Advances in Cross-Source Intelligent Security Monitoring and Resilience Strategies for Urban Cyber-Physical Power Systems: A Comprehensive Review

Beike Gao[1]

(1. Academy Europe, Hamburg, Germany 29314)

ABSTRACT he rapid integration of cyber-physical systems (CPS) into power grids has transformed traditional electricity networks into cyber-physical power systems (CPPS), enhancing efficiency but introducing profound cybersecurity vulnerabilities. Coordinated cyber-physical attacks, cascading failures, and information asymmetry exacerbate risks, as evidenced by incidents like the 2019 Venezuela blackout and disruptions during the Russia-Ukraine conflict [3]. This review synthesizes advancements in cross-source intelligent security monitoring and analysis for power systems, focusing on urban CPPS models. Key technologies examined include multi-source log data aggregation for topology modeling [1], anomaly detection via self-supervised contrastive learning for missing node identification, tri-level optimization defenses against coordinated attacks [21], and vulnerability assessments using spectral metrics [27]. We further discuss fault recovery strategies incorporating information delay models and graph convolutional networks (GCN) for optimal repair paths [14]. Innovations such as multi-functional module integration (monitoring, powering, control) and asymmetric topology-aware attacks address gaps in high-security urban cores. By evaluating resilience metrics like load loss rates and islanding efficacy [35], this paper highlights pathways to enhance grid robustness, reduce outage costs, and support smart grid evolution. Future directions emphasize scalable AI-driven platforms for real-time threat mitigation, offering a comprehensive framework for researchers and engineers to bolster CPPS resilience.

Keywords Cyber-Physical Power Systems (CPPS), Network Security, Vulnerability Assessment, Fault Recovery, Intelligent Monitoring.

I. Introduction

1.1 Background and Significance

The electrification of modern societies hinges on the reliability of power systems, which have evolved from isolated physical infrastructures to deeply intertwined cyber-physical power systems (CPPS). This fusion, driven by advancements in information and communication technologies (ICT), enables precise sensing, automated control, and efficient energy distribution [1]. However, the bidirectional dependencies between cyber (information) and physical (power) layers introduce cascading vulnerabilities: a cyber intrusion can propagate to physical disruptions, and vice versa, amplifying outage risks in urban settings [2]. High-profile incidents underscore this peril; for instance, the 2019 Venezuela blackout, triggered by malware and electromagnetic sabotage, left millions without power for days [3], while cyber operations in the Russia-Ukraine war caused widespread urban blackouts affecting tens of thousands [3]. In China, the push toward "informatization driving industrialization" since the 1990s has accelerated CPPS adoption in urban grids, yet it heightens exposure to coordinated attacks, natural disasters, and supply chain threats [9].

Urban CPPS, particularly in central business districts (CBDs) and airports, exhibit unique complexities: heterogeneous multi-layer networks, high-stakes dependencies on critical infrastructure, and stringent protection levels [10]. Traditional reliability analyses, focused on probabilistic low-impact events, fall short against deliberate high-impact assaults [28]. Resilience engineering—emphasizing connectivity retention and rapid recovery—emerges as imperative [13]. This review addresses these challenges by surveying cross-source intelligent monitoring technologies, from log aggregation to AI-enhanced defenses, aiming to quantify vulnerabilities, predict cascades, and optimize recoveries. By bridging

theoretical models with practical platforms, it supports China's smart grid ambitions, potentially averting economic losses exceeding billions in downtime [38].

1.2 Evolution of CPPS Security Research

Early CPPS modeling relied on reductionist approaches, dissecting cyber and physical layers via tools like EPOCHS for detailed simulations [5,6]. Physics-informed models abstracted energy flows [7] and information processing [8], while complex network theory introduced interdependent frameworks, such as Buldyrev's catastrophic cascade model [10]. Subsequent variants—partial [11], unidirectional [12], and asymmetric couplings [14]—captured urban dynamics but overlooked multi-functional modules (e.g., monitoring via PMUs, powering via UPS) [9].

Attack methodologies have matured from single-vector exploits (e.g., replay [16], DoS [20]) to hybrid cyber-physical assaults [22,23]. Critical node identification blends topology metrics (e.g., dependency matrices [24]) with operational states (e.g., voltage offsets [30]), yet struggles with information asymmetry [33]. Resilience assessments leverage spectral clustering for islanding [37] and Q-learning for attack sequencing [42], revealing that cyber failures can double physical load losses [36]. Recovery strategies, often siloed to physical grids [38–41], increasingly incorporate cyber-physical synergies, like dual-layer island partitioning [42] and GCN-optimized paths [14].

