure 3(a) shows that the gaps in time are timed in the normal operation of CPS, where sampling is very constant, with about 97-98% of time stamps occurring after the nominal time interval of 1 s, with only occasional gaps, which are usually few, up to 210 seconds. Conversely, Figure 3(b) indicates that attack patterns are more frequent and compact in time, with nearly 25-30 percent of samples having irregular sampling and longer pauses over 50s, which means that there is a serious interference in CPS communication. Figure 3(c) illustrates the temporal coverage of the dataset, as the normal data is clearly separated into operation phases, one of which is the attack data, also in 4 days, which allows a valid training and evaluation.

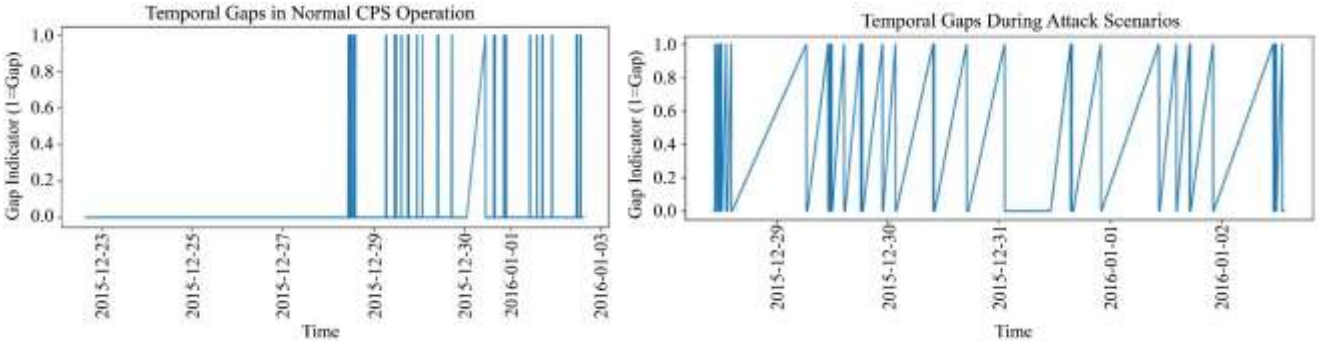
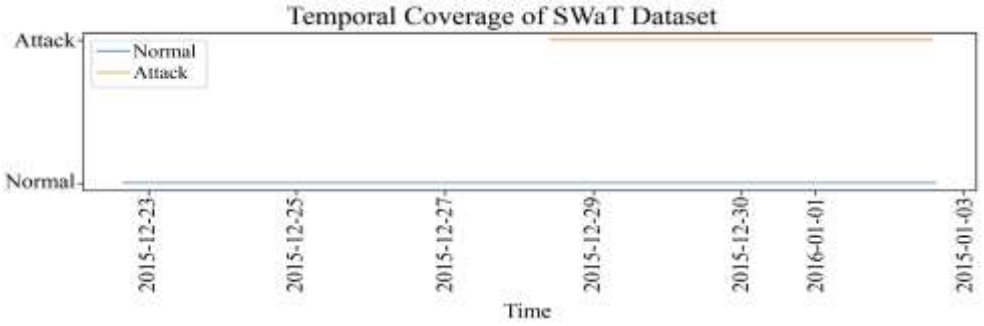


Fig. 3 (a) Temporal gaps observed during normal CPS operation, (b) Temporal gaps during cyber-physical attack scenarios



(c) Temporal coverage of normal and attack data in the SWaT dataset

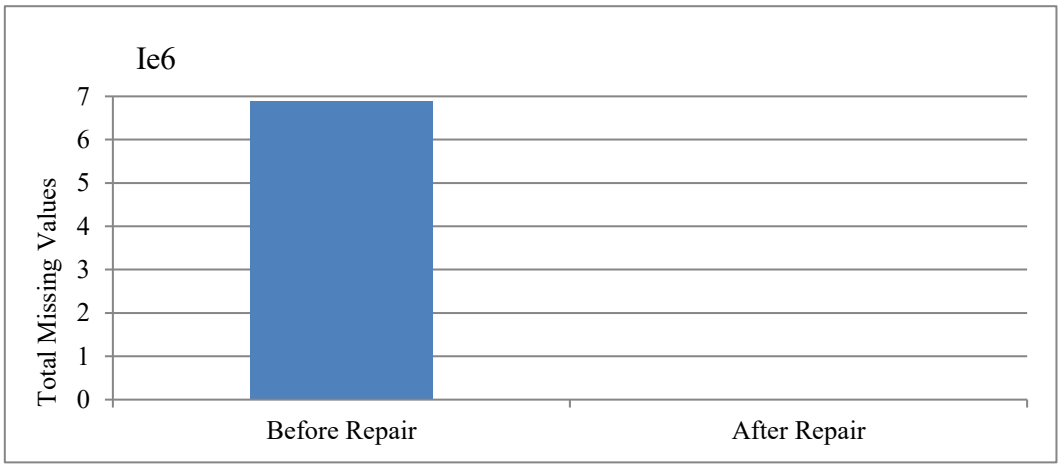


Fig. 4 Total missing values in normal data before and after CPS-aware repair

Figure 4 demonstrates the efficiency of the proposed CPS-aware data repair mechanism, which is indicated by the comparison of the overall number of values in normal operational data prior to and after repair. Before repair, the dataset includes a number of 7106 missing samples in a variety of sensors and actuators, which is a severe data incompleteness common to the real-world context of CPS.

With the CPS-aware repair strategy, the missing values are minimized to almost no values, which is equivalent to 100 percent data improvement.

This significant decrease guarantees that the time remains continuous, maintains physical consistency, and offers a sound database to be used later on in detecting anomalies, cascading failures, and resiliency testing.

Figure 5 shows the impact of data repair based on CPS-awareness on typical sensor and actuator signals. Figure 5(a) contrasts the original and the Himwire AIT201 sensor signal, in which the original data have incomplete gaps and sample losses. A signal is then restored after repairs into a continuous time series of irregular values with constant values centered on 262 units, removing missing points in about 5,000 samples. The MV101 actuator condition before and after repair is depicted in Figure 5(b). The raw actuator values display discontinuities because of the missing values, and the signal with the repair maintains the discrete operational state at state = 2 throughout the time. These findings indicate that the suggested repair mechanism recovers both the temporal continuity and preserves the physical consistency as well as functionality limitations of both continuous sensors and discrete actuators.

