Review

Toward Mission-Centric Cyber-Physical Defense: Coordinated, Explainable, and Human-in-the-Loop Strategies for Power CPS

Gang Zhang *

Posted Date: 19 May 2025

doi: 10.20944/preprints202505.1425.v1

Keywords: Power Cyber-Physical Systems; Mission-Centric Cyber Defense; Human-in-the-Loop Security; Explainable Artificial Intelligence; Multi-Agent and Distributed Defense; Resilience Metrics and Post-Attack Recovery

doi:10.20944/preprints202505.1425.v1

Review

Toward Mission-Centric Cyber-Physical Defense: Coordinated, Explainable, and Human-in-the-Loop Strategies for Power CPS

Gang Zhang

School of Electrical and Electronic information, Xihua University, Chengdu, China; gang_ee@outlook.com

Abstract: The convergence of cyber, physical, and human elements in modern power systems brings both operational advantages and escalating security challenges. Beyond traditional False Data Injection Attack (FDIA) defenses, emerging threats now involve coordinated, multi-stage, and AI-driven cyber-physical attacks across technical, organizational, and market layers. This review proposes a mission-centric defense paradigm for Power Cyber-Physical Systems (Power CPS), integrating architectural resilience through redundancy, diversity, and trustworthy sensing with real-time, explainable, and human-in-the-loop defense mechanisms. It emphasizes the role of multi-agent coordination, edge-cloud collaboration, and operator-centered situational awareness in ensuring effective response and mission continuity. Post-attack recovery strategies, including data reconstruction, adaptive reconfiguration, and resilience metric integration, are also explored. Finally, the review highlights future research and cross-sector collaboration needs to advance holistic cyber-physical-human resilience for secure energy system operations.

Keywords: Power Cyber-Physical Systems; Mission-Centric Cyber Defense; Human-in-the-Loop Security; Explainable Artificial Intelligence; Multi-Agent and Distributed Defense; Resilience Metrics and Post-Attack Recovery

1. Introduction

1.1. Background: Cyber-Physical Integration in Modern Power Systems

The rapid digitalization of modern power systems has led to the emergence of Power Cyber-Physical Systems (Power CPS), which tightly integrate physical electrical infrastructure with digital computing, communication, and control technologies [1–3]. This integration has transformed the way power systems are monitored, controlled, and optimized, enabling new capabilities such as real-time state estimation, distributed energy resource (DER) integration, wide-area monitoring, and autonomous control [4,5]. Advanced components such as Phasor Measurement Units (PMUs), Supervisory Control and Data Acquisition (SCADA) systems, smart meters, Internet of Things (IoT) devices, and Artificial Intelligence (AI)-driven analytics now play central roles in ensuring reliable and efficient grid operations [6–9].

However, this convergence of cyber and physical domains has also introduced new cyber vulnerabilities that traditional power system security practices were not designed to address [10]. Cyber attackers can exploit communication channels, software vulnerabilities, and human factors to compromise system integrity, confidentiality, and availability. Among the most well-documented and studied cyber threats in the Power CPS domain are False Data Injection Attacks (FDIAs), which target the state estimation process by stealthily manipulating measurement data while evading traditional bad data detection mechanisms [11–13].

While FDIAs have received significant attention in the literature over the past decade, real-world cyber-physical incidents such as the 2015 and 2016 Ukraine power grid attacks, the Stuxnet attack on industrial control systems, and the Colonial Pipeline ransomware incident have demonstrated that attackers increasingly employ coordinated, multi-stage strategies that go beyond simple data manipulation [14]. These attacks exploit cross-layer and cross-domain dependencies between cyber, physical, market, and human elements, often leveraging advanced persistent threats (APTs), supply chain compromises, and social engineering techniques to achieve their objectives [15].

1.2. Limitations of Detection-Only Paradigms and FDIA-Focused Reviews

Despite growing awareness of these evolving threat landscapes, much of the current research remains narrowly focused on detection-centric paradigms, particularly on FDIAs [16–19]. While detecting FDIAs is undoubtedly important, an overemphasis on detection alone presents several limitations:

- **Narrow Threat Coverage:** Detection methods often target specific attack models, such as linear FDIA formulations, without addressing broader multi-vector and coordinated threats that exploit multiple system layers.
- **Post-Compromise Detection:** Most detection mechanisms operate after the attacker has already penetrated the system, which limits their ability to prevent initial compromise or mitigate cascading effects in real time [20,21].
- **Lack of Coordinated Response:** Detection alone does not guarantee effective response or recovery. Without coordinated defense mechanisms that involve both automated systems and human operators, detected attacks may still cause significant operational disruptions [22].
- **Neglect of Human Factors:** Many detection algorithms assume fully automated operation and overlook the critical role of human operators in interpreting, validating, and responding to security alerts [23–25].
- **Insufficient Integration with Operational Objectives:** Detection methods rarely account for the broader mission objectives of power system operators, such as maintaining service reliability, economic efficiency, and regulatory compliance under attack conditions [26].

Existing review articles tend to reinforce these limitations by narrowly framing the cybersecurity challenge as a detection problem, often focusing on comparing machine learning (ML) algorithms or proposing incremental improvements to residual-based detection methods [27–29]. This perspective fails to address the need for **mission-centric**, **coordinated**, and **human-in-the-loop** defense strategies that can proactively safeguard power systems against a wide range of cyber-physical threats.

1.3. Why Mission-Centric, Coordinated, and Human-in-the-Loop Defense Matters

Power systems are **mission-critical infrastructures**, where the primary mission is to ensure the continuous, reliable, and secure delivery of electrical energy to consumers [1,30]. Cybersecurity measures must therefore be aligned with this mission, prioritizing **operational continuity** and **resilience** over purely technical metrics such as detection accuracy or computational efficiency [31,32].

A **mission-centric** defense perspective recognizes that:

- The ultimate goal of cyber defense is not merely to detect attacks but to maintain the safe and reliable operation of the power grid, even in the presence of ongoing cyber-physical disruptions [2].
- Defense strategies must be **coordinated across cyber, physical, market, and human layers**, leveraging distributed intelligence and multi-agent cooperation to detect, respond to, and recover from attacks in real time [33–35].
- Human operators play an **indispensable role** in interpreting complex situations, making informed decisions, and executing response actions that automated systems alone may not be capable of handling. Therefore, **human-in-the-loop** defense mechanisms that provide situational awareness, explainable AI support, and cognitive load management are essential for effective cyber-physical security [36].

By shifting from a narrow detection focus to a **holistic defense paradigm** that integrates **coordinated automation** with **human judgment**, power system operators can better prepare for, withstand, and recover from the increasingly sophisticated cyber-physical threats facing modern energy infrastructures.

1.4. Contributions of This Review

This review offers a comprehensive and forward-looking synthesis of **mission-centric, coordinated, and human-in-the-loop defense strategies** for securing Power CPS. Building upon recent advances in cyber-physical resilience, explainable artificial intelligence (XAI), human-machine collaboration, and distributed defense architectures, the key contributions of this review are summarized as follows:

- **Holistic Characterization of Evolving Cyber-Physical Threats:**
  This review broadens the traditional FDIA-focused perspective by systematically analyzing multi-stage, AI-enhanced, and cross-layer coordinated attacks, including adversarial exploitation of human factors. It highlights the need to move beyond isolated detection toward integrated defense strategies that address threats across the cyber, physical, market, and human layers.
- **Architectural and Mechanistic Foundations for Coordinated and Explainable Defense**: The review proposes mission-centric architectural design principles, incorporating redundancy, diversity, modularity, and cross-layer trust mechanisms to enhance system resilience. It further synthesizes state-of-the-art multi-agent coordination, edge-cloud collaboration, and explainable AI techniques, providing actionable pathways for achieving distributed and operator-trustworthy defense mechanisms.
- **Integration of Human-in-the-Loop and Post-Attack Recovery Strategies:** Recognizing the critical role of human operators in complex grid operations, this review emphasizes situational awareness enhancement, cognitive engineering, and human-machine teaming. It also addresses post-attack recovery, including data reconstruction, operational reconfiguration, and the integration of resilience metrics to sustain mission assurance even under cyber-physical disruptions.
- **Research Roadmap and Cross-Sector Collaboration Agenda:**
  Finally, the review identifies key research gaps, standardization needs, and policy challenges, proposing a collaborative roadmap that unites academia, industry, and regulatory bodies to operationalize scalable, trustworthy, and human-aware cyber-physical defense for future energy systems.

1.5. Structure of This Review

The remainder of this review is structured as follows. Section 2 explores the evolution of cyber-physical threats, emphasizing their growing complexity and coordination. Section 3 introduces architectural foundations for mission-centric defense, while Section 4 presents real-time strategies enabled by explainable and distributed mechanisms. Section 5 turns to human-in-the-loop defense, underscoring the role of operators. Section 6 focuses on post-attack recovery and mission assurance. Section 7 outlines future research directions and collaboration needs, and Section 8 concludes with key insights and a call to action.

2. Evolution of Cyber-Physical Threats in Power CPS

The cybersecurity landscape for Power CPS has rapidly evolved over the past decade [37–39]. While early research largely centered on single-vector threats such as FDIAs, real-world incidents and emerging studies have revealed a far more complex, coordinated, and dynamic adversarial environment [40,41]. This section analyzes this evolving landscape across several dimensions: from isolated data manipulation to coordinated, multi-agent campaigns; from static threat models to AI-enhanced adversarial strategies; and from purely technical attacks to sophisticated exploitation of human and organizational vulnerabilities.

2.1. From Isolated FDIAs to Coordinated Multi-Stage, Multi-Agent Attacks

FDIAs demonstrated that attackers could inject mathematically crafted data into the state estimation process without triggering traditional bad data detection mechanisms [42,43]. These attacks leveraged the inherent linearity of state estimation algorithms to introduce undetectable biases, misleading system operators into making incorrect operational decisions. While this foundational work sparked significant research interest, it represented only the initial stage in the evolution of cyber-physical threats [44–46].

2.1.1. Limitations of Early FDIA Models

Early FDIA models typically made several idealized assumptions [47,48], such as:

- The attacker having full knowledge of the system's topology and parameters.
- The attacker having unrestricted access to all measurement channels.
- The attack targeting a single objective, such as load redistribution or topology masking.

However, real-world attackers operate under constraints such as partial information, limited access, and noisy communication channels [49–51]. These limitations have driven adversaries to develop multi-stage attack strategies that combine reconnaissance, lateral movement, privilege escalation, and coordinated manipulation of cyber and physical assets.

2.1.2. Examples of Multi-Stage, Coordinated Attacks

Real-world incidents such as the 2015 Ukraine power grid attack exemplify this evolution. The attackers:

- Conducted long-term reconnaissance using phishing and malware (BlackEnergy).
- Compromised operator credentials to gain remote access to Supervisory Control and Data Acquisition (SCADA) systems [52].
- Simultaneously manipulated circuit breakers in multiple substations.
- Deployed disk-wiping malware (KillDisk) to hinder recovery efforts.

Similarly, the Stuxnet worm, though not targeting power systems directly, illustrated how malware could manipulate industrial control processes while masking its presence, operating as a multi-agent, multi-vector threat.

These examples underscore the shift from isolated technical exploits to coordinated campaigns involving multiple attack vectors, objectives, and system layers [53–55].

2.2. AI-Enhanced Adversarial Attacks and Model Poisoning Risks

As defenders increasingly adopt **machine learning (ML)** and **artificial intelligence (AI)** for anomaly detection, attackers have begun leveraging AI to design **adaptive and evasive attack strategies** [56–60].

Adversarial Machine Learning Threats

Adversarial ML allows attackers to:

- **Craft adversarial examples** that exploit blind spots in ML-based detection models.
- **Train surrogate models** to simulate the defender's detection system.
- **Optimize attack strategies** using reinforcement learning or evolutionary algorithms to maximize stealth and impact [61].

For example, an attacker could simulate various FDIA patterns offline, selecting those that evade a target's detection model before launching them in a real system.

Federated Learning Poisoning

Federated Learning (FL) has been proposed to enable **privacy-preserving, distributed anomaly detection** across substations, microgrids, and DERs [62–65]. However, FL introduces **new attack surfaces**, such as:

- **Model Poisoning:** Malicious participants submit manipulated model updates to degrade detection performance [66,67].
- **Backdoor Attacks:** Attackers embed hidden triggers that activate malicious behavior under specific conditions [68].
- **Sybil Attacks:** A single attacker mimics multiple legitimate participants to overwhelm model aggregation [69].

Mitigating these risks requires robust aggregation algorithms, participant authentication, and anomaly detection at the model update level.

2.3. Human Factor Exploitation and Social Engineering

While much of the literature focuses on technical exploits, human factors represent a significant and often overlooked vulnerability in Power CPS security [70–72].

Social Engineering and Phishing: Human operators, engineers, and administrators are frequent targets of **social engineering** attacks, including:

- **Phishing Emails:** Trick users into revealing credentials or downloading malware.
- **Impersonation:** Exploit trust relationships to gain unauthorized access.
- **Physical Intrusion:** Manipulate on-site personnel to bypass security controls.

The Ukraine 2015 attack, for instance, began with phishing emails that tricked operators into installing malware, demonstrating the critical role of human vulnerabilities in real-world cyber-physical attacks [73–75].

Cognitive Overload and Alert Fatigue: Even when detection systems function correctly, human operators may:

- **Misinterpret or ignore alerts** due to excessive false positives.
- **Delay response** due to uncertainty or lack of actionable insights.
- **Overlook coordinated attacks** that span cyber, physical, and market layers.

Thus, human-in-the-loop defense strategies must address situational awareness, cognitive load management, and operator training to ensure effective response [76–78].

2.4. Cross-Layer Propagation Across ICT, OT, and Market Operations

Power CPS do not operate in isolation. They depend on:

- **Information and Communication Technology (ICT) networks**, such as public and private telecommunication infrastructures [79].
- **Operational Technology (OT)** systems, including SCADA, Energy Management System (EMS), and DER management platforms [80–82].
- **Energy markets**, where economic signals influence operational decisions.

Cross-Layer Attack Scenarios: Adversaries increasingly exploit **interdependencies** between these layers [83–85]. For example:

- **Telecom Outages:** Disrupt operator situational awareness during grid emergencies.
- **Market Manipulation:** Inject false data to trigger price spikes or imbalance penalties [86].
- **Supply Chain Attacks:** Compromise third-party software or hardware to gain persistent access [87,88].

These cross-layer threats require **integrated situational awareness** that bridges cyber, physical, and market domains.

2.5. Summary of Emerging Threat Characteristics and Gaps

The emerging threat characteristics and gaps are summarized in Table 1.

Table 1. Emerging Threat Characteristics and Gaps.

Threat Dimension	Description	Defense Gap
Multi-Stage, Multi-Agent Attacks	Coordinated campaigns combining multiple attack vectors and objectives	Lack of holistic, coordinated detection and response mechanisms
AI-Enhanced Adversarial Attacks	Adaptive, stealthy attacks exploiting ML detection blind spots	Limited resilience of current ML models to adversarial manipulation
Federated Learning Poisoning	Compromising distributed learning frameworks through malicious model updates	Absence of robust aggregation and participant verification techniques
Human Factor Exploitation	Social engineering, cognitive overload, and operator misjudgment	Insufficient human-in-the-loop defense mechanisms and cognitive engineering support
Cross-Layer Propagation	Exploiting dependencies across ICT, OT, and market operations	Fragmented situational awareness and lack of cross-domain defense coordination

In summary, the cyber threat landscape for Power CPS has evolved beyond isolated technical exploits, demanding coordinated, mission-aware, and human-centered defense strategies [89,90]. The next section will propose architectural foundations for building such defenses.

3. Design Foundations of Mission-Centric Cyber-Physical Defense

In light of the evolving threat landscape outlined in Section 2, defending Power CPS requires more than isolated detection algorithms or ad-hoc countermeasures. It calls for a systematic, architectural shift toward mission-centric defense, where cybersecurity is embedded into the design, operation, and governance of power systems [91–93]. This section presents the foundational design principles necessary to achieve such defense, emphasizing cross-layer architecture, redundancy and diversity, secure sensing and communication, and resilience-enabling modularity.

3.1. Defining Mission-Centric Resilience: Beyond Asset Protection

Traditional security strategies often focus on protecting specific system assets, such as SCADA servers, PMUs, or communication links [94–96]. While important, this asset-centric view falls short of addressing the mission assurance objective of Power CPS—ensuring safe, reliable, and continuous electricity delivery even under attack [97].

Mission-Centric Defense Principles

- **Mission First:** Prioritize maintaining core grid operations (e.g., frequency stability, voltage regulation, black start capabilities) over perfect asset security.
- **Graceful Degradation:** Design systems to continue operating in a degraded but safe state if parts of the system are compromised.
- **Resilience over Robustness:** Enable the system to **adapt and recover** from attacks, rather than merely resisting them through static barriers.

This mission-centric perspective requires rethinking system architecture to support cross-layer defense, where cyber, physical, market, and human elements collaboratively safeguard operational objectives [98–100].

3.2. Cross-Layer Defense Architecture: Cyber, Physical, Market, Human

A **mission-centric defense architecture** must span **cyber**, **physical**, **market**, and **human layers** to comprehensively address the multi-faceted attack surface of Power Cyber-Physical Systems [101,102]. These layers are interdependent, and effective defense requires coordinated mechanisms across all of them [103].

At the **cyber layer**, defense efforts focus on protecting the digital backbone of the grid. This includes securing communication protocols such as **IEC 61850** and **DNP3**, which are widely used for substation automation and real-time grid control. It also involves hardening **SCADA** and **EMS** platforms that manage grid-wide operations [104–106]. Additionally, safeguarding **data storage systems** and **computational resources**, whether centralized in control centers or distributed at the grid edge, is critical to preventing data tampering, service disruption, and computational hijacking attacks [107–110]. The **physical layer** encompasses the tangible assets and sensing infrastructure that constitute the operational core of the power system. This includes **generation units**, **transmission lines**, and **distribution networks**, as well as **DERs**, **microgrids**, and **energy storage systems** that enable renewable integration and local flexibility [111–113]. Critical to physical layer security are the **sensing and actuation devices**, such as **PMUs** and **Remote Terminal Units (RTUs)**, which provide real-time measurements and control signals essential for situational awareness and operational stability [114,115].

Moving to the **market layer**, cyber-physical defense must also account for **economic and market-based mechanisms** that influence system behavior. This includes securing **energy pricing and bidding platforms**, ensuring the integrity of **ancillary service markets** such as frequency regulation and voltage support, and safeguarding **demand response programs** that rely on prosumer participation [116–118]. Manipulation of market signals or exploitation of bidding mechanisms can have cascading impacts on grid reliability and economic fairness, making market-layer security a critical but often overlooked dimension of power system defense [119].

Finally, the **human layer** addresses the role of **system operators**, **field technicians**, **market participants**, **policy makers**, and **cybersecurity analysts** in maintaining grid resilience [120,121]. These human actors are responsible for interpreting data, making real-time decisions, and implementing defense strategies. However, they are also potential targets for **social engineering**, **cognitive overload**, and **insider threats**. Empowering human operators with **situational awareness tools**, **cognitive support systems**, and **decision-making frameworks** is essential to ensuring that technological defenses are effectively managed and adapted in practice [122–124].

In summary, defending Power CPS requires **cross-layer coordination mechanisms** that promote **information sharing**, **trust management**, and **joint decision-making** across these cyber, physical, market, and human layers, moving beyond isolated or siloed defense strategies toward a holistic and mission-centric security architecture **[**125**]**.

3.3. Redundancy, Diversity, and Modularity for Systemic Resilience

Redundancy: Eliminating Single Points of Failure

- **Sensing Redundancy:** Deploy multiple, independent measurement sources (e.g., PMUs, smart meters) to cross-validate data.
- **Communication Redundancy:** Utilize diverse communication channels (e.g., fiber, LTE/5G, satellite) to maintain data flow during disruptions.
- **Control Logic Redundancy:** Implement fallback control strategies on edge devices to maintain safe operation if centralized control is compromised [126].

Diversity: Breaking Homogeneity to Increase Attack Complexity

- **Vendor Diversity:** Avoid reliance on single suppliers for critical hardware or software.
- **Software and Firmware Diversity:** Deploy varying versions or configurations to prevent system-wide exploitation of a single vulnerability.
- **Protocol Diversity:** Support multiple communication standards with isolation mechanisms to contain protocol-specific attacks [127,128].

Modularity: Isolating Risks through Segmentation

- **Microgrids and Virtual Power Plants (VPPs):** Enable localized operation independent of central control [129,130].
- **Regional Control Zones:** Partition the grid into semi-autonomous areas with localized situational awareness and response capabilities.
- **Network Segmentation:** Enforce strict separation between critical operational networks and corporate IT environments [131].

These architectural elements collectively support **systemic resilience**, allowing the grid to **contain, absorb, and recover** from cyber-physical attacks without catastrophic performance loss.

3.4. Secure Sensing and Communication: From Cryptography to Trustworthy Learning

Secure-by-Protocol Approaches

- **Cryptographic Techniques:** Use Message Authentication Codes (MACs), digital signatures, and end-to-end encryption to protect data integrity and confidentiality.
- **Standards Compliance:** Implement protocols such as IEC 62351 to secure power system communications [132].

However, protocol-level security alone is insufficient, especially when attackers exploit insider threats or compromised trusted nodes [133–135].

Secure-by-Learning Approaches

- **Physics-Informed Learning:** Validate data consistency with physical laws (e.g., Kirchhoff's laws) to detect manipulation [136].
- **Behavioral Baselines:** Use machine learning to establish normal operational profiles and flag deviations.
- **Cross-Domain Anomaly Detection:** Correlate cyber, physical, and market data streams to detect coordinated attacks [137].

Challenges and Research Gaps

- **Model Explainability:** Ensuring that AI-driven detection models provide interpretable results for operator validation.
- **Adversarial Robustness:** Hardening learning-based models against adversarial manipulation and model poisoning.
- **Computational Feasibility:** Deploying real-time learning and detection capabilities on **edge devices** with limited resources.

By combining cryptographic assurance with data-driven trust validation, Power CPS can achieve layered security that adapts to evolving threat landscapes [138–170].

In summary, mission-centric cyber-physical defense requires a **coordinated architectural foundation** that integrates cross-layer awareness, systemic resilience through redundancy and diversity, and trustworthy sensing and communication mechanisms. The next section will build on this foundation by presenting **coordinated, explainable, and human-in-the-loop defense mechanisms** designed for real-time cyber [171–173].

4. Coordinated and Explainable Defense Mechanisms

While architectural design sets the foundation for mission-centric cyber-physical defense, effective protection requires dynamic, real-time defense mechanisms capable of detecting, interpreting, and mitigating threats as they unfold [174]. These mechanisms must operate coherently across distributed assets, provide explainable insights to human operators, and support coordinated response actions that minimize operational impact [175]. This section presents the emerging defense paradigms of multi-agent coordination, edge-cloud collaboration, and XAI, alongside the critical role of attack attribution and accountability in response management.

doi:10.20944/preprints202505.1425.v1

4.1. Multi-Agent and Distributed Defense Architectures

4.1.1. Limitations of Centralized Defense

Traditional centralized Security Operations Centers (SOCs), while widely deployed in critical infrastructure sectors, face notable limitations when applied to large-scale and distributed Power CPS environments [176]. High latency often arises when attempting to detect and respond to geographically dispersed threats, reducing the ability to react in real time. Moreover, centralized architectures inherently create single points of failure—attractive targets for adversaries seeking to paralyze grid-wide defense capabilities. As power systems scale in size and complexity, centralized solutions also suffer from limited scalability, making it increasingly difficult to maintain visibility and control across heterogeneous assets such as substations, microgrids, and DERs [177].

4.1.2. Advantages of Multi-Agent Defense Systems

To overcome these limitations, multi-agent defense architectures distribute cybersecurity functions across the hierarchical layers of Power CPS [178]. Local agents deployed in substations and microgrids are empowered to perform real-time anomaly detection and execute autonomous control adjustments. At a higher level, DER aggregators and VPPs can monitor distributed prosumer activities and detect irregularities in market interactions. Transmission control centers serve as coordinating hubs, maintaining wide-area situational awareness and facilitating inter-agent communication [179,180]. These agents operate collaboratively, sharing threat intelligence in near real-time, cross-validating anomaly detections, and coordinating localized response actions. Such distributed architectures not only enhance detection coverage but also relieve central operators from information overload, enabling more agile and resilient defense operations [181].

4.1.3. Key Design Considerations

Designing effective multi-agent defense systems requires careful consideration of autonomy versus coordination. While local agents must make timely, context-aware decisions, they must also contribute to global situational awareness to prevent fragmented or conflicting actions [182]. Communication overhead presents another challenge; efficient protocols must be designed to ensure that bandwidth usage is minimized without compromising information freshness and completeness. Finally, securing inter-agent communication is paramount. Defense frameworks must protect against spoofing, message tampering, and agent compromise, ensuring that the distributed defense network itself does not become a new attack vector [183].

4.2. Edge and Cloud-Based Real-Time Defense Coordination

4.2.1. Role of Edge Computing

Edge computing plays a critical role in enabling real-time cyber-physical defense by moving data processing and security analytics closer to the operational assets of the power system [184]. By deploying Intelligent Electronic Devices (IEDs), local controllers, and other edge computing nodes directly within substations, microgrids, and DER sites, organizations can significantly reduce communication latency, bandwidth consumption, and dependency on centralized infrastructure [185]. These edge nodes are capable of executing lightweight anomaly detection algorithms, applying immediate fallback control actions to contain threats locally, and maintaining secure local logs for post-incident forensic analysis. Such capabilities ensure that even in the face of network congestion or partial isolation, critical defense functions remain active at the grid edge [186].

4.2.2. Role of Cloud Computing

While edge computing offers speed and locality, cloud-based platforms provide the scalability and computational power necessary for large-scale data aggregation, long-term analytics, and global

doi:10.20944/preprints202505.1425.v1

situational awareness [187]. The cloud enables cross-agent coordination by synthesizing insights from distributed edge nodes and facilitating global model updates that improve system-wide defense performance over time. Moreover, the cloud serves as the ideal environment for training advanced AI models using historical and large-scale datasets, enabling the continuous improvement of detection algorithms that can later be deployed to the edge for real-time execution [188].

4.2.3. Hybrid Edge-Cloud Defense Framework

Recognizing the complementary strengths of edge and cloud computing, a hybrid edge-cloud defense architecture integrates both layers to achieve distributed yet coordinated cybersecurity operations. In this framework, edge nodes handle low-latency detection and localized response, ensuring immediate containment of threats, while cloud platforms maintain broader situational awareness, perform model refinement, and provide strategic decision support to human operators and automated agents. This architecture enhances the resilience of the defense system by ensuring that even if cloud connectivity is temporarily degraded or lost, critical edge-based defense mechanisms continue to operate autonomously, maintaining grid security without interruption [189,190].

4.3. Explainable AI for Operator-Trustworthy Defense Decision Support

4.3.1. Challenges of Black-Box AI Models

While AI and machine learning have shown great promise in automating threat detection and response, black-box models—such as deep neural networks—pose significant challenges for deployment in critical infrastructure like Power CPS. These models often lack interpretability, making it difficult for human operators to trust or understand the rationale behind AI-driven alerts or recommendations. In high-stakes operational environments, such lack of transparency can lead to operator hesitation, over-reliance on automation, or even the rejection of valid defense actions, ultimately undermining the effectiveness of AI-assisted cyber-physical defense systems [191].

4.3.2. Role of Explainable AI in Enhancing Operator Trust

XAI addresses this challenge by providing transparent, human-understandable explanations for AI-generated outputs. By offering insights into which features influenced a detection result, how anomalies are characterized, or why certain mitigation actions are recommended, XAI empowers operators to validate AI decisions and maintain human oversight. This transparency not only increases operator trust in automated systems but also supports collaborative human-machine decision-making, ensuring that AI augments rather than replaces expert judgment [192].

4.3.3. Human-AI Interaction in Defense Operations

Effective integration of XAI into cyber-physical defense workflows requires aligning explanation granularity with operator cognitive load and situational urgency. Visual analytics dashboards, ranked feature importance lists, and counterfactual reasoning tools are among the techniques that can be used to present explanations in actionable formats. Furthermore, XAI should be tightly coupled with real-time situational awareness systems, allowing operators to interactively explore AI recommendations and make informed, context-aware decisions. By bridging the gap between AI autonomy and human accountability, XAI plays a critical role in achieving operator-trustworthy and mission-centric cyber-physical defense [193].

4.4. Attack Attribution and Accountability in Distributed Defense

4.4.1. Importance of Attack Attribution for Coordinated Response

In distributed Power CPS environments, accurate and timely attack attribution is essential for coordinating defense actions across organizational and jurisdictional boundaries. Without reliable attribution, defense teams risk responding to false positives, misidentifying the source of an attack, or failing to coordinate properly across affected entities. Effective attribution not only improves the precision of mitigation actions but also supports post-incident forensics, legal accountability, and cross-sector information sharing. In multi-stakeholder environments involving utilities, market operators, and DER aggregators, establishing a shared understanding of the threat landscape through trusted attribution mechanisms is a cornerstone of mission-centric defense [194].

4.4.2. Methods for Attribution in Power CPS Environments

Attribution in Power CPS can leverage a combination of technical, behavioral, and contextual analysis. Technical methods include network forensics, log correlation, and traffic fingerprinting to trace attack vectors and identify responsible entities. Behavioral analysis leverages machine learning models to recognize attacker tactics, techniques, and procedures (TTPs) based on historical patterns [195]. Contextual analysis incorporates environmental factors, such as known vulnerabilities or recent threat intelligence reports, to strengthen attribution confidence. Together, these methods enable multi-source, evidence-based attribution that supports both real-time response and strategic post-event analysis.

4.4.3. Accountability and Legal Considerations in Multi-Stakeholder Defense

Attribution is only effective if it leads to accountable actions. In distributed power systems, legal and regulatory frameworks must define responsibilities, liabilities, and escalation procedures for responding to cyber-physical incidents. This includes establishing evidence standards for cross-organizational attribution, data sharing agreements, and collaborative incident response protocols. Transparent accountability mechanisms ensure that all stakeholders—whether utilities, third-party service providers, or regulatory authorities—are held responsible for their security roles while empowering coordinated and legally compliant defense actions. Building this accountability framework is critical for sustaining trust and collaboration in large-scale, distributed defense ecosystems.

5. Human-in-the-Loop and Operator-Centered Defense Strategies

While automation and AI are essential for improving cyber-physical defense scalability and speed, human operators remain irreplaceable in mission-critical decisions. Human judgment provides the contextual reasoning, operational experience, and adaptive flexibility that fully automated systems often lack. However, humans are also prone to cognitive overload, alert fatigue, and misinterpretation when overwhelmed by poor system design or excessive information. This section presents how Human-in-the-Loop (HITL) strategies bridge these gaps by integrating human expertise with machine intelligence to achieve coordinated, explainable, and trustworthy cyber-physical defense [196].

5.1. Human-Machine Teaming in Cyber-Physical Defense Operations

While fully automated defense systems excel at rapid data processing and rule-based threat detection, they frequently struggle with ambiguity, unforeseen scenarios, and contextual understanding. Such systems may incorrectly classify benign behaviors as attacks, for example, flagging a False Data Injection Attack (FDIA) where none exists. This could trigger unnecessary actions such as grid reconfiguration, inadvertently reducing system stability if human validation is bypassed [197].

To address these limitations, effective human-machine teaming must be designed around four core principles. Complementarity ensures that machines handle large-scale data analytics while humans provide contextual interpretation. Transparency allows AI systems to explain their reasoning to build operator trust. Controllability ensures that human operators retain override authority, preventing over-reliance on automation. Finally, collaboration fosters joint human-machine decision-making, moving beyond passive alerting toward active engagement. These principles enable synergistic defense operations, maximizing the strengths of both human and machine actors.

5.2. Situational Awareness and Cognitive Load Management

Situational awareness is the operator's ability to perceive, comprehend, and anticipate the system's state under both normal and attack conditions. It is frequently compromised by information overload, alert fatigue, and fragmented system views. Unfiltered data streams and repetitive false alarms can desensitize operators, reducing their ability to detect genuine threats. Similarly, fragmented dashboards that fail to integrate cyber, physical, and market data can obscure the full operational context [198].

To mitigate these challenges, systems must incorporate cognitive load management techniques. This includes providing prioritized alerts ranked by mission impact, contextual dashboards that unify multi-domain data, and progressive disclosure that allows operators to drill down into details only when necessary. Adaptive interfaces can further optimize information presentation based on operator workload and task criticality. Together, these features help maintain clear situational understanding without overwhelming the operator, ensuring effective real-time decision-making.

5.3. Operator Training, Decision Support Tools, and Incident Response Readiness

Operator competence is built through continuous training and the availability of decision support tools. Cyber-physical training simulators and tabletop exercises provide realistic environments for operators to practice responding to complex, coordinated attacks. Adversarial thinking workshops help operators develop an attacker's mindset, improving their ability to recognize sophisticated threat patterns.

Advanced decision support tools such as what-if analysis engines, playbook recommendation systems, and collaborative platforms enable teams to evaluate and coordinate response strategies across geographic and organizational boundaries. Establishing incident response readiness requires clearly defined roles and responsibilities, pre-approved mitigation playbooks to accelerate action, and post-incident learning loops to capture lessons and continuously improve defense capabilities [199].

5.4. Integrating Human Factors into Security Engineering and Policy

Finally, embedding human factors engineering into defense tool design and organizational policy is essential. Explainable interfaces should present AI outputs in clear, operator-friendly formats, while feedback channels allow operators to report misleading system behavior, informing future model refinements. User-centered design methodologies involving operator input throughout the development lifecycle ensure that tools are not only functional but also usable and trusted in high-pressure environments.

From a policy perspective, fostering a cybersecurity-aware organizational culture, investing in workforce development that integrates cybersecurity and power engineering, and ensuring regulatory alignment with standards like NERC CIP and NIS2 are critical. These measures ensure that human factors are not treated as afterthoughts but as core components of cyber-physical security strategy.

In summary, Human-in-the-Loop defense strategies are not optional add-ons but foundational pillars of resilient and mission-centric Power CPS security. By empowering operators with situational awareness, explainable AI, decision support tools, and comprehensive training, power system organizations can fully leverage human expertise to confront and adapt to evolving cyber-physical threats.

6. Post-Attack Recovery and Mission Assurance

No defense mechanism can guarantee absolute protection against sophisticated cyber-physical attacks. Therefore, post-attack recovery and mission assurance have emerged as essential pillars of resilience-oriented security strategies for Power CPS. These capabilities enable grid operators to restore compromised functions, maintain critical services, and learn from incidents to strengthen future defense. This section explores methods for data reconstruction, adaptive control reconfiguration, integration of resilience metrics, and lessons learned from both real-world and simulated incidents.

6.1. Data Reconstruction, System Restoration, and Operational Continuity

A major challenge following a cyber-physical attack is the loss or corruption of critical system data. While intrusion detection systems may successfully flag compromised data, they rarely offer clear methods to restore trustworthy system states. Simply discarding all suspicious data risks blinding operators, compromising situational awareness and potentially leading to unsafe control actions.

To address this, several data reconstruction strategies are emerging. Model-based reconstruction leverages physical system models, such as power flow equations and robust optimization techniques, to estimate missing or corrupted values. Data-driven methods use historical and real-time data to train AI models capable of imputing missing measurements or correcting anomalies, including the use of physics-informed neural networks (PINNs) that combine data learning with physical constraints. Additionally, multi-source data fusion techniques cross-validate information from diverse sensors like PMUs, RTUs, and smart meters, improving data reliability. Finally, operator-guided validation ensures that reconstructed states are reviewed by human experts, especially in high-risk or ambiguous scenarios. These methods collectively support continuity of grid observability, enabling informed decision-making even when data integrity is partially compromised [200].

6.2. Adaptive Reconfiguration and Mission-Aware Control Strategies

Once a reliable system state is reconstructed, the next step is reconfiguring control strategies to contain the impact of the attack and maintain critical services. Adaptive reconfiguration involves isolating compromised components, redirecting power flows, and activating local control modes in microgrids or VPPs. Specific examples include enabling islanded microgrid operation to protect local loads by disconnecting affected regions from the bulk grid, prioritizing load shedding based on service criticality (e.g., keeping hospitals and data centers online), and re-optimizing market dispatch to account for degraded system visibility or compromised assets.

While automation can perform these reconfigurations rapidly, human oversight remains essential. Operators can use what-if simulators to preview potential outcomes, assess confidence scores to gauge reliability, and rely on explainable AI recommendations to support their decisions. This combination of automated execution and human validation ensures the system can deliver acceptable levels of service under degraded conditions while avoiding unintended consequences [201].

6.3. Integration of Resilience Metrics in Grid Operations and Market Mechanisms

Traditional cybersecurity metrics—such as the number of blocked attacks or alerts generated—provide little insight into the actual resilience of power systems. To close this gap, operators are increasingly adopting mission-oriented resilience metrics. These include service continuity (percentage of load served during and after an attack), time to recovery (duration required to restore functionality), quality of service (voltage and frequency stability), and economic impact (costs of service disruption and corrective actions).

Embedding these metrics into market operations can further align economic incentives with resilience objectives. For example, flexible resources such as DERs, energy storage, and demand response can be rewarded for providing services that enhance grid resilience during emergencies. Additionally, new resilience-based market products can be introduced, valuing capabilities like black start services, grid-forming inverters, and operational flexibility. This integration ensures that both technical and economic layers of the power system contribute to overall mission assurance [202].

6.4. Lessons from Real-World Incidents and Simulated Benchmarks

Real-world cyber-physical incidents provide valuable lessons that go beyond technical vulnerabilities. The 2015 Ukraine blackout highlighted the importance of operator training and multi-layered defense coordination. Stuxnet demonstrated the need for supply chain security and stealthy threat detection, while the Colonial Pipeline ransomware incident emphasized the risks of cross-sector interdependencies and the importance of coordinated response planning. These events underline that technical solutions alone are insufficient without organizational readiness and cross-sector collaboration.

Complementing these real-world insights, simulated testbeds and red team/blue team exercises provide controlled environments to evaluate detection, response, and recovery strategies. These activities stress-test defense mechanisms, identify operational gaps, and benchmark resilience metrics against standardized scenarios. By continuously engaging in empirical testing and validation, organizations can operationalize resilience and build adaptive defense postures based on real-world and simulated evidence [203].

In summary, post-attack recovery and mission assurance require a holistic approach that integrates data reconstruction, adaptive control, resilience metrics, and organizational learning. These capabilities ensure that Power CPS can sustain essential services, recover effectively, and continuously improve defense strategies in response to evolving threats.

7. Future Research and Cross-Sector Collaboration Directions

While this review has outlined a comprehensive vision for defending Power CPS, turning that vision into operational reality demands sustained research, standardization, and multi-stakeholder collaboration. This section highlights key open research questions, technology gaps, and collaborative pathways necessary to transition from conceptual frameworks to validated, deployable defense solutions.

7.1. Toward Cyber-Physical-Human Co-Resilience Modeling and Validation

Current research in Power CPS security remains fragmented, often addressing cyber and physical layers in isolation. Even when these layers are modeled together, they tend to overlook human behavior, organizational response dynamics, and interdependencies with other critical infrastructures like telecommunications and energy markets.

Future research must advance multi-layered resilience modeling frameworks that explicitly capture interactions across cyber, physical, market, and human layers. This includes integrating behavioral and cognitive models that represent operator decision-making processes, cognitive limitations, and team dynamics during attacks. Additionally, cross-infrastructure modeling should account for cascading failures spanning energy, communications, and market systems under coordinated cyber-physical assaults. Finally, the development and validation of mission-centric resilience metrics—such as service continuity, time to recovery, and economic impact—are essential to quantify a system's ability to sustain critical operations under adverse conditions [204].

7.2. Bridging Policy, Regulation, and Operational Practices

Despite technological advancements, a persistent gap exists between research outputs and policy adoption. Regulatory frameworks often lag behind emerging technologies, leading to misalignment between compliance requirements and operational best practices. Additionally, operational procedures may fail to incorporate AI-driven or distributed defense mechanisms due to the lack of certification, regulatory recognition, or industry standards.

Bridging this gap requires regulatory co-design, involving researchers, operators, and regulators in the joint development of cybersecurity guidelines that balance technological feasibility with enforceable policies. Contributions to standards development bodies such as IEEE, IEC, and NERC CIP are also crucial to operationalize mission-centric defense principles. To translate policies into practice, organizations need toolkits and training programs that align regulatory requirements with operational workflows. Strengthening cross-sector information sharing mechanisms further ensures that cyber threat intelligence and lessons learned are shared across the energy sector and other critical infrastructures, enhancing collective resilience.

7.3. Building Open Testbeds and Benchmarks for Realistic Evaluation

Many defense solutions are evaluated in overly simplified environments, limiting their relevance to real-world Power CPS operations. The absence of benchmark datasets—due to security restrictions, proprietary limitations, or lack of standardization—further impedes objective comparison of defense mechanisms.

Addressing these limitations calls for the development of open cyber-physical testbeds that replicate realistic operational conditions, including human-in-the-loop simulations. Establishing standardized evaluation scenarios and benchmarks enables consistent comparison across different defense strategies. Additionally, privacy-preserving data sharing techniques, such as federated learning and synthetic data generation, are needed to securely share operational data without exposing sensitive information. Community-driven activities like capture-the-flag (CTF) competitions and red team/blue team exercises can further crowdsource innovative defense solutions, stress-test them under realistic threats, and drive continuous improvement through empirical validation [205].

7.4. Roadmap for Cross-Sector and International Collaboration

Power CPS are interdependent with sectors such as telecommunications, transportation, water systems, and financial markets. Effective defense requires cross-sector collaboration to address shared vulnerabilities and respond to coordinated multi-domain threats.

On an international scale, building global threat intelligence networks is critical to facilitate the sharing of attack signatures, tactics, techniques, and threat actor profiles. Launching multi-country research consortia can accelerate the development of cross-infrastructure resilience models and AI-based defense solutions. Harmonizing cybersecurity standards across regulatory jurisdictions will further ensure consistent protection levels globally. Finally, capacity building efforts—including training programs, technical exchanges, and policy dialogues—will help disseminate best practices and strengthen cyber defense capabilities worldwide.By building a globally coordinated ecosystem of researchers, operators, regulators, and policy makers, the energy sector can better address the complex, multi-domain challenges of securing Power CPS against evolving cyber-physical threats.

In summary, advancing the security and resilience of Power CPS requires cross-disciplinary research, regulatory alignment, realistic evaluation platforms, and international collaboration. By building a globally coordinated ecosystem of researchers, operators, regulators, and policymakers, the energy sector can transform mission-centric defense from a conceptual aspiration into an operational reality, safeguarding critical infrastructures against future cyber-physical threats.

8. Conclusions

The digitalization of power systems via Power CPS has enhanced grid operations but also exposed new vulnerabilities to sophisticated, multi-stage cyber-physical attacks, rendering traditional, isolated defense strategies inadequate for ensuring reliable and secure power delivery. This review advocates for a paradigm shift toward mission-centric, coordinated, and human-in-the-loop cyber-physical defense, covering the full security lifecycle from threat anticipation and detection to response, recovery, and mission assurance. The key insights and contributions are summarized as follows:

1) This review expands the understanding of power system security by moving beyond isolated False Data Injection Attacks (FDIAs) to address AI-enhanced, multi-agent, and cross-layer attack campaigns. These evolving threats exploit not only cyber and physical infrastructures, but also market dynamics and human factors, requiring holistic and multi-domain defense strategies.

2) It proposes cross-layer architectural principles that integrate redundancy, diversity, modularity, and trustworthy sensing and communication to enhance system resilience. Building on this foundation, the review synthesizes multi-agent coordination frameworks, edge-cloud collaborative defense models, and explainable AI techniques to enable real-time, distributed defense operations that balance automated intelligence with operator trust and oversight.

3) Recognizing the indispensable role of human operators, this review highlights the importance of situational awareness tools, cognitive load management, and interactive decision support systems. It further emphasizes post-attack recovery strategies, including data reconstruction, adaptive control reconfiguration, and the integration of resilience metrics into grid and market operations to ensure service continuity under degraded conditions.

4) Finally, the review identifies the need for cross-disciplinary research, regulatory and policy co-design, open testbeds, and international collaboration to bridge the gap between conceptual frameworks and operational deployment, paving the way for a scalable, trustworthy, and mission-aware cyber-physical defense ecosystem.

As cyber-physical threats escalate in scale and complexity, advancing power system security demands cross-sector collaboration among industry, academia, and government. This requires breaking down disciplinary silos, embedding resilience as a core design principle, strengthening workforce capabilities, and fostering national and international partnerships for knowledge and threat intelligence sharing. By embracing a mission-centric, coordinated, and human-aware defense paradigm, the energy sector can move beyond detection-centric limitations and secure the resilient, reliable, and digitalized energy systems of the future.

References

1. Bakirtzis G, Carter B T, Fleming C H, et al. MISSION AWARE: Evidence-based, mission-centric cybersecurity analysis[J]. arXiv preprint arXiv:1712.01448, 2017.
2. Beling P A, Clifford M M, Sherburne T, et al. The “Mission Aware” Concept for Design of Cyber-Resilience[J]. Systems engineering for the digital age: Practitioner perspectives, 2023: 507-521.
3. Qu Z, Zhao T, Zhang Y, et al. Determination Method of Network Risk Propagation Threshold in Power CPS Based on Percolation Theory[J]. Automation of Electric Power Systems, 2020, 44(4): 16-23.
4. Haque M A, Shetty S, Kamhoua C A, et al. Integrating mission-centric impact assessment to operational resiliency in cyber-physical systems[C]//GLOBECOM 2020-2020 IEEE Global Communications Conference. IEEE, 2020: 1-7.
5. Wang L, Qu Z, Li Y, et al. Method for Extracting Patterns of Coordinated Network Attacks on Electric Power CPS Based on Temporal-Topological Correlation[J]. IEEE Access, 2020, 8: 57260-57272.
6. Qin B, Liu D. Research Progress and Prospects on Analysis and Control of Power Grid Cyber-Physical Systems[J]. Proceedings of the CSEE, 2020, 40(18): 5816-5826.

7. Barrère M, Hankin C, O'Reilly D. Cyber-physical attack graphs (CPAGs): Composable and scalable attack graphs for cyber-physical systems[J]. Computers & security, 2023, 132: 103348.
8. Pecharich J L, Viswanathan A, Stathatos S, et al. Mission-centric cyber security assessment of critical systems[M]//AIAA SPACE 2016. 2016: 5603.
9. Barrère M, Hankin C, O'Reilly D. Cyber-physical attack graphs (CPAGs): Composable and scalable attack graphs for cyber-physical systems[J]. Computers & security, 2023, 132: 103348.
10. Sherburne T, Clifford M M, Horowitz B M, et al. The Cyber Security Requirements Methodology and Meta-Model for Design of Cyber-Resilience[J]. Systems engineering for the digital age: Practitioner perspectives, 2023: 539-554.
11. Cao J, Wang Q, Qu Z, et al. Method for identifying false data injection attacks in power grid based on improved CNN-LSTM[J]. Electrical Engineering, 2025: 1-26.
12. Hoenig A, Roy K, Acquaah Y T, et al. Explainable AI for cyber-physical systems: Issues and challenges[J]. IEEE access, 2024, 12: 73113-73140.
13. Zhao J, An K, Wang X. Research on Fast Early Warning of False Data Injection Attack in CPS of Electric Power Communication Network[J]. Journal of Cyber Security and Mobility, 2024: 1331–1356-1331–1356.
14. Jiang Y, Wu S, Ma R, et al. Monitoring and defense of industrial cyber-physical systems under typical attacks: From a systems and control perspective[J]. IEEE Transactions on Industrial Cyber-Physical Systems, 2023, 1: 192-207.
15. Li Y, Cao J, Xu Y, et al. Deep learning based on Transformer architecture for power system short-term voltage stability assessment with class imbalance[J]. Renewable and Sustainable Energy Reviews, 2024, 189: 113913.
16. Qu Z, Dong Y, Qu N, et al. Quantitative Assessment of Survivability of Power CPS Considering Load Optimization and Reconfiguration[J]. Automation of Electric Power Systems, 2019, 43(6): 15-24.
17. Bo X, Chen X, Li H, et al. Modeling Method for the Coupling Relations of Microgrid Cyber-Physical Systems Driven by Hybrid Spatiotemporal Events[J]. IEEE Access, 2021, 9: 19619-19631.
18. Batewela S, Liyanage M, Zeydan E, et al. Security Orchestration in 5G and Beyond Smart Network Technologies[J]. IEEE Open Journal of the Computer Society, 2025.
19. Wang L, Xu P, Qu Z, et al. Coordinated Cyber-Attack Detection Model of Cyber-Physical Power System Based on the Operating State Data Link[J]. Frontiers in Energy Research, 2021, 9: 666130.
20. Miao B, Wang H, Liu Y J, et al. Adaptive security control against false data injection attacks in cyber-physical systems[J]. IEEE Journal on Emerging and Selected Topics in Circuits and Systems, 2023, 13(3): 743-751.
21. Qu Z, Xie Q, Liu Y, et al. Power Cyber-Physical System Risk Area Prediction Using Dependent Markov Chain and Improved Grey Wolf Optimization[J]. IEEE Access, 2020, 8: 82844-82854.
22. Wang T, Sun C, Gu X, et al. Modeling of Power Communication Coupled Networks and Their Vulnerability Analysis[J]. Proceedings of the CSEE, 2018, 38(12): 3556-3567.
23. Yang T, Liu Y, Li W. Attack and defence methods in cyber-physical power system[J]. IET Energy Systems Integration, 2022, 4(2): 159-170.
24. Yao P, Yan B, Yang Q. Game Theoretical Decision-Making of Dynamic Defense in Cyber-Physical Power Systems under Cyber-Attacks[J]. ACM Transactions on Cyber-Physical Systems, 2025, 9(2): 1-21.
25. Bo X, Qu Z, Liu Y, et al. Review of active defense methods against power cps false data injection attacks from the multiple spatiotemporal perspective[J]. Energy Reports, 2022, 8: 11235-11248.

26. Chen J, Zhu Q. A cross-layer design approach to strategic cyber defense and robust switching control of cyber-physical wind energy systems[J]. IEEE Transactions on Automation Science and Engineering, 2022, 20(1): 624-635.
27. Xin S, Guo Q, Sun H, et al. Cyber-Physical Modeling and Cyber-Contingency Assessment of Hierarchical Control Systems[J]. IEEE Transactions on Smart Grid, 2015, 6(5): 2375-2385.
28. Wang W, Di Maio F, Zio E. Adversarial risk analysis to allocate optimal defense resources for protecting cyber–physical systems from cyber attacks[J]. Risk Analysis, 2019, 39(12): 2766-2785.
29. Liu X, Wu Z. Research on Online Defense against Stealthy Data Injection Attacks in Smart Grids[J]. Proceedings of the CSEE, 2020, 40(8): 2546-2558.
30. Mitchell R, Chen R. Modeling and analysis of attacks and counter defense mechanisms for cyber physical systems[J]. IEEE Transactions on Reliability, 2015, 65(1): 350-358.
31. Yu W, Xue Y, Luo J, et al. An UHV Grid Security and Stability Defense System: Considering the Risk of Power System Communication[J]. IEEE Transactions on Smart Grid, 2016, 7(1): 491-500.
32. Liu Y, Ning P, Reiter M. False Data Injection Attacks against State Estimation in Electric Power Grids[J]. ACM Transactions on Information and System Security (TISSEC), 2011, 14(1): 1-16.
33. Qu Z, Zhang Y, Qu N, et al. Method for Quantitative Estimation of the Risk Propagation Threshold in Electric Power CPS Based on Seepage Probability[J]. IEEE Access, 2018, 6: 68813-68823.
34. Shukla S K. Cyber security of cyber physical systems: Cyber threats and defense of critical infrastructures[C]//2016 29th International Conference on VLSI Design and 2016 15th International Conference on Embedded Systems (VLSID). IEEE, 2016: 30-31.
35. Xu S, Xia Y, Shen H L. Cyber protection for malware attack resistance in cyber-physical power systems[J]. IEEE Systems Journal, 2022, 16(4): 5337-5345.
36. Li Y, Li Z, Chen L. Dynamic State Estimation of Generators Under Cyber Attacks[J]. IEEE Access, 2019, 7: 125252-125267.
37. Ni M, Li M, Li J, et al. Concept and research framework for coordinated situation awareness and active defense of cyber-physical power systems against cyber-attacks[J]. Journal of Modern Power Systems and Clean Energy, 2020, 9(3): 477-484.
38. Qu Z, Dong Y, Li Y, et al. Localization of Dummy Data Injection Attacks in Power Systems Considering Incomplete Topological Information: A Spatio-Temporal Graph Wavelet Convolutional Neural Network Approach[J]. Applied Energy, 2024, 360: 122736.
39. Li Y, Wei X, Li Y, et al. Detection of False Data Injection Attacks in Smart Grid: A Secure Federated Deep Learning Approach[J]. IEEE Transactions on Smart Grid, 2022, 13(6): 4862-4872.
40. Wang L, Qu Z, Li Y, et al. Method for Extracting Patterns of Coordinated Network Attacks on Electric Power CPS Based on Temporal–Topological Correlation[J]. IEEE Access, 2020, 8: 57260-57272.
41. Qu Z, Dong Y, Qu N, et al. Survivability Evaluation Method for Cascading Failure of Electric Cyber Physical System Considering Load Optimal Allocation[J]. Mathematical Problems in Engineering, 2019, 2019: 2817586.
42. Qu Z, Qu N, Zhou Y, et al. Extraction of Typical Operating Scenarios of New Power System Based on Deep Time Series Aggregation[J]. CAAI Transactions on Intelligence Technology, 2024, 1-17. DOI: 10.1049/cit2.12369.
43. Niu H, Jagannathan S. Optimal defense and control of dynamic systems modeled as cyber-physical systems[J]. The Journal of Defense Modeling and Simulation, 2015, 12(4): 423-438.
44. Chen L, Gu S, Wang Y, et al. Stacked Autoencoder Framework of False Data Injection Attack Detection in Smart Grid[J]. Mathematical Problems in Engineering, 2021, 2021(1): 2014345.

45. Li Y, Li Z, Chen L, et al. A false data injection attack method for generator dynamic state estimation[J]. Transactions of China Electrotechnical Society, 2019, 34: 3651-3660.
46. Wang Q, Tai W, Tang Y, et al. A Review of False Data Injection Attack Research for Power Cyber-Physical Systems[J]. Acta Automatica Sinica, 2019, 45(1): 72-83.
47. Wang J, Li Y, Xu T. Modeling of False Data Injection Attacks and Rapid Screening of Vulnerable Lines under Attacks[J]. Electric Power Construction, 2022, 43(1): 104-112.
48. Karamdel S, Liang X, Faried S O, et al. Optimization models in cyber-physical power systems: A review[J]. IEEE Access, 2022, 10: 130469-130486.
49. Zang T, Tong X, Li C, et al. Research and Prospect of Defense for Integrated Energy Cyber–Physical Systems Against Deliberate Attacks[J]. Energies, 2025, 18(6): 1479.
50. Li Y, Li J, Chen L. Dynamic state estimation of synchronous machines based on robust cubature Kalman filter under complex measurement noise conditions[J]. transactions of china electrotechnical society, 2019, 34(17): 3651-60.
51. Shen Y, Zhang W, Ni H, et al. Guaranteed Cost Control of Networked Control Systems with DoS Attack and Time-varying Delay[J]. International Journal of Control, Automation and Systems, 2019, 17(4): 811-821.
52. Liang Y, Wang Y, Liu K, et al. Fault Simulation of Distribution Grid CPS Considering Network Information Security[J]. Power System Technology, 2020, 45(1): 235-242.
53. Lian Z, Shi P, Chen M. A Survey on Cyber-Attacks for Cyber-Physical Systems: Modeling, Defense and Design[J]. IEEE Internet of Things Journal, 2024.
54. Yang T, Cai S, Yan P, et al. Saturation defense method of a power cyber-physical system based on active cut set[J]. IEEE Transactions on Smart Grid, 2022.
55. Wang Z, Chen Y, Zeng J, et al. Modeling and Reliability Assessment of Microgrid Cyber-Physical Systems for Fully Distributed Control[J]. Power System Technology, 2019, 43(7): 2413-2421.
56. Zhang Z, Huang S, Chen Y, et al. Cyber-physical coordinated risk mitigation in smart grids based on attack-defense game[J]. IEEE Transactions on Power Systems, 2021, 37(1): 530-542.
57. Shi J, Chen B, Yu L. Hidden FDIA Detection Based on Laplacian Eigenmap Learning[J]. Acta Automatica Sinica, 2021, 47(10): 2494-2500.
58. Jin Z, Liu Y, Diao J, et al. Covert False Data Injection Attacks on Remote State Estimation in Cyber-Physical Systems[J]. Acta Automatica Sinica, 2025, 51(2): 1-10.
59. Shu H, Yang Y, Zhao H, et al. Detection of False Data Injection Attacks in Power Grids Based on Adaptive Weighted Hybrid Prediction[J]. Power System Technology, 2024, 49(3): 1246-1256.
60. Liu X, Bao Z, Lu D, et al. Modeling of Local False Data Injection Attacks With Reduced Network Information[J]. IEEE Transactions on Smart Grid, 2015, 6(4): 1686-1696.
61. Liu S, Tan Y, Zhao F, et al. Coupled Modeling Method for Power Information Systems[J]. Journal of Power Systems and Automation, 2021, 33(3): 89-93.
62. Ribas Monteiro L F, Rodrigues Y R, Zambroni de Souza A C. Cybersecurity in cyber–physical power systems[J]. Energies, 2023, 16(12): 4556.
63. Long X, Ding Y, et al. Privacy-Preserving Graph Inference Network for Multi-Entity Wind Power Forecast: A Federated Learning Approach[J]. IEEE Transactions on Network Science and Engineering, 2025. DOI: 10.1109/TNSE.2025.3547227.
64. Li Y, He S, Li Y, et al. Federated multiagent deep reinforcement learning approach via physics-informed reward for multimicrogrid energy management[J]. IEEE Transactions on Neural Networks and Learning Systems, 2024, 35(5): 5902 - 5914.

65. Li Y, Wang R, Li Y, et al. Wind power forecasting considering data privacy protection: A federated deep reinforcement learning approach[J]. Applied Energy, 2023, 329: 120291..
66. Liu S, Martínez S, Cortés J. Stabilization of linear cyber-physical systems against attacks via switching defense[J]. IEEE Transactions on Automatic Control, 2023, 68(12): 7326-7341.
67. Qu Z, Bo X, Yu T, et al. Active and Passive Hybrid Detection Method for Power CPS False Data Injection Attacks with Improved AKF and GRU-CNN[J]. IET Renewable Power Generation, 2022, 16: 1490-1508. DOI: 10.1049/rpg2.12432.
68. Shafae M S, Wells L J, Purdy G T. Defending against product-oriented cyber-physical attacks on machining systems[J]. The International Journal of Advanced Manufacturing Technology, 2019, 105: 3829-3850.
69. Cai X, Wang Q, Huang J, et al. Dual-Layer Cyber-Physical Collaborative Emergency Control Method for Power System Network Attacks[J]. Global Energy Interconnection, 2020, 3(6): 560-568.
70. Wang Y, Lin Z, Liang X, et al. On modeling of electrical cyber-physical systems considering cyber security[J]. Frontiers of Information Technology & Electronic Engineering, 2016, 17(5): 465-478.
71. Banik S, Ramachandran T, Bhattacharya A, et al. Automated adversary-in-the-loop cyber-physical defense planning[J]. ACM Transactions on Cyber-Physical Systems, 2023, 7(3): 1-25.
72. Jain H, Kumar M, Joshi A M. Intelligent energy cyber physical systems (iECPS) for reliable smart grid against energy theft and false data injection[J]. Electrical Engineering, 2022, 104(1): 331-346.
73. Zhu W, Tang Y, Wei X, et al. Defense Methods Against Adversarial Attacks on Data-Driven Algorithms in Power CPS[J]. Electric Power, 2024, 57(9):32-40.
74. Sridhar S, Hahn A, Govindarasu M. Cyber-Physical System Security for the Electric Power Grid[J]. Proceedings of the IEEE, 2012, 100(1): 210-224.
75. Wang J, Li Y, Xu T. False Data Detection in Smart Grids Based on Extended Kalman Filtering[J]. Smart Power, 2022, 50(3): 50-56.
76. Xiong X, Hu S, Sun D, et al. Detection of false data injection attack in power information physical system based on SVM-GAB algorithm[J]. Energy Reports, 2022, 8(5): 1156-1164.
77. Huang H, Wlazlo P, Mao Z, et al. Cyberattack defense with cyber-physical alert and control logic in industrial controllers[J]. IEEE Transactions on Industry Applications, 2022, 58(5): 5921-5934.
78. Qu Z, Shi H, Wang Y, et al. Active and Passive Defense Strategies of Cyber-Physical Power System against Cyber Attacks Considering Node Vulnerability[J]. Processes, 2022, 10(7): 1351.
79. Wang Z, Chen Y, Liu F, et al. Power System Security Under False Data Injection Attacks With Exploitation and Exploration Based on Reinforcement Learning[J]. IEEE Access, 2018, 6: 48785-48796.
80. Chen Y, Huang S, Liu F, et al. Evaluation of Reinforcement Learning-Based False Data Injection Attack to Automatic Voltage Control[J]. IEEE Transactions on Smart Grid, 2019, 10(2): 2158-2169.
81. Liu Y, Wang Y. Evolution Mechanism and Active Defense Exploration of Cross-Domain Cascading Failures in New Power Systems[J]. Electric Power, 2022, 55(2): 62-72+81.
82. Xia Y, Wang Y, Zhou L, et al. Detection Method for False Data Injection Attacks Based on Improved Generative Adversarial Networks[J]. Electric Power Construction, 2022, 43(3): 58-65.
83. Sun J, et al. Indicator & crowding distance-based evolutionary algorithm for combined heat and power economic emission dispatch[J]. Applied Soft Computing, 2020, 90: 106158.
84. Yang F, Wang J, Pan Q, et al. Resilient Event-Triggered Control for Cyber-Physical Integrated Power Systems Under Network Attacks[J]. Acta Automatica Sinica, 2019, 45(1): 110-119.

85. Chen L, Li Y, Huang M, et al. Robust Dynamic State Estimator of Integrated Energy Systems Based on Natural Gas Partial Differential Equations[J]. IEEE Transactions on Industry Applications, 2022, 58(3): 3303-3312.
86. Susuki Y, Koo T, Ebina H, et al. A Hybrid System Approach to the Analysis and Design of Power Grid Dynamic Performance[J]. Proceedings of the IEEE, 2012, 100(1): 225-239.
87. Zhang Z, Tian Y, Deng R, et al. A double-benefit moving target defense against cyber–physical attacks in smart grid[J]. IEEE Internet of Things Journal, 2022, 9(18): 17912-17925.
88. Liu X, Li Z, Shuai Z, et al. Cyber Attacks Against the Economic Operation of Power Systems: A Fast Solution[J]. IEEE Transactions on Smart Grid, 2017, 8(2): 1023-1025.
89. Wei L, Zhang Q. Detection of False Data Attacks in Smart Grids Based on Improved UKF[J]. Journal of System Simulation, 2023, 35(7): 1508.
90. Fu J, Hu B, Xie K, et al. Power System Generation-Transmission Expansion Stochastic Programming for Coordinated Attacks[J]. Automation of Electric Power Systems, 2021, 45(2): 21-29.
91. Sanjab A, Saad W. Data Injection Attacks on Smart Grids With Multiple Adversaries: A Game-Theoretic Perspective[J]. IEEE Transactions on Smart Grid, 2016, 7(4): 2038-2049.
92. Zhou Z, Zhang J, Zhang X. A review on defense mechanism against the denial of service and false data injection in cyber-physical power systems[C]//2023 IEEE 6th International Electrical and Energy Conference (CIEEC). IEEE, 2023: 4539-4545.
93. Chen K, Wen F, Tseng C L, et al. A game theory-based approach for vulnerability analysis of a cyber-physical power system[J]. Energies, 2019, 12(15): 3002.
94. Li Y, Yang Z. Application of EOS-ELM with Binary Jaya-Based Feature Selection to Real-Time Transient Stability Assessment Using PMU Data[J]. IEEE Access, 2017, 5: 23092-23101.
95. Zhu B, Guo Y, Guo C, et al. A Review of Security Assessment and Defense for Power Cyber-Physical Systems Under Information Failure Threats[J]. Power System Protection and Control, 2021, 49(1): 178-187.
96. Kong X, Lu Z, Guo X, et al. Resilience evaluation of cyber-physical power system considering cyber attacks[J]. IEEE Transactions on Reliability, 2023, 73(1): 245-256.
97. Tian J, Wang B, Li T, et al. TOTAL: Optimal protection strategy against perfect and imperfect false data injection attacks on power grid cyber–physical systems[J]. IEEE Internet of Things Journal, 2020, 8(2): 1001-1015.
98. Luo X, He J, Wang X, et al. Topology Optimization for Resilient Defense Strategies Against False Data Injection Attacks in Smart Grids[J]. Acta Automatica Sinica, 2023, 49(6): 1326-1338.
99. Deng R, Zhuang P, Liang H. CCPA: Coordinated Cyber-Physical Attacks and Countermeasures in Smart Grid[J]. IEEE Transactions on Smart Grid, 2017, 8(5): 2420-2430.
100. Jiang X, Zhang J, Harding B, et al. Spoofing GPS Receiver Clock Offset of Phasor Measurement Units[J]. IEEE Transactions on Power Systems, 2013, 28(3): 3253-3262.
101. Risbud P, Gatsis N, Taha A. Vulnerability Analysis of Smart Grids to GPS Spoofing[J]. IEEE Transactions on Smart Grid, 2019, 10(4): 3535-3548.
102. Alabadi M, Albayrak Z. Q-learning for securing cyber-physical systems: a survey[C]//2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA). IEEE, 2020: 1-13.
103. Huang D, Wang Y, Hu A, et al. False Data Injection Attack Detection Combining Unsupervised and Supervised Learning[J]. Electric Power Engineering Technology, 2024, 43(2): 134-141.
104. Yin H, Liu D, Chen G, et al. Collaborative Network Attack Model and Cross-Space Fault Propagation Mechanism for Virtual Power Plants[J]. Automation of Electric Power Systems, 2023, 47(8): 34-43.

105. Giraldo J A, El Hariri M, Parvania M. Moving target defense for cyber–physical systems using iot-enabled data replication[J]. IEEE Internet of Things Journal, 2022, 9(15): 13223-13232.
106. Chen L, Hui X, et al. Dynamic state estimation for integrated natural gas and electric power systems[C]//2021 IEEE/IAS Industrial and Commercial Power System Asia (I&CPS Asia). IEEE, 2021: 397-402.
107. Yang T, Xu Z, Zhao Y, et al. A Review of Attacks and Defense Methods for Digitalized New Power Systems[J]. Automation of Electric Power Systems, 2024, 48(6): 112-126.
108. Ali M, Sun W. Securing Critical Infrastructures: Restoration from Cyber-Physical Attacks in Active Distribution Grids[C]//2024 IEEE Power & Energy Society General Meeting (PESGM). IEEE, 2024: 1-5.
109. Fan Q, Liu D, Wang Y, et al. Key Technologies and Progress in the Morphological Evolution of Power Cyber-Physical Systems[J]. Proceedings of the CSEE, 2023, 44(21): 8341-8352.
110. He Z, Gao S, Wei X, et al. Research on Attack-Defense Game Model of False Topology Attacks with Branch and Protection Coordination[J]. Power System Technology, 2022, 46(11): 4346-4355.
111. Li X, Yi L, Liu C, et al. Data-Driven Detection of False Data Injection Attacks in Power Systems[J]. Smart Power, 2023, 51(2): 30-37.
112. Weng P, Chen B, Yu L. Fusion Estimation of False Data Injection Attack Signals[J]. Acta Automatica Sinica, 2021, 47(9): 2292-2300.
113. Patel C D, Aggarwal M, Chaubey N K. Enhancing Cyber-Physical Systems Security Through Advanced Defense Mechanisms[M]//Advancing Cyber Security Through Quantum Cryptography. IGI Global, 2025: 307-342.
114. Krishnaveni S, Chen T M, Sathiyanarayanan M, et al. CyberDefender: an integrated intelligent defense framework for digital-twin-based industrial cyber-physical systems[J]. Cluster Computing, 2024, 27(6): 7273-7306.
115. Li Y, Zhang S, Li Y, et al. PMU Measurements Based Short-Term Voltage Stability Assessment of Power Systems via Deep Transfer Learning[J]. IEEE Transactions on Instrumentation and Measurement, 2023, 72: 2526111.
116. Zhou X, Feng J, et al. Non-intrusive load decomposition based on CNN–LSTM hybrid deep learning model[J]. Energy Reports, 2021, 7: 5762-5771.
117. Yan B, Yao P, Wang J, et al. Game theoretical dynamic cybersecurity defense strategy for electrical cyber physical systems[C]//2021 IEEE 5th Conference on Energy Internet and Energy System Integration (EI2). IEEE, 2021: 2392-2397.
118. Li Y, Ma W, Li Y, et al. Enhancing Cyber-Resilience in Integrated Energy System Scheduling with Demand Response Using Deep Reinforcement Learning[J]. Applied Energy, 2025, 379:124831.
119. Fahmeeda S, Bhagyashree B K. Detection and prevention of false data injection attack in cyber physical power system[C]//2021 IEEE International Conference on Mobile Networks and Wireless Communications (ICMNWC). IEEE, 2021: 1-5.
120. Yang J. A controllable false data injection attack for a cyber physical system[J]. IEEE Access, 2021, 9: 6721-6728.
121. Xing W, Shen J. Security Control of Cyber–Physical Systems under Cyber Attacks: A Survey[J]. Sensors, 2024, 24(12): 3815.
122. Yang J. A controllable false data injection attack for a cyber physical system[J]. IEEE Access, 2021, 9: 6721-6728.
123. Chen H, Li T, Fan X, et al. Feature selection for imbalanced data based on neighborhood rough sets[J]. Information Sciences, 2019, 483: 1-20.

124. Wang S, Ko R K L, Bai G, et al. Evasion attack and defense on machine learning models in cyber-physical systems: A survey[J]. IEEE communications surveys & tutorials, 2023, 26(2): 930-966.

125. Hu Y, Zhu P, Xun P, et al. CPMTD: Cyber-physical moving target defense for hardening the security of power system against false data injected attack[J]. Computers & Security, 2021, 111: 102465.

126. Xiao K, Zhu C, Xie J, et al. Dynamic defense against stealth malware propagation in cyber-physical systems: a game-theoretical framework[J]. Entropy, 2020, 22(8): 894.

127. Zhao Z, Shang Y, Qi B, et al. Research on defense strategies for power system frequency stability under false data injection attacks[J]. Applied Energy, 2024, 371: 123711.

128. Xiong X, Hu S, Sun D, et al. Detection of false data injection attack in power information physical system based on SVM–GAB algorithm[J]. Energy Reports, 2022, 8: 1156-1164.

129. Zhu H, Xu L, Bao Z, et al. Secure control against multiplicative and additive false data injection attacks[J]. IEEE Transactions on Industrial Cyber-Physical Systems, 2023, 1: 92-100.

130. Zhong C, Li H, Zhou Y, et al. Virtual synchronous generator of PV generation without energy storage for frequency support in autonomous microgrid[J]. International Journal of Electrical Power & Energy Systems, 2022, 134: 107343.

131. Li Y, Zhang M, Chen C. A deep-learning intelligent system incorporating data augmentation for short-term voltage stability assessment of power systems[J]. Applied Energy, 2022, 308: 118347.

132. Costilla-Enriquez N, Weng Y. Attack power system state estimation by implicitly learning the underlying models[J]. IEEE Transactions on Smart Grid, 2022, 14(1): 649-662.

133. Chu X, Yi Y, Tang M, et al. Defensive resource allocation for cyber-physical systems in global energy interconnection[C]//IOP Conference Series: Earth and Environmental Science. IOP Publishing, 2019, 227(4): 042002.

134. Khalid H, Peng J. Immunity Toward Data-Injection Attacks Using Multisensor Track Fusion-Based Model Prediction[J]. IEEE Transactions on Smart Grid, 2017, 8(2): 697-707.

135. Liu X, Chang P, Sun Q. Detection of False Data Injection Attacks in Power Grids Based on XGBoost and Unscented Kalman Filter Adaptive Hybrid Prediction[J]. Proceedings of the CSEE, 2021, 41(16): 5462-5476.

136. Alsharif G O, Anagnostopoulos C, Marnerides A K. Energy Market Manipulation via False-Data Injection Attacks[J]. IEEE Access, 2025.

137. Zhou B, Sun B, Zang T, et al. Security risk assessment approach for distribution network cyber physical systems considering cyber attack vulnerabilities[J]. Entropy, 2022, 25(1): 47.

138. Le J, Lang H, Tan T, et al. A Review of Information Security Issues in Distributed Economic Dispatch of New Distribution Systems[J]. Automation of Electric Power Systems, 2024, 48(12): 177-191.

139. Jiang Z, Yao P, Yan B, et al. Cyber-physical system defense decision-making based on priori knowledge of traffic anomaly detection[C]//2023 IEEE 7th Conference on Energy Internet and Energy System Integration (EI2). IEEE, 2023: 5196-5201.

140. Zideh M J, Khalghani M R, Solanki S K. An unsupervised adversarial autoencoder for cyber attack detection in power distribution grids[J]. Electric Power Systems Research, 2024, 232: 110407.

141. Jahromi A A, Kundur D. Fundamentals of cyber-physical systems[M]//Cyber-physical systems in the built environment. Cham: Springer International Publishing, 2020: 1-13.

142. Fan X, Du L, Duan D. Synchrophasor Data Correction Under GPS Spoofing Attack: A State Estimation-Based Approach[J]. IEEE Transactions on Smart Grid, 2018, 9(5): 4538-4546.

143. Dorbala S Y, Bhadoria R S. Analysis for security attacks in cyber-physical systems[J]. Cyber-Physical Systems: A Computational Perspective, 2015: 395-414.

144. Dorbala S Y, Bhadoria R S. Analysis for security attacks in cyber-physical systems[J]. Cyber-Physical Systems: A Computational Perspective, 2015: 395-414.

145. Mosaad N, Abdel-Rahim O, Rahouma W, et al. Identification and Alleviation of False Data Injection within the Cyber Layer of an Enhanced Distributed Secondary Control in DC Islanded Microgrids[J]. IEEE Access, 2025.

146. Lydia M, Prem Kumar G E, Selvakumar A I. Securing the cyber-physical system: A review[J]. Cyber-Physical Systems, 2023, 9(3): 193-223.

147. Hasan K, Shetty S, Islam T, et al. Predictive cyber defense remediation against advanced persistent threat in cyber-physical systems[C]//2022 International Conference on Computer Communications and Networks (ICCCN). IEEE, 2022: 1-10.

148. Kang B G, Seo K M, Kim T G. Model-based design of defense cyber-physical systems to analyze mission effectiveness and network performance[J]. IEEE Access, 2019, 7: 42063-42080.

149. Chen B, Li M. Research on a Data-Driven Framework for Defending Against False Data Injection Attacks in Power Systems[J]. Electric Measurement & Instrumentation, 2024, 61(12): 10-16.

150. Li Y, Bu F, Li Y, et al. Optimal scheduling of island integrated energy systems considering multi-uncertainties and hydrothermal simultaneous transmission: A deep reinforcement learning approach[J]. Applied Energy, 2023, 333: 120540.

151. Farraj A, Hammad E, Kundur D. A Distributed Control Paradigm for Smart Grid to Address Attacks on Data Integrity and Availability[J]. IEEE Transactions on Signal and Information Processing over Networks, 2018, 4(1): 70-81.

152. Wan Y, Cao J. A brief survey of recent advances and methodologies for the security control of complex cyber–physical networks[J]. Sensors, 2023, 23(8): 4013.

153. Zheng Y, Mudhangulla S B, Anubi O M. Moving-horizon false data injection attack design against cyber–physical systems[J]. Control Engineering Practice, 2023, 136: 105552.