Despite progress, gaps persist: urban models undervalue functional heterogeneity [4]; attacks neglect high-security zones [21]; and recoveries ignore delay-induced interactions [43,44]. This review fills these voids by integrating multi-source analytics and self-supervised learning, drawing on 44 seminal works [1–44].

1.3 Contributions and Structure

This paper contributes a unified taxonomy of CPPS security technologies, emphasizing urban applicability. It innovates by proposing a resilience evaluation framework fusing spectral vulnerabilities with GCN-driven recoveries, validated via IEEE benchmarks [21]. Section 2 details modeling and assessment; Section 3 explores attack and defense strategies; Section 4 covers recovery mechanisms; Section 5 discusses platforms and future trends; and Section 6 concludes.

II. Modeling and Assessment of Urban CPPS

The foundational step in enhancing the resilience of urban cyber-physical power systems (CPPS) lies in accurate modeling, which captures the intricate interdependencies between cyber and physical layers. Urban CPPS, characterized by dense, heterogeneous networks in areas like central business districts (CBDs) and airports, demand models that integrate multi-functional modules—such as monitoring via phasor measurement units (PMUs), powering through uninterruptible power supplies (UPS), and control via automatic generation control inter-control center communications (AGC-ICBs)—while accounting for real-world dynamics like geographic constraints and log data heterogeneity [9]. This section reviews modeling paradigms and resilience assessment frameworks, highlighting advancements in multi-source data aggregation and spectral vulnerability metrics.

2.1 Paradigms in CPPS Modeling

CPPS modeling has evolved from siloed representations to interdependent frameworks, addressing the limitations of traditional power system analyses that overlook cyber influences [1]. Three primary paradigms dominate: reductionist, physics-based, and complex network theory.

Reductionist approaches emphasize detailed layer-wise simulations. For instance, Xu et al. [4] proposed a refined modeling method that separates cyber and physical networks to preserve internal details, while Hranisavljevic et al. [5] and Chen et al. [6] leveraged joint simulation tools like EPOCHS and GECO for hybrid CPPS analysis. These methods excel in granularity but suffer from computational complexity, rendering them less scalable for urban scenarios with thousands of nodes.

Physics-based models abstract core processes into mathematical expressions. Li et al. [7] focused on energy flow computations, Elma et al. [8] on bidirectional vehicle-to-grid (V2G) information flows, and Sheng et al. [9] integrated socio-physical perspectives for power-traffic couplings. Such models capture fault-state linkages effectively but exhibit poor extensibility, often neglecting dynamic cyber interactions like latency-induced delays.

Complex network theory has gained prominence for its ability to model interdependencies. Buldyrev et al. [10] pioneered the interdependent network model, applied to Italy's grid, revealing catastrophic cascades from single failures. Extensions include partial couplings [11], unidirectional dependencies [12], weak interdependencies [13], and asymmetric models [14], which better reflect urban asymmetries (e.g., one-way information flows from control centers). However, these often ignore physical attributes, limiting applicability to operational control [24].

A unified framework remains elusive: reductionist models are precise yet brittle, physics-based ones dynamic but inflexible, and network-theoretic ones scalable but abstracted [4–14]. Urban CPPS modeling must bridge these by incorporating 5G/IoT-enabled expansions, emphasizing equipment states (e.g., monitoring, control) alongside topology [2].

2.2 Multi-Functional Urban CPPS Models

To address urban heterogeneities, recent models integrate multi-functional modules into layered architectures. Grounded in urban planning norms (e.g., road-aligned power/communication lines), these construct topologies from geographic data, as illustrated in CBD and airport ring networks.

A prototypical urban CPPS framework comprises three layers: physical (power nodes/lines), cyber (information nodes/links), and coupling (functional interlinks) [9,12]. Power layers model nodes (generators,

substations, loads) and edges (transmission lines) via adjacency matrices:

Ap=[aijp],aijp={1if line connects i and j0otherwise

Cyber layers follow similarly. Coupling is captured by an association matrix M encoding functions:

M=[MsMmMc]

where Ms denotes supplying (power to cyber), Mmmonitoring (PMU/adjacent states), and Mccontrol (to generators/loads). Information flow viability depends on supply and link states, enabling simulations of functional failures.

This multi-functional approach enhances fidelity: e.g., UPS ensures short-term cyber uptime during power outages, while PMUs enable real-time state estimation [8]. Evaluations via Monte Carlo sampling of fault states accelerate convergence in multi-state spaces, yielding performance curves for resilience metrics like connectivity retention [13].

2.3 Multi-Source Log Aggregation for Topology Inference

Urban CPPS topologies are inferred from heterogeneous logs (e.g., SCADA, PMU, communication traces) via aggregation techniques. Analysis of CBD/airport logs reconstructs networks by fusing spatial data (roads, coordinates) with temporal logs, optimizing node interactions via association matrices [1,24].

Complex network metrics—degree distributions, clustering coefficients—refine intra-layer topologies, while cross-layer analysis quantifies dependencies (e.g., cyber latency impacting power flows) [10]. Self-supervised methods, like graph convolutional networks (GCNs), embed logs for anomaly-aware inference [25], addressing data sparsity in high-security zones.

2.4 Resilience Assessment Frameworks

Resilience quantifies connectivity under attacks, extending beyond reliability to post-failure recovery [28]. Assessments bifurcate into topological and operational metrics.

Topological evaluations use node loss rates, path lengths, and clustering under random/targeted attacks [35]. Wang et al. [27] proposed a three-stage network-theory model, incorporating spectral gaps for vulnerability scoring. Cascade-aware metrics, like information-link augmented graphs [36], identify fragile links triggering chains.

Operational assessments integrate physics: electrical centrality [28], open-circuit vulnerability [29], and voltage deviations [30] gauge state impacts. Lu et al. [31] combined these with ideal-solution approximations for critical sets, while Li et al. [32] analyzed load-altering attacks via observers.

Spectral vulnerabilities distinguish pure (topology-only) from extended (electrical-weighted) models [27]. Pure spectra use unweighted Laplacians for algebraic connectivity λ2:

λ2(L)=minf_0x≠0,1Tx=0xTLxxTx

Extended versions weight edges by admittance (yij) or flows (pij), yielding vulnerability indices:

Vk=Δηη0

where Δηis performance degradation under k-order contingencies, ηa metric (e.g., throughput) [27]. For N-component networks, k-order analysis scales exponentially, mitigated by random subsets for k⩽3[28].

2.5 Islanding and Evaluation Strategies

Post-fault islanding partitions grids into stable subnetworks via spectral clustering on normalized Laplacians [37]. Optimal island count emerges from eigengaps; fitness balances expansion (internal connectivity) and volume (load equity) scores:

Ec=｜∂Sc｜｜Sc｜

Low Ecindicates robust islands [37]. Rocchetta [37] statistically linked clustering to post-contingency metrics, enhancing recovery baselines.

Correlational analyses across fault scales (e.g., via MATPOWER [35]) reveal islanding efficacy: e.g., optimal partitions minimize worst-case expansions under 10–50% line losses. Q-learning optimizes attack sequences for vulnerability probing [42], though underutilized in urban contexts.

Gaps and Outlook: While multi-functional models advance realism [9], they undervalue runtime states [4]; assessments overlook cyber-physical synergies in cascades [36]. Future work should fuse GCNs with physics-informed neural networks for dynamic, urban-scale evaluations [25].

III. Attack and Defense Strategies in Urban CPPS

Coordinated cyber-physical attacks (CCPAs) exploit the interdependencies in urban CPPS, propagating failures across layers to maximize disruption [21]. Unlike isolated cyber intrusions (e.g., DDoS) or physical sabotage, CCPAs synchronize digital deception with hardware compromise, as seen in hybrid assaults blending false data injection (FDIA) with line cuts [15–23]. This section surveys attack typologies, critical node targeting, and countermeasures, emphasizing urban high-security contexts like CBDs where direct access is restricted [21]. Advances in self-supervised learning address information asymmetry, while tri-level defenses optimize resource allocation [21].

3.1 Typologies of CPPS Attacks

Attacks are categorized by CIA triad impacts: integrity (data/command falsification), confidentiality (data exfiltration), and availability (disruption) [15]. Integrity breaches dominate urban scenarios, enabling stealthy cascades without immediate detection.

Replay and man-in-the-middle (MitM) attacks manipulate measurements/commands [16,17]; e.g., replaying stale PMU data can induce erroneous load shedding [16]. Malware insertions target confidentiality in high-value nodes, such as substations [18,19], while availability strikes like DoS jamming or topology poisoning sever communications [20,21]. Hybrid variants alternate vectors—e.g., FDIA followed by physical strikes—to evade anomaly detectors [22,23].

Urban specificity amplifies risks: dense topologies facilitate lateral movement, but elevated protections (e.g.,

air-gapped controls) necessitate indirect paths [3]. Game-theoretic models frame attackers as rational agents maximizing load loss under resource constraints [23], with empirical validation from Ukraine blackouts [3].