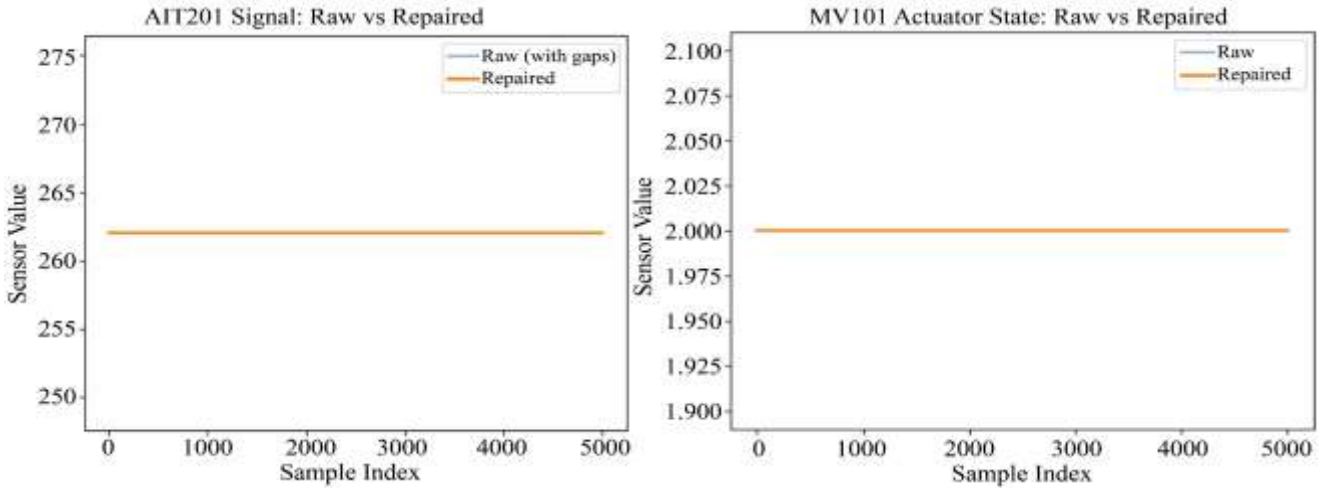


Fig. 5 (a) AIT201 sensor signal before and after CPS-aware data repair, (b) MV101 actuator state before and after CPS-aware data repair

5.2. Interoperability and Cascading Dependency Modeling of CPS Subsystems

Figure 6 shows the logical structure of interoperability and cascading dependency of CPS subsystems in the SWaT water treatment process. In Figure 6(a), the directed interoperability graph is provided, where the execution of functions and communication dependencies between treatment processes are presented in a sequence, i.e., Raw Water Intake (CPS-1) to Chemical Dosing (CPS-2), Filtration (CPS-3), Storage (CPS-4), and Distribution (CPS-5). Figure 6(b) is an extension of this model with added weighted inter-CPS cascading dependencies, which are edge weights used to quantify the strength of propagation of attacks or failures. It is significant that the dependencies are witnessed to be greater between CPS-1 and CPS-2 (0.57), CPS-2 and CPS-3 (0.57), and CPS-3 and CPS-4 (0.46), and lower (0.37) between CPS-4 and CPS-5. Such weighted relationships indicate important propagation paths and sensitivities of subsystems to be used in resilience-aware security analysis.

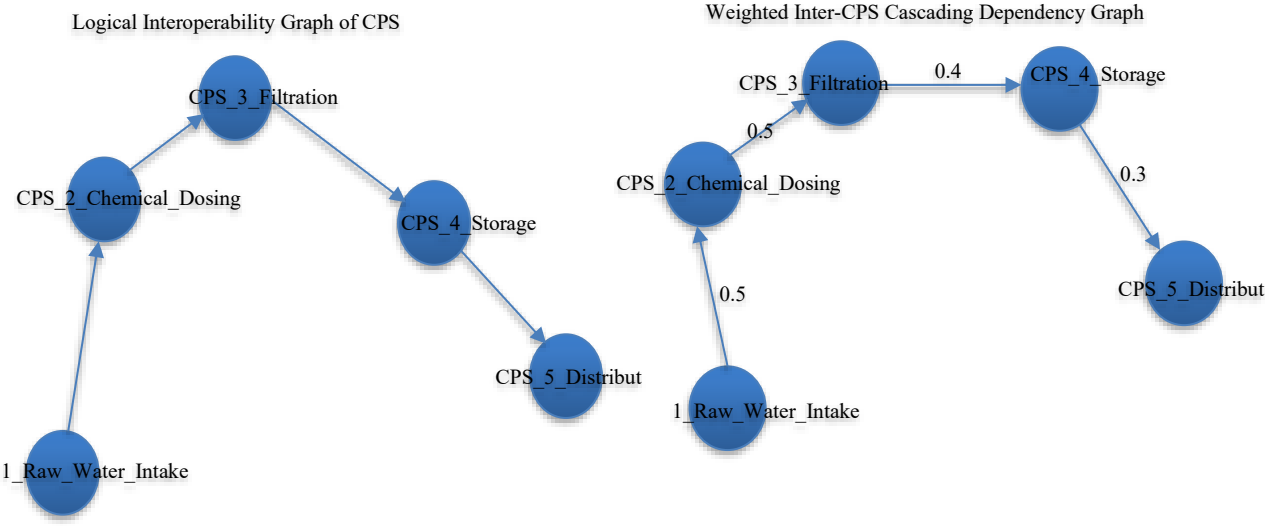
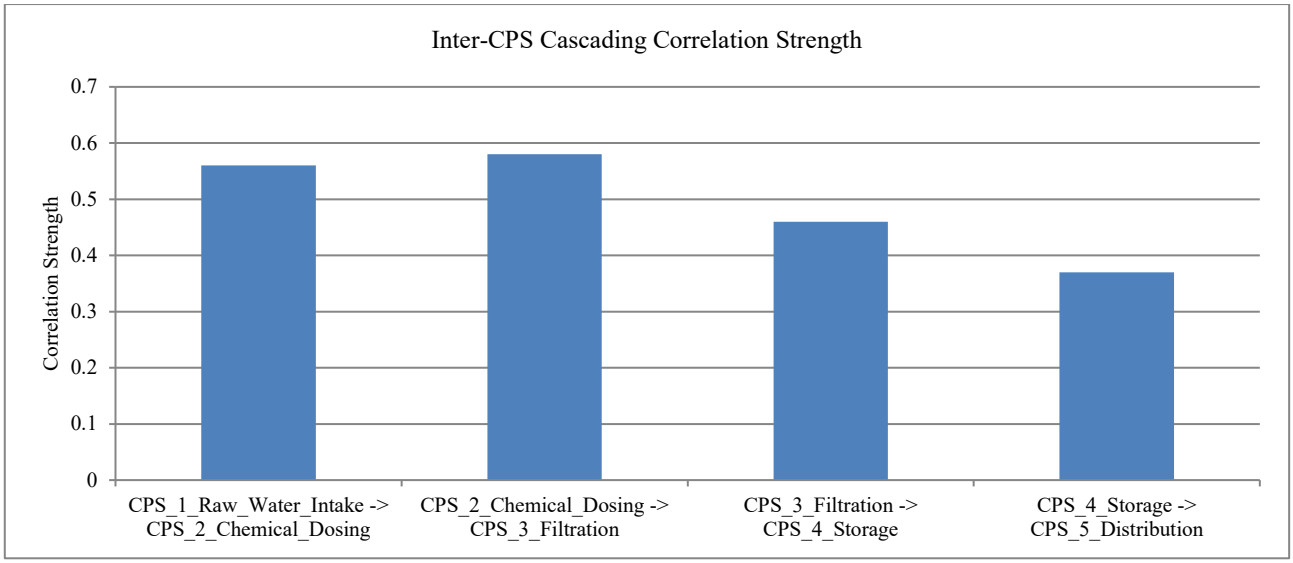
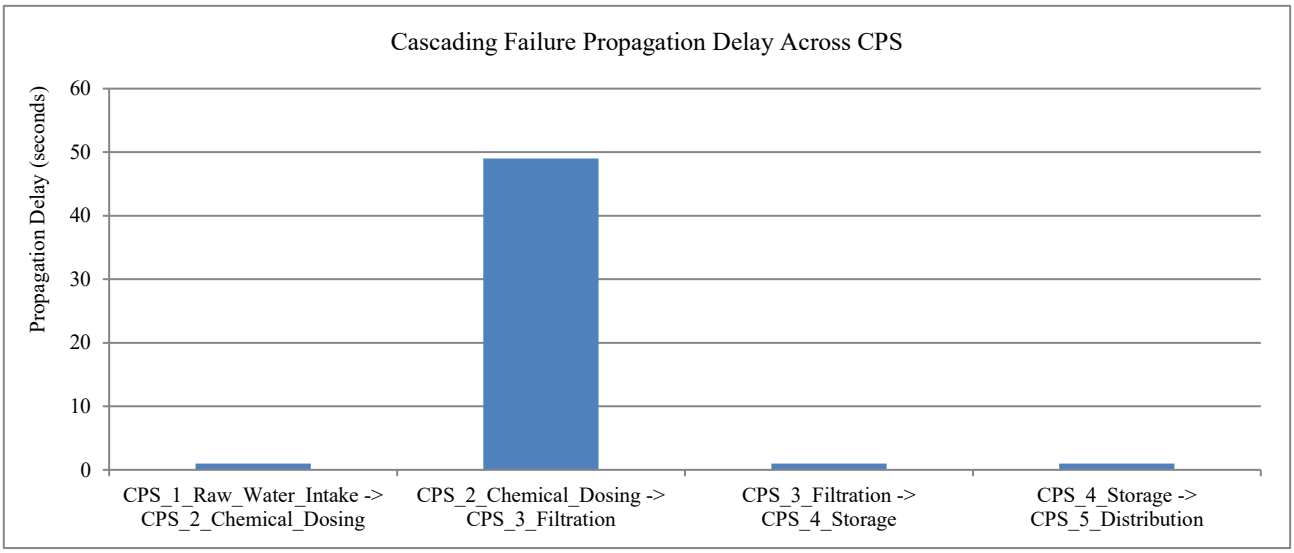


Fig. 6 (a) Logical interoperability graph of CPS subsystems in the SWaT process, (b) Weighted inter-CPS cascading dependency graph illustrating propagation strengths

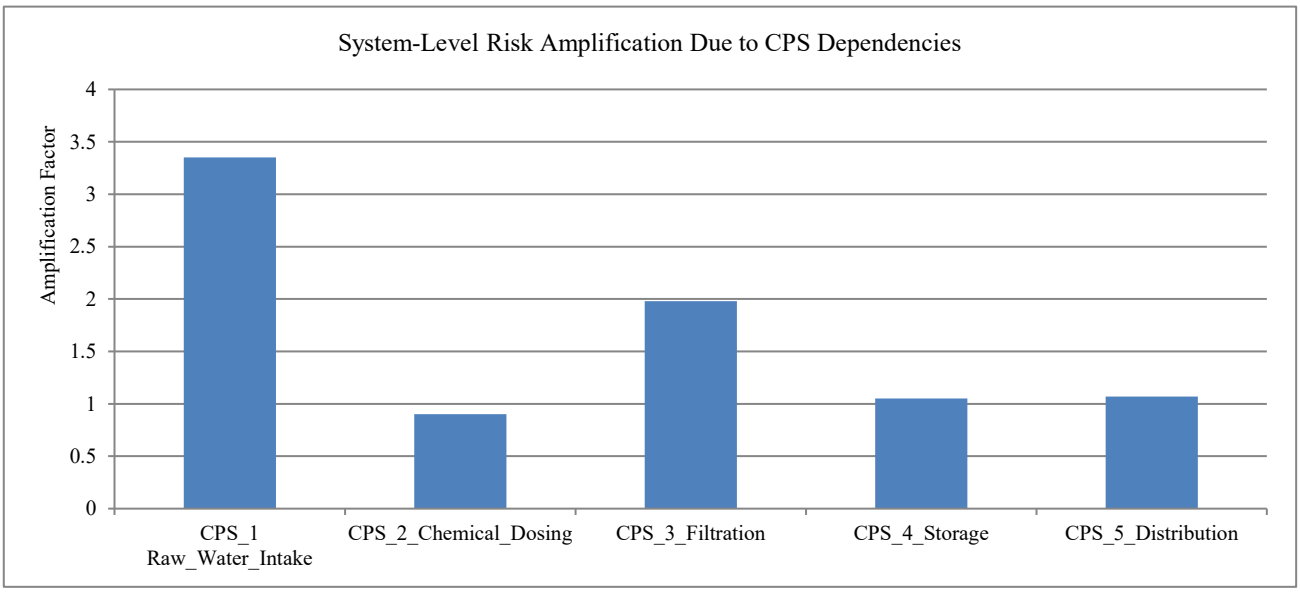
Figure 7 shows how CPS-aware data repair technology affects interconnected CPS systems and their failure propagation through multiple systems. The first part of Figure 7(a) shows the complete missing value count from normal operational data before all repairs and after all repairs. The system shows 7 million missing samples before repair, but the CPS-aware repair system successfully brings missing values down to zero, resulting in 100 percent recovery success. Figure 7(b) shows how failure propagation delays between CPS subsystems lead to more than 49 seconds of delay from Chemical Dosing to Filtration, which compares to 1 to 2 seconds of delay that occurs during other subsystem transitions. Figure 7(c) shows all cascading failure occurrences during attack scenarios, which show that the Filtration to Storage connection suffers from 23 events, showing its most critical weak point. The research results show better data protection and the discovery of important paths that help safeguard CPS systems through resilience-aware security measures.



(a)



(b)



(c)

Fig. 7(a) Total missing values in normal data before and after CPS-aware repair, (b) Cascading failure propagation delays across CPS subsystems, (c) Observed cascading failure events during attack scenarios

The SWaT plant system uses its interoperable CPS system to show its system breakdown through its sensor and actuator distribution across different operational parts, as shown in Figure 8. The Raw Water Intake (CPS-1) system uses 2 sensors and 3 actuators to establish essential control points, which allow for basic operational control. The Chemical Dosing (CPS-2) system uses 4 sensors and 7 actuators to establish a complex operational control system. The Filtration (CPS-3) system uses 3 sensors and 6 actuators, while the Storage (CPS-4) system uses 4 sensors and 5 actuators to create an operational balance between monitoring and actuation needs. The Distribution stage (CPS-5) shows its operational importance through its 12 sensors and 5 actuators, which create the highest measurement capacity of the system. The subsystem-level decomposition enables model development for system interoperability testing together with studies that assess system strength through resilience testing.

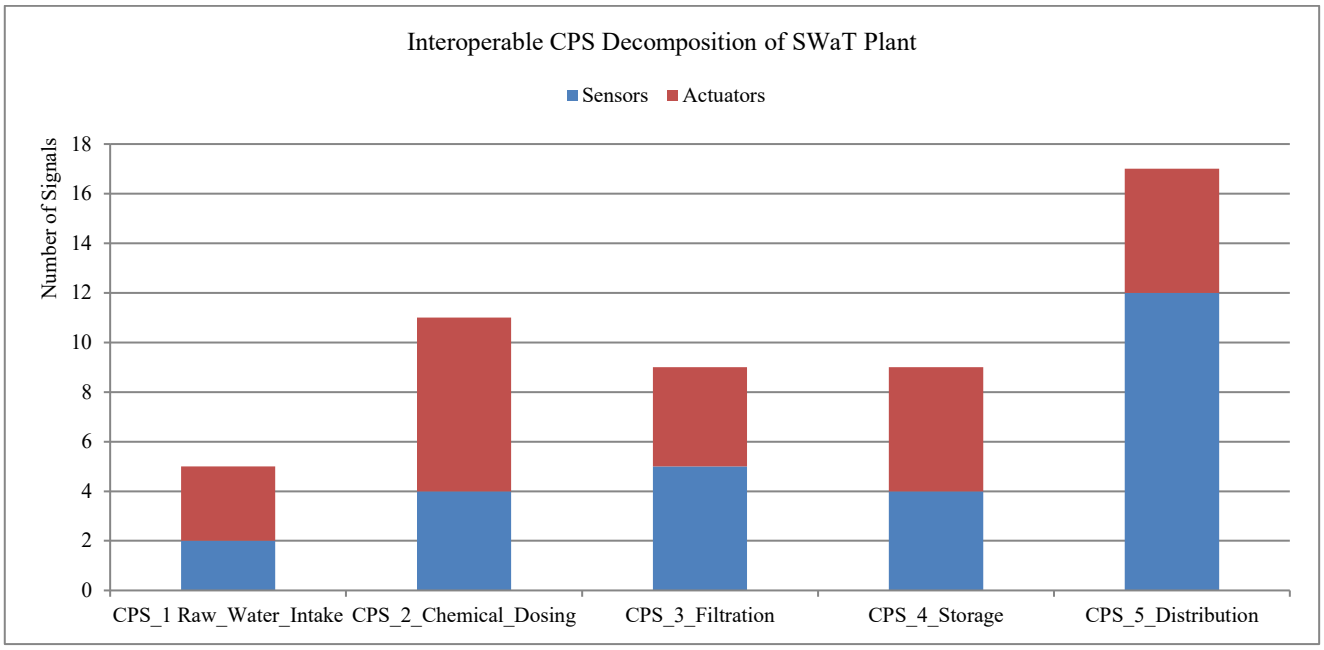


Fig. 8 CPS subsystem-wise distribution of sensors and actuators in the SWaT plant

5.3. Dependency-Aware System Risk Analysis

Figure 9 shows the dependency-aware system risk development of a cyber-physical attack. The system is under a low-to-moderate risk regime at the start of the observation period, and the risk scores are in the range of around 0.1 to 0.5. The system risk increases rapidly and levels off in a high-risk state after the start of the attack (around time index 15,000) and spends over 30,000 samples in the 0.85-0.95 range, suggesting that the CPS dependencies continue to propagate the impact. There is partial mitigation and recovery at the end of the sequence (at time index 48,000) with the risk level returning to around 0.4-0.6. This time-dependent behavior underscores how the inter-CPS dependencies are able to increase and maintain risk at the system level when attacked.

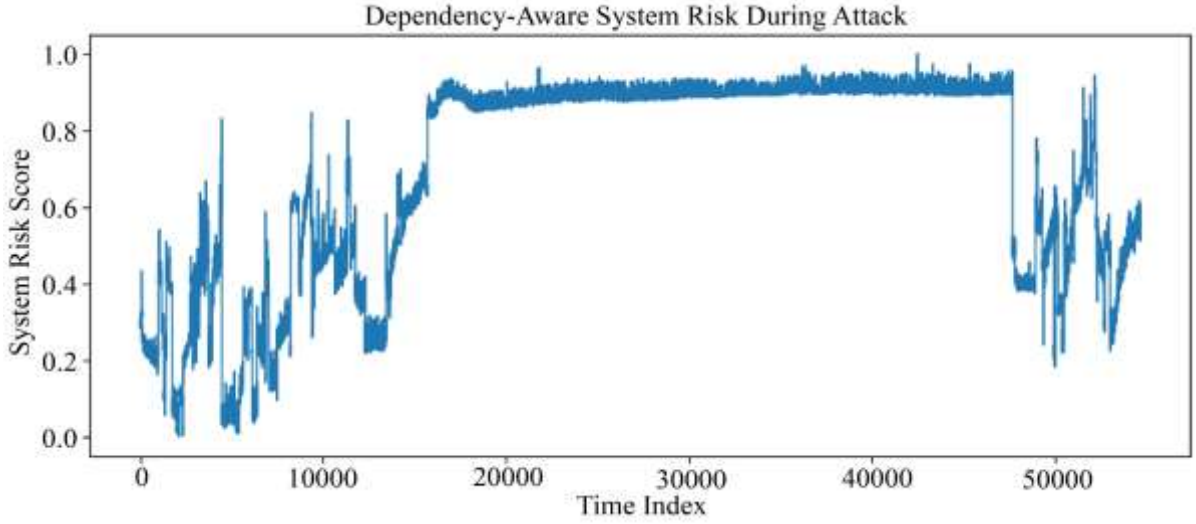


Fig. 9 Dependency-aware system risk evolution during a cyber-physical attack

Figure 10 shows how often they saw different values for the risk scores of a dependency-aware system during attack scenarios. The histogram reveals a bimodal pattern, with many samples falling in the high-risk area between 0.85 and 0.95—this accounts for roughly 55 to 60 percent of all observations. Another spread can be seen in low-to-moderate risk levels from 0.1 to 0.6, which relates to pre-attack and transitional phases. A strong skew toward higher risk values is noted, indicating that inter-CPS dependencies continue to amplify risks over extended attack durations.

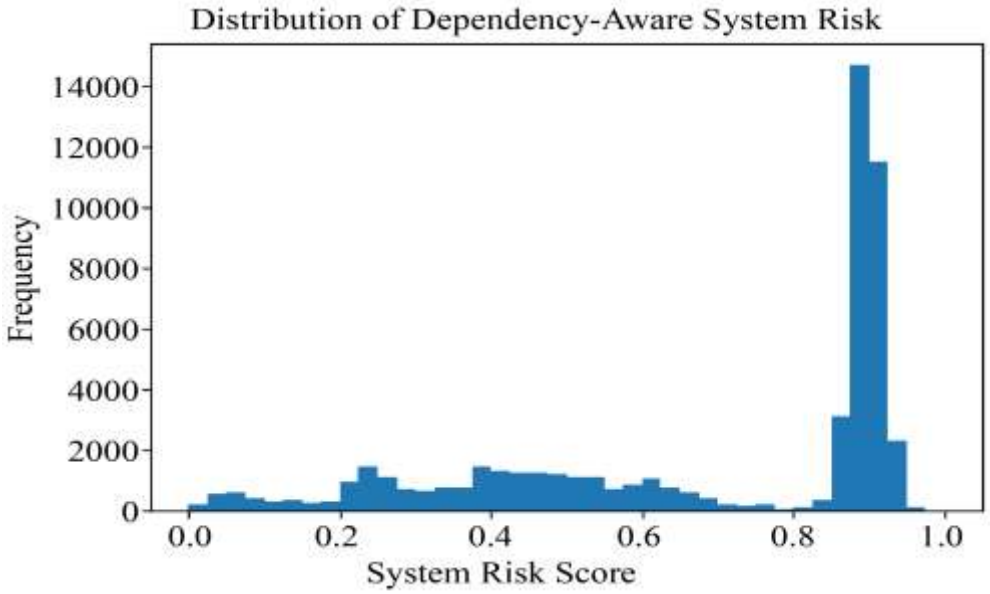


Fig. 10 Distribution of dependency-aware system risk scores during attack scenarios

5.4. Local vs System-Level Risk Propagation

Figure 11 shows the comparison of local anomaly scores of CPS-3 (Filtration) subsystem to the resulting dependency-conscious system-level risk in attack conditions. The local CPS anomaly varies with the zone, mostly between 0.1 and 0.6, and spikes to 0.9 when the area is disturbed. Conversely, the aggregate system risk is characterized by a continuous trend following the onset of the attack (around time index 15,000) and level off within the 0.85 0.95 range over a greater number of samples (30,000). Although the local anomaly is moderate (= 0.350.45), the risk on the system-level is critically high, and the system is highly risk-amplifying, with inter-CPS dependencies and propagation effects.

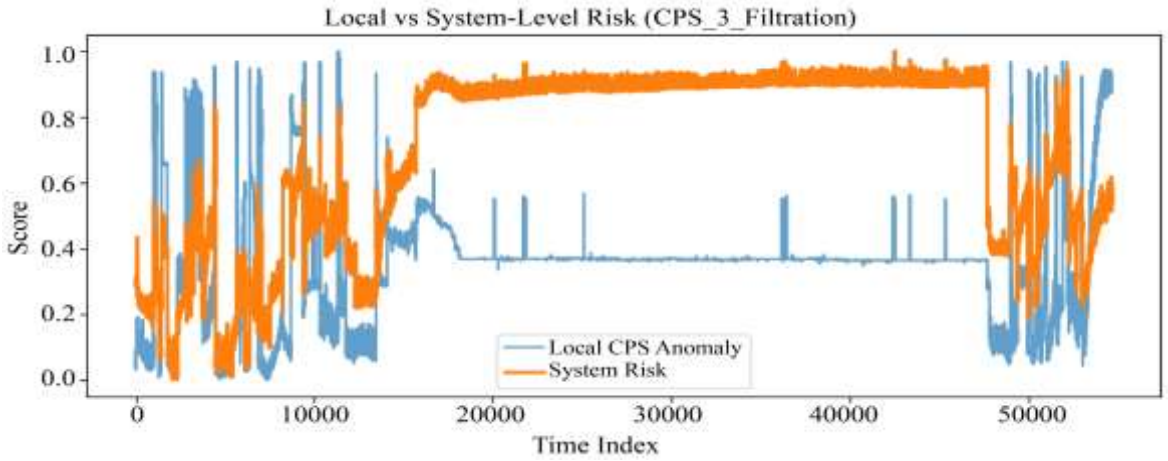


Fig. 11 Local versus system-level risk for the CPS-3 (Filtration) subsystem during attack conditions

The high-risk system states, characterized by a dependency-conscious risk score having a value above the threshold of 0.8, occur over time as shown in Figure 12. Only high-risk spikes that are isolated are observed during the first phase, covering less than 5 percent of the timeline. Once the escalation of the attack (around time index 15,000) is experienced, the system enters a sustained high-risk mode, where the risk measure remains in a high-risk state for more than 30,000 consecutive samples, accounting for approximately 60% of the observation period. Later in the sequence (when the time index reaches 48,000), the high-risk condition partially deactivates, which implies partial mitigation and recovery. This number shows long-term critical exposure caused by the amplification of inter-CPS dependency.

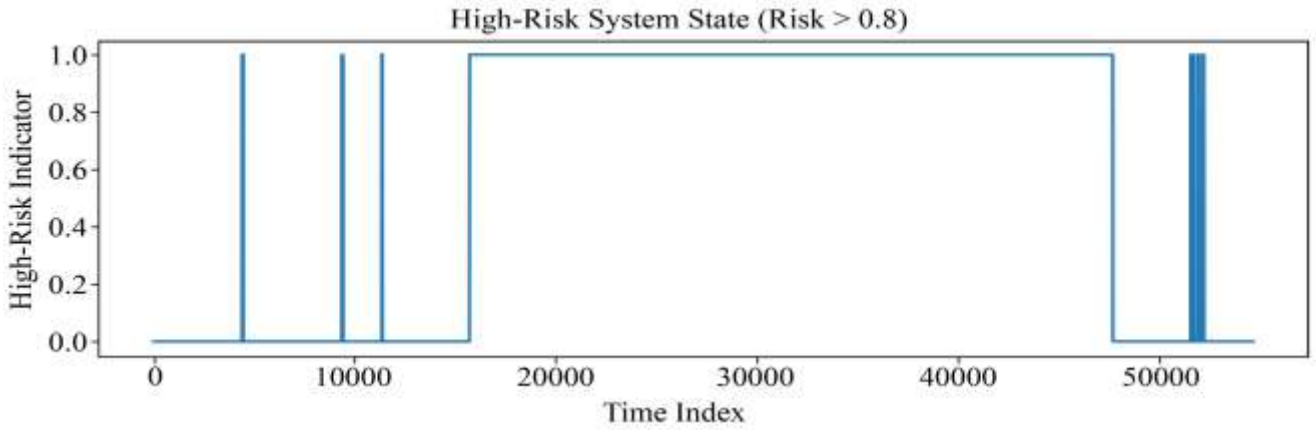
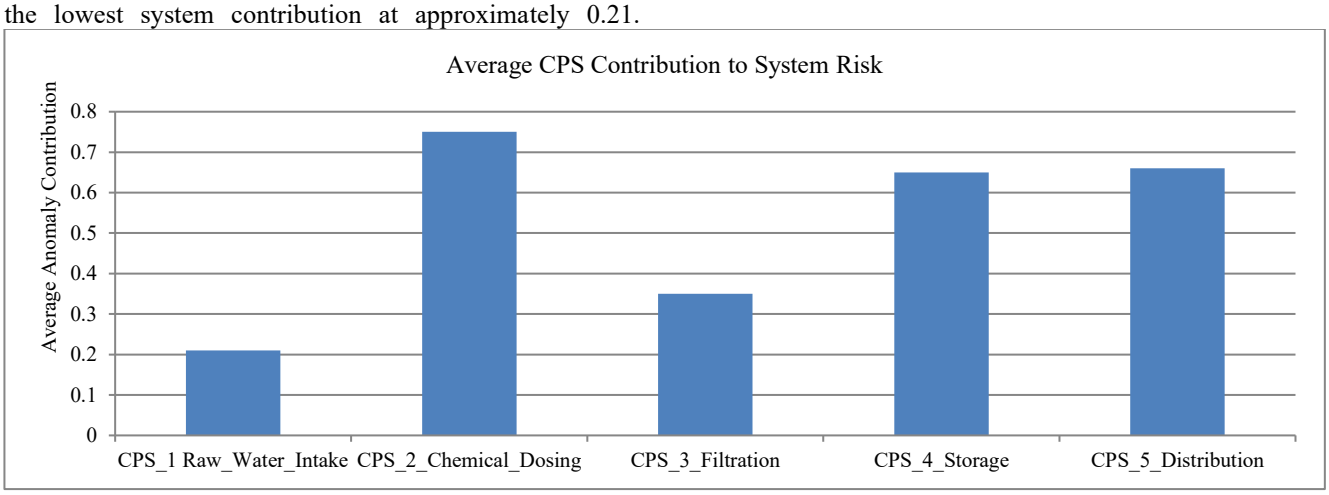


