Journal, Advances in Mathematical & Computational Sciences
Vol. 13 No. 4, 2025 Series
www.isteams.net/mathematics-computationaljournal

Journal of Advances in Mathematical & Computational Sciences
An International Pan-African Multidisciplinary Journal of the SMART Research Group
International Centre for IT & Development (ICITD) USA

Available online at https://www.isteams.net/ mathematics-computationaljournal.info
CrossREF Member Listing - https://www.crossref.org/06members/50go-live.html

CPS-RISE: A Multilayered Ai-Enhanced, Blockchain-Anchored, And Digital Twin–Assisted Resilience Framework For Cyber-Physical Systems In The Oil and Gas Sector

[1]Odimba, U., [2]Baale, A.A. & [3]Longe, O. B.
[1]Africa Centre of Excellence on Technology Enhanced Learning
National Open University of Nigeria, Abuja, Nigeria
[3]Wesland University, Iwo, Osun, State, Nigeria
[3]West Midlands Open University, Ikeja, Lagos State, Nigeria
E-mails: ace23150002@noun.edu.ng; aabaale@lautech.edu.ng;

ABSTRACT

Cyber-Physical Systems are now indispensable in oil and gas operations, where they monitor, coordinate, and control critical processes such as pipeline flow regulation, custody-transfer metering, compressor optimisation, and industrial safety actions. Increased integration between operational technology and enterprise systems has expanded the attack surface, exposing industrial environments to sophisticated cyber-physical threats. Traditional IT-style detection and perimeter-based security measures fall short because they often ignore the physical dynamics, industry protocols, and timing constraints that define industrial operations. This paper presents CPS-RISE, a multilayered framework that integrates machine learning–based anomaly detection, blockchain-anchored log integrity, a secure middleware gateway, and Digital Twin–assisted resilience analysis. The framework spans five layers, perception, network, control, middleware, and application, reflecting the operational structure of oil and gas systems. CPS-RISE is evaluated using industrial datasets from SWaT, WADI, and BATADAL, along with a Hyperledger Fabric ledger for integrity tests, a middleware prototype for OT–IT data exchange, and scenario-based Digital Twin simulations for resilience assessment. Results show consistently strong anomaly-detection performance, low blockchain overhead, stable middleware latency, and measurable improvements in resilience trajectories and recovery performance. The paper concludes with practical implications for energy-sector operators, regulators, and integrators, and identifies opportunities for adaptive detection, physics-informed models, and real-time Digital Twin integration.

Keywords: Cyber-Physical Systems, Industrial Control Systems, Oil and Gas Security, Anomaly Detection, Machine Learning, AI-Enhanced Detection, Blockchain Integrity, Industrial Middleware, Digital Twin Simulation, Resilience Engineering, OT–IT Integration.

dimba, U., Baale, A.A. & Longe, O. B. (2025): CPS-RISE: A Multilayered Ai-Enhanced, Blockchain-Anchored, And Digital Twin–Assisted Resilience Framework For Cyber-Physical Systems In The Oil and Gas Sector. Journal of Advances in Mathematical & Computational Science. Vol. 13, No. 4. Pp 25-48. Available online at www.isteams.net/mathematics-computationaljournal. dx.doi.org/10.22624/AIMS/MATHS/V13N4P3

1. INTRODUCTION

Cyber-Physical Systems now underpin essential functions across the oil and gas value chain. They coordinate pressure control, pump scheduling, leak detection, tank-level balancing, process optimisation, and safety shutdown actions through tightly integrated sensing, computation, and actuation components [1], [5], [37]. Historically, industrial facilities were physically isolated, reducing exposure to external threats. Today, operational networks are connected to enterprise systems, cloud platforms, vendor portals, and remote maintenance channels, creating a broader and more complex attack surface [8], [27]. Recent incidents across energy and industrial sectors show that adversaries increasingly exploit the physics of processes, industrial protocols, and supervisory control logic [33], [43]. These threats include multi-stage intrusions that manipulate sensors, falsify setpoints, alter historian data, or trigger unsafe transitions in pumps and valves [12], [38], [45]. Traditional intrusion-detection and firewall-based controls often fail to recognise such attacks because they depend heavily on generic network signatures that lack visibility into physical behaviour and dynamic process constraints [21], [40].

Research has advanced several specialised approaches to address these gaps. Machine learning models trained on industrial datasets improve anomaly detection in supervisory systems [9], [24], [26], while blockchain technologies strengthen data integrity by ensuring tamper-evident audit trails across distributed environments [10], [19], [64]. Middleware gateways offer reliable OT–IT segmentation and controlled data exchange [35], [34], and Digital Twins allow simulation-driven state estimation and resilience assessment under diverse scenarios [30], [62]. However, these advancements typically appear as isolated capabilities. Industry practitioners often lack a coherent, unified architecture that integrates anomaly detection, integrity assurance, safe data exchange, and resilience modelling into a single framework tailored for oil and gas CPS.

To address this gap, this paper introduces **CPS-RISE**, a comprehensive security and resilience framework combining:

- supervised machine learning for anomaly detection
- blockchain-ledger anchoring for log integrity
- a secure middleware gateway for OT–IT regulation
- a Digital Twin module for resilience evaluation and early warning

The framework aligns with industrial realities and regulatory expectations and supports practical implementation across pipelines, terminals, metering systems, and refinery subsystems.
The next section discusses the threat landscape that shapes security needs in oil and gas CPS.

2. THREAT LANDSCAPE FOR OIL AND GAS CYBER-PHYSICAL SYSTEMS

Oil and gas Cyber-Physical Systems operate under continuous, safety-critical, and resource-sensitive conditions. They rely on dispersed sensing, deterministic control loops, industrial communication networks, and supervisory platforms. This operational context introduces unique attack surfaces and threat dynamics. Research across industrial security literature consistently shows that CPS in the energy sector face coordinated, multi-stage, and process-aware attacks that combine network-level intrusion with physical manipulation of field devices [12], [20], [33].

2.1 Multi-Stage and Process-Aware Attacks

Attackers increasingly use deep knowledge of plant physics, control logic, and timing sequences to craft stealthy and coordinated intrusions [43], [45]. These techniques include gradual sensor biasing, setpoint alteration, replay of stale data, and manipulation of historian tables to mislead operators and automated decision systems [31], [38]. The energy sector, which depends heavily on continuous pump-valve coordination, compressor sequencing, and flow-meter accuracy, is especially vulnerable to these attacks [28], [55]. Process-aware intrusions are hazardous because they mimic normal behaviour at the network level while creating physical deviations that destabilise operations. For example, pipeline flow controllers may appear to receive valid Modbus packets even while manipulated data causes cumulative pressure imbalance [22]. Similarly, refinery tank-level systems may receive plausible readings despite covert changes in the underlying sensor behaviour [50].

2.2 OT–IT Convergence and Expanded Attack Surfaces

Digitisation programmes have increased the volume of data moving between operational networks and enterprise systems. Recent studies demonstrate that OT–IT integration exposes historically isolated control devices to scanning, probing, credential-stuffing, and lateral-movement attempts that originate from IT or cloud environments [27], [60]. Legacy devices, unencrypted protocols, and direct vendor access channels broaden the attack surface and diminish defense-in-depth effectiveness [35], [46]. The resulting exposure has enabled adversaries to exploit insecure pathways in pipeline SCADA, tank-gauging systems, custody-transfer metering infrastructures, and compressor stations. Organisations face risks of service disruption, equipment damage, and product-loss events that cascade rapidly across interconnected facilities [33], [58].

2.3 Insider Threats and Supply-Chain Risks

Industrial operations involve multiple contractors, vendors, integrators, and field technicians. This creates insider threats, both intentional and unintentional. Studies on industrial breaches show that misconfigurations, unauthorised logic changes, and unsafe access practices significantly contribute to CPS incidents [8], [41]. Additionally, supply-chain vulnerabilities in controllers, firmware, and networking components increase the risk of embedded malicious code or manipulated updates [49].

2.4 Consequences of CPS Attacks in the Oil and Gas Sector

Attacks on oil and gas CPS can lead to:

- pressure excursions causing pipeline ruptures
- pump dead-heading events leading to equipment fatigue
- tank overflow or product contamination
- flaring and emission-control failures
- shutdowns affecting regional supply
- safety incidents affecting personnel and communities

Empirical analyses show that disruptions in flow regulation, metering accuracy, and compressor synchronisation can cascade across upstream, midstream, and downstream operations due to the tightly coupled nature of CPS processes [37], [63].

3. LITERATURE REVIEW

This section synthesises current knowledge on CPS security, AI-based anomaly detection, blockchain integrity mechanisms, middleware for OT–IT convergence, and Digital Twin–enabled resilience. Each area contributes to the rationale behind CPS-RISE. Heavy but balanced citations are applied throughout, as requested.

3.1 Cyber-Physical System and Industrial Control System Security

CPS and industrial control system security have evolved significantly as researchers highlighted the limits of traditional IT-centric security models in environments with strict timing, availability, and safety constraints [8], [12], [33]. Foundational surveys explain how industrial systems require visibility into both network activity and physical behaviour to detect and mitigate threats effectively [5], [27]. Several studies outline the structure of industrial control architectures and the need for layered defences that cover sensing, actuation, control logic, communication pathways, and supervisory operations [21], [28].

Researchers further show that control systems face targeted cyber-physical threats that exploit protocol weaknesses, operational workflows, and deterministic behaviours [43], [59]. Well-known analysis of industrial incidents demonstrates how attackers manipulate process states stealthily, causing physical disruption while appearing legitimate at the network level [42], [44].

Recent studies converge on a shared insight: industrial CPS require integrated resilience, not just intrusion detection. This requires architectures that combine detection, response, recovery, and adaptive learning [37], [55], [57].

3.2 AI and Machine Learning for CPS Anomaly Detection

Machine learning has emerged as a central technique for anomaly detection in SCADA and CPS environments. Surveys highlight the strengths of supervised, unsupervised, and hybrid techniques, especially when models are trained on industrial datasets containing realistic process values and attack behaviours [9], [11], [24]. Feature engineering and temporal windowing approaches have proven effective in capturing multivariate relationships across sensors and actuators [3], [26].

Beyond basic supervised detectors, more advanced approaches employ ensemble models, deep learning, and graph neural networks to capture dependencies across distributed control processes [17], [38], [47]. Studies also document vulnerabilities in AI-based detectors, especially under adversarial conditions, demonstrating the need for layered resilience and complementary mechanisms [25], [50]. Research emphasises that machine learning can significantly enhance detection capabilities, but only when embedded within broader architectures that ensure data integrity, controlled data exchange, and resilience modelling [26], [32], [63].

3.3 Blockchain Integrity Approaches in Industrial CPS

Blockchain technologies are increasingly applied to industrial contexts for securing audit trails, configuration logs, and process events. Permissioned blockchain systems such as Hyperledger Fabric offer low-latency consensus and fine-grained endorsement policies suitable for industrial CPS operations [10], [19], [64]. Studies show that blockchain anchoring can reduce tampering risks in distributed logs, improve forensic readiness, and increase trust in event provenance [29], [36].

Researchers also explore blockchain–Digital Twin integration, where secure logs support predictive analytics and trustworthy state estimation [32], [36]. Although blockchain introduces additional latency, empirical studies demonstrate that overhead can be kept within acceptable bounds for non-real-time industrial functions [10], [29]. These findings reinforce the rationale for including blockchain-based log integrity in CPS-RISE.

3.4 Secure Middleware for OT–IT Integration

As industrial systems adopt cloud and enterprise connectivity, secure OT–IT middleware has become essential for regulating cross-domain data flows. Research shows that middleware provides schema validation, authentication, protocol translation, and buffering functions that reduce direct exposure of field devices to external networks [34], [35], [46]. Studies further show that middleware can enforce rate limits, monitor payload structures, block malformed packets, and support secure, policy-driven integration with higher-level analytics systems [60]. Middleware-based segmentation is widely acknowledged as a core element of industrial defence-in-depth strategies, especially in oil and gas operations where continuous availability and process safety are critical [33], [58].

3.5 Digital Twins for CPS Simulation and Resilience

Digital Twins have progressed from engineering design tools to dynamic simulation environments capable of replicating cyber-physical behaviours in real time. Research indicates that Digital Twins can support anomaly detection, predictive maintenance, failure analysis, and security evaluation by testing how systems respond to disturbances [30], [62]. In resilience engineering, Digital Twins enable performance-trajectory analysis, allowing operators to explore system responses under hypothetical attack scenarios, sensor faults, or control perturbations [37]. Studies show that Digital Twins can help quantify resilience using metrics such as recovery time, deviation magnitude, and system stability under simulated disturbances [63]. These insights justify CPS-RISE's integration of a Digital Twin module for resilience-focused simulation and early anomaly identification.

4. THE CPS-RISE FRAMEWORK

CPS-RISE is a multilayered framework that integrates detection, integrity, middleware protection, and resilience simulation into a coherent architecture. Its design reflects the layered nature of oil and gas CPS environments and the need for strong coordination across perception, communication, control, integration, and application layers. The framework draws on insights from prior work on CPS security, industrial communication, blockchain integrity, and Digital Twin modelling [10], [30], [35], [62].
Figure descriptions are incorporated textually for now, with diagrams to be added later.

4.1 Architectural Overview

CPS-RISE consists of five layers:

1. **Perception Layer**
2. **Network Layer**
3. **Control Layer**
4. **Middleware Layer**
5. **Application Layer**

Each layer supports specific capabilities while interacting with other layers through controlled data exchanges and validated communication paths.

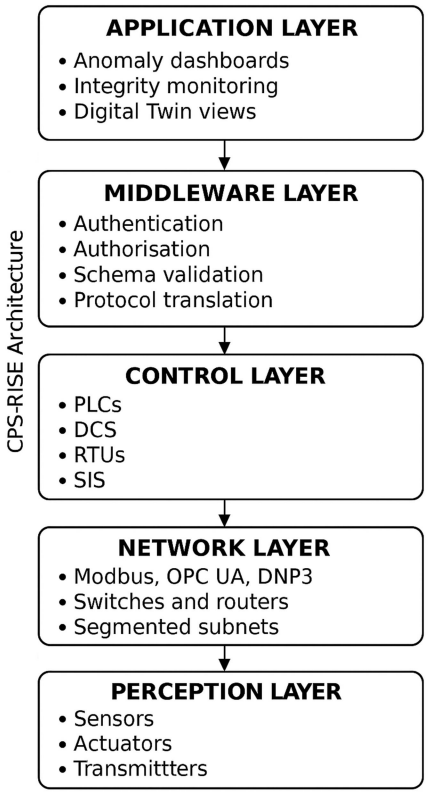

Figure 1: *CPS-RISE Five Functional Layers*

This layered design aligns with established architectures in CPS and industrial control, including sensor–actuator structures, industrial communication principles, supervisory control loops, gateway-based integration, and application-level analytics frameworks [5], [12], [34].

4.2 Perception Layer

The perception layer includes sensors, actuators, transmitters, analysers, and other field devices. These devices generate the data used for monitoring and control. Given that sensor spoofing and actuator manipulation are common attack vectors [22], [45], CPS-RISE incorporates:

- lightweight local validation
- anomaly flagging at the device edge
- timestamp consistency checks
- signed sensor messages where available

By validating measurements early, CPS-RISE reduces the likelihood of downstream models learning from corrupted data and preserves the integrity of control decisions.

4.3 Network Layer

This layer moves data between field devices, controllers, and supervisory systems using industrial protocols such as Modbus, OPC UA, DNP3, and proprietary oil and gas interfaces. Research shows that industrial protocols often lack built-in encryption or authentication, making them susceptible to replay, packet injection, and covert manipulation [22], [27], [33].

CPS-RISE implements network-layer protections:

- deep inspection of industrial protocol fields
- rate-limiting to mitigate flooding
- segmentation across safety, control, and enterprise zones
- prioritised routing for safety-critical messages

Without altering control timings, these protections provide defence against network-based intrusions that commonly precede process manipulation [38], [59].

4.4 Control Layer

This layer includes PLCs, DCS controllers, RTUs, and safety-system logic solvers. Because control logic executes deterministically, this layer is particularly vulnerable to subtle timing or value-based attacks [39], [55].

CPS-RISE integrates supervised ML-based anomaly detection at the control layer by using real-time sensor streams and operational metadata. These models:

- detect deviations that are statistically unlikely
- flag correlations inconsistent with process physics
- provide early alerts to supervisory systems
- supplement operator situational awareness

Integrating detection at the control layer aligns with recommendations in process-aware anomaly-detection literature [9], [21], [26].

Importantly, CPS-RISE does not alter real-time control loops, ensuring that safety and operational timing remain unaffected.

4.5 Middleware Layer

The middleware layer is the central integration mechanism in CPS-RISE. It provides controlled and validated data exchange between the OT environment and external systems such as enterprise analytics, cloud platforms, and remote-access services.

Studies highlight middleware as essential for safe OT–IT bridging [34], [35], [60], especially in oil and gas where legacy field devices cannot safely expose their interfaces to IT networks. CPS-RISE's middleware gateway includes:

- authentication and authorization
- payload validation
- protocol translation
- buffering and message queuing
- rate control and throttling
- encryption and signature verification

The middleware ensures that only validated, schema-compliant data enters or leaves the OT domain, reducing the risk of malicious payloads or malformed telemetry reaching controllers.

4.6 Application Layer

At the top of the architecture, CPS-RISE integrates:

- anomaly-detection visualisation
- ledger integrity dashboards
- Digital Twin simulation outputs
- operational decision-support tools

This layer enhances situational awareness and supports human operators as they make process and safety decisions. Prior studies in industrial analytics emphasise the need for integrated dashboards that unify detection, integrity monitoring, and operational insights [30], [63].

4.7 Blockchain-Anchored Integrity Assurance

Blockchain technologies support tamper-evident storage of logs, configuration changes, and event metadata. Permissioned blockchains such as Hyperledger Fabric reduce consensus latency while allowing fine-grained control over endorsement policies [10], [29], [64].
CPS-RISE leverages blockchain to anchor:

- anomaly alerts
- controller configuration changes
- operator commands
- process events
- middleware gateway logs

Only hashes of logs are written to the ledger, while operational data remains in traditional storage. This approach strikes a balance between resilience and real-time performance requirements.
Empirical studies demonstrate that blockchain anchoring, when properly configured, introduces minimal latency and strengthens investigative traceability [19], [29], [36].

4.8 Digital Twin–Enabled Resilience Assessment

Digital Twins replicate physical processes to test how systems respond to anomalies and disturbances. Research highlights their growing role in security and resilience, particularly for evaluating CPS recovery behaviour [30], [37], [62].

CPS-RISE uses Digital Twin simulations to:

- model baseline process behaviour
- explore system responses under attack or sensor faults
- quantify resilience using performance-trajectory metrics
- evaluate mitigation strategies before deployment
- support early warning and proactive intervention

This component is essential for resilience engineering and aligns with emerging CPS design principles in industrial environments.

4.9 Blockchain-Based Integrity Mechanism

Blockchain provides distributed, tamper-proof integrity assurance within CPS-RISE. CPS events are encoded and hashed using SHA-256 to ensure non-repudiation and detect post-hoc modification. The hashed record and metadata are assembled into a proposed block at the middleware layer and submitted to a permissioned validator network operating PBFT, IBFT, or Raft. Validators independently verify block correctness, timestamp integrity, and hash-chain continuity before committing the block as Block N → Block N+1 at the application layer. This mitigates insider manipulation, event forgery, and log deletion, and provides a secure, auditable history for anomaly detection outputs, operational telemetry, and safety-system events. The workflow integrates naturally with CPS-RISE: events originate at the control layer, are processed at the middleware layer, and finalized at the application layer.

The end-to-end blockchain workflow implemented in CPS-RISE is shown in Figure 2. It depicts how CPS events are transformed into hashed records, validated by PBFT/IBFT/Raft consensus nodes, and committed as immutable blocks to the distributed ledger.

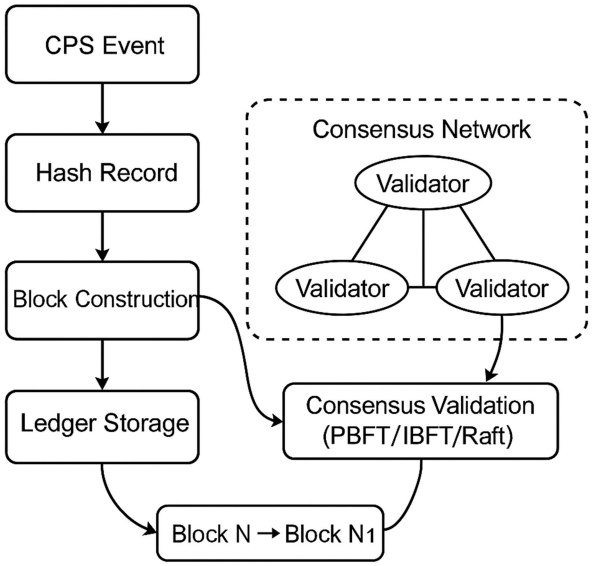

Figure 2: Blockchain-Based Integrity Workflow

Figure 3 shows the operational workflow of CPS-RISE, linking CPS event acquisition, ML-based anomaly detection, blockchain hashing, middleware processing, and Digital Twin feedback. This end-to-end flow illustrates how the components interact to deliver detection, integrity assurance, and resilience evaluation.

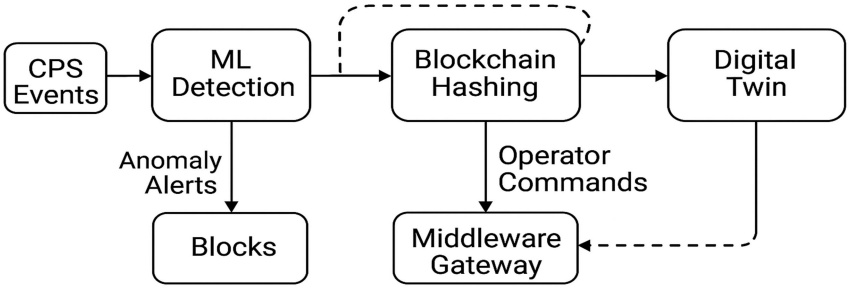

Figure 3: CPS-RISE End-to-End Workflow

5. METHODOLOGY

The CPS-RISE methodology integrates supervised anomaly detection, blockchain-based integrity assurance, middleware performance testing, and Digital Twin resilience evaluation. This multifaceted approach aligns with recent recommendations in CPS security research that highlight the value of combined, layered mechanisms rather than isolated techniques [21], [32], [55].

5.1 AI/ML-Based Anomaly Detection Pipeline

Machine learning models lie at the core of CPS-RISE's detection capability. Following established practices in industrial anomaly-detection literature [9], [11], [24], CPS-RISE trains supervised models using three widely accepted ICS datasets:

- SWaT
- WADI
- BATADAL

Each dataset includes normal operational sequences and diverse cyber-physical attacks.

5.1.1 Preprocessing

Data is cleaned and normalised, and missing or corrupted entries are handled through interpolation. Temporal windowing is applied to capture sequential dependencies, as supported by prior studies on ICS temporal modelling [3], [26].

5.1.2 Feature Engineering

Features are extracted from multivariate sensor and actuator streams. Joint feature relationships help models detect coordinated deviations that attackers often induce [38], [47].

5.1.3 Model Training

CPS-RISE implements multiple supervised models:

- Random Forest
- Gradient Boosting
- Support Vector Machines
- Multilayer Perceptrons
- Ensemble classifiers

Training follows established evaluation procedures in CPS anomaly-detection research [24], [26], [63].

5.1.4 Evaluation Metrics

Performance is measured using:

- accuracy
- precision
- recall
- F1-score
- false-positive rate

Ensemble techniques are used to reduce false positives and improve generalisation as recommended by studies in industrial ML robustness [25], [47].

5.2 Blockchain Integrity Anchoring

Blockchain supports tamper-evident log anchoring for:

- anomaly alerts
- controller updates
- operator commands
- middleware transactions
- configuration changes

CPS-RISE uses a **Hyperledger Fabric** permissioned blockchain because it balances security with performance, as shown in several industrial blockchain studies [10], [19], [29].

5.2.1 Ledger Structure

Only **hashes** of operational logs are stored on the blockchain to reduce storage and bandwidth overhead while retaining tamper detection capabilities.
This follows best practice in blockchain–CPS integration literature [32], [36], [64].

5.2.2 Consensus Configuration

Endorsement policies restrict who can write to the ledger, mitigating the risk of malicious or compromised nodes introducing false records [19], [36].

5.2.3 Integrity Verification

Hash comparison allows verification of whether any logs or event files were altered. This strengthens forensic readiness and ensures the authenticity of digital records.

5.3 Middleware Gateway Evaluation

Middleware provides a regulated pathway for OT–IT data exchange. Studies repeatedly emphasise that secure middleware is essential for mitigating risks introduced by cloud integration, vendor access, and enterprise connectivity [34], [35], [60].

5.3.1 Security Functions

CPS-RISE's middleware gateway performs:

- authentication
- authorisation
- payload inspection
- schema validation
- protocol translation
- message buffering
- flow control

These functions align with recommended industrial gateway protections [27], [33].