3.2 Critical Node and Link Identification

Effective attacks hinge on pinpointing chokepoints—nodes/links whose failure triggers cascades [24–34]. Approaches bifurcate: topology-centric and state-aware.

Topology-based methods leverage network invariants. Liu et al. [24] introduced fault-link matrices for heterogeneous dependencies, quantifying coupling effects on fragility. Metrics like hop-surface connectivity [25], communication medians [26], and electrical medians [27] distill structural vulnerabilities, revealing that 5–10% targeted removals can disconnect 40% of urban grids [10].

State-aware identification incorporates dynamics. Electrical importance [28] and open-circuit fragility [29] evaluate fault probabilities, while voltage offsets [30] simulate post-failure equilibria. Lu et al. [31] fused these into TOPSIS-like ideals for node sets, and Li et al. [32] used sliding-mode observers for dynamic load attacks. Hybrid models refine further: Nikolakis et al. [33] decoupled controls in containerized simulations, and Zhu et al. [34] enhanced PageRank with directionality for transmission criticality.

Challenges persist in urban cores: topology abstraction ignores protections, yielding non-attackable nodes [21]. Observability theory counters this by seeking minimal sensor sets (MSP) for indirect access. Using BFS for path enumeration and greedy optimization:

$$A=\arg f_0\min f_0 S\subseteq V \mid S \mid \text{s.t.Obs}(G\setminus S)\supseteq T$$

where V is vertices, Ttargets, and Obs denotes observable subspace. This identifies proxy nodes, e.g., adjacent relays, evading air-gaps [21].

3.3 Tri-Level Optimization Defenses Against CCPAs

Defenses must anticipate coordinated threats, balancing proactive hardening with reactive isolation [21]. A tri-level framework structures this: defender (resource allocation), attacker (target selection), and system (response simulation).

Qin et al. [21] formalized it as a bilevel Stackelberg game atop DCOPF for cascades:

Upper Level (Defender):$\min f_0 d \sum L(d,a^*)$, where dhardens components (e.g., IDS deployment), a^* optimal attacker response.

Middle Level (Attacker):$\max f_0 aE[\Delta P \mid d]$, maximizing expected load loss ΔPvia FDIA/physical hits.

Lower Level (System): Solves post-attack OPF: $\min f_0 cgPg+cl\Delta L$s.t. flow balances, limits.

Graph models represent components as nodes/edges, simulating propagations via BFS on substation topologies [21]. IEEE RTS-96 benchmarks show 20–30% load loss reductions via sensitivity-tuned hardening [21]. MFOD extends observability: functional matrices Cf via bipartite matching (HK algorithm) compute losses:

$$\Delta Pt=\Theta y-yf$$

with Θ transmission matrix, yielding rates like node loss $rn=\Delta Pn/Pn0$. This quantifies urban impacts, e.g., 15% higher fragility in CBDs [21].

3.4 Addressing Asymmetric Information in Attacks

Attackers often lack full topologies, leading to mismatched targeting. Self-supervised contrastive learning detects omissions, enhancing consistency [25].

A three-module pipeline anonymizes graphs, detects gaps, and identifies nodes. GCN embeds neighborhoods:

$$H(l+1)=\sigma(D-1/2AD-1/2H(l)W(l))$$

Pair representations hij=[hi;hj]feed MLPs for binary classification, minimized via BCE. Positive pairs (1st-order neighbors) signal gaps; negatives (2nd-order) balance [3.3.2.1].

Contrastive alignment maximizes intra-node similarity [3.3.2.3], boosting F1-scores by 10–15% over baselines in synthetic CPPS graphs [25]. Supplemented topologies unify defender-attacker views, e.g., converging PageRank ranks by 8% [34].

3.5 Gaps and Future Directions

Current strategies undervalue temporal dynamics in hybrids [22] and urban zoning [21]; defenses assume perfect observability [31]. Evolutionary algorithms like GIEA [35] promise adaptive targeting, but require physics integration [27]. Future efforts should embed LLMs for behavioral simulation [18] and federated learning for privacy-preserving sharing [1], scaling to 10k-node urban simulations.

IV. Recovery Mechanisms in Urban CPPS

Recovery mechanisms in urban cyber-physical power systems (CPPS) aim to restore functionality post-disruption, minimizing load loss and downtime while navigating inter-layer dependencies [38–44]. Traditional approaches focused on physical reconfiguration, but recent advancements emphasize cyber-physical synergies, accounting for information delays and resource coordination [42–44]. With urban grids facing compounded faults from attacks or disasters [3], strategies now integrate optimization models, graph-based pathing, and multistate failure considerations. This section reviews evolution from siloed recoveries to holistic frameworks, highlighting quantifiable gains like 20–40% faster restoration via collaborative models [40,42].

