Review

Multi-Domain Moving Target Defense for Resilient Security in Power Cyber-Physical Systems: A Review

He Wu *

Posted Date: 2 June 2025

doi: 10.20944/preprints202506.0030.v1

Keywords: power cyber-physical systems; moving target defense; grid topology reconfiguration; market security; human-in-the-loop cyber defense; digital twin validation

 doi:10.20944/preprints202506.0030.v1

Review

Multi-Domain Moving Target Defense for Resilient Security in Power Cyber-Physical Systems: A Review

He Wu

School of Electric Power, Shenyang Institute of Engineering, Shenyang, China; wu_er02@outlook.com

Abstract: The increasing complexity and digitalization of Power Cyber-Physical Systems (Power CPS) have amplified their exposure to persistent and adaptive cyber-physical threats. Static configurations across cyber, physical, and market layers offer adversaries stable attack surfaces for reconnaissance, manipulation, and disruption. In response, this review introduces Moving Target Defense (MTD) as a proactive and dynamic paradigm for enhancing Power CPS security. The paper systematically analyzes multi-domain MTD strategies—including IP randomization, topology reconfiguration, market rule variability, and adaptive control mode switching—and evaluates their effectiveness in disrupting attacker planning while preserving operational stability. Human-in-the-loop orchestration frameworks, supported by AI-driven monitoring and explainable decision support, are proposed to coordinate safe and scalable MTD deployment. Additionally, we discuss digital twin-based validation platforms, resilience metrics, and real-world deployment challenges. The review concludes by outlining future research priorities and cross-sector collaboration pathways to operationalize adaptive MTD as a foundational pillar of resilient grid security.

Keywords: power cyber-physical systems; moving target defense; grid topology reconfiguration; market security; human-in-the-loop cyber defense; digital twin validation

---

1. Introduction

1.1. Limitations of Static and Perimeter-Based Cyber Defenses in Power CPS

The convergence of digital technologies with physical grid operations has given rise to Power Cyber-Physical Systems (Power CPS), enabling real-time monitoring, control, and optimization of power generation, transmission, and consumption [1–3]. These systems integrate sensors, actuators, communication networks, control algorithms, and market mechanisms to manage increasingly complex and decentralized energy infrastructures, including distributed energy resources (DERs) [4–6], microgrids [7–9], and virtual power plants (VPPs) [10].

However, this digital transformation has significantly expanded the attack surface of power systems. Traditional perimeter-based defenses—such as firewalls, static access controls, and fixed network segmentation—were designed under the assumption that once the boundary is secured, internal operations are safe [11]. This assumption no longer holds in Power CPS for several reasons [12–14]:

- **Interconnectedness**: Power CPS are increasingly connected to external networks, cloud services, and third-party platforms, making perimeter boundaries fluid and porous.
- **Insider Threats**: Compromised insiders or supply chain attacks can bypass perimeter defenses.
- **Advanced Persistent Threats**: Attackers often penetrate static defenses and maintain long-term stealthy presence.

 doi:10.20944/preprints202506.0030.v1

- **Static Configurations**: Fixed system configurations provide attackers with stable targets to study, exploit, and compromise over time.

Examples of real-world cyber-physical incidents—such as the 2015 Ukraine grid attack, the Stuxnet worm, and more recent ransomware attacks on critical infrastructure—demonstrate the insufficiency of static defenses. These events reveal the need for dynamic, adaptive security mechanisms that continuously evolve to counter evolving threats [15].

1.2. Concept and Relevance of Moving Target Defense

Moving Target Defense (MTD) is an emerging security paradigm that seeks to increase system unpredictability by continuously changing the system's attack surface [16,17]. By dynamically reconfiguring aspects of the system—such as network topology, control paths, authentication keys, or even market mechanisms—MTD makes it more difficult for attackers to:

- Gather accurate system knowledge.
- Maintain persistent footholds.
- Launch successful, repeatable attacks.

The key principle of MTD is to shift the security advantage from static defenders to dynamic defenders, forcing attackers to adapt faster than they can reliably exploit. MTD has shown promise in network security, cloud computing, and military systems, but its application to Power CPS remains underexplored [18–20].

In the context of Power CPS, MTD strategies can extend beyond the cyber layer to include [21–23]:

- **Physical Layer Variations**: Changing grid topology or switching operational modes (e.g., islanded vs. grid-connected).
- **Market Mechanism Dynamics**: Introducing variability in market rules, pricing algorithms, or bidding processes to thwart economic manipulation.
- **Human-Operator Engagement**: Involving operators in orchestrating and validating MTD strategies to ensure safety and operational feasibility.

This multi-domain perspective on MTD represents a promising shift toward proactive, adaptive security in Power CPS, complementing traditional static defenses and AI-driven detection mechanisms [24,25].

1.3. Contributions and Structure of This Review

This review aims to provide the first comprehensive exploration of multi-domain MTD strategies for adaptive Power CPS security. Its key contributions are as follows:

- **Identification of Static Configuration Vulnerabilities**: Analyzing how fixed system parameters in cyber, physical, and market layers create exploitable attack surfaces.
- **Systematic Classification of MTD Techniques**: Categorizing MTD strategies across multiple domains and evaluating their applicability to Power CPS.
- **Design Trade-Off Analysis**: Discussing the operational costs, security benefits, and coordination challenges of deploying MTD.

 doi:10.20944/preprints202506.0030.v1

- **Human-in-the-Loop and AI-Augmented MTD Orchestration**: Proposing frameworks for integrating human oversight and AI-driven decision support in MTD management.
- **Validation Platforms and Deployment Considerations**: Reviewing simulation tools, resilience metrics, and practical challenges in operationalizing MTD.
- **Future Research Agenda**: Highlighting open research questions, regulatory considerations, and cross-sector collaboration needs.

The remainder of this review is structured as follows. Section 2 examines the threat surfaces and defense challenges in Power CPS, highlighting the limitations of static configurations. Section 3 introduces the principles and classification of multi-domain MTD. Section 4 and Section 5 detail MTD strategies for the cyber, physical, and market layers, respectively. Section 6 discusses human-in-the-loop and AI-augmented MTD coordination. Section 7 reviews validation platforms, resilience metrics, and deployment challenges. Section 8 outlines future research directions and collaboration opportunities. Finally, Section 9 concludes the review with key insights and a call to action for advancing dynamic, adaptive defense paradigms in Power CPS.

2. Threat Surfaces and Defense Challenges in Power CPS

Power CPS are inherently complex, multi-layered infrastructures where cyber, physical, market, and human elements interact to manage energy production, distribution, and consumption [26–28]. While this integration enhances operational efficiency and flexibility, it also amplifies system vulnerabilities, especially when system configurations remain static over time. This section analyzes the key threat surfaces across different domains and explains why static configurations create long-term security risks.

2.1. Static Configuration Vulnerabilities in Cyber, Physical, and Market Layers

2.1.1. Cyber Layer Vulnerabilities

The cyber layer includes communication networks, software platforms, and control interfaces that enable real-time monitoring and management of power systems [29,30]. Static configurations in this layer include:

- **Fixed IP Addresses and Network Topologies**: These provide stable targets for attackers to map and exploit through scanning and reconnaissance.
- **Unchanging Authentication Credentials or Keys**: Static passwords or cryptographic keys are susceptible to brute-force attacks, credential theft, and reuse attacks.
- **Predefined Control Paths and Protocol Configurations**: Predictable control command paths and protocol settings make it easier for attackers to craft protocol-specific exploits or man-in-the-middle attacks [31].

Such static elements allow attackers to study the system over time, identify weak points, and develop tailored exploits that maximize impact while minimizing detection.

2.1.2. Physical Layer Vulnerabilities

The physical layer consists of power generation units, substations, DERs, and grid control devices such as Phasor Measurement Units (PMUs) and Remote Terminal Units (RTUs) [32–35]. Static configurations here include:

 doi:10.20944/preprints202506.0030.v1

- **Fixed Grid Topologies**: Long-standing transmission and distribution network structures that, once mapped, reveal critical dependencies and single points of failure [36].
- **Static Control Modes**: Fixed operational settings for DERs, energy storage systems, or microgrid controllers, making them predictable targets for control manipulation [37,38].
- **Unchanging Load Profiles or Dispatch Patterns**: Repetitive scheduling patterns that adversaries can exploit to time their attacks for maximum disruption [39].

These static physical configurations expose the system to targeted manipulation, such as cascading outages, DER misoperation, or incorrect state estimation.

2.1.3. Market Layer Vulnerabilities

Modern power systems operate within market frameworks where bidding, pricing, and settlement processes are automated and data-driven [40,41]. Static vulnerabilities include:

- **Fixed Market Rules and Pricing Algorithms**: These can be reverse-engineered by attackers to manipulate price signals or create artificial congestion.
- **Predictable Bidding Patterns**: Attackers can mimic or disrupt legitimate market participants by exploiting consistent bidding behaviors [42].
- **Unchanging Demand Response Schedules**: Static schedules make it easier for adversaries to predict and exploit load control events.

Such vulnerabilities enable economic attacks, including market manipulation, financial fraud, and artificial scarcity creation.

2.2. Cross-Layer Attack Propagation and Systemic Risk Amplification

One of the defining characteristics of Power CPS is the interdependence between layers. Cyber, physical, and market layers are tightly coupled, meaning that vulnerabilities in one layer can propagate and amplify risk across others [43,44].

Examples of Cross-Layer Attacks

- **Cyber-Physical Attacks**: An attacker exploits a cyber vulnerability to inject false data into grid control systems, causing physical instability or equipment damage.
- **Cyber-Market Manipulation**: Compromised market data streams lead to incorrect pricing, which in turn drives grid imbalances and operational risks [45].
- **Physical-Cyber Reconnaissance**: Physical monitoring of substations or DER installations provides attackers with insights to craft cyber exploits targeting those assets [46].

Systemic Risk Amplification

Cross-layer attacks can escalate localized vulnerabilities into system-wide failures by:

- Triggering cascading outages across interconnected grids.
- Exploiting market dynamics to amplify financial impact.
- Overwhelming operators with misleading or conflicting information.

 doi:10.20944/preprints202506.0030.v1

This highlights the need for defense strategies that span all layers and adapt dynamically to evolving cross-layer threats [47].

2.3. Gaps in Existing Defense Mechanisms

Despite advancements in intrusion detection systems (IDS), machine learning-based anomaly detection, and perimeter security technologies, existing defenses face several limitations:

- **Static Defense Posture**: Most security measures are configured once and remain unchanged, making them vulnerable to long-term reconnaissance and exploitation [48].
- **Siloed Defense Layers**: Cyber, physical, and market defenses are often developed and managed in isolation, missing cross-layer attack correlations.
- **Reactive Detection Focus**: Existing systems prioritize detecting known attack signatures or anomalies after they occur, rather than proactively disrupting attacker reconnaissance and planning [49].
- **Operator Overload**: Static rule-based systems generate high volumes of alerts, many of which are false positives, overwhelming human operators.

These limitations underscore the need for proactive, dynamic, and coordinated defense approaches that continuously change the system's attack surface, making it harder for attackers to maintain a stable foothold or execute successful attacks [50–52]. A summary of threat surfaces and defense gaps is listed in Table 1.

Table 1. Summary of Threat Surfaces and Defense Gaps.

Layer	Static Configuration Vulnerabilities	Resulting Risks
Cyber Layer	Fixed IPs, static credentials, predictable control paths	Long-term reconnaissance, targeted exploitation, persistent threats
Physical Layer	Fixed grid topologies, static control modes, load patterns	Cascading failures, equipment damage, grid instability
Market Layer	Unchanging rules, bidding patterns, demand response schedules	Market manipulation, artificial scarcity, financial losses
Cross-Layer	Coupled cyber-physical-market dependencies	Systemic risk amplification, operator confusion, widespread impact

In summary, the static nature of most Power CPS configurations creates predictable, long-term vulnerabilities that adversaries can exploit. To counter these risks, the next section introduces the principles of MTD as a proactive, multi-domain defense paradigm for disrupting attacker strategies and enhancing system resilience.

3. Principles of Moving Target Defense for Power CPS

Building on the threat analysis presented in the previous section, this section introduces the conceptual foundations, classification, and multi-domain applicability of MTD as a strategy to counter static system vulnerabilities and disrupt adversarial planning in Power CPS [53–55]. By continuously altering system configurations and parameters across cyber, physical, market, and human layers, MTD aims to increase system unpredictability, limit attacker reconnaissance effectiveness, and shift the advantage to defenders [56].

3.1. Conceptual Foundations and Classification of MTD Techniques

3.1.1. Definition and Core Philosophy of Moving Target Defense

 doi:10.20944/preprints202506.0030.v1

MTD represents a proactive cybersecurity strategy designed to continuously or periodically alter the characteristics and configurations of a system's attack surface [57]. Unlike traditional static defense measures that offer attackers stable targets for persistent reconnaissance, MTD dynamically shifts the operational environment, significantly elevating attacker uncertainty and complicating their efforts to develop reliable attack models. By continually changing critical system parameters and configurations, MTD dramatically reduces the vulnerability exploitation window, compelling adversaries to continuously restart reconnaissance and adapt their strategies. While not removing vulnerabilities entirely, MTD effectively disrupts the adversary's ability to predict, analyze, and successfully exploit system weaknesses [58–60].

3.1.2. Core Objectives and Strategic Benefits of MTD

The fundamental objectives underpinning MTD are rooted in undermining attacker strategies by continually invalidating their knowledge and assumptions about system operations [61,62]. First, MTD aims to disrupt adversary planning efforts, preventing them from constructing accurate and lasting models of system behaviors and configurations. Secondly, it seeks to substantially reduce exploit longevity; even if an attacker succeeds in compromising an asset, frequent configuration changes ensure such footholds are temporary, minimizing long-term damage. Finally, MTD strategies intentionally force attackers into a continuous state of adaptation, thereby significantly increasing their operational costs and risks [63]. This continuous adaptation not only exhausts attacker resources but also raises the probability of detection, as adversaries must frequently probe the system anew.

