Review

Not peer-reviewed version

Resilient-by-Design: A Paradigm Shift in Securing Power CPS against False Data Injection and Beyond

Shuaizheng Peng *

Posted Date: 15 May 2025

doi: 10.20944/preprints202505.1170.v1

Keywords: power cyber-physical systems; false data injection attacks; resilient-by-design; federated learning; edge intelligence; adaptive cyber defense

 doi:10.20944/preprints202505.1170.v1

Review

Resilient-by-Design: A Paradigm Shift in Securing Power CPS Against False Data Injection and Beyond

Shuaizheng Peng

School of Electrical Engineering & Automation, Henan Institute of Technology, Xinxiang, China; ee_dreamer@outlook.com

Abstract: With the increasing integration of cyber and physical layers, power cyber-physical systems (CPS) face growing risks from advanced cyber threats, especially False Data Injection Attacks (FDIAs). Existing defense methods mainly focus on detection, leaving gaps against evolving, multi-stage attacks. This review advocates a shift toward Resilient-by-Design CPS, emphasizing system-level co-design of secure architectures, distributed detection, edge intelligence, and recovery mechanisms. It further discusses adaptive defense strategies using reinforcement learning, generative models, and explainable AI. Future directions include integrating resilience into grid planning, adversarial testing, and cross-sector policy coordination, aiming to enable secure and intelligent power systems.

Keywords: power cyber-physical systems; false data injection attacks; resilient-by-design; federated learning; edge intelligence; adaptive cyber defense

1. Introduction

1.1. Motivation: From Reactive Detection to Proactive Resilience

The digitalization of power systems marks a significant leap in grid management capabilities, enabling real-time data acquisition, advanced analytics, distributed control, and predictive maintenance [1–3]. Modern power grids have evolved into complex **cyber-physical systems (CPS)**, integrating millions of sensors, intelligent electronic devices (IEDs), renewables, and control systems with sophisticated communication networks [4,5]. This convergence empowers operators to optimize energy production, transmission, and distribution with unprecedented accuracy [6].

However, this transformation also introduces **new cyber vulnerabilities** [7–9]. As critical functions increasingly rely on information and communication technology (ICT), attackers can target not only physical infrastructure but also the digital pathways that control it [10]. Among these emerging threats, **False Data Injection Attacks (FDIAs)** stand out for their stealth, scalability, and potentially devastating consequences. Unlike conventional cyber-attacks that cause immediate service disruptions, FDIAs **silently corrupt system data**, deceiving state estimation algorithms and triggering incorrect operational decisions that may lead to **cascading failures, blackouts, or equipment damage [11–13]**.

Notably, real-world incidents have already demonstrated the feasibility and impact of cyber-physical attacks on energy infrastructure. The **2015 Ukraine power grid cyberattack** caused widespread blackouts affecting over 230,000 people, leveraging a multi-stage attack chain involving malware, remote access, and control manipulation. The **Colonial Pipeline ransomware attack** in 2021 disrupted fuel supplies across the U.S. East Coast, highlighting the interdependence of energy and cyber infrastructure. These events emphasize that **critical infrastructure is no longer protected by physical barriers alone [14,15]**.

Over the past decade, researchers have made significant progress in **developing detection algorithms** to identify FDIAs, leveraging techniques such as state estimation residual analysis, machine learning, and data fusion. However, these solutions are largely **reactive**, focusing on

 doi:10.20944/preprints202505.1170.v1

detecting and responding to attacks *after* they have penetrated the system. This reactive posture has several limitations [16–18]:

- **Detection delays** may allow attacks to inflict damage before mitigation can occur.
- **False positives and false negatives** can undermine operator trust and lead to inappropriate responses.
- **Over-reliance on centralized detection architectures** creates bottlenecks and single points of failure.
- **Limited scalability and adaptability** restrict deployment across large, heterogeneous grid environments.

To break this reactive cycle, the research community and industry must **shift toward proactive resilience**—designing power CPS that can **withstand, absorb, recover from, and adapt to cyber-physical disruptions** without catastrophic performance degradation [19]. This concept, known as **"Resilient-by-Design"**, treats resilience not as a patchwork of add-on defenses but as a **core design principle** embedded throughout the system's lifecycle [20–22].

1.2. Scope: What Does "Resilient-by-Design" Mean in Power CPS?

"Resilient-by-Design" represents a **systematic, holistic approach** to security, emphasizing **prevention, detection, response, and recovery** as **interconnected layers of defense**. In the context of power CPS, this paradigm involves [23,24]:

- **Secure Sensing and Communication**: Ensuring the authenticity, integrity, and availability of measurement and control data through cryptographic protocols, secure communication architectures, and data validation mechanisms.
- **Distributed, Real-Time Detection and Response**: Empowering local control entities—such as substations, microgrids, and edge devices—with **autonomous detection and mitigation capabilities**, reducing response latency and improving scalability.
- **Data Recovery and Control Reconfiguration**: Providing mechanisms for **state estimation recovery, topology inference, and control reconfiguration** to maintain grid observability and controllability after a cyber compromise.
- **Adaptive and Explainable Defense Mechanisms**: Leveraging **AI-driven algorithms** that can **learn, adapt, and explain** their behavior in evolving threat landscapes, bridging the gap between machine intelligence and operator trust.
- **Cross-Domain Coordination**: Aligning cyber defense with **physical grid operations**, **regulatory policies**, and **market mechanisms** to ensure resilience extends beyond technical layers to include organizational and societal dimensions.

This review adopts this Resilient-by-Design perspective, integrating insights from cybersecurity, control theory, artificial intelligence, and energy systems engineering. It extends the research frontier beyond FDIA detection, addressing broader questions of systemic resilience, cross-layer defense integration, and operational feasibility.

1.3. Industry and Policy Drivers for Resilient Power CPS

Global policy frameworks increasingly recognize the **national security implications** of power CPS cyber vulnerabilities [25]. Key initiatives include:

- The North American Electric Reliability Corporation's Critical Infrastructure Protection (NERC CIP) standards, which mandate baseline cybersecurity practices for U.S. and Canadian utilities.
- The European Union's Network and Information Systems (NIS2) Directive, expanding cybersecurity obligations for operators of essential services, including energy providers.
- China's Cybersecurity Law and Critical Information Infrastructure Protection regulations, emphasizing sovereignty and supply chain security in critical sectors.
- The U.S. Department of Energy's Cybersecurity Capability Maturity Model (C2M2), providing a framework for utilities to assess and improve their cyber resilience.

 doi:10.20944/preprints202505.1170.v1

These policies reflect growing recognition that **cyber resilience is a strategic imperative**, not merely a technical challenge. Utilities, grid operators, and policymakers must work together to **operationalize resilience requirements** through:

- Investment in secure infrastructure upgrades.
- Integration of resilience metrics into planning and procurement.
- Cross-sector information sharing and threat intelligence.
- Development of workforce skills in cybersecurity and power engineering.

1.4. Key Contributions and Structure of This Review

This review aims to bridge research, policy, and industry practices, providing a comprehensive roadmap for Resilient-by-Design power CPS. Key contributions include:

- **Characterization of the evolving threat landscape**, highlighting the shift from isolated FDIA to coordinated, multi-vector, and AI-driven attacks.
- **Framework for security-aware grid architecture design**, emphasizing redundancy, diversity, and modularity.
- **Review of distributed detection and response mechanisms**, including federated learning, multi-agent systems, and edge intelligence.
- **Insights into post-attack data reconstruction and control recovery**, essential for maintaining operational continuity.
- **Exploration of adaptive AI-driven security strategies**, including reinforcement learning, generative modeling, and explainable AI.
- **Identification of future research directions and policy challenges**, promoting actionable strategies for cross-sector resilience.

2. Evolution of Power CPS Threat Landscape

2.1. From Classic FDIA to Coordinated Multi-Stage Attacks

The first formal definition of FDIA by Liu et al. in 2009 was a landmark contribution to power system cybersecurity [27]. It demonstrated that attackers could **mathematically craft stealthy false data** that aligns with the physical constraints of power flow models, making it **undetectable by conventional bad data detection** based on residual checks. This inspired a wave of research focusing on **state estimation security**, laying the foundation for cyber-physical security as a research discipline in power systems [28–30].

Limitations of Early FDIA Models

However, early models often assumed **full system knowledge** and **unrestricted access** to measurements—assumptions that may not hold in real-world attacks [31,32]. In practice, adversaries may face **partial information**, **limited access**, and **stochastic network conditions**. Despite these practical barriers, real-world incidents have shown that attackers **do not need perfect information** to cause significant disruption [33].