4.1 Traditional Physical Recovery Strategies

Early recovery targeted physical components—generation, reconfiguration, and load restoration—often under resource constraints like crew availability and travel times [38–41].

Dong et al. [38] minimized crew dispatch and outage costs in hurricane scenarios via pre-scheduling, formulating as mixed-integer programming (MIP):

$$\min f_0 \sum (cttr+clLd)$$

s.t. resource limits, distance matrices, where ct,clare time/load costs, trrepair times, Lddisrupted loads. For distribution networks, a two-stage heuristic allocates faults

to centers then optimizes switches/generators [39], boosting recovery rates by 15–25% under constraints.

Collaborative models address interactions: Dong et al. [40] used random forests for convex optimization in distributed generation, reducing solve times by 30%. Wan et al. [41] incorporated repair uncertainties via improved particle swarm, modeling stochastic times tr~ N(μ,σ2)for transmission emergencies.

These excel in physical isolation but neglect cyber influences, e.g., delayed state estimation prolonging cascades [42]. Urban applicability is limited by scale, with MIPs infeasible beyond 500 nodes without heuristics [38].

4.2 Cyber-Physical Synergistic Recovery

Synergistic strategies fuse layers, treating cyber outages as amplifiers of physical faults [42–44]. Chen et al. [42] proposed dual-layer islanding via dependency theory, partitioning interdependent nodes for synchronous restoration, achieving 18% lower losses in regional grids.

Wu et al. [43] framed natural disaster defenses with cyber aids (e.g., monitoring during repairs), integrating measurement promotion into OPF. Chen et al. [44] gridded distribution for dual-fault models, optimizing power-communication repairs geographically:

$$\max f_0 \sum \eta p+\lambda\eta cs.t.dij \leqslant R,rp+\delta rc \leqslant T$$

where ηare recovery efficiencies, δcyber-physical delays, Rgrid radius. Recent extensions consider interdependencies: Chen and Wang modeled cascading recoveries in interdependent CPS, using Markov chains for state transitions, reducing vulnerability by 25% in simulations. Zhang et al. extended to transportation-CP couplings, optimizing multi-network paths for 10–20% faster urban restores.

Multistate failures add realism: Wu et al. optimized resilience via degraded states (e.g., partial cyber uptime), employing Benders decomposition for large-scale CPPS, outperforming MILP by 40% in convergence.

4.3 Information Delay Models and Optimal Path Prediction

Urban recoveries must model cyber delays—e.g., faulty comms hindering diagnosis—via delay functions. An information delay model quantifies impacts:

$$\tau d=f(If,Dp)=\alpha(1-uc)+\beta tdiag$$

where Ifis information failure rate, Dpphysical damage, uccyber uptime, α,βcoefficients from logs [44]. This informs control: delayed scheduling cascades to reconfiguration, increasing losses by 10–15% [43].

Graph convolutional networks (GCNs) predict optimal paths for crews/vehicles across layers [14]. Embeddings aggregate topologies, outputting paths minimizing total delay/cost:

$$P* = \arg f_0 \min f_0 \sum (de+\tau d(e)+cr)$$

via GNN policy networks, e.g., in multi-agent RL [40]. Li et al. recovered ML states post-FDIA using generative models, restoring 90% accuracy in cyber estimates. Dynamic simulations iterate: initialize flows, fault nodes/lines, optimize under partial observability, recompute until stable [41]. Assumptions like UPS buffering prevent immediate cross-failures, with survival ratios as metrics (e.g., 85% branch retention post-20% attack) [42].

4.4 Gaps and Future Directions

Traditional methods undervalue cyber delays [38–41]; synergies overlook multistate dynamics . Urban gaps include scalable pathing for 10k+ nodes and real-time adaptation [44]. Future: hybrid GNN-RL for predictive recoveries , federated learning for privacy-safe sharing [18], and quantum-inspired optimization for uncertainties . Integrating LLMs for scenario generation could simulate rare events, targeting <5% residual losses [43].

V. Platforms and Future Trends in CPPS Security

As urban cyber-physical power systems (CPPS) mature, practical platforms bridge theoretical models with real-world deployment, enabling simulation, monitoring, and validation of security strategies. These platforms simulate layered interactions, from topology inference to cascade recovery, while future trends leverage emerging technologies like digital twins and AI-driven defenses to address evolving threats. This section examines demonstration platforms, drawing on multi-source integration and optimization, before exploring 2025+ trajectories amid IT/OT convergence and AI-augmented risks.