3.1.3. Systematic Classification and Application Domains of MTD

MTD techniques can be comprehensively classified based on the specific aspects or parameters of a system that are dynamically altered [64,65]. Each type of MTD addresses unique vulnerabilities and comes with distinct operational considerations:

- **Spatial MTD:** This category focuses on dynamically adjusting the spatial configurations of the system, including network topologies or physical resource allocations. In the context of Power CPS, spatial MTD strategies might involve dynamically rerouting network traffic, periodically changing grid interconnection patterns, or reconfiguring the operational boundaries of microgrids. Such alterations complicate attackers' spatial reasoning, hindering targeted exploitation of specific components or locations [66].
- **Temporal MTD:** Temporal MTD methods periodically vary operational parameters and configurations over time, such as regularly rotating cryptographic keys, authentication credentials, or even control logic modes. By introducing unpredictability into the timing and duration of operational states, temporal MTD substantially narrows attackers' opportunities to exploit any specific operational mode, reducing the likelihood of sustained system compromise [67,68].
- **Behavioral MTD:** Behavioral approaches aim to introduce controlled randomness or unpredictability into system responses and actions, such as varying control signal outputs, operational setpoints, or market transaction parameters. Behavioral variability disrupts attackers' attempts to accurately predict system responses, undermining their ability to design effective manipulation or deception-based attacks [69].
- **Information MTD:** This approach focuses on altering the visibility, accuracy, or representation of system data accessible to potential adversaries. Information MTD could involve deceptive data streams, dynamic obfuscation of monitoring outputs, or the strategic dissemination of misleading information during reconnaissance phases [70]. These techniques significantly impede attackers' ability to confidently assess system status and vulnerabilities, compelling them to expend substantial resources distinguishing genuine system states from deceptive signals [71,72].

 doi:10.20944/preprints202506.0030.v1

3.1.4. Trade-Offs and Considerations in MTD Implementation

Despite the substantial defensive advantages, implementing MTD strategies involves careful consideration of several critical trade-offs. Each MTD domain introduces distinct challenges related to complexity, operational overhead, and potential impacts on system stability and performance [73–75]. For instance, spatial reconfigurations can inadvertently affect grid stability or communication reliability if not properly synchronized with operational constraints. Similarly, frequent temporal adjustments could result in increased system latency or operational disruptions if transitions between states are not managed effectively. Behavioral and informational MTD techniques, while highly effective at deception, risk confusion among legitimate operators and may introduce unforeseen complications in routine operational decision-making [76–78].

Therefore, the successful deployment of MTD in Power CPS requires a balanced and integrated approach that carefully assesses defense effectiveness against operational feasibility. It demands comprehensive cross-layer coordination, robust real-time management tools, and significant investment in operator training and adaptive decision support systems to achieve optimal security gains without compromising system reliability or regulatory compliance [79].

3.2. Multi-Domain MTD: Cyber, Physical, Market, and Human Layer Dynamics

3.2.1. Cyber Layer MTD

Moving Target Defense strategies within the cyber domain primarily aim at dynamically altering network configurations, communication protocols, and authentication mechanisms, thus directly confronting the reconnaissance efforts that cyber attackers typically rely on [80–82]. Techniques such as IP address randomization periodically shift the network identities of critical components, rendering attackers' mapping efforts obsolete. Similarly, dynamic routing techniques continuously vary data transmission paths, effectively mitigating persistent surveillance or man-in-the-middle interception attempts. Furthermore, MTD includes strategies like protocol parameter variation, which introduce unpredictability into communication settings, impeding protocol-specific exploitation and significantly increasing the complexity for attackers to reliably execute known attack patterns [83]. Complementing these, the regular rotation of cryptographic keys and authentication credentials significantly diminishes the risk of credential reuse, credential stuffing, or brute-force attacks, forcing adversaries into perpetual cycles of re-acquisition and recalibration of their attacks [84,85].

3.2.2. Physical Layer MTD

In the physical realm of Power CPS, MTD addresses vulnerabilities tied to static configurations of grid infrastructures and control settings [86]. The core method, grid topology reconfiguration, involves dynamically activating or deactivating transmission lines, switching transformer connections, or temporarily modifying substation connectivity. These changes obscure critical interdependencies and pathways that attackers might exploit, while also limiting the potential spread of disruptions through strategic segmentation [87,88]. Further, physical MTD encompasses dynamic control mode switching, alternating control settings of DERs—such as transitioning between voltage control, frequency regulation, and reactive power management modes—to prevent attackers from accurately predicting operational behaviors [89]. Additionally, virtual islanding strategies periodically segment parts of the grid into self-sufficient microgrids [90,91]. Such controlled segmentation localizes potential disruptions, providing intrinsic resilience by containing failures and limiting cascading effects across interconnected networks [92].

3.2.3. Market Layer MTD

Beyond technical infrastructure, energy markets represent another crucial attack surface susceptible to manipulation. Attackers aiming for economic exploitation depend heavily on predictable market dynamics, such as fixed pricing algorithms or static demand response schedules

 doi:10.20944/preprints202506.0030.v1

[93,94]. To counteract this, Market Layer MTD employs strategies like dynamic rotation of market rules and pricing algorithms, introducing controlled unpredictability in bidding processes and market clearing outcomes. This unpredictability effectively reduces adversaries' abilities to reverse-engineer and exploit market mechanisms [95]. Further extending this unpredictability, randomized demand response signaling varies the timing, duration, and magnitude of demand-side interventions, significantly complicating adversarial planning aimed at load manipulation. Additionally, strategic adjustments in market clearing intervals and timing serve to further complicate attackers' synchronization with market operations, thereby safeguarding economic stability and fairness [96,97].

3.2.4. Human Layer MTD

Recognizing the critical role of human operators, Human Layer MTD emphasizes orchestrating dynamic defenses through human oversight and interactive control mechanisms [98–100]. Operators empowered by real-time situational awareness can engage in manual triggering of defense actions, proactively initiating MTD measures in response to emergent threats or anomalies. Furthermore, structured but adaptive playbooks offer operators predefined yet randomized defensive scenarios, enhancing their ability to rapidly and effectively respond without predictable patterns [101]. To ensure operators remain adept at managing dynamic scenarios, MTD emphasizes continuous training and simulation exercises, fostering familiarity and competence with rapidly changing operational landscapes. This human-centered approach ensures that MTD deployments remain operationally safe, context-aware, and adaptable to unexpected circumstances [102].

3.3. Design Trade-Offs: Security Gains vs. Operational Overhead

3.3.1. Security Benefits of Implementing MTD

Deploying Moving Target Defense across cyber, physical, market, and human layers significantly enhances the security posture of Power CPS [103–105]. Foremost, MTD strategies substantially increase attacker uncertainty, disrupting their reliance on stable, predictable system configurations. By introducing continual variations, adversaries are forced to operate under conditions of incomplete and frequently obsolete information, dramatically lowering the probability of successful exploitation [106,107]. Another critical advantage is the pronounced reduction in the exploit window, limiting the duration for which any discovered vulnerability remains actionable. Frequent changes rapidly invalidate attacker reconnaissance data and disrupt persistent footholds, thus significantly shortening attackers' opportunities to cause sustained harm [108]. Additionally, the continuous adaptive nature of MTD strategies results in considerably higher attacker costs, both in terms of operational complexity and resource allocation, effectively deterring prolonged or large-scale attack campaigns by increasing the probability of detection and failure [109–120].

3.3.2. Operational Challenges Associated with MTD

Despite these substantial security benefits, deploying dynamic MTD mechanisms across multiple domains inherently introduces operational challenges [121–123]. One primary concern is the potential risk to system stability, particularly prevalent in the physical domain, where frequent grid reconfigurations or control-mode switching could inadvertently destabilize operational processes or create unforeseen vulnerabilities. Another significant challenge is the increased complexity arising from maintaining, monitoring, and managing dynamically changing configurations [124]. Such complexity demands advanced, real-time situational awareness tools and rigorous operator training to ensure that these dynamic defenses remain transparent, manageable, and operationally sound [125]. Furthermore, the necessity for cross-domain coordination introduces additional overhead, requiring precise synchronization among cyber, physical, market, and human layers. This complexity demands sophisticated orchestration frameworks and robust inter-domain communication to maintain cohesive defensive operations without disrupting routine activities [126–128].

 doi:10.20944/preprints202506.0030.v1

3.3.3. Strategically Balancing Defense Effectiveness and Operational Integrity

Successful implementation of Multi-Domain MTD requires carefully balancing enhanced security with the maintenance of operational reliability and compliance [129]. Strategic design considerations must ensure that dynamic configuration changes neither compromise system reliability nor violate regulatory standards and compliance frameworks. Critical to achieving this balance is ensuring transparency and controllability of defense actions by human operators. Operators must have clear insights into the rationale, expected outcomes, and potential impacts of any proposed dynamic adjustment, supported by advanced, explainable decision-support systems [130]. Furthermore, to mitigate operational disruptions, real-time system performance must be continuously monitored, validated, and managed, enabling operators to rapidly identify and rectify any unintended consequences of defensive actions. By thoughtfully addressing these trade-offs, Multi-Domain MTD can be deployed safely and effectively, significantly enhancing overall system resilience against sophisticated cyber-physical adversaries [131–133].

A summary of MTD principles and their associated trade-offs is presented in Table 2.

Table 2. Summary of MTD Principles and Trade-offs.

MTD Domain	Example Strategies	Security Benefits	Operational Challenges
Cyber Layer	IP randomization, dynamic routing, rotating keys	Disrupts reconnaissance and persistence	Network management complexity, potential latency impacts
Physical Layer	Grid reconfiguration, DER mode switching, virtual islanding	Localizes disruptions, prevents single-point-of-failure attacks	Grid stability risks, coordination with physical operations
Market Layer	Variable market rules, dynamic clearing times	Thwarts market manipulation attempts	Regulatory compliance, market participant acceptance
Human Layer	Adaptive playbooks, operator-in-the-loop control	Ensures oversight and reduces automation risks	Training and cognitive load on operators

4. MTD Strategies for Cyber Layer Protection

The cyber layer forms the digital backbone of Power CPS, encompassing communication networks, data protocols, control platforms, and digital interfaces that enable real-time grid monitoring and management [134,135]. This layer is highly exposed to cyber intrusions, persistent reconnaissance, and protocol-specific exploits, especially when system configurations remain static.

This section introduces cyber-specific MTD strategies designed to continuously alter the digital attack surface, thereby increasing attacker uncertainty and reducing exploitation success rates.

4.1. Dynamic Network Reconfiguration and IP Randomization

4.1.1. Conceptual Rationale and Importance

Dynamic network reconfiguration and IP randomization represent widely recognized and extensively implemented MTD techniques within network security [136]. In traditional Power CPS, critical infrastructure assets—including substations, DER controllers, and supervisory control and data acquisition (SCADA) systems—often utilize static network addresses and fixed network configurations [137–139]. These static attributes provide attackers with stable, easily discoverable targets for systematic reconnaissance and persistent surveillance [140].

By periodically randomizing IP addresses and dynamically altering network topologies, defenders proactively disrupt the attackers' operational models [141–143]. These methods effectively invalidate existing attacker reconnaissance, abruptly terminate persistent connections from compromised devices, and compel attackers into repeated cycles of re-scanning and reconnaissance. Consequently, attackers face substantially elevated operational costs, decreased efficiency, and increased detection likelihood [144–146].

4.1.2. Technical Implementation and Methodologies

 doi:10.20944/preprints202506.0030.v1

Several well-established methodologies enable the realization of these dynamic strategies:

- **IP Hopping**: Periodically assigning new IP addresses to networked devices at randomized intervals, preventing attackers from reliably tracking device locations over time and disrupting persistent targeted attacks [147].
- **Network Address Translation (NAT) Randomization**: Continuously modifying external-to-internal IP mappings while ensuring internal network consistency. This approach complicates attacker attempts at accurately identifying and targeting critical assets through external scanning [148].
- **Topology Obfuscation**: Altering logical network architectures, such as shifting among mesh, ring, star, or hybrid topologies. Regularly changing network structures prevents attackers from forming durable models of the system's communication pathways and dependencies, significantly complicating network-based attacks [149,150].

4.1.3. Operational Considerations and Practical Challenges

Despite their defensive advantages, these dynamic techniques pose several critical operational considerations. Effective network reconfiguration necessitates precise synchronization to maintain session continuity and avoid operational disruptions [151–153]. Without careful management, poorly timed IP or topology changes could result in increased latency, packet loss, or interruptions in critical control communications. Furthermore, compatibility with legacy infrastructure presents another considerable challenge; older SCADA and control devices might lack the requisite capabilities to handle dynamic address resolution protocols or frequent reconfiguration commands, requiring either substantial upgrades or the introduction of hybrid solutions that balance legacy and modern components seamlessly [154–156].

4.2. Rotating Authentication and Key Management Protocols

4.2.1. Conceptual Rationale and Security Justification

Static cryptographic keys and unchanging authentication credentials constitute prevalent targets for attackers employing brute-force attacks, dictionary attacks, credential stuffing, or sophisticated cryptographic exploits [157–159]. Regular rotation of keys and credentials fundamentally mitigates these risks by continuously limiting the temporal validity of compromised credentials, drastically reducing attacker opportunities for prolonged exploitation [160]. Furthermore, frequent credential rotations compel attackers to persistently expend significant effort reacquiring valid credentials, thereby heightening their resource expenditures and exposure to detection [161–163].

4.2.2. Advanced Technical Implementation Strategies

Several robust techniques underpin effective key management practices in dynamic environments:

- **Time-Based Key Rotation**: Implementing scheduled and predictable rotations of cryptographic keys to ensure that any compromised credentials swiftly become obsolete, minimizing exploitation windows [164].
- **Event-Driven Key Changes**: Triggering immediate and proactive key updates in response to identified anomalies, potential security breaches, or significant policy modifications, thereby containing emergent threats swiftly [165].
- **Distributed Key Management**: Utilizing blockchain-based or federated key distribution systems to enhance resilience against centralized attacks, eliminate single points of compromise, and ensure secure and decentralized credential management across geographically dispersed grid assets [166,167].

