# Design of a Security Operations Center (SOC) for Cyber-Physical Situational Awareness in Microgrid SCADA Systems

Swetha Rani Kasimalla
*Electrical and Computer Engineering*
*University of Michigan-Dearborn*
Michigan, USA
sweraka@umich.edu

Kuchan Park
*Electrical and Computer Engineering*
*University of Michigan-Dearborn*
Michigan, USA
kuchan@umich.edu

Junho Hong
*Electrical and Computer Engineering*
*University of Michigan-Dearborn*
Michigan, USA
jhwr@umich.edu

Chul-Sang Hwang
*Smart Grid Research Division*
*Korea Electrotechnology Research Institute (KERI)*
Gwangju-si, South Korea
hcs1006@keri.re.kr

Young-Woo Youn
*Smart Grid Research Division*
*Korea Electrotechnology Research Institute (KERI)*
Gwangju-si, South Korea
ywyoun@keri.re.kr

***Abstract*—Traditional SCADA systems in microgrids rely on cyber communication for monitoring and control but lack mechanisms to verify data integrity, making them vulnerable to cyber-physical disruptions. This paper demonstrates a Security Operation Center (SOC) framework developed at the Korea Electrotechnology Research Institute (KERI) to enable realistic testing, visualization, and mitigation of cyberattacks on microgrid SCADA environments. Using a cyber-physical testbed integrating a real-time simulator and hardware-in-the-loop (HIL) components, replay, denial-of-service, and false-data-injection attacks were emulated to illustrate their operational impact. Experimental results, including real-time voltage, current, and breaker status waveforms under attack conditions, highlight how malicious commands and falsified measurements can compromise microgrid stability. To enhance resilience, the SOC incorporates SDN-based traffic control and a reliability-aware load prioritization strategy for maintaining critical loads during disturbances. The study demonstrates KERI's capability to conduct comprehensive SOC-level evaluations and underscores the need for coordinated cyber-physical monitoring to ensure secure and reliable microgrid operation.**

***Index Terms*—Security Operation Center (SOC), microgrid, Software-Defined Networking (SDN), cyber-physical system, cybersecurity**

## I. Introduction

The increasing digitalization of electric power systems has brought unprecedented visibility and controllability but has also expanded the potential attack surface of modern grid infrastructures. In particular, supervisory control and data acquisition (SCADA) systems, once isolated and physically protected, now rely heavily on Internet Protocol (IP)-based communication to acquire measurements and issue control commands. While this connectivity enables advanced monitoring and optimization, it also introduces cyber vulnerabilities that can directly compromise physical operations. Conventional SCADA systems inherently assume that the data transmitted from field devices are trustworthy; however, recent incidents and experiments have shown that malicious data manipulation, packet replay, and denial-of-service attacks can lead to false operational decisions, unintentional tripping of breakers, and even widespread service interruptions [1], [2].

Microgrids have demonstrated a proven ability to enhance system reliability and resilience; however, their increasing digitization and interconnected control layers also expose them to potential vulnerabilities [3]. Hence it is important to develop systematic mechanisms that ensure cyber-physical situational awareness, i.e., a real-time understanding of both the cyber state (e.g., communication integrity and latency) and the physical state (e.g., voltage, current, and frequency stability) of the system [4]. To address these challenges, this paper proposes the design and implementation of a SOC tailored for microgrid SCADA systems. The SOC functions as a supervisory intelligence layer that continuously correlates cyber events with physical system responses, enabling the detection, visualization, and mitigation of coordinated cyber-physical anomalies.