5.1 Demonstration Platforms for Monitoring and Recovery

Demonstration platforms operationalize CPPS security by replicating urban environments—e.g., CBDs and airports—with geographic fidelity, facilitating end-to-end testing of attacks, defenses, and recoveries. A core exemplar is a hierarchical cyber layer atop physical graphs: nodes (generators, substations, loads) and edges (lines) embed 2D coordinates for spatial accuracy, while cyber tiers (access, backbone, core) ensure robust data flows via full-mesh subgraphs.

Static modeling establishes baselines: adjacency matrices Ap,Acfor power/cyber, with virtual dependencies reflecting overlaps (e.g., fiber along lines). Dynamic cascades employ DCOPF iterations:

1.Initialize flows per demand.

2.Apply initial faults (node/edge removals, e.g., 10–20% simulating attacks [3]).

3.Recompute/optimize under partial observability (last-known states for unmonitored nodes).

4.Loop until equilibrium, yielding survival ratios (e.g., 80–90% branch retention) [41].

Assumptions like UPS buffering mitigate immediate cross-failures, while edge-induced faults (e.g., line cuts disabling comms) amplify realism [42]. Optimization minimizes costs:

$$\min f_0 \sum cgPg+cl\Delta Ls.t.Pb=d-\Delta d, \mid fe \mid \leqslant femax$$

balancing generation (Pg) and shedding (ΔL) [4.3.4.2].

Recovery integrates GCNs for path prediction [14]: embeddings forecast crew routes minimizing delays τd, linking cyber repairs to power restoration—e.g., restoring

15–25% more load via info-physical feedback [44]. Platforms like those in EPOCHS [5] or MATPOWER [35] validate: IEEE RTS-96 tests show 30% outage reductions with delay modeling [21]. Scalability to 1k+ nodes demands containerization [33], enabling urban demos with <5s latencies [40].

These platforms not only benchmark metrics (e.g., load loss rates <10%) but foster hybrid simulations, e.g., fusing real logs with synthetic attacks for anomaly training [1].

5.2 Future Trends in CPPS Security

By 2025, CPPS security will pivot toward proactive, adaptive paradigms amid escalating AI-orchestrated threats and IT/OT convergence. Digital twins (DTs) emerge as transformative: real-time replicas of CPPS fuse sensor data with predictive models, enhancing resilience via "what-if" simulations of cascades. For instance, DTs could forecast 20–40% faster recoveries by mirroring urban grids, integrating GCNs with physics-informed NNs for anomaly detection.

Microsegmentation and zero-trust architectures will granularize protections, isolating OT segments from IT breaches—critical as 2024 incidents highlighted legacy vulnerabilities . Energy-efficient controls counter DoS via lightweight ML, reducing battery drain in edge devices by 30% . Blockchain bolsters integrity: distributed ledgers for tamper-proof logs and decentralized auth, mitigating FDIA in high-stakes zones .

AI-driven threats demand counter-AI defenses: generative models simulate adversarial behaviors, while federated learning enables privacy-preserving topology sharing across utilities [18]. Quantum-resistant crypto addresses post-quantum risks in comms, and 6G-enabled sensing accelerates monitoring [2]. Physical-cyber fusion trends include AI-enhanced surveillance for hybrid threats, e.g., drone-detected line sabotage triggering auto-isolation.

Policy-wise, NIST frameworks emphasize integrated risk assessments, aligning with China's smart grid mandates [9]. Challenges: scaling DTs to exascale sims and ethical AI use . Outlook: hybrid platforms blending DTs with edge AI could achieve >95% threat detection, slashing urban outage costs by billions .

5.3 Gaps and Opportunities

Platforms lag in real-time federated validation [33]; trends overlook socio-economic factors [9]. Opportunities: LLM-orchestrated twins for rare-event training and open-source benchmarks for global collab . By 2030, resilient CPPS could underpin net-zero cities, contingent on interdisciplinary advances.

VI. Conclusion

The integration of cyber-physical systems into urban power grids has revolutionized energy management, yet it has concurrently amplified vulnerabilities to coordinated attacks, cascading failures, and information asymmetries [1,3]. This review has systematically explored the landscape of cross-source intelligent security monitoring and analysis for CPPS, synthesizing modeling paradigms, attack-defense dynamics, recovery mechanisms, and platform implementations. From multi-functional urban models incorporating monitoring, powering, and control modules [9] to tri-level optimizations countering hybrid threats [21], advancements underscore a shift toward resilient, adaptive frameworks that quantify vulnerabilities via spectral metrics [27] and self-supervised gap detection [25].

