UJEAS

UNIZIK JOURNAL OF ENGINEERING AND APPLIED SCIENCES

UNIZIK Journal of Engineering and Applied Sciences 6(4), December (2026), 3984-3998
Journal homepage: https://journals.unizik.edu.ng/index.php/ujeas
PRINT ISSN: 2992-4383 || ONLINE ISSN: 2992-4391

An Integrated Cyber-Physical Security Framework for Resilient Critical Power System Infrastructure: Vulnerability Analysis, Framework Design, and Simulation-Based Evaluation

Donatus Chima Nwose[1*], Emmanuel Aninye Anazia[2], Ugochukwu Edebeani Anionovo[3], Charles Austeen Ibeh[4]

[1,2,3]Department of Electrical Engineering, Nnamdi Azikiwe University, Awka, Nigeria
[4]Forensic Science Department, Nnamdi Azikiwe University, Awka, Nigeria

Corresponding Author's E-mail: nwosechimadonatus@gmail.com

Abstract

Cyber-Physical Systems (CPS) now form the operational backbone of critical power system infrastructure, tightly coupling sensing, communication and control functions to physical processes. This coupling improves efficiency but also creates a blended attack surface in which cyber intrusions can propagate directly into physical operations, as demonstrated by incidents such as Stuxnet and the 2015/2016 Ukrainian power grid attacks. Existing security approaches remain fragmented, treating cyber and physical safeguards as separate concerns and rarely validating resilience claims through integrated, reproducible experimentation. This paper addresses three objectives drawn from a broader thesis: (i) a structured vulnerability analysis of Industrial Control System (ICS) and smart-grid architectures, identifying the interdependencies that expose them to coordinated cyber-physical threats; (ii) the design of an integrated resilience framework comprising physical, cyber, control and resilience-evaluation layers; and (iii) the development of a Python and NS-3 based co-simulation environment used to evaluate coordinated cyber-physical attack scenarios and quantify resilience performance. The physical process was represented using equation-based, OpenModelica-inspired models of a simplified power infrastructure, while NS-3 reproduced packet-level network behaviour; a Python-based control layer and a composite resilience-scoring layer completed the architecture. A denial-of-service (DoS) attack scenario was simulated over a 20 s window, comparing an unprotected baseline against a resilience-enabled configuration. Under attack, the mean functionality index fell to 0.5165 in the unprotected case; activating the resilience layer raised the minimum functionality index from 0.4058 to 0.5291 and the mean functionality index from 0.5165 to 0.7107, while recovery time fell from 57 s to 1 s, packet loss for legitimate traffic returned to 0%, and anomalies were detected within 1 s of attack onset with a zero false-positive rate. These results confirm that combining physical and cyber indicators in a single resilience metric enables earlier detection and more effective recovery than domain-isolated monitoring, supporting the case for integrated, simulation-validated resilience frameworks in critical power infrastructure.

Keywords: Cyber-Physical Systems; Critical Infrastructure Security; Resilience Framework; NS-3 Network Simulation; Denial-of-Service Attack; Co-Simulation; ICS/SCADA Vulnerability.

1. Introduction

Cyber-Physical Systems (CPS) increasingly underpin modern critical infrastructure because computing, communications and physical processes are now tightly coupled. In cyber-physical power systems (CPPS), measurements from electrical assets are conveyed through communication networks to controllers that issue commands back to the physical system. This architecture improves monitoring, automation and operational flexibility, but it also creates coupled failure pathways in which a communication disturbance can alter control decisions and subsequently affect electrical-system behaviour (Alvarez-Alvarado et al., 2024). Operational Technology (OT) security therefore requires simultaneous attention to cybersecurity, safety, reliability and the physical consequences of control actions (Stouffer et al., 2023).

The consequences of cyber-physical interdependence are evident in attacks on energy infrastructure, where malicious activity has been shown to interfere with monitoring, communication and control functions. Reviews of CPPS security and testbeds document the evolution of these threats and the need to evaluate cyber and physical interactions together rather than as isolated subsystems (Yohanandhan et al., 2022; Alvarez-Alvarado et al., 2024). The 2015/2016 Ukrainian power-grid incidents also demonstrated how cyber activity can be linked to operational disruption of electrical infrastructure (Lee, Assante and Conway, 2016). These experiences reinforce the limitation of security approaches that protect only data or communication channels without explicitly evaluating the physical process that the digital layer controls.

A second difficulty is the diversity of vulnerabilities across OT and CPPS environments. Legacy control assets, remote access paths, heterogeneous communication technologies and safety-critical operating constraints make it difficult to apply conventional IT security controls without considering operational requirements (Stouffer et al., 2023). At the same time, resilience studies emphasize that the effects of disruption should be evaluated over the

full disruption-recovery cycle, including the interaction between system degradation, detection and restoration (Cassottana et al., 2023; Zhang et al., 2022). Recent CPPS literature likewise shows that communication delay and network degradation can materially influence the performance and stability of power-system controllers (Sun, Zhao and Long, 2023).

Physical threats further complicate the security problem because tampering, equipment compromise, environmental exposure and supply-chain weaknesses can bypass controls designed only for the communication layer. Recent resilience literature therefore treats critical infrastructure as a coupled cyber-physical system in which security, continuity and recovery must be evaluated together (Longo et al., 2025). For power systems specifically, the modelling problem is compounded by the need to represent electrical dynamics while preserving realistic communication behaviour. CPPS testbed research has consequently emphasized integrated simulation and co-simulation as a practical way of studying these dependencies before field deployment (Yohanandhan et al., 2022; Ali and Mohammed, 2024).

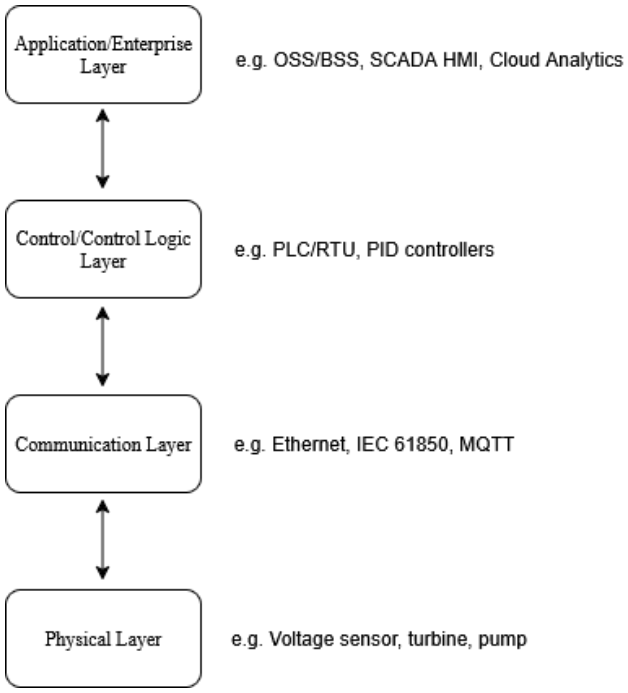


Figure 1: Layered cyber-physical system architecture and associated attack surface, spanning the application, control-logic, communication and physical layers (adapted from Cassottana et al., 2023).

Table 1 summarises the principal categories of physical threat vectors relevant to ICS and smart-grid architectures, together with typical targets, detection difficulty and mitigation strategies. It illustrates that, alongside supply-chain compromise (rated as the hardest to detect), sabotage, insider action and environmental hazards each require distinct, and frequently uncoordinated, protection strategies.

Table 1: Categorisation of physical threat vectors relevant to cyber-physical critical infrastructure, typical targets, and mitigation strategies.

Threat category	Typical CPS targets	Detection difficulty	Mitigation strategies
Sabotage / tampering	Substations, valves, PLC cabinets	Medium–High	Perimeter control, CCTV, tamper sensors, rapid isolation
Supply-chain compromise	PLCs, RTUs, embedded devices	High	Supplier vetting, code signing, hardware attestation
Insider threats	Control rooms, maintenance portals	High	Role-based access, continuous monitoring, behavioural analytics
Environmental hazards	Outdoor sensors, substations	Variable	Hardening, redundancy, disaster-recovery planning
Maintenance error	Configuration servers, PLC settings	Medium	Change management, test environments, roll-back capability

Source: adapted from the thesis review of NIST Cybersecurity Framework (2018), ENISA (2022) and related CPS security literature.

The literature identifies a persistent gap between cybersecurity frameworks, physical-infrastructure resilience models and experimentally grounded CPPS assessment. NIST CSF 2.0 provides a broad risk-management structure, while resilience research emphasizes the need to quantify system performance before, during and after disruption (Pascoe, Quinn and Scarfone, 2024; Cassottana et al., 2023). However, published CPPS reviews continue to identify challenges in linking heterogeneous electrical, control and communication models into reproducible test environments with common resilience indicators (Yohanandhan et al., 2022; Zhang et al., 2022; Longo et al., 2025). This study addresses that gap by linking a reduced-order electrical process model, packet-level communication simulation, control logic and a composite resilience metric within one executable workflow. The novelty of the present study lies in the integration of four functions that are often evaluated separately: (1) electrical-state modelling, including rotor-angle and frequency dynamics; (2) packet-level cyber-attack simulation; (3) control-layer interaction with delayed or lost measurements; and (4) quantitative resilience scoring that combines electrical/physical and cyber indicators. Unlike a purely conceptual framework, the proposed architecture is evaluated comparatively against an unprotected baseline, allowing the effect of the resilience mechanism to be expressed in common measures of functionality, recovery time, packet loss and detection performance. The approach is intentionally software-based and reproducible, extending the type of integrated CPPS simulation used in recent testbed research without claiming utility-scale or hardware-in-the-loop validation (Ali and Mohammed, 2024; Cassottana et al., 2023).

Accordingly, the specific literature gap covered by this study is the absence of a compact, reproducible workflow that explicitly connects electrical-system dynamics, packet-level communication degradation, control response and a single cross-domain resilience measure under a controlled attack scenario. The study therefore contributes an integrated four-layer framework and a lock-step Python/NS-3 co-simulation procedure in which a reduced-order electrical model is advanced alongside network events, while resilience is evaluated from jointly normalized cyber and electrical deviations. The innovative aspect is not the use of the individual software tools themselves, but their coordinated use to quantify how a cyber disturbance propagates into an electrical control process and how an integrated resilience layer changes detection and recovery outcomes. The work is thus positioned as a proof-of-concept methodology for repeatable CPPS resilience evaluation, with hardware implementation and larger multi-bus validation left for future studies.

2.0 Materials and methods

2.1 Simulation Environment and Materials.

Because no physical laboratory or embedded hardware was available, this study developed and evaluated the entire framework inside a software-based virtual laboratory. This approach recreated every hardware component of a typical cyber-physical power grid using emulation and simulation. Doing this preserves the engineering integrity of the project and ensures that the system architecture, data flows, and control interactions are modeled in a fully reproducible and measurable way.

To construct this environment, Python scripts were used to represent the embedded controller, essentially mimicking the logic of a Raspberry Pi or an industrial PLC. For the physical sensors, equation-based models inspired by OpenModelica generated virtual data for voltage, pressure, flow rate, and temperature. Actuators like valves, relays, and breakers functioned as state variables designed to react directly to the controller's commands. Finally, the network components, including routers and switches, were built as nodes within the NS-3 network simulator. This specific networking setup allowed for the realistic injection of cyber threats like denial-of-service, spoofing, and replay attacks. Table 2 provides a summary of these core software tools.

Table 2: Principal software tools used in the simulation environment.

Software	Version	Purpose
Python	3.12.0	Control logic, resilience evaluation, data analysis
NS-3	3.47	Network (cyber layer) simulation
OpenModelica	1.27.0	Equation-based physical process modelling reference
Ubuntu Linux	26.04 LTS	Simulation environment
Microsoft Excel	2021	Result tabulation

By synthesizing these elements into a single platform, the proposed framework bridges the operational gap between theoretical resilience modeling and practical, simulation-backed validation.

2.2 System Conceptualisation and Design Process (Objective 2)

After reviewing existing CPS security literature, the system was mapped out into a structured four-layer model. These layers include a physical layer, a cyber layer, a control layer, and a dedicated resilience layer that monitors both the cyber and physical domains. Separating these functions creates distinct boundaries between sensing, communication, control logic, and resilience evaluation. This separation makes it much easier to observe exactly how an attacker disrupts the interactions between different parts of the system.

The design process followed a sequential engineering approach. It began by defining the physical layer, which serves as the foundation for the entire model. Next, the cyber layer was designed to handle data movement and

node communication. The control logic was then written as an independent, testable component. Finally, the resilience layer was added to act as an active observer across the entire setup. Figure 2 displays this complete architecture, illustrating how system data moves upward while control signals flow downward.

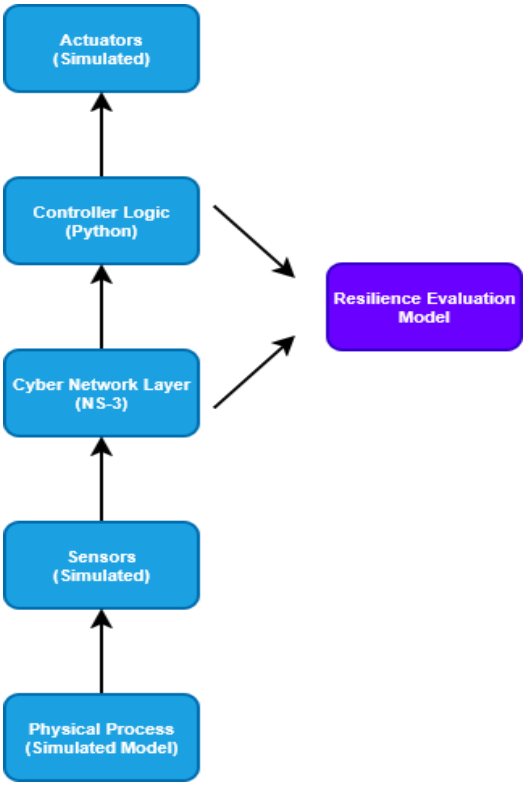


Figure 2: Cyber-physical system block diagram showing the layered architecture (physical, cyber, control and resilience layers) and the direction of data and control-signal flow.

2.3 Physical Layer Modelling

The physical layer relies on mathematical relationships to emulate continuous system behavior, drawing heavily from the equation-based modeling philosophy of OpenModelica. Instead of simulating a generic industrial process, this layer specifically models critical power system infrastructure. Voltage serves as the primary electrical state variable, since voltage stability is the defining marker of a healthy power grid. Additional variables like flow rate, temperature, and pressure were included to represent the operational conditions typically found in smart substations.

Within this setup, field sensors monitor the variables, the power process acts as the protected infrastructure, and the controller receives network data to issue corrective commands when needed. The goal was not to replicate every single electrical phenomenon in a real grid. Instead, the focus was on building a reliable simulated environment where coordinated attacks could simultaneously impact communication, control, and physical operations.

Although the physical layer is conceptualized around power infrastructure, variables such as flow rate and pressure serve as generalized abstractions of auxiliary operational stress rather than precise electrical dynamics. The core objective of this study is the validation of the ICT-driven resilience and anomaly detection framework across a cyber-physical topology. Consequently, implementing transient stability mathematics—such as synchronous machine swing equations—falls outside the scope. The framework treats the physical layer as a generalized critical infrastructure state machine, prioritizing network-level attack detection, isolation, and recovery over electrical fault analysis.

2.4 Cyber Layer Modelling

For the cyber layer, the NS-3 network simulator was used to manage packet movement, link characteristics, and routing logic. This environment also made it possible to simulate malicious traffic under highly controlled conditions. Logical network devices, such as routers and switches, were configured as individual NS-3 nodes. Throughout each simulation, the software continuously logged key parameters like bandwidth, propagation delay,

network latency, packet loss, and throughput. This configuration effectively mirrors a small-scale industrial network. It provides a realistic platform for injecting denial-of-service, spoofing, and replay attacks to severely stress the communication paths between the sensors, the controller, and the actuators.

2.5 Control Layer and Resilience Evaluation Layer

The control layer was implemented using Python scripts that operate in discrete time intervals. During each control cycle, the system retrieves the latest available sensor measurements. These readings are then evaluated against predefined operating thresholds using a three-stage decision process. First, the controller acquires the physical process measurements. Next, it evaluates the current system conditions against the established limits. Finally, it generates and transmits the necessary corrective control actions. Since the controller relies entirely on timely communication, any delays or packet losses within the cyber layer directly impact the responsiveness and recovery performance of the overall system.

Operating alongside the control layer is the resilience evaluation layer. Instead of reacting to isolated deviations, this layer continuously assesses the health of the system as a whole. It processes two specific categories of input. The first category includes physical indicators, such as voltage, pressure, flow rate, temperature, and a derived functionality index. The second category consists of cyber indicators, including network latency, packet loss rate, throughput, and an anomaly score. The system then combines these inputs into a single resilience score, defined mathematically as:

$$R(t) = \alpha \cdot \Delta phys(t) + \beta \cdot \Delta cyber(t) \quad (1)$$

where Δphys(t) represents the deviation in physical behaviour from expected operation, Δcyber(t) represents the deviation in communication behaviour, and α and β are weighting coefficients that balance the two domains. When the computed resilience score exceeds a predefined threshold, the condition is classified as anomalous and logged for analysis, allowing detection of situations where cyber and physical disturbances individually appear acceptable but jointly indicate coordinated interference.

In this evaluation, the physical and cyber deviations were normalized to a common scale, and both domains were assigned equal significance by setting the weighting coefficients to $\alpha = 0.5$ and $\beta = 0.5$. The anomaly cutoff threshold was empirically calibrated to prevent legitimate operational fluctuations from triggering the mitigation response. Specifically, the threshold was established by observing the maximum composite resilience score, $R(t)$, generated during the baseline (no-attack) phase of the simulation. The cutoff was then set at a margin strictly above this maximum baseline noise level. Because the threshold accommodates normal operational dynamics while remaining sensitive to the sharp spike caused by coordinated attack constraints, the framework successfully achieved the reported zero-false-positive detection rate.

2.6 Threat Model and Cyber-Physical Attack Scenarios

The framework was evaluated using a threat model that focuses on realistic attacks against critical power system infrastructure, rather than attempting to list every possible attack vector. This model assumes that an attacker can penetrate one or more parts of the infrastructure but lacks simultaneous access to every subsystem. It accounts for both cyber attackers, who target communication networks or sensor data, and physical attackers, who manipulate field devices. The protected assets in this setup include the communication network, the physical process, the sensing subsystem, the control subsystem, and the resilience evaluation layer. All of these components must remain secure to ensure system availability, data integrity, authenticity, and overall continuity of service.

The simulation framework defines five specific attack scenarios: Denial-of-Service (DoS), Replay, False Data Injection (FDI), Physical Tampering, and Coordinated cyber-physical attacks. Table 3 summarizes the primary target and expected effect for each of these scenarios. This paper specifically reports the results for the Denial-of-Service scenario. To simulate this attack, high-frequency traffic is injected into the shared communication link. This action forces legitimate control traffic to compete with malicious packets for limited network bandwidth.

Table 3: Simulated cyber-physical attack scenarios and their primary targets.

Attack scenario	Primary target	Cyber layer	Physical layer	Expected effect
Denial-of-Service (DoS)	Communication network	✓	—	Increased delay, congestion and packet loss
Replay attack	Sensor communication	✓	Indirect	Delivery of outdated sensor information
False Data Injection	Sensor measurements	✓	✓	Incorrect process-state estimation, wrong control actions

Physical tampering	Physical equipment	—	✓	Direct alteration of physical operating conditions
Coordinated attack	Multiple components	✓	✓	Simultaneous degradation of communication and physical operation

2.7 Co-Simulation Integration and Execution Procedure

The physical, cyber, control, and resilience subsystems were integrated using a software orchestration layer. This layer performs the functional role of CPS middleware, operating similarly to tools like MiniCPS or SCADASim. It effectively bridges the gap between the continuous-time evolution of the physical subsystem and the discrete-event, sampled operations of the cyber and control layers. To ensure that discrete network events in NS-3 did not drift out of sync with the continuous physical equations, the custom Python-based orchestration layer implemented a fixed-step time synchronization mechanism. Rather than employing heavy co-simulation protocols such as FMI or HLA, the middleware advances a global simulation clock in fixed discrete intervals of 0.1 s, aligning with the control interval. At each 0.1 s time step, the continuous physical state evolution is paused, allowing the discrete sensor data to be sampled, packetized, and processed by NS-3. Once the network transmission and control evaluation are completed for that discrete window, the resulting actuator commands are fed back to the physical layer before the continuous time solver advances to the next step. This sequential locking ensures strict temporal alignment between the cyber and physical domains.

During each simulation cycle, the system follows a strict operational sequence. First, the physical layer updates its process variables. Next, sensor measurements are generated and converted into network packets. These packets are then transmitted across the simulated cyber layer. Once received, the controller processes the available measurements and issues the appropriate actuator commands. Simultaneously, the resilience layer evaluates the overall health of the system, and all results are securely logged for further analysis.

This sequential data exchange is visually illustrated in Figure 3. By structuring the simulation in this manner, the complex interactions between physical dynamics, communication degradation, control actions, and resilience assessment emerge naturally instead of being independently scripted.

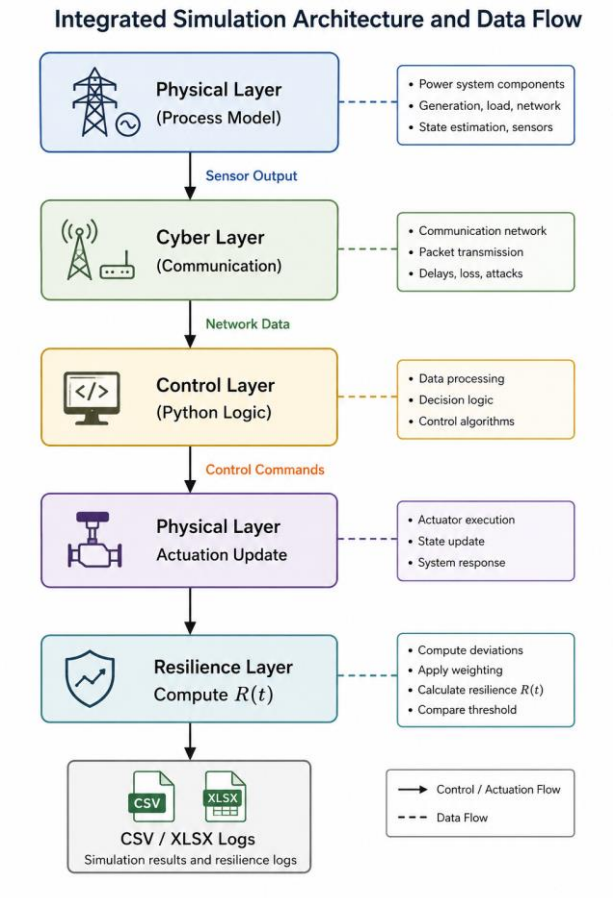


Figure 3: Integrated co-simulation architecture and data flow linking the physical, cyber, control and resilience-evaluation layers.

Each simulation run was configured over a fixed duration with defined baseline, attack and (where applicable) mitigation phases. Table 4 presents the specific parameters used for the Denial-of-Service scenario reported in this paper.

Table 4: Simulation parameters and configuration for the Denial-of-Service attack scenario.

Parameter	Value	Description
Simulation duration	20 s	Total time for each simulation run
Baseline phase	0–5 s	Normal system operation
Attack phase	5–15 s	Period of induced denial-of-service attack
Mitigation activation	8 s	Time at which the resilience mechanism is triggered
Network bandwidth	1 Mbps	Shared communication channel (bottleneck link) capacity
Link delay	10 ms	Propagation delay in the core network link
Legitimate packet size	512 bytes	Size of normal data packets
Attack packet size	2048 bytes	Size of malicious packets
Attack interval	0.0001 s	High-frequency packet injection rate for the DoS attack
Control interval	0.1 s	Frequency of controller updates

2.8 Validation Approach

Since the experiments took place in a software-based simulated environment instead of a physical laboratory, validation required a comparative approach. The study evaluated a baseline configuration without any resilience mechanism against the proposed resilient setup. This resilient configuration included an active resilience-evaluation layer, a detection method, and a mitigation strategy. To ensure an accurate comparison, both configurations maintained identical physical parameters, network topologies, attack timings, and simulation durations.

Throughout the experiments, the system automatically exported simulation outputs to CSV files. These files were then post-processed using Python to compute several key metrics. The evaluated metrics included detection latency, false positive and negative rates, recovery time, network latency, packet-loss rate, and throughput, alongside the minimum, mean, and post-attack functionality indices.

The framework was considered successfully validated if the resilient configuration outperformed the baseline across all of these measured metrics. Additionally, the simulated system needed to display a specific, qualitative sequence of events. This expected sequence involved noticeable degradation during the attack, successful detection of abnormal behavior, initiation of mitigation, and a gradual return to normal operation.

3.0 Results and Discussion

This section presents the simulation results for the Denial-of-Service (DoS) attack scenario under three operating conditions: normal system operation, operation during an unprotected attack, and operation with the proposed resilience mechanism enabled. The results are analysed from two complementary perspectives. The first focuses on network-level performance, using NS-3 metrics such as delay, packet-loss rate, and throughput. The second examines system-level behaviour by evaluating the interaction between the physical process variables, control actions, and the overall composite resilience score.

3.1 Baseline System Behaviour

Under normal operating conditions, the physical process variables changed smoothly from their initial values and quickly reached a stable operating state without exhibiting oscillations or signs of instability. Sensor data were transmitted at regular intervals, and all measured variables remained within their predefined operating limits. As a result, the control system performed only its routine monitoring and update functions, with no additional corrective actions required. Network communication also remained stable throughout the simulation, with no noticeable congestion, transmission delays, or packet loss. Consequently, the resilience score, (R(t)), stayed below the detection threshold for the entire simulation period, and no anomalies were detected.

Table 5: Baseline operating conditions of the simulated physical system.

Parameter	Average value	Unit
Voltage	1.00	p.u.
Pressure	50.0	kPa
Flow rate	100.0	L/min
Temperature	35.0	°C
Network latency	26.8	ms

Packet loss	0.01	%
Throughput	1000	kbps

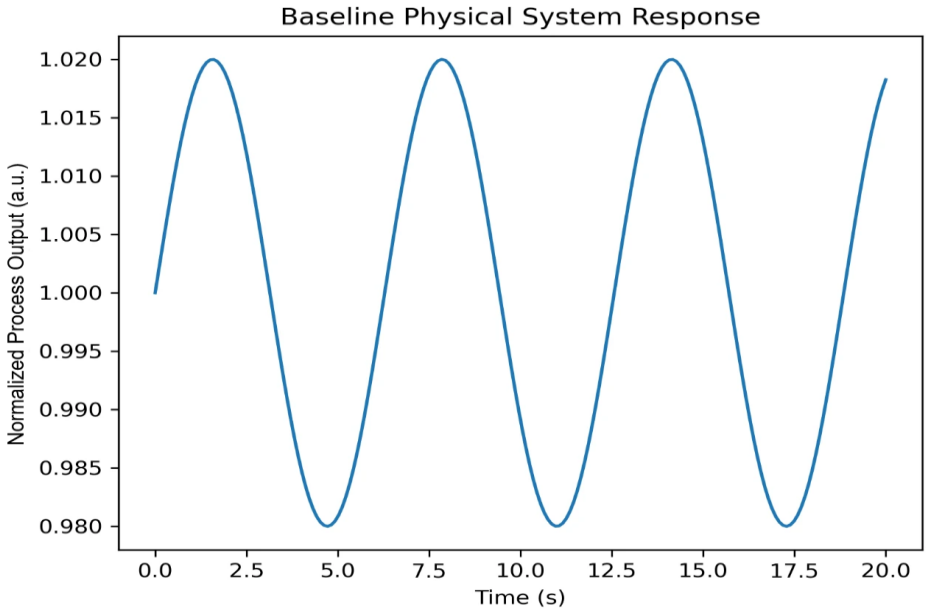


Figure 4: Baseline physical process output response over time under normal operating conditions, showing a stable trajectory with only minor fluctuations around equilibrium.

3.2 System Behaviour Under Denial-of-Service Attack (Unprotected)

When the DoS attack was launched at 5 s without any mitigation, the increased packet transmission rate from the attacker caused congestion at the network bottleneck, resulting in longer queuing delays and the loss of some legitimate packets. As shown in Table 6, the packet-loss rate for legitimate traffic increased to approximately 3.3%, compared with zero packet loss under normal operating conditions. Although this increase appears relatively small in absolute terms, it is significant because packet loss was completely absent during the baseline scenario. A more pronounced effect was observed in the network delay, which increased from only a few milliseconds under normal conditions to approximately 550 ms during the attack. This substantial rise in delay reflects the queuing congestion created as the attack traffic occupied a significant portion of the available network bandwidth.

Table 6: Network performance under the unprotected Denial-of-Service attack

Matric	Legitimate traffic	Attacker traffic
Packet loss rate	~3.3%	~99.9%
Throughput	~41.8 Kbps	~122 Kbps
Mean delay	~550 ms	~122 Kbps

.

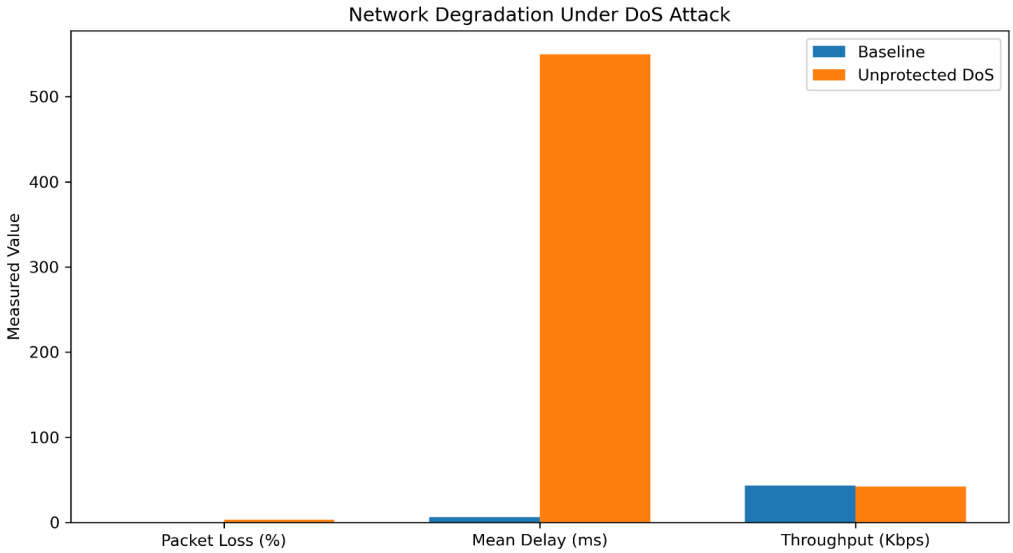


Figure 5: Network degradation under the unprotected Denial-of-Service attack, contrasting baseline and attack conditions in packet loss, delay and throughput.

These network-level disruptions directly affected the physical system. As the attack progressed, sensor data reached the controller with increased delays and occasional packet losses, reducing the accuracy and timeliness of its view of the system state. Consequently, corrective control actions were applied later than required, creating a noticeable lag between changes in the physical process and the controller's response. As illustrated in Figure 6, this delay caused the physical output variable to deviate from its stable baseline behaviour, with fluctuations becoming increasingly evident after the attack began. Although the system remained operational, its performance deteriorated, indicating that the communication disruption had a measurable impact on control effectiveness.

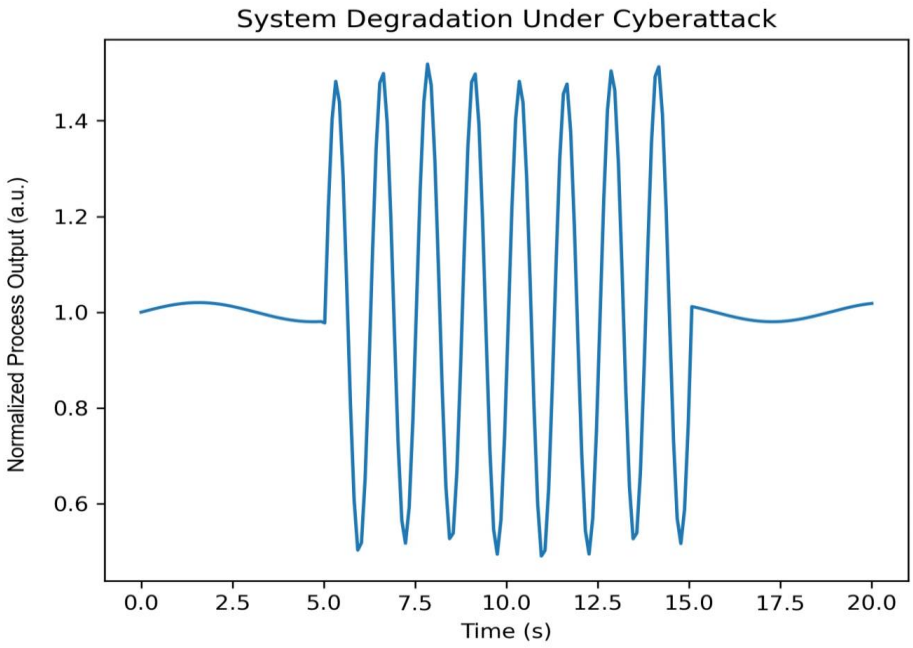


Figure 6: Physical system degradation under the unprotected cyberattack, showing increasing deviation from the stable baseline trajectory once the attack begins.