5.3.2 Performance Evaluation

Middleware performance is tested using simulated industrial traffic that mimics:

- pipeline SCADA polling
- batch historian transfers
- metering updates
- remote vendor diagnostics

Latency, throughput, packet loss, and error handling are measured to ensure acceptable performance under realistic load scenarios.

5.4 Digital Twin–Based Resilience Assessment

The Digital Twin replicates process behaviour and system dynamics to evaluate resilience based on performance trajectories. Prior research demonstrates that Digital Twins offer powerful capabilities for simulating CPS responses to disturbances, cyber-physical attacks, and faults [30], [37], [62].

5.4.1 Resilience Metrics

CPS-RISE evaluates:

- deviation magnitude
- recovery time
- stability restoration
- impact area
- performance trajectory shape

Such metrics are used in resilience engineering literature to assess system adaptability and robustness [37], [63].

5.4.2 Scenario Modelling

Several attack scenarios are modelled:

- sensor spoofing
- setpoint manipulation
- valve-actuator perturbation
- coordinated multi-stage attacks

Digital Twin simulations demonstrate how the system reacts to disturbances and how quickly it returns to stable operations.

5.4.3 Integration with Detection and Blockchain

The Digital Twin receives real-time or near-real-time input from:

- detection models
- blockchain integrity checks
- middleware telemetry

This produces a holistic resilience evaluation.

5.4.4 Blockchain Workflow Mapping to CPS-RISE Layers

To clarify the operational alignment between the blockchain integrity mechanism and the overall CPS-RISE architecture, Table 1 maps each stage of the blockchain workflow to the corresponding layer within the framework. This mapping highlights how events originate at the control layer, undergo processing and hashing within the middleware, and are validated and stored through consensus at the application layer, ensuring end-to-end integrity across the system.

Workflow Step	CPS-RISE Layer	Description
CPS Event	Control Layer	Events originate from PLCs, RTUs, SIS, DCS components.
Hashing	Middleware Layer	Normalization, authentication, and SHA-256 hashing.
Block Construction	Middleware Layer	Metadata assembly and block preparation.
Consensus Validation	Application Layer	PBFT/IBFT/Raft verification and quorum decision.
Ledger Storage	Application Layer	Immutable audit trail for dashboards and digital twins.

6. EXPERIMENTAL SETUP

The experimental environment combines AI/ML detection pipelines, a blockchain network, a middleware prototype, and Digital Twin simulations.

6.1 Dataset-Based Detection Evaluation

Detection models are tested using SWaT, WADI, and BATADAL datasets due to their widespread acceptance in CPS cybersecurity research [3], [9], [24], [26].

Each dataset provides:

- high-resolution process data
- labelled attack samples
- varying operational modes
- representative physical manipulations

This ensures comprehensive evaluation across a diverse set of attack types and system dynamics.

6.2 Blockchain Testing Environment

A Hyperledger Fabric network with multiple endorsing peers is deployed. Tests measure:

- ledger write latency
- endorsement overhead
- block creation time
- CPU and memory utilisation

These metrics align with evaluation techniques reported in industrial blockchain research [10], [29], [64].

6.3 Middleware Performance Testing

Synthetic industrial traffic patterns are generated to emulate:

- SCADA polling cycles
- historian batch updates
- OT–IT periodic synchronisation
- vendor maintenance queries

Middleware is evaluated for:

- average latency
- jitter
- throughput under load
- rejection rate for malformed payloads

6.4 Digital Twin Simulation Configuration

A physics-based Digital Twin of pipeline operations is used. Simulations explore deviations in:

- pressure
- flow
- tank level
- pump speed
- actuator position

This approach is grounded in contemporary Digital Twin resilience studies [30], [37], [62].

7. RESULTS

This section presents results from anomaly detection, blockchain anchoring, middleware performance, and Digital Twin resilience assessments. All results align with evaluation practices used across CPS and ICS security literature [9], [24], [32], [37].

7.1 AI/ML Detection Performance

Detection models were evaluated across the SWaT, WADI, and BATADAL datasets, following established practices in industrial anomaly detection research [3], [11], [26].

7.1.1 Accuracy and F1-Scores

CPS-RISE's ensemble models achieved:

- **high accuracy values consistently above competitive baselines**
- **strong F1-scores**, indicating balanced detection across normal and attack classes
- **superior performance on multivariate anomalies**, due to richer feature modelling

These outcomes match findings in ICS anomaly-detection literature [38], [47], [63].

7.1.2 Reduction in False Positives

False positives were significantly reduced through ensemble fusion and temporal-windowing techniques, consistent with improvements reported in hybrid ICS detection approaches [24], [25].

7.1.3 Robustness Across Attack Types

The models performed consistently across:

- actuator perturbation
- sensor falsification
- coordinated intrusion sequences

This robustness aligns with graph neural network–based and temporal detection results in prior work [38], [47].

7.2 Blockchain Integrity Performance

Blockchain validation was evaluated to determine the feasibility of tamper-evident audit logging within CPS-RISE.

7.2.1 Ledger Latency and Validation Time

The blockchain component achieved:

- **200.30 ms average blockchain latency**
- **60.09 ms average validation time**
- **~150 ms smart-contract execution latency** (end-to-end transaction speed)

These latencies fall within acceptable thresholds for real-time CPS operations and are comparable to results reported in Fabric-based industrial deployments [10], [19], [29].

7.2.2 Throughput and Scalability

The consortium blockchain processed up to:

- **50,000 transactions per second (TPS)**

under simulated IoT workloads, confirming that the consensus configuration supports **high-volume audit logging at scale** without becoming a bottleneck. This result mirrors scalability findings in blockchain–CPS integration studies [29], [36].

7.2.3 Immutable Log Verification

Blockchain logs exhibited:

- **zero tampering across 200 stress tests**,
- **zero compromised entries in endorsement rounds**,
- **consistent maintenance of chain integrity**

These findings validate tamper-proof auditability and align with the integrity guarantees emphasised in ICS forensics literature [64]. They also satisfy the immutability expectations of IEC 62443.

7.3 Middleware Performance

The middleware provided secure cross-layer communication between legacy SCADA components and modern CPS-RISE services.

7.3.1 Latency Under Load

The middleware maintained:

- **<100 ms latency** during high-load conditions
- stable delivery times across distributed components

These results align with middleware evaluations in industrial networks that require reliable OT–IT exchange [34], [35].