Transition to Multi-Stage and Coordinated Attacks

Over the past decade, attack strategies have evolved from isolated data injection toward **multi-stage, coordinated campaigns** that combine [34]:

- **Initial reconnaissance**, such as scanning network ports or phishing operator credentials.
- **Lateral movement**, compromising multiple devices or systems to escalate privileges.
- **Persistence**, embedding malware to maintain long-term system access.
- **Coordinated manipulation**, simultaneously targeting measurement data, control signals, and operator interfaces.

 doi:10.20944/preprints202505.1170.v1

These attacks often leverage **supply chain vulnerabilities**, **insider threats**, or **third-party software exploits**. The **2015 and 2016 Ukraine grid attacks** serve as prime examples, where attackers combined malware (BlackEnergy and Industroyer), remote access tools, and manual control room manipulation to orchestrate widespread outages.

Adversarial Goals Beyond Outages

Modern cyber-physical adversaries may pursue objectives beyond service disruption, including [35–37]:

- **Economic manipulation**, such as exploiting electricity markets by causing price spikes or imbalance penalties.
- **Physical equipment damage**, as seen in Stuxnet's targeted sabotage of centrifuges.
- **Erosion of operator trust**, causing hesitation or incorrect responses during critical events.
- **Long-term espionage**, gathering data on system operations, vulnerabilities, or market behaviors.

Understanding these multi-dimensional attack objectives is crucial for developing defense strategies that go beyond availability protection, addressing integrity, confidentiality, and trust.

2.2. Emerging Attack Vectors: AI-Driven Attacks, Federated Poisoning, Time-Sync Attacks

AI-Driven Adversarial Strategies

As defenders increasingly adopt **machine learning (ML)** and **artificial intelligence (AI)** for anomaly detection, attackers are adapting by **using AI themselves** to optimize their attacks. **Adversarial machine learning** techniques enable attackers to [38–40]:

- **Train surrogate models** of the grid based on observed data.
- **Craft adversarial examples** that exploit the detection model's blind spots.
- **Deploy adaptive attacks** that evolve in response to defense updates.

For example, an attacker might **simulate different FDIA patterns** using reinforcement learning to identify the most stealthy and effective manipulation strategies.

Federated Learning Poisoning Risks

Federated learning allows distributed agents to collaboratively train models without sharing raw data, improving privacy [41–43]. However, this **opens new attack surfaces**, such as:

- **Model poisoning**, where compromised agents submit malicious updates to degrade detection performance.
- **Sybil attacks**, where a single adversary controls multiple seemingly independent agents.
- **Backdoor insertion**, embedding hidden triggers in the global model.

Mitigating these risks requires robust aggregation techniques (e.g., Krum, Bulyan) and participant verification mechanisms.

Time Synchronization and GPS Spoofing

Time synchronization is critical for PMU-based state estimation [44]. **GPS spoofing attacks** can introduce:

- **Timestamp misalignment**, leading to inaccurate state estimation.
- **Inter-PMU desynchronization**, degrading the performance of wide-area monitoring systems.
- **Control instability**, if protection or control schemes rely on precise timing.

Given the low-cost and accessible nature of GPS spoofers, this attack vector poses a significant operational risk, especially in wide-area or islanded microgrid applications [45–47].

Advanced Control Hijacking and Data-Driven Control Manipulation

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 May 2025 doi:10.20944/preprints202505.1170.v1

Adversaries may go beyond data corruption to **manipulate control logic itself**, for instance by [48]:

- Exploiting weakly secured remote terminal units (RTUs) to inject malicious setpoints.
- Manipulating distributed energy resource (DER) controllers to destabilize frequency or voltage.
- Targeting energy management systems (EMS) to disrupt optimal dispatch or market operations.

These attacks are **difficult to detect** if they mimic legitimate operator behavior or exploit **trust relationships between devices and control centers**.

2.3. Cross-Domain Attack Modeling: ICT-OT Coupling Dynamics

The Need for Cross-Domain Security Models

Power CPS are not isolated from other infrastructures. They **rely on telecommunications, IT services, and cloud platforms**, creating **cross-domain dependencies** that adversaries can exploit [49,50].

For instance:

- **Telecom network failures** can block operator communications during cyber-physical events.
- **Cloud service compromises** may expose configuration or credential data.
- **Third-party vendors** providing SCADA or EMS software may introduce supply chain risks.

Example: Coordinated Attack on Energy and Telecom

Consider a hypothetical scenario where an attacker:

(1) Launches a **DDoS attack** on the telecom provider's network, delaying operator situational awareness.
(2) Simultaneously **injects false data** into substation measurement streams.
(3) Exploits **compromised VPN credentials** to access control systems.

Such cross-layer, multi-domain attacks require defense mechanisms that integrate cyber and physical situational awareness, bridging the gap between ICT and OT domains [51–53].

Modeling Multi-Layered Propagation Effects

Advanced simulation tools, such as **co-simulation platforms** that link power system models with communication network models, are essential to [54,55]:

- Analyze propagation effects of cross-domain attacks.
- Evaluate cascading risks across ICT and OT layers.
- Design coordinated defense strategies that account for multi-domain interdependencies.

2.4. Summary of Threat Evolution

Threat Evolutions are summarized in Table 1.

Table 1. Characteristics and Defense Challenges of Threat Evolutions.

Threat Category	Characteristics	Challenges for Defense
Classic FDIAs	Linear state estimation manipulation	Stealthy, undetectable by residual checks
Multi-Stage Attacks	Coordinated cyber-physical campaigns	Hard to attribute and mitigate in real time
AI-Driven Attacks	Adaptive, model-aware adversarial strategies	Evasive and evolving attack patterns

 doi:10.20944/preprints202505.1170.v1

Federated Poisoning	Compromising collaborative learning	Degrades distributed detection effectiveness
Time-Sync Attacks	GPS spoofing, desynchronization	Undermines wide-area monitoring and control
Cross-Domain Attacks	Exploiting ICT-OT dependencies	Requires integrated multi-layer defense

3. Design Foundations for Resilient Power CPS

Building resilience into power CPS requires **rethinking system architecture, control strategies, and operational workflows**. Instead of retrofitting security onto legacy systems, a **Resilient-by-Design** approach integrates defense mechanisms from the ground up, balancing **operational efficiency**, **security assurance**, and **scalability [56–58]**.

3.1. Security-Aware Grid Architecture: Redundancy, Diversity, and Modularity

Redundancy: Engineering Out Single Points of Failure

Redundancy is a well-known principle in power system reliability engineering, traditionally applied to **physical infrastructure** such as transmission lines, transformers, and protection relays. However, **cyber redundancy**—including **sensing, communication, and control redundancy**—is equally critical in mitigating cyber-physical threats [59,60].

- **Redundant Sensing**: Deploying **multi-source measurements** (e.g., PMUs, RTUs, and smart meters) provides cross-verification capabilities, reducing reliance on any single data stream.
- **Redundant Communication**: Establishing **diverse communication paths**, such as **wired fiber networks and wireless LTE/5G links**, ensures that data can flow even if one channel is disrupted.
- **Redundant Control Logic**: Implementing **parallel control algorithms**, possibly on **independent hardware or software platforms**, provides fallback options if one control path is compromised.

The goal is to **localize the impact** of cyber-physical disruptions and **enable graceful degradation** rather than total system collapse [61–63].

Diversity: Breaking Homogeneity to Increase Attack Complexity

Homogeneous systems—those built on identical hardware, software, and protocols—present an **attractive target for attackers**, who can **generalize their exploits across the entire infrastructure**. Diversity, in contrast, increases the **cost and complexity of attacks** by forcing adversaries to **navigate heterogeneous defense surfaces [64,65]**.

- **Vendor Diversity**: Using equipment from **multiple manufacturers** reduces the risk of a single vendor vulnerability affecting the entire system.
- **Software Diversity**: Running **different firmware versions** or **diverse operating systems** mitigates the impact of zero-day exploits.
- **Protocol Diversity**: Supporting **multiple communication protocols** (e.g., IEC 61850, DNP3, Modbus) with **gateway isolation** can prevent protocol-specific attacks from spreading system-wide.

However, managing diversity introduces operational challenges, such as interoperability management and training requirements. These must be balanced against the security benefits through risk-informed engineering trade-offs [66–69].

Modularity: Isolating Risks through System Segmentation

 doi:10.20944/preprints202505.1170.v1

Modularity involves partitioning the grid into semi-independent, self-sufficient segments with clear trust boundaries [70–72]. Examples include:

- **Microgrids** capable of **islanded operation** during cyber or physical disturbances.
- **Virtual Power Plants (VPPs)** aggregating DERs with **autonomous control capabilities**.
- **Regional Control Zones** with **localized monitoring and response mechanisms**.

Modular architectures enable **localized resilience**, reducing the risk of **cascading failures** across the entire grid. They also support **incremental deployment** of advanced security features without requiring a complete system overhaul [73].

Supply Chain and Physical Security Integration

True Resilient-by-Design architectures must also consider [74,75]:

- Supply chain security, ensuring that hardware and software components are free from embedded vulnerabilities.
- Physical security integration, protecting critical cyber-physical assets from tampering, sabotage, or insider threats.