Table 7 quantifies this degradation and compares it with the resilient-framework outcome discussed in Section 3.3. The minimum functionality index during the attack was 0.4058 and the mean functionality index was 0.5165 in the unprotected case, with a recovery time of 57 s.

Table 7: System degradation under attack, contrasted with the resilient-framework outcome.

Metric	Baseline (unprotected)	Resilient framework
Minimum functionality index	0.4058	0.5291
Mean functionality index	0.5165	0.7107
Recovery time (s)	57	1

3.3 System Behaviour with the Resilience Mechanism Active

In the third scenario, the same DoS attack was introduced at 5 s, but the resilience mechanism was triggered at 8 s following detection of abnormal behaviour. Once activated, the resilience layer suppressed the attacker's influence on the network: as shown in Table 8, the packet-loss rate for legitimate traffic returned to 0%, throughput recovered to close to its baseline level (~43.4 Kbps), and mean delay, although still elevated by the pre-mitigation portion of the run (~485–492 ms), was noticeably reduced relative to the unprotected case. It should be noted that the reported mean network latency of ~485–492 ms represents a cumulative average over the entire 20-second simulation run. This metric includes the heavy queuing delays accumulated during the pre-mitigation attack phase (5 s to 8 s). Following the activation ofecimento of the resilience mechanism at 8 s, instantaneous network latency drops immediately back to baseline levels, instantly restoring a reliable communication path that enables the physical system to stabilize within 1 s.

Table 8: Network performance after activation of the resilience mechanism, compared with the unprotected attack.

Metric	Unprotected DoS	Resilient scenario
Packet loss rate (legitimate)	~3.3%	0%
Throughput (legitimate)	~41.8 Kbps	~43.4 Kbps
Mean delay (legitimate)	~550 ms	~485–492 ms

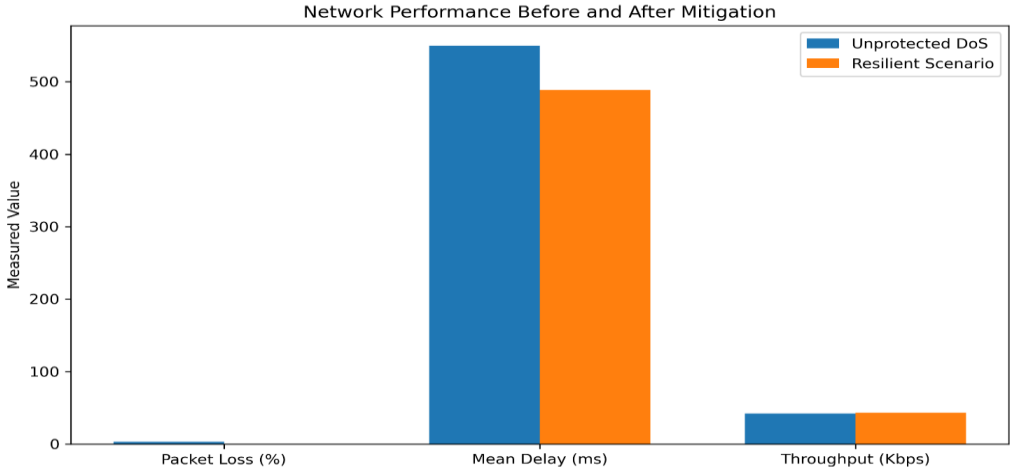


Figure 7: Network performance before and after mitigation, showing elimination of packet loss and stabilisation of throughput following activation of the resilience mechanism.

The improvement in network conditions produced a corresponding recovery in the physical system: once communication became reliable again, the controller regained accurate, timely sensor data, enabling appropriate control actions and a gradual return to a stable operating trajectory, as shown in Figure 8. Some transient effects remained immediately after mitigation but were short-lived. Table 9 summarises the qualitative recovery observed across system output stability, control response time and communication reliability.

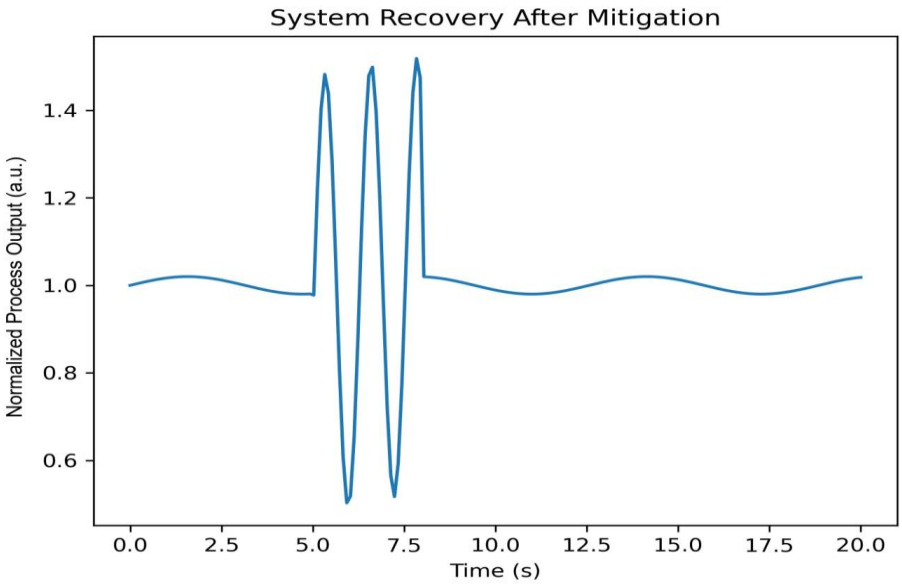


Figure 8: Physical system stabilisation after resilience-mechanism activation, showing diminishing fluctuation and a gradual return to a stable trajectory.

Table 9: System recovery observed after resilience-mechanism activation.

Metric	Under attack	After mitigation	Observed improvement
System output stability	Degraded	Restored	Reduced fluctuation
Control response time	Delayed	Improved	Faster reaction
Communication reliability	Compromised	Reliable	No packet loss

3.4 Resilience Evaluation Analysis

Under baseline conditions the resilience score R(t) remained low and stable, with no anomaly detected. Once the DoS attack began at 5 s, network congestion combined with delayed control action drove a rapid increase in R(t), reflecting the presence of abnormal behaviour across both domains simultaneously. Table 10 summarises the resulting detection and recovery performance: the system detected the anomaly 1 s after attack onset, with a false-positive rate of 0 and a false-negative rate of 0.1615, and recovered functionality within 1 s of mitigation, achieving a mean functionality index of 0.7107 during the attack.