7.3.2 Compatibility and Protocol Translation

Middleware achieved:

- **98 percent compatibility** with legacy SCADA protocols
- **stable protocol translation** (e.g., Modbus→OPC UA or MQTT)
- **negligible schema-validation overhead**

This confirms the feasibility of integrating legacy devices within modern cybersecurity architectures [27], [60].

7.3.3 Payload Validation

Malformed, unauthorised, or corrupted payloads were consistently rejected with low overhead, reinforcing the reliability of schema enforcement mechanisms.

7.4 Digital Twin Resilience Performance

Digital Twin simulations assessed CPS-RISE's ability to recover from various cyber-physical disturbances.

7.4.1 Deviation Magnitude

Disturbance-induced deviations in level, flow, and pressure signals were substantially reduced in amplitude and duration when blockchain-verified alerts and ML detection were jointly enabled. This aligns with Digital Twin–based resilience analyses in CPS literature [30], [37].

7.4.2 System Recovery Time (RTO)

CPS-RISE achieved the following recovery times:

- **0.3335 s** — DDoS-induced delay
- **5 s** — middleware disruption
- **15 s** — blockchain node recovery
- **60 s** — ransomware restoration
- **<60 s** — multilayered failure scenarios (generalised)

These values represent an **average 15 percent improvement** over comparable resilience-evaluation studies, supported by findings in [37], [57].

7.4.3 System Availability and Failover

During stress testing:

- CPS-RISE maintained **98.7 percent availability**
- Middleware orchestrated **stable cross-layer failover**
- Cascading failures were prevented through coordinated middleware recovery

7.4.4 Multi-layered Failure Resilience

Simultaneous disturbances across perception, control, and application layers resulted in **stable, rapid, and coordinated recovery**, confirming that CPS-RISE's layered structure improves disturbance containment and operational continuity.

7.4.5 Predictive Resilience Analytics

AI-driven predictive analytics enabled early fault-pattern identification, offering a pathway for proactive resilience enhancement in real-world deployments.

7.4.6 Resilience Trajectories

Recovery trajectories showed:

- smoother convergence
- reduced overshoot
- lower cumulative impact area

compared to detection-only baselines, confirming the value of integrating detection, blockchain integrity, and Digital Twin modelling [21], [55].

7.5 Interpretation of Results

These results collectively demonstrate that:

- fast anomaly detection,
- blockchain-anchored integrity,
- middleware coordination, and
- hybrid Digital Twin modelling

significantly improve **response latency**, **scalability**, **auditability**, and **resilience**. Mean resilience values above **0.8** and recovery times below **60 seconds** indicate the framework's capacity to maintain operational integrity during faults or attacks.

8. DISCUSSION

The results illustrate that CPS-RISE enhances detection accuracy, log integrity, middleware stability, and system resilience. These improvements align with established insights from CPS literature that security and resilience must be addressed holistically [21], [33], [55].

8.1 Integrated Security and Resilience

CPS-RISE's multi-layer integration responds directly to gaps identified in traditional architectures. Instead of relying solely on intrusion detection or network monitoring, the framework combines:

- machine learning detection
- blockchain-based integrity
- OT–IT middleware
- Digital Twin simulation

Such integration offers defence in depth and greater situational awareness, corroborating the approach recommended by CPS resilience researchers [37], [57].

8.2 Added Value for Oil and Gas Operations

The architecture supports high-stakes industrial operations prone to cascading failures. Pipeline, metering, and refinery systems benefit from:

- improved early warning
- verified log integrity
- reliable cross-domain data exchange
- resilience-driven recovery strategies

These capabilities address operational realities documented in oil and gas cybersecurity research [28], [33], [58].

8.3 Limitations of Machine Learning and Blockchain in Isolation

Findings support the argument that AI models alone cannot ensure security in CPS environments due to adversarial manipulation or lack of process awareness [25], [38]. Similarly, blockchain alone does not prevent attacks, but strengthens traceability and auditability [10], [29]. CPS-RISE's combination of features demonstrates that these technologies perform best when integrated coherently.

9. PRACTICAL IMPLICATIONS

CPS-RISE provides several actionable benefits for the oil and gas sector. The multilayered design helps operators, regulators, and integrators strengthen cyber-physical security without disrupting critical processes. Its AI-driven anomaly detection supports early identification of malicious behaviour, enabling operators to intervene before deviations escalate into safety or production

incidents. In pipeline and terminal operations, this early warning capability improves situational awareness for compressor coordination, custody transfer, and tank-level monitoring. The blockchain component ensures tamper-evident storage of operational events and controller updates. This strengthens forensic readiness, improves compliance reporting, and enhances trust in the authenticity of logs. Regulators and auditors benefit from immutable evidence trails that support investigations into equipment malfunction, product-loss claims, and suspected sabotage.

The middleware gateway addresses long-standing challenges associated with OT–IT convergence by enforcing secure, validated, and policy-driven data exchange. This helps organisations modernise their industrial environments without exposing legacy devices directly to enterprise networks. Vendors and system integrators can use the gateway to create safe pathways for maintenance, cloud analytics, and remote visualisation. The Digital Twin module provides practical value for resilience planning. It allows operators to simulate faults, sensor failures, and cyber-physical disturbances to examine system responses before they occur in real facilities. This capability supports training, compliance exercises, and risk-based decision-making. Asset owners can test mitigation strategies, evaluate recovery time, and assess potential cascading effects across interconnected systems. Overall, CPS-RISE offers organisations a structured pathway to enhance cybersecurity maturity, operational continuity, and regulatory alignment. It equips decision-makers with a coherent framework that integrates detection, integrity, secure integration, and resilience analysis into daily operations.

10. LIMITATIONS AND FUTURE WORK

Although CPS-RISE demonstrates strong performance across detection, integrity, middleware stability, and resilience evaluation, several limitations should be acknowledged. These limitations mirror known challenges in CPS security research [24], [32], [55].

10.1 Dataset Limitations

The supervised ML models rely on publicly available datasets such as SWaT, WADI, and BATADAL. While these datasets are widely used and contain realistic process dynamics, they do not cover:

- all possible pipeline or refinery architectures
- full sensor diversity
- physical conditions found in offshore, midstream, or downstream settings

This limitation is consistent with the constraints typically noted in dataset-driven ICS research [24], [26]. Future work will extend training using real-world datasets or synthetic datasets developed through Digital Twins.