This requires end-to-end security assurance, covering procurement, installation, operation, and decommissioning phases [76,77].

3.2. Trustworthy Sensing and Communication: Secure-by-Protocol vs. Secure-by-Learning

Secure-by-Protocol: Cryptographic Protection of Data Integrity

Protocol-level security remains **foundational** for defending against data manipulation and eavesdropping. Key mechanisms include [78–80]:

- **Message Authentication Codes (MACs)**: Verifying that messages have not been altered in transit.
- **Digital Signatures**: Providing **non-repudiation** and **source authentication**.
- **End-to-End Encryption**: Protecting data confidentiality from source to destination.

Standards such as **IEC 62351** provide guidelines for **securing SCADA and substation communications**. However, practical challenges include [81]:

- **Key management complexity** in large, distributed systems.
- **Computational overhead** on resource-constrained edge devices.
- **Legacy system limitations**, where older devices lack cryptographic capabilities.

Secure-by-Learning: Data-Driven Trust Validation

Complementing protocol-level security, **data-driven validation mechanisms** can detect:

- **Statistical anomalies** in measurement patterns.
- **Physical model inconsistencies**, such as violations of power flow equations.
- **Temporal or spatial deviations** from normal system behavior.

Machine learning models, including **physics-informed neural networks**, can **learn normal operational baselines** and **flag deviations** that may indicate cyber-physical manipulation. These methods are particularly valuable when [82–84]:

- Cryptographic protection is infeasible or compromised.
- Anomalies bypass signature-based detection.

However, model generalizability, explainability, and resilience to adversarial manipulation remain active research challenges [85].

Hybrid Secure-By-Design Integration

The most resilient architectures combine secure-by-protocol and secure-by-learning approaches, providing defense-in-depth. For example:

- Cryptographic mechanisms ensure data authenticity at the transport layer.

- Anomaly detection models validate data plausibility at the application layer.

This layered defense ensures that even if one protection mechanism is bypassed, **complementary safeguards** remain in place [86–88].

3.3. Control-Theoretic Resilience Metrics and Stability under Adversarial Perturbation

Quantifying Cyber-Physical Robustness

Control-theoretic resilience metrics provide a **quantitative foundation** for designing systems that can **tolerate bounded cyber-physical disturbances [89,90]**. Key metrics include:

- **Input-output stability margins**: Measuring the system's ability to absorb input disturbances without destabilizing output responses.
- **Region of attraction under uncertainty**: Defining the **safe operating region** despite model uncertainties or data corruption.
- **Resilient controllability and observability**: Ensuring that **critical states remain observable and controllable** even if some data channels are compromised.

Stability-Aware Control Algorithm Design

Resilient control algorithms can be designed using [91–93]:

- **Robust control techniques** (e.g., H-infinity control) that **minimize worst-case impacts** of bounded disturbances.
- **Adaptive control methods** that **adjust controller parameters** in response to detected anomalies.
- **Sliding mode control** that **enforces stability** through **discontinuous control actions**, effective against model uncertainties.

Graceful Degradation and Emergency Protocols

In severe attack scenarios, **maintaining partial functionality** may be preferable to total shutdown. **Graceful degradation strategies** include [94,95]:

- **Prioritizing critical loads** (e.g., hospitals, data centers).
- **Selective islanding** of microgrids.
- **Fallback to manual control** when automation is compromised.

Pre-defined emergency control protocols, validated through simulation and field exercises, ensure that operators know when and how to transition to degraded modes safely.

4. Real-Time Distributed Detection and Response Mechanisms

4.1. Federated and Privacy-Preserving FDIA Detection

The growing scale and geographical distribution of power CPS make **centralized detection architectures increasingly impractical**. Centralized methods face scalability challenges, high communication overhead, and data privacy concerns. To address these limitations, **federated learning** has emerged as a **distributed and privacy-preserving paradigm** for collaborative FDIA detection [96–98].

In federated learning, local agents (e.g., substations, microgrids, or edge devices) train detection models on **locally available data** without sharing raw data with a central server. Only **model updates or gradients** are exchanged and aggregated to form a global model. This approach offers several advantages:

- **Data privacy preservation**, as raw measurements never leave local devices.
- **Reduced communication overhead**, since model updates are typically smaller than raw datasets.
- **Scalability**, enabling large-scale deployments across geographically distributed infrastructures.

 doi:10.20944/preprints202505.1170.v1

However, federated learning also introduces new challenges, including **model poisoning attacks**, where malicious participants submit deceptive updates to degrade global model performance. To mitigate this risk, **robust aggregation algorithms** and **participant reputation mechanisms** must be integrated into the federated learning process [99,100].

4.2. Multi-Agent-Based Cooperative Defense Strategies

Power CPS inherently consist of **interconnected yet semi-autonomous subsystems**, such as regional control centers, microgrids, and substations [101–103]. These subsystems can be modeled as **intelligent agents** capable of:

- **Local detection**, based on their own measurements and historical data.
- **Cooperative information sharing**, exchanging detection results, alerts, or suspicious patterns with neighboring agents.
- **Distributed decision-making**, coordinating response actions to contain or mitigate detected threats.

Multi-agent systems enable **cooperative defense** without over-relying on a single point of control. For example, if one agent detects anomalous behavior, it can **propagate warnings** to its neighbors, enabling **collective situational awareness [104–106]**. This **peer-to-peer defense mechanism** enhances resilience against stealthy attacks that target isolated subsystems.

Effective multi-agent cooperation requires [107,108]:

- **Consensus protocols** to resolve conflicting assessments among agents.
- **Trust management frameworks** to evaluate the credibility of information sources.
- **Secure communication channels** to prevent attackers from hijacking agent interactions.

By leveraging the distributed nature of power CPS, multi-agent systems can provide **scalable, robust, and adaptive defense capabilities**.

4.3. Edge Intelligence and On-Device Learning for Local Anomaly Detection

As computational resources become increasingly available at the network edge (e.g., in substations or IoT devices), **edge intelligence** offers a promising solution for **real-time, localized FDIA detection [109,110]**.

Edge intelligence involves deploying **lightweight machine learning models** or **streaming analytics engines** directly on edge devices, enabling them to [111–113]:

- Continuously monitor local data streams (e.g., voltage, current, frequency).
- Detect anomalies in real time, without relying on centralized processing.
- Trigger immediate local responses, such as isolating compromised components or raising alarms.

Key enablers of edge intelligence include [114]:

- **Model compression** and **resource-aware learning algorithms**, which reduce the computational footprint of machine learning models.
- **Online and incremental learning**, allowing models to adapt to evolving grid conditions without full retraining.
- **Explainable AI techniques**, providing interpretable detection results to support operator trust and human-in-the-loop decision-making.

By shifting detection and response capabilities closer to the data sources, edge intelligence **reduces detection latency**, **improves scalability**, and **enhances system autonomy**, making it a critical component of resilient power CPS defense architectures.

5. Data Reconstruction and Recovery after Compromise

While **detection and isolation** are crucial first steps in cyber defense, **what happens after an attack is equally critical**. Simply **discarding compromised data or disconnecting affected assets** can leave the grid in a **degraded or unobservable state**, potentially leading to **secondary failures** or **operational blind**

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 May 2025 doi:10.20944/preprints202505.1170.v1

spots. Therefore, **resilient power CPS must include data reconstruction and system recovery capabilities** to safely restore operations [115–117].

5.1. Resilient State Estimation and Control Recovery

While much of the existing literature focuses on **detecting FDIAs**, less attention has been given to **what happens after detection [118–120]**. In practice, simply flagging or discarding suspected data may not be sufficient, especially if large portions of measurement data are compromised. This could lead to **loss of observability** and **unreliable control actions [121]**.

Resilient state estimation addresses this challenge by enabling the power system to:

- **Reconstruct missing or corrupted states** using redundant measurements, historical data, or predictive models.
- **Estimate confidence levels** for reconstructed states, supporting risk-informed operational decisions.
- **Reconfigure control strategies** based on partially trusted data, prioritizing stability and safety.

Advanced techniques, such as **moving horizon estimation**, **robust Kalman filtering**, and **physics-informed neural networks**, have shown potential for enhancing state estimation resilience under partial data loss. These methods combine physical system models with data-driven insights, enabling **adaptive estimation** even in degraded sensing environments [123–125].

5.2. Topology and Data Restoration after Multi-Point Compromise

Multi-point FDIAs often target **both measurement data and network topology information**, making recovery particularly challenging. Effective **topology restoration** requires [126–128]:

- **Cross-validation of topology information** using multiple independent data sources (e.g., PMU data vs. SCADA data).
- **Topology inference algorithms**, capable of reconstructing the most likely network structure based on surviving measurements and physical constraints.
- **Anomaly-tolerant network reconfiguration**, which can isolate suspicious areas while maintaining system-wide observability.