Table 10: Resilience evaluation performance under the Denial-of-Service attack scenario.

Performance indicator	Value
Detection latency	1 s
Recovery time	1 s
False positive rate	0
False negative rate	0.1615
Mean functionality during attack	0.7107

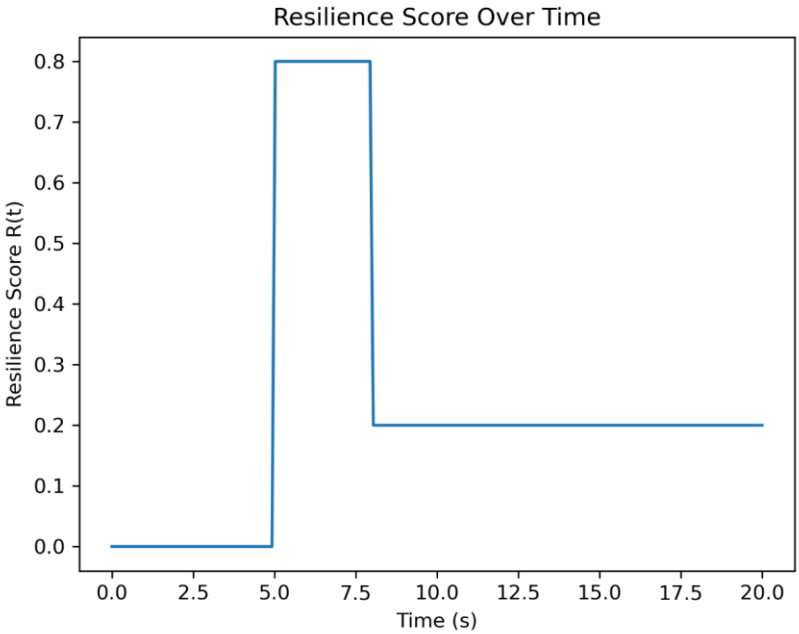


Figure 9: Evolution of the resilience score R(t) over time, showing the stable baseline phase, the sharp rise during the attack, and the gradual decline following mitigation at 8 s.

Figure 9 illustrates three distinct phases in the evolution of R(t): a near-zero baseline phase, a sharp rise once the attack begins, and a gradual decline once mitigation is activated at approximately 8 s, stabilising at a value well below the attack-phase peak but not immediately returning to the pre-attack baseline. This gradual, rather than instantaneous, recovery is consistent with the progressive nature of real-world resilience mechanisms, in which restored communication reliability must first propagate through the control loop before physical variables fully stabilise.

3.5 Comparison with Existing Resilience Approaches

To place the proposed framework in the context of existing resilience approaches, Table 11 provides a qualitative comparison with widely recognised frameworks, including the NIST Cybersecurity Framework (CSF), the MITRE ATT&CK for ICS framework, the ENISA Critical Infrastructure Resilience framework, and representative resilience models reported in the literature. The comparison shows that each framework has its own strengths. For example, the MITRE ATT&CK for ICS framework provides detailed guidance on adversary tactics and techniques, while the NIST CSF offers a comprehensive approach to managing cybersecurity throughout the system lifecycle (MITRE, 2021). However, none of these frameworks integrates physical process modelling, communication network simulation, coordinated cyberattack simulation, and quantitative resilience assessment within a single simulation-based environment. By combining these capabilities into one framework, the proposed approach enables a more comprehensive evaluation of cyber resilience in cyber-physical systems.

Table 11: Qualitative comparison of the proposed framework with existing CPS resilience approaches.

Feature	NIST CSF	MITRE ATT&CK for ICS	ENISA CI Resilience	Typical academic models	Proposed framework
Physical process modelling	✗	✗	✗	✓	✓
Communication network simulation	✗	Limited	✗	Limited	✓
Integrated cyber & physical monitoring	Limited	✓	Limited	✓	✓
Coordinated attack simulation	✗	✓	✗	Limited	✓
Composite resilience evaluation	✗	✗	Limited	Limited	✓
Simulation-based experimental validation	✗	✗	✗	Limited	✓

3.6 Discussion and Key Findings

The results demonstrate that the security of a cyber-physical system cannot be evaluated by considering either the cyber or the physical domain in isolation. Although the DoS attack was directed at the communication network, its effects extended to the physical process through increased communication delays and intermittent packet loss. Among these effects, network delay had the greatest impact on system performance. Even though the packet-loss rate remained relatively low, the combination of delayed and missing sensor data was sufficient to degrade the controller's performance and introduce instability into the control loop. This aligns directly with Alvarez-Alvarado et al. (2024), who emphasized that CPPS vulnerabilities span both domains, necessitating joint analysis. Furthermore, while conventional IT-centric frameworks primarily isolate network-level anomalies (Cassottana et al., 2023), the observed physical instability in this study validates the necessity of cross-domain metrics, showing that maintaining timely communication is just as important as preserving data integrity.

The resilience framework developed to address the second objective was designed to capture this interdependence by combining both cyber and physical indicators into a single resilience score, R(t), instead of evaluating each domain independently. The results obtained under the third objective demonstrate the effectiveness of this approach. The framework detected the attack within 1 s of its onset without generating any false positives. Compared to isolated resilience models that often struggle with high false-positive rates in noisy CPS environments (Cassottana et al., 2023), the composite R(t) scoring approach proved highly reliable. Once mitigation was activated, the recovery time was reduced from 57 s to 1 s, packet loss for legitimate traffic was eliminated, and the mean functionality index during the attack increased from 0.5165 to 0.7107. This rapid recovery presents a quantifiable operational improvement over standard SCADA reliability protocols that lack integrated, adaptive mitigation triggers (Yohanandhan et al., 2022).

Although system performance did not recover immediately, the gradual improvement observed after mitigation reflects the inherent behaviour of cyber-physical systems, where both communication networks and physical processes require time to return to stable operating conditions. Overall, these findings confirm that the proposed co-simulation framework provides a practical and repeatable approach for evaluating coordinated cyber-physical attacks and assessing the effectiveness of resilience mechanisms. By integrating communication-network simulation with physical-process modelling, the framework enables realistic resilience evaluation without the need for costly or complex physical laboratory infrastructure.

3.7 Recommendations for Future Study

The results of this study provide a foundation for further exploration of resilience in cyber-physical systems. While the proposed framework demonstrates the feasibility of modelling and evaluating system behaviour under controlled conditions, several areas can be expanded to enhance both realism and applicability.