4.2.3. Operational Considerations and Management Challenges

 doi:10.20944/preprints202506.0030.v1

Efficient management of dynamic key rotations involves meticulous planning and significant operational oversight. The secure and timely distribution of keys poses logistical and technical overhead, necessitating sophisticated key management infrastructure to avoid disruptions in critical services [168,169]. Additionally, seamless transitions during key updates are critical to maintaining continuous operations, demanding rigorous adherence to industry standards such as IEC 62351, which specifies requirements for secure communications in power systems. Failure to comply with such standards can introduce vulnerabilities and undermine the entire authentication infrastructure [170].

4.3. Control Path Diversity and Switching Strategies

4.3.1. Conceptual Rationale and Necessity

Typical control communications within Power CPS follow predictable, predefined network paths, presenting attackers with stable targets for interception, man-in-the-middle attacks, or injection-based sabotage [171]. Implementing diversity and dynamic switching strategies in control communication paths disrupts attackers' assumptions and complicates their planning by continuously altering the routes through which critical control commands travel [172].

4.3.2. Innovative Techniques and Implementation Approaches

The realization of control path diversity encompasses multiple advanced approaches:

- **Multi-Channel Control Communication**: Employing parallel and redundant communication channels (e.g., fiber optics, LTE, satellite) for the transmission of critical control signals, ensuring resilience against single-channel failures or targeted disruptions [173].
- **Random Path Selection**: Dynamically and probabilistically selecting communication routes based on real-time network conditions, threat intelligence, or randomized policies, thereby continuously invalidating attackers' surveillance and path interception efforts [174].
- **Protocol Switching**: Alternating among secure communication protocol variants (such as IEC 60870-5-104 and DNP3 Secure Authentication) to prevent attackers from reliably exploiting known protocol-specific vulnerabilities, forcing adversaries to continuously adapt their attack methodologies [175].

4.3.3. Operational Considerations and Deployment Challenges

Managing control path diversity introduces operational complexities and performance considerations. Ensuring continuous availability and reliability of alternative communication paths requires significant investments in infrastructure redundancy and robust real-time orchestration tools [176]. Variability in latency and performance across different communication channels demands meticulous management to maintain system responsiveness. Furthermore, implementing protocol switching strategies requires sophisticated orchestration capabilities and extensive operator training to avoid disruptions arising from protocol mismatches or interoperability issues [177,178].

4.4. Adaptive Service Virtualization and Obfuscation

4.4.1. Conceptual Rationale and Security Advantages

Attackers routinely rely on port scanning and service fingerprinting techniques to systematically map network services, identify vulnerabilities, and target exploitation efforts [179,180]. Adaptive service virtualization and obfuscation methodologies actively mislead adversaries by dynamically altering visible service characteristics and responses, thus introducing considerable uncertainty into attackers' reconnaissance activities [181].

4.4.2. Implementation Strategies and Tactical Techniques

Adaptive obfuscation approaches include several sophisticated methods:

 doi:10.20944/preprints202506.0030.v1

- **Moving Target Honeypots**: Deploying dynamically configurable decoy systems designed to imitate real assets and attract attackers' attention, effectively diverting adversarial efforts away from genuine critical infrastructure [182].
- **Service Masking**: Regularly altering identifiable characteristics of network services—such as banners, port assignments, and signature identifiers—to prevent accurate fingerprinting and complicate attackers' attempts to associate services with known vulnerabilities.
- **Protocol Behavior Variability**: Introducing subtle and controlled randomness into protocol-level interactions and responses to thwart automated exploitation scripts and confuse attackers attempting protocol-specific reconnaissance or exploitation [183].

4.4.3. Operational Risks and Strategic Management Considerations

These obfuscation strategies, while powerful, also carry the potential for operational interference. Introducing dynamic and deceptive service characteristics may inadvertently disrupt legitimate network diagnostics or asset management tools that rely on stable service identities [184–186]. Additionally, running honeypots and maintaining adaptive obfuscation introduces non-negligible computational and network resource overhead. Thus, careful orchestration and clear separation of genuine and deceptive assets are critical, necessitating advanced management frameworks capable of reliably differentiating legitimate operator requests from adversarial probes [187,188].

A summary of cyber layer MTD strategies is presented in Table 3.

Table 3. Summary of Cyber Layer MTD Strategies.

MTD Strategy	Security Benefits	Operational Considerations
Dynamic Network Reconfiguration	Disrupts attacker reconnaissance and persistence	Requires synchronization and may impact session continuity
Rotating Authentication and Keys	Limits credential reuse and theft	Requires secure and seamless key distribution mechanisms
Control Path Diversity and Switching	Prevents predictable attack paths	Increases complexity in managing network and protocol diversity
Service Virtualization and Obfuscation	Misleads attackers and absorbs attack attempts	Requires careful management to avoid operational confusion

In summary, cyber-layer MTD strategies offer powerful tools to disrupt attacker planning and execution, but they must be carefully integrated into operational workflows to maintain system reliability. The next section extends this discussion to physical and market layer MTD strategies, which further broaden the defensive posture of Power CPS.

5. MTD Strategies for Physical and Market Layer Protection

While cyber-layer MTD strategies primarily address digital attack surfaces, physical and market layers present equally critical, yet often overlooked, opportunities for dynamic defense [189]. Static physical configurations—such as fixed grid topologies and operational modes—and predictable market mechanisms provide adversaries with stable targets for physical disruption or economic manipulation [190,191]. This section explores how MTD principles can be extended to these layers, enhancing overall system resilience through topology reconfiguration, market dynamics variation, and adaptive operational strategies.

5.1. Reconfigurable Grid Topologies and Virtual Islanding

5.1.1. Conceptual Rationale and Strategic Significance

Static grid topologies inherently expose Power CPS to predictable vulnerabilities, including single points of failure and cascading outages [192,193]. Attackers often exploit well-known, static grid configurations to propagate failures deliberately, maximizing damage and disruption. MTD

 doi:10.20944/preprints202506.0030.v1

strategies mitigate these risks by introducing deliberate and controlled variability into grid topology. Through periodic reconfiguration, attackers lose their static reference points, complicating their attempts to map critical paths and operational dependencies, thus significantly reducing the likelihood of successful targeted disruptions [194,195].

Additionally, dynamic topological adjustments enable operators to strategically isolate impacted regions via temporary segmentation—referred to as virtual islanding. By containing faults and localizing impacts within controlled segments, cascading effects are effectively curtailed, enhancing overall grid resilience and operational continuity even amidst adversarial disruptions.

5.1.2. Advanced Techniques and Implementation Approaches

- **Dynamic Tie-Line Management**: This involves real-time activation or deactivation of interconnection lines based on ongoing threat assessments or system operational conditions. By strategically controlling these connections, operators can dynamically alter the grid's electrical connectivity, preventing attackers from reliably predicting network states and significantly mitigating cascading failure propagation [196].
- **Virtual Islanding of Microgrids**: Temporarily transitioning microgrids between connected and autonomous islanded states allows localized management of disturbances. By enabling autonomous operation, islanded segments maintain critical functions independently, reducing the potential for widespread disruption and aiding in rapid post-event recovery [197].
- **Reconfigurable Protection Schemes**: Adaptively adjusting protective relay settings and system control policies to match dynamically changing grid topologies. This technique ensures consistent, reliable, and context-sensitive protection across varying operational configurations, safeguarding against erroneous relay actions or protection failures resulting from rapid topological changes [198].

5.1.3. Operational Considerations and Practical Challenges

Frequent topological reconfigurations introduce significant operational challenges, notably risks to system stability, voltage regulation, and frequency control. Ensuring smooth transitions between different configurations necessitates advanced monitoring and rapid-response control systems [199]. Additionally, the coordination complexity escalates, demanding high levels of operator training and situational awareness tools capable of real-time decision support. Regulatory and market constraints may further complicate dynamic reconfiguration strategies, as certain actions—such as islanding—could conflict with existing reliability standards, contractual obligations, and market participation rules, thereby necessitating careful alignment and compliance measures [200].

5.2. Dynamic Market Mechanism Variations to Thwart Economic Attacks

5.2.1. Conceptual Rationale and Economic Security Implications

Energy markets, encompassing day-ahead, real-time, and ancillary service operations, typically employ fixed algorithmic rules and predictable clearing mechanisms [201,202]. Attackers leveraging static market dynamics can execute economically disruptive attacks, such as market manipulation or strategic bidding interference. Introducing controlled variability into market mechanisms—through MTD techniques—actively disrupts attacker modeling and planning, significantly reducing the predictability and thus the vulnerability of economic operations.

By varying market operations dynamically, adversaries lose stable benchmarks for synchronization and manipulation, increasing the operational complexity and uncertainty for potential attackers, and thus safeguarding the integrity and fairness of market transactions [203,204].

5.2.2. Technical Approaches and Implementation Techniques

 doi:10.20944/preprints202506.0030.v1

- **Variable Market Clearing Intervals**: Strategically varying the timing and frequency of market clearing processes disrupts attackers' synchronization, complicating the precise timing required for manipulative bidding or price influencing schemes, and thereby preserving market integrity.
- **Rotating Pricing Algorithms**: Regularly alternating between distinct locational marginal pricing (LMP) methodologies or congestion management strategies prevents adversaries from effectively reverse-engineering and exploiting predictable pricing structures. Such rotations significantly impair attackers' strategic planning capabilities and reduce economic attack feasibility [205].
- **Randomized Demand Response Signals**: Introducing controlled randomization into the timing, duration, and magnitude of demand response (DR) events significantly hinders attackers attempting to exploit predictable load-shifting patterns. This unpredictability safeguards the reliability of demand response mechanisms, ensuring their effectiveness in maintaining grid stability.

5.2.3. Operational Considerations and Stakeholder Implications

Although dynamic market variability offers substantial defensive advantages, it must be balanced against the imperative to maintain market transparency, efficiency, and participant confidence [206]. Excessive variability can potentially be perceived as arbitrary or unfair by legitimate market participants, thus potentially undermining trust and market participation. Regulatory compliance also presents significant considerations, as market rules and operational transparency are typically mandated by regulators. Additionally, the introduction of variability inevitably involves trade-offs in economic efficiency, necessitating careful analysis and design to balance market resilience with economic optimality [207].

5.3. Adaptive Resource Dispatch and Control Mode Switching

5.3.1. Conceptual Rationale and Operational Necessity

Traditional, static resource dispatch schedules and DER control settings offer attackers predictable operational patterns, providing opportunities for precise timing attacks aimed at disrupting or destabilizing power system operations. Adaptive resource dispatch and dynamic DER control mode switching directly counter these threats by continuously altering operational baselines, thereby complicating attacker efforts to accurately model and predict grid behavior [208,209].

Dynamic operational adjustments not only impede adversarial exploitation efforts but also enhance overall operational flexibility, empowering operators to rapidly respond to evolving threats or emergent operational conditions with adaptive dispatch and control mode adjustments [210].

5.3.2. Advanced Implementation Techniques

- **Dynamic DER Mode Switching**: Alternating DER operational modes—such as voltage regulation, frequency support, and power factor correction—in response to real-time grid conditions and threat intelligence. This variability significantly complicates adversarial targeting, while simultaneously optimizing grid performance under fluctuating conditions.
- **Adaptive Dispatch Scheduling**: Introducing controlled yet systematic variability into power generation dispatch orders and ramping sequences to prevent attackers from exploiting fixed or repetitive scheduling patterns. This approach enhances operational security without significantly compromising dispatch efficiency.
- **Real-Time Re-Optimization**: Continuously updating Optimal Power Flow (OPF) solutions based on real-time situational assessments, threat intelligence, and changing operational objectives. This approach maintains optimized and secure grid operation in dynamically evolving threat landscapes, ensuring robustness against targeted disruptions.

5.3.3. Operational Challenges and Practical Implementation Issues

 doi:10.20944/preprints202506.0030.v1

Implementing adaptive resource dispatch and control mode switching introduces notable operational challenges, including increased computational complexity and coordination overhead. Real-time re-optimization and frequent mode changes require substantial computational resources and sophisticated coordination mechanisms to maintain operational reliability and performance consistency [211]. Improper synchronization or overly aggressive mode transitions could inadvertently cause operational instability or control oscillations. Consequently, successful deployment of these adaptive strategies mandates robust, real-time visualization and decision-support tools, extensive operator training, and clearly defined procedural guidelines, ensuring operators effectively manage and safely execute dynamic operational actions [212].

A summary of MTD strategies in the physical and market layers is presented in Table 4.

Table 4. Summary of Physical and Market Layer MTD Strategies.

MTD Strategy	Security Benefits	Operational Considerations
Reconfigurable Grid Topologies & Islanding	Limits propagation of failures; invalidates attacker topology models	Requires careful stability management and cross-layer coordination
Dynamic Market Mechanism Variations	Disrupts economic manipulation attempts	Must balance fairness, transparency, and market efficiency
Adaptive Dispatch & Control Mode Switching	Reduces predictability of operational behaviors	Increases control and optimization complexity; requires operator oversight

In summary, physical and market layer MTD strategies extend the defense perimeter beyond cyber infrastructure, enabling cross-layer resilience that addresses both operational and economic threat surfaces. The next section will introduce human-in-the-loop and AI-augmented orchestration frameworks to coordinate these multi-domain MTD strategies effectively.

6. Human-in-the-Loop and AI-Augmented MTD Coordination

While MTD introduces dynamic adaptability to Power CPS, effective coordination of MTD strategies presents significant operational challenges. Uncoordinated or overly aggressive MTD actions risk service disruption, system instability, or operator disorientation. To balance defense effectiveness with operational reliability, Power CPS require human-in-the-loop (HITL) orchestration frameworks, supported by AI-driven monitoring and decision support tools. This section discusses the roles of human operators, AI-based orchestration, and explainable interfaces in managing safe and adaptive MTD deployments [213].