For example, if an attacker manipulates breaker status data to hide the true network topology, data-driven topology estimation methods can help **reconstruct the likely physical configuration**, reducing the risk of operating on false assumptions [129].

Furthermore, **redundant data pathways**, such as alternative communication channels or secondary measurement systems, can **provide fallback information** to support post-attack recovery. Leveraging such redundancy is critical to restoring **situational awareness** after a coordinated attack [130].

5.3. Redundant Data Pathways and Confidence-Aware Data Fusion

Resilient recovery also relies on **fusing data from multiple, potentially imperfect sources**. Confidence-aware data fusion techniques aim to [131–133]:

- **Quantify uncertainty** in each data source, based on historical reliability, detection results, or model consistency checks.
- **Combine multiple data streams** in a weighted manner, giving higher priority to more trusted sources.
- **Provide operators with confidence scores**, supporting informed decision-making under uncertainty.

For instance, if PMU data appears suspicious due to detected time-sync attacks, the system can **downgrade its confidence** in that data and rely more on SCADA or historical trend data. This **adaptive trust management** helps maintain operational awareness even when some data sources are compromised [134].

 doi:10.20944/preprints202505.1170.v1

Additionally, **blockchain-based data provenance** and **secure logging mechanisms** can help track the **integrity and origin** of measurement data, providing further assurance during recovery processes.

In summary, resilient power CPS require **not only detection but also intelligent recovery mechanisms** that leverage redundancy, cross-validation, and confidence-aware fusion to **restore safe and reliable operations** after cyber-physical compromises [135,136].

6. Autonomy-Driven Adaptive Security: From Rules to Reasoning

Conventional cyber defense for power CPS often relies on **static security policies**, **fixed detection thresholds**, and **manual operator intervention**. While these methods provide basic protection, they **fail to scale** in the face of **dynamic, evolving, and adaptive adversaries [137]**. Moreover, **overly rigid defenses** risk generating **excessive false positives**, overwhelming operators and degrading trust in security systems. To address these limitations, **autonomy-driven adaptive security** leverages **artificial intelligence (AI)** and **machine learning (ML)** to enable **self-learning, self-adaptive, and self-explainable defense mechanisms [138–140]**. This section explores cutting-edge techniques that transform static defenses into **reasoning-capable, autonomous security agents**.

6.1. Reinforcement Learning for Adaptive Cyber Response

Traditional cyber defense mechanisms often rely on **static rule sets or pre-defined thresholds**, which struggle to cope with the evolving and dynamic nature of cyber-physical attacks. Reinforcement learning (RL) provides a promising paradigm for **adaptive cyber response**, enabling power CPS to **learn optimal defense strategies through interaction with the environment [141–143]**.

In an RL framework:

- The **power CPS** is modeled as an environment with **states** (e.g., grid measurements, detection alerts), **actions** (e.g., isolating a node, switching control modes), and **rewards** (e.g., maintaining stability, minimizing false positives).
- An **agent** learns a **policy** that maps observed states to actions that maximize long-term resilience [144].

Key advantages of RL-based defense include:

- **Adaptability** to unseen attack patterns or evolving grid conditions.
- **Autonomous policy improvement** through continuous learning.
- **Balance between false alarms and missed detections**, optimizing operational impact.

Recent research has demonstrated the feasibility of **deep reinforcement learning (DRL)** for cyber-physical defense, leveraging neural networks to handle high-dimensional state spaces [145–147]. However, ensuring **safe exploration**, **policy interpretability**, and **real-time convergence** remain open challenges for practical deployment [148].

6.2. Generative Models for Anticipatory Defense

While detection and response are reactive by nature, **anticipatory defense** aims to **predict and preempt attacks before they fully materialize [149,150]**. **Generative models**, such as generative adversarial networks (GANs) and variational autoencoders (VAEs), offer tools for [151–154]:

- Simulating potential attack scenarios to stress-test defense mechanisms.
- Generating synthetic attack data to improve detection model robustness.
- Forecasting likely system states under adversarial conditions, enabling preemptive mitigation.

For example, GAN-based frameworks can generate **plausible false data injection patterns**, allowing the defender to **train detection models on a wider variety of attack vectors**. Similarly, VAEs can **model normal system behavior**, flagging deviations that might indicate stealthy attacks [155–160].

By integrating generative models into the cyber defense lifecycle, power CPS can **proactively explore the adversarial space**, improving preparedness against sophisticated and adaptive attackers.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 May 2025 doi:10.20944/preprints202505.1170.v1

6.3. Explainable AI for Operator Trust and Human-in-the-Loop Security

As AI and machine learning increasingly drive cyber defense, **explainability becomes critical** for operator trust and effective human-machine collaboration [161–163]. **Explainable AI (XAI)** aims to make AI-driven decisions **transparent, interpretable, and actionable** for human operators [164–168].

Key aspects of XAI in power CPS defense include [169,170]:

- **Visualizing detection rationale**, such as highlighting which sensors or features contributed most to a detection decision.
- **Providing confidence scores and uncertainty estimates**, supporting risk-informed operator actions [171].
- **Enabling what-if analyses**, allowing operators to explore the implications of different response strategies [172].

Human-in-the-loop security frameworks combine AI automation with human judgment, ensuring that high-consequence decisions (e.g., grid reconfiguration, load shedding) are informed by both machine insights and operator expertise [173–175].

Ultimately, explainable and human-centered AI enhances **trust, accountability, and operational reliability**, ensuring that advanced defense mechanisms are **not black boxes** but **transparent allies** in securing power CPS [176–178].

7. Future Directions and Open Challenges

7.1. Resilience Co-Design with Grid Planning and Market Mechanisms

Most existing cyber defense research treats security as a **runtime feature**, decoupled from long-term **grid planning and market design [179–181]**. However, true resilience requires integrating **security objectives into infrastructure planning, investment strategies, and market operations [182,183]**.

Future work should explore:

- **Co-optimization of security and economic objectives**, ensuring that resilience measures do not undermine market efficiency.
- **Incentive mechanisms** for distributed energy resources and microgrids to **participate in grid-wide cyber defense**, leveraging their local intelligence and control capabilities.
- **Security-aware planning models** that account for the costs and benefits of redundant infrastructure, diverse vendor ecosystems, and modular grid segmentation.

By embedding resilience into the **economic and regulatory fabric** of power systems, operators can move beyond reactive defense toward **proactive, economically justified security investments [184–186]**.

7.2. Adversarial Testing and Red-Teaming Frameworks

Current defense solutions are often validated under **limited, idealized scenarios**. There is a pressing need for **systematic adversarial testing** to evaluate resilience under **realistic, worst-case attack conditions [187–190]**.

Future research should focus on:

- **Red-teaming frameworks**, where expert adversaries simulate advanced cyber-physical attack strategies against defense mechanisms [191].
- **Adversarial AI techniques** to stress-test detection models, revealing blind spots and robustness limits [192–194].
- **Digital twin environments**, providing safe, high-fidelity simulation platforms for end-to-end security validation without risking real-world operations.

Such testing frameworks can **build confidence** in proposed solutions and **accelerate their transition** from academic prototypes to operational deployment [195].

 doi:10.20944/preprints202505.1170.v1

7.3. Benchmarking and Datasets for Realistic Evaluation

The lack of standardized datasets and benchmarking frameworks remains a major bottleneck in advancing power CPS security research [196–198]. Many studies rely on synthetic data or simplified test systems, limiting the generalizability of their findings [199–201].

To address this, the community needs [202–205]:

- **Open, realistic datasets**, including multi-domain (cyber-physical) measurements, labeled attack scenarios, and diverse operating conditions.
- **Standardized evaluation metrics**, enabling fair comparison of detection accuracy, response latency, scalability, and resilience impact.
- **Shared benchmarking platforms**, where researchers can test their methods under **consistent and challenging conditions**.

Collaboration among academia, industry, and government is essential to **curate and maintain these resources**, ensuring **reproducibility and comparability** across studies [206–210].

7.4. Policy, Standardization, and Cross-Sector Collaboration

Technical advancements alone are **insufficient** to secure power CPS [211–213]. **Policy, governance, and cross-sector collaboration** are equally critical [214].

Key priorities include [215–217]:

- **Establishing security standards and compliance frameworks** for power CPS, covering sensing, communication, control, and data management layers.
- **Facilitating information sharing** among utilities, manufacturers, cybersecurity experts, and regulators to accelerate threat intelligence dissemination and best practice adoption.
- **Promoting cross-sector resilience planning**, recognizing that power systems are interdependent with telecommunications, transportation, and other critical infrastructures.

Building a **trusted ecosystem** of stakeholders, supported by **clear policies and standards**, is vital to achieving **systemic, cross-domain resilience** in the face of evolving cyber threats [218].

8. Conclusions

The evolution of power systems into complex cyber-physical systems has unlocked unprecedented operational capabilities but has also exposed the grid to a rapidly expanding range of cyber-physical threats. Among these, false data injection attacks have emerged as particularly stealthy and damaging, capable of undermining grid stability and operator trust.