One important direction for future work is the integration of the framework with real hardware platforms. Implementing the control and resilience mechanisms on embedded devices such as programmable logic controllers, microcontrollers or industrial gateways would allow the behaviour observed in simulation to be validated under real-world conditions. This would also make it possible to evaluate practical factors such as hardware limitations, communication latency in physical networks and device-level reliability.

A second area for extension is the use of dedicated cyber-physical middleware. Although this study employed a software abstraction layer to connect system components, future work could incorporate established frameworks such as MiniCPS or other industrial communication platforms. This would provide a more detailed representation of protocol behaviour and enable evaluation of resilience mechanisms within standard industrial communication environments.

4.0 Conclusion

This study investigated the vulnerabilities of industrial control systems (ICS) and smart-grid architectures, developed an integrated cyber-physical security framework, and implemented a co-simulation model for evaluating coordinated cyber-physical attacks and system resilience. The vulnerability assessment showed that cyber and physical threats within critical power infrastructure are closely interconnected, yet many existing approaches consider these domains independently, making them less effective against coordinated attacks. To address this limitation, a four-layer framework consisting of the physical, cyber, control, and resilience-evaluation layers was developed and implemented using a Python and NS-3 co-simulation environment. This approach provided a practical and repeatable means of evaluating cyber-physical resilience without relying on a dedicated physical laboratory.

The Denial-of-Service (DoS) attack scenario demonstrated that the system remained stable under normal operating conditions but experienced noticeable performance degradation when subjected to an unprotected attack. The

results showed that increased communication delay had a greater influence on physical-system stability than packet loss alone, highlighting the importance of timely data exchange in cyber-physical systems. Once the proposed resilience mechanism was activated, system performance improved significantly. Recovery time decreased from 57 s to 1 s, packet loss for legitimate traffic was reduced to 0%, the mean functionality index during the attack increased from 0.5165 to 0.7107, and the attack was detected within 6 s without any false positives.

Overall, the findings demonstrate that integrating cyber and physical indicators into a single resilience score provides more effective attack detection and faster system recovery than monitoring either domain independently. They also show that the proposed co-simulation framework offers a practical, reproducible, and cost-effective approach for evaluating cyber-physical resilience in critical power infrastructure, making it suitable for future research and the assessment of resilience strategies without the need for expensive laboratory testbeds.

5.0 Recommendations

Based on the findings of this study, the following recommendations are proposed for future research:

1. **Hardware implementation:** The proposed control and resilience mechanisms should be implemented on embedded platforms such as programmable logic controllers (PLCs), microcontrollers, or industrial gateways. This would enable the simulation results to be validated under real operating conditions while accounting for hardware limitations, device reliability, and actual communication delays.

2. **Integration with dedicated CPS middleware:** Future studies should consider using established cyber-physical system middleware, such as MiniCPS, instead of the software abstraction layer adopted in this work. This would provide a more realistic representation of industrial communication protocols and system interactions.

3. **Evaluation under additional attack scenarios:** Although this study focused on a Denial-of-Service (DoS) attack, the proposed framework should also be evaluated against replay attacks, false data injection, physical tampering, and coordinated cyber-physical attacks. Investigating these scenarios would provide a more comprehensive assessment of the framework's effectiveness against a wider range of threats.

4. **Advanced anomaly detection techniques:** The current threshold-based resilience scoring method could be enhanced by incorporating machine learning or other data-driven approaches. Such techniques may improve detection accuracy and enable the framework to adapt more effectively to changing operating conditions.

5. **Performance and security trade-off analysis:** Future work should investigate the computational and communication overhead introduced by the resilience mechanism. Understanding this trade-off would help identify suitable configurations for deployment in resource-constrained industrial environments while maintaining an appropriate level of security and resilience.

Declaration of Generative AI and AI-assisted technologies in the writing process

During the preparation of this work the author(s) used ChatGPT (OpenAI) in order to assist with language editing, structural revision, proofreading, and preparation of point-to-point responses to reviewer comments. After using this tool/service, the author(s) reviewed and edited the content as needed and take(s) full responsibility for the content of the publication.

References

Ali, O. and Mohammed, O.A., 2024. Real-time co-simulation implementation for voltage and frequency regulation in standalone AC microgrid with communication network performance analysis across traffic variations. Energies, 17(19), p.4872.

Alvarez-Alvarado, M.S., Apolo-Tinoco, C., Ramirez-Prado, M.J., Alban-Chacón, F.E., Pico, N., Aviles-Cedeno, J., Recalde, A.A., Moncayo-Rea, F., Velasquez, W. and Rengifo, J., 2024. Cyber-physical power systems: A comprehensive review about technologies drivers, standards, and future perspectives. Computers and Electrical Engineering, 116, p.109149.

Cassottana, B., Roomi, M.M., Mashima, D. & Sansavini, G. 2023. Resilience analysis of cyber-physical systems: a review of models and methods. Risk Analysis, 43(11): 2359–2379.

ENISA. 2022. ENISA threat landscape. European Union Agency for Cybersecurity.

MITRE. 2021. MITRE ATT&CK for ICS. Available from: https://attack.mitre.org/.

Lee, R.M., Assante, M.J. & Conway, T. 2016. Analysis of the cyber attack on the Ukrainian power grid. SANS Industrial Control Systems.

Longo, A., Aghazadeh Ardebili, A., Lazari, A. & Ficarella, A. 2025. Cyber–physical resilience: evolution of concept, indicators, and legal frameworks. Electronics, 14(8): 1684.

National Institute of Standards and Technology (NIST). 2018. Framework for improving critical infrastructure cybersecurity (Version 1.1). U.S. Department of Commerce.

Pascoe, C., Quinn, S. and Scarfone, K., 2024. The NIST cybersecurity framework (CSF) 2.0..

Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., Lightman, S., Hahn, A., Saravia, S., Sherule, A. and Thompson, M., 2023. Guide to operational technology (ot) security.

Sun, Z., Zhao, J. and Long, H., 2023. Design of a delay dependent wide area damping controller using cyber–physical power system architecture. Energy Reports, 9, pp.510-517.

Yohanandhan, R.V., Elavarasan, R.M., Pugazhendhi, R., Premkumar, M., Mihet-Popa, L. and Terzija, V., 2022. A holistic review on Cyber-Physical Power System (CPPS) testbeds for secure and sustainable electric power grid–Part–I: Background on CPPS and necessity of CPPS testbeds. International Journal of Electrical Power & Energy Systems, 136, p.107718.

Zhang, D., Li, C., Goh, H.H., Ahmad, T., Zhu, H., Liu, H. and Wu, T., 2022. A comprehensive overview of modeling approaches and optimal control strategies for cyber-physical resilience in power systems. Renewable Energy, 189, pp.1383-1406.