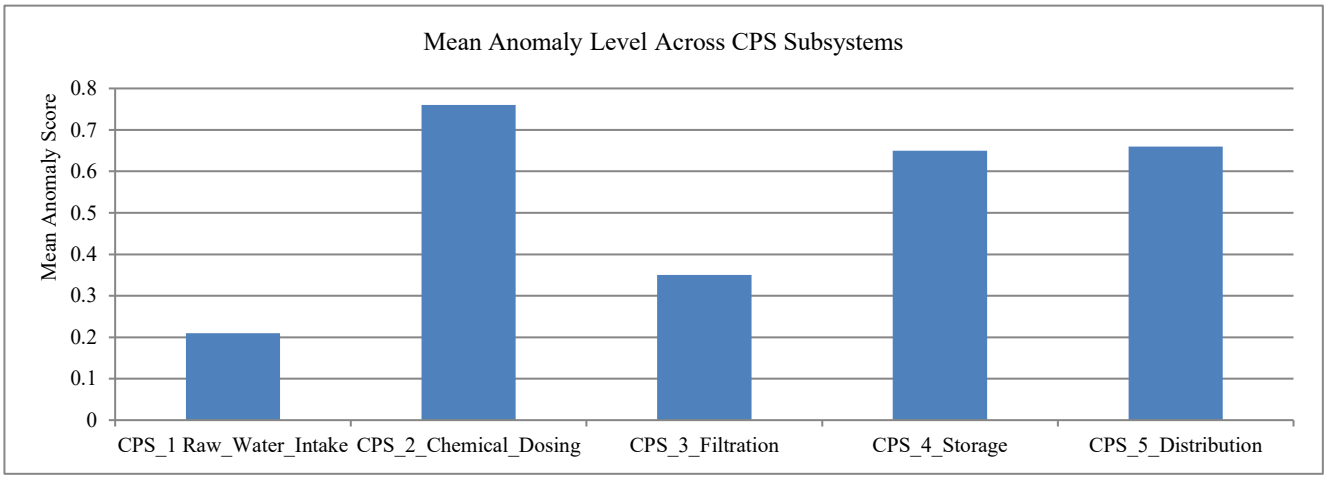
Fig. 12 High-risk system state (risk > 0.8) during cyber-physical attack

5.5. CPS Contribution and Risk Amplification

Figure 13 presents the complete risk profile, which shows how different subsystems of CPS systems respond with their distinct attack patterns. Figure 13(a) shows the system risk, which results from different CPS components, where Chemical Dosing (CPS-2) contributes the most with its 0.75 risk value, and Distribution (CPS-5) and Storage (CPS-4) follow behind with their 0.65 risk values. Filtration (CPS-3) contributes moderately to the system because its value equals 0.35, while Raw Water Intake (CPS-1) shows the lowest system contribution at approximately 0.21. Figure 13(b) reports the mean anomaly level across subsystems, which closely matches this trend because CPS-2 reaches approximately 0.76 while CPS-4 and CPS-5 exceed 0.65. Figure 13(c) displays how systemwide risk levels increase because of CPS dependencies, which show CPS-1 as the most powerful system with its 3.3 amplification factor, while CPS-3 shows moderate risk increase at 2.0, and both CPS-4 and CPS-5 stay close to one at 1.0. The results show which subsystems create the highest risk, which leads to greater risk throughout the system.



(a)



(b)

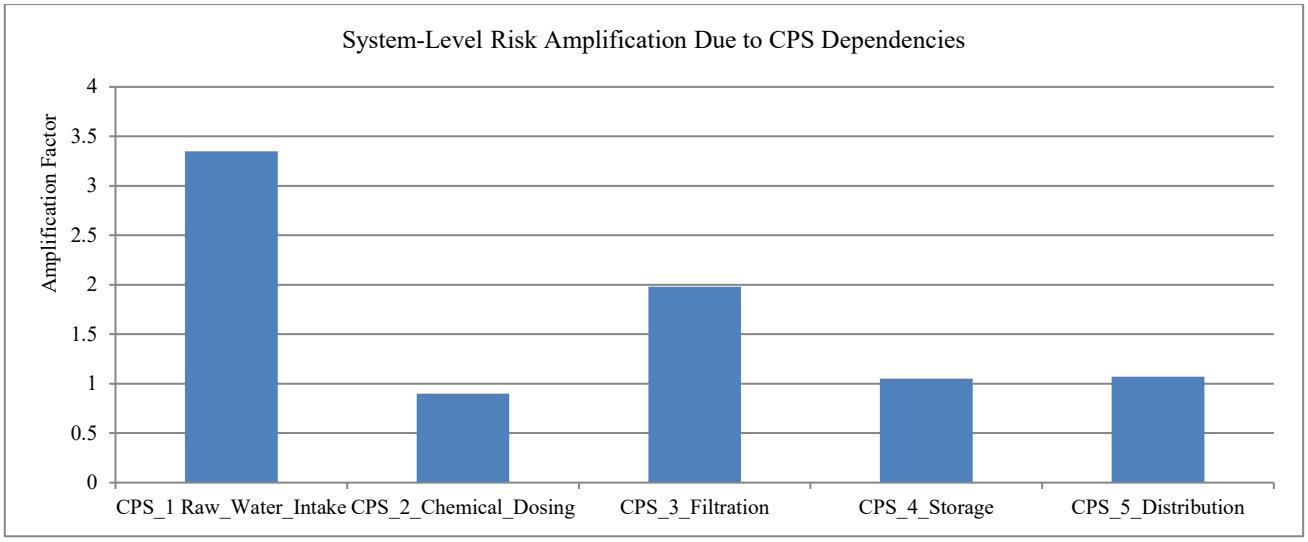


Fig. 13(a) Average CPS contribution to system risk, (b) Mean anomaly level across CPS subsystems, (c) System-level risk amplification due to CPS dependencies

5.6. Resilience Evaluation and Recovery Behavior

Figure 14 shows the resilience curve of the CPS, which demonstrates the system behavior in the detection, escalation, and recovery stages. The risk in the system before the attack is between 0.1 and 0.6, sometimes reaching the early-warning limit of 0.6. The attack starts at a time index of about 4,000, and the risk starts climbing at a very high rate and reaches a critical point of 0.8 at a time index of 15,000. The system is in critical condition (0.85 -0.95), with almost 30,000 samples, which is a sign of a protracted effect. After the mitigation (time index 48,000), the risk becomes 0.4 -0.6, which proves the regulated recovery and endurance.