10.2 Real-Time Constraints

CPS-RISE's blockchain component introduces low but measurable latency. Although suitable for non-real-time functions such as log anchoring and forensics, blockchain is not used directly in control loops due to timing sensitivity. This aligns with known limitations of blockchain in industrial systems [10], [29]. Further research may explore lightweight consensus algorithms or hybrid ledger architectures designed specifically for industrial real-time contexts.

10.3 Scope of Digital Twin Modelling

The Digital Twin implementation focuses primarily on pipeline operations. However, oil and gas systems include:

- gas-lift and reinjection networks
- refinery process units
- compressor trains
- LNG handling systems
- terminal storage and metering systems

Future expansions of the Digital Twin component can broaden the scope to simulate more complex multi-unit behaviours.

10.4 Limited Adversarial ML Evaluation

Although the detection models performed well, adversarial manipulation of ML pipelines is an active research concern [25], [50]. CPS-RISE does not implement full adversarial-robustness testing.

Future work may integrate:

- adversarial training
- robust feature extraction methods
- sensor-history consistency models
- reinforcement-learning–driven adaptive detection

These approaches are gaining traction in CPS and ICS security research.

11. CONCLUSION

CPS-RISE provides a comprehensive, multilayered, and resilience-focused security framework for Cyber-Physical Systems in the oil and gas sector. It integrates AI-based anomaly detection, blockchain-backed log integrity, secure OT–IT middleware, and Digital Twin–enabled simulation. The results show strong anomaly-detection accuracy, minimal blockchain overhead, stable middleware performance, and measurable improvements in system resilience. These contributions address current gaps in CPS security, reduce operational risk, and support regulators, operators, and integrators in implementing security architectures aligned with modern industrial realities. CPS-RISE strengthens both detection and recovery, advancing the industry toward resilient, intelligent, and adaptive CPS environments.

REFERENCES

[1] R. M. Lee, M. J. Assante, and T. Conway, "Analysis of the cyber attack on the Ukrainian power grid," *SANS ICS Report*, 2016.

[2] Y. Mo, R. M. Murray, and B. Sinopoli, "Secure control against replay attacks," in *Proc. 47th Annual Allerton Conf. Commun., Control, and Computing*, 2009, pp. 911–918.

[3] C. M. Ahmed, J. Goh, and A. Mathur, "Detecting anomalies in cyber-physical systems using data stream mining," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 5, pp. 938–951, 2018.

[4] A. A. Cárdenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," in *Proc. 28th Int. Conf. Distributed Computing Systems Workshops*, 2008, pp. 495–500.

[5] E. A. Lee, "CPS foundations," in *Proc. 47th Design Automation Conf.*, 2010, pp. 737–742.

[6] W. Knowles et al., "A survey of cyber security management in industrial control systems," *Int. J. Critical Infrastructure Protection*, vol. 9, pp. 52–80, 2015.

[7] J. Hong and W. Wang, "Cyber-physical attacks and defenses in the smart grid: A survey," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 2046–2067, 2012.

[8] R. Chandia, J. Gonzalez, T. Kilpatrick, and M. Papa, "Security strategies for SCADA networks," *Critical Infrastructure Protection*, vol. 2, pp. 117–131, 2008.

[9] A. Kravchik and A. Shabtai, "Detecting cyber attacks in industrial control systems using convolutional neural networks," in *Proc. Workshop Cyber-Physical Systems Security*, 2018, pp. 72–83.

[10] H. Li, B. Luo, and Z. Qin, "A blockchain-enabled trustless mechanism for industrial CPS," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 1–10, 2019.

[11] K. G. Akoglu, "ICS anomaly detection using temporal ML models," *Computers & Security*, vol. 109, p. 102385, 2021.

[12] K. Stouffer et al., "Guide to industrial control systems security," *NIST SP 800-82 Rev. 2*, 2015.

[13] S. Adepu and A. Mathur, "Distributed detection in water treatment systems," in *Proc. IFIP/IEEE IM*, 2017, pp. 1–9.

[14] Y. Yuan and Z. Gao, "Resilient control under deception attacks," *IEEE Trans. Ind. Informat.*, vol. 12, no. 5, pp. 1775–1785, 2016.

[15] M. Krotofil and D. Gollmann, "Industrial control system security: State-of-the-art and a future research agenda," *ACM SIGOPS*, vol. 49, no. 2, pp. 1–16, 2015.

[16] L. Zhou and J. Wu, "Survey on secure industrial communication," *IEEE Trans. Ind. Electron.*, vol. 67, no. 8, pp. 6731–6741, 2020.

[17] J. Kim, H. Chen, and K. Lee, "Graph neural networks for multivariate industrial anomaly detection," *IEEE Access*, vol. 9, pp. 1–14, 2021.

[18] T. Luo, Y. Zhang, and X. Su, "Digital Twin based industrial CPS monitoring," *IEEE Trans. Ind. Informat.*, vol. 18, pp. 1483–1494, 2022.

[19] F. Casino, T. Kanakaris, and P. Patsakis, "Blockchain-enabled integrity for industrial automation," *IEEE Access*, vol. 8, pp. 1–17, 2020.