While substantial progress has been made in **FDIA detection**, this review highlights the urgent need to move **beyond reactive defense** toward a **Resilient-by-Design** paradigm. Such a paradigm reimagines power CPS security as a **system-level, co-designed capability**, embedded across sensing, communication, control, and recovery layers.

Key takeaways from this review include:

- The **evolving threat landscape** now extends beyond classic FDIAs to include coordinated multi-stage, AI-driven, and cross-domain attacks.
- **Security-aware grid architectures**, emphasizing redundancy, diversity, and modularity, form the foundation for systemic resilience.
- **Distributed, real-time defense mechanisms**, leveraging federated learning, multi-agent systems, and edge intelligence, offer scalable and adaptive protection.
- **Data reconstruction and recovery** are essential for maintaining situational awareness and operational continuity after an attack.
- **Autonomy-driven adaptive security**, powered by reinforcement learning, generative modeling, and explainable AI, enhances the system's ability to learn, adapt, and build operator trust.

Looking ahead, achieving practical, large-scale deployment of resilient power CPS requires:

- Integrating resilience objectives into grid planning and market mechanisms.

 doi:10.20944/preprints202505.1170.v1

- Systematic adversarial testing and red-teaming to validate defense strategies under realistic conditions.
- Standardized datasets and benchmarking frameworks to enable reproducibility and comparability of research findings.
- Cross-sector collaboration and policy alignment to foster a trusted, resilient energy ecosystem.

By embracing these directions, the power systems community can transition from a fragmented, detection-centric security posture to a **holistic, proactive, and resilient defense framework**, capable of safeguarding critical infrastructure in an increasingly adversarial cyber-physical landscape.

References

1. Zografopoulos I, Srivastava A, Konstantinou C, et al. Cyber-Physical Interdependence for Power System Operation and Control[J]. IEEE Transactions on Smart Grid, 2025, 16(3): 2554-2573.
2. Khaloopour L, Su Y, Raskob F, et al. Resilience-by-Design in 6G Networks: Literature Review and Novel Enabling Concepts[J]. IEEE access, 2024, 12: 155666-155695.
3. 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, 2025, 12(2): 1343-1367.
4. Liu W, Wang C, Cao Y, et al. A method for generating wind power output scenarios based on improved conditional generative diffusion model[J]. Electric Power Systems Research, 2025, 247: 111779.
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. Manias D M, Saber A M, Radaideh M I, et al. Trends in Smart Grid Cyber-Physical Security: Components, Threats and Solutions[J]. IEEE Access, 2024, 12: 161329-161356.
8. Franzè G, Famularo D, Lucia W, et al. Cyber–physical systems subject to false data injections: A model predictive control framework for resilience operations[J]. Automatica, 2023, 152: 110957.
9. Shang Y, et al. Explainable spatiotemporal multi-task learning for electric vehicle charging demand prediction[J]. Applied Energy, 2025, 384: 125460.
10. Kumar R, Singh C, Raju Y, et al. Schemes and Security Attacks on the Integrity of Cyber-Physical Systems in Energy Systems[J]. Cyber Physical Energy Systems, 2024: 415-444.
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. Li Y, Zhang S, Li Y. AI-enhanced resilience in power systems: Adversarial deep learning for robust short-term voltage stability assessment under cyber-attacks[J]. Chaos, Solitons & Fractals, 2025, 196: 116406.
13. Maleki S, Pan S, Lakshminarayana S, et al. Survey of load-altering attacks against power grids: Attack impact, detection and mitigation[J]. IEEE Open Access Journal of Power and Energy, 2025.
14. 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.
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. Parhamfar M, Zabihi A, Taheri M, et al. Enhancing Cyber Attack Detection in Microgrids for Resilient Energy Networks[J]. Journal of Modern Technology, 2024: 75-86.
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.

 doi:10.20944/preprints202505.1170.v1

20. Wang Z, Xie W, Wang B, et al. A survey on recent advanced research of CPS security[J]. Applied Sciences, 2021, 11(9): 3751.
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. 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.
24. Wang Y F, Qiu J, Li J E. Early Warning Method for Cross-Space Cascading Failures in Power Grid CPS Considering Attack Gain-Loss[J]. China Electric Power, 2020, 53(1): 92-99.
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. Wang Z J, Liu Y, Bao Y Y, et al. Power System Security Simulation Technology: Engineering Security, Cybersecurity and Cyber-Physical Integrated Security[J]. SCIENCE CHINA Technological Sciences, 2017, 60: 1975.
27. Liu Y, Ning P, Reiter M K. False data injection attacks against state estimation in electric power grids[J]. ACM Transactions on Information and System Security (TISSEC), 2011, 14(1): 1-33.
28. Liang Y, Wang Y K, Liu K Y, et al. Cyber-Physical Fault Simulation of Distribution Network CPS Considering Cybersecurity[J]. Power System Technology, 2020, 45(1): 235-242.
29. Luo X Y, He J N, Wang X Y, et al. Topology Optimization of Resilient Defense Strategies Against False Data Injection Attacks in Smart Grids[J]. Acta Automatica Sinica, 2023, 49(6): 1326-1338.
30. Shu H C, Yang Y Y, Zhao H F, 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.
31. Yin H Y, Liu D, Chen G H, et al. Collaborative Cyber Attack Model for Virtual Power Plants and Cross-Space Fault Propagation Mechanism[J]. Automation of Electric Power Systems, 2023, 47(8): 34-43.
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. Zhang S, et al. A critical review of data-driven transient stability assessment of power systems: principles, prospects and challenges[J]. Energies, 2021, 14(21): 7238.
35. Rekeraho A, Cotfas D T, Balan T C, et al. Cybersecurity Threat Modeling for IoT-Integrated Smart Solar Energy Systems: Strengthening Resilience for Global Energy Sustainability[J]. Sustainability, 2025, 17(6): 2386.
36. Li Y, Li Z, Chen L. Dynamic State Estimation of Generators Under Cyber Attacks[J]. IEEE Access, 2019, 7: 125252-125267.
37. Zhou T, Xiahou K, Zhang L L, et al. Real-time detection of cyber-physical false data injection attacks on power systems[J]. IEEE Transactions on Industrial Informatics, 2020, 17(10): 6810-6819.
38. Standen M, Kim J, Szabo C. Adversarial Machine Learning Attacks and Defences in Multi-Agent Reinforcement Learning[J]. ACM Computing Surveys, 2025, 57(5): 1-35.
39. Deng S, Cai Q Y, Gao K L, et al. Data Security Risk Identification Algorithm for Energy Cyber-Physical Systems Based on Function Mining[J]. China Electric Power, 2021, 54(3): 23-30, 37.
40. Xie Y Y, Yan X T, Yan Z A, et al. Optimization of False Data Injection Attack Strategies for Hybrid AC/DC Power Grids[J]. Electric Power Engineering Technology, 2023, 42(4).
41. 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.
42. Jafari M, Rahman M A, Paudyal S. Optimal false data injection attack against load-frequency control in power systems[J]. IEEE Transactions on Information Forensics and Security, 2023, 18: 5200-5212.