Unlike traditional intrusion detection systems that focus solely on network signatures, the proposed SOC integrates power system observability and cyber telemetry to distinguish between legitimate physical disturbances, such as voltage sags or equipment faults and cyber-induced anomalies such as false data injection (FDI) or control-command spoofing. The concept was validated through a cyber-physical microgrid testbed developed at the Korea Electrotechnology Research Institute (KERI) Gwangju Branch, which integrates a real-time simulator and HIL components. This digital-twin-based environment allows emulation of realistic control and communication conditions prior to field deployment. Several representative

979-8-3315-8138-1

cyberattacks, including replay, denial-of-service, and FDI were implemented on microgrid assets such as photovoltaic inverters, transformers, and protective relays. The SOC was then utilized to analyze network traffic patterns, detect abnormal behavior, and initiate mitigation responses. Mitigation strategies were evaluated from both the cyber and physical perspectives. On the cyber side, Software-Defined Networking (SDN) was employed to dynamically isolate malicious traffic and enforce flow-level control policies, minimizing the propagation of attacks across network segments [5]. On the physical side, a reliability-aware load management algorithm was applied to preserve the supply continuity of critical loads during cyber-physical disturbances. The combined SOC–SDN–HIL framework demonstrated significant improvement in operational resilience and detection accuracy compared to conventional SCADA monitoring.

The key contributions of this paper are as follows: (1) Cyber-Physical Situational Awareness using SOC: A unified Security Operation Center architecture is developed to correlate cyber network anomalies with physical power system behavior, achieving real-time cyber-physical situational awareness in microgrid SCADA systems. (2) Reliability Assessment–Based Cyber-Physical Mitigation: A reliability-driven control and load management framework is proposed to maintain operational continuity during cyber-physical disturbances, validated through the PHIL-based testbed at KERI. Overall, the proposed framework provides a scalable, experimentally validated pathway toward secure and resilient operation of future distributed energy systems.

The remainder of the paper is organized as follows: Section II outlines the SOC model and the configuration of the cyber-physical system. Section III presents the assessment of cyber-physical threats along with corresponding mitigation strategies. Section IV discusses the reliability analysis for critical load management under fault and cyber event scenarios. Finally, Section V concludes the paper.

## II. SOC for Cyber-Physical Systems

### A. Cyber Physical Systems

To validate advanced low-voltage distribution network technologies under realistic operating conditions, the integrated demonstration platform incorporates a comprehensive range of power system components, as depicted in Fig. 1. The corresponding cyber-physical single-line diagram (SLD) provides an intuitive visualization of the real-time operational status of each line within the microgrid, enabling effective monitoring and coordination between electrical and communication layers. Green-colored lines represent energized lines that are actively carrying current and operating under nominal conditions. Orange-colored lines indicate the presence of voltage without active current flow, suggesting that the line is energized but not under load. Gray-colored lines denote segments that are either completely de-energized or disconnected due to fault isolation or switching events. Additionally, lines highlighted in a gray-blue combination reflect segments maintaining communication connectivity, yet trending toward a shutdown state due to upstream or downstream contingencies. This layered visual encoding enables intuitive monitoring of both electrical and communication statuses across the network, supporting timely fault identification and response. The indoor facilities include AC/DC hybrid microgrid pilot plants, power amplifiers, on-load tap-changing (OLTC) transformers, and various programmable loads. The outdoor test facilities include diesel generators, photovoltaic arrays, battery energy storage, green hydrogen production units, and fuel cell systems. Real-time simulators are interconnected to support synchronized cyber-physical experiments and power hardware-in-the-loop (PHIL) validation. All components are centrally managed through an integrated supervisory control system enabling unified monitoring, data acquisition, and coordinated operation. This setup ensures repeatable, high-fidelity testing of cyber-physical microgrid performance. Table I summarizes the major equipment and components of the demonstration platform.

TABLE I
EQUIPMENT CONFIGURATION OF THECYBER PHYSICAL SYSTEMS OF MICROGRID

| Item | Rated Capacity | Quantity | Location |
|---|---|---|---|
| Diesel Generator | Research-use 100k | 1 | Outdoor |
| Photovoltaic (PV) System | Power generation 200k, 100k | 2 | Outdoor |
| | Research-use 50k | 1 | Outdoor |
| Green Hydrogen | Research-use 50k, 10Nm^3/h | 1 | Outdoor |
| Fuel Cell | Research-use 10k | 1 | Outdoor |
| Energy Storage System (ESS) | Research-use 100kW/220kWh | 2 | Outdoor |
| | Research-use 50kW/100kWh | 2 | Indoor |
| ACMG Pilot Plant | 200kW-level (lines, DER, etc.) | Several | Indoor |
| DCMG Pilot Plant | 100kW-level (lines, DER, etc.) | Several | Indoor |
| Real Loads | TR2500, TR1500, TR750, TR400 | 4 | Outdoor |
| Research Loads | RLC 600k, 100k, 150k | Several | Indoor |
| Power Amplifier | AC 21kVA (Linear) | 1 | Indoor |
| | AC 600k, 60k (Switching) | 2 | Indoor |
| | DC 600k, 60k, 60k (Switching) | 3 | Indoor |
| Real-Time Emulator | RTDS, OPAL-RT, Speedgoat | 3 | Indoor |
| Software | Integrated Program | 1 | Indoor |

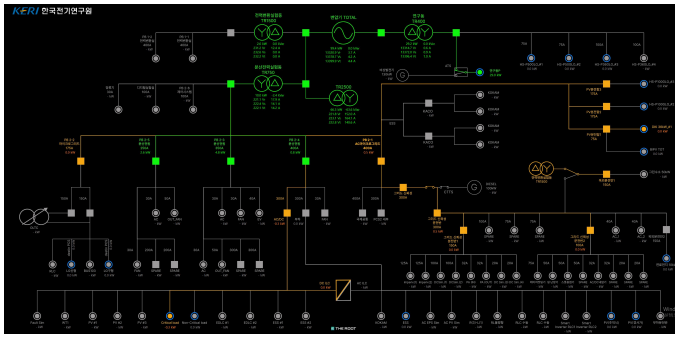

Fig. 1. Single Line Diagram of Cyber Physical Systems of Microgrid.

### B. PHIL Testbed

To complement the integrated infrastructure introduced earlier, a PHIL testbed has been established to enable safe and repeatable validation of new devices and cyber-physical interactions. Because the available real-world resources are limited, the PHIL environment is used to emulate and validate various operational scenarios, including equipment testing, control verification, and the impact analysis of cyberattacks.

To complement the integrated infrastructure introduced earlier, a PHIL testbed has been established to enable safe and repeatable validation of new devices and cyber-physical interactions. Because the available real-world resources are limited, the PHIL environment, illustrated in Fig. 2, is used to emulate and validate various operational scenarios, including equipment testing, control verification, and the impact analysis of cyberattacks.

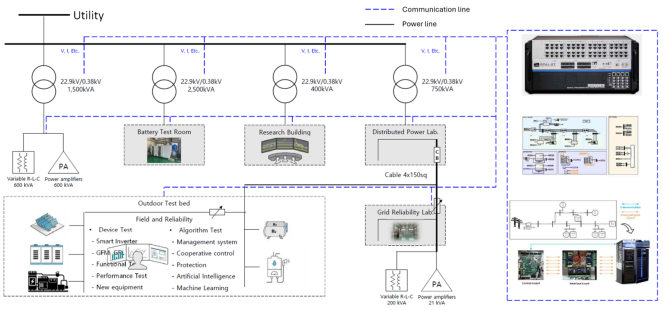


Fig. 2. PHIL testbed for SOC.

### C. Security Operations Center (SOC)

The SOC serves as the supervisory layer of the proposed cyber-physical microgrid framework, providing real-time monitoring, detection, and coordinated response across both cyber and physical domains. Unlike conventional IT SOCs, it integrates operational-technology data by combining network telemetry with real-time measurements from SCADA, IEDs, and DER controllers. Built on a cyber-physical assessment architecture, it fuses a Security Information and Event Management (SIEM) engine with a Physical System State Analyzer [6] to detect replay, DoS, and FDI attacks while validating measurement consistency against grid models. Through tight integration with a SDN interface, the SOC dynamically isolates compromised communication flows, reroutes control traffic, and triggers priority-based load management to maintain service continuity. Validated through a PHIL testbed, the framework demonstrates reduced detection latency, faster recovery, and sustained delivery of critical loads, showcasing its capability to enable adaptive, secure, and resilient microgrid operation under cyber-physical stress.

## III. Cyber Physical Systems of Microgrid

### A. Cyber vulnerability assessment

This subsection evaluates representative cyber threats to the microgrid SCADA and DER ecosystem and summarizes the criteria used to select attack types for experimental validation. We focus on three classes of attacks, replay, DoS, and FDI because they are (i) well-documented in the literature, (ii) practical to execute against common OT protocols (e.g., Modbus-TCP, DNP3, IEC-61850), and (iii) capable of producing distinct and consequential cyber-to-physical impacts on inverter, breaker, and protection behavior.

- Replay attacks involve retransmitting previously captured control or measurement signals to mislead devices with outdated information [7]. In microgrids, this can trigger false operations such as repeated breaker switching or incorrect inverter settings. These attacks exploit the absence of sequence or freshness checks. Their effects are observable in PHIL setups through abnormal switching or protection behavior.
- Denial-of-Service (DoS) attacks flood network resources with excessive traffic, causing delays and packet loss [8]. In microgrids, this disrupts time-sensitive operations like inverter control and protection coordination. Such disruptions can lead to delayed tripping or forced islanding. We analyze DoS to assess SOC detection delay and the impact of network-level mitigations.
- FDI attacks manipulate measurement or control signals without disrupting normal communication protocols, thereby deceiving the control logic. Such attacks can mask hazardous operating conditions such as network stress or voltage instability while the system appears stable. Breaker control commands are particularly vulnerable, as they are transmitted through communication networks and can be maliciously altered by attackers.

Fig. 3, illustrates the impact of an FDI attack on the PCC breaker. Up to 0.05 s, the system operates under normal grid-connected conditions, with balanced voltage and current waveforms. However, when the breaker is abnormally opened due to a falsified command, both voltage and current collapse to near zero, indicating an unintended islanding condition. A small residual voltage persists due to the floating-bus effect or partial inverter operation. Subsequently, at approximately 0.10 s, an abnormal breaker reclosure occurs without proper synchronization. This asynchronous reconnection produces severe transient spikes in current and significant phase distortion in voltage, reflecting a loss of synchronism with the upstream grid. Such unsynchronized reclosing leads to large inrush currents and phase-angle mismatches that can cause equipment damage, relay misoperation, and system instability. This scenario underscores the necessity of physics-aware validation within the SOC framework to ensure that breaker operations occur only after verified synchronization commands, thereby maintaining grid stability and secure operation under cyber threats.

### B. Cyber Mitigation Strategies

SDN decouples control from data forwarding, enabling centralized, programmable management of distributed switches. This offers global traffic visibility and dynamic flow control across the microgrid. In the proposed framework, the SOC detects cyber-physical anomalies, while the SDN controller enforces mitigation actions such as isolation, rerouting, or rate limiting. Together, they transform static infrastructure into an adaptive, resilient cyber-physical defense layer.

*1) Replay Attack Mitigation:* Replay attacks reintroduce previously valid control or measurement packets, causing devices to act on outdated information. SDN mitigates these attacks by detecting duplicate payloads and irregular timestamps using protocol-aware monitoring and immediately enforcing

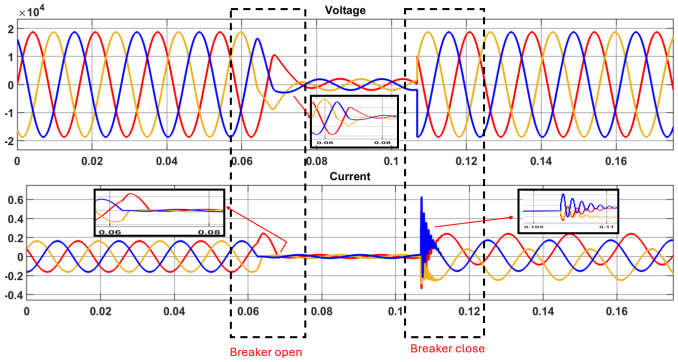


Fig. 3. Voltage and current response at the PCC under cyber-induced abnormal breaker operation. Unauthorized breaker actions cause transient spikes and phase asynchronization, which can destabilize the microgrid system.

flow redirection or rate limits to isolate suspicious traffic. For safety-critical commands, the controller applies a verification proxy, validating command freshness and logical consistency before execution. This ensures only authentic, time-valid operations reach field devices, reducing false actuation risks while maintaining real-time responsiveness.

*2) DoS Attack Mitigation:* DoS attacks overload devices or links with excessive traffic, delaying or blocking legitimate control messages. Leveraging its global flow visibility, the SDN controller detects sudden traffic surges or abnormal latency patterns and applies metering and QoS policies to preserve bandwidth for critical control traffic. When attack persistence is confirmed, the controller enforces drop or reroute rules to isolate the offending source. This hierarchical mitigation preserves operational continuity even under severe network stress [9].

*3) FDI Mitigation:* FDI attacks manipulate sensor or control data to mislead decision-making. In response, the SDN-enabled defense enforces write access through verified paths and validates payloads via range checks, rate limits, and sensor redundancy. Abnormal flows are blocked or rerouted for operator review, preserving cyber-physical integrity.

Integrated with SOC, SDN offers adaptive defense against replay, DoS, and FDI by isolating malicious flows and securing critical communication. This enhances system resilience and ensures reliable operation under coordinated attacks. Building on these security capabilities, the next section evaluates how the system maintains reliability through critical load management during disturbance conditions.

## IV. Reliability Assessment for Critical Load Management

To ensure continuous operation of critical infrastructure under cyber–physical disturbances, a reliability-aware control algorithm is developed. The algorithm dynamically balances available generation with prioritized load demand to preserve essential services even during severe uncertainty such as generation shortage, communication faults, or cyber intrusions. The proposed framework quantifies system reliability in real time through the reliability factor $\eta_{\text{rel}}(t)$, representing the ratio of served to total critical load demand.

The algorithm operates on the fundamental power-balance principle given by Eq. (1):

$$\sum_{g=1}^{N_{DG}} P_g(t) = P_{\text{load}}(t) + P_{\text{loss}}(t) + \Delta_{LG}(t), \tag{1}$$

where $P_g(t)$ is the generation from each distributed generator, $P_{\text{load}}(t)$ is total demand, and $P_{\text{loss}}(t)$ represents system losses. When a deficit occurs ($\Delta_{LG}(t) > 0$), non-critical loads are curtailed to restore balance:

$$LC(t) = \max(0, \Delta_{LG}(t)). \tag{2}$$

The corresponding critical-load reliability is defined as:

$$\eta_{\text{rel}}(t) = 1 - \frac{LC_{\text{critical}}(t)}{P_{\text{critical,total}}(t)}. \tag{3}$$

A priority-based allocation function ensures that power is distributed according to the importance of each load. Let $L_i(t)$ denote the demand of load $i$ and $\omega_i \in [0, 1]$ its priority weight ($\omega_i = 1$ for critical loads). The optimization objective is:

$$\max \sum_{i=1}^{N_L} \omega_i \tilde{P}_i(t), \tag{4}$$

subject to the generation constraint:

$$\sum_{i=1}^{N_L} \tilde{P}_i(t) \leq \sum_{g=1}^{N_{DG}} P_g(t), \tag{5}$$

where $\tilde{P}_i(t)$ represents the allocated power to each load. High-priority loads are served first, while non-essential loads are curtailed if a deficit remains. This allocation minimizes non-consequential load loss and maintains $\eta_{\text{rel}}(t)$ close to unity during emergencies.

The time-averaged system reliability across a simulation horizon $T$ is expressed as:

$$R_{\text{sys}} = \frac{1}{T} \sum_{t=1}^{T} \eta_{\text{rel}}(t), \tag{6}$$

where $R_{\text{sys}} \to 1$ indicates uninterrupted service to all critical loads. A complementary risk indicator $A_{\text{risk}}(t)$ is defined such that $A_{\text{risk}}(t) = 1$ when $\Delta_{LG}(t) > 0$ or when the SOC detects abnormal cyber conditions. This flag provides immediate feedback for the SOC to activate corrective actions such as reserve deployment, load reallocation, or islanding transition—to maintain reliability.

The framework differentiates between planned and unplanned islanding. Planned islanding is initiated intentionally under known contingencies, allowing optimized generation scheduling, whereas unplanned islanding is triggered automatically during disturbances such as frequency deviations or cyber intrusions. In both cases, the SOC oversees the transition, validates sensor integrity, and maintains supply to critical loads. Islanding thresholds follow IEEE 1547–2018 and IEEE 2030.7/2030.8, with disconnection occurring when

$|f - f_{\text{nom}}| > 0.5$–$1.0$ Hz or $|V - V_{\text{nom}}| > 0.1V_{\text{nom}}$, and reconnection allowed only after parameters return to nominal limits.

### A. Reserve-Aware Reliability Enhancement

To enhance operational realism, the instantaneous active power balance is extended to include both spinning and non-spinning reserves. Let $p_g(t)$ denote the scheduled generation, $r_g^{sp}(t)$ and $r_g^{ns}(t)$ the available spinning and non-spinning reserves, and $x_g^{sp}(t)$ and $x_g^{ns}(t)$ the deployed portions. The extended power balance is:

$$\sum_{g=1}^{N_{DG}} [p_g(t) + x_g^{sp}(t) + x_g^{ns}(t)] = P_{\text{load}}(t) + P_{\text{loss}}(t) - LC(t). \tag{7}$$

Generator operating and reserve constraints are:

$$0 \le p_g(t) \le P_g^{\max} u_g(t), \tag{8}$$

$$0 \le r_g^{sp}(t) \le P_g^{\max} u_g(t) - p_g(t), \tag{9}$$

$$0 \le r_g^{ns}(t) \le P_g^{\max}(1 - u_g(t)), \tag{10}$$

where $u_g(t) \in \{0, 1\}$ denotes the generator commitment status.

Reserve deployment is bounded by:

$$0 \le x_g^{sp}(t) \le r_g^{sp}(t), \tag{11}$$

$$0 \le x_g^{ns}(t) \le r_{g,\text{avail}}^{ns}(t), \tag{12}$$

where delayed non-spinning reserve activation is modeled as:

$$r_{g,\text{avail}}^{ns}(t) = y_g(t - \tau_g) r_g^{ns}(t - \tau_g), \tag{13}$$

with $\tau_g$ representing the start-up delay and $y_g(t)$ the start command signal.

The initial generation deficit before reserve activation is:

$$\Delta L_0(t) = P_{\text{load}}(t) + P_{\text{loss}}(t) - \sum_{g=1}^{N_{DG}} p_g(t), \tag{14}$$

and the residual deficit after reserve deployment:

$$\Delta L_1(t) = \max\left(0, \Delta L_0(t) - \sum_{g=1}^{N_{DG}} [x_g^{sp}(t) + x_g^{ns}(t)]\right). \tag{15}$$

The instantaneous load curtailment is thus defined as:

$$LC(t) = \Delta L_1(t). \tag{16}$$

System-level reserve adequacy is maintained through:

$$\sum_{g=1}^{N_{DG}} r_g^{sp}(t) \ge R_{sp}^{\text{req}}(t), \tag{17}$$

$$\sum_{g=1}^{N_{DG}} [r_g^{sp}(t) + r_g^{ns}(t)] \ge R_{tot}^{\text{req}}(t), \tag{18}$$

ensuring compliance with $N-1$ reliability criteria. $R_{sp}^{\text{req}}(t)$ maintains synchronized spinning margin to counter short-term deviations, while $R_{tot}^{\text{req}}(t)$ guarantees that total reserves can recover from the largest generator outage or abrupt demand surge. This reserve-aware model integrates spinning and non-spinning reserves for time-coordinated mitigation. Coupled with SOC-based cyber monitoring, it dynamically reallocates reserves or curtails non-critical loads based on detected risks, thereby enhancing microgrid resilience through unified physical and cyber reