Cyber-Secure Operation of Networked Microgrids for Enhancing Power Grid Resilience

Mohammad Shahidehpour
Illinois Institute of Technology, Chicago, IL 60616, U.S.

ABSTRACT

The advancement of operational methodologies together with the progress of information technologies strengthens the resilient performance of networked microgrids (NMGs), while the increasing cyber-physical coupling also exposes NMGs to greater risk surfaces under cyber-attacks. To this end, this chapter examines the cyber secure operation of NMGs and their role in enhancing power grid resilience. It begins with a clear presentation of physical networking and cyber networking in NMGs and then describes how coordinated cyber-physical operation supports local power service. A taxonomy of cyber vulnerabilities is provided, and the operational consequences of cyber incidents are analyzed. Next, the chapter outlines methods to classify operational states under degraded conditions and to assess impacts on power supply continuity. The potential of advanced information technologies to strengthen security is evaluated, with separate sections on software-defined networking, blockchain, artificial intelligence, and quantum technology for secure and efficient control. A layered defense in depth framework is thus proposed that assigns resilience measures across sensing, local control, distributed energy resources (DERs), aggregated multi-DER coordination, sub-system microgrid control, and system-level coordination. Accordingly, two illustrative case studies test cyber-secure operation performance at the individual microgrid level and the NMG level. The chapter closes with research directions that include cyber-physical contingency-based risk assessment, real-time co-simulation testbeds, human factors in cybersecurity analysis, and integration pathways for emerging technologies to increase attack resistance and operational flexibility.

1. COLLABORATIVE OPERATION OF NETWORKED MICROGRIDS

Networked microgrids (NMGs), composed of geographically close microgrids linked by flexible tie-lines, provide concrete resilience advantages for power grids [1], [2]. In particular, local control and islanding capability enable uninterrupted service to critical loads during bulk grid disturbances; peer energy exchange among neighboring microgrids enables resource sharing and localized restoration without reliance on long-distance transmission; aggregation of distributed energy resources (DERs) in NMGs reduces stress on upstream assets and shortens restoration times after extreme events [3]. Meanwhile, with the extensive use of information technologies (ITs), NMGs have evolved as typical cyber-physical systems in which the functions of cyber and power components are tightly coupled in their operations. As shown in Fig. 1, by exploiting advanced ITs and proven operational technologies (OTs), NMGs are regarded as a typical cyber-physical system, where the microgrid master controller (MMC) is the control center of each microgrid and the centralized main controller (CMC) is responsible for coordinating the microgrid operations in NMGs. NMGs could thus function as modular resilience building blocks for cyber-secure modern power grids. In particular, the operation of NMGs is based on physical level networking, cyber level networking, and cyber-physical collaboration, which is the focus of the following content.

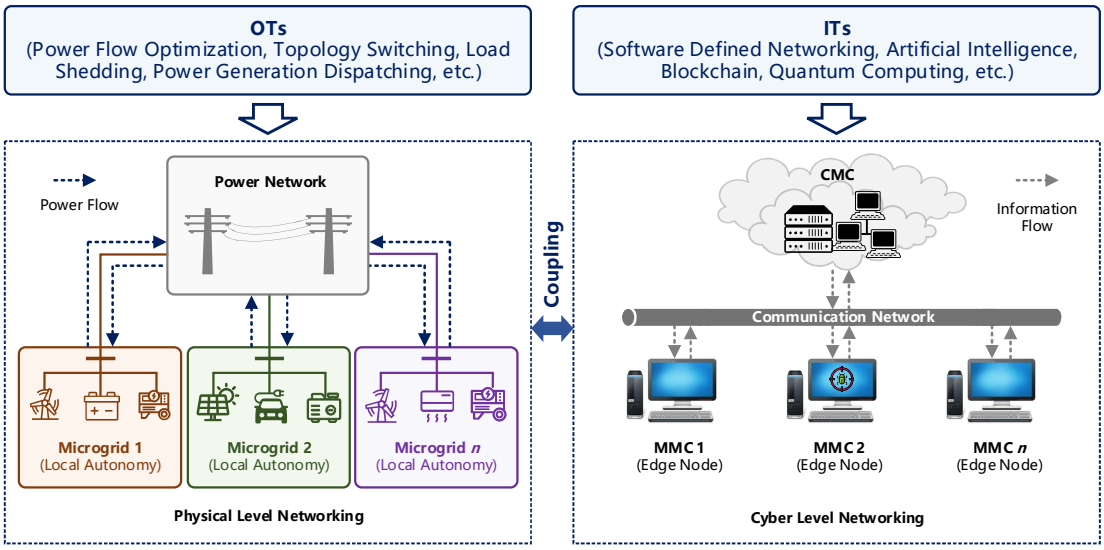


Fig. 1 Extensive use of OTs and ITs in the respective physical level and cyber level of NMGs.

1.1 Physical Level Networking

The physical topology of NMGs serves as the fundamental infrastructure for enabling collaborative operation and ensuring reliable energy supply. In practical applications, as shown in Fig. 2, four distinct topological structures have been widely adopted, each characterized by unique operational features and performance trade-offs [4].

(a) Radial Structure. This configuration features a simple, linear layout with power flowing exclusively in a unidirectional downstream manner from the main supply point to end-users. Its primary advantages lie in low construction and maintenance costs, along with straightforward design principles. However, this structure exhibits inherent limitations in flexibility when confronting contingency events (e.g., component failures or load fluctuations), as it lacks alternative power transmission paths.

(b) Tree Structure. By aggregating multiple radial branches into a hierarchical framework, this structure establishes clear and hierarchical protection relationships, facilitating simplified fault identification and isolation. Nevertheless, faults occurring in upstream segments can trigger the mandatory separation of all downstream microgrids from the main grid, thereby significantly elevating the risk of unserved energy and disrupting continuous power supply to downstream loads.

(c) Looped Structure. This topology forms closed, interconnected paths among participating microgrids, integrating redundant power transmission channels that enable dynamic rerouting of power flows following fault occurrences. Equipped with motor-operated switches, microgrids are empowered to rapidly isolate faulted sections while maintaining energy exchange along intact, healthy paths, effectively enhancing system resilience and reducing downtime during contingency events.

(d) Meshed Structure. Building on the looped configuration, this structure further increases multi-point interconnections, ensuring that the majority of microgrid pairs maintain either direct connections or short-path links. Consequently, the meshed structure delivers enhanced redundancy and controllability, supporting finer-grained allocation of voltage and frequency support services across the network. A notable trade-off, however, is the increased complexity in protection coordination logic and operational organization, requiring sophisticated control strategies to manage interdependent power flows.

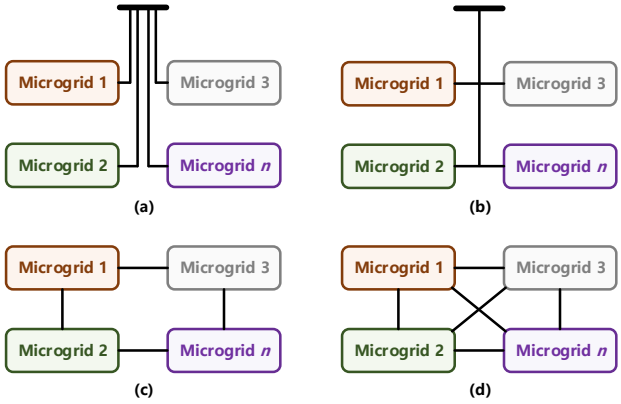


Fig. 2 Physical level networking topology of NMGs. (a) Radial structure; (b) Tree structure; (c) Looped structure; (d) Meshed structure

The selection of an appropriate topology is highly scenario-dependent, aligned with specific operational requirements and performance objectives. Radial or tree structures are well-suited for application scenarios where longer restoration times following contingencies can be tolerated, such as non-critical load areas with lower reliability demands [5]. Corridors requiring continuous service availability (e.g., critical infrastructure or industrial zones) favor looped structures integrated with preset automatic switching sequences and network reconfiguration strategies, ensuring rapid recovery from faults. High renewable energy penetration, frequent inter-microgrid energy exchange, and stringent resilience targets necessitate a meshed operating framework [6]. This structure achieves enhanced stability and elasticity through precise power-sharing mechanisms and coordinated control schemes, which in turn demand tighter protection setting configurations and switching interlock protocols to manage complex interdependencies.

Oriented towards cyber security and resilience enhancement, collaborative resilient operation regimes for physical networks of NMGs can be categorized into four core operational modes, each tailored to specific network states:

(a) Normal Interconnected Operation. The primary focus centers on optimizing economic energy exchanges, implementing loss minimization and congestion management strategies, operating within predefined tie-line capacity limits, and facilitating mutual support among neighboring microgrids to balance load fluctuations and improve overall energy efficiency.

(b) Contingency Operation. Upon the occurrence of faults, NMGs execute rapid isolation of faulted sections, initiate reconnection along healthy network paths, and prioritize power supply to critical load corridors, ensuring that essential services remain unaffected while mitigating the impact of disruptions.

(c) Intentional Islanding Operation. During this mode, NMGs dynamically form independent operating subareas centered around grid-forming sources (e.g., energy storage systems or synchronous generators). Subsequent to the recovery of the distribution network or adjacent subareas, NMGs implement resynchronization and reconnection procedures under predefined synchronization conditions to restore full networked operation.

(d) Black Start and Restoration Operation. This process commences with the activation of local DERs (e.g., diesel generators or battery energy storage) to establish an initial power supply. The supply area is then gradually expanded along predefined restoration routes, with a sequence of controlled network switching operations executed to systematically rebuild the complete networked structure, restoring full functionality and connectivity.

Meanwhile, topology and control are tightly coupled in collaborative resilient operation. Under multipath conditions, active and reactive power can be shared across parallel routes through droop and secondary control, and meshed structures are more favorable for fine-grained sharing and congestion relief [7]. Grid-forming sources located in different microgrids can provide coordinated inertia and damping through virtual impedance or power-synchronization strategies. After any topology adjustment or network switching, controllers need reconfiguration

awareness. They should promptly receive switch status and topology change information and rapidly update power-sharing setpoints, transfer limits, and protection coordination to ensure a smooth transition before and after switching.

1.2 Cyber Level Networking

The cyber level of NMGs acts as the information transmission and control backbone for realizing collaborative operation, serving as a critical bridge connecting physical components and operational strategies. The cyber topological structure directly determines data exchange efficiency, control responsiveness, and cyber security resilience, with design needing to balance functionality, scalability, and risk mitigation. In practical deployments, as highlighted in Fig. 3, five typical cyber topological structures have been developed, each with distinct communication mechanisms, performance characteristics, and security requirement profiles [8].

(a) Centralized Structure: Each local controller connects directly to the CMC, with no intermediate aggregators. The CMC manages all data collection and supervisory exchanges, which simplifies orchestration and supports fast actions such as emergency curtailment. The cyber risk concentrates at a single point. Strong identity for every node, mutual authentication before any command or measurement is accepted, signed and time-stamped messages, strict traffic segmentation, and hot-standby failover are required to prevent a single coordinator fault from disabling the network.

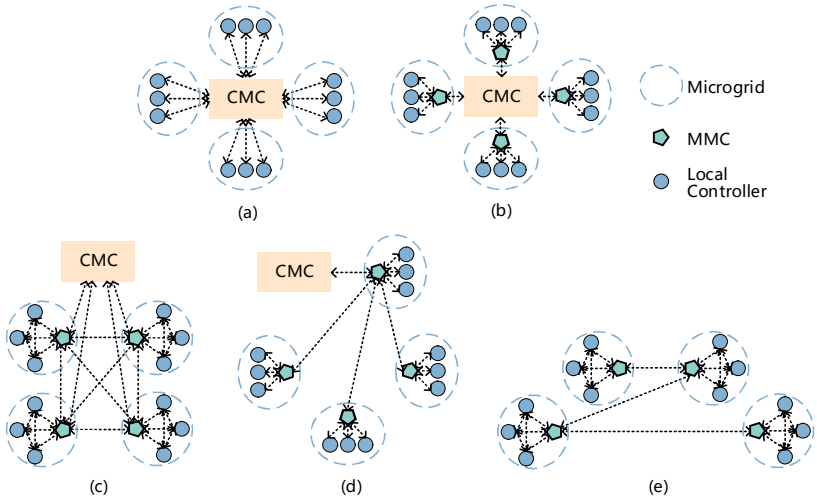


Fig. 3 Cyber level networking topology of NMGs. (a) Centralized structure; (b) Aggregated structure; (c) Meshed structure; (d) Pinning structure; (e) Peer-to-peer structure

(b) Aggregated Structure. A controller inside each microgrid serves as an aggregator that handles local traffic and exchanges summaries with the CMC. This structure reuses site networks and scales well for large NMGs with frequent exchanges. The CMC remains a critical dependency, and emergency response can be slower than in pure centralization. Gateways must enforce minimal disclosure, per-class allow lists for protection, control, metering, and maintenance, and authenticated sessions with rapid path failover so latency budgets are met during incidents.

(c) Meshed Structure. Compared with the aggregated layout, redundant links are provisioned among MMCs to raise flexibility and reliability for inter-MG exchanges. Redundancy removes single points of failure yet increases routing complexity and cost. Cyber security should convert this physical diversity into dependable service by enforcing zero-trust communication on every hop, end-to-end integrity checks, deterministic quality of service for control traffic, and fast reroute that keeps secondary control within its timing bounds.

(d) Pinning Structure. One MMC is appointed as a leader who communicates with the CMC, while other MMCs rely on the leader to disseminate supervisory commands. This structure limits the exposure of most participants and helps preserve privacy because only the leader shares operational information centrally. The leader's path becomes critical. Strong attestation of the leader, frequent key rotation, continuous time-integrity checks, and seamless leader

rotation with hot backup are needed so that cooperation does not stall when the leader or coordinator is impaired.

(e) Peer-to-Peer Structure. No central coordinator is present, and MMCs communicate directly as peers. This structure avoids single points of failure and preserves privacy since operational data need not be collected centrally. The main concern is control coherence and the time to reach consensus when many peers must agree. Cyber controls emphasize secure membership, message freshness with sequence numbers and time stamps, authenticated exchanges, and quorum rules that fall back to local authority when partitions occur, followed by safe reconciliation on rejoin.

Meanwhile, the growing complexity of communication technologies in NMGs stems primarily from the coexistence of wired and wireless solutions (see Table I). Both categories serve distinct roles in connecting field devices, MMCs, and the CMC, but their integration introduces unique cybersecurity challenges, especially in enforcing uniform protection policies across diverse architectures.

(a) Wireless Communication. Wireless communication technologies (e.g., Zigbee [9], Wi-Fi [10]) have gained popularity for interconnecting scattered field devices in microgrids [11], as they eliminate the need for physical cabling and support flexible deployment. However, their pervasive access points significantly enlarge potential exposures to cyber threats. Without strict access controls, attackers can exploit wireless vulnerabilities to gain direct access to the NMG cyber system, potentially disrupting real-time operations. Additionally, wireless devices often rely on protocols that may lack built-in security, further amplifying risk.

(b) Wired Communication. Wired communication remains a staple for critical links (e.g., between control centers and key substations) due to its higher stability and lower latency. Nevertheless, wired communication faces challenges from protocol diversity. Alongside proprietary protocols specific to vendor equipment, NMGs increasingly adopt open standards (e.g., IEC 61850 [12]) to enhance interoperability. These open protocols, while facilitating cross-vendor integration, carry inherent vulnerabilities that expand the attack surface. Moreover, the mix of wired and wireless networks complicates consistent policy enforcement, as security measures effective for one may not apply to the other.

Table I
TECHNICAL COMPARISON OF DIFFERENT COMMUNICATION TECHNOLOGIES APPLICABLE TO NMGS

Type	Technology	Security	Cost	Application
Wireless Communication	GSM	Moderate	Costly	Wide Area Network, Field Area Network
	GPRS	Low	Costly	Wide Area Network, Field Area Network
	Wi-MAX	Moderate	Moderate	Field Area Network
	ZigBee	Low	Low	Home Area Network
	Wi-Fi	Moderate	Moderate	Home Area Network
	Bluetooth	Low	Low	Home Area Network
Wired Communication	PLC	Low	Low	Field Area Network
	Optical Fibers	High	Costly	Wide Area Network
	DSL	Moderate	Low	Field Area Network

1.3 Cyber-Physical Collaborative Operation

From the perspective of a cyber-physical system, the underlying power network and the communication & control network have been incorporated as two highly interdependent subsystems in NMG operations.

(a) Structural interdependencies. As shown in Fig. 4, NMGs represent a sophisticated cyber-physical system, graphically representable as a hierarchy of interacting cyber and physical subsystems. In the physical subsystem, interconnection lines between microgrids and internal power corridors are abstracted as edges, while physical components (e.g., energy storage systems and local load aggregations) within a single microgrid are abstracted as a single aggregated node [13]. Similarly, cyber components (e.g., sensing devices, local controllers) associated with the same microgrid are abstracted as a single aggregated node in the cyber subsystem, with communication links

(including routers, switches, and protocol converters) serving as edges. Extensive structural interdependencies exist between the two subsystems, depicted as vertical cross-subsystem links in Fig. 4. Each microgrid's physical assets connect to a remote terminal unit or local controller for real-time monitoring and control of local processes, while the remote terminal unit and local controller rely on the microgrid's local power supply to maintain functionality.

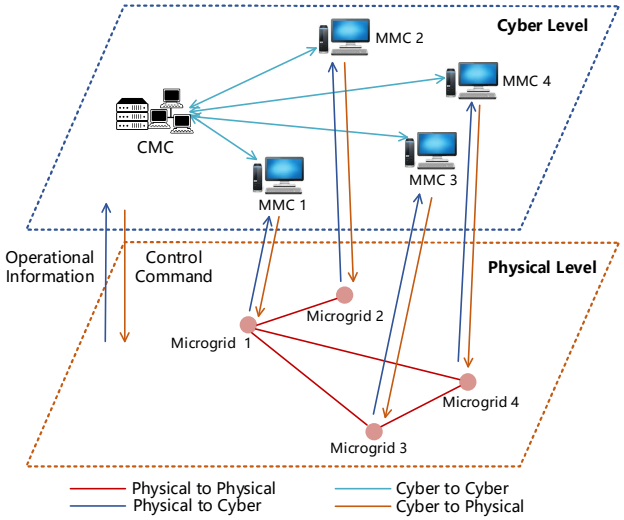


Fig. 4 Cyber-physical structural interdependencies of NMGs.

(b) Functional Interdependencies. Building on structural interdependencies, the physical and cyber subsystems of NMGs achieve mutual functional support and collaborative operations. The cyber subsystem plays a key role in maintaining the observability and controllability of the physical subsystem, while the physical subsystem provides the essential power foundation for cyber components to fulfill their tasks [14]. In principle, NMG operation can be abstracted as a closed loop where the two subsystems are tightly coupled. More specifically, remote terminal units or local controllers manage field devices to collect real-time measurements reflecting the physical subsystem's operating conditions, including analog data such as microgrid bus voltage magnitudes and digital data such as interconnection line breaker statuses. MMCs or distributed control nodes continuously interact with these terminal units via the communication network to achieve situational awareness, thereby continuously monitoring the physical subsystem's state. Subsequently, control nodes facilitate the MMCs' and the CMC's decision-making (e.g., adjusting power sharing ratios, optimizing renewable energy utilization, and re-dispatching distributed generation) and instruct terminal units via the communication network to implement control actions in response to changes in microgrid operating states or interconnection conditions.

2. The Role of Cyber Security in Networked Microgrids

Although NMGs pose significant potential in sustaining local power services under emergency operating conditions, they are also subjected to cyber incidents. Especially considering the close cyber-physical couplings, the impacts of cyberattacks not only threaten cybersecurity but also extend to the physical subsystem. Hence, it is necessary to first identify cyber vulnerabilities in NMGs, then analyze the impacts of cyber incidents on cyber and physical systems, and finally determine the system's operational state.

2.1 Cyber Vulnerabilities in Networked Microgrids

The tight cyber-physical coupling and closed-loop operational logic of NMGs render data the lifeline of reliable collaborative operation, which demands strict adherence to core data security pillars in availability, integrity, and confidentiality [15]. These pillars collectively underpin the effectiveness of situational awareness, decision-making, and control execution, directly safeguarding the safe operation of physical subsystems and the trustworthiness of cyber components.

(a) Availability. Availability means operators can obtain measurements, setpoints, and status in time to act, especially during contingencies [16]. Since operational data are time sensitive, excessive latency or loss of synchronization erodes situational awareness and degrades frequency, voltage, and restoration performance.

(b) Integrity. Integrity means data are trustworthy across their entire life cycle. Values collected by sensors should remain authentic and consistent as they traverse wired or wireless links, are processed by analytics, displayed on a human-machine interface, and archived in historians. Under all operating conditions, the reported information must reflect the real system state [17]. Unauthorized alteration needs to be prevented since corrupted measurements or commands can drive unsafe or inefficient behavior.

(c) Confidentiality. Confidentiality means only authorized parties can access or understand the information. Unintended disclosure can expose sensitive operational details and local data, which creates safety, financial, or privacy harm [18]. The preservation of confidentiality must not compromise timeliness or integrity, so protections are engineered with real-time control in mind.

After establishing availability, integrity, and confidentiality as the operational objectives, the next step is to identify where these guarantees are most likely to fail. In NMGs, the weaknesses are not uniform, but cluster in three layers (i.e., application software, communication network, and field devices). Each layer threatens availability, integrity, and confidentiality through different mechanisms (see Table II), for example, software misconfiguration corrupts data, network flaws enable interception and delay, and insecure devices undermine trust at the source. We thus review typical vulnerabilities layer by layer and indicate how each one degrades the three objectives.

(a) Application Software. Application software is often weakened by poor code quality, weak configuration and patch management, inadequate permissions and access governance, missing integrity checks, fragile error handling, and insufficient database protection [19]. These defects jeopardize integrity and confidentiality and can also collapse availability when faults or exploits crash services.

(b) Communication Network. Communication networks may lack effective intrusion detection and prevention, rely on weak or misconfigured encryption, provide limited monitoring and auditing, and miss anomaly tracking [20]. Such weaknesses enable eavesdropping, tampering, replay, and delay, which undermine availability, integrity, and confidentiality at once. The vulnerabilities resemble those of the IT domain, yet their consequences are amplified in NMGs because timing and ordering directly affect control stability.

(c) Field Device. Field devices introduce risks specific to OTs. Typical issues include unprotected physical access, improper device configuration, inadequate firmware protection, absence of tamper-resistant hardware, and weak authentication and authorization. These weaknesses threaten integrity at the source of truth, reduce confidentiality when local data can be read out, and compromise availability if devices are disabled or taken over. In practice, protocols and media reused from IT inherit their baseline risks, while the exact mix of devices and applications depends on the NMG design and configuration [21]. This is why vulnerability profiles and mitigation priorities are system-dependent and must be validated for each deployment.

TABLE II
Typical vulnerabilities in NMGs

Vulnerability Layer	Application Software	Communication Network	Field Device
Detailed Vulnerabilities Aspects	Bugs, Insecure Defaults	Protocol Misconfigurations	Wrong Device Settings
	Excessive Admin Rights	Open Interfaces among Microgrids	Local Accounts with Default Creds
	Missing End-to-End Protection	Unencrypted Links, Replay Risk	Insecure Firmware Signing
	Slow Updates, Legacy Libraries	Difficulty Patching Network Stacks	Hard to Update Remote Units
	Monolithic Service Stacks	Flat Networks, Lateral Movement	Device Networks Exposed
	Single Factor, Weak Tokens	No Mutual Authentication	Weak Device Identity
	Sparse Telemetry	Limited Flow and Intrusion Visibility	Local Logs not Retained

Further, compared with individual microgrid cases, cyber vulnerabilities in NMGs are substantially amplified by networking. The interconnection that enables collaborative operation also creates new attack vectors and expands the scope of potential disruptions, which are not present in standalone microgrid scenarios. These networking-induced vulnerabilities manifest most distinctly in two interconnected dimensions, each posing unique threats to the three core data security pillars.

(a) External Exposure Amplified by Interconnections. Networking extends the outward-facing interaction points of NMGs far beyond the boundaries of standalone microgrids. MMCs maintain continuous communication with the CMC to enhance overall energy system performance, connect to the Internet to access auxiliary data (e.g., weather forecasts, fuel prices) that optimize cross-microgrid energy management, and exchange operational information with peer MMCs to support cluster-level coordination [22]. Each of these connections creates potential entry points for external threats. For instance, compromised partner networks can transmit delayed telemetry data, replayed control commands, or corrupted time references into NMGs. Internet access further exposes systems to risks such as routing irregularities, distributed denial of service attacks, and application programming interface misuse. Shared infrastructure, such as network time protocol servers, adds another layer of risk. Time asynchrony from compromised sources can disrupt secondary control mechanisms, directly impairing availability. Software supply chains introduce additional vulnerabilities, too, as insecure third-party libraries or compromised update servers can exploit transitive trust relationships to infiltrate NMG cyber systems.

(b) Internal Vulnerabilities Aggravated by Heterogeneity. Interconnection introduces greater diversity in components, network architectures, and applications within NMGs, which in turn expands the overall attack surface. NMGs integrate MMCs, feeder interconnection devices, and boundary protection equipment from multiple vendors, each with different firmware versions. This diversity complicates patch management processes and lifecycle security oversight. Communication within NMGs spans multiple media, including substation buses, cellular backhaul links, and ad hoc wireless networks, each with unique trust requirements and timing constraints. This variety leads to inconsistent security postures across the system. Upper-layer applications, such as coordinated power dispatch, inter-MG energy trading, cross-cluster state estimation, and shared cybersecurity monitoring, require large volumes of data and precise time synchronization. The cybersecurity status of individual microgrids is thus linked to the stability of the entire NMG cluster. A single vulnerability in any part of the system, such as configuration inconsistencies, insecure edge device updates, or weak encryption keys, can enable threats to spread laterally across the cluster. For example, compromised sensing devices, such as sensors with outdated firmware, can degrade shared situational awareness. Misconfigured cross-site authentication mechanisms can grant unauthorized control access, which destabilizes the cooperative operation of the NMGs. In essence, while NMGs deliver enhanced flexibility and resilience, they also bind the cyber hygiene of all participating microgrids to the overall system stability, requiring more robust governance frameworks, defense-in-depth strategies, and continuous security verification processes.

2.2 Impact of Cyber Incidents on Operations

As integral components of the evolving smart energy ecosystem, NMGs feature dense cyber-physical integration, linking DERs to larger systems. The interconnected architecture, while enabling efficient energy sharing and resilience, also amplifies the consequences of cyber incidents, as attacks can exploit communication dependencies to disrupt both digital decision-making and physical power distribution. Below is an analysis of typical cyber incidents, derived cybersecurity requirements, impacts on operational states, and the intertwined cyber-physical consequences.

2.2.1 Cyber Incidents

Cyber incidents in NMGs exploit interconnected vulnerabilities to target data flows and control logic, with consequences of cyber incidents amplified by transitive trust relationships and power flow coupling. These incidents range from stealthy data manipulation to outright service disruption, often cascading across cluster members due to shared operational dependencies.

TABLE III
Typical cyber-incidents in NMGs

Attack Type	Availability Centric Incidents	Integrity Centric Incidents	Confidentiality Centric Incidents
Attack Incident Description	False Data Injection Tampering Sensor Readings and Phasor Streams	Denial of Service Flooding Cluster Links and Gateways	Data Exfiltration from Databases
	Man in the Middle Altering Commands and Messages	Controller Hijack via Malware or Stolen Credentials	Interception of Telemetry and Market Bids
	Forged Setpoints or Topology Files	Supply Chain Impacts for Persistent Disruption	Third Party Compromise Exposing Topology and Credentials
	Credential Theft and Replay Enabling Data Manipulation	Physical Cuts or Jamming of Communication Links	Insider Leakage of Schedules, Credentials

As shown in Table III, common types can be categorized based on the attack targets of cyber incidents.

(a) Availability Centric Incidents. Availability-centric incidents focus on preventing data or commands from moving where they are needed. Typical manifestations include denial of service on cluster coordination links, congestion at station gateways, failure of time distribution, and loss of cloud-hosted functions [23]. In NMGs, loss of availability does not simply slow supervisory tasks. It also pushes secondary and tertiary control into fallback, widens dead-bands, and forces conservative operating points that can increase losses and reduce transfer capability at tie lines. A cyber-secure design anticipates partial unavailability through deterministic local control, priority queues for protection and primary loops, and pre-validated setpoints that can hold the system in a safe region while higher layers recover. The 2015 Ukrainian power grid attack, for instance, caused power outages for 225,000 users through this type of attack. Man-in-the-middle attacks intercept communication data between microgrids and disrupt coordinated dispatching by forging or tampering with information. For example, inserting false commands into the power sharing process of DERs can lead to imbalanced current distribution. Additionally, credential abuse attacks exploit weak passwords or configuration vulnerabilities to steal access rights or forge cross-site authentication to gain control permissions. Such actions create pathways for subsequent attacks.

(b) Integrity Centric Incidents. Integrity-centric incidents seek to alter what the control system believes about the electrical state or to change issued actions without detection. Typical mechanisms include coordinated false data injection on phasor or meter streams, status falsification for breakers and tie switches, stealthy tampering of inverter setpoints, and manipulation of topology or asset models [24]. Since NMG control and restoration decisions rely on aggregated estimates across sites, small biases or inconsistent signals can propagate through cluster-level dispatch and protection logic and produce large unintended consequences. Physical validation of measurements, multi-source sensing with cross checks, signed commands combined with device-level plausibility filters, and reconciliation of state estimates across electrical boundaries reduce the attack surface and improve detectability. For example, an attacker who introduces small, correlated offsets into frequency and voltage measurements across several DERs can cause the cluster dispatcher to shift setpoints in a way that overloads a tie line and triggers protection relays. Another illustrative case is falsified breaker status information that causes the restoration algorithm to attempt reclosure of a transformer that is actually isolated, leading to miscoordination and delayed recovery.

(c) Confidentiality Centric Incidents. Confidentiality-centric incidents focus on extracting sensitive information about topology, asset capabilities, control relationships, or market bids [25]. Such leakage does not immediately alter control but materially increases risk by revealing choke points, maintenance windows, and identity relationships that an adversary can exploit later. The risk is amplified in NMGs by shared coordination platforms and third-party service providers that centralize visibility. Countermeasures include least privilege access, partitioned identity domains for inter-site functions, strict need to know for optimization and trading data, strong encryption and key management, and careful logging and anomaly detection for data exfiltration while preserving the fidelity needed for feasible schedules. As an example, access to planned maintenance and bidding schedules could allow an adversary to time an availability or integrity attack to maximize disruption or economic harm. Similarly, compromise of a third-party

coordination service that exposes topology maps and control relationships can reveal the most effective targets for subsequent attacks.In networked deployments, the three incident classes are tightly coupled and should not be treated as independent. Transitive trust, shared coordination platforms, and coupled power flows create attack chains in which a single event can touch confidentiality, integrity, and availability simultaneously. Examples include a supply chain compromise that first exfiltrates credentials and topology files, then injects forged firmware to alter setpoints while opening persistent backdoors for later denial of service, and an insider leak of schedules that enables timed man-in-the-middle operations combining data theft with command manipulation and channel disruption. Increasing cyber and physical vulnerabilities after networking microgrids, unfortunately, open up a new front to a potential "cyber-Pearl Harbor". It is thus of significance to identify the impact of cyber incidents on the operations of NMGs. Also, it is critical to pay further attention to strengthening the capabilities of NMGs for sustaining power services in the event of cyber incidents and protecting local customers when cyber-induced power outages occur.

2.2.2 Cyber and Physical Impacts

NMGs exhibit tightly coupled cyber and physical behaviors. Cyber incidents change the fidelity, timeliness, and privacy of information flows. Physical disturbances change electrical states and constraints. In a networked setting, these effects reinforce each other through coordination algorithms, shared infrastructure, and boundary controllers. Impact analysis should thus separate cyber-only impacts, physical-only impacts, and the coupling mechanisms that turn local faults into cluster-scale events.

(a) Cyber Impacts. In NMGs, the cyber layer spans cross-site telemetry, coordination services, boundary controllers, and shared identity systems. Incidents that hit availability slow or fragment cluster coordination links, degrade time distribution, and interrupt cloud-assisted optimization [15]. The result is a fallback of local and systematic control, wider dead-bands, and conservative setpoints that lower transfer capability at tie lines. Incidents that hit integrity bias phasor streams and breaker statuses, alter inverter setpoints in flight, or corrupt topology models used by cluster estimators. Small biases at one site propagate into cluster-level dispatch and restoration plans because aggregation hides local anomalies. Incidents that hit confidentiality expose topology, reserve posture, and maintenance windows. Leakage lets an adversary time low-grade interference to coincide with islanding or resynchronization [16].

(b) Physical Impacts. In NMGs, the physical layer couples members through tie lines, voltage support, and shared stability margins. Under cyber-attacks, NMGs may exhibit deeper frequency nadirs in weak islands, larger voltage excursions at peripheral feeders, and higher thermal loading on interconnections [19]. Conflicts between local droop and cluster secondary control can create poorly damped oscillations near boundaries. If corrective actions lag, operators must reconfigure topology, curtail generation, or shed load. Repeated operation near limits accelerates aging through thermal cycling and increases protection misoperations during frequent switching. These effects appear even when cyber services are nominal because power transfers, reserve sharing, and reactive exchange create interdependence among sites.

(c) Cyber Physical Coupling Impacts

Coupling in NMGs transforms small information faults into large power effects and small power disturbances into large information burdens. A biased phasor stream or forged breaker status at one site shifts cluster optimization toward unsafe transfers. The neighbor approaches thermal or voltage limits, although its local telemetry looks healthy. The initial information error becomes a physical overload that then propagates back as new alarms and estimator residuals, which further degrade decision quality at the cluster level. Time trust loss is a frequent catalyst for cascading [20]. Degraded or spoofed timing breaks the alignment of synchronous phasors and weakens differential and distance protection that rely on precise time. Resynchronization becomes hazardous. Controllers issue actions that are individually reasonable yet out of phase in aggregate. Out-of-phase closing and repeated reclose attempts increase mechanical and thermal stress. What began as a timing disturbance turns into persistent oscillations and extended restoration.

Further, boundary controllers will act as amplifiers for cascades. Selective delay or jitter on inter-site gateways desynchronizes local secondary loops from cluster coordination. One side damps while the other excites. Power oscillations persist and move across ties. As flows fluctuate, voltage control interacts with inverter limits and taps. Controllers chase a moving target and generate more switching, which produces additional data traffic and status churn that obscures the original cause [1]. Restoration phases intensify two-way cascades because topology and time change quickly, and operator workload is high. Partial communications create split views of network state. One controller believes a tie is open while another prepares a close. Inconsistent models drive conflicting actions that prolong islanding and increase energy not served. Each failed attempt adds more alarms and retransmissions, which congests channels that are already strained by high telemetry demand in weak islands [8].

As shown in Fig. 5, these cyber-to-physical and physical-to-cyber feedback loops create self-reinforcing cycles. The cluster drifts from secure toward alert as observability and controllability erode. If limits are crossed, the NMGs enter emergency mode with widespread constraint violations. If timing and topology awareness collapse together, the state can tip into extreme conditions with mis-segmentation, loss of synchronism, and equipment damage. Understanding these pathways clarifies why NMGs require impact analysis that treats information and power as a single coupled system rather than separate layers.

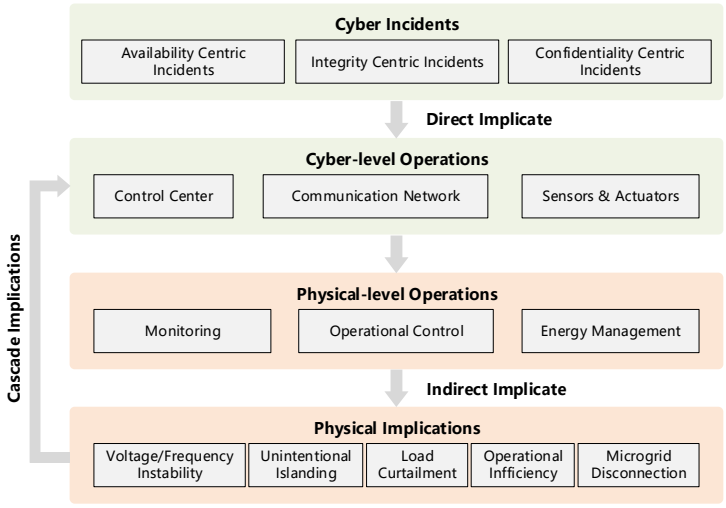


Fig. 5 Cyber-physical structural interdependencies of NMGs.

2.3 Operational State Classification

NMGs tightly couple the physical process with networked control and communications. Compared with a single microgrid, NMGs are more complex in measurement and control paths, cross-site coordination, and shared services, which improve observability and controllability, yet they also enlarge the information attack surface. Security awareness covers both physical security and cybersecurity. Physical security concerns whether states such as frequency, voltage, and current satisfy stability and equipment limits. Cybersecurity concerns whether availability, integrity, and confidentiality meet the service quality required by operations. Similar to the transitions among four states shown in Fig. 6, a failure on either side can be amplified by networked coupling into a cross-site supply risk [26], [27].

(a) Secure State. Both physical security and cybersecurity are satisfied. During grid-connected or cluster coordinated operation, measurements are trustworthy, communications are healthy, and control loops are stable. Power flows, and reserves across microgrids follow the plan, and boundary protection and synchronization work as designed, which is the target zone for normal operation.

(b) Alert State. Physical security remains within limits, yet cybersecurity is degraded. A typical case is denial of service or congestion on coordination links. Cluster energy management and secondary control must be downgraded.

Controllers inside and across sites rely on local default or preset steady settings to keep running. Cross-site trading and coordinated reactive support are paused or moved to conservative strategies. Since local loops of loads and DERs still function, voltage and frequency can stay near limits for a short time, but margins shrink. If the condition persists, the probability of entering a worse state increases.

(c) Emergency State. Cybersecurity can still be maintained, yet physical security is degraded. Typical cases include sustained thermal overload on lines or transformers due to extreme weather, or unintended topology changes that push tie-line flows beyond limits. Measurements and communications remain available, and control commands can be issued. Since physical constraints are active, flows must be reconfigured, load must be shed, or islands must be formed to return quickly to a stable region. For NMGs, this state often comes with cross-site constraint conflicts, for example, a clash between cluster-level reserves and local limits.

(d) Extreme State. Both cybersecurity and physical security are degraded. Natural disasters, long-lived malware combined with physical damage, or simultaneous deception of time synchronization and topology awareness can cause multiple microgrids to mis-segment, lose synchronism, mis-set protections, and suffer equipment damage. The cluster must quickly enter islanding and black start sequences, perform partitioned self-rescue, and prepare to regroup under trustworthy conditions.

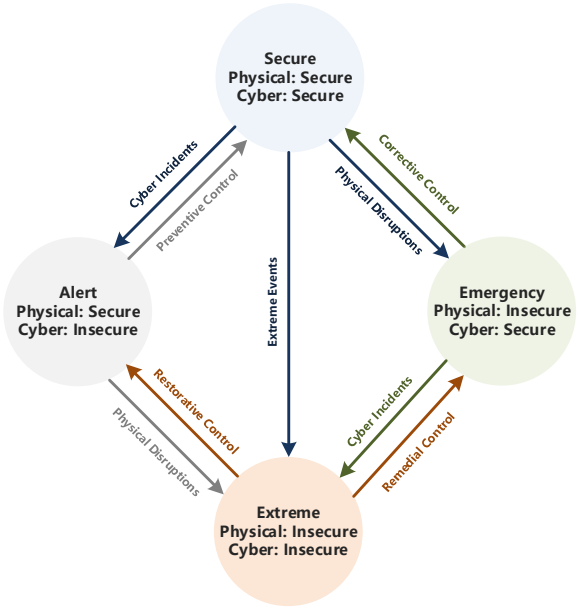


Fig. 6. Operational states for NMGs.

Among these states, NMGs define four control types to enable ordered transitions and recovery [28]-[30].

(a) Preventive Control. Preventive control returns the NMGs from alert to secure. The focus is to restore cybersecurity while preserving physical security. Actions include communication segmentation and allow list recovery, bandwidth and latency guarantees on critical links, rapid identity and key rotation, and smooth switching of cluster coordination from downgraded to planned modes. Preventive actions should be transparent to operations and should not disturb the real-time behavior of primary and secondary control.

(b) Corrective Control. Corrective control returns the NMGs from the emergency to secure. The focus is to restore physical security while maintaining cybersecurity. Actions include minimal topology reconfiguration by splitting or tying, redistribution of tie line flows, constraint-aware active and reactive retuning, and staged load shedding when required. For NMGs, the choice of corrective paths should use cluster-level state estimation and should prefer options that minimize impact on neighbors, so that a local issue does not spread.

(c) Remedial Control. Remedial control elevates the NMGs from extreme to emergency. The goal is to stop the

bleeding on the cyber side first and prevent further physical degradation. Actions include isolating compromised control domains and the management plane, switching to trusted local clocks and ordered buffers, enabling local autonomous droop and protection settings, and restoring situational awareness step by step through read-only monitoring channels. During this phase, the physical side may remain in a constrained yet controllable emergency region. Regaining basic command and observability is the priority.

(d) Restorative Control. Restorative control elevates the NMGs from extreme to alert. The goal is to restore physical security first and to avoid new cyber degradation. Actions include partitioned black start, layered recovery of frequency and voltage setpoints, stepwise synchronization and phase checks, and configuration and firmware recovery over trustworthy out-of-band channels. After the physical side returns to steady operation with adequate margins, Preventive control completes the restoration of cybersecurity and transitions the system to Secure.

Continuity and quality of supply ultimately depend on stability on the physical side, yet the cyber side has a leading and amplifying effect on that stability. Cyber-attacks can trigger incorrect commands and maloperations directly, and can also erode safety margins indirectly by reducing observability and controllability [31]. In NMGs, there is an additional concern about cross-site cascading. A wrong local state reported to cluster coordination can magnify neighbor tie line flows and reactive oscillations, or cause phase mismatch and closing shocks during restoration. The paired design of states and controls should follow the logic of isolate, stabilize, and reassemble: first constrain propagation, then stabilize locally, and finally recover coordination safely. In this way, the physical consequences of information attacks can be kept within the smallest controllable region, and security and resilience can be achieved at the cluster scale.

3. Cybersecurity Enhancement Enabled by Advanced Information Technologies

This section surveys cybersecurity enhancements for NMGs enabled by advanced ITs and focuses on four representative technologies (i.e., software-defined networking (SDN), blockchain, artificial intelligence (AI), and quantum computing). For each technology, we summarize its security benefits, key integration challenges, and implications for the cyber-secure operation of NMGs.

3.1 Software-Defined Networking

As DERs and edge control devices are integrated at scale into microgrids, communication and control structures inside NMGs show high dynamism, vendor heterogeneity, and real-time requirements. Conventional security mechanisms that rely on static rules and device-level configuration struggle to meet such demands. Fortunately, as shown in Fig. 7, SDN separates the control plane from the forwarding plane and enables centralized programmability and global visibility, thus offering a novel paradigm for NMGs' secure operation. The advantages of SDN and its potential applications in NMGs are clarified as follows:

(a) Security Management. Centralized and programmable control brought by SDN delivers clear advantages for security management. A logically centralized controller maintains a global view of network topology and traffic patterns, while installing fine-grained forwarding rules based on application context and flow characteristics [32]. The implementation of information flow-level policies enables network segmentation, strict information technology access control, and least privilege communication for control loops and measurement channels. Compared with static access control lists or fixed virtual local area networks, in the context of NMGs, SDN allows on-demand reconfiguration of communication paths, rapid isolation of compromised nodes, and mitigation of lateral movement by attackers [33]. Controller-side analytics in local microgrids can integrate real-time traffic visualization and correlation to improve detection of anomalies such as unexpected flows or latency spikes.