43. 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.
44. 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.
45. Liu T, Tian J, Wang J Z, et al. Comprehensive Security Threats and Defenses for Cyber-Physical Systems[J]. Acta Automatica Sinica, 2019, 45(1): 5-24.
46. Dong Y, et al. Identification of False Data Injection Attacks in Power Grid Based on Oversampling and Cascade Machine Learning[J]. Power System Automation, 2023, 47(8): 179-188.
47. Liang H L, Liu D Q, Zeng X J, et al. Construction of Loss Path Map and Risk Assessment for Cyber Attacks on Power Advanced Metering Infrastructure[J]. Automation of Electric Power Systems, 2024, 48(12): 89-99.
48. He Z L, Gao S B, Wei X G, et al. Game-Theoretic Model for False Topology Attacks with Collaborative Branch and Protection Tampering in Power Systems[J]. Power System Technology, 2022, 46(11): 4346-4355.
49. Zhu J, Huang L, Chen Y. Post-Attack Security Control Strategy for Power Systems Based on Agent Gradient Deep Reinforcement Learning[J]. Power Grid Technology, 2024, 48(10): 4041-4049.
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. Pang Q L, Han S Y, Zhou T, et al. Detection of False Data Injection Attacks in Cyber-Physical Power Systems Based on ASRUKF and IMC Algorithms[J]. Smart Power, 2024, 52(7): 111-118.
52. 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.
53. Gong L, Wang X, Tian M, et al. Concept and Advancement of Resilience in Power Cyber-Physical Systems[J]. Power System Protection and Control, 2023, 51(14): 169-187.
54. Liu K, Ma S, Ma O, et al. Security Control of Cyber-Physical Systems Based on Machine Learning[J]. Acta Automatica Sinica, 2021, 47(6): 1273-1283.
55. 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.
56. 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.
57. Li Y, Zhang S, 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: 1-11.
58. 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 Grid Technology, 2024, 49(3): 1246-1256.
59. Yang T, Xu Z M, Zhao Y J, et al. Review of Attack and Defense Methods for Digitalized New Power Systems[J]. Automation of Electric Power Systems, 2024, 48(6): 112-126.
60. Wang S, Zhao Y, You D, et al. A Survey on Cyber-Physical Systems Attacks in the Framework of Discrete Event Systems[J]. Control and Decision, 2022, 37(8): 1934-1944.
61. Yin H, Liu D, Chen G, et al. Collaborative Network Attack Model and Cross-Space Fault Propagation Mechanism for Virtual Power Plants[J]. Power System Automation, 2023, 47(8): 34-43.
62. Luo X, Pan X, Wang X, et al. False Data Injection Attack Detection in Smart Grids Based on Adaptive Kalman Filtering[J]. Acta Automatica Sinica, 2022, 48(12): 2960-2971.
63. Du L, Sha J X, Fan B, et al. Electricity Theft Detection Method for Distribution Network CPS Based on Cyber-Physical Bilateral Data[J]. Integrated Intelligent Energy, 2024, 46(5):112-120..
64. 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.
65. Zhang L, Xu Y, Wu X, et al. Distributed Resilient Control for AC Microgrids to Defend Against False Data Injection Attacks[J]. Power System Automation, 2023, 47(8): 44-52.
66. Wang W, Ren Z, Sun Y, et al. Transmission Grid False Data Detection Method Based on Wavelet-Sparse Autoencoders[J]. Electric Power New Technologies, 2022, 41(1): 51-59.

 doi:10.20944/preprints202505.1170.v1

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. Yang J, Guo Y H, Guo C X, et al. Review of Dynamic Security Protection for Cyber-Physical Power Systems Considering Dual-Driven Models and Data[J]. Power System Protection and Control, 2022, 50(7): 176-187.
69. Cyber Physical Energy Systems[M]. John Wiley & Sons, 2024.
70. Dong Y C, Wang Q M, Cao J, et al. Identification of False Data Injection Attacks in Power Grids Based on Oversampling and Cascaded Machine Learning[J]. Automation of Electric Power Systems, 2023, 47(8): 179-188.
71. Luo X, Pan X, Wang X, et al. False Data Injection Attack Detection in Smart Grids Based on Adaptive Kalman Filtering[J]. Acta Automatica Sinica, 2022, 48(12): 2960-2971.
72. 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.
73. Zhang L, Xu Y, Wu X, et al. Distributed Resilient Control for AC Microgrids to Defend Against False Data Injection Attacks[J]. Power System Automation, 2023, 47(8): 44-52.
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. Zhang D F, Duan H B. Secure State Estimation Based on Distributed Sparse Optimization Under Malicious Attacks[J]. Acta Automatica Sinica, 2021, 47(4): 813-824.
76. Luo X Y, Pan X Y, Wang X Y, et al. Detection of False Data Injection Attacks in Smart Grids Based on Adaptive Kalman Filtering[J]. Acta Automatica Sinica, 2022, 48(12): 2960-2971.
77. 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.
78. Chen L, Liu D. Detection Methods for False Data Injection Attacks in Interactive Demand Response[J]. Power System Automation, 2021, 45(3): 15-23.
79. Kou L, Wu J, Zhang F, et al. Image encryption for Offshore wind power based on 2D-LCLM and Zhou Yi Eight Trigrams[J]. International Journal of Bio-Inspired Computation, 2023, 22(1): 53-64.
80. Zhu J, Zhang G X, Wang T, et al. Review of Fraudulent Data Attacks and Defenses in Power System State Estimation[J]. Power System Technology, 2016, 40(8): 2406-2415.
81. Wang Q, Tai W, Tang Y, et al. A Review of False Data Injection Attacks for Power Cyber-Physical Systems[J]. Acta Automatica Sinica, 2019, 45(1): 72-83.
82. Zhu J Z, Huang L Y, Chen Y X. Post-Attack Security Control Strategy for Cyber Attacks in Power Systems Based on Proxy Gradient Deep Reinforcement Learning[J]. Power System Technology, 2024, 48(10): 4041-4049.
83. Gallardo C, Burgos-Mellado C, Muñoz-Carpintero D, et al. Reinforcement learning-based false data injection attacks detector for modular multilevel converters[J]. IEEE Transactions on Industrial Electronics, 2023, 71(7): 7927-7937.
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. Wang Y F, Li J E, Liu Y L, et al. Cascading Failure Early Warning Method Induced by Tolerated Phased Faults in Coordinated Cyber Attacks on Power Grids[J]. Automation of Electric Power Systems, 2021, 45(3): 24-32.
87. Lu J, Yang C, Du R, et al. False Data Injection Attacks in Power CPS[J]. Intelligent Computer and Applications, 2022, 12(6): 121-126.
88. Yang Y, Guo L, Wang H, et al. Fast Defense Strategy Against False Data Injection Attacks in DC Microgrids Based on Data-Driven Approaches[J]. Electric Power Automation Equipment, 2021, 41(5): 102-110.

 doi:10.20944/preprints202505.1170.v1

89. Guo F, Zheng X, Deng C, et al. Detection and System Recovery Methods for Unbounded False Data Injection Network Attacks in DC Microgrids[J]. Power System Automation, 2023, 47(2): 146-153.
90. Al-Matari N Y, Zahary A T, A. Al-Shargabi A. A survey on advancements in blockchain-enabled spectrum access security for 6G cognitive radio IoT networks[J]. Scientific Reports, 2024, 14(1): 30990.
91. Yang R, et al. Resilience assessment and improvement for electric power transmission systems against typhoon disasters: a data-model hybrid driven approach[J]. Energy Reports, 2022, 8: 10923-10936.
92. Gao Q, Du Z Y, Ji Y H, et al. Resilient Load Frequency Control for Interconnected Multi-Area Power Systems Under Denial-of-Service Attacks[J]. Electric Power Construction, 2023, 44(4): 54-62.
93. Chen L, Li Y, Cai J, et al. SCKF-LSTM-Based Trajectory Tracking for Electricity–Gas Integrated Energy System[J]. IEEE Transactions on Industrial Informatics, 2025. DOI: 10.1109/TII.2024.3523544
94. 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.
95. Cui Y, Xu 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.
96. He S, Zhou Y, Yang Y, et al. Cascading Failure in Cyber–Physical Systems: A Review on Failure Modeling and Vulnerability Analysis[J]. IEEE Transactions on Cybernetics, 2024, 54(2): 7936 - 7954 .
97. Liang G, Weller S, Zhao J, et al. A Framework for Cyber-Topology Attacks: Line-Switching and New Attack Scenarios[J]. IEEE Transactions on Smart Grid, 2019, 10(2): 1704-1712.
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. Cai X P, Wang Q, Huang J Y, et al. Cyber-Physical Bi-Layer Cooperative Emergency Control Method for Cyber Attacks in Power Systems[J]. Global Energy Interconnection, 2020, 3(6): 560-568.
100. Wei L, Zhang Q. False Data Injection Attack Detection in Smart Grids Based on Improved UKF[J]. Journal of System Simulation, 2023, 35(7): 1508.
101. 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.
102. Le J, Lang H, Tan T, et al. A Review of Information Security Issues in Distributed Economic Dispatch of New Distribution Systems[J]. Power System Automation, 2024, 48(12): 177-191.
103. Yu S, Zhou X, Shen X C, et al. Risk Assessment of Source-Grid-Load-Storage Systems Considering Impacts of Cyber Attacks[J]. Integrated Intelligent Energy, 2024, 46(5).
104. Zhang Y, Li S, Gu X, et al. Resilience Assessment Method for Backbone Network Considering Malicious Physical Attacks and Secondary Faults[J]. Electric Power Construction, 2023, 44(12): 95-105.
105. Chen J, Rao J, Li W, et al. Detection Method of False Data Injection Attacks on Power Grids Based on Vector Auto-Regression Model[J]. Journal of Electric Power Science and Technology, 2024, 39(3): 1-9.
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. Wang D, Huang L, Liu J, et al. Defense Strategy for Power Cyber-Physical Systems Against Load False Data Injection Attacks[J]. Power System Protection and Control, 2019, 47(1): 28-34.
108. Shi Z, et al. Short-term load forecasting based on LS-SVM optimized by bacterial colony chemotaxis algorithm[C]//2009 international conference on information and multimedia technology. IEEE, 2009: 306-309.
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. Sun K, Qiu W, Li K, et al. Network Attack Defense Control Strategy for Fast Frequency Response Systems[J]. Chinese Journal of Electrical Engineering, 2021, 41(16): 5476-5485.
111. Zhang J J, Wu J Y, Qi X J, et al. Cascading Failure Analysis and Risk Assessment of CPPS Based on Cyber-Physical Interdependencies[J]. Power System Protection and Control, 2023, 51(5): 164-171.
112. Syrmakesis A D, Alhelou H H, Hatziargyriou N D. A novel cyberattack-resilient frequency control method for interconnected power systems using SMO-based attack estimation[J]. IEEE Transactions on Power Systems, 2023, 39(4): 5672-5686.