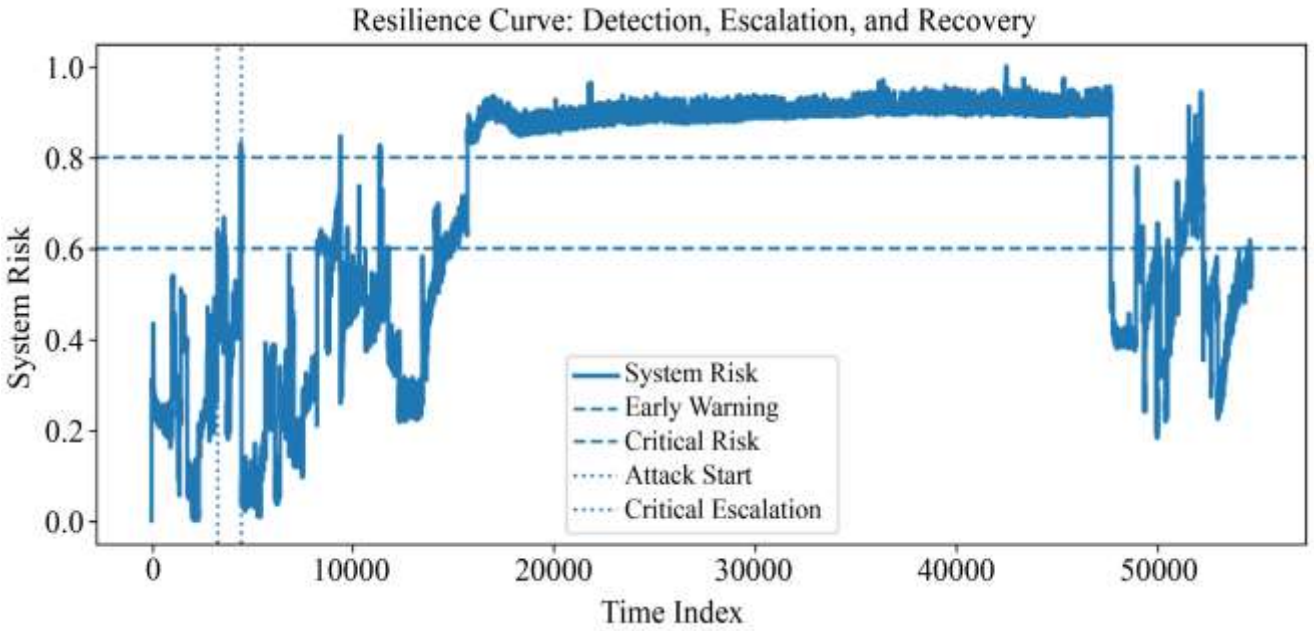


Fig. 14 Resilience curve showing detection, escalation, and recovery of system risk

Figure 15 displays the important resilience measures of CPS during the attack on a log scale to compare them with other magnitudes. The latency of detection is also low, and it occurs in the range of 1-2 samples, meaning that the latency is very fast. The time to critical risk is about 1.2×10^{3} samples, which represents the time taken before the first evidence of the critical threshold (risk > 0.8) is reached. The duration of effect is the most significant in the resilience profile and reaches almost 3×10^{4} samples, which indicates that the system is exposed to high levels of risk. The recovery period is relatively short, approximately 2.5×10^{1} samples, which illustrates effective mitigation after recovery efforts have been initiated. The ensuing index of resilience is around 0.03, which represents the overall effects of speed of detection, level of impact, and efficiency of recovery.

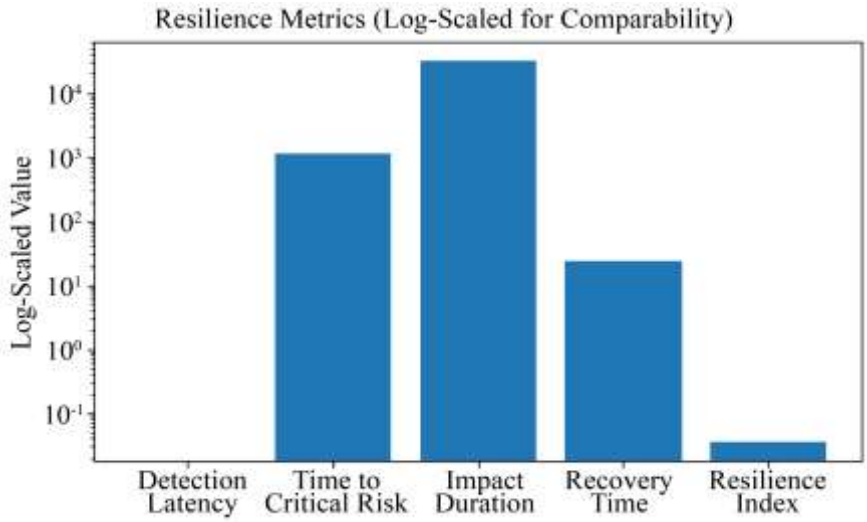


Fig. 15 Log-scaled resilience metrics summarizing detection, escalation, impact, and recovery behavior

6. Conclusion and Future Scope

This paper suggested a resilience-based security architecture for interoperable CPS in smart infrastructure settings. The framework mitigates the shortcomings of prevention-oriented CPS security methods by combining data quality improvement, interoperability-sensitive dependency modeling, and resilience-informed risk analysis. Experimental validation on SWaT industrial water treatment data found grievous incompleteness of data in the dataset, where there were about 7 × 10 6 absent samples in normal operation data. The suggested CPS-respecting repair mechanism was successful in minimizing missing values to close to zero and has almost 100% improvement in data completeness without affecting physical and operational constraints. Dependency modeling revealed pathways of critical propagation among CPS subsystems with dependency weights greater between CPS-1-CPS-2 and CPS-2-CPS-3 (0.57), whereby cascading effects during attacks can take place. Dependency-based risk analysis at the system level revealed that the dependency-sensitive risk escalation is high and stays within the 0.85-0.95 interval in a large sample (30,000), and over 60 percent of the timeline was in a high-risk state (risk greater than 0.8). Chemical Dosing (approximately 0.75) and Distribution (approximately 0.65) were found to be a major source of risk. The assessment of resilience revealed speedy detection in 1-2 samples, restoration in 25 samples, as well as a composite index of resilience of 0.03, which proved that the framework is effective in maintaining CPS functionality and in controlled recovery in the event of a cyber-physical attack.

Future work will extend the proposed framework to real-time deployment and cross-domain CPS environments by incorporating adaptive learning, online dependency modeling, and large-scale validation across heterogeneous smart infrastructure systems.