(b) Intrusion Detection and Automated Response. SDN enables additional approaches for intrusion detection and automated response. Flow statistics, packet mirroring, and sampling exposed via southbound interfaces feed supervisory control and data acquisition (SCADA) modules equipped in NMGs with rich telemetry. Detection outputs can translate directly into enforcement actions issued by the controller [34]. Example actions include insertion of

flow rules to block malicious traffic, rerouting critical control messages along safer paths, or triggering local backup controllers and protection schemes. Such closed-loop defensive capability becomes especially valuable for attacks that target timing or integrity of control signals, and that can otherwise disrupt wide parts of a microgrid within seconds.

(c) Flexible Placement of Security Functions. A combination of SDN and network function virtualization produces flexible placement of security functions such as firewalls, deep packet inspection, and timing integrity checks [34]. Virtualized security functions can reside near edge devices or close to a controller in local microgrids, depending on latency and compute constraints. Placement flexibility supports resource-efficient operation while preserving the real-time performance required by control applications. Logical network slicing and multi-tenant isolation enabled by SDN further reduce the risk of cross-contamination among control traffic, telemetry flows, and maintenance or third-party services.

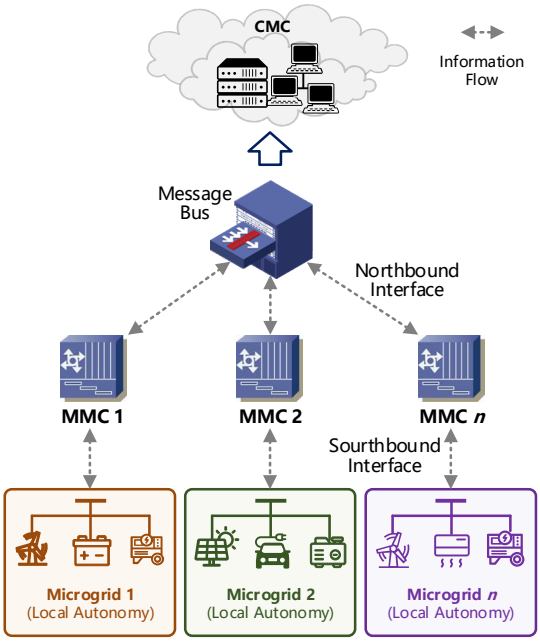


Fig. 7. SDN technology for NMGs.

Nevertheless, several important considerations deserve attention for secure SDN deployment inside NMGs, especially since real-time performance and overall resilience rank high owing to timing demands imposed by protective and control functions [1]. Common control algorithms for NMGs require bounded latency and tight synchronization across distributed controllers and field devices. Any added control plane delay or compromise of a single highly privileged controller can cascade into degraded stability of physical processes and unintended activation of protection schemes. To mitigate such risks, current research places emphasis on distributed controller architectures together with careful controller placement optimization, aiming to provide redundancy, reduce failover time, and maintain bounded control loop delays despite varying network conditions [7], [8]. At the same time, hardening controller platforms through strong authentication, role-based access control, deployment of trusted execution environments, and integration of hardware security modules helps shrink the attack surface and increases the effort needed for an adversary to obtain global control of NMGs. Besides, numerous microgrid assets communicate over industrial protocols or proprietary application programming interfaces. The secure integration of SDN with such equipment requires the development of standardized middleware and secure gateways that translate between SDN southbound semantics and legacy interfaces while enforcing authentication and policy constraints.

When SDN combines with complementary IT technologies, security posture and operational resilience can improve

significantly [1]. Integration with machine learning yields adaptive anomaly detection that learns normal traffic patterns and flags subtle deviations, while reinforcement learning can guide automated policy updates to reduce human intervention during incidents. Coupling with network function virtualization enables flexible chaining and scaling of security services, so resource-heavy inspection runs where compute capacity exists, while lightweight enforcement stays at edge devices. Trusted execution environments and hardware security modules provide hardware-rooted assurance for controllers and certificate management, thus raising the cost for adversaries seeking full system compromise. Distributed ledger technology offers tamper-resistant audit trails for policy changes and forensics without reliance on a single audit server. Further, convergence with industrial protocol gateways and secure middleware eases interoperation with legacy devices by translating southbound semantics into specific interfaces while enforcing authentication and authorization before commands reach control equipment in microgrids.

In summary, SDN offers a powerful toolbox for monitoring, segmenting, and defending NMGs' communication networks. Programmability enables automated and fine-grained policy enforcement, while telemetry and control integration allow detection outcomes to translate quickly into mitigation actions. The turn of research prototypes into robust industrial solutions will require work on controller trust, latency assurance, legacy device integration, and broad-scale validation. Cross-disciplinary collaboration among network security experts and power system engineers will accelerate the development of secure, controllable, and stable operation of NMGs supported by SDN.

3.2 Smart Contracts-Aided Blockchain

As microgrids evolve from isolated systems into collaborative NMGs that share energy, flexibility, and services across multiple operators, trust and coordination among independent actors become central concerns. Conventional centralized marketplaces and registries introduce single points of failure and raise questions about auditability, settlement speed, and cross-operator trust [35]. Blockchain technology, paired with programmable contracts, commonly called smart contracts, as represented in Fig. 8, offers a decentralized substrate for secure, auditable, and automated inter-microgrid transactions. Smart contract logic encodes business rules for energy trading, demand response settlement, and service level enforcement, while distributed ledger replication provides tamper-resistant records that support audit and accountability across administrative boundaries.

(a) Decentralized Energy Trading. Decentralized settlement and automated coordination brought by smart contracts deliver clear operational benefits, especially considering potential cyber-attacks. Peer-to-peer energy trades and flexibility exchanges among microgrids can be negotiated and recorded without reliance on a central broker when performing preventive power flow dispatch or implementing energy mutual aid under attacks [36]. Time-stamped ledger entries create an immutable audit trail for every exchange and support dispute resolution through transparent evidence. Automated settlement reduces manual reconciliation and associated latency in payment and balancing settlement, which improves economic efficiency for small-scale transactions that would be impractical under legacy clearing processes [37]. In addition, programmable contracts enable the enforcement of compliance rules such as certified renewable content, emissions attributes, and local congestion constraints, so grid resilience and policy goals remain aligned with market activity.

(b) Secure Consensus Mechanism. Secure consensus mechanisms inside a blockchain-based interconnection provide resilience and cross-validation of critical data flows [38]. Replicated transaction logs eliminate single-point corruption and make unauthorized retroactive changes extremely difficult without the consensus of multiple network participants. Consensus algorithms help guard against double-spending of flexible resources, while cryptographic identities and signatures ensure non-repudiation of offers and confirmations. Nevertheless, trade-offs exist among consistency, latency, and throughput that require careful design choices. Permissioned ledgers that limit the validator set to authorized microgrids can reduce consensus latency and improve privacy compared with open permissionless chains, yet governance and access control remain necessary to prevent validator capture. Also, privacy-preserving techniques such as zero-knowledge proofs and selective disclosure make it possible to publish settlement proofs on

a shared ledger without exposing microgrid-level data, thereby reconciling auditability.

(c) Advanced Coordination. Smart contracts support advanced coordination patterns that improve operational resilience when combined with edge automation and local controls. For example, contracts can implement conditional reserve procurement in which a microgrid requests backup capacity and a neighboring microgrid automatically commits resources when pre-defined thresholds are met and signed verification from phasor or meter readings confirms delivery [39]. Such automation reduces human intervention and shortens response time during contingencies. Contracts can also encode accreditation and certification workflows so only well-certified assets participate in inertia or frequency support processes, helping preserve power quality when cross-border services are activated. Finally, ledger-based timestamps and signed telemetry help establish provenance of control commands and measurement streams for NMGs, so forensic analysis after an attack incident becomes simpler and more reliable.

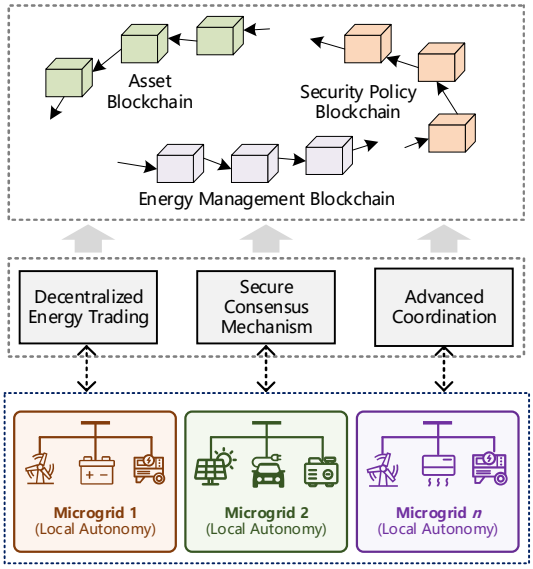


Fig. 8. Smart contracts-aided blockchain for NMGs.

Despite potential benefits, several important technical and institutional considerations deserve attention before large-scale adoption in NMGs. Performance and latency limits of many ledger implementations impose constraints on near real-time control applications, and bridging that gap calls for architectural patterns that separate fast control loops from slower settlement processes. Hybrid approaches that keep operational control at local MMCs while recording summary events and settlement triggers on a ledger appear promising because they preserve real-time stability while gaining tamper-resistant audit [40]. Interoperability remains another major issue because multiple microgrids may use incompatible data models, contract languages, and identity schemes. Standardized ontologies for energy products, meter data formats, and contract templates will reduce and simplify cross-network verification, which is critical for seamless coordination among microgrids. Governance and legal recognition of ledger records also require careful design to align with NMGs' distributed management structure, where no single entity controls all nodes. Contract code can automate many tasks in NMG operations, such as cross-microgrid energy trading or reserve sharing, yet legal frameworks must accept smart contract outcomes as binding and provide remedies for bugs or ambiguous clauses that could disrupt power flow or settlement in interconnected microgrids.

Further, the combination of SDN-governed control with smart contract-backed ledgers for inter-microgrid coordination produces mutual benefits that raise security and operational efficiency while preserving real-time stability [41]. SDN supplies fine-grained flow control, fast enforcement, and telemetry that keep local control loops deterministic and resilient, while ledgers provide tamper-resistant settlement, identity binding, and automated enforcement of cross-operator agreements. Practical integration follows several patterns. SDN can identify and

prioritize traffic tied to cryptographically signed market events or contract triggers so verification messages reach local controllers with minimal delay, and SDN telemetry can feed authenticated oracles that smart contracts use to determine settlement outcomes [42]. Conversely, finalized ledger entries and contract state changes can drive automated policy updates on SDN controllers so routing, slicing, and firewall rules reflect verified commitments instead of manual configuration. Hybrid architectures place latency-sensitive control inside SDN-managed local domains while recording summary events on ledgers through off-chain channels, thereby reconciling control loop timing with auditability and non-repudiation. Secure key management and trusted execution at both controller and validator endpoints reduce joint attack surface, while standardized application programming interfaces for meter data, contract schemas, and northbound SDN intents simplify cross-vendor integration. Co-designed validation and routing policies, together with formal verification of contract logic and oracle integrity, create a closed-loop that enhances trust, speeds response, and limits scope for fraudulent settlement triggers.

In summary, smart contracts aided blockchains present a compelling framework for decentralized inter-microgrid coordination that enhances trust, automates settlement, and provides auditable records across administrative boundaries. Realizing those benefits at scale requires careful attention to latency and throughput trade-offs, privacy of meter-level data, governance and legal acceptance, and secure oracle design. Research that combines cryptographic innovation, formal verification, scalable architecture, and cross-domain integration with SDN will accelerate the maturation of ledger-based solutions for secure and resilient inter-microgrid operation.

3.3 Artificial-Intelligence-Enabled Secure Operation

AI is emerging as a key enabler for improving cybersecurity and resilience of NMGs. Different AI paradigms provide complementary strengths (see Fig. 9), ranging from adaptive control through reinforcement learning, to physics-informed machine learning for anomaly detection, to federated training frameworks that preserve privacy across distributed controllers, and to large language models (LLMs) that assist operational decision making and interaction. The combination of diverse AI approaches enhances situational awareness, improves attack resistance, and facilitates coordinated operation of NMGs under dynamic and uncertain attack conditions.

(a) Reinforcement Learning Guided by Real-Time Control Feedback

Reinforcement learning agents can be trained to adapt cyber defense strategies by interacting with control environments and receiving feedback based on operational performance of NMGs, communication latency, and threat indicators [43]. Such agents learn policies that balance protection strength against control stability, for example, isolating suspicious flows while keeping control loops functional. Online learning allows policies to evolve as adversarial tactics change, which is crucial in networked microgrids where new attack vectors may emerge during reconfiguration or energy trading. Integration with programmable SDN controllers and blockchain settlement systems ensures that learned policies translate into actionable routing changes, contract verification triggers, or automated activation of backup resources.

(b) Physics-Informed Machine Learning for Anomaly Detection

Machine learning models that embed physical system knowledge provide stronger generalization and interpretability than purely data-driven approaches. By enforcing power flow equations, device dynamics, and operational constraints within the learning process, physics-informed models reduce false alarms caused by noisy telemetry and distinguish between natural fluctuations and malicious perturbations [44]. For example, spoofed phasor or meter data that violates Kirchhoff's laws can be flagged with high confidence, while normal renewable variability is tolerated [45]. Such models support anomaly detection, fault prediction, and event reconstruction, and are especially valuable in networked environments where multiple microgrids exchange both energy and data.

(c) Federated Learning across Microgrids

Privacy concerns and regulatory constraints often limit the sharing of raw operational data across different microgrids. Federated learning offers a distributed training paradigm where each MMC trains models locally on its own data and

shares only model parameters with a coordinating server or consortium ledger. Horizontal federation enables peer microgrids to collectively learn robust anomaly detectors or forecasting models without exposing raw measurements, while vertical federation allows integration of different feature sets from local subsystems into more comprehensive models managed by a higher-level central controller [46], [47]. Such approaches preserve privacy, comply with data sovereignty requirements, and simultaneously enhance accuracy by leveraging diverse datasets from multiple sites. Blockchain-based logging of model updates can further provide auditability and accountability in collaborative training.

(d) Large Language Models and Generative AI for Operator Support

Large language models (LLMs) bring new capabilities for human-centric interaction, knowledge management, and incident response in cyber secure NMGs' operation [48]. The MMCs and CMC can query system state in natural language, receive concise summaries of alarms, and obtain recommended mitigation steps drawn from technical playbooks and regulatory codes. Generative models produce structured reports, translate technical data into plain language, and assist in drafting access control policies or smart contract templates. LLMs can also help integrate heterogeneous logs, event reports, and vulnerability feeds, turning them into actionable intelligence. Careful oversight, validation, and alignment with safety constraints are essential to avoid unintended actions or inaccurate recommendations.

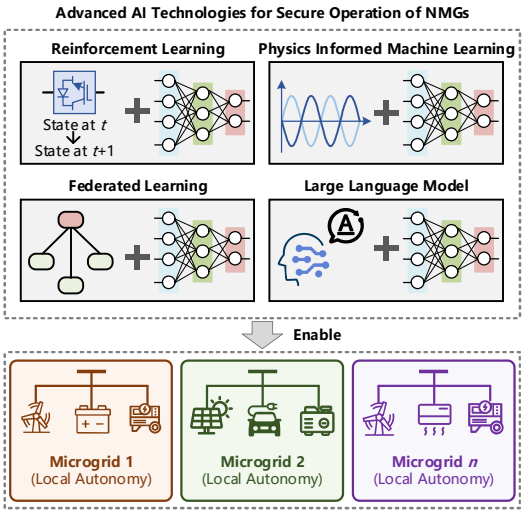


Fig. 9. Typical AI technologies for secure operation of NMGs.

Building on the advantages outlined above, AI clearly enhances situational awareness, anomaly detection, and adaptive defense for NMGs, while also raising several problems and risks. AI models are highly dependent on the quality and diversity of training data, making them vulnerable to poisoning, imbalance, or insufficient representation of attack scenarios [49]. Operational variations, device replacements, and topology changes may cause model drift, reducing performance if retraining pipelines are not maintained. The lack of transparency in many advanced models raises challenges for trust and regulatory approval of NMGs, while high computational costs can exceed the limits of edge devices, creating latency issues in time-sensitive control loops. Moreover, AI components themselves introduce new attack surfaces, since adversaries can attempt to steal parameters, manipulate inference outcomes, or exploit generative models to produce misleading recommendations.

To address emerging challenges, research could focus on hybrid and ensemble learning so that multiple models complement each other, which improves stability and ensures fallback choices when one method becomes unreliable [50]. For example, continuous learning pipelines combined with human participation provide a way to detect and correct model drift, allowing algorithms to adapt to operational variation, equipment replacement, and network

reconfiguration according to the operational states of NMGs without blindly accepting poisoned or misleading data. Uncertainty quantification together with digital twin validation enables the CMC and MMCs to assess confidence levels of prediction and to reveal weaknesses under simulated contingencies before models are deployed in real systems. Governance frameworks for federated learning, along with standardized audit records and certification processes, help strengthen accountability and build trust across different microgrids. Clear operational boundaries for LLMs further ensure that outputs remain supportive, focused on summarization and decision assistance, while critical control actions continue to rely on validated and transparent mechanisms.

Overall, AI functions as both an enabler and a source of new challenges for the cyber-secure operation of NMGs. AI benefits in adaptability and efficiency are significant, but sustainable progress depends on balancing innovation with caution, integrating AI tightly with physical system constraints, secure communication infrastructures, and institutional governance.

3.4 Quantum-Enhanced Secure and Efficient Operation

Growing attack complexity and richer IT stacks are pushing computational demand to new levels. SDN introduces fine-grained policies, dynamic slicing, and flow telemetry that must be optimized and checked in near real-time. Blockchain adds smart contract logic, settlement verification, and audit proofs across many parties. AI brings heavy training workloads, online inference, drift monitoring, and uncertainty tracking. Joint adoption of diverse ITs significantly increases state dimension, tightly couples cyber and physical decisions, and expands multiplies scenario space for risk analysis. Adversaries can coordinate across layers, craft low-and-slow campaigns, and exploit timing or data integrity. The CMC and MMC must solve large mixed integer programs, fast state estimation, contingency ranking, and accurate control under tight latency. Privacy and regulatory limits further restrict data sharing across microgrids, which complicates collaborative optimization. Such pressure motivates quantum technology as a complementary path that targets decision speed and link security towards resilience goals.

(a) Quantum Communication

Quantum communication could offer diverse benefits (e.g., higher robustness, synchronicity, connectivity, efficiency, and security) in the operation of NMGs. The most crucial advantage of quantum communication is its unparalleled security feature [51]. Quantum communication is based on the principles of quantum mechanics, such as the Heisenberg uncertainty principle and the quantum no-cloning theorem [52]. These principles ensure that any attempt to eavesdrop on the communication will inevitably disrupt the quantum state, immediately alerting the communicating parties. In NMGs, where control commands, energy production data, and consumption information are constantly being transmitted, this property can prevent malicious actors from intercepting and misusing this data. For example, if an attacker tries to measure the quantum-encoded data to obtain information about the power generation schedules of DERs in a microgrid, the very act of measurement will change the quantum state, and the cyber system of NMGs will detect this anomaly. Quantum communication is thus in stark contrast to classical communication, where sophisticated eavesdropping techniques can sometimes go undetected, leading to potential security breaches [53].

When extending to the cases of NMGs, the quantum key distribution (QKD) technology will serve as a reinforcement guarantee for secure communication among microgrids, where the classical channel is in parallel with the quantum channel [54]. As illustrated in Fig. 10, every individual microgrid within the network is outfitted with a quantum-capable controller. The quantum-capable controller undertakes two core functions: execution of local control protocols (including but not limited to frequency regulation, voltage support, and active/reactive power control) and exchange of secure information with controllers of peer microgrids. The information exchange process relies on the MMC, which serves as a central coordinator to facilitate inter-microgrid communication and maintain systemic consistency.

In particular, the secure quantum distributed control scheme adopted in this networked architecture operates through

three hierarchical layers arranged in a top-to-bottom structure (i.e., control layer, data layer, and physical layer). Each layer undertakes distinct yet interdependent roles to ensure overall system security and operational efficiency. The control layer assumes responsibility for systemic-level control tasks, management of inter-layer communication, and distribution of encryption keys to the data layer. These keys are generated via QKD protocols, which leverage the principles of quantum mechanics to ensure unconditional security against eavesdropping attempts [55]. The quantum channel is dedicated to the transmission of quantum states, and it incorporates built-in eavesdropping detection mechanisms, which exploit quantum properties such as the no-cloning theorem and wavefunction collapse. Any attempt to intercept or measure quantum states during transmission will introduce detectable disturbances, enabling real-time identification of malicious access. In contrast, the classical channel supports two primary operations: transmission of conventional data (e.g., microgrid operating parameters, control commands) and decryption of encrypted information using keys distributed by the control layer. The synergy between the control layer and the data layer establishes a secure information transmission and processing loop, which in turn enables secure, efficient, and distributed control of the underlying microgrid clusters located in the physical layer.