154. Sun C, Liu D, Li Q. Study on Dynamic Power Flow in Active Distribution Networks Integrated with Cyber-Physical Systems[J]. Proceedings of the CSEE, 2016, 36(6): 1509-1516.

155. Cao K, Li R, Zhang X, et al. Research on Uncertainty for Complex Event Streams in Cyber-Physical Systems[J]. Computer Engineering and Science, 2015, 37(3): 415-421.

156. Yin Z, Zhang K, Du H, et al. Event-Driven Modeling of Cyber-Physical Systems[J]. Microelectronics & Computer, 2015, 32(12): 126-129.

157. Chamana M, Bhatta R, Schmitt K, et al. An integrated testbed for power system cyber-physical operations training[J]. Applied Sciences, 2023, 13(16): 9451.

158. Sun S, Hossain-McKenzie S, Al Homoud L, et al. An AI-based Approach for Scalable Cyber-Physical Optimal Response in Power Systems[C]//2024 IEEE Texas Power and Energy Conference (TPEC). IEEE, 2024: 1-6.

159. Chen L, Jin P, Yang J, et al. Robust Kalman Filter-Based Dynamic State Estimation of Natural Gas Pipeline Networks[J]. Mathematical Problems in Engineering, 2021, 2021(1): 5590572.

160. Chen J, Wang Q, Tang Y, et al. Anomaly Detection Method for Power Cyber-Physical Systems Considering Bilateral Characteristics[J]. Power System Technology, 2022, 46(6): 2339-2348.

161. Fu Y, Chen L, Ma Z, et al. Preventive Control of Power Systems Including Data-Driven Stability Constraints[J]. Proceedings of the CSEE, 2022, 42(15): 5417-5430.

162. Feng Y, Huang R, Zhao W, et al. A survey on coordinated attacks against cyber–physical power systems: Attack, detection, and defense methods[J]. Electric Power Systems Research, 2025, 241: 111286.

163. Li B, Xiao Y, Shi Y, et al. Anti-honeypot enabled optimal attack strategy for industrial cyber-physical systems[J]. IEEE Open Journal of the Computer Society, 2020, 1: 250-261.
164. Li T, Zhao H, Wang S, et al. Attack and Defense Strategy of Distribution Network Cyber-Physical System Considering EV Source-Charge Bidirectionality[J]. Electronics, 2021, 10(23): 2973.
165. Lei C, Bu S, Wang Q, et al. Observability defense-constrained distribution network reconfiguration for cyber-physical security enhancement[J]. IEEE Transactions on Smart Grid, 2023, 15(2): 2379-2382.
166. Fang S W, Portante A, Husain M I. Moving target defense mechanisms in cyber-physical systems[J]. Securing Cyber-Physical Systems, 2015: 63.
167. Cui Y, et al. Deep reinforcement learning based optimal energy management of multi-energy microgrids with uncertainties[J]. CSEE Journal of Power and Energy Systems, 2024: 1-12. DOI: 10.17775/CSEEJPES.2023.05120.
168. Ao W, Song Y, Wen C. Adaptive cyber-physical system attack detection and reconstruction with application to power systems[J]. IET Control Theory & Applications, 2016, 10(12): 1458-1468.
169. Yang X, et al. Gaussian Mixture Model Uncertainty Modeling for Power Systems Considering Mutual Assistance of Latent Variables[J]. IEEE Transactions on Sustainable Energy, 2024, 1-4. DOI: 10.1109/TSTE.2024.3356259.
170. Wang Y, et al. Collaborative optimization of multi-microgrids system with shared energy storage based on multi-agent stochastic game and reinforcement learning[J]. Energy, 2023, 280: 128182.
171. Ding X, Wang H, Zhang X, et al. Dual nature of cyber–physical power systems and the mitigation strategies[J]. Reliability Engineering & System Safety, 2024, 244: 109958.
172. Mansour R F. Artificial intelligence based optimization with deep learning model for blockchain enabled intrusion detection in CPS environment[J]. Scientific Reports, 2022, 12(1): 12937.
173. Zhang F, Huang Z, Kou L, et al. Data Encryption Based on a 9D Complex Chaotic System with Quaternion for Smart Grid[J]. Chinese Physics B, 2023, 32(1): 010502.
174. Qu Z, Dong Y, Mugemanyi S, et al. Dynamic Exploitation Gaussian Bare-Bones Bat Algorithm for Optimal Reactive Power Dispatch to Improve the Safety and Stability of Power System[J]. IET Renewable Power Generation, 2022, 16: 1401-1424.
175. Fang Z, Zhao D, Chen C, et al. Nonintrusive Appliance Identification with Appliance-Specific Networks[J]. IEEE Transactions on Industry Applications, 2020, 56(4): 3443-3452.
176. Zhong X, xin Li G, Zhng C. False data injection in power smart grid and identification of the most vulnerable bus; a case study 14 IEEE bus network[J]. Energy Reports, 2021, 7: 8476-8484.
177. BaSin D, Cremers C, Kim T, et al. Design, Analysis, and Implementation of ARPKI: an Attack-Resilient Public-Key Infrastructure[J]. IEEE Transactions on Dependable and Secure Computing, 2016, 15(3): 393-408.
178. Yan K, Liu X, Lu Y, et al. A cyber-physical power system risk assessment model against cyberattacks[J]. IEEE Systems Journal, 2022, 17(2): 2018-2028.
179. Kesici M, Pal B, Yang G. Detection of false data injection attacks in distribution networks: A vertical federated learning approach[J]. IEEE Transactions on Smart Grid, 2024.
180. Li Y, Li J, Wang Y. Privacy-preserving spatiotemporal scenario generation of renewable energies: A federated deep generative learning approach[J]. IEEE Transactions on Industrial Informatics, 2021, 18(4): 2310-2320.
181. Yu J, Li Q, Li L. Localization of coordinated cyber-physical attacks in power grids using moving target defense and machine learning[J]. Electronics, 2024, 13(12): 2256.

182. Keçeci C, Davis K R, Serpedin E. Federated learning based distributed localization of false data injection attacks on smart grids[J]. arXiv preprint arXiv:2306.10420, 2023.

183. Kausar F, Deo S, Hussain S, et al. Federated Deep Learning Model for False Data Injection Attack Detection in Cyber Physical Power Systems[J]. Energies, 2024, 17(21): 5337.

184. Li Y, Li J, Qi J, et al. Robust Cubature Kalman Filter for Dynamic State Estimation of Synchronous Machines Under Unknown Measurement Noise Statistics[J]. IEEE Access, 2019, 7: 29139-29148.

185. Xu K, Niu Y. Decentralized attack detection for multi-area power systems via interconnection-decoupled sliding mode observer[J]. International Journal of Robust and Nonlinear Control, 2023, 33(12): 6697-6714.

186. Preeti G, Sanjeev Kumar P. A Blockchain Based Decentralized Application System for Vanet FDIA Detection[C]//International Conference on Computing and Communication Networks. Singapore: Springer Nature Singapore, 2023: 95-119.

187. Bai M, Liu P, Lv F, et al. Adversarial Attack against Intrusion Detectors in Cyber-Physical Systems With Minimal Perturbations[C]//2024 IEEE International Symposium on Parallel and Distributed Processing with Applications (ISPA). IEEE, 2024: 816-825.

188. Dong Z, Tang M, Tian M. Allocating defense resources for spatial cyber-physical power systems based on deep reinforcement learning[C]//2023 IEEE 6th International Conference on Industrial Cyber-Physical Systems (ICPS). IEEE, 2023: 1-6.

189. Ullrich J, Weippl E R. CyPhySec: Defending cyber-physical systems[J]. ERCIM News, 2015, 102: 18-18.

190. Xu A, Jiang Y, Zhang Y, et al. A Double-Layer Cyber Physical Cooperative Emergency Control Strategy Modification Method for Cyber-Attacks Against Power System[C]//2020 12th IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC). IEEE, 2020: 1-5.

191. Sun C, Su Q, Li J. Secure Tracking Control and Attack Detection for Power Cyber-Physical Systems based on Integrated Control Decision[J]. IEEE Transactions on Information Forensics and Security, 2024.

192. Wang P, Zhang R, He X. New Approaches to Detection and Secure Control for Cyber-physical Systems Against False Data Injection Attacks[J]. International Journal of Control, Automation and Systems, 2025, 23(1): 332-345.

193. Kaloudi N, Li J. The ML-based sensor data deception targeting cyber–physical systems: A review[J]. Computer Science Review, 2025, 57: 100753.

194. Busari W A, Bello A A. Security, Trust, and Privacy in Cyber-physical Systems (CPS)[C]//2024 2nd International Conference on Cyber Physical Systems, Power Electronics and Electric Vehicles (ICPEEV). IEEE, 2024: 1-6.

195. Noor U, Shahid S, Kanwal R, et al. A Machine Learning based Empirical Evaluation of Cyber Threat Actors High Level Attack Patterns over Low level Attack Patterns in Attributing Attacks[J]. arXiv preprint arXiv:2307.10252, 2023.

196. Samad T. Human-in-the-loop control and cyber–physical–human systems: applications and categorization[J]. Cyber–physical–human systems: fundamentals and applications, 2023: 1-23.

197. Gil M, Albert M, Fons J, et al. Engineering human-in-the-loop interactions in cyber-physical systems[J]. Information and software technology, 2020, 126: 106349.

198. Iyenghar P. Clever Hans in the Loop? A Critical Examination of ChatGPT in a Human-in-the-Loop Framework for Machinery Functional Safety Risk Analysis[J]. Eng, 2025, 6(2): 31.

199. Adil M, Farouk A, Abulkasim H, et al. NG-ICPS: Next Generation Industrial-CPS, Security Threats in the Era of Artificial Intelligence, Open Challenges With Future Research Directions[J]. IEEE Internet of Things Journal, 2024.

200. Agarwal M, Venkateswaran S K, Sivakumar R. Human-in-the-loop rl with an eeg wearable headset: On effective use of brainwaves to accelerate learning[C]//Proceedings of the 6th ACM Workshop on Wearable Systems and Applications. 2020: 25-30.
201. Nguyen T T, Kadavil R, Hooshyar H. A Real-time Cyber-Physical Simulation Testbed for Cybersecurity Assessment of Large-Scale Power Systems[J]. IEEE Transactions on Industry Applications, 2024.
202. Li P, Fu J, Xie K, et al. A Defense Planning Model for a Power System Against Coordinated Cyber-Physical Attack[J]. Protection and Control of Modern Power Systems, 2024, 9(5): 84-95.
203. Ravikumar G, Hyder B, Babu J R, et al. Cps testbed architectures for wampac using industrial substation and control center platforms and attack-defense evaluation[C]//2021 IEEE Power & Energy Society General Meeting (PESGM). IEEE, 2021: 1-5.
204. Jiang Y, Wu S, Ma R, et al. Monitoring and defense of industrial cyber-physical systems under typical attacks: From a systems and control perspective[J]. IEEE Transactions on Industrial Cyber-Physical Systems, 2023, 1: 192-207.
205. Fan Y, Li J, Zhang D, et al. Supporting sustainable maintenance of substations under cyber-threats: An evaluation method of cybersecurity risk for power CPS[J]. Sustainability, 2019, 11(4): 982.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.