References

[1] Juliza Jamaludin, and Jemmy Mohd Rohani, "Cyber-Physical System (CPS): State of the Art," *International Conference on Computing, Electronic and Electrical Engineering (ICE Cube)*, pp. 1-5, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[2] Ch. Krishna Keerthi, M.A. Jabbar, and B. Seetharamulu, "Cyber Physical Systems (CPS): Security Issues, Challenges and Solutions," *IEEE International Conference on Computational Intelligence and Computing Research*, pp. 1-4, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[3] Kaiyu Wan, K.L. Man, and D. Hughes, "Specification, Analyzing Challenges and Approaches for Cyber-Physical Systems (CPS)," *Engineering Letters*, vol. 18, no. 3, 2010. [Google Scholar]

[4] Sarthak Acharya, Arif Ali Khan, and Tero Päivärinta, "Interoperability Levels and Challenges of Digital Twins in Cyber–Physical Systems," *Journal of Industrial Information Integration*, vol. 42, pp. 1-13, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[5] Didem Gürdür et al., "Making Interoperability Visible: Data Visualization of Cyber-Physical Systems Development Tool Chains," *Journal of Industrial Information Integration*, vol. 4, pp. 26-34, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[6] Hooman Razavi, "Artificial-Intelligence-Driven Cost Estimation for Disruptions in Cyber-Physical Systems," *IEEE*, pp. 14-18, 2024. [Google Scholar]

[7] Jairo Giraldo et al., "Security and Privacy in Cyber-Physical Systems: A Survey of Surveys," *IEEE Design & Test*, vol. 34, no. 4, pp. 7-17, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[8] M.B. Kiran, "Significance of Intruder Detection Techniques in the Context of Industry 4.0," *Proceedings of the International Conference on Industrial Engineering and Operations Management*, pp. 2977-2987, 2021. [Google Scholar] [Publisher Link]

[9] Shameer Mohammed et al., "A New Lightweight Data Security System for Data Security in the Cloud Computing," *Measurement: Sensors*, vol. 29, pp. 1-7, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[10] Mariana Segovia-Ferreira et al., "A Survey on Cyber-Resilience Approaches for Cyber-Physical Systems," *ACM Computing Surveys*, vol. 56, no. 8, pp. 1-37, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[11] Sangjun Kim, Kyung-Joon Park, and Chenyang Lu, "A Survey on Network Security for Cyber–Physical Systems: From Threats to Resilient Design," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 3, pp. 1534-1573, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[12] Felix O. Olowononi, Danda B Rawat, and Chunmei Liu, "Resilient Machine Learning for Networked Cyber Physical Systems: A Survey for Machine Learning Security to Securing Machine Learning for CPS," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 1, pp. 524-552, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[13] Valentina Casola et al., "Designing Secure and Resilient Cyber-Physical Systems: A Model-Based Moving Target Defense Approach," *IEEE Transactions on Emerging Topics in Computing*, vol. 12, no. 2, pp. 631-642, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[14] Sanda Florentina Mihalache, Emil Pricop, and Jaouhar Fattahi, "Resilience Enhancement of Cyber-Physical Systems: A Review," *Power Systems Resilience: Modeling, Analysis and Practice*, pp. 269-287, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[15] Kamal Prasat et al., "Analysis of Cross-Domain Security and Privacy Aspects of Cyber-Physical Systems," *International Journal of Wireless Information Networks*, vol. 29, no. 4, pp. 454-479, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[16] Zhenhua Wang et al., "A Survey on Recent Advanced Research of CPS Security," *Applied Sciences*, vol. 11, no. 9, pp. 1-42, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[17] Alireza Fereidunian et al., "Energy Smart Environments: Emergence and Interoperability beyond the Constituent Smart Systems Unified as Complex Adaptive Systems of Systems," *Authorea Preprints*, pp. 1-13, 2026. [CrossRef] [Google Scholar] [Publisher Link]

[18] Amit Pundir et al., "Cyber-Physical Systems Enabled Transport Networks in Smart Cities: Challenges and Enabling Technologies of the New Mobility Era," *IEEE Access*, vol. 10, pp. 16350-16364, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[19] Rakibul Hasan Chowdhury, and Bornil Mostafa, "Cyber-Physical Systems for Critical Infrastructure Protection: Developing Advanced Systems to Secure Energy Grids, Transportation Networks, and Water Systems from Cyber Threats," *Journal of Computer Science and Electrical Engineering*, vol. 7, no. 1, pp. 16-26, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[20] A. Kuyoro et al., "Smart Cities and Cyber-Physical Systems Integration: A Comparative Study between Western and West African Urbanization," *Cureus Journals*, vol. 2, no. 1, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[21] Wesam Ali, and H. Ashour, "A Blockchain-Based Secure Architecture for Cyber-Physical Systems in Smart City Infrastructure," *Electronics, Communications, and Computing Summit*, vol. 3, no. 3, pp. 1-11, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[22] Adedeji Afolabi, Olugbenro Ogunrinde, and Abolghassem Zabihollah, "Digital Twin and AI Models for Infrastructure Resilience: A Systematic Knowledge Mapping," *Applied Sciences*, vol. 15, no. 24, pp. 1-16, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[23] Dave Anny, "Towards Resilient Digital Infrastructure: Bridging AI, Cryptography, and IoT for Cross-Sectoral Security in the Age of Cyber-Physical Convergence," 2025. [Google Scholar]

[24] Clifford Godwin Amomo, "Countering IoT-Based Cyber-Physical Manipulation: A Framework for National Resilience against Systemic Disruption," *Zenodo*, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[25] Lawal Qudus, "Resilient Systems: Building Secure Cyber-Physical Infrastructure for Critical Industries against Emerging Threats," *International Journal of Research Publication and Reviews*, vol. 6, no. 1, pp. 3330-3346, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[26] Habeeb A. Shittu, Mujeeb A. Shittu, and Funminiyi Olagunju, "Cyber Physical Resilience in Digital Substations: IoT Enabled Adaptive Protection for Secure DER Integration," *International Journal of Science Architecture Technology and Environment*, vol. 1, no. 3, pp. 81-99, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[27] Ali Aghazadeh Ardebili et al., "Smart Critical Infrastructures Security Management and Governance: Implementation of Cyber Resilience KPIs for Decentralized Energy Asset," *CEUR Workshop Proceedings-Italian Conference on Cyber Security 2024: Proceedings of the 8th Italian Conference on Cyber Security*, 2024. [Google Scholar] [Publisher Link]

[28] Ioannis Zografopoulos et al., "Cyber-Physical Interdependence for Power System Operation and Control," *IEEE Transactions on Smart Grid*, vol. 16, no. 3, pp. 2554-2573, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[29] Theresa Sobb, Nour Moustafa, and Benjamin Turnbull, "Responsible Resilience in Cyber–Physical–Social Systems: A New Paradigm for Emergent Cyber Risk Modeling," *Future Internet*, vol. 17, no. 7, pp. 1-24, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[30] Elahe Taherianfard et al., "Future Smart Cities as Cyber-Physical Systems: Economic Challenges and Opportunities," 2024. [Google Scholar] [Publisher Link]