6.1. Operator-Centered MTD Orchestration Platforms

6.1.1. Significance of Human Oversight

While automated MTD mechanisms offer rapid response capabilities and adaptability, the role of human operators remains critically indispensable. Humans possess unique capabilities in evaluating nuanced contextual information, exercising judgment in ambiguous situations, and ensuring that automated defense measures align with broader operational safety and regulatory requirements. Specifically, human operators play a crucial role in verifying the practical feasibility and safety of proposed MTD actions, particularly when automated systems lack comprehensive situational context or risk introducing unintended operational disruptions. Furthermore, operators are vital for managing complex, cross-domain coordination across cyber, physical, market, and human layers, ensuring holistic synchronization and coherent strategy implementation. In emergency or unexpected scenarios, operators can decisively override automated recommendations, safeguarding system integrity and reliability [214,215].

6.1.2. Key Functional Capabilities of Operator-Centric Platforms

 doi:10.20944/preprints202506.0030.v1

- **Situational Awareness Dashboards**:
  Advanced visualization platforms present operators with real-time, intuitive displays of current system conditions, active MTD strategies, operational risks, and evolving threat landscapes. These dashboards significantly enhance operators' capability to rapidly comprehend complex dynamics, enabling swift and informed decision-making.
- **MTD Playbook Management**:
  Interactive tools allow operators to select, tailor, and deploy pre-validated dynamic defense strategies quickly and effectively. These playbooks support structured yet adaptable defense execution, empowering operators to respond proactively while ensuring consistency and reliability in operational processes.
- **Risk-Benefit Analysis Tools**:
  Decision-support modules systematically evaluate the operational implications and defensive effectiveness of potential MTD actions, providing transparent, data-driven recommendations. These tools enable operators to explicitly weigh operational risks against anticipated security benefits, thereby facilitating informed and strategic decision-making.
- **Collaboration and Communication Platforms**:
  Integrated platforms foster seamless coordination and effective communication among diverse teams spanning cyber-security, operational control, and market management domains. These collaborative tools enhance shared situational understanding, streamlining the coordinated implementation of complex, multi-layered MTD actions.

6.2. AI-Driven Attack Surface Monitoring and Adaptive Strategy Selection

6.2.1. Real-Time Attack Surface Monitoring

Advanced artificial intelligence (AI) techniques significantly enhance system resilience by continuously assessing and adapting to evolving threat landscapes. Real-time AI-driven monitoring tools provide comprehensive visibility of current attack surfaces, meticulously tracking network configurations, service exposure, communication pathways, and system configurations. By proactively identifying static and vulnerable elements within the network that may benefit from immediate reconfiguration, AI-based monitoring substantially mitigates potential attack vectors, providing operators with actionable intelligence drawn from real-time threat indicators [216].

6.2.2. Adaptive Selection of MTD Strategies

Employing sophisticated AI methodologies, such as reinforcement learning (RL) and multi-objective optimization algorithms, MTD platforms dynamically determine the most effective defense actions under varying operational contexts. These AI algorithms rigorously balance the inherent trade-offs between security enhancement and operational continuity, considering real-time constraints, system stability, and resource availability. Additionally, AI systems continuously refine their strategic recommendations through iterative learning from observed outcomes and operator feedback, ensuring sustained adaptability and effectiveness [217].

6.2.3. Human-in-the-Loop Validation for Strategic Decision-Making

Given the critical nature of operational decisions, AI recommendations must maintain transparency and interpretability to secure operator trust and validation. Platforms incorporating explainable AI methodologies enable operators to fully comprehend the rationale behind suggested actions, simulate and visualize potential operational impacts, and explicitly review and adjust recommended strategies prior to deployment. This human-centric validation mechanism ensures that dynamic defense actions align with safety standards, regulatory compliance, and practical feasibility [218].

6.3. Explainable MTD Recommendations for Operator Trust and Validation

 doi:10.20944/preprints202506.0030.v1

6.3.1. Necessity of Explainable AI (XAI) in Critical Environments

In safety-critical systems such as Power CPS, operators are typically hesitant to adopt recommendations from opaque, "black-box" AI systems. Consequently, ensuring the interpretability and transparency of AI-driven decisions is paramount. XAI methods foster operator trust by clearly elucidating the reasoning behind specific MTD recommendations, explicitly highlighting operational implications, security benefits, and potential risks [219].

6.3.2. Innovative Techniques for Providing Explainability

- **Feature Attribution Analysis**: Clearly identifying and visualizing specific system parameters, configurations, or threat indicators that significantly influenced the AI's recommendation. Operators thus clearly understand the decision-making factors and can quickly assess recommendation validity.
- **Counterfactual Scenario Analysis**: Demonstrating hypothetical alternative outcomes if different defense actions had been selected or avoided. This analysis provides operators with comparative insights, enabling them to clearly grasp the necessity and potential consequences of chosen strategies.
- **Visual Impact Simulations**: Graphically illustrating projected system states before and after implementing recommended MTD actions. Visual simulations facilitate intuitive understanding of potential operational impacts and enable effective risk assessment by operators.
- **Interactive What-If Tools**: Allowing operators to dynamically explore alternative MTD actions and their implications in a controlled, virtual environment. Such interactive exploration empowers operators to systematically evaluate and confidently validate recommended actions, significantly enhancing operational trust and decision-making effectiveness [220].

6.4. Feedback Loops for Continuous MTD Refinement

6.4.1. Integration of Operator Feedback

Sustaining the efficacy and relevance of MTD mechanisms requires iterative and continuous refinement. Real-time operator feedback, drawn from actual operational experiences, provides invaluable insights into the practical effectiveness, operational safety, and unforeseen challenges associated with specific MTD implementations. Operators actively contribute by highlighting unexpected outcomes, identifying unintended operational disruptions, and suggesting improvements derived from direct field experience [221].

6.4.2. Adaptive AI Learning from Feedback

Leveraging advanced adaptive learning frameworks, AI systems incorporate operator feedback to continuously refine underlying attack surface models, strategy selection algorithms, and recommendation logic. This continuous learning paradigm ensures ongoing enhancement of defensive effectiveness, operational resilience, and human-AI collaboration quality. Adaptive AI mechanisms thus become increasingly attuned to practical operational considerations, significantly improving their strategic relevance, decision accuracy, and operator acceptance over time [222].

Through the integration of continuous feedback loops, explainable interfaces, and robust human oversight, human-in-the-loop and AI-augmented MTD orchestration frameworks provide a comprehensive and adaptive defensive posture, ensuring optimal balance between dynamic security measures and operational stability within Power CPS environments.

A summary of human-in-the-loop and AI-augmented MTD coordination approaches is presented in Table 5.

Table 5. Summary of Human-in-the-Loop and AI-Augmented MTD Coordination.

 doi:10.20944/preprints202506.0030.v1

Coordination Component	Key Capabilities	Operational Benefits
Operator-Centered Orchestration Platforms	Interactive dashboards, playbooks, and decision support tools	Ensures human oversight and cross-domain coordination
AI-Driven Monitoring and Strategy Selection	Real-time attack surface mapping and adaptive MTD recommendations	Enhances defense agility while balancing operational constraints
Explainable MTD Interfaces	Transparent explanations, impact simulations, and what-if analysis	Builds operator trust and facilitates informed decision-making
Feedback Loops for Continuous Refinement	Integration of operator feedback into AI learning processes	Improves long-term system resilience and human-AI collaboration

In summary, human-in-the-loop and AI-augmented orchestration frameworks are critical for safe, effective, and trustworthy MTD deployment in Power CPS. These frameworks enable dynamic defense without compromising operational stability or human control.

7. Validation Platforms, Metrics, and Real-World Deployment Challenges

While MTD offers promising strategies for dynamic and adaptive defense, realizing these capabilities in operational Power CPS requires rigorous validation and careful consideration of deployment challenges. This section outlines the requirements for validation platforms, proposes resilience metrics, and discusses practical barriers to real-world adoption, including scalability, interoperability, and human factors [223,224].

7.1. Digital Twin and Co-Simulation-Based MTD Validation

7.1.1. Strategic Role of Digital Twins in MTD Evaluation

Digital twins, representing precise, real-time virtual counterparts of physical power systems, offer an indispensable validation environment for MTD strategies. By replicating complex system dynamics accurately, digital twins provide operators and researchers a secure, controllable, and highly realistic testbed. Crucially, these digital replicas facilitate rigorous experimentation involving attack-defense scenarios without endangering operational stability of actual physical infrastructures. Moreover, advanced digital twins enable comprehensive, multi-layer modeling, effectively capturing intricate interdependencies among cyber, physical, market, and human dimensions of Power CPS. Through detailed, scenario-driven experimentation, operators can validate the efficacy and feasibility of proposed MTD strategies under realistic and diverse operational conditions, significantly enhancing confidence before practical deployment [225].

7.1.2. Multi-Domain Co-Simulation Frameworks

Effective validation of MTD necessitates integrated co-simulation platforms that harmonize disparate modeling domains, including power system simulators, network emulators, market operation models, and human-interaction simulators. Such co-simulation environments enable operators to assess cross-layer impacts and interactions in real time, effectively evaluating MTD strategies through comprehensive end-to-end resilience tests. Real-time operator-in-the-loop simulations further allow for nuanced validation, considering human decision-making behaviors and operational responses to dynamic defensive measures [226].

7.1.3. Representative Validation Scenarios

- **Topology Reconfiguration Stress Tests**: Evaluating the stability implications and grid performance under frequent and dynamic switching of grid topology and virtual islanding configurations, highlighting critical thresholds for operational reliability and safety.

 doi:10.20944/preprints202506.0030.v1

- **Market Manipulation Defense Simulations**: Testing robustness of randomized market mechanisms against sophisticated economic attacks and manipulative behaviors, providing insights into trade-offs between economic efficiency and defensive variability.
- **Human-AI Collaboration Exercises**: Examining operator acceptance, decision effectiveness, and operational efficiency in scenarios involving explainable AI recommendations, ensuring seamless integration of human judgment and AI-driven defense strategies.

7.1.4. Challenges to Realism in Simulation

Despite their significant utility, digital twin and co-simulation approaches face critical limitations. Achieving sufficient model fidelity remains challenging, as overly simplified simulations might inadequately reflect the intricate complexities of operational environments. Additionally, robust calibration and validation of digital twins demand high-quality, real-world data, which are often scarce or restricted due to privacy and security considerations. Scalability is another significant concern, as comprehensive simulations involving extensive grid systems require considerable computational resources, often necessitating dedicated high-performance computing infrastructures [227].

7.2. Resilience and Effectiveness Metrics for MTD Strategies

Beyond Traditional Security Metrics

Traditional cybersecurity metrics—such as detection accuracy or false-positive rates—fail to adequately capture the systemic and dynamic nature of MTD strategies. A more sophisticated and comprehensive set of resilience metrics is imperative to assess the broader impacts of MTD on Power CPS security and operational continuity. Metrics must extend beyond mere detection efficacy, encompassing attacker disruption effectiveness, system adaptability, operational resilience, and human factors such as operator trust and usability [228].

Proposed Advanced Metrics

- **Security Effectiveness**: Evaluating attacker time-to-compromise, required attacker resources, and degree of disruption to adversarial planning and operational effectiveness, providing a nuanced measure of defensive success.
- **Operational Impact**: Quantifying service continuity and stability under dynamic defense conditions, including performance degradation indices, latency impacts, and overall operational resilience during defense activations.
- **Adaptability and Flexibility**: Tracking the frequency and effectiveness of successful defense adaptations to evolving threats, as well as measuring system learning rates and responsiveness to new operational contexts.
- **Human Factors**: Gauging operator acceptance, decision confidence levels, cognitive workload, and usability metrics, ensuring that dynamic defense implementations remain practically manageable and operationally accepted.

A summary of the proposed metrics is presented in Table 6.

Table 6. Proposed Metrics.

Metric Category	Example Metrics
Security Effectiveness	Attacker time-to-compromise, attacker resource cost
Operational Impact	Service continuity rate, performance degradation index
Adaptability and Flexibility	Frequency of successful defense adaptations, learning rate
Human Factors	Operator acceptance rate, decision confidence levels

 doi:10.20944/preprints202506.0030.v1

7.3. Scalability, Performance, and Usability Considerations for Deployment

7.3.1. Addressing Scalability Challenges

Successful real-world MTD deployment demands robust scalability, capable of accommodating large, heterogeneous power grids with extensive numbers of nodes, diverse generation resources, and complex interconnections. Effective scalability requires advanced computational resources and sophisticated algorithms to manage real-time monitoring, strategy selection, and cross-domain coordination without compromising system responsiveness or stability [229].

7.3.2. Ensuring Real-Time Performance

Critical infrastructures necessitate MTD strategies that can promptly respond to emerging threats without introducing detrimental delays or operational interruptions. Balancing real-time constraints with computationally intensive decision-making processes demands optimized algorithms and infrastructure that prioritize operational responsiveness alongside defense efficacy.

7.3.3. Prioritizing Usability and Human Factors

Human operators play a pivotal role in dynamic defense management, necessitating interfaces designed for clarity, intuitive use, and minimized cognitive load. Continuous operator education, reinforced through realistic training simulators, remains essential for maintaining operator preparedness and competence. Ensuring organizational alignment, including buy-in from operations teams, IT departments, market operators, and regulatory bodies, is crucial for successful practical adoption and sustained effectiveness of MTD strategies [230].

7.4. Regulatory and Standardization Barriers

7.4.1. Alignment with Industry Standards

Effective deployment of dynamic defense strategies must align with prevailing industry standards, such as the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) and International Electrotechnical Commission (IEC) 62351. Compliance with these standards ensures interoperability, operational transparency, and trustworthiness of MTD deployments within the broader regulatory and operational landscape [231].

7.4.2. Certification and Validation Pathways

Currently, formal certification frameworks specifically tailored for dynamic and adaptive defense mechanisms in critical infrastructures remain underdeveloped, leading to regulatory uncertainty and increased hesitancy among utility stakeholders. The absence of clear certification processes may heighten regulatory risks, deterring utilities from adopting potentially disruptive or unproven MTD approaches due to concerns about non-compliance or operational penalties [232].

7.4.3. Recommendations for Policy Evolution and Industry Collaboration

Overcoming these regulatory barriers necessitates proactive engagement with regulatory bodies from early stages of MTD strategy development. Collaborative efforts must define acceptable practices, develop standardized validation methodologies, and establish clear metrics for assessing MTD performance and reliability. Demonstrating tangible operational benefits through pilot projects and controlled field trials will provide robust, evidence-based arguments supporting the adoption and integration of MTD strategies. Moreover, active participation with industry standards organizations to formalize and disseminate comprehensive guidelines and best practices will further facilitate regulatory acceptance and widespread industry adoption [233].

A summary of validation and deployment considerations is presented in Table 7.

Table 7. Summary of Validation and Deployment Considerations.

 doi:10.20944/preprints202506.0030.v1

Validation and Deployment Aspect	Key Considerations
Validation Platforms	Digital twins, co-simulation, scenario-based testing
Resilience Metrics	Effectiveness, operational continuity, adaptability, human factors
Scalability and Performance	Real-time responsiveness, computational efficiency, large-scale applicability
Usability and Human Factors	Operator training, cognitive load management, stakeholder coordination
Regulatory and Standardization Alignment	Compliance with industry standards, development of certification pathways

In summary, while MTD offers promising avenues for enhancing Power CPS security, rigorous validation and thoughtful deployment planning are essential to ensure safe, effective, and scalable adoption. The final section will outline future research priorities and cross-sector collaboration opportunities to accelerate the transition of MTD from concept to practice.

8. Future Research Directions and Cross-Sector Collaboration

While MTD offers a transformative shift toward proactive, adaptive security for Power CPS, significant research and collaboration gaps remain. Addressing these gaps will require coordinated efforts across academia, industry, government, and standards bodies. This section outlines key research priorities, cross-sector collaboration pathways, and recommendations for operationalizing MTD at scale.

8.1. Theoretical and Practical Gaps in Multi-Domain MTD

8.1. Need for Unified Multi-Domain MTD Frameworks

Current MTD research remains largely fragmented, with most studies focusing on single domains—particularly the cyber layer—while neglecting the critical interdependencies that exist across physical, market, and human dimensions within Power CPS. This siloed approach limits the systemic effectiveness of MTD. Future research must therefore prioritize the development of holistic, cross-layer MTD frameworks capable of:

- Capturing and modeling interconnected dependencies among infrastructure layers.
- Balancing the often conflicting objectives of cybersecurity, grid reliability, and economic efficiency.
- Incorporating human-in-the-loop coordination to ensure the practical feasibility and operator acceptance of dynamic strategies.

Such integrated frameworks would provide a foundational architecture for designing, analyzing, and deploying MTD at system scale while maintaining operational resilience and regulatory compliance.

8.2. Formal Modeling of MTD Effectiveness and Trade-Offs

There is a pressing need for formal, quantitative models that can capture and evaluate the effectiveness of various MTD strategies under realistic constraints. These models should aim to:

- Characterize the evolution of attack surfaces as a function of deployed MTD techniques.
- Quantify security-performance trade-offs, evaluating how changes in configuration improve security while affecting system latency, cost, or service quality.
- Simulate adversarial adaptation dynamics, enabling defenders to anticipate how intelligent attackers may respond and evolve in the presence of moving targets.

Such rigorous modeling will support data-driven strategy design and provide the analytical backbone for comparative performance evaluations.

8.3. Standardization and Benchmarking of Resilience Metrics

 doi:10.20944/preprints202506.0030.v1

At present, the absence of standardized metrics to evaluate the impact of MTD strategies remains a significant bottleneck. Research must focus on the development and consensus-building of resilience indicators, including:

- Core MTD effectiveness metrics, such as attacker resource cost, disruption potential, and exploit longevity.
- Benchmarking frameworks that enable comparative evaluations of different MTD architectures under standardized test scenarios.
- Performance baselines for various grid configurations and threat models to support reproducibility and cross-institutional comparison.

Establishing a standardized metric suite will be critical for guiding research, validating prototypes, and achieving regulatory recognition.

8.2. Integration with Regulatory and Market Frameworks

8.2.1. Challenges to Regulatory Acceptance

A significant obstacle to MTD deployment lies in its limited alignment with existing regulatory frameworks. Current standards, such as NERC CIP and IEC 62351, emphasize static controls and deterministic compliance measures. The lack of regulatory precedent for adaptive, dynamic defenses creates uncertainty and risk aversion among utility stakeholders, who may fear penalties for deviating from compliance norms—even if such deviations are motivated by improved security.

8.2.2. Policy Recommendations for Enabling MTD Adoption

- **Collaborative Policy Development:** Early engagement with regulators, utilities, and researchers is essential to co-develop MTD-specific guidelines that clarify acceptable practices, define boundaries, and integrate dynamic security into regulatory frameworks.
- **Operational Demonstrations and Pilots:** Field trials and sandbox demonstrations provide empirical evidence of MTD's operational benefits and feasibility. These pilots can serve as reference models to inform policy and encourage incremental regulatory inclusion.
- **Regulatory Sandbox Environments:** Regulatory sandboxes allow utilities to test and refine MTD strategies in controlled, consequence-free settings, enabling iterative learning and reducing the risk of penalties while innovation occurs.

Together, these approaches offer a path toward regulatory transformation that both respects existing compliance structures and enables future-ready adaptive defense mechanisms.

8.3. Roadmap for Cross-Sector Implementation and Standardization

8.3.1. Multi-Stakeholder Collaboration Models

Realizing the full potential of MTD requires coordinated action across academia, industry, government, and standardization bodies. Key mechanisms include:

- **Industry-Academic Consortia**: Joint research centers that focus on applied MTD development, supported by utility testbeds and academic expertise.
- **Public-Private Partnerships**: Government-backed initiatives that fund operational MTD pilots and foster cross-sector knowledge transfer.
- **Standards Development Organizations**: Bodies such as IEEE, IEC, and NERC must be actively engaged to formalize MTD best practices, develop interoperable protocols, and define certification criteria.

8.3.2. Knowledge-Sharing Platforms and Open Innovation

 doi:10.20944/preprints202506.0030.v1

- **Threat Intelligence Sharing**: Establishing secure, cross-sector platforms for disseminating information about emerging attack patterns, MTD case studies, and deployment lessons learned.
- **Open-Source MTD Toolkits**: Supporting community-driven development of reusable MTD components—such as simulation frameworks, playbooks, and orchestration engines—to lower adoption barriers and accelerate innovation.

8.3.3. International Cooperation and Grid Resilience Alignment

With energy systems increasingly operating across national and regional boundaries, MTD standardization must be globally coordinated. Key opportunities include:

- **Alignment of Global Standards**: Harmonizing MTD definitions, metrics, and compliance requirements across jurisdictions to support multinational grid operations.
- **Cross-Border Resilience Programs**: Joint development of transnational defense strategies for interconnected grids vulnerable to spillover effects from cross-border cyber or physical attacks.

8.4. Emerging Research Opportunities

8.4.1. AI-Driven MTD Strategy Optimization

Future research should prioritize the development of autonomous, intelligent agents capable of dynamically co-evolving MTD strategies in real time. These AI-driven systems must be able to integrate live threat intelligence feeds and system telemetry, enabling continuous situational awareness. Moreover, they should possess the ability to learn iteratively from both operator feedback and observed system responses, thereby refining their strategy selection over time. Optimization should consider multiple competing objectives—such as security effectiveness, operational cost, and system latency—to ensure that defense actions remain balanced and adaptive. Such real-time, context-aware AI agents will be crucial for maintaining robust and responsive defense postures in the face of evolving and sophisticated threats [234].

8.4.2. Behavioral MTD and Human Deception Engineering

While conventional MTD strategies primarily focus on introducing technical unpredictability, emerging research suggests promising directions in behavioral deception, targeting the human cognition of adversaries. This includes the strategic dissemination of misinformation to distort attacker reconnaissance and impair situational awareness. In parallel, deploying dynamic honeynets—configured as moving targets—can lure and analyze attacker behavior in real time, enhancing intelligence gathering while misleading adversaries. Additionally, psychological decoys can be used to manipulate attacker expectations about system topology or operational states. These techniques shift MTD from purely technical disruption to influencing the attacker's decision-making processes, opening a novel and underexplored front in cyber-physical defense [235].

8.4.3. Federated MTD for Distributed Grids

As energy infrastructures become increasingly decentralized—with the rise of microgrids, DERs, and VPPs—there is a growing need for federated MTD frameworks. Such approaches involve distributed entities collaboratively learning and implementing defense strategies without sharing raw or sensitive data, preserving privacy while enhancing collective resilience. Federated learning architectures can enable these decentralized agents to co-train robust models against emerging threats [235–237]. Moreover, hierarchical coordination mechanisms will be essential to ensure

 doi:10.20944/preprints202506.0030.v1

consistency and synchronization of MTD actions across multi-layered control architectures, allowing local autonomy while maintaining global coherence in distributed grid environments.

8.4.4. Digital Twin-Enhanced Operator Training and Simulation

To ensure operators are well-prepared to manage increasingly dynamic and AI-augmented defense strategies, future research should focus on building immersive training and simulation platforms powered by high-fidelity digital twins. These environments can simulate realistic attack-defense scenarios across cyber, physical, and market layers, enabling operators to practice cross-domain coordination and real-time decision-making in a risk-free setting. Integration with AI systems will allow operators to refine their trust calibration and response behaviors under uncertainty, while enabling researchers to continuously assess and improve human-AI interaction dynamics. Ultimately, such platforms will serve as critical tools for capacity building, skill retention, and operational readiness in the face of adaptive threats [238].

A summary of future research and collaboration priorities is presented in Table 8.

Table 8. Summary of Future Research and Collaboration Priorities.

Priority Area	Key Actions
Unified MTD Framework Development	Model cross-layer dynamics, establish standardized metrics
Regulatory and Market Integration	Collaborate on policy evolution, demonstrate operational benefits
Cross-Sector Collaboration	Build consortia, share knowledge, develop open-source toolkits
Emerging Research Directions	Optimize AI-driven MTD, explore behavioral deception, advance digital twin platforms

In summary, realizing the full potential of MTD for Power CPS requires multi-disciplinary research, regulatory engagement, cross-sector collaboration, and international standardization efforts. The concluding section will synthesize these insights and call for a unified effort to operationalize proactive, dynamic, and adaptive grid security.

9. Conclusion

In response to the growing complexity and interdependence of Power CPS, this review has positioned MTD as a transformative paradigm that shifts security from static and reactive to dynamic and proactive. By systematically analyzing threat surfaces across cyber, physical, market, and human layers, we identified how fixed system configurations enable long-term attacker reconnaissance and exploitation. We proposed a multi-domain classification of MTD strategies—ranging from IP randomization and grid reconfiguration to adaptive market mechanisms—and emphasized the critical role of human-in-the-loop and AI-augmented orchestration in ensuring safe, explainable, and effective deployment. Moreover, we underscored the importance of digital twin-based validation, resilience metrics, and scalable deployment architecture to bridge the gap between theoretical innovation and operational feasibility.

Looking forward, the successful operationalization of MTD will depend on coordinated efforts across research, industry, regulation, and international collaboration. Future work must prioritize the development of unified, cross-layer MTD frameworks, formal modeling of dynamic defense trade-offs, and standardization of evaluation metrics. Regulatory adaptation—through sandbox environments, pilot demonstrations, and updated compliance models—will be essential for industry uptake. Meanwhile, emerging research frontiers such as AI-driven defense adaptation, behavioral deception engineering, federated MTD for distributed grids, and immersive digital twin training offer exciting opportunities to further enhance resilience. Ultimately, advancing MTD from concept to practice will be foundational for securing next-generation energy systems against persistent and adaptive threats in an increasingly uncertain cyber-physical landscape.

References

 doi:10.20944/preprints202506.0030.v1

1. Han K, Zhang K, Wang Z P, et al. Resilient predictive load frequency control of multi-area interconnected power systems with privacy preserving and active detection against stealthy cyber attacks[J]. IEEE Internet of Things Journal, 2024.
2. [2 Lakshminarayana S, Chen Y, Konstantinou C, et al. Survey of moving target defense in power grids: Design principles, tradeoffs, and future directions[J]. arXiv preprint arXiv:2409.18317, 2024.
3. Qu Z, Zhao T, Zhang Y, et al. Determination Method of Network Risk Propagation Threshold in Power CPS Based on Percolation Theory[J]. Automation of Electric Power Systems, 2020, 44(4): 16-23.
4. Hamada A, Hassan S M, Samy S, et al. A Review: State-of-the-Art of Integrating AI Models with Moving-target Defense for Enhancing IoT Networks Security[C]//2024 IEEE 15th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON). IEEE, 2024: 108-114.
5. Li Y, Yang Z, et al. Optimal scheduling of an isolated microgrid with battery storage considering load and renewable generation uncertainties[J]. IEEE Transactions on Industrial Electronics, 2018, 66(2): 1565-1575.
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. 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.
8. Suprabhath Koduru S, Machina V S P, Madichetty S. Cyber attacks in cyber-physical microgrid systems: A comprehensive review[J]. Energies, 2023, 16(12): 4573.
9. 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.
10. Abdelkader S, Amissah J, Abdel-Rahim O. Virtual power plants: an in-depth analysis of their advancements and importance as crucial players in modern power systems[J]. Energy, Sustainability and Society, 2024, 14(1): 52.
11. Cao J, Wang Q, Qu Z, et al. Method for identifying false data injection attacks in power grid based on improved CNN-LSTM[J]. Electrical Engineering, 2025: 1-26.
12. Hoenig A, Roy K, Acquaah Y T, et al. Explainable AI for cyber-physical systems: Issues and challenges[J]. IEEE access, 2024, 12: 73113-73140.
13. Zhao J, An K, Wang X. Research on Fast Early Warning of False Data Injection Attack in CPS of Electric Power Communication Network[J]. Journal of Cyber Security and Mobility, 2024: 1331–1356-1331–1356.
14. Jiang Y, Wu S, Ma R, et al. Monitoring and defense of industrial cyber-physical systems under typical attacks: From a systems and control perspective[J]. IEEE Transactions on Industrial Cyber-Physical Systems, 2023, 1: 192-207.
15. Li Y, 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.
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. Zhang D, Li X, Zhou L, et al. The Control Strategy for Power CPS Microgrid under Network Attack[C]//2022 4th Asia Energy and Electrical Engineering Symposium (AEEES). IEEE, 2022: 161-165.
18. Soussi W, Christopoulou M, Xilouris G, et al. Moving target defense as a proactive defense element for beyond 5G[J]. IEEE Communications Standards Magazine, 2021, 5(3): 72-79.
19. Wang L, Xu P, Qu Z, et al. Coordinated Cyber-Attack Detection Model of Cyber-Physical Power System Based on the Operating State Data Link[J]. Frontiers in Energy Research, 2021, 9: 666130.
20. Li T, Pan Y, Zhu Q. Decision-dominant strategic defense against lateral movement for 5g zero-trust multi-domain networks[M]//Network Security Empowered by Artificial Intelligence. Cham: Springer Nature Switzerland, 2024: 25-76.
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. Seo S, Moon H, Lee S, et al. D3GF: A study on optimal defense performance evaluation of drone-type moving target defense through game theory[J]. IEEE Access, 2023, 11: 59575-59598.