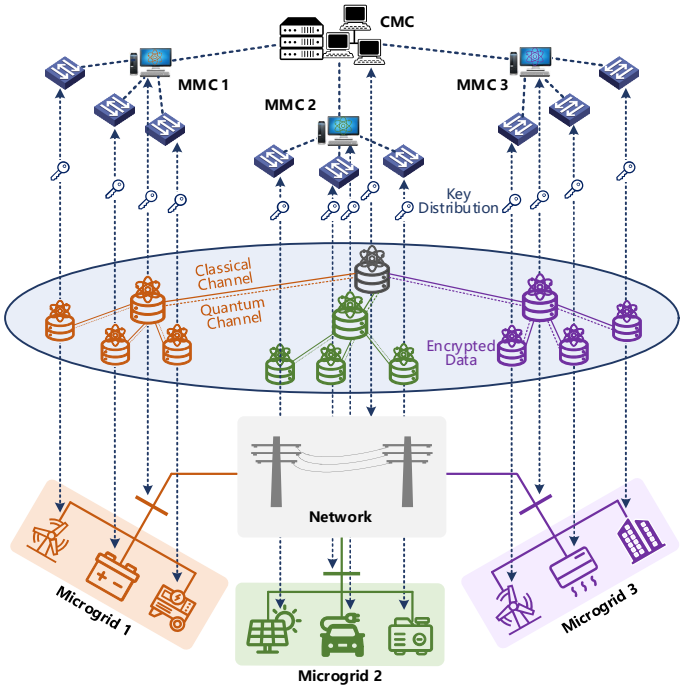


Fig. 10. QKD-enabled secure distributed control scheme among NMGs.

(b) Quantum Computing

Quantum algorithms offer acceleration for core bottlenecks in dispatch, topology reconfiguration, reserve allocation, restoration routing, and market clearing [56]. Variational circuits, such as quantum approximate optimization algorithms and annealing-style solvers, search large combinatorial spaces with high sampling efficiency and can return good policies within strict timing budgets [57]. Quantum linear algebra subroutines shorten regression, sensitivity studies, and fast updates in state estimation after disturbances. Amplitude estimation reduces samples for risk metrics compared with classical Monte Carlo, which supports rapid tuning of reserves during volatility. However, constrained by the limited number of qubits, obvious noise, decoherence, and other issues, practical pipelines commonly keep a hybrid form of quantum and classical computing [58]. Quantum backends make core decisions and explore candidate actions, while classical pre- and post-processing enforces hard constraints and shrinks problem size. Alternatively, the quantum and classical parts can be executed alternately by respective quantum processing units (QPUs) and classical processing units (CPUs) in an iterative manner to enhance generalization and scalability

[59]. For example, when a microgrid is attacked and a systematic defense decision is made, the cyber part of the problem contains a large number of discrete variables (e.g., signals, channel switches), which is naturally suitable for quantum computing, while the physical part mainly makes decisions on continuous variables (e.g., power, bus voltage, and power flow distribution), which is what classical solvers excel at.

Based on the above-mentioned models for respective MGs, as shown in Fig. 11, the overall decision-making process for NMGs is typically a peer-to-peer game, and this dynamic becomes even more complex under information attacks. Malicious actors may intercept price signals, distort energy demand/supply data, or disrupt communication between prosumers, undermining the fairness and efficiency of peer-to-peer negotiations. For instance, attackers could manipulate real-time balancing data to skew the Nash equilibrium toward their interests, or tamper with demand response coalition information to break cooperative game structures among aggregators. In such scenarios, quantum computing and quantum game theory emerge as critical safeguards to enhance game outcomes [60]. Quantum game theory introduces entangled strategic spaces that go beyond classical constraints. When prosumers adopt entangled strategies, they can achieve more robust equilibria (e.g., Nash equilibria with higher collective welfare) that are resilient to attack-driven data distortions, as quantum correlations reduce the impact of falsified information on payoff calculations. Meanwhile, quantum communication ensures that peer-to-peer interactive signals (e.g., price quotes, energy availability) remain unaltered and untappable, eliminating attack-induced information asymmetry that distorts classical game dynamics. Additionally, hybrid quantum-classical optimizers enable faster re-computation of market equilibria (e.g., Cournot or Stackelberg) in the event of an attack, allowing NMG stakeholders to quickly adjust strategies and restore fair, efficient peer-to-peer interactions before further losses occur.

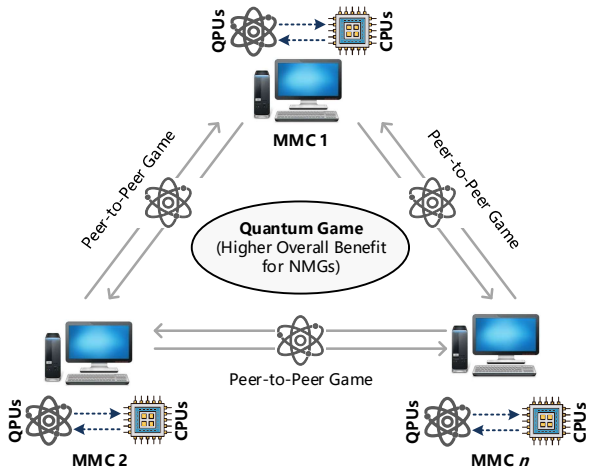


Fig. 11. Quantum-enhanced trading game in the energy market.

However, quantum hardware is costly and scarce, so per-site deployment of quantum resources across microgrids is rarely feasible [61]. A practical route relies on outsourcing, where hard subproblems are sent to a small pool of advanced and wealthy microgrids with quantum resources or to external quantum clouds. Blind quantum computing provides privacy during outsourcing, since each MMC can mask inputs, submit circuits to an untrusted server, and later verify outputs or recover results without revealing bids or meter data. Secure computing assurance is thus improved with verifiable delegation and lightweight proofs that catch tampering.

(c) Quantum Assisted Distributed Control

By combining quantum communication and quantum computing technologies, a typical application in NMGs is quantum-assisted distributed control [62]. The inherent parallelism characteristic of quantum information processing confers ultra-fast convergence of control algorithms to the distributed optimal control of NMGs, which allows controllers of neighboring microgrids to achieve coordination at speeds unattainable by classical control schemes. A

typical application scenario involves mitigation of sudden fluctuations in renewable energy generation (e.g., abrupt changes in solar irradiance or wind speed). In such cases, quantum-capable controllers detect deviations in renewable generation output in real time, then share updates on microgrid operating states through the secure quantum-classical dual channel. The secure state sharing mechanism triggers joint adjustment actions across multiple microgrids, including adjustments to energy storage system discharge rates or load shedding ratios, to maintain systemic stability and power balance.

To validate the effectiveness of this quantum distributed control scheme, some case studies have been conducted across both alternating current microgrids and direct current microgrids. For instance, the National Renewable Energy Laboratory in the United States simulates real-world operating conditions [63], including real-time disturbances such as sudden load changes, renewable generation intermittency, and communication channel noise. Results from these cases highlight three key performance enhancements (i.e., rapid synchronization of operating parameters across interconnected microgrids, smooth power sharing between microgrids with minimal deviation from setpoints, and robust system performance that maintains stability even under severe disturbance conditions). Such findings confirm the feasibility and superiority of the quantum distributed control scheme for application in NMG environments.

4. Deployment of Layered Defense-in-Depth Strategies

Effective cybersecurity uses a layered model from the device to the system level. Multi-layer defense framework includes the sensor/actuator layer, DER controller (device) layer, DER aggregation (aggregator) layer, individual microgrid (sub-system) layer, and overall NMG (system) layer.

4.1 Attack Resilient Sensing Layer

With the sensing layer acting as the first line of defense, its primary objective is to detect and localize information manipulation and communication interruption that target DER controllers. The detection needs to cover attacks that compromise an aggregate multi-DER controller and attacks that corrupt the communication links between primary DER controllers and the aggregate multi-DER controller. The sensing architecture must thus provide both high-fidelity local measurements and aggregated views that permit cross-device correlation. The hardware and signal paths in the sensing layer support multiple detection modalities [64]. Local voltage and current sensors supply the DER primary controller and a local detector. Measurement streams are duplicated where possible so that an independent cyber intrusion detector can compare the original and duplicate streams.

Meanwhile, detection algorithms exploit the different spatio-temporal signatures of local faults and coordinated attacks [65]. At the primary control layer, anomalies are fast and localized, appearing as small but rapid deviations in inverter output or in high-frequency spectral content. At the aggregate control layer, anomalies emerge through coherent deviations across many DERs and through persistent biases in aggregated power and voltage at the feeder level. Combining time series analysis, spectral methods, and cross-device correlation may improve sensitivity to these distinct signatures. In particular, fast local detectors monitor high bandwidth signals and trigger immediate mitigation actions when they detect unsafe dynamics [66]. An aggregate cyber intrusion detector ingests summarized and raw streams from many DERs and applies correlation tests, model-based consistency checks, and watermark verification. The aggregate detector also ranks anomalies by confidence and scope so that appropriate remediation steps can be taken without disrupting benign transients.

In practical engineering, watermark injection design should balance detectability and operational impact. Also, watermarks should be low amplitude and spectrally shaped to avoid degrading power quality [67]. As shown in Fig. 12, verification routines at the cyber intrusion detector test for the presence, phase, and amplitude of the watermark. Missing or distorted watermarks are a high-fidelity indicator of tampering or of path-level failures. Data fusion and trust scoring reduce false positives while improving location accuracy. The sensing layer should fuse measurements from the inverter, combiner box, local SCADA, and the transformer secondary. Each data source receives a trust score based on recent consistency, watermark integrity, and link-level indicators such as latency and packet loss. An

anomaly that affects only low-trust sources is deprioritized, while anomalies that span high-trust sources trigger elevated responses. Besides, the watermark is better pseudo-random and device unique when possible, so that replay attacks are harder to mount.

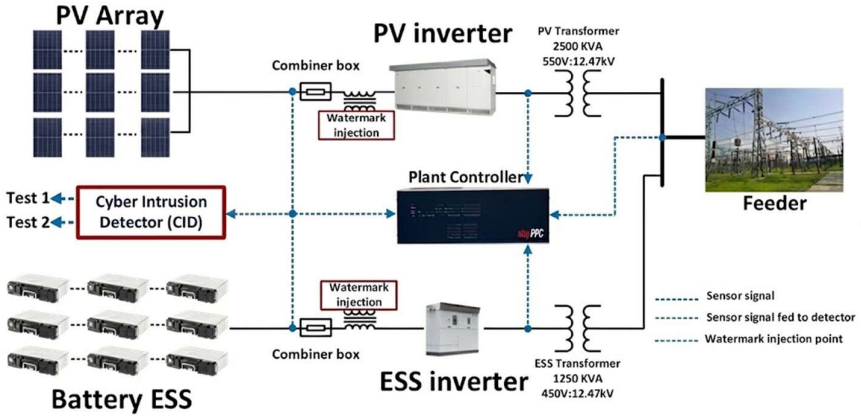


Fig. 12. Watermarking implementation in local devices of NMGs for detecting cyber-attacks on sensor information.

The sensing layer serves as the "perceptual nervous system" of NMGs, undertaking the fundamental task of collecting, transmitting, and preprocessing key operational data, including real-time electrical parameters (voltage, current, frequency, and power flow), environmental conditions (temperature, humidity, and irradiance for renewable energy sources), and device status (inverter operation mode, battery state of charge, and switchgear position). This data forms the basis for all upper-layer functions of NMGs, such as coordinated control of DERs, load forecasting, fault location, and optimal dispatch [68]. With the deepening interconnection of multiple microgrids, the sensing layer has evolved from a single-microgrid localized system to a distributed, multi-node networked architecture. However, this evolution also expands its attack surface: malicious actors can target sensing devices, communication links, or data preprocessing units to disrupt data integrity, availability, or confidentiality, thereby triggering cascading failures such as incorrect DER scheduling, false fault alarms, or even large-scale power outages across interconnected microgrids. Thus, the construction of an attack-resilient sensing layer has become a core prerequisite for ensuring the stable, secure, and reliable operation of NMGs.

With the widespread adoption of power electronics in NMGs, attack-resilient sensing has become increasingly complex. Faster dynamics, greater device heterogeneity, and tighter coordination increase both the signal space that detectors must monitor and the ways attackers can hide, motivating three complementary families of detection methods with different tradeoffs [69]-[71].

(a) Signature-Based Detection. This family matches incoming patterns to a curated library of known attack traces. It offers fast, low-cost decisions and performs well against replay attacks and well-studied false data injection tactics. The main weakness is brittleness, because adaptive adversaries or small timing and amplitude mutations can evade exact matches, and evolving operating points in NMGs produce drift. Practical improvements include continuous library updates with online learning, active testing through drills, physics-informed templates that encode power balance and protection rules, and similarity scoring that tolerates jitter and scale changes.

(b) Learning-Based Detection. Neural and representation learning models fuse many streams, such as phasors, setpoints, and logs, to detect subtle multivariate anomalies that are hard to handcraft. The strengths are flexibility and the capacity to learn complex boundaries, while the barriers are data hunger, label scarcity, and concept drift. A pragmatic recipe for NMGs is self-supervised or contrastive pretraining on large volumes of normal data, few-shot fine-tuning on curated attack simulations, uncertainty-aware outputs, and physics-grounded guardrails that penalize outputs violating power conservation or feeder limits. Federated training across sites helps capture diversity while protecting privacy, and continuous monitoring for drift enables lightweight retraining or fallbacks.

(c) Time-Based Stochastic Models. Hidden Markov, semi-Markov, and change point methods encode temporal structure and yield interpretable state sequences such as normal, stressed, and compromised. They require modest data, support online inference, and provide clear alarms tied to state transitions. The limitation is the stationarity assumptions that conflict with nonstationary NMG conditions. To remain valid, these models can use switching or time-varying parameters, incorporate exogenous inputs including attack signals, and combine residuals from physics-based observers with robust change detection that controls false alarms during planned reconfiguration and islanding.

4.2 Attack-Resilient Local DER Control Layer

Under cyber-attacks, conventional resilient local control emphasizes preservation of local stability while reducing dependence on external communications. For example, information-centric local control strategies minimize routine exchanges and transmit only when control-relevant variables change, thereby shrinking the exposed attack surface and lowering bandwidth requirements. Event-triggered and self-triggered schemes put this principle into practice, and local estimators produce compact indicators such as incremental Lyapunov differences and residual tests to govern communication and setpoint updates [72]. Robust inner loops designed on passivity or H_∞ principles enforce bounded gains, anti-windup, and rate limiting, and setpoint filters together with timing buffers treat variable latency and jitter as disturbances so that delayed or corrupted messages do not drive the plant toward unsafe operating points [73]. When the integrity of external inputs degrades, controllers move into safe degradation modes that hold external references, prioritize locally synthesized frequency and voltage, and enforce conservative droop and thermal limits to preserve operation without coordinated cues.

The increasing predominance of inverter-based DERs amplifies the importance of strong local control. Primary control at each inverter closes fast local loops and generates setpoints from local measurements while treating higher-level objectives as soft references. The immediate requirement is maintenance of voltage, frequency, and current within safe bounds under imperfect or adversarial communications. Cyber incidents that disrupt coordination typically appear as small, rapid deviations, which can accumulate because inverter dynamics evolve on millisecond to sub-second timescales. Local controllers must detect, isolate, and mitigate such disturbances before they propagate through the network. Clear delineation of roles between grid-forming and grid-following units enhances resilience (see Table IV). Grid-forming inverters sustain frequency and voltage through droop and virtual inertia together with conservative gain scheduling under uncertainty [74]. Grid-following units track those references with phase-locked loops that incorporate spoofing-aware filters and anomaly checks on phase and frequency excursions [75].

(a) Grid-Following Control. In the NMG context, the grid-following units are hardened by improving phase estimation and by limiting the impact of corrupted references while the microgrid operates in either islanded or grid-connected mode. The phase-locked loop uses adaptive notch filters and dual second-order generalized integrators to ride through harmonics and direct current offsets measured at the point of common coupling. Guards on the rate of change of frequency and on abrupt phase steps reject implausible jumps, and residual tests compare predicted and measured quadrature axis errors to flag spoofed inputs. When time references from the wider grid are mistrusted, the controller falls back to a local oscillator that is disciplined by multiple time sources rather than a single global positioning system feed. If the angle estimate remains uncertain, the control relaxes into power synchronization or virtual oscillator operation that does not rely on a tight phase-locked loop, which preserves stable current regulation and bounded tracking error for the connected feeders and loads within the microgrid.

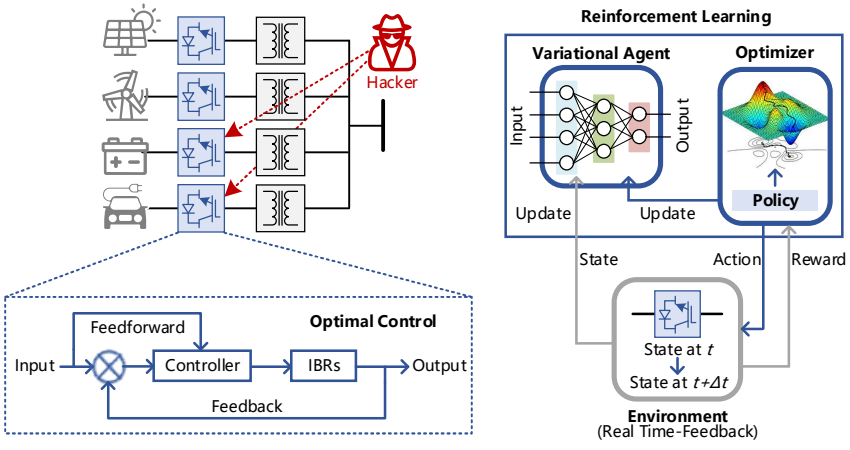
(b) Grid-Forming Control. In the same NMG setting, the grid-forming units protect network quality by shaping impedance and enforcing safe current delivery for critical buses and feeders. Virtual impedance and scheduled droop gains tame circulating currents among parallel inverters and damp low-frequency interactions across the microgrid lines. Current limiters with bumpless transfer keep converters within thermal and protection limits without large voltage sags at sensitive loads. During faults or spoofed commands, the voltage references are rate limited and filtered to avoid abrupt steps. The unit synthesizes local frequency and voltage for the islanded microgrid, holds conservative

droop gains, restores phase with a slow locked ramp toward the main grid, and closes tie breakers only after angle, frequency, and voltage mismatches fall within thresholds for a defined dwell time. These measures keep local operations stable under compromised information and enable a smooth return to coordinated service once trust and integrity are reestablished.

TABLE IV
GRID-FOLLOWING AND GRID-FORMING CONTROL STRATEGIES FOR INVERTER-BASED DERS UNDER ATTACKS

	Grid-Following Control	Grid-Forming Control
Primary Function	Track External Voltage and Frequency References	Provide Voltage and Frequency References for Local Nodes
Control Elements	Phase Tracking, Current Regulator, Reference Tracking	Virtual Inertia, Droop Control, Voltage Regulator
Detection	Phase-Locked Loop Anomaly Checks and Residual Tests	Integrity Checks on Incoming Setpoints
Mitigation	Hold Last Trusted Reference and Apply Conservative Limits	Conservative Gain Scheduling and Islanding Fallback
Recovery Behavior	Operate on Held References and Bounded Commands	Smooth Ramp from Autonomous to Coordinated Mode
Typical Timescale	Millisecond to Sub-Second	Sub-Second to Seconds

Further, recent advances in ITs strengthen the local DER control layer, and reinforcement learning represents the most prominent example of this advancement with respect to the dynamic environment under cyber-attacks. As shown in Fig. 13, integration of reinforcement learning with optimal control functions strengthens the local DER control layer by combining adaptive, data-driven policies with constraint-aware optimization and formal performance guarantees [76]. Optimal control in Fig. 13(a) with quadratic or nonlinear cost functions provides an explicit handling of voltage frequency and current constraints and of thermal limits through receding horizon optimization. Value functions from reinforcement learning in Fig. 13(b) can supply informed terminal costs and warm start policies for the optimization, reducing online computation and improving robustness to model mismatch. Safe or constrained reinforcement learning formulations supply policy priors that respect hard limits, while robust optimal control techniques such as H_∞ synthesis or tube-based model predictive control offer worst-case stability margins when uncertainty or spoofed inputs arise. A detection-guided architecture enables detectors and residual tests to trigger short-horizon re-optimization or a switch to a certified fallback controller when anomalies are detected, thereby preserving safety during adaptation. Practical real-time operation relies on convex formulations, fast quadratic program solvers, warm starting, or explicit model predictive control lookup tables together with compact policy networks for inference bounded in time. Offline co-training across varied attack and timing scenarios and domain randomization improves transfer to field hardware and reduces online tuning needs. The resulting hybrid preserves the local performance priorities of the primary control layer while adding adaptivity to evolving cyberattack patterns and maintaining provable constraint satisfaction.



(a) (b)

Fig. 13. Reinforcement learning for local DER control. (a) Optimal control for inverter-based DER under cyber-attacks; (b) Real-time reinforcement learning scheme for inverter-based DER.

4.3 Attack-Resilient Aggregated Multi-DER Coordinative Control Layer

Attacks can enter a microgrid through communication channels, aggregators, and the coordination layer, disrupting normal operation. The most damaging pattern is a stealthy attack that spreads gradually, which makes early detection by conventional protection and single-layer anomaly detectors very difficult. A stealthy false data injection attack targets control signals so that effects are not immediately visible to controllers or detectors, while selected states drift toward instability. Divergence can remain hidden until the system reaches a tipping point, at which time individual DER controllers begin to fail, and cascading effects emerge, rendering measurement-centric intrusion detection largely ineffective. The objective of the aggregated multi-DER coordinative control layer is to lower the likelihood of such attacks succeeding and to limit their impact. The aggregated multi-DER coordinative control layer commonly introduces a guard control unit within the primary coordinator that makes timely decisions with minimal communication, strengthening resilience from the earliest moments of an event and shrinking the attack surface [77]. The guard unit identifies safe operating regions in real time, estimates short-horizon trajectories for resource clusters, and isolates misbehaving subsets promptly. Once an anomaly is confirmed, the coordinator issues coordinated corrective actions by reconfiguring operating modes and adjusting setpoints of healthy resources, thereby restoring voltage and frequency autonomously.