Key contributions include a unified taxonomy bridging reductionist, physics-based, and network-theoretic approaches [4–14]; enhanced critical node identification via observability and GCN embeddings [24,34]; synergistic recoveries modeling delays for 20–40% efficiency gains [42–44]; and scalable platforms simulating urban cascades with <5s latencies [5,35]. These innovations address persistent gaps—such as functional heterogeneity oversight [4] and high-security zoning [21]—providing quantifiable tools like load loss rates and islanding efficacy to minimize outages, potentially averting billions in economic impacts [38].

Ultimately, bolstering CPPS resilience demands interdisciplinary convergence: fusing AI with policy-driven standards [9] to fortify smart grids against 2025+ threats like quantum-enabled exploits . By democratizing these technologies through open platforms, researchers and utilities can cultivate self-healing infrastructures, ensuring sustainable electrification amid escalating cyber-physical interdependencies. Future endeavors should prioritize real-world validations, ethical AI deployments, and global collaborations to realize zero-trust, net-zero grids.

Acknowledgment

This research was funded by the Fundamental Research Funds of CAF, grant numbers CAFYBB2022SY033 ("Spatio-temporal Data Organization Model and Application for Forest and Grassland Based on GeoSOT Encoding").

REFERENCES

[1] Zhang X, et al. An integrated modeling framework for cascading failure study and robustness assessment of cyber-coupled power grids. Reliability Engineering & System Safety, 2022; 226: 108654.

[2] Menezes AS, et al. Hybrid cooperative spectrum sensing for improving cognitive power line communication systems. Computers and Electrical Engineering, 2022; 103: 108286.

[3] Center for International Strategic Studies. Cyber Operations during the Russian-Ukrainian War, 2023.

[4] Xu S, et al. Resilience enhancement of renewable cyber – physical power system against malware attacks. Reliability Engineering & System Safety, 2023; 229: 108830.

[5] Hranisavljevic N, et al. Discretization of hybrid CPPS data into timed automaton using restricted Boltzmann machines. Engineering Applications of Artificial Intelligence, 2020; 95: 103826.

[6] Chen LJ, et al. Cyber-physical system fusion modeling and robustness evaluation. Electric Power Systems Research, 2022; 213: 108654.

[7] Li JK, et al. Reliability analysis on energy storage system combining GO-FLOW methodology with GERT network. Reliability Engineering & System Safety, 2024; 243: 109860.

[8] Elma O, et al. An overview of bidirectional electric vehicles charging system as a Vehicle to Anything (V2X) under Cyber – Physical Power System (CPPS). Energy Reports, 2022; 8(14): 25-32.

[9] Sheng YJ, et al. Modeling and collaborative optimization of power-traffic coupled networks from cyber-physical-social perspectives. Automation of Electric Power Systems, 2024; 48(07): 62-85. (In Chinese)

[10] Buldyrev SV, et al. Catastrophic cascade of failures in interdependent networks. Nature, 2010; 464(7291): 1025.

[11] Lu ZG, et al. Optimal defense strategy selection method for CPS considering integrated cyber – physical losses. Sustainable Energy, Grids and Networks, 2023; 36: 101143.

[12] Hu FY, et al. Modeling and fault analysis of cyber-physical power systems. Computer Simulation, 2024; 41(02): 74-80. (In Chinese)

[13] Wang SL, et al. Robustness improvement strategy of cyber-physical systems with weak interdependency. Reliability Engineering & System Safety, 2023; 229: 108837.

[14] Yang T, et al. Fault communication recovery strategy for cyber-physical power systems. Power System Technology, 2024: 1-11. (In Chinese)

[15] Wang J, et al. Adversarial Malware Examples for Terminal Cyberspace Attack Analysis in Cyber-Physical Power Systems. 2021 International Conference on Power System Technology (POWERCON), 2021: 1865-1870.

[16] Li X, et al. Improving Kalman filter for cyber physical systems subject to replay attacks: An attack-detection-based compensation strategy. Applied Mathematics and Computation, 2024; 466: 128444.

[17] Solat A, et al. On the control of microgrids against cyber-attacks: A review of methods and applications. Applied Energy, 2024; 353: 122037.

[18] Biswas B, et al. A hybrid framework using explainable AI (XAI) in cyber-risk management for defence and recovery against phishing attacks. Decision Support Systems, 2024; 177: 114102.

[19] Geng JX, et al. A survey of strategy-driven evasion methods for PE malware: Transformation, concealment, and attack. Computers & Security, 2024; 137: 103595.

[20] Wang MF, et al. Observer – based H ∞ control for cyber – physical systems encountering DoS jamming attacks: An attack-tolerant approach. ISA Transactions, 2020; 104: 1-14.