 doi:10.20944/preprints202506.0030.v1

24. Yao P, Yan B, Yang Q. Game Theoretical Decision-Making of Dynamic Defense in Cyber-Physical Power Systems under Cyber-Attacks[J]. ACM Transactions on Cyber-Physical Systems, 2025, 9(2): 1-21.
25. Bo X, Qu Z, Liu Y, et al. Review of active defense methods against power cps false data injection attacks from the multiple spatiotemporal perspective[J]. Energy Reports, 2022, 8: 11235-11248.
26. Chen J, Zhu Q. A cross-layer design approach to strategic cyber defense and robust switching control of cyber-physical wind energy systems[J]. IEEE Transactions on Automation Science and Engineering, 2022, 20(1): 624-635.
27. Soussi W, Christopoulou M, Gür G, et al. MERLINS–moving target defense enhanced with Deep-RL for NFV in-depth security[C]//2023 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN). IEEE, 2023: 65-71.
28. Wang W, Di Maio F, Zio E. Adversarial risk analysis to allocate optimal defense resources for protecting cyber–physical systems from cyber attacks[J]. Risk Analysis, 2019, 39(12): 2766-2785.
29. Barboni A, Rezaee H, Boem F. Detection of Covert Cyber-Attacks in Interconnected Systems: A Distributed Model-Based Approach[J]. IEEE Transactions on Automatic Control, 2020, 65(9): 3728-3741.
30. Mitchell R, Chen R. Modeling and analysis of attacks and counter defense mechanisms for cyber physical systems[J]. IEEE Transactions on Reliability, 2015, 65(1): 350-358.
31. Wang L, Qu Z, 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.
32. 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.
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 Yaqin, Ma Duohe, Xiaoyan Sun, et al. Research on Moving Target Defense Technology Based on Cyberspace Deception[J]. Journal of Information Security, 2025, 10(02): 180–195.
35. 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.
36. Hu Y, Zhu P, Xun P, et al. CPMTD: Cyber-physical moving target defense for hardening the security of power system against false data injected attack[J]. Computers & Security, 2021, 111: 102465.
37. Li Y, Feng B, Li G, et al. Optimal distributed generation planning in active distribution networks considering integration of energy storage[J]. Applied Energy, 2018, 210: 1073-1081.
38. Ni M, Li M, Li J, et al. Concept and research framework for coordinated situation awareness and active defense of cyber-physical power systems against cyber-attacks[J]. Journal of Modern Power Systems and Clean Energy, 2020, 9(3): 477-484.
39. 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.
40. Wang L, Qu Z, Li Y, et al. Method for Extracting Patterns of Coordinated Network Attacks on Electric Power CPS Based on Temporal–Topological Correlation[J]. IEEE Access, 2020, 8: 57260-57272.
41. Qu Z, Dong Y, Qu N, et al. Survivability Evaluation Method for Cascading Failure of Electric Cyber Physical System Considering Load Optimal Allocation[J]. Mathematical Problems in Engineering, 2019, 2019: 2817586.
42. Qu Z, Qu N, Zhou Y, et al. Extraction of Typical Operating Scenarios of New Power System Based on Deep Time Series Aggregation[J]. CAAI Transactions on Intelligence Technology, 2024, 1-17. DOI: 10.1049/cit2.12369.
43. Niu H, Jagannathan S. Optimal defense and control of dynamic systems modeled as cyber-physical systems[J]. The Journal of Defense Modeling and Simulation, 2015, 12(4): 423-438.
44. Chen L, Gu S, Wang Y, et al. Stacked Autoencoder Framework of False Data Injection Attack Detection in Smart Grid[J]. Mathematical Problems in Engineering, 2021, 2021(1): 2014345.
45. Li Y, 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.
46. Wang Q, Tai W, Tang Y, et al. A Review of False Data Injection Attack Research for Power Cyber-Physical Systems[J]. Acta Automatica Sinica, 2019, 45(1): 72-83.
47. Wang J, Li Y, Xu T. Modeling of False Data Injection Attacks and Rapid Screening of Vulnerable Lines under Attacks[J]. Electric Power Construction, 2022, 43(1): 104-112.

 doi:10.20944/preprints202506.0030.v1

48. Karamdel S, Liang X, Faried S O, et al. Optimization models in cyber-physical power systems: A review[J]. IEEE Access, 2022, 10: 130469-130486.
49. Zang T, Tong X, Li C, et al. Research and Prospect of Defense for Integrated Energy Cyber–Physical Systems Against Deliberate Attacks[J]. Energies, 2025, 18(6): 1479.
50. Li Y, Li J, Chen L. Dynamic state estimation of synchronous machines based on robust cubature Kalman filter under complex measurement noise conditions[J]. transactions of china electrotechnical society, 2019, 34(17): 3651-60.
51. Liu Chensheng, Li Yuanqi, Yang Ming, et al. A Review of Moving Target Defense for False Data Injection Attacks in Power Systems[J]. Automation Instrumentation, 2024, 45(11): 1–7.
52. Lydia M, Prem Kumar G E, Selvakumar A I. Securing the cyber-physical system: A review[J]. Cyber-Physical Systems, 2023, 9(3): 193-223.
53. Chen L, Jin P, Yang J, et al. Robust Kalman Filter-Based Dynamic State Estimation of Natural Gas Pipeline Networks[J]. Mathematical Problems in Engineering, 2021, 2021(1): 5590572.
54. Li Q., Wu J. Optimizing the Effectiveness of Moving Target Defense in a Probabilistic Attack Graph: A Deep Reinforcement Learning Approach[J]. Electronics, 2024, 13(19): 3855–3855.
55. Fu X., Qiao Z., Xu Z. Attack–defense strategy of UAV swarm based on DEP-SIQ in the active target defense scenario[J]. Soft Computing, 2024, 28(17–18): 10463–10473.
56. Chamana M, Bhatta R, Schmitt K, et al. An integrated testbed for power system cyber-physical operations training[J]. Applied Sciences, 2023, 13(16): 9451.
57. Jue T ,Rui T ,Xiaohong G , et al. Moving Target Defense Approach to Detecting Stuxnet-Like Attacks[J]. IEEE Transactions on Smart Grid,2020,11(1):291-300.
58. Dorbala S Y, Bhadoria R S. Analysis for security attacks in cyber-physical systems[J]. Cyber-Physical Systems: A Computational Perspective, 2015: 395-414.
59. Yifan H ,Guomin Z ,Xiulei W , et al. Controlled measurement set randomization–based moving target defense against coordinated cyber–physical attack in smart grids[J].Electric Power Systems Research, 2023, 224: 109749.
60. 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.
61. Dantas Silva F S, Neto E P, Nunes R S S, et al. Securing Software-Defined Networks Through Adaptive Moving Target Defense Capabilities[J]. Journal of Network and Systems Management, 2023, 31(3): 61.
62. Tan J ,Jin H ,Hu H , et al.WF-MTD: Evolutionary Decision Method for Moving Target Defense Based on Wright-Fisher Process[J]. IEEE Transactions on Dependable and Secure Computing,2023,20(6):4719-4732.
63. 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.
64. Sun S, Hossain-McKenzie S, Al Homoud L, et al. An AI-based Approach for Scalable Cyber-Physical Optimal Response in Power Systems[C]//2024 IEEE Texas Power and Energy Conference (TPEC). IEEE, 2024: 1-6.
65. Fan X, Du L, Duan D. Synchrophasor Data Correction Under GPS Spoofing Attack: A State Estimation-Based Approach[J]. IEEE Transactions on Smart Grid, 2018, 9(5): 4538-4546.
66. Wan Y, Cao J. A brief survey of recent advances and methodologies for the security control of complex cyber–physical networks[J]. Sensors, 2023, 23(8): 4013.
67. Babadi N, Doustmohammadi A. A moving target defence approach for detecting deception attacks on cyber-physical systems[J]. Computers and Electrical Engineering, 2022, 100: 107931.
68. Subhash L ,Veronica E B ,Vincent H P.Moving-Target Defense Against Cyber-Physical Attacks in Power Grids via Game Theory[J]. IEEE Transactions on Smart Grid, 2021, 12(6):5244-5257.
69. Khaitan S K, McCalley J D. Cyber physical system approach for design of power grids: A survey[C]//2013 IEEE Power & Energy Society General Meeting. IEEE, 2013: 1-5.
70. Bo L ,Hongyu W .Optimal Planning and Operation of Hidden Moving Target Defense for Maximal Detection Effectiveness[J]. IEEE Transactions on Smart Grid, 2021,12(5):4447-4459.
71. Banik S, Ramachandran T, Bhattacharya A, et al. Automated adversary-in-the-loop cyber-physical defense planning[J]. ACM Transactions on Cyber-Physical Systems, 2023, 7(3): 1-25.
72. Jain H, Kumar M, Joshi A M. Intelligent energy cyber physical systems (iECPS) for reliable smart grid against energy theft and false data injection[J]. Electrical Engineering, 2022, 104(1): 331-346.

 doi:10.20944/preprints202506.0030.v1

73. E. R N, Frederic C, Boulahia N C, et al. MTD, Where Art Thou? A Systematic Review of Moving Target Defense Techniques for IoT[J]. IEEE Internet Of Things Journal, 2021,8(10):7818-7832.
74. Sridhar S, Hahn A, Govindarasu M. Cyber-Physical System Security for the Electric Power Grid[J]. Proceedings of the IEEE, 2012, 100(1): 210-224.
75. Wang Bin, Chen Liang, Qian Yaguan, et al. Moving Target Defense Against Adversarial Example Attacks [J]. Journal of Network and Information Security, 2021, 7(01): 113–120.
76. Xiong X, Hu S, Sun D, et al. Detection of false data injection attack in power information physical system based on SVM-GAB algorithm[J]. Energy Reports, 2022, 8(5): 1156-1164.
77. Huang H, Wlazlo P, Mao Z, et al. Cyberattack defense with cyber-physical alert and control logic in industrial controllers[J]. IEEE Transactions on Industry Applications, 2022, 58(5): 5921-5934.
78. Qu Z, Shi H, Wang Y, et al. Active and Passive Defense Strategies of Cyber-Physical Power System against Cyber Attacks Considering Node Vulnerability[J]. Processes, 2022, 10(7): 1351.
79. Presekal A, Ştefanov A, Semertzis I, et al. Spatio-temporal advanced persistent threat detection and correlation for cyber-physical power systems using enhanced GC-LSTM[J]. IEEE Transactions on Smart Grid, 2024.
80. Chen Y, Huang S, Liu F, et al. Evaluation of Reinforcement Learning-Based False Data Injection Attack to Automatic Voltage Control[J]. IEEE Transactions on Smart Grid, 2019, 10(2): 2158-2169.
81. Park K, Hong J, Su W, et al. Machine Learning based Post Event Analysis for Cybersecurity of Cyber-Physical System[C]//2024 IEEE Power & Energy Society General Meeting (PESGM). IEEE, 2024: 1-5.
82. Martin H ,Fei T ,Thomas P .Stealthy MTD Against Unsupervised Learning-Based Blind FDI Attacks in Power Systems[J]. IEEE Transactions on Information Forensics and Security, 2021, 161275-1287.
83. Sun J, et al. Indicator & crowding distance-based evolutionary algorithm for combined heat and power economic emission dispatch[J]. Applied Soft Computing, 2020, 90: 106158.
84. Yang F, Wang J, Pan Q, et al. Resilient Event-Triggered Control for Cyber-Physical Integrated Power Systems Under Network Attacks[J]. Acta Automatica Sinica, 2019, 45(1): 110-119.
85. Chen L, Li Y, Huang M, et al. Robust Dynamic State Estimator of Integrated Energy Systems Based on Natural Gas Partial Differential Equations[J]. IEEE Transactions on Industry Applications, 2022, 58(3): 3303-3312.
86. Susuki Y, Koo T, Ebina H, et al. A Hybrid System Approach to the Analysis and Design of Power Grid Dynamic Performance[J]. Proceedings of the IEEE, 2012, 100(1): 225-239.
87. Zhang Z, Tian Y, Deng R, et al. A double-benefit moving target defense against cyber–physical attacks in smart grid[J]. IEEE Internet of Things Journal, 2022, 9(18): 17912-17925.
88. Liu X, Li Z, Shuai Z, et al. Cyber Attacks Against the Economic Operation of Power Systems: A Fast Solution[J]. IEEE Transactions on Smart Grid, 2017, 8(2): 1023-1025.
89. Wei L, Zhang Q. Detection of False Data Attacks in Smart Grids Based on Improved UKF[J]. Journal of System Simulation, 2023, 35(7): 1508.
90. Aris K ,G. K V .A Moving Target Defense Control Framework for Cyber-Physical Systems[J]. IEEE Transactions on Automatic Control, 2020, 65(3):1029-1043.
91. Sanjab A, Saad W. Data Injection Attacks on Smart Grids With Multiple Adversaries: A Game-Theoretic Perspective[J]. IEEE Transactions on Smart Grid, 2016, 7(4): 2038-2049.
92. 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.
93. Hee J C ,P. D S ,Hooman A , et al.Toward Proactive, Adaptive Defense: A Survey on Moving Target Defense[J]. IEEE Communications Surveys & Tutorials,2020,22(1):709-745.
94. Xu S, Xia Y, Shen H L. Cyber protection for malware attack resistance in cyber-physical power systems[J]. IEEE Systems Journal, 2022, 16(4): 5337-5345.
95. Alvarez-Alvarado M S, Apolo-Tinoco C, Ramirez-Prado M J, et al. Cyber-physical power systems: A comprehensive review about technologies drivers, standards, and future perspectives[J]. Computers and Electrical Engineering, 2024, 116: 109149.
96. Kong X, Lu Z, Guo X, et al. Resilience evaluation of cyber-physical power system considering cyber attacks[J]. IEEE Transactions on Reliability, 2023, 73(1): 245-256.
97. Chen L, Wang B. Robustness assessment of weakly coupled cyber-physical power systems under multi-stage attacks[J]. Electric Power Systems Research, 2024, 231: 110325.