In particular, the attack-resilient aggregated multi-DER coordinative control layer operates as one integrated pipeline that starts at ingress, formalizes safety online, and coordinates recovery in real time. The guard control unit first compresses risk where commands and measurements enter the system, so subtle manipulation becomes observable, which motivates the input enhancement to expose early anomalies. The same guard unit then turns state estimates into enforceable margins through certificates that define where the cluster can move safely, which sets up the coordinative safety certification. With a certified boundary in hand, the coordinator drives short-horizon prediction and resilient agreement across heterogeneous resources so healthy devices act in concert even under adversarial behavior, which delivers the guarded predictive coordination. Together, these stages shrink the attack surface early, anchor decisions to provable safety, and restore service through coordinated actions.

(a) Input Enhancement to Expose Early Anomalies. Multi-DER coordinative control first compresses risk at the point of entry, then makes stealthy manipulation visible. Envelope limits and rate limits keep active and reactive setpoints inside device ratings and interconnection codes [78]. To defeat replay and stealthy false data injection, the coordinator could inject low-amplitude dynamic watermarks on low-sensitivity channels, then watch for watermark distortion in the response to produce detectable residuals. Dynamic or physics-aware watermarking has been shown to expose replay and false data injection in energy systems, including inverter-dominated settings. The residuals are strengthened by model-based observers. An unknown input observer reduces sensitivity to corrupted channels while a Kalman framework reconstructs trustworthy signals, which helps separate genuine disturbances from adversarial injections. Parity or null-space tests can run in parallel to widen coverage in direct current or alternating current microgrids. Recent studies demonstrate designs that blend unknown input observers with Kalman filtering and report robust detection for microgrid scenarios [79].

(b) Coordinative Safety Certification. When inputs still look normal, yet evidence hints that trouble is forming, multi-DER coordinative control fuses estimation with certificates that define an actionable safety boundary [80]. A bank of observers produces a unified state picture, after which the coordinator evaluates control barrier functions and control Lyapunov functions online to certify safe sets for frequency and voltage. Distributed barrier-certificate methods have been formulated specifically for inverter-based NMGs and provide computable procedures to keep trajectories inside certified regions during transients. Extensions verify transient safety via invariant set conditions derived from fundamental results such as Nagumo’s theorem, giving constructive algorithms for safety-admissible controls [81]. If wider operating envelopes are required, physics-guided learning can be wrapped with certificate constraints. Neural or layered controllers are trained with barrier and Lyapunov conditions so that the run-time policy

carries an explicit safety margin that feeds the downstream coordinator without sacrificing responsiveness. Surveys and preprints on safe inverter-based voltage control summarize these certificate-guided learning approaches for NMG operation.

(c) Guarded Predictive Coordination. Multi-DER coordinative control drives recovery with short-horizon guarded prediction on aggregated photovoltaic and battery states. Tube-based model predictive control treats measurement tampering and acknowledgement delay as bounded uncertainty, so predicted trajectories remain inside certified safe sets. Precomputed mode switches enable temporary grid-forming behavior at anchors, adaptive droop near weak buses, rapid battery support that arrests the rate of change of frequency, plus staggered ramps that avoid lightly damped oscillations [82]. Byzantine-resilient consensus uses weighted mean-subsequence-reduced logic, so extreme proposals lose influence and group targets stay inside the convex hull of normal agents. Reputation or trusted anchors raise fault tolerance under sparse gossip schedules and hold-last sampling. Template-based reconfiguration maps anomaly fingerprints to verified action sequences so isolation, re-dispatch, and service restoration proceed as a single integrated loop.

In practice, given the implementation complexity, response speed requirements, and the need for lightweight communication and computing resource consumption, consistency algorithms emerge as a viable solution [83]. Fig. 14 presents a structured consistency control approach for coordinated *V*-*Q* and *f*-*P* regulation among multiple DERs. When a microgrid in NMGs is subject to a cyber-attack that distorts node voltages and line power flows, rapid coordinated containment among DERs is necessary to avoid propagation into the interconnected network and the onset of system-level oscillations or instability. Consistency control operates at the multi-DER level to provide a fast response to local deviations while confining the disturbance inside the attacked microgrid. According to the prevailing power flow, the downstream microgrid is represented as an equivalent load (with voltage $U_{\mathrm{down},t}$, active power $P_{\mathrm{down},t}$, and reactive power $Q_{\mathrm{down},t}$), and the upstream microgrid is treated as the slack bus (with voltage $U_{\mathrm{up},t}$, active power $P_{\mathrm{up},t}$, and reactive power $Q_{\mathrm{up},t}$). Under this representation, energy storage units carry out consistency control focused on *f*-*P* adjustment while photovoltaic units provide consistency control aimed at voltage support and reactive power balancing. The coordinated actions strive to maintain the attacked microgrid's external equivalents so that upstream and downstream interfaces observe minimal change. Such coordination among DER controllers and the aggregator gateway enables transition back to nominal operation once data integrity and timing are restored.

4.4 Attack-Resilient Sub-System-Level Individual Microgrid Control Layer

Individual microgrids encompass fast primary controllers for individual DERs operating on a microsecond time scale, followed by an upstream aggregate controller that ensures coordinated control of the multi-DER in the millisecond time scale [84]. Fig. 15 depicts a multi-scale, multi-layer control architecture for a microgrid in which an attack detection system (ADS) is co-located at critical interfaces to enable continuous monitoring and rapid response. At the DER level, primary and secondary controllers close fast local loops on microsecond to millisecond timescales, and the ADS units at those boundaries detect anomalies that may arise from spoofed measurements or timing attacks. At the coordination layer, a multi-DER controller operating on millisecond timescales exchanges resilient communications with DER controllers and the ADS units, so that detection events can trigger either local safe degradation or short-horizon re-optimization depending on severity and timing. An aggregator gateway spans the millisecond to second timescale, serving as a client to utility services and as a server to local facilities, and it supports higher-level functions such as consistency checks, signature-based validation, and policy-based mitigation. Sub-system level SDN techniques assist tertiary controls by providing correctness verification, policy enforcement, and automated vulnerability discovery, which in turn reduces attack surface and improves coordinated recovery [85]. The overall architecture thus implements detection, isolation, and mitigation across nested timescales while preserving local stability and enabling smooth transitions back to coordinated operation once integrity and timing are restored [86].

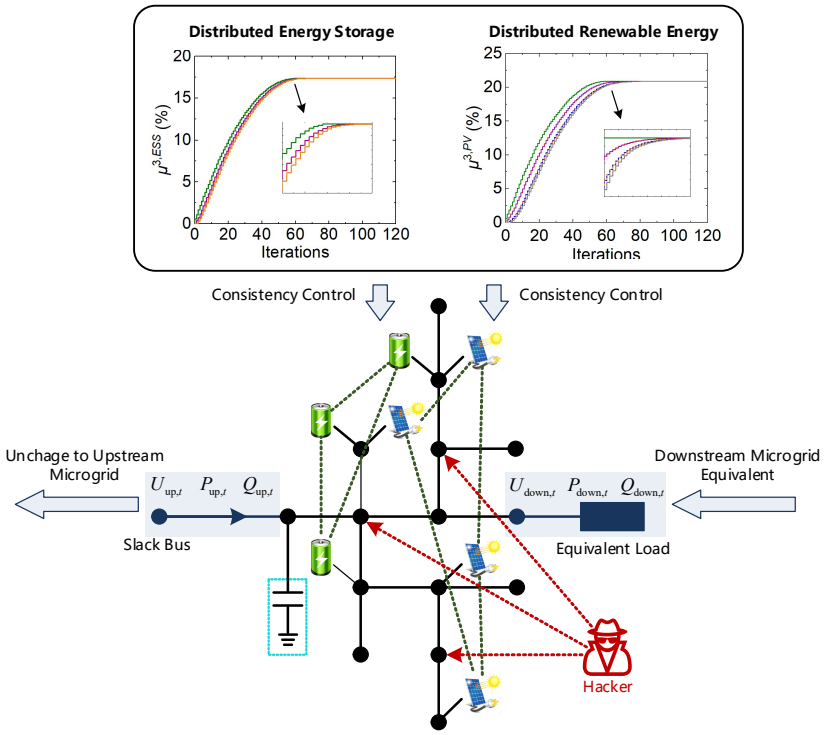


Fig. 14. Consistency control for multi-DERs under attacks.

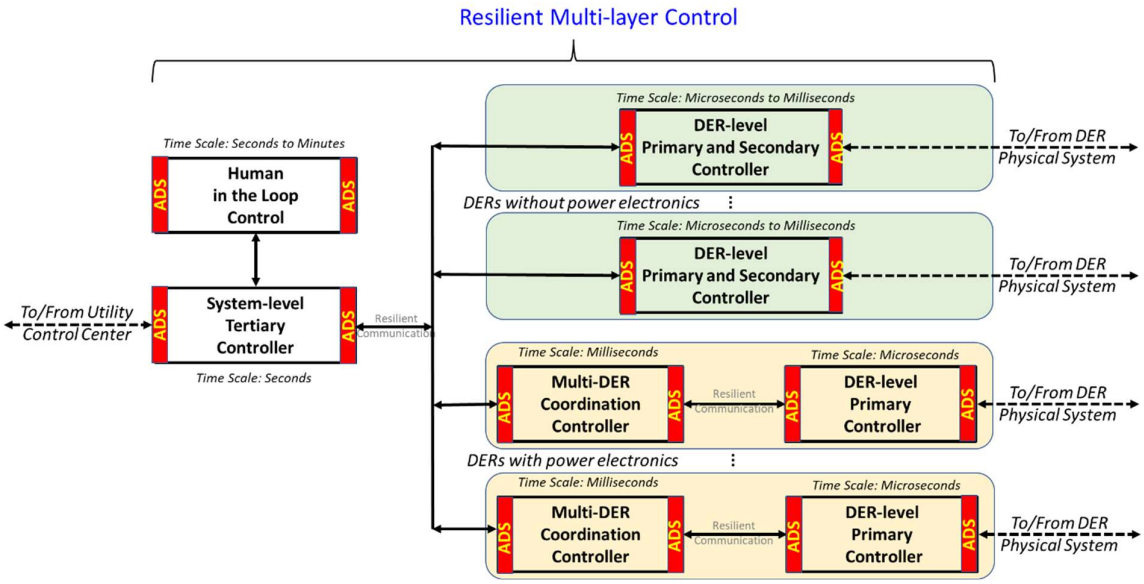
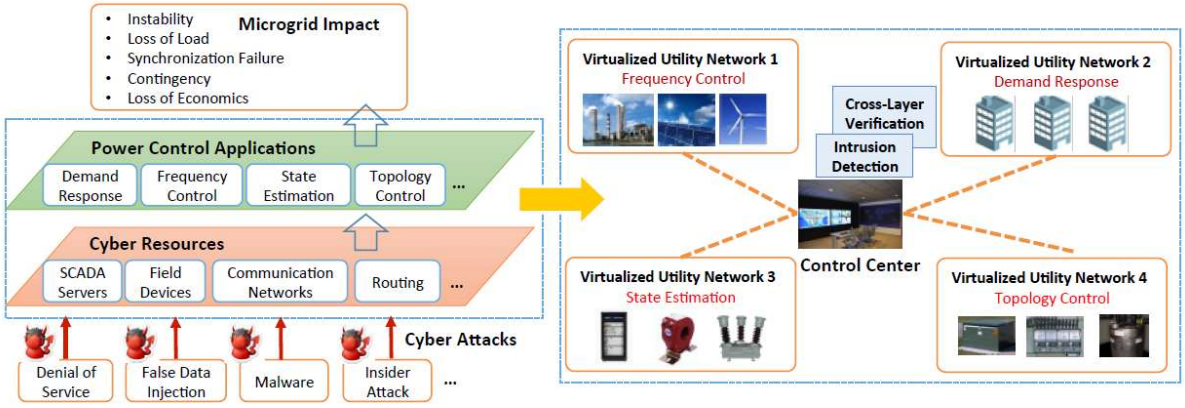


Fig. 15. Multi-scale multi-layer resilient control scheme with ADS for individual microgrids.

There have been several industrial and government-led efforts to create awareness of cybersecurity issues at the microgrid level, but the recommendations and standards have not considered the technical details of the problems that arise when power grids are under attack. In practice, current solutions are dominated by applying the commercial off-the-shelf Internet security techniques, such as firewalls, anti-virus or anti-spyware software, to secure microgrid control systems [87]. However, those security solutions can only provide fine-grained protection for single devices. Various gaps exist, including system-wide visualization, real-time monitoring capability, strictly defined communication paths, and a deny-by-default security model. Fortunately, SDN technologies can technically

minimize those gaps by applying an SDN architecture in the microgrid communication network. The investigation of SDN technologies in the context of microgrids is a new but promising research topic. Recent works include applications in substation automation, reliability evaluation, quality-of-service optimization, and a fast failover mechanism. However, those works are still in the very initial stage and do not particularly focus on security.

In practical engineering, researchers at Illinois Institute of Technology (IIT) plan to transform the current IIT microgrid to the next generation SDN-enabled microgrid [88], as shown in Fig. 16. Fig. 16(a) summarizes many known cyber-attacks and their implications in the context of microgrid. The unique features offered by SDN, such as global visibility and direct programmability of network control, enable us to develop effective and efficient means to detect and mitigate those cyber threats [89]. From the aspects of frequency control, state estimation, demand response, and topology control, as shown in Fig. 16(b), the specific research tasks of the IIT microgrid include building a novel intrusion detection system and an innovative cross-layer verification framework.



(a) (b)

Fig. 16. Transformation to a cyber-attack-resilient microgrid with SDN technology. (a) Current microgrid: potential cyber-attacks and their implication; (b) Future SDN-enabled microgrid: a cyber-attack-resilient platform

(a) Frequency Control. An SDN controller provides state-dependent, deny-by-default paths for inverter setpoints, sampled values, and protection traffic, which yields bounded delay and fast failover that match droop and virtual-inertia timing needs. OpenFlow fast-failover groups and controller-assisted rerouting reduce recovery latency during link or switch faults, supporting stable power sharing in islanded and grid-connected modes. Studies of SDN in power and substation networks document these timing and resilience gains.

(b) State Estimation. For state estimation, an SDN fabric contributes to defense by enforcing authenticated, whitelisted telemetry paths and by exporting in-band telemetry for cross-layer checks. Suspicious flows can be mirrored to intrusion detection system engines and quarantined at the switch, while estimator residual tests provide the physics side of the verification. Recent surveys and methods highlight both the false data injection attack threat and the value of coordinated detection across network and estimator layers.

(c) Demand Response. Shape demand-response traffic with SDN class-based queuing and per-flow rate limits so price and control signals reach aggregations on time, even during congestion. Intent policies restrict each resource to only its authorized coordinator, which reduces lateral movement risk. Feedback from the SDN controller on delay and loss lets the demand-response optimizer down-weight poorly performing channels and adjust dispatch without over-subscribing scarce links.

(d) Topology Control. Topology reconfiguration becomes a programmable function in the SDN plane. Pre-validated paths and fast-failover groups enable sub-second switchover, while policy verification checks that installed rules remain consistent with protection and operating policies before activation. Prototype platforms for resilient microgrids and IEC 61850 testbeds show that SDN control can shorten recovery time and keep critical services online during faults or cyber events.

Further, the MMC that optimizes the economic energy flow with a tri-level control scheme has been developed to manage the IIT microgrid [90]. The CMC serves as an information hub for many grid applications. Hence, it is the ideal location to deploy a SDN controller. Based on a SDN-enabled real-time network verification framework, the customizable consistency generator vets communication networks continuously as the network states (e.g., forwarding tables contained in routers and switches) evolve with millisecond-level latency. A novel network model is also developed in the customizable consistency generator to handle the inevitable uncertainty in message timing during network transitions, which is a critical issue not well addressed in conventional studies. The IIT campus network, which consists of over 240 backbone routers and supports over 70,000 machines, has discovered a variety of errors, including a globally exploitable vulnerability and many internal loops. Such a design will enable global visibility of microgrids and rigorous cross-layer control with rich information from the communication network layer and the power grid application layer.

4.5 Attack-Resilient System-Level NMGs Control Layer

Building on control strategies at the DER level, the multi-DER level, and the microgrid subsystem level, the CMC can coordinate multiple MCs to achieve systematic global control over both information and physical layers. On the information side, the subsystem should be strengthened to limit an attacker's ability to infiltrate and manipulate critical components, and to detect and mitigate attacks effectively. On the physical side, when the information subsystem is interrupted, control functions should still execute correctly to reduce the impact of cyber-attacks on the physical subsystem [91]. To meet these goals, an information-physical collaborative defense-in-depth framework can be established to secure inter-microgrid information and physical interactions and to safeguard resource mutual support. As shown in Fig. 17, the joint defense-in-depth framework comprises three generalized lines of defense that take effect in sequence. The first line detects and identifies potential intrusions into the information network and isolates follow-on attacks. The second line activates after an attacker has entered the information subsystem, augments subsystem operating modes to mislead the adversary, limits the attack's impact, and prevents goal attainment. The third line preserves physical safety and restores network security when system operation is disrupted by an attack. In practice, NMGs can adopt proactive defense ideas together with SDN to coordinate and implement these three generalized lines of defense.

(a) The First Line of Defense. After deploying SDN controllers behind each participant, the information subsystem can be continuously monitored for data flows, with special attention to traffic at potential entry points used by attackers. The system checks for anomalous communications and suspicious connections, delivers global visibility into the real-time performance of NMGs, and supports the monitoring and verification of intrusions. By accounting for the spatiotemporal correlation of traffic within each microgrid, the controller performs time series analysis and content inspection to detect abnormalities and tags suspicious flows for later forensics [92]. In parallel, intrusion detection techniques that follow participant-specific policies are developed locally. Each participant defines a unique and legitimate behavior profile. Compared with traditional detection methods, NMGs can differentiate and target potential cyber-attacks against local assets, which reduces false positives and greatly improves the efficiency of identifying malicious data. Without altering physical communication links, the controller can segment the network virtually. When on-site devices are compromised, the CMC or the MMC can promptly detect malicious behavior. The corresponding controller can temporarily limit local network traffic to shrink the attack surface and avoid wasting defensive resources, which enables more effective tracking and response.

(b) The Second Line of Defense. SDN enables proactive augmentation of operating modes for the information subsystem through powerful network reconfiguration and traffic control. Through southbound interfaces, the controller can frequently modify device addresses and routing rules on site while keeping the integrity of local configurations intact [93]. The SDN controller can also dynamically manage connections between DERs and the CMC or the MMC. When attackers manipulate DERs, local controllers are not always reachable, and adversaries

who tamper with idle physical devices may expose their behavior unintentionally. A defensive deception strategy can be adopted to counter targeted cyber-attacks by actively misleading adversaries. Key control information related to the operation of each microgrid is obfuscated, for example, device start and stop commands and inter-participant interconnection commands, which distorts the attacker's understanding of the system and makes vulnerabilities harder to discover. Mature honeypot-style active defense from computing can be adapted by disguising network traffic, for example, fabricating non-existent measurements, and by deliberately exposing exploitable weaknesses as bait. Once an attacker interacts with the bait, the affected participant is notified immediately to respond and analyze the malicious activity.

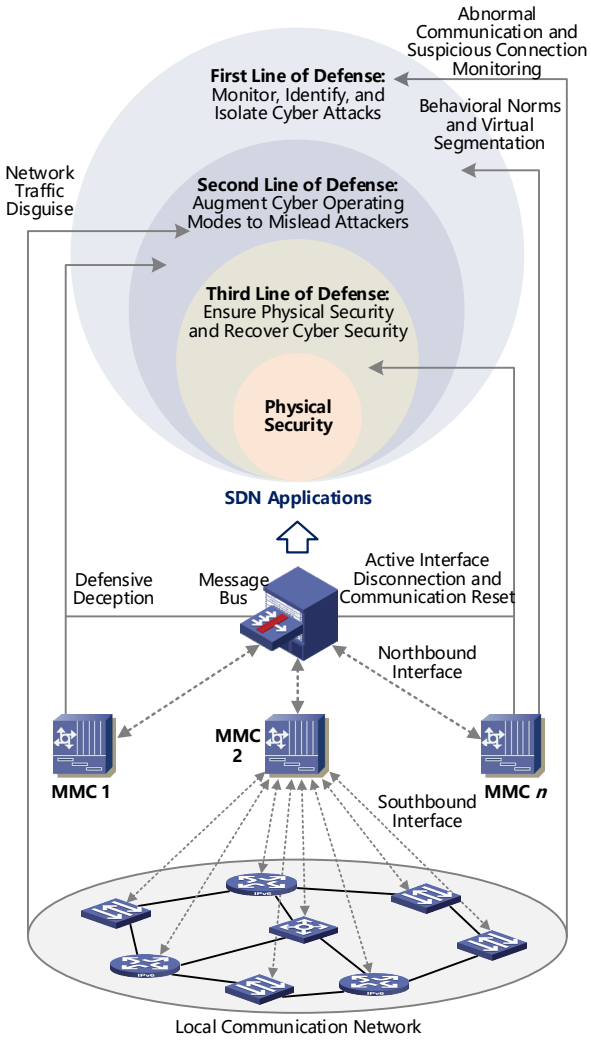


Fig. 17. Attack-resilient system-level NMGs control layer with three lines of defense in depth.

(c) At the Third Line of Defense. The inherent layered and distributed architecture of the CMC and the MC allows controllers to reconfigure the communication network dynamically while adjusting NMG operating modes to keep the physical subsystem safe. The layered and distributed design combines the advantages of centralized and decentralized control. If the CMC is degraded or interrupted by a cyber-attack, each microgrid retains autonomous operation independent of the CMC and can proactively sever its northbound interface to the message bus, then regulate local resources in a decentralized manner. After identifying compromised sources and interrupted components, each participant can use southbound interfaces locally to reset the network, such as reconnecting switches and rerouting routers, which contains the spread of the incident. A two-stage mathematical optimization that

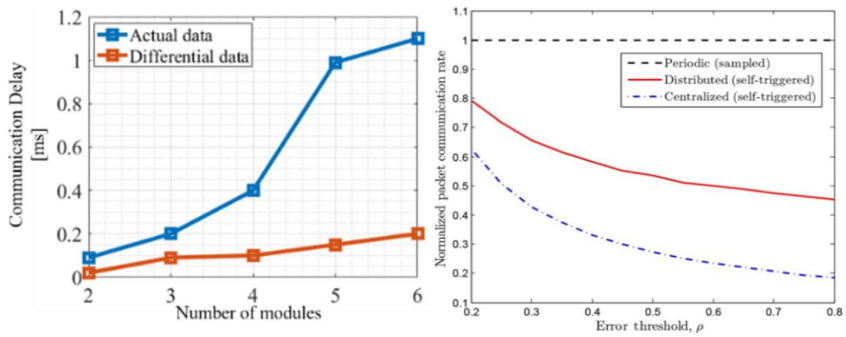
integrates preventive and corrective actions can be used. Before an incident, traffic uncertainty is considered, and offline robust or stochastic optimization determines the best anticipated failover plan. After an incident, the controller rapidly matches the predefined plan, reconfigures the network automatically, and adjusts the configuration dynamically according to real-time traffic monitoring.

5. ILLUSTRATIVE CASE STUDY

Simulation is implemented in MATLAB R2024a environment on a personal computer with an AMD Ryzen 7 8845H CPU and 32 GB RAM. We first test the sense and defense performance of individual microgrids under cyber-attacks and then test the performance of a real-world case of ICM-BCM NMGs.

5.1 Individual Microgrid Test

We first test the communication performance for an individual microgrid in Fig. 18. The information exchange between the primary (DER) control layer and the aggregate (multi-DER) control layer of the microgrid is enabled to achieve a higher level of resilience via the synthesis of an event-driven resilient control scheme. By conveying information with a reduced number of bits, the ability to support communication among a large number of DERs increases, thereby enhancing scalability, as illustrated in Fig. 18(a). By reducing the communication rate, the vulnerability of the network can be significantly enhanced, as illustrated in Fig. 18(b). Thus, by using a combination of event-driven and differential-coding mechanisms, a microgrid can reduce the number of bits in local communication that need to be transmitted and the frequency of their transmission.



(a) (b)

Fig. 18. Communication performance test for an individual microgrid. (a) Latency reduction using the differential-coding method to reduce the number of bits needed to communicate; (b) Packet rate comparison of event-based self-triggered communication regarding periodic communication.

Then, as shown in Fig. 19, we test the hierarchical protection scheme based on localized differential protection. During the cyber-attack, Fig. 19(b) is a preliminary analysis for real-time safe operation region identification, and Fig. 19(c) illustrates all critical operational curves for the microgrid, including voltage, current, and active power. The normal/safe operation region of DER clusters in Fig. 19(b) will be used for sanity authentication of the commands executed by the main aggregate controller module for mitigating the cyber-attack impact and ensuring stable and synchronized operation of DERs before a catastrophic event. Based on local control, multi-DER coordinator control, and the functional decision-making module at the microgrid level, when an anomaly is detected, as shown in Fig. 19(c), the oscillations in voltage, current, and active power can be recovered, but the recovery process is lengthy. Under more severe attack scenarios, it is reasonable to infer that recovery time may be even longer, or the microgrid may fail to recover under multiple attacks. Hence, it is essential to implement systematic control at the NMG level to better resist cyber-attacks.

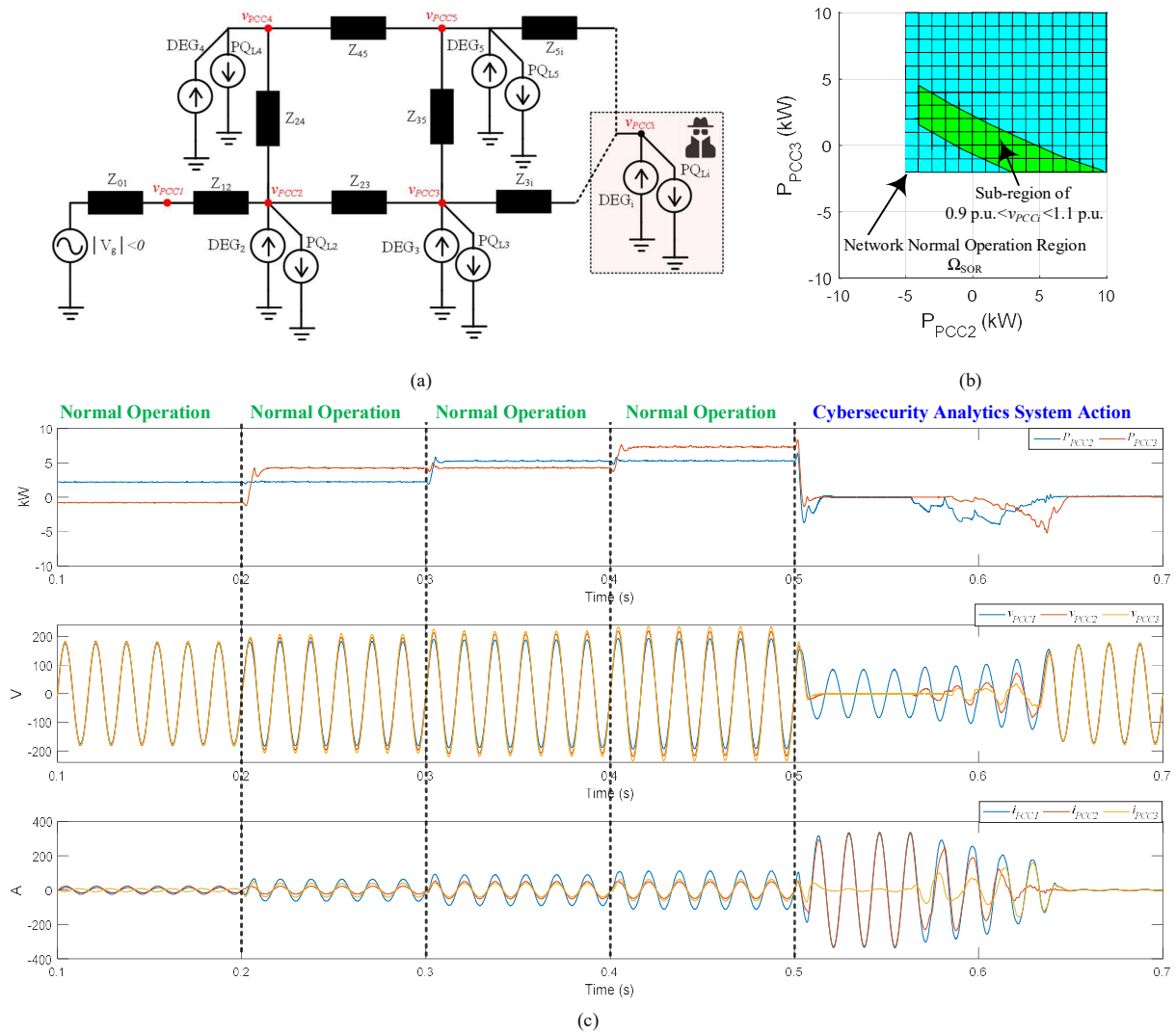


Fig. 19. Test on a microgrid under a cyber-attack. (a) Illustration of a microgrid under attack; (b) Preliminary analysis for real-time safe operation region identification; (c) Operational performance of voltage, current, and active power in a microgrid.

5.2 Networked Microgrid Test

5.2.1 Experimental Setup

The 39-bus IIT campus microgrid and Bronzeville community microgrid (ICM-BCM) NMGs, comprising pseudo measurements, SCADA modules, and phasor measurement units (PMUs), is employed as the testbed for the proposed approaches, as shown in Fig. 20. The 37 pseudo measurements measure the active/reactive power injections at all buses, except for the reference buses #1 and #39. The two SCADA modules deployed at the reference buses, #1 and #39, measure the real and imaginary parts of the bus voltages. The other 11 SCADA modules distributed over the system measure the active/reactive power flows on different branches. The 2 PMUs are only deployed at the reference buses #1 and #39, which measure the real and imaginary parts of bus voltages. Note that the real-time measurements include all SCADA modules and PMUs.

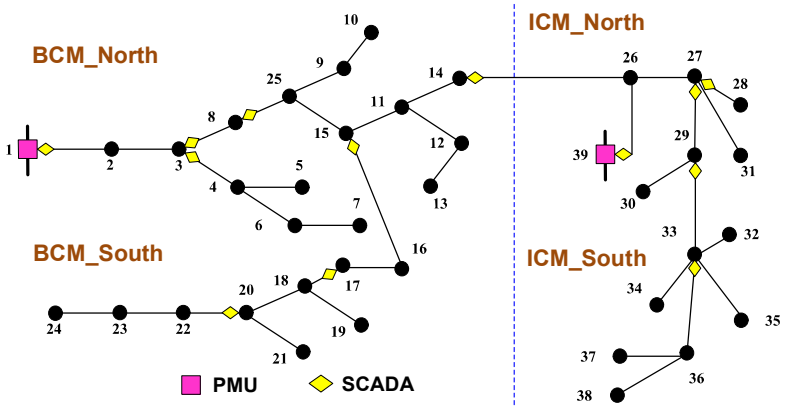


Fig. 20. The 39-bus ICM-BCM NMGs.

Referring to the U.S. National Vulnerability Database, specific information on the exploitable loopholes is tabulated in Table V, where each loophole is unique and denoted by a common vulnerability and exposure (CVE)-ID. The assigned values of the common vulnerability scoring system (CVSS) scores are presented in Table V. With the CVSS scores, each loophole's exploitability is summarized in the third column in Table VI. The attack graphs for compromising the pseudo and real-time measurements are shown in Fig. 21. Router's loopholes are L_1 and L_2. Substation's loopholes are L_3 and L_4. Access the network's loopholes is L_5 and L_6. Scale and shape parameters of the Pareto distribution are set as: k_1 = 0.00161 and k_2 = 0.26. To derive the measurement vulnerability value, the defender resource fraction DF is set to 0.1 for all measurements, and the costs DC are set as 100, 200, and 300 for the 37 pseudo measurements, 13 SCADA modules, and 2 PMUs, respectively, to address their varying security levels.

TABLE V
EXPLOITABLE SECURITY LOOPHOLES AT ATTACK PORTALS

No.	CVE-ID	CVSS Scores	Exploitability
L_1	CVE-2016-5053	C^{AV}: N/C^{AC}: L/C^{AU}: N	0.5403
L_2	CVE-2020-10923	C^{AV}: A/C^{AC}: L/C^{AU}: N	0.3848
L_3	CVE-2015-7599	C^{AV}: N/C^{AC}: H/C^{AU}: N	0.3088
L_4	CVE-2018-5678	C^{AV}: N/C^{AC}: L/C^{AU}: N	0.5387
L_5	CVE-2018-19524	C^{AV}: N/C^{AC}: L/C^{AU}: N	0.5368
L_6	CVE-2020-8958	C^{AV}: N/C^{AC}: L/C^{AU}: N	0.5282
L_7	CVE-2018-0453	C^{AV}: L/C^{AC}: L/C^{AU}: S	0.2498
L_8	CVE-2015-4684	C^{AV}: N/C^{AC}: L/C^{AU}: S	0.3873

TABLE VI
ASSIGNED VALUES OF CVSS SCORES

Metric	Level	Value
Access Vector C^{AV}	Local (C^{AV}: L)	0.55
	Adjacent Network (C^{AV}: A)	0.62
	Network (C^{AV}: N)	0.85
Access Complexity C^{AC}	High (C^{AC}: H)	0.44
	Medium (C^{AC}: M)	0.58
	Low (C^{AC}: L)	0.77
Authentication C^{AU}	Multiple (C^{AU}: M)	0.27
	Single (C^{AU}: S)	0.61
	None (C^{AU}: N)	0.85

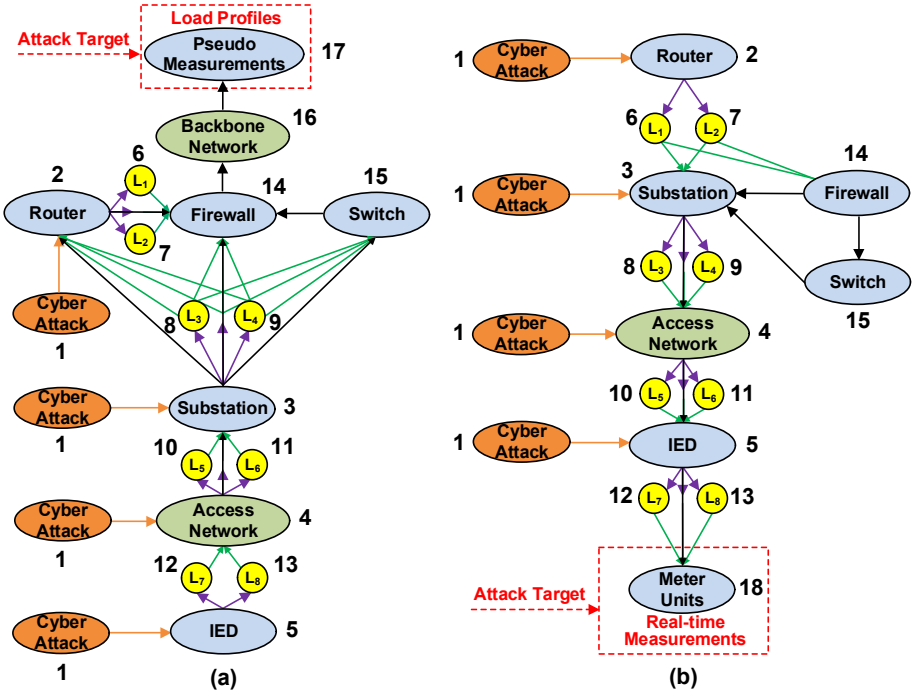


Fig. 21. Two attack graphs. (a) Pseudo measurement attack; (b) Real-time measurement attack.

5.2.2 Security Risk Assessment

The 39-bus ICM-BCM NMGs are assumed to be exposed to external cyber-attacks in this subsection, where the defensive budget value τ^D is initialized to 0 (i.e., without deploying any defense resources). For each measurement, success probabilities of single-target cyber-attacks are calculated and displayed in Fig. 22. As seen, attacks against pseudo measurements generally yield a higher success rate (ranging from 0.15 to 0.2), while the ones for SCADA units and PMUs are at relatively low levels (about 0.08 to 0.1).

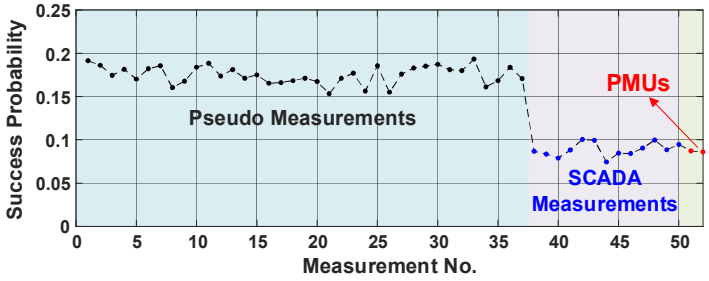


Fig. 22. Success probabilities of single-target attacks for each measurement.

For a single-target attack, each attack path's success probability is shown in Fig. 22. In Fig. 22(a), with more exploitable attack paths, pseudo measurements are more susceptible to cyber intrusions, in contrast with SCADA units and PMUs in Fig. 23(b) and 23(c). This is because the attack paths of pseudo measurements (20 paths) are more than those (12 paths) against SCADA units or PMUs. Since the success probabilities are calculated by accumulating the success rates of multiple paths, pseudo measurement attacks are therefore more likely to succeed than real-time measurement attacks in ICM-BCM.

Coordinated cyber-attacks can be categorized according to the number of targets. That is the attack indexed by $N_{\mathcal{M}}$ indicates to randomly choose $N_{\mathcal{M}}$ targets out of all the vulnerable state variables. This study considers coordinated cyber-attacks indexed from 1 to 10 ($N_{\mathcal{M}}$ = 1, 2, …, 10), where each index is randomly launched 10 times against

pseudo, SCADA modules, or PMUs. The risk value ($R_{N_{\mathcal{M}}}^{CO}$) and success probability ($P_{N_{\mathcal{M}}}^{CO}$) are both cumulatively calculated for each $N_{\mathcal{M}}$. Utilizing the proposed approach, the risk assessment results under coordinated cyber-attacks are summarized in Table VII.

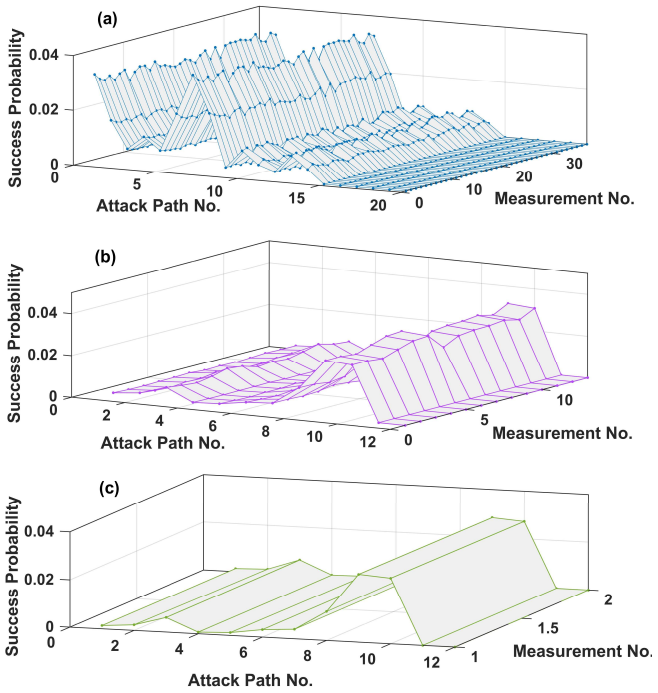


Fig. 23. Success probabilities of different attack paths of single-target attacks for each measurement. (a) Pseudo measurements; (b) SCADA modules; (c) PMUs.

TABLE VII
SECURITY RISK ASSESSMENT RESULTS UNDER COORDINATED CYBER-ATTACKS

$N_{\mathcal{M}}$	$P_{N_{\mathcal{M}}}^{CO}$	$R_{N_{\mathcal{M}}}^{CO}$	$N_{\mathcal{M}}$	$P_{N_{\mathcal{M}}}^{CO}$	$R_{N_{\mathcal{M}}}^{CO}$
1	0.1397	0.5838	6	4.5891×10^{-6}	6.4566×10^{-5}
2	0.0375	0.1690	7	1.1358×10^{-12}	3.3212×10^{-11}
3	5.7023×10^{-5}	6.9832×10^{-4}	8	5.8418×10^{-10}	1.4020×10^{-8}
4	7.2295×10^{-9}	1.4629×10^{-7}	9	3.4565×10^{-14}	1.1759×10^{-12}
5	1.9030×10^{-8}	3.8655×10^{-7}	10	2.4228×10^{-18}	9.7000×10^{-17}

It can be seen that attacks with a smaller index $N_{\mathcal{M}}$ tend to yield a higher success possibility $P_{N_{\mathcal{M}}}^{CO}$. The reason is that when $N_{\mathcal{M}}$ is greater than 1, calculating the success probability of a coordinated attack involves a cumulative multiplication, i.e., the success probability is inversely proportional to the number of attack targets $N_{\mathcal{M}}$. Overall, it can be concluded that the overall system risk. R^{Sys} is mostly dominated by the first two indices ($N_{\mathcal{M}}$ = 1 and 2), because $\sum_{i=1}^{2} R_i^{CO}/R^{Sys}$ = 0.7528/0.7536 = 99.89%.

5.2.3 Risk-Oriented Defense Resource Allocation

In this subsection, we present two effective methods for allocating the defense resources. The proposed risk assessment approach has been applied beforehand, and two allocation methods are integrated into ICM-BCM NMGs, which is tested under varying coordinated cyber-attacks ($N_{\mathcal{M}}$ = 1, 2, …, 10).

Method I: For a coordinated attack indexed by $N_{\mathcal{M}}$, the overall defense resource budget τ^D is distributed according to each cyber-attack's risk ratio to the overall risk R^{Sys}, i.e., $R_{N_{\mathcal{M}}}^{CO}/R^{Sys}$.

Method II: The overall defense resource τ^D is first divided into multiple units (τ^D/x^D) by the allocation precision x^D. At each iteration, a single unit τ^D/x^D is assigned for the measurement that results in the highest risk reduction

value.

The defense resource budget τ^D and allocation precision x^D are both initialized to 5000. Comparative defense resource allocation results for each measurement are presented in Fig. 24. It can be observed from Fig. 24(a) that both **Methods I and II** distribute a considerable amount of resources to specific pseudo measurements. Comparing Fig. 24(b) with 24(a), it is seen that **Method I** distributes some resources to #4th, #8th, #13th SCADA and the #2nd PMU, while **Method II** assigns all its budget τ^D for pseudo measurements in Fig. 24(a). The reason for this discrepancy is that numerous pseudo measurements are generally more vulnerable to external cyber-attacks than SCADA units/PMUs. This observation is also consistent with the results derived in Section 5.2.2.

In summary, the core idea of **Method I** is to allocate resources in proportion to risk values. The core idea of **Method II** is focusing on the single measurement that triggers the highest risk reduction value in each iteration. In practice, **Methods I and II** can be combined to protect as many measurements as possible. For example, when τ^D = 5000, we can assign a half to **Method I**, while **Method II** distributes the other half.

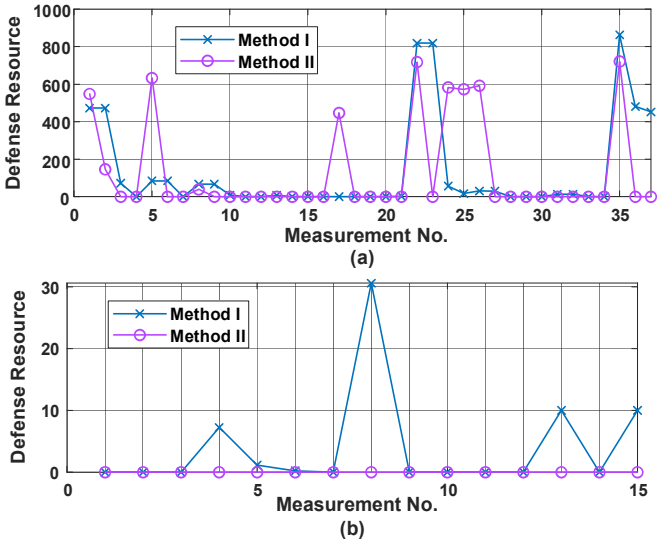


Fig. 24. Defense resource allocation results. (a) Pseudo measurements; (b) SCADA and PMUs.

By applying the two allocation methods above, the risk incurred by each coordinated cyber-attack and the overall system risk are both cumulatively calculated. As shown in Table VIII, the overall system risk R^{Sys} is still dominated by attacks with $N_{\mathcal{M}}$ = 1 and 2, which is consistent with the results in Table VII.

According to the 3rd and 4th columns, it is validated that both **Methods I** and **II** can effectively reduce the overall security risk R^{Sys} when $N_{\mathcal{M}}$ ranges from 1 to 10.

Method I is dependent on the risk ratio of $R^{CO}_{N_{\mathcal{M}}}$ to R^{Sys}. Although **Method I**'s overall risk reduction is lower than **Method II**, its advantage is to allocate τ^D for as many measurements as possible.

Method II deploys each single unit τ^D/x^D according to the fastest descent direction of R^{Sys}, thereby the measurement corresponding to the highest risk reduction value is prioritized at each iteration. As shown in the bottom row, **Method II** outperforms **Method I** in terms of reducing R^{Sys}.

TABLE VIII
SECURITY RISK VALUES USING DIFFERENT ALLOCATION METHODS

$N_{\mathcal{M}}$	No Defense	Method I	Method II
1	0.5838	0.0074	1.0397×10^{-7}
2	0.1690	1.5526×10^{-4}	1.8889×10^{-8}
3	6.9832×10^{-4}	1.9499×10^{-4}	9.4631×10^{-9}
4	1.4629×10^{-7}	2.6300×10^{-9}	6.7626×10^{-19}
5	3.8655×10^{-7}	8.4439×10^{-18}	1.0846×10^{-24}
6	6.4566×10^{-5}	9.3699×10^{-14}	2.5145×10^{-14}

7	3.3212×10^{-11}	1.4543×10^{-21}	3.5287×10^{-24}
8	1.4020×10^{-8}	1.5578×10^{-28}	5.8028×10^{-29}
9	1.1759×10^{-12}	4.0434×10^{-35}	6.8965×10^{-37}
10	9.7000×10^{-17}	9.9108×10^{-29}	2.7164×10^{-40}
R^{Sys}	**0.7536**	**0.0077**	**1.3232×10^{-7}**

6. OUTLOOK

6.1 Incorporation of Cyber-Physical Contingencies in Risk Assessment

Cybersecurity risk assessment and contingency analysis in NMGs have conventionally been treated as separate tasks, with cybersecurity engineers focusing on defenses like firewalls and antivirus software, and system operators handling physical faults and operational errors. However, this siloed approach misses critical interdependencies. Even seemingly minor firmware vulnerabilities could escalate into severe instabilities if the compromised component is instrumental in maintaining generation-demand balance. Recognizing this gap, as shown in Fig. 25, we could advocate an integrated risk assessment framework that merges cyber and physical contingency analyses. By considering dynamic parameters, such as changing operational conditions or renewable forecasts, and conducting simulation-based evaluations, this approach can more accurately capture how complex cyber threats propagate into physical disruptions, guiding stakeholders to identify and protect mission-critical assets [94].

A key feature of the proposed framework is its reliance on both physical principles (e.g., grid models and system behavior) and data-driven analysis (e.g., statistical patterns in network flows). This dual perspective highlights synthetic vulnerabilities where IT and OT dependencies intersect across people, processes, and devices. The framework in Fig. 25 identifies cyber, operational, and physical weaknesses, then surfaces synthetic vulnerabilities that span both IT and OT, hence the analyst sees how faults can propagate across layers rather than in isolation. Guidance from industrial control system practice supports this integrated view and motivates security requirements that respect real-time and safety constraints in operational technology. The analysis engine then performs contingency studies with simulation-based approaches to estimate the impact of the identified weaknesses and to rank assets and systems by their contribution to overall security posture. Through co-simulation, the workflow couples discrete-event network behavior with continuous-time power dynamics so that a cyber event at the information layer can be traced to operational effects in DERs and to follow-on physical outcomes in voltage, frequency, and protection. Open-source and commercial tools provide practical substrates for related studies (e.g., HELICS for cross-domain co-simulation [95], OpenDSS for microgrid behavior [96], and Simulink for microgrid control modeling [97]).

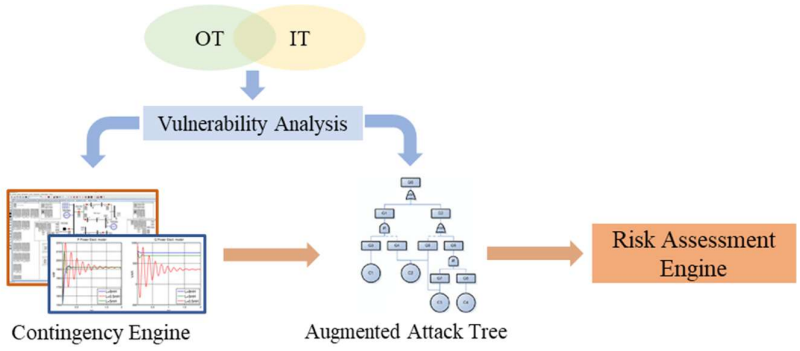


Fig. 25. Augmented cybersecurity risk assessment considering IT and OT.

The assessment workflow augments studies with an attack-tree model so researchers can reason about entry points, escalation paths, negative impacts, and mitigation choices in a structured way. Factors, devices, applications, and networks are categorized into nodes that describe where and how assaults can occur, while outcomes are quantified through the linked simulations to estimate ripple effects such as load imbalance, power quality degradation, and mis-

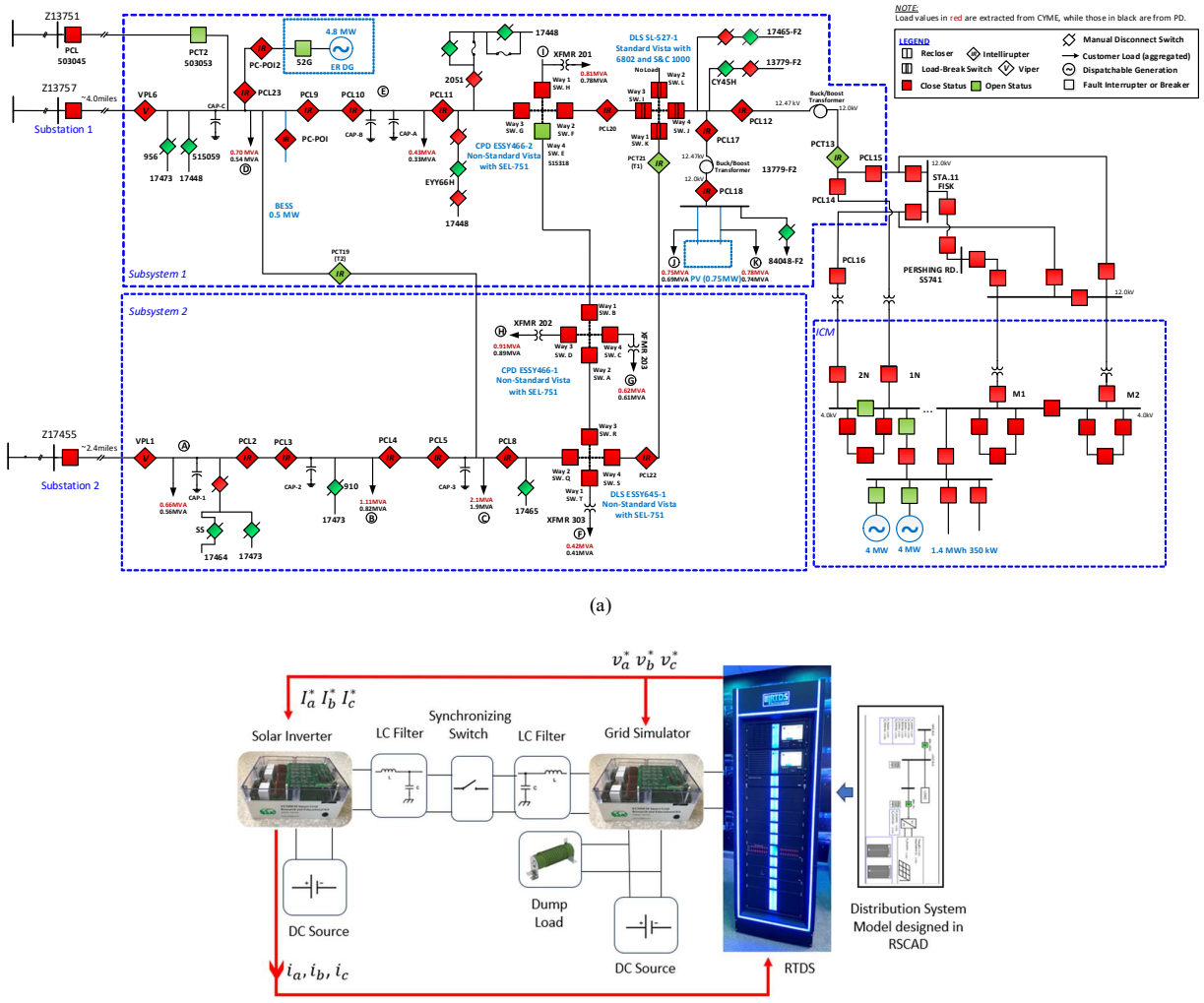
operation of protection. To ensure traceability from technique to consequence, the augmented attack-tree view can be aligned with widely used industrial control system taxonomies so that each hypothesized step maps to an adversary behavior category and each defense maps to a specific control objective. This holistic process offers a direct path to hardening the operations of NMGs because both IT and OT vulnerabilities are addressed proactively with evidence from integrated cyber-physical tests.

6.2 Real-Time HIL Co-simulation Testbed Development for Cyber-Physical Impact Analysis

The increasing cyber-physical nature of the NMGs requires rethinking how their behavior should be addressed in planning and operation studies. As in any cyber-physical system, the power network and its components, and the IT infrastructure are two parts of a larger and heterogeneous system. Co-simulation has emerged as an effective way to analyze the increasingly intertwined cyber and physical aspects of modern power systems. By coupling discrete-event communication models (e.g., sending and receiving network packets) with the continuous-time dynamics of NMGs, co-simulation enables a more comprehensive view of how events in one domain affect the other. The corresponding mathematical model is often represented by differential-algebraic equations. When enhanced with real-time emulation and hardware-in-the-loop (HIL) capabilities, co-simulation platforms can include actual physical devices (e.g., inverter hardware) interacting with virtual models, providing an environment that closely mirrors real-world operations. The HIL capabilities are vital for identifying underlying interactions and evaluating how control strategies or security features perform under realistic operating conditions, without risking actual infrastructure.

However, building an HIL-based co-simulation testbed for NMG introduces practical challenges, including higher development costs and time to integrate physical components with sophisticated software models. On the other hand, these platforms offer distinct advantages, which allow for rapid testing of multiple scenarios and more accurate assessments of new technologies. For instance, at the IIT, a fully functional model of the ICM-BCM NMGs already exists in a real-time digital simulator (RTDS) (see Fig. 26) [98]. If we pair the existing model with a dedicated communication network simulator like ns3 [99] or Mininet [100], along with the ability to emulate critical DER components in hardware using reconfigurable and reprogrammable SynDEM kits, to create a highly granular, real-time cyber-physical co-simulation testbed. This setup will serve as a benchmark for testing and refining detection and mitigation strategies against various cyber threats, bridging the gap between purely virtual simulations and costly field tests on the actual NMGs.

In particular, as shown in Fig. 26, to turn the platform into a repeatable benchmark for cyber-physical impact studies, the RTDS model of the ICM-BCM cluster should be time-synchronized with a packet-level network domain via a co-simulation bus, then exercised through staged red-team scenarios that range from latency/jitter stress to crafted false-data injections and controller impersonation. A practical path is to couple the RTDS side to a communications sandbox built in ns-3 or Mininet and exchange measurements and setpoints through a co-simulation framework so that discrete-event traffic affects continuous-time dynamics and vice versa. This architecture already appears in recent co-simulation efforts and gives fine control over topology, protocols, and delays, while preserving real-time fidelity on the power side for power-hardware-in-the-loop experiments with inverter controllers. With that plumbing in place, a standardized playbook can log synchronized traces and score key performance indicators, including frequency nadir, voltage recovery time, protection mis-operation rate, and mean time to safe reconfiguration under Byzantine behaviors. Further, the testbed then supports a phased workflow: 1) validate the baseline RTDS cluster model and its interfaces; 2) introduce communication faults and cyber-attacks in the ns-3/Mininet layer; 3) close the loop with power-hardware-in-the-loop inverter or protection relays for the most critical cases; 4) harden the guard-control and consensus settings using the same scenarios to demonstrate measurable resilience gains.



(a)

(b)

Fig. 26. (a) ICM-BCM model in PSCAD (b) HIL setup of a solar inverter interfaced with the distribution system at IIT.

6.3 Incorporation of Human Characteristics in Cybersecurity Analysis

On the personnel level, the individual differences (e.g., personality traits, interests, and attitudes) of system operators that contribute to efficient cyber-attack detection and response will be analyzed, and personnel selection and training plans will be developed to promote the cyber agility and accuracy of humans in the loop. A recent survey of network operators shows that 89% of operators are never sure that their configuration changes are bug-free, and 82% are concerned that changes would cause problems with existing functionality [101]. While previous studies have examined end-user behaviors in conventional IT environments, this task shifts focus to the more complex context of NMGs. Operators must manage fast-moving events, and potentially severe consequences should a cyber-attack occur. By integrating insights from organizational psychology, human factors, and cybersecurity, we plan to explore how various individual personality traits and situational factors affect operators' competencies in identifying suspicious activities, responding promptly to threats, and adhering to security guidelines during cyber threats.

However, in the pursuit of building secure and resilient NMGs, little is known about the security impacts and risks from human behaviors. We believe that an effective solution requires joint efforts from both engineering and human science aspects. On the one hand, we need an efficient engineering approach to secure cyber resources (e.g., communication networks), which are often transparent to most grid applications by design. The solutions must

address the unique challenges of NMGs (e.g., no interference to real-time operations) and leverage the opportunities (e.g., relatively fixed infrastructure). On the other hand, individuals working within a cyber system (i.e., human-in-the-loop) play important roles beyond autonomous operations and remain a critical and possibly the weakest link in securing cyberspace [102].

Besides, we could create simulated operational scenarios, both normal and malicious, for the operators of NMGs, accompanied by behavioral guidelines informed by cybersecurity best practices and organizational science. Through surveys and controlled experiments, researchers will examine the effects of 1) personality traits (using Big Five personality factors and narrow facets within the Big Five), 2) vocational interests (using RIASEC interest types as well as more specific, basic interest scales) [103], 3) attitudes (technology acceptance) [104], and 4) cognitive and emotional states [105] on operators' competencies to accurately detect malicious cyber-attacks, immediacy to react to cyber security threats, and compliance with security behavioral guidelines during the process of handling cyber-attacks. Further research will then guide efforts in recruitment (selecting operators with desirable personality and interest profiles), training (enhancing operators' technology acceptance and cybersecurity awareness), and job design (minimizing the negative impacts of stress and cognitive load). Ultimately, this comprehensive approach aims to fortify the human-in-the-loop against evolving cyber threats in critical power infrastructure. The goal is not only to understand which attributes promote better security performance but also to develop training and selection strategies that strengthen operator resilience against attacks.

7. Conclusion

NMGs offer substantial potential for sustaining local power service continuity under emergency operating conditions, yet they remain highly vulnerable to cyber incidents during practical operations. Consequently, identifying cyber vulnerabilities in NMG operations, deploying targeted measures to mitigate cyber threats, enhancing the system's capacity to maintain power supply amid cyber-attacks, and safeguarding local customers against cyber-induced power outages have emerged as critical priorities in both academic research and engineering practice. In this context, a systematic cybersecure operational framework for NMGs is of paramount significance to achieving a highly resilient power supply.

Future research can be expanded in several directions. Efforts may focus on advancing the application of cyber-physical co-simulation technologies in NMG vulnerability assessment, integrating digital twin technology to enable real-time dynamic risk early warning. Exploration of the integration pathways between emerging technologies such as blockchain and quantum key distribution with layered defense architectures is also warranted to enhance the attack resistance and flexibility of defense mechanisms. Additionally, the development of cybersecurity-oriented collaborative optimization models that account for the interests of multiple stakeholders, along with the improvement of cross-microgrid resource scheduling mechanisms under emergency conditions, will provide more comprehensive theoretical support and engineering solutions for the safe and stable operation of NMGs.

References

[1] Z. Li, X. Han, M. Farhoumandi, and M. Shahidehpour, "Microgrid Clustering for Enhancing the Grid Resilience in Extreme Conditions, In Power Grid Resilience: Theory and Applications," Springer, 193-260, 2025.

[2] X. Han, Z. Li, J. Ge, Y. Yan and X. Xiao, "Coordinated Planning of Transmission Network Expansion and Distribution Network Modernization With Microgrids Under Non-Uniform Discrete Choices," IEEE Transactions on Smart Grid, vol. 16, no. 2, pp. 1405-1421, 2025.

[3] X. Han, Z. Li, et al., "Privacy-Preserving Operational Decision-Making for Networked Autonomous Microgrids Based on Bilevel Mixed-Integer Optimization," IEEE Transactions on Smart Grid, vol. 15, no. 3, pp. 2881-2897, 2023.

[4] X. Ma, H. Zhou, and Z. Li, “On the resilience of modern power systems: A complex network perspective,” Renewable Sustainable Energy Reviews, vol. 152, pp. 111646, 2021.

[5] C. Nan and G. Sansavini, “A quantitative method for assessing resilience of interdependent infrastructures,” Reliability Engineering & System Safety, vol. 157, pp. 35-53, 2017.

[6] B. Chen, J. Wang, X. Lu, C. Chen, and S. Zhao, “Networked microgrids for grid resilience, robustness, and efficiency: A review,” IEEE Transactions on Smart Grid, vol. 12, no. 1, pp. 18-32, 2020.

[7] Z. Li, M. Shahidehpour, F. Aminifar, A. Alabdulwahab, and Y. Al-Turki, “Networked microgrids for enhancing the power system resilience,” Proceedings of the IEEE, vol. 105, no. 7, pp. 1289-1310, 2017.

[8] Q. Zhou, M. Shahidehpour, A. Paaso, S. Bahramirad, A. Alabdulwahab, and A. Abusorrah, “Distributed control and communication strategies in networked microgrids,” IEEE Communications Surveys & Tutorials, vol. 22, no. 4, pp. 2586-2633, 2020.

[9] M. Setiawan, F. Shahnia, S. Rajakaruna, and A. Ghosh, “ZigBee-based communication system for data transfer within future microgrids,” IEEE Transactions on Smart Grid, vol. 6, no. 5, pp. 2343-2355, 2015.

[10] A. Khodaei, “Provisional microgrids,” IEEE Transactions on Smart Grid, vol. 6, no. 3, pp. 1107-1115, 2014.

[11] A. Khodaei, “Provisional microgrid planning,” IEEE Transactions on Smart Grid, vol. 8, no. 3, pp. 1096-1104, 2015.

[12] X. Niu, Y. Tong, and J. Sun, “Vulnerability assessment for PMU communication networks,” International Conference on Smart Computing and Communication, Springer, pp. 29-38, 2018.

[13] X. Han, Z. Li, et al., “Privacy-Preserving Outsourced Computation of Collaborative Operational Decisions among Microgrids in an Active Distribution Network,” IEEE Transactions on Power Systems, vol. 40, no. 1, pp. 850-865, 2024.

[14] Z. Li, M. Shahidehpour and F. Aminifar, “Cybersecurity in Distributed Power Systems,” Proceedings of the IEEE, vol. 105, no. 7, pp. 1367-1388, 2017.

[15] Y. Wang, S. Mondal, C. Deng, K. Satpathi, Y. Xu and S. Dasgupta, “Cyber-resilient cooperative control of bidirectional interlinking converters in networked AC/DC microgrids,” IEEE Transactions on Industrial Electronics, vol. 68, no. 10, pp. 9707-9718, 2021

[16] Q. Zhou, M. Shahidehpour, A. Alabdulwahab and A. Abusorrah, “Flexible division and unification control strategies for resilience enhancement in networked microgrids,” IEEE Transactions on Power Systems, vol. 35, no. 1, pp. 474-486, 2020.

[17] S. Sahoo and J. C. -H. Peng, “A localized event-driven resilient mechanism for cooperative microgrid against data integrity attacks,” IEEE Transactions on Cybernetics, vol. 51, no. 7, pp. 3687-3698, 2021.

[18] X. Han, Z. Li, et al., “Privacy-Preserving Collaborative assessment of multi-day operation security in distribution systems with high levels of PV penetration,” IEEE Transactions on Sustainable Energy, early access.

[19] L. Wang, P. Zhang, Z. Tang and Y. Qin, “Programmable crypto-control for IoT networks: An application in networked microgrids,” IEEE Internet of Things Journal, vol. 10, no. 9, pp. 7601-7612, 2023.

[20] X. Cai, B. Gao, X. Nan and J. Yuan, “Resilient discrete-time quantization communication for distributed secondary control of AC microgrids under DoS attacks,” IEEE Systems Journal, vol. 18, no. 3, pp. 1798-1808, 2024.

[21] E. Naderi and A. Asrari, “Experimental Validation of a Remedial Action via Hardware-in-the-Loop System Against Cyberattacks Targeting a Lab-Scale PV/Wind Microgrid,” IEEE Transactions on Smart Grid, vol. 14, no. 5, pp. 4060-4072, 2023.

[22] X. Han and Z. Li, “Resilience-oriented collaborative operational decision-making for active distribution networks by privacy-preserving outsourced computation,” IEEE SmartGridComm, 2023.

[23]B. Zhou, J. Zou, C. Chung, H. Wang, N. Liu, N. Voropai, and D. Xu, "Multi-microgrid energy management systems: Architecture, communication, and scheduling strategies," Journal of Modern Power Systems and Clean Energy, vol. 9, no. 3, pp. 463-476, 2021.

[24]M. Husák, J. Komárková, E. Bou-Harb, and P. Čeleda, "Survey of attack projection, prediction, and forecasting in cyber security," IEEE Commun. Surv. Tut., vol. 21, no. 1, pp. 640-660, 2018.

[25]Z. Li and M. Shahidehpour, "Privacy-preserving collaborative operation of networked microgrids with the local utility grid based on enhanced benders decomposition," IEEE Transactions on Smart Grid, vol. 11, no. 3, pp. 2638-2651, 2019.

[26]C. Feng, Z. Li, M. Shahidehpour, F. Wen, W. Liu and X. Wang, "Decentralized short-term voltage control in active power distribution systems," IEEE Transactions on Smart Grid, vol. 9, no. 5, pp. 4566-4576, 2018.

[27]H. Huang et al., "Toward resilient modern power systems: From single-domain to cross-domain resilience enhancement," Proceedings of the IEEE, vol. 112, no. 4, pp. 365-398, 2024.

[28]J. Kandasamy, R. Ramachandran, V. Veerasamy, and A. Irudayaraj, "Distributed leader-follower based adaptive consensus control for networked microgrids," Applied Energy, vol. 353, pp. 122083, 2024.

[29]A. Sargolzaei, K. K. Yen, and M. N. Abdelghani, "Preventing time-delay switch attack on load frequency control in distributed power systems," IEEE Transactions on Smart Grid, vol. 7, no. 2, pp. 1176-1185, 2015.

[30]C. Yang, W. Yang, and H. Shi, "DoS attack in centralised sensor network against state estimation," IET Control Theory & Applications, vol. 12, no. 9, pp. 1244-1253, 2018.

[31]X. Liu, M. Shahidehpour, Z. Li, X. Liu, Y. Cao, and Z. Li, "Power system risk assessment in cyber attacks considering the role of protection systems," IEEE Transactions on Smart Grid, vol. 8, no. 2, pp. 572-580, 2016.

[32]J. Zhong, C. Chen, Z. Bie and M. Shahidehpour, "Strategic SDN-Based Microgrid Formation for Managing Communication Failures in Distribution System Restoration," IEEE Transactions on Power Systems, vol. 40, no. 3, pp. 2506-2518, 2025.

[33]J. Dai, Z. Dai, and V. Thing, "Cyber-resilience enhancement with cross-domain software-defined network for cyber-physical microgrids against denial of service attacks," IEEE Transactions on Industrial Cyber-Physical Systems, vol. 3, pp. 273-284, 2025.

[34]D. Jin et al., "Toward a cyber resilient and secure microgrid using software-defined networking," IEEE Transactions on Smart Grid, vol. 8, no. 5, pp. 2494-2504, 2017.

[35]M. Shahidehpour, M. Yan, S. Pandey, S. Bahramirad, and A. Passo, "Blockchain for peer-to-peer transactive energy trading in networked microgrids," IEEE Electrification Magazine, vol. 8, no. 4, pp. 80-90, 2020.

[36]J. Dai, J. Yang, Y. Wang and Y. Xu, "Blockchain-enabled cyber-resilience enhancement framework of microgrid distributed secondary control against false data injection attacks," IEEE Transactions on Smart Grid, vol. 15, no. 2, pp. 2226-2236, 2024.

[37]X. Han, X. Fang, Z. Li, B. Tan, R. Luo, "Two-Stage Operation Strategy for Leasing Shared Energy Storage to Renewable Power Producers with Bounded Rationality," Journal of Energy Storage, vol. 123, p. 116729, 2025.

[38]S. Ma, S. Wang and W. -T. Tsai, "Delay analysis of consensus communication for Blockchain-based applications using network calculus," IEEE Wireless Communications Letters, vol. 11, no. 9, pp. 1825-1829, 2022.

[39]M. Yan, M. Shahidehpour, et al., "Blockchain for Transacting Energy and Carbon Allowance in Networked Microgrids," IEEE Transactions on Smart Grid, vo. 12, no. 6, pp. 4702-4714, 2021.

[40]H. Bokkisam, S. Singh, R. M. Acharya and M. P. Selvan, "Blockchain-based peer-to-peer transactive energy system for community microgrid with demand response management," CSEE Journal of Power and Energy Systems, vol. 8, no. 1, pp. 198-211, 2022.

[41]M. J. Islam et al., "Blockchain-SDN-Based Energy-Aware and Distributed Secure Architecture for IoT in Smart Cities," IEEE Internet of Things Journal, vol. 9, no. 5, pp. 3850-3864, 2022.

[42]Y. Gao, Y. Chen, X. Hu, H. Lin, Y. Liu and L. Nie, “Blockchain based IIoT data sharing framework for SDN-enabled pervasive edge computing,” IEEE Transactions on Industrial Informatics, vol. 17, no. 7, pp. 5041-5049, 2021.

[43]Y. Zheng, Z. Yan, et al., “Vulnerability assessment of deep reinforcement learning models for power system topology optimization,” IEEE Transactions on Smart Grid, vol. 12, no. 4, pp. 3613-3623, 2021.

[44]Y. Fassi, V. Heiries, J. Boutet and S. Boisseau, “Toward physics-informed machine-learning-based predictive maintenance for power converters—A review,” IEEE Transactions on Power Electronics, vol. 39, no. 2, pp. 2692-2720, 2024.

[45]D. Dwivedi, P. Yemula and M. Pal, “DynamoPMU: A physics informed anomaly detection, clustering, and prediction method using nonlinear dynamics on μ PMU measurements,” IEEE Transactions on Instrumentation and Measurement, vol. 72, pp. 1-9, 2023,

[46]B. Mcmahan, E. Moore, D. Ramage, S. Hampson, and B. Arcas, “Communication-efficient learning of deep networks from decentralized data,” Proc. Artificial Intelligence and Statistics. PMLR, pp. 1273-1282, 2017.

[47]T. Li, A. Sahu, M. Zaheer, M. Sanjabi, A. Talwalkar, and V. Smith, “Federated optimization in heterogeneous networks,” Proc. Machine Learning and Syst., vol. 2, pp. 429-450, 2020.

[48]Z. Yan and Y. Xu, “Real-time optimal power flow with linguistic stipulations: Integrating GPT-agent and deep reinforcement learning,” IEEE Transactions on Power Systems, vol. 39, no. 2, pp. 4747-4750, 2024.

[49]Q. Yu, Z. Li, X. Han, et al., “End-to-end learning for stochastic preventive dispatch of renewables-rich power systems in abnormal weather conditions,” Renewable Energy, vol. 234, p. 121107, 2024.

[50]W. Ali, I. Ud Din, A. Almogren, and J. Rodrigues, “GreenTrust: Trust assessment using ensemble learning in internet of microgrid things,” IEEE Internet of Things Journal, vol. 12, no. 17, pp. 34636-34643, 2025.

[51]Z. Tang, P. Zhang, and W. Krawec, “Enabling resilient quantum-secured microgrids through software-defined networking,” IEEE Transactions on Quantum Engineering, vol. 3, pp. 1-11, 2022.

[52]Z. Tang, Y. Qin, Z. Jiang, W. Krawec, and P. Zhang, “Quantum-secure microgrid,” IEEE Transactions on Power Systems, vol. 36, no. 2, pp. 1250-1263, 2021.

[53]C. Cheng, Y. Qin, R. Lu, T. Jiang, and T. Takagi, “Batten down the hatches: securing neighborhood area networks of smart grid in the quantum era,” IEEE Transactions on Smart Grid, vol. 10, no. 6, pp. 6386-6395, 2019.

[54]P. Kong, “A review of quantum key distribution protocols in the perspective of smart grid communication security,” IEEE Systems Journal, vol. 16, no. 1, pp. 41-54, 2020.

[55]R. Yan, Y. Wang, J. Dai, Y. Xu, and A. Liu, “Quantum-key-distribution-based microgrid control for cybersecurity enhancement,” IEEE Transactions on Industry Applications, vol. 58, no. 3, pp. 3076-3086, 2022.

[56]X. Han, Z. Li, et al., “Quantum computing for stochastic economic dispatch in renewables-rich power systems,” IEEE Transactions on Smart Grid, vol. 16, no. 5, pp. 4113-4127, 2025.

[57]Y. Xu, Z. Li, X. Han, et al., “Joint generation-transmission expansion planning in renewables-dominated power systems based on hybrid quantum-classical computing,” International Journal of Electrical Power & Energy Systems, early access.

[58]Y. Xu, Z. Li, X. Han, et al., “Hybrid quantum-classical stochastic programming for co-planning 5G base stations and photovoltaic power stations in urban communities,” Scientific Reports, early access.

[59]X. Han, Z. Li, and Y. Xu, Quantum-assisted stochastic economic dispatch for renewables-rich power systems, IEEE PES General Meeting, 2024.

[60]C. Jiang et al., “Privacy preservation for cloud-edge-collaborative energy management system using post-quantum homomorphic encryption,” IEEE Transactions on Smart Grid, vol. 16, no. 4, pp. 3282-3294, 2025.

[61]R. Yu, R. Dutta, and J. Liu, “On topology design for the quantum Internet,” IEEE Network, vol. 36, no. 5, pp. 64-70, Sept. 2022.

[62]P. Babahajiani, P. Zhang, T. Wei, J. Liu, and X. Lu, “Employing interacting qubits for distributed microgrid control,” IEEE Transactions on Power Systems, vol. 38, no. 4, pp. 3123-3135, 2023.

[63]NREL, https://www.nrel.gov/news/detail/program/ 2023/quantum-computers-can-now-interface-with-power-grid-equipment, Accessed 2025.

[64]W. Yao, Y. Wang, Y. Xu and C. Deng, “Cyber-resilient control of an islanded microgrid under latency attacks and random DoS attacks,” IEEE Transactions on Industrial Informatics, vol. 19, no. 4, pp. 5858-5869, 2023.

[65]P. S. Tadepalli and D. Pullaguram, “Distributed control microgrids: Cyber-attack models, impacts and remedial strategies,” IEEE Transactions on Signal and Information Processing over Networks, vol. 8, pp. 1008-1023, 2022.

[66]I. Zografopoulos and C. Konstantinou, “Detection of malicious attacks in autonomous cyber-physical inverter-based microgrids,” IEEE Transactions on Industrial Informatics, vol. 18, no. 9, pp. 5815-5826, 2022.

[67]M. Z. Shahabadi, H. Atrianfar and H. A. Abyaneh, “An enhanced detection scheme and distributed resilient asynchronous event-triggered control of AC microgrids subject to replay attacks,” IEEE Transactions on Cybernetics, vol. 55, no. 11, pp. 5161-5176, 2025.

[68]G. Zhuang, J. Zhu, G. Zong and J. Xia, “Observer-based resilient adaptive neural sliding mode control for DC-MGs under blended attacks with multidomain attack-aware scheduling protocol,” IEEE Internet of Things Journal, vol. 12, no. 14, pp. 28229-28244, 2025.

[69]P. Chen, S. Liu, B. Chen and L. Yu, “Multi-agent reinforcement learning for decentralized resilient secondary control of energy storage systems against DoS attacks,” IEEE Transactions on Smart Grid, vol. 13, no. 3, pp. 1739-1750, 2022.

[70]F. Cheng, J. Lai and Z. Zeng, “Bilevel distributed secure control of DC microgrid clusters under scale random cyberattacks,” IEEE Transactions on Smart Grid, vol. 16, no. 6, pp. 4324-4334, 2025.

[71]H. Guo, X. Dai, S. Bu and Z. Zhang, “Distributed secondary control of DC microgrids under unreliable communication networks,” IEEE Transactions on Automation Science and Engineering, vol. 22, pp. 22900-22911, 2025.

[72]Y. Zhang, C. Peng, C. Cheng and Y. Wang, “Attack intensity dependent adaptive load frequency control of interconnected power systems under malicious traffic attacks,” IEEE Transactions on Smart Grid, vol. 14, no. 2, pp. 1223-1235, 2023.

[73]Y. Zhang, C. Peng, S. Xie and X. Du, “Deterministic network calculus-based H_∞ load frequency control of multiarea power systems under malicious DoS attacks,” IEEE Transactions on Smart Grid, vol. 13, no. 2, pp. 1542-1554, 2022.

[74]Y. Ding, F. Gao and M. M. Khan, “Transient stability analysis of microgrid considering impact of grid-following converter's current controller,” IEEE Transactions on Power Electronics, vol. 39, no. 8, pp. 9100-9105, 2024.

[75]Y. Tang, Z. Tian, X. Zha, X. Li, M. Huang and J. Sun, “An improved equal area criterion for transient stability analysis of converter-based microgrid considering nonlinear damping effect,” IEEE Transactions on Power Electronics, vol. 37, no. 9, pp. 11272-11284, 2022.

[76]B. She, F. Li, H. Cui, J. Zhang and R. Bo, “Fusion of microgrid control with model-free reinforcement learning: Review and vision,” IEEE Transactions on Smart Grid, vol. 14, no. 4, pp. 3232-3245, 2023.

[77]A. Selim, J. Zhao, J. Dong and J. Lian, “Safe deep reinforcement learning for robust frequency and voltage-constrained networked microgrid restoration,” IEEE Transactions on Industry Applications, early access.

[78]M. Mahmoodi, et al., “DER capacity assessment of active distribution systems using dynamic operating envelopes”, IEEE Transactions on Smart Grid, vol. 15, no. 2, pp. 1778-1791, 2024.

[79]O. Salem, A. Serhrouchni, A. Mehaoua and R. Boutaba, “Event detection in wireless body area networks using Kalman filter and power divergence,” IEEE Transactions on Network and Service Management, vol. 15, no. 3, pp. 1018-1034, 2018.

[80]X. Xiao, Z. Li, X. Han, et al., “A convex approximation method for smoothing out control of voltage profile at a critical distribution bus under sharp PV power fluctuations,” IEEE Transactions on Sustainable Energy, vol. 15, no. 3, pp. 2038-2049, 2024.

[81]Q. Zhou, Z. Tian, M. Shahidehpour, X. Liu, A. Alabdulwahab and A. Abusorrah, “Optimal consensus-based distributed control strategy for coordinated operation of networked microgrids,” IEEE Transactions on Power Systems, vol. 35, no. 3, pp. 2452-2462, 2020.

[82]M. Shi, M. Shahidehpour, Q. Zhou, X. Chen and J. Wen, “Optimal consensus-based event-triggered control strategy for resilient DC microgrids,” IEEE Transactions on Power Systems, vol. 36, no. 3, pp. 1807-1818, 2021.

[83]X. Han and Y. Zhang, “Decomposition-coordination-based voltage control for high photovoltaic-penetrated distribution networks under cloud-edge collaborative architecture,” International Transactions on Electrical Energy Systems, vol. 2022, no. 1, p. 7280220, 2022.

[84]Q. Zhou, Z. Li, Q. Wu and M. Shahidehpour, “Two-stage load shedding for secondary control in hierarchical operation of islanded microgrids,” IEEE Transactions on Smart Grid, vol. 10, no. 3, pp. 3103-3111, 2019.

[85]P. Danzi, M. Angjelichinoski, Č. Stefanović, T. Dragičević, and P. Popovski, “Software-defined microgrid control for resilience against denial-of-service attacks,” IEEE Transactions on Smart Grid, vol. 10, no. 5, pp. 5258-5268, 2019.

[86]X. Wu, X. Chen, M. Shahidehpour, Q. Zhou and L. Fan, “Distributed cooperative scheme for forced oscillation location identification in power systems,” IEEE Transactions on Power Systems, vol. 35, no. 1, pp. 374-384, 2020.

[87]Y. Li, Y. Qin, P. Zhang and A. Herzberg, “SDN-enabled cyber-physical security in networked microgrids,” IEEE Transactions on Sustainable Energy, vol. 10, no. 3, pp. 1613-1622, 2019.

[88]D. Jin et al., “Toward a cyber resilient and secure microgrid using software-defined networking,” IEEE Transactions on Smart Grid, vol. 8, no. 5, pp. 2494-2504, 2017.

[89]T. Yang, X. Han, H. Li, W. Li and A. Y. Zomaya, “Parallel scientific power calculations in cloud data center based on decomposition-coordination directed acyclic graph,” IEEE Transactions on Cloud Computing, vol. 11, no. 3, pp. 2491-2502, 2023.

[90]Microgrid, https://www.iit.edu/microgrid, Accessed 2025.

[91]Y. Zhang, C. Peng, C. Cheng, and Y. Wang, “Attack intensity dependent adaptive load frequency control of interconnected power systems under malicious traffic attacks,” IEEE Transactions on Smart Grid, vol. 14, no. 2, pp. 1223-1235, 2023.

[92]Q. Zhou, M. Shahidehpour, A. Alabdulwahab and A. Abusorrah, “Unification scheme for managing master controller failures in networked microgrids,” IEEE Transactions on Power Systems, vol. 35, no. 4, pp. 3004-3014, 2020.

[93]M. Yan, W. Guo, H. Zheng and T. Qin, “Joint NTP-MAPPO and SDN for energy trading among multi-base-station microgrids,” IEEE Internet of Things Journal, vol. 11, no. 10, pp. 18568-18579, 2024.

[94]Z. Li, X. Han, M. Shahidehpour, P. Ju, and Q. Yu, “Analyzing the resilience of active distribution networks to hazardous weather considering cyber-physical interdependencies,” Engineering, vol. 51, pp. 2881-2897, 2024.

[95]HELICS, https://helics.org/introduction, Accessed 2025.

[96]OpenDSS, https://www.epri.com/pages/sa/opendss, Accessed 2025.

[97]Simulink, https://www.mathworks.com/products/simulink.html, Accessed 2025.

[98]M. Sheikholeslami, M. Shahidehpour, A. Paaso, S. Bahramirad and Z. Li, "Challenges of modeling and simulation of clustered Bronzeville Community Microgrid (BCM) and IIT Campus Microgrid (ICM) using RTDS," 2020 IEEE Power & Energy Society General Meeting (PESGM), Montreal, QC, Canada, 2020, pp. 1-5.

[99]V. Venkataramanan, Y. Zhou and A. Srivastava, "Analyzing impact of communication network topologies on reconfiguration of networked microgrids," 2016 North American Power Symposium (NAPS), Denver, CO, USA, 2016, pp. 1-6.

[100] L. L. Zulu, K. A. Ogudo and P. O. Umenne, "Simulating software defined networking using mininet to optimize host communication in a realistic programmable network," 2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD), Durban, South Africa, 2018, pp. 1-6.

[101] E. Al-Shaer and H. Hamed, "Firewall policy advisor for anomaly discovery and rule editing," In Proc. of IFIP/IEEE Eighth International Symposium on Integrated Network Management, pages 17-30, IEEE, 2003.

[102] H. Liao, P. Armstrong, and J. Rounds, "Development and initial validation of public domain basic interest markers," Journal of Vocational Behavior, vol. 73, no. 1, pp.159-183, 2008.

[103] A. Cahn, J. Hoyos, M. Hulse, and E. Keller. Software-defined energy communication networks: From substation automation to future smart grids. In Proc. of the 2013 IEEE International Conference on Smart Grid Communications (SmartGridComm), 2013.

[104] North American Electric Reliability Corporation (NERC). Critical infrastructure protection. http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx, Accessed 2008.

[105] I. Balepin, S. Maltsev, J. Rowe, and K. Levitt, "Using specification-based intrusion detection for automated response," In Recent Advances in Intrusion Detection, pp. 136-154. Springer, 2003.

ACKNOWLEDGEMENT

This article was made possible in part by the US Department of Energy grant # DE-CR0000042, titled 2MC: Midwest Center for Microgrid Cybersecurity.

AUTHORS' BIOGRAPHIES

Xutao Han is currently pursuing the Ph.D. degree in electrical engineering at Zhejiang University, Hangzhou, China. His research interest includes cyber-physical power systems.

Zhiyi Li received the Ph.D. degree from the Department of Electrical and Computer Engineering, Illinois Institute of Technology, Chicago, USA, in 2017. From August 2017 to May 2019, he was a Senior Research Associate with the Robert W. Galvin Center for Electricity Innovation, Illinois Institute of Technology. Since June 2019, he has been a Tenure-Track Associate Professor with the College of Electrical Engineering, Zhejiang University, Hangzhou, China. His research interests include cyber physical systems and power system optimization.

Shuheng Wei received the B.S. degree in electrical engineering and its automation from Wuhan University, Wuhan, China, in 2020. He is currently pursuing the Ph.D. degree at the School of Electrical Engineering, Southeast University, Nanjing, China. His research interests include state estimation and cybersecurity of power distribution networks.

Mohammad Shahidehpour is a University Distinguished Professor, Galvin Chair Professor and Director of the Robert W. Galvin Center for Electricity Innovation, Illinois Institute of Technology, Chicago, IL, USA. He is a Fellow

of the IEEE, the American Association for the Advancement of Science, and the National Academy of Inventors. Dr. Shahidehpour is a member of the U.S. National Academy of Engineering and listed as a highly cited researcher on the Web of Science (ranked in the top 1% by citations demonstrating significant influence among his peers).