[21] Qin C, et al. A tri-level optimal defense method against coordinated cyber-physical attacks considering full substation topology. Applied Energy, 2023; 339: 120961.

[22] Zhang P, et al. Event-Triggered Ultimately Bounded Filtering for Two-Dimensional Discrete-Time Systems under Hybrid Cyber Attacks. Journal of the Franklin Institute, 2023.

[23] Ge H, et al. A game theory based optimal allocation strategy for defense resources of smart grid under cyber-attack. Information Sciences, 2024; 652: 119759.

[24] Liu HQ, et al.Grid critical node identification and partitioning method based on network fault link matrix. Proceedings of the CSEE, 2024; 24(05): 1-13. (In Chinese)

[25] Varbella A, et al. Geometric deep learning for online prediction of cascading failures in power grids. Reliability Engineering & System Safety, 2023; 237: 109341.

[26] Garcia A, et al. Containerized edge architecture for manufacturing data analysis in Cyber-Physical Production Systems. Procedia Computer Science, 2022; 204: 378-384.

[27] Wang SL, et al. A three-stage model of quantifying and analyzing power network resilience based on network theory. Reliability Engineering & System Safety, 2024; 241: 109681.

[28] Rostami A, et al. Reliability assessment of cyber-physical power systems considering the impact of predicted cyber vulnerabilities. International Journal of Electrical Power & Energy Systems, 2023; 147: 108892.

[29] Hu FY, et al. Robustness assessment of cyber-physical power systems based on critical nodes. Complex Systems and Complexity Science, 2024: 1-9. (In Chinese)

[30] Li J, et al. Analysis of cascading failures of power cyber-physical systems considering false data injection attacks. Global Energy Interconnection, 2021; 4(2): 204-213.

[31] Lu ZG, et al. Optimal defense strategy selection method for CPS considering integrated cyber – physical losses. Sustainable Energy, Grids and Networks, 2023; 36: 101143.

[32] Li J, et al. Dynamic load altering attack detection for cyber physical power systems via sliding mode observer. International Journal of Electrical Power & Energy Systems, 2023; 153: 109320.

[33] Nikolakis N, et al. On a containerized approach for the dynamic planning and control of a cyber-physical production system. Robotics and Computer-Integrated Manufacturing, 2020; 64: 101919.

[34] Zhu DR, et al. Research on critical node identification method for transmission networks based on improved PageRank algorithm. Power System Protection and Control, 2022; 50(05): 86-93. (In Chinese)

[35] Wu GY, et al. A Gene Importance based Evolutionary Algorithm (GIEA) for identifying critical nodes in Cyber – Physical Power Systems. Reliability Engineering & System Safety, 2021; 214: 107760.

[36] Yin YH, et al. Syncretic K-shell algorithm for node importance identification and invulnerability evaluation of urban rail transit network. Applied Mathematical Modelling, 2023; 120: 400-419.

[37] Rocchetta R. Enhancing the resilience of critical infrastructures: Statistical analysis of power grid spectral clustering and post-contingency vulnerability metrics. Renewable and Sustainable Energy Reviews, 2022; 159: 112185.

[38] Dong GC, et al. Coordinated recovery method for post-disaster distribution network cyber-physical systems considering network reconstruction and emergency resources. Electric Power Automation Equipment, 2024: 1-9. (In Chinese)

[39] Resilient Disaster Recovery Logistics of Distribution Systems: Co-Optimize Service Restoration With Repair Crew and Mobile Power Source Dispatch. IEEE Transactions on Smart Grid, 2019; 10(6): 10. (Note: Original citation appears truncated; assumed full reference based on context.)

[40] Dong ZC, et al. Research on the connection radius of dependency links in interdependent spatial networks against cascading failures. Physica A: Statistical Mechanics and its Applications, 2019; 513: 555-564.

[41] Dong ZC, et al. Mitigating cascading failures of spatially embedded cyber – physical power systems by adding additional information links. Reliability Engineering & System Safety, 2022; 225: 108559.

[42] Chen X, et al. Q-learning based strategy analysis of cyber-physical systems considering unequal cost. Intelligent and Converged Networks, 2023; 4(2): 116-126.

[43] Wu YY, et al. Target layer state estimation in multilayer complex dynamical networks using functional observability. Journal of the Franklin Institute, 2023; 360(12): 8178-8199.

[44] Chen B, et al. Grid-based coordinated recovery strategy for power-communication in extreme post-disaster distribution networks. Power System Technology, 2021; 45(05): 2009-2017. (In Chinese)