 doi:10.20944/preprints202506.0030.v1

98. Luo X, He J, Wang X, et al. Topology Optimization for Resilient Defense Strategies Against False Data Injection Attacks in Smart Grids[J]. Acta Automatica Sinica, 2023, 49(6): 1326-1338.
99. Deng R, Zhuang P, Liang H. CCPA: Coordinated Cyber-Physical Attacks and Countermeasures in Smart Grid[J]. IEEE Transactions on Smart Grid, 2017, 8(5): 2420-2430.
100. Lakshminarayana S, Chen Y, Konstantinou C, et al. Survey of moving target defense in power grids: Design principles, tradeoffs, and future directions[J]. arXiv preprint arXiv:2409.18317, 2024.
101. Risbud P, Gatsis N, Taha A. Vulnerability Analysis of Smart Grids to GPS Spoofing[J]. IEEE Transactions on Smart Grid, 2019, 10(4): 3535-3548.
102. Alabadi M, Albayrak Z. Q-learning for securing cyber-physical systems: a survey[C]//2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA). IEEE, 2020: 1-13.
103. Huang D, Wang Y, Hu A, et al. False Data Injection Attack Detection Combining Unsupervised and Supervised Learning[J]. Electric Power Engineering Technology, 2024, 43(2): 134-141.
104. Mortlock T, Al Faruque M A. Adaptive Data Fusion for State Estimation and Control of Power Grids Under Attack[J]. IEEE Transactions on Industrial Informatics, 2024.
105. Giraldo J A, El Hariri M, Parvania M. Moving target defense for cyber–physical systems using iot-enabled data replication[J]. IEEE Internet of Things Journal, 2022, 9(15): 13223-13232.
106. Chen L, Hui X, et al. Dynamic state estimation for integrated natural gas and electric power systems[C]//2021 IEEE/IAS Industrial and Commercial Power System Asia (I&CPS Asia). IEEE, 2021: 397-402.
107. Tian J ,Tan R ,Guan X , et al.Enhanced Hidden Moving Target Defense in Smart Grids[J]. IEEE Transactions on Smart Grid, 2019, 10(2):2208-2223
108. Ali M, Sun W. Securing Critical Infrastructures: Restoration from Cyber-Physical Attacks in Active Distribution Grids[C]//2024 IEEE Power & Energy Society General Meeting (PESGM). IEEE, 2024: 1-5.
109. Fan Q, Liu D, Wang Y, et al. Key Technologies and Progress in the Morphological Evolution of Power Cyber-Physical Systems[J]. Proceedings of the CSEE, 2023, 44(21): 8341-8352.
110. He Z, Gao S, Wei X, et al. Research on Attack-Defense Game Model of False Topology Attacks with Branch and Protection Coordination[J]. Power System Technology, 2022, 46(11): 4346-4355.
111. Li X, Yi L, Liu C, et al. Data-Driven Detection of False Data Injection Attacks in Power Systems[J]. Smart Power, 2023, 51(2): 30-37.
112. Weng P, Chen B, Yu L. Fusion Estimation of False Data Injection Attack Signals[J]. Acta Automatica Sinica, 2021, 47(9): 2292-2300.
113. Patel C D, Aggarwal M, Chaubey N K. Enhancing Cyber-Physical Systems Security Through Advanced Defense Mechanisms[M]//Advancing Cyber Security Through Quantum Cryptography. IGI Global, 2025: 307-342.
114. Krishnaveni S, Chen T M, Sathiyanarayanan M, et al. CyberDefender: an integrated intelligent defense framework for digital-twin-based industrial cyber-physical systems[J]. Cluster Computing, 2024, 27(6): 7273-7306.
115. Purohit S, Neupane R, Bhamidipati N R, et al. Cyber threat intelligence sharing for co-operative defense in multi-domain entities[J]. IEEE Transactions on Dependable and Secure Computing, 2022, 20(5): 4273-4290.
116. Zhou X, Feng J, et al. Non-intrusive load decomposition based on CNN–LSTM hybrid deep learning model[J]. Energy Reports, 2021, 7: 5762-5771.
117. Yan B, Yao P, Wang J, et al. Game theoretical dynamic cybersecurity defense strategy for electrical cyber physical systems[C]//2021 IEEE 5th Conference on Energy Internet and Energy System Integration (EI2). IEEE, 2021: 2392-2397.
118. Zhou Z, Zhang J, Zhang X. A review on defense mechanism against the denial of service and false data injection in cyber-physical power systems[C]//2023 IEEE 6th International Electrical and Energy Conference (CIEEC). IEEE, 2023: 4539-4545.
119. Fahmeeda S, Bhagyashree B K. Detection and prevention of false data injection attack in cyber physical power system[C]//2021 IEEE International Conference on Mobile Networks and Wireless Communications (ICMNWC). IEEE, 2021: 1-5.
120. Yang J. A controllable false data injection attack for a cyber physical system[J]. IEEE Access, 2021, 9: 6721-6728.
121. Xing W, Shen J. Security Control of Cyber–Physical Systems under Cyber Attacks: A Survey[J]. Sensors, 2024, 24(12): 3815.
122. Yang J. A controllable false data injection attack for a cyber physical system[J]. IEEE Access, 2021, 9: 6721-6728.

 doi:10.20944/preprints202506.0030.v1

123. Chen H, Li T, Fan X, et al. Feature selection for imbalanced data based on neighborhood rough sets[J]. Information Sciences, 2019, 483: 1-20.
124. Wang S, Ko R K L, Bai G, et al. Evasion attack and defense on machine learning models in cyber-physical systems: A survey[J]. IEEE communications surveys & tutorials, 2023, 26(2): 930-966.
125. Li Y, Li Z, Chen L. Dynamic State Estimation of Generators Under Cyber Attacks[J]. IEEE Access, 2019, 7: 125252-125267.
126. Xiao K, Zhu C, Xie J, et al. Dynamic defense against stealth malware propagation in cyber-physical systems: a game-theoretical framework[J]. Entropy, 2020, 22(8): 894.
127. Zhao Z, Shang Y, Qi B, et al. Research on defense strategies for power system frequency stability under false data injection attacks[J]. Applied Energy, 2024, 371: 123711.
128. Xiong X, Hu S, Sun D, et al. Detection of false data injection attack in power information physical system based on SVM–GAB algorithm[J]. Energy Reports, 2022, 8: 1156-1164.
129. Zhu H, Xu L, Bao Z, et al. Secure control against multiplicative and additive false data injection attacks[J]. IEEE Transactions on Industrial Cyber-Physical Systems, 2023, 1: 92-100.
130. Zhong C, Li H, Zhou Y, et al. Virtual synchronous generator of PV generation without energy storage for frequency support in autonomous microgrid[J]. International Journal of Electrical Power & Energy Systems, 2022, 134: 107343.
131. Li Y, Zhang M, Chen C. A deep-learning intelligent system incorporating data augmentation for short-term voltage stability assessment of power systems[J]. Applied Energy, 2022, 308: 118347.
132. Costilla-Enriquez N, Weng Y. Attack power system state estimation by implicitly learning the underlying models[J]. IEEE Transactions on Smart Grid, 2022, 14(1): 649-662.
133. Chu X, Yi Y, Tang M, et al. Defensive resource allocation for cyber-physical systems in global energy interconnection[C]//IOP Conference Series: Earth and Environmental Science. IOP Publishing, 2019, 227(4): 042002.
134. Khalid H, Peng J. Immunity Toward Data-Injection Attacks Using Multisensor Track Fusion-Based Model Prediction[J]. IEEE Transactions on Smart Grid, 2017, 8(2): 697-707.
135. Liu X, Chang P, Sun Q. Detection of False Data Injection Attacks in Power Grids Based on XGBoost and Unscented Kalman Filter Adaptive Hybrid Prediction[J]. Proceedings of the CSEE, 2021, 41(16): 5462-5476.
136. Alsharif G O, Anagnostopoulos C, Marnerides A K. Energy Market Manipulation via False-Data Injection Attacks[J]. IEEE Access, 2025.
137. Zhou B, Sun B, Zang T, et al. Security risk assessment approach for distribution network cyber physical systems considering cyber attack vulnerabilities[J]. Entropy, 2022, 25(1): 47.
138. Le J, Lang H, Tan T, et al. A Review of Information Security Issues in Distributed Economic Dispatch of New Distribution Systems[J]. Automation of Electric Power Systems, 2024, 48(12): 177-191.
139. Jiang Z, Yao P, Yan B, et al. Cyber-physical system defense decision-making based on priori knowledge of traffic anomaly detection[C]//2023 IEEE 7th Conference on Energy Internet and Energy System Integration (EI2). IEEE, 2023: 5196-5201.
140. Zideh M J, Khalghani M R, Solanki S K. An unsupervised adversarial autoencoder for cyber attack detection in power distribution grids[J]. Electric Power Systems Research, 2024, 232: 110407.
141. Zhang Z, Huang S, Chen Y, et al. Cyber-physical coordinated risk mitigation in smart grids based on attack-defense game[J]. IEEE Transactions on Power Systems, 2021, 37(1): 530-542.
142. Shafae M S, Wells L J, Purdy G T. Defending against product-oriented cyber-physical attacks on machining systems[J]. The International Journal of Advanced Manufacturing Technology, 2019, 105: 3829-3850.
143. Long X, Ding Y, et al. Privacy-Preserving Graph Inference Network for Multi-Entity Wind Power Forecast: A Federated Learning Approach[J]. IEEE Transactions on Network Science and Engineering, 2025. DOI: 10.1109/TNSE.2025.3547227.
144. Lian Z, Shi P, Chen M. A Survey on Cyber-Attacks for Cyber-Physical Systems: Modeling, Defense and Design[J]. IEEE Internet of Things Journal, 2024.
145. 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.
146. Liu S, Tan Y, Zhao F, et al. Coupled Modeling Method for Power Information Systems[J]. Journal of Power Systems and Automation, 2021, 33(3): 89-93.

 doi:10.20944/preprints202506.0030.v1

147. Yang T, Cai S, Yan P, et al. Saturation defense method of a power cyber-physical system based on active cut set[J]. IEEE Transactions on Smart Grid, 2022.
148. 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.
149. 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.
150. Khanna K, Govindarasu M. Resiliency-driven cyber–physical risk assessment and investment planning for power substations[J]. IEEE Transactions on Control Systems Technology, 2024, 32(5): 1743-1754.
151. Sun S, Huang H, Payne E, et al. A graph embedding-based approach for automatic cyber-physical power system risk assessment to prevent and mitigate threats at scale[J]. IET Cyber-Physical Systems: Theory & Applications, 2024, 9(4): 435-453.
152. Jin Z, Liu Y, Diao J, et al. Covert False Data Injection Attacks on Remote State Estimation in Cyber-Physical Systems[J]. Acta Automatica Sinica, 2025, 51(2): 1-10.
153. Shi J, Chen B, Yu L. Hidden FDIA Detection Based on Laplacian Eigenmap Learning[J]. Acta Automatica Sinica, 2021, 47(10): 2494-2500.
154. Ribas Monteiro L F, Rodrigues Y R, Zambroni de Souza A C. Cybersecurity in cyber–physical power systems[J]. Energies, 2023, 16(12): 4556.
155. 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.
156. Shen Y, Zhang W, Ni H, et al. Guaranteed Cost Control of Networked Control Systems with DoS Attack and Time-varying Delay[J]. International Journal of Control, Automation and Systems, 2019, 17(4): 811-821.
157. Liu S, Martínez S, Cortés J. Stabilization of linear cyber-physical systems against attacks via switching defense[J]. IEEE Transactions on Automatic Control, 2023, 68(12): 7326-7341.
158. Liang Y, Wang Y, Liu K, et al. Fault Simulation of Distribution Grid CPS Considering Network Information Security[J]. Power System Technology, 2020, 45(1): 235-242.
159. Barrère M, Hankin C, O'Reilly D. Cyber-physical attack graphs (CPAGs): Composable and scalable attack graphs for cyber-physical systems[J]. Computers & security, 2023, 132: 103348.
160. 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.
161. Fu Y, Chen L, Ma Z, et al. Preventive Control of Power Systems Including Data-Driven Stability Constraints[J]. Proceedings of the CSEE, 2022, 42(15): 5417-5430.
162. Feng Y, Huang R, Zhao W, et al. A survey on coordinated attacks against cyber–physical power systems: Attack, detection, and defense methods[J]. Electric Power Systems Research, 2025, 241: 111286.
163. Li B, Xiao Y, Shi Y, et al. Anti-honeypot enabled optimal attack strategy for industrial cyber-physical systems[J]. IEEE Open Journal of the Computer Society, 2020, 1: 250-261.
164. Li T, Zhao H, Wang S, et al. Attack and Defense Strategy of Distribution Network Cyber-Physical System Considering EV Source-Charge Bidirectionality[J]. Electronics, 2021, 10(23): 2973.
165. Lei C, Bu S, Wang Q, et al. Observability defense-constrained distribution network reconfiguration for cyber-physical security enhancement[J]. IEEE Transactions on Smart Grid, 2023, 15(2): 2379-2382.
166. Fang S W, Portante A, Husain M I. Moving target defense mechanisms in cyber-physical systems[J]. Securing Cyber-Physical Systems, 2015: 63.
167. Cui Y, et al. Deep reinforcement learning based optimal energy management of multi-energy microgrids with uncertainties[J]. CSEE Journal of Power and Energy Systems, 2024: 1-12. DOI: 10.17775/CSEEJPES.2023.05120.
168. Ao W, Song Y, Wen C. Adaptive cyber-physical system attack detection and reconstruction with application to power systems[J]. IET Control Theory & Applications, 2016, 10(12): 1458-1468.
169. Yang X, et al. Gaussian Mixture Model Uncertainty Modeling for Power Systems Considering Mutual Assistance of Latent Variables[J]. IEEE Transactions on Sustainable Energy, 2024, 1-4. DOI: 10.1109/TSTE.2024.3356259.
170. Barrère M, Hankin C, O'Reilly D. Cyber-physical attack graphs (CPAGs): Composable and scalable attack graphs for cyber-physical systems[J]. Computers & security, 2023, 132: 103348.