 doi:10.20944/preprints202505.1170.v1

113. Zhang M, Li J, Li Y, et al. Deep learning for short-term voltage stability assessment of power systems[J]. IEEE Access, 2021, 9: 29711-29718.
114. 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.
115. 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.
116. 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.
117. Li Y, Li G, Gu X, et al. Transient stability assessment of power systems based on ensemble OS-ELM[J]. Transactions of China Electrotechnical Society, 2015, 30(14): 412-418.
118. Sui Q, Lin X N, Wei F R, et al. A Novel Scheduling Strategy for Smart Microgrids Considering Cyber Attack Risks[J]. Proceedings of the CSEE, 2021, 41(15): 5179-5188.
119. Lian X L, Zhang W H, Qian T, et al. Vulnerability Assessment Method for Cyber-Physical Power Systems Considering Information Node Failures[J]. Journal of Global Energy Interconnection, 2019, 2(6).
120. Sandoval C J K. Cybersecurity Paradigm Shift: The Risks of Net Neutrality Repeal to Energy Reliability, Public Safety, and Climate Change Solutions[J]. San Diego J. Climate & Energy L., 2018, 10: 91.
121. Parizad A, Baghaee H R, Rahman S. Overview of Smart Cyber-Physical Power Systems: Fundamentals, Challenges, and Solutions[J]. Smart Cyber-Physical Power Systems: Fundamental Concepts, Challenges, and Solutions, 2025, 1: 1-69.
122. Yang S, Tan B, Guo J. False Data Injection Attack Detection for New Energy Internet Based on Double Markov Chains[J]. Electric Power Automation Equipment, 2021, 41(2): 212-220.
123. Dongmei H, Zhonghui D, Anduo H, et al. Low-Cost Adversarial Stealthy False Data Injection Attack and Detection Method[J]. Power System Technology, 2023, 47(4): 1531-1539.
124. Meera V M, Arjun K P. Challenges in Ensuring Security for Smart Energy Management Systems Based on CPS[J]. Cyber Physical Energy Systems, 2024: 217-254.
125. Li P, Liu Y, Xin H, et al. Vulnerability Assessment of Distribution Network Cyber-Physical Systems Under Distributed Collaborative Control Mode[J]. Automation of Electric Power Systems, 2018, 42(10): 22-29+59.
126. Li X, Li W T, Du D J, et al. Dynamic State Estimation in Smart Grids Under Denial-of-Service Attacks Based on UKF[J]. Acta Automatica Sinica, 2019, 45(1): 120-131.
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. Tang Z, Zeng C, Zeng Y. Research on data security in industry 4.0 manufacturing industry against the background of privacy protection challenges[J]. International Journal of Computer Integrated Manufacturing, 2025: 1-13..
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. Feng C, Li Y, Xu T. Security Evaluation Method for Distribution Network Cyber-Physical Systems Considering Risk Propagation and Expected Failure Analysis[J]. Science & Technology and Engineering, 2022, 22(23): 1011-10122.
133. Arafah M, Phillips I, Adnane A, et al. Anomaly-based network intrusion detection using denoising autoencoder and Wasserstein GAN synthetic attacks[J]. Applied Soft Computing, 2025, 168: 112455.
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.

 doi:10.20944/preprints202505.1170.v1

136. Taher M A, Behnamfar M, Sarwat A I, et al. False data injection attack detection and mitigation using non-linear autoregressive exogenous input-based observers in distributed control for dc microgrid[J]. IEEE Open Journal of the Industrial Electronics Society, 2024.
137. 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.
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. Seid E, Popov O, Blix F. Towards Security Attack Event Monitoring for Cyber Physical-Systems[C]//ICISSP. 2023: 722-732.
140. Alijoyo F A, Kaur C, Anjum A, et al. Enhancing Cyber-Physical Systems Resilience: Adaptive Self-Healing Security Using Long Short-Term Memory Networks[C]//2024 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI). IEEE, 2024: 1-8.
141. Yang Q, Yang J, Ma X. Research on False Data Injection Attacks in Power Systems[J]. Microelectronics & Computer, 2011, 28(12): 175-179.
142. Wang S, Zhao Y, You D, et al. A Survey on Cyber-Physical Systems Attacks in the Framework of Discrete Event Systems[J]. Control and Decision, 2022, 37(8): 1934-1944.
143. Unsal D B, Ustun T S, Hussain S M S, et al. Enhancing Cybersecurity in Smart Grids: False Data Injection and Its Mitigation. Energies 2021, 14, 2657.
144. Cai X, Wang Q, Tai W, et al. Defense Method for False Data Injection Attacks in Power CPS Based on Multi-Stage Game[J]. Electric Power Construction, 2019, (5): 48-54.
145. Zhang Y, Li S, Gu X, et al. Resilience Assessment Method for Backbone Network Considering Malicious Physical Attacks and Secondary Faults[J]. Electric Power Construction, 2023, 44(12): 95-105.
146. Khater H M, Sallabi F, Serhani M A, et al. Empowering Healthcare with Cyber-Physical System–A Systematic Literature Review[J]. IEEE Access, 2024.
147. Wang D, Huang L, Liu J, et al. Defense Strategy for Power Cyber-Physical Systems Against Load False Data Injection Attacks[J]. Power System Protection and Control, 2019, 47(1): 28-34.
148. Sun K, Qiu W, Li K, et al. Network Attack Defense Control Strategy for Fast Frequency Response Systems[J]. Chinese Journal of Electrical Engineering, 2021, 41(16): 5476-5485.
149. Thirupathi L, Bandari M, Sreeramamurthy K, et al. Cyber-Physical Systems Security and Quantum Computing Applications in Disaster Recovery for Industry 6.0[M]//The Rise of Quantum Computing in Industry 6.0 Towards Sustainability. Springer, Cham, 2024: 221-235.
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. Dai J, Dai Z, Thing V L L, et al. Cyber-Resilience Enhancement with Cross-Domain Software-Defined Network for Cyber-Physical Microgrids against Denial of Service Attacks[J]. IEEE Transactions on Industrial Cyber-Physical Systems, 2025.
152. Liu Y, Lu Y. Event-Triggered Sliding Mode Control of Direct-Current Microgrid System Under Network Attack[J]. Journal of Electric Power Science and Technology, 2025, 39(6): 212-221.
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. Wang Y, Fu J. Computational Intelligence in Smart Cities and Smart Energy Systems[M]//Cutting Edge Applications of Computational Intelligence Tools and Techniques. Cham: Springer Nature Switzerland, 2023: 305-325.
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. Feng Y, Jia W. Research Status and Prospect of Smart Microgrids Under Network Attack Models[J]. Smart Grid, 2022, 12: 119-125.
157. Zhang P, Xiong Y, Jian J. Research on False Data Injection Attacks in Smart Grids Based on Multi-Objective Bi-Level Programming[J]. Operations Research and Management, 2023, 32(1): 22.