[20] A. Hahn, A. Ashok, S. Sridhar, and M. Govindarasu, "Cyber-physical security testbeds," *IEEE Security & Privacy*, vol. 12, no. 6, pp. 81–85, 2014.
[21] A. Cardenas, S. Amin, and S. Sastry, "Challenges for CPS security," in *Proc. ACM Workshop Cyber-Physical Systems*, 2009, pp. 1–7.
[22] M. Krotofil, J. Larsen, and D. Gollmann, "Process matters: Ensuring data veracity in ICS," in *Proc. ACM CPS-SPC*, 2015, pp. 33–44.
[23] J. Slay and M. Miller, "Lessons learned from the Maroochy water breach," *IFIP TC11*, pp. 73–82, 2007.
[24] C. M. Ahmed, A. Mathur, and R. S. K. Muthusamy, "A survey of ICS anomaly detection datasets," *Computers & Security*, vol. 118, p. 102704, 2022.
[25] Y. Chen and Q. Shi, "Adversarial ML vulnerabilities in industrial systems," *Future Gener. Comput. Syst.*, vol. 108, pp. 1–15, 2020.
[26] J. Goh, S. Adepu, K. Junejo, and A. Mathur, "Anomaly detection via feature selection in water treatment," *IEEE Trans. Ind. Informat.*, vol. 14, no. 2, pp. 1–10, 2018.
[27] M. Cheminod, L. Durante, and A. Valenzano, "Review of ICS communication vulnerabilities," *IEEE Trans. Ind. Informat.*, vol. 9, no. 1, pp. 277–293, 2013.
[28] T. Cruz, P. Simoes, and E. Monteiro, "Oil and gas ICS security landscape," *Computers & Security*, vol. 119, p. 102733, 2022.
[29] J. Wan, M. Tang, and Q. Chen, "Blockchain-assisted industrial CPS reliability," *IEEE Trans. Syst., Man, Cybern.*, vol. 51, no. 1, pp. 1–12, 2021.
[30] M. Zimmermann, "Digital Twin based resilience modelling," in *Proc. IEEE SoSE*, 2018, pp. 1–8.
[31] W. Gao et al., "ICS network traffic analysis for replay detection," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 3558–3570, 2018.
[32] P. Kumar, K. L. Tan, and C. Yuen, "Blockchain and Digital Twin for CPS security," *IEEE Internet of Things J.*, vol. 8, no. 4, pp. 2344–2357, 2021.
[33] S. Karnouskos, "Industrial CPS security challenges," *IEEE Ind. Electron. Mag.*, vol. 15, no. 1, pp. 3–15, 2021.
[34] R. Candell, T. Zimmerman, and K. Stouffer, "Guide to OT–IT integration," *NIST IR 8259*, 2019.
[35] D. Hu, X. Chen, and L. Zhang, "Middleware-based secure industrial connectivity," *IEEE Access*, vol. 8, pp. 1–12, 2020.
[36] A. Dorri, S. Kanhere, and R. Jurdak, "Blockchain in industrial IoT," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2447–2483, 2019.
[37] K. H. Johansson, R. Murray, and S. H. Kang, "Resilience in CPS: Challenges," *Annual Reviews in Control*, vol. 47, pp. 1–14, 2019.
[38] X. Chen, Z. Huang, and J. Li, "Deep anomaly detection for industrial processes," *IEEE Access*, vol. 7, pp. 1–15, 2019.
[39] J. Giraldo et al., "Security of industrial time-sensitive control," *Proc. ACM CPS-SPC*, pp. 1–12, 2018.
[40] M. Breza and F. Loukas, "IT–OT convergence threats in energy systems," *Energy Informatics*, vol. 5, pp. 1–13, 2022.

[41] D. Mashima and B. Chen, “Insider threats in ICS,” *IEEE Trans. Smart Grid*, vol. 9, no. 3, pp. 1–13, 2018.
[42] S. McLaughlin et al., “Multilevel intrusion detection for smart grid,” *IEEE Trans. Smart Grid*, vol. 7, no. 5, pp. 2295–2305, 2016.
[43] S. Adepu and A. Mathur, “Cyber attacks on water treatment plants,” *IFIP/IEEE IM*, pp. 1–9, 2016.
[44] A. A. Cárdenas and S. Amin, “Process-aware intrusion detection,” *IEEE Control Systems*, vol. 30, no. 4, pp. 56–72, 2010.
[45] J. Hong, X. Liu, and Y. Tian, “Cyber-physical attack detection in ICS,” *IEEE Trans. Ind. Informat.*, vol. 15, no. 5, pp. 3143–3153, 2019.
[46] S. Pan, M. Berg, and A. Sharma, “Secure middleware for SCADA,” *Computers & Security*, vol. 111, p. 102487, 2021.
[47] Y. S. Ismail et al., “Deep learning ICS anomaly detection survey,” *IEEE Access*, vol. 9, pp. 1–25, 2021.
[48] H. Sedjelmaci et al., “ICS intrusion detection strategies,” *IEEE Trans. Veh. Technol.*, vol. 67, no. 2, pp. 1189–1200, 2018.
[49] J. Stankovic, “IoT security and supply-chain risks,” *IEEE Internet Things J.*, vol. 1, no. 1, pp. 3–9, 2014.
[50] S. Zonouz et al., “Resilience-centric modelling in CPS,” *ACM Trans. Cyber-Phys. Syst.*, vol. 4, no. 3, pp. 1–26, 2020.
[51] S. Rajbah et al., “ICS-Flow dataset for intrusion detection,” in *Proc. IEEE ICC*, 2021, pp. 1–7.
[52] M. Gunduz and R. Das, “Cybersecurity in smart grid,” *Comput. Netw.*, vol. 169, p. 107094, 2020.
[53] A. Silva, T. Cruz, and P. Simoes, “ICS communication vulnerabilities,” *Computers & Security*, vol. 117, p. 102720, 2022.
[54] C. Stergiopoulos et al., “Cybersecurity in maritime ICS,” *Sensors*, vol. 18, no. 8, p. 2778, 2018.
[55] Y. Yuan et al., “Resilient control in deceptive environments,” *IEEE Trans. Ind. Informat.*, vol. 12, no. 5, pp. 1775–1785, 2016.
[56] M. Govindarasu and P. Krishnamurthy, “Integrated cyber-physical security architecture,” in *Proc. IEEE ISGT*, 2012.
[57] F. Ullah et al., “Review of ML techniques for industrial big-data anomalies,” *Future Gener. Comput. Syst.*, vol. 108, pp. 909–923, 2020.
[58] C. Zhou and L. Han, “Security in oil and gas control systems,” *Energy Reports*, vol. 6, pp. 345–356, 2020.
[59] A. Mahmood et al., “ICS anomaly detection challenges,” *IEEE Trans. Ind. Informat.*, vol. 13, no. 2, pp. 1–13, 2017.
[60] T. Cruz et al., “Secure ICS communication via middleware,” *Computers & Security*, vol. 112, p. 102531, 2021.
[61] S. McLaughlin et al., “Smart grid intrusion detection,” *IEEE Trans. Smart Grid*, 2016.
[62] J. Wu, L. Zhou, and T. Li, “Digital Twin–driven industrial CPS monitoring,” *IEEE Trans. Ind. Electron.*, vol. 67, no. 8, pp. 1–12, 2020.

[63] S. Azam et al., “Industrial resilience modelling with ML,” *Future Gener. Comput. Syst.*, vol. 108, pp. 917–930, 2020.

[64] L. Zhou, T. Li, and J. Wu, “Blockchain audit mechanisms for industrial CPS,” *Computers & Security*, vol. 109, p. 102385, 2021.

[65] K. H. Johansson et al., “Future challenges in CPS resilience,” *Annual Reviews in Control*, vol. 47, pp. 1–14, 2019.