 doi:10.20944/preprints202506.0030.v1

171. Setitra M, Fan M, Benkhaddra I. DoS/DDoS Attacks in Software Defined Networks: Current Situation, Challenges and Future Directions[J]. Computers and Communications, 2024, 222: 77-96.
172. Wei J, Yan X, Zhu X, Xu M, Ma R, Du H. New Stability Conditions of CPSs with Multiple Transportation Channels under DoS Attacks[J]. Science China Information Sciences, 2022, 65(11): 219202.
173. Xiao Y, Chai S, Dai L, Xia Y, Chai R. Stochastic Tube-Based Model Predictive Control for Cyber-Physical Systems under False Data Injection Attacks with Bounded Probability[J]. arXiv preprint arXiv:2503.07385, 2025.
174. Alguliyev R, Imamverdiyev Y, Sukhostat L. Cyber-Physical Systems and Their Security Issues[J]. Computers in Industry, 2018, 100: 212-223.
175. Jeong S, Baek Y, Son S. Component-Based Interactive Framework for Intelligent Transportation Cyber-Physical Systems[J]. Sensors, 2020, 20(1): 264.
176. Song S, Park J H, Zhang B, Song X. Event-Based Adaptive Fuzzy Fixed-Time Secure Control for Nonlinear CPSs Against Unknown False Data Injection and Backlash-Like Hysteresis[J]. IEEE Transactions on Fuzzy Systems, 2022, 30(6): 1939-1951.
177. Li Y, Wei X, Li Y, Dong Z, Shahidehpour M. Detection of False Data Injection Attacks in Smart Grid: A Secure Federated Deep Learning Approach[J]. arXiv preprint arXiv:2209.00778, 2022.
178. Zhao H J, Li Q Z, Zeng X, Liu Z M. Safe Reinforcement Learning Algorithm and Its Application in Intelligent Control for CPS[J]. International Journal of Software and Informatics, 2022, 12(4): 453-483.
179. Hasan M, Habib A, Shukur Z, Ibrahim F, Islam S, Razzaque M A. Review on Cyber-Physical and Cyber-Security System in Smart Grid: Standards, Protocols, Constraints, and Recommendations[J]. Journal of Network and Computer Applications, 2023, 209: 103540.
180. Fan X, Lin W, Liu Z, Zhao L. Reachable Set Control for Nonlinear Markov Jump Cyber-Physical Systems with False Data Injection Attacks[J]. Journal of The Franklin Institute, 2024, 361(1): 224-233.
181. Ye D, Zhang T. Summation Detector for False Data-Injection Attack in Cyber-Physical Systems[J]. IEEE Transactions on Cybernetics, 2019, 50(6): 2338-2345.
182. Eslami A, Khorasani K. Zero Dynamics Attack Detection and Isolation in Cyber-Physical Systems with Event-Triggered Communication[J]. arXiv preprint arXiv:2505.06070, 2025.
183. Razaque A, Amsaad F H, Abdulgader M, Alotaibi B, Alsolami F, Gulsezim D. A Mobility-Aware Human-Centric Cyber-Physical System for Efficient and Secure Smart Healthcare[J]. IEEE Internet of Things Journal, 2022, 9(22): 22434-22452.
184. Xue K. Securing Power Cyber-Physical Systems Against False Data Injection Attacks: Trends, Techniques, and Future Directions[J]. Preprints, 2025.
185. Chattopadhyay A, Mitra U. Security Against False Data-Injection Attack in Cyber-Physical Systems[J]. IEEE Transactions on Control of Network Systems, 2019, 7(2): 1015-1027.
186. Koley I, Adhikary S, Dey S. An RL-Based Adaptive Detection Strategy to Secure Cyber-Physical Systems[J]. arXiv preprint arXiv:2103.02872, 2021.
187. Zhang X, Han H. Event-Triggered Finite-Time Filtering for Nonlinear Networked System with Quantization and DoS Attacks[J]. IEEE Access, 2024, 12: 1308-1320.
188. Rieger C G, Gertman D I, McQueen M A. Resilient Control Systems: Next Generation Design Research[J]. 2nd IEEE Conference on Human System Interaction, 2009: 632-636.
189. Rinaldi S M, Peerenboom J P, Kelly T K. Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies[J]. IEEE Control Systems Magazine, 2001, 21(6): 11-25.
190. Rinaldi S M, Peerenboom J P, Kelly T K. Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies[J]. IEEE Control Systems Magazine, 2001, 21(6): 11-25.
191. Sun C, Su Q, Li J. Secure Tracking Control and Attack Detection for Power Cyber-Physical Systems based on Integrated Control Decision[J]. IEEE Transactions on Information Forensics and Security, 2024.
192. Wang P, Zhang R, He X. New Approaches to Detection and Secure Control for Cyber-physical Systems Against False Data Injection Attacks[J]. International Journal of Control, Automation and Systems, 2025, 23(1): 332-345.
193. Kaloudi N, Li J. The ML-based sensor data deception targeting cyber–physical systems: A review[J]. Computer Science Review, 2025, 57: 100753.
194. Busari W A, Bello A A. Security, Trust, and Privacy in Cyber-physical Systems (CPS)[C]//2024 2nd International Conference on Cyber Physical Systems, Power Electronics and Electric Vehicles (ICPEEV). IEEE, 2024: 1-6.

 doi:10.20944/preprints202506.0030.v1

195. Noor U, Shahid S, Kanwal R, et al. A Machine Learning based Empirical Evaluation of Cyber Threat Actors High Level Attack Patterns over Low level Attack Patterns in Attributing Attacks[J]. arXiv preprint arXiv:2307.10252, 2023.
196. Samad T. Human-in-the-loop control and cyber–physical–human systems: applications and categorization[J]. Cyber–physical–human systems: fundamentals and applications, 2023: 1-23.
197. Gil M, Albert M, Fons J, et al. Engineering human-in-the-loop interactions in cyber-physical systems[J]. Information and software technology, 2020, 126: 106349.
198. Iyenghar P. Clever Hans in the Loop? A Critical Examination of ChatGPT in a Human-in-the-Loop Framework for Machinery Functional Safety Risk Analysis[J]. Eng, 2025, 6(2): 31.
199. Adil M, Farouk A, Abulkasim H, et al. NG-ICPS: Next Generation Industrial-CPS, Security Threats in the Era of Artificial Intelligence, Open Challenges With Future Research Directions[J]. IEEE Internet of Things Journal, 2024.
200. Agarwal M, Venkateswaran S K, Sivakumar R. Human-in-the-loop rl with an eeg wearable headset: On effective use of brainwaves to accelerate learning[C]//Proceedings of the 6th ACM Workshop on Wearable Systems and Applications. 2020: 25-30.
201. Nguyen T T, Kadavil R, Hooshyar H. A Real-time Cyber-Physical Simulation Testbed for Cybersecurity Assessment of Large-Scale Power Systems[J]. IEEE Transactions on Industry Applications, 2024.
202. Li P, Fu J, Xie K, et al. A Defense Planning Model for a Power System Against Coordinated Cyber-Physical Attack[J]. Protection and Control of Modern Power Systems, 2024, 9(5): 84-95.
203. Ravikumar G, Hyder B, Babu J R, et al. Cps testbed architectures for wampac using industrial substation and control center platforms and attack-defense evaluation[C]//2021 IEEE Power & Energy Society General Meeting (PESGM). IEEE, 2021: 1-5.
204. Jiang Y, Wu S, Ma R, et al. Monitoring and defense of industrial cyber-physical systems under typical attacks: From a systems and control perspective[J]. IEEE Transactions on Industrial Cyber-Physical Systems, 2023, 1: 192-207.
205. Fan Y, Li J, Zhang D, et al. Supporting sustainable maintenance of substations under cyber-threats: An evaluation method of cybersecurity risk for power CPS[J]. Sustainability, 2019, 11(4): 982.
206. Chen Y, Li T, Long Y, Bai W. Attacks Detection and Security Control for Cyber-Physical Systems under False Data Injection Attacks[J]. Journal of The Franklin Institute, 2023, 360(14): 10476-10498.
207. Abdelmalak M. Effects of Unobservable Bus States on Detection and Localization of False Data Injection Attacks in Smart Grids[D]. University of South Florida, 2024.
208. Feng H, Han Y, Si F, Zhao Q. Detection of False Data Injection Attacks in Cyber-Physical Power Systems: An Adaptive Adversarial Dual Autoencoder with Graph Representation Learning Approach[J]. IEEE Transactions on Instrumentation and Measurement, 2024, 73: 1-11.
209. Guan Y, Ge X. Distributed Attack Detection and Secure Estimation of Networked Cyber-Physical Systems Against False Data Injection Attacks and Jamming Attacks[J]. IEEE Transactions on Signal and Information Processing over Networks, 2017, 4(1): 48-59.
210. Barboni A, Rezaee H, Boem F, Parisini T. Detection of Covert Cyber-Attacks in Interconnected Systems: A Distributed Model-Based Approach[J]. IEEE Transactions on Automatic Control, 2020, 65(9): 3728-3741.
211. 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.
212. Hu Y. Research on moving target defense for smart grid cyber-physical security[M]. National University of Defense Technology, 2021.
213. Yan K, Liu X, Lu Y, et al. A cyber-physical power system risk assessment model against cyberattacks[J]. IEEE Systems Journal, 2022, 17(2): 2018-2028.
214. Kausar F, Deo S, Hussain S, et al. Federated Deep Learning Model for False Data Injection Attack Detection in Cyber Physical Power Systems[J]. Energies, 2024, 17(21): 5337.
215. 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.
216. BaSin D, Cremers C, Kim T, et al. Design, Analysis, and Implementation of ARPKI: an Attack-Resilient Public-Key Infrastructure[J]. IEEE Transactions on Dependable and Secure Computing, 2016, 15(3): 393-408.
217. 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.

 doi:10.20944/preprints202506.0030.v1

218. Bai M, Liu P, Lv F, et al. Adversarial Attack against Intrusion Detectors in Cyber-Physical Systems With Minimal Perturbations[C]//2024 IEEE International Symposium on Parallel and Distributed Processing with Applications (ISPA). IEEE, 2024: 816-825.
219. Preeti G, Sanjeev Kumar P. A Blockchain Based Decentralized Application System for Vanet FDIA Detection[C]//International Conference on Computing and Communication Networks. Singapore: Springer Nature Singapore, 2023: 95-119.
220. 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.
221. Dong Z, Tang M, Tian M. Allocating defense resources for spatial cyber-physical power systems based on deep reinforcement learning[C]//2023 IEEE 6th International Conference on Industrial Cyber-Physical Systems (ICPS). IEEE, 2023: 1-6.
222. Yu J, Li Q, Li L. Localization of coordinated cyber-physical attacks in power grids using moving target defense and machine learning[J]. Electronics, 2024, 13(12): 2256.
223. Ullrich J, Weippl E R. CyPhySec: Defending cyber-physical systems[J]. ERCIM News, 2015, 102: 18-18.
224. 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.
225. Zhong X, xin Li G, Zhng C. False data injection in power smart grid and identification of the most vulnerable bus; a case study 14 IEEE bus network[J]. Energy Reports, 2021, 7: 8476-8484.
226. 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.
227. Keçeci C, Davis K R, Serpedin E. Federated learning based distributed localization of false data injection attacks on smart grids[J]. arXiv preprint arXiv:2306.10420, 2023.
228. Mansour R F. Artificial intelligence based optimization with deep learning model for blockchain enabled intrusion detection in CPS environment[J]. Scientific Reports, 2022, 12(1): 12937.
229. Ding X, Wang H, Zhang X, et al. Dual nature of cyber–physical power systems and the mitigation strategies[J]. Reliability Engineering & System Safety, 2024, 244: 109958.
230. Kesici M, Pal B, Yang G. Detection of false data injection attacks in distribution networks: A vertical federated learning approach[J]. IEEE Transactions on Smart Grid, 2024.
231. Mitchell S M, Mannan M S. Designing Resilient Engineered Systems[J]. Chemical Engineering Progress, 2006, 102(4): 33-39.
232. Wing J. Cyber-Physical Systems Research Charge[J]. Cyber-Physical Systems Summit, 2008.
233. McJunkin T R, Rieger C G, Johnson B K, Naidu D S, Gardner J F, Beaty L H, Ray I, Le Blanc K L, Guryan M. Interdisciplinary Education through “Edu-tainment”: Electric Grid Resilient Control Systems Course[J]. ASEE Annual Conference and Exposition, 2015.
234. Hahn E M, Perez M, Schewe S, Somenzi F. Model-Free Reinforcement Learning for Branching Markov Decision Processes[J]. Computer Aided Verification, 2021, 12760: 651-673.
235. van Hasselt H, Guez A, Silver D. Deep Reinforcement Learning with Double Q-Learning[J]. AAAI Conference on Artificial Intelligence, 2016, 30: 2094-2100.