 doi:10.20944/preprints202505.1170.v1

158. Yuan K, Luo P, Wang G, et al. New Detection Method for Covert Data Attacks in Power Systems Based on Grey Relational Analysis[J]. New Electrical Technology, 2019, 38(1): 17-23.
159. Siddique K. A game theoretic framework to secure cyber physical systems (CPS) against cyber attacks[J]. 2018.
160. Gallardo C, Burgos-Mellado C, Muñoz-Carpintero D, et al. Reinforcement learning-based false data injection attacks detector for modular multilevel converters[J]. IEEE Transactions on Industrial Electronics, 2023, 71(7): 7927-7937.
161. Bo X, Qu Z, Wang L, et al. Active defense research against false data injection attacks of power CPS based on data-driven algorithms[J]. Energies, 2022, 15(19): 7432.
162. Wu Y, Ru Y, Liu J, et al. Detection of False Data Injection Attacks in Automatic Generation Control Systems Based on Set Member Filtering[J]. Power System Automation, 2022, 46(1): 33-41.
163. Li Y, Li Y, Sun Y. Online Static Security Assessment Of Power Systems Based On Lasso Algorithm[J]. Applied Sciences, 2018, 8(9): 1442.
164. Amin R. Cyber attack detection and mitigation in smart power systems[D]. Macquarie University, 2021.
165. Feng C, Li Y, Xu T. Security Evaluation Method for Distribution Network Cyber-Physical Systems Considering Risk Propagation and Expected Failure Analysis[J]. Science & Technology and Engineering, 2022, 22(23): 10116-10122.
166. Pruengkarn R. Enhancing classification performance by handling noise and imbalanced data with fuzzy classification techniques[D]. Perth, Australia: Murdoch University, 2018.
167. Zhou H, Xu F, Liu X, et al. A Machine Learning Approach for False Data Injection Attack Detection in Power Systems[J]. Journal of Power Systems, 2024, 45(7): 1254-1264.
168. Golpîra H, Francois B. Artificial intelligence-based approach for islanding detection in cyber-physical power systems[J]. Chaos, Solitons & Fractals, 2024, 185: 115165.
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. 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.
171. Alomari M A, Al-Andoli M N, Ghaleb M, et al. Security of Smart Grid: Cybersecurity Issues, Potential Cyberattacks, Major Incidents, and Future Directions[J]. Energies, 2025, 18(1): 141.
172. Li X, Wang X, Liu G, et al. Comprehensive Evaluation of False Data Injection Attacks in Power Systems Using a Data-Driven Approach[J]. IEEE Transactions on Industrial Informatics, 2023, 19(4): 2345-2353.
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. Agnew D, Boamah S, Bretas A, et al. Network security challenges and countermeasures for software-defined smart grids: A survey[J]. Smart cities, 2024, 7(4): 2131-2181.
177. Lazaridis G, Drosou A, Chatzimisios P, et al. Unraveling the Threat Landscape of CPS: Modbus TCP Vulnerabilities in the Era of I4. 0[C]//2024 IEEE International Conference on Cyber Security and Resilience (CSR). IEEE, 2024: 593-598.
178. 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.
179. Zhang W, Liang J, Wu T. Survey of Attack Detection and Defense Methods for Smart Grids[J]. Journal of Control and Decision, 2023, 38(10): 2567-2575.
180. Karangelos E, Wehenkel L. Cyber–physical risk modeling with imperfect cyber-attackers[J]. Electric Power Systems Research, 2022, 211: 108437.

 doi:10.20944/preprints202505.1170.v1

181. Lin W T, Chen G, Zhou X. Privacy-preserving federated learning for detecting false data injection attacks on power system[J]. Electric Power Systems Research, 2024, 229: 110150.
182. Xu S, Lu Y, Wu F. Cyber-Attack Detection and Resilience Strategy in Smart Grids Based on Big Data Analytics[J]. Power System Automation, 2023, 47(12): 1859-1871.
183. Fang Y, Liu Z, Chen D. Hybrid Machine Learning Methods for Cyber-Attack Detection in Power Systems[J]. Journal of Energy Engineering, 2024, 10(2): 134-145.
184. 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.
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. Tabish N, Chaur-Luh T. Maritime autonomous surface ships: A review of cybersecurity challenges, countermeasures, and future perspectives[J]. IEEE Access, 2024, 12: 17114-17136.
187. Bhattacharjee A, Bai G, Tushar W, et al. Deebbaa: A benchmark deep black box adversarial attack against cyber-physical power systems[J]. IEEE Internet of Things Journal, 2024.
188. Bai Z, Chen Y, Wei L, et al. Application of AI and ML Techniques in Cybersecurity of Power CPS[J]. Power and Energy Systems, 2024, 46(5): 2267-2278.
189. 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.
190. Li B, Lu R, Bao H. Behavior rule specification-based false data injection detection technique for smart grid[J]. Cyber Security for Industrial Control Systems: From the Viewpoint of Close-Loop, 2016: 119-150.
191. Gao S, Zhang H, Wang Z, et al. Data-driven injection attack strategy for linear cyber-physical systems: An input-output data-based approach[J]. IEEE Transactions on Network Science and Engineering, 2023, 10(6): 4082-4095.
192. Wang G, Sun Q, et al. Detection and Mitigation of Coordinated False Data Injection Attacks in Power Grids[J]. Journal of Control Engineering Practice, 2024, 25(7): 347-359.
193. Amissah J, Abdel-Rahim O, Mansour D E A, et al. Developing a three stage coordinated approach to enhance efficiency and reliability of virtual power plants[J]. Scientific Reports, 2024, 14(1): 13105.
194. Honarvar E, Daeichian A, Priscoli F D, et al. A PCA-based algorithm for online false data injection and jamming attacks detection in cyber-physical systems[J]. Transactions of the Institute of Measurement and Control, 2024: 01423312241273857.
195. 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.
196. Bindra S S, Aggarwal A. Deep Learning-based Enhanced Security in Cyber-Physical Systems: A Multi-Attack Perspective[C]//2024 International Conference on Computational Intelligence and Computing Applications (ICCICA). IEEE, 2024, 1: 347-352.
197. Esmalifalak M, Nguyen H, Zheng R, et al. A Stealthy Attack Against Electricity Market Using Independent Component Analysis[J]. IEEE Systems Journal, 2018, 12(1): 297-307.
198. Li W, Fu H, Wu S, et al. RETRACTED: A Kalman Filter-Based Distributed Cyber-Attack Mitigation Strategy for Distributed Generator Units in Meshed DC Microgrids[J]. Energies, 2023, 16(24): 7959
199. Li R, Liu S, Yan L. CPS Network Attack Detection Method for New Energy Distribution Networks Based on FP-Growth Algorithm[J]. Telecommunications Science, 2024, 40(11): 103-113.
200. Patel N A, Parekh D A, Shah Y A, et al. 4s framework: A practical cps design security assessment & benchmarking framework[J]. Cyber Security and Digital Forensics, 2022: 163-204.
201. Ezechi C, Akinsolu M O, Sangodoyin A O, et al. Software-defined networking in cyber-physical systems[J]. Cyber Physical System 2.0: Communication and Computational Technologies, 2024: 44.
202. Sugunaraj N, Balaji S R A, Chandar B S, et al. Distributed Energy Resource Management System (DERMS) Cybersecurity Scenarios, Trends, and Potential Technologies: A Review[J]. IEEE Communications Surveys & Tutorials, 2025.
203. Du Y, Chatterjee S, Bhattacharya A, et al. Role of reinforcement learning for risk-based robust control of cyber-physical energy systems[J]. Risk Analysis, 2023, 43(11): 2280-2297.

204. Benouachane H. Cyber Security Challenges in the Era of Artificial Intelligence and Autonomous Weapons[M]//Cyber Security in the Age of Artificial Intelligence and Autonomous Weapons. CRC Press, 2025: 24-42.
205. Saheed Y K, Chukwuere J E. CPS-IIoT-P2Attention: Explainable Privacy-Preserving with Scaled Dot-Product Attention in Cyber Physical System-Industrial IoT Network[J]. IEEE Access, 2025.
206. Rayabagi S T, Jena P K, Ghosh S. Design of False Data Injection Attack for Automatic Generation Control[C]//2020 IEEE First International Conference on Smart Technologies for Power, Energy and Control (STPEC). IEEE, 2020: 1-5.
207. Halabi T, Haque I, Karimipour H. Adaptive Control for Security and Resilience of Networked Cyber-Physical Systems: Where Are We?[C]//2022 IEEE 4th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA). IEEE, 2022: 239-247.
208. 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
209. Liu F, Li Y, Li B, et al. Bitcoin transaction strategy construction based on deep reinforcement learning[J]. Applied Soft Computing, 2021, 113: 107952.
210. Yen S J. Defense Strategies Against False Data Injection Attacks in the Smart Grid[D]. National University of Singapore (Singapore), 2022.
211. Ghosh S, Zaboli A, Hong J, et al. A Physics-Based Context-Aware Approach for Anomaly Detection in Teleoperated Driving Operations Under False Data Injection Attacks[J]. arXiv preprint arXiv:2410.13962, 2024.
212. Jin Z W, Liu Y, Diao J D, et al. Stealthy False Data Injection Attacks Against Remote State Estimation in Cyber-Physical Systems[J]. Acta Automatica Sinica, 2025, 51(2): 1-10.
213. Saeed S, Gull H, Aldossary M M, et al. Digital Transformation in Energy Sector: Cybersecurity Challenges and Implications[J]. Information, 2024, 15(12): 764.
214. Qian C, Guo Y, Hussaini A, et al. A new layer structure of cyber-physical systems under the era of digital twin[J]. ACM Transactions on Internet Technology, 2024.
215. Abshari D, Sridhar M. A survey of anomaly detection in cyber-physical systems[J]. arXiv preprint arXiv:2502.13256, 2025.
216. Nguyen T T, Reddi V J. Deep reinforcement learning for cyber security[J]. IEEE Transactions on Neural Networks and Learning Systems, 2021, 34(8): 3779-3795.
217. Tan Z, Li Z. Digital twins for sustainable design and management of smart city buildings and municipal infrastructure[J]. Sustainable Energy Technologies and Assessments, 2024, 64: 103682.
218. Atıcı S, Tuna G. Impact of cybersecurity attacks on electrical system operation[M]//Cyber Security Solutions for Protecting and Building the Future Smart Grid. Elsevier, 2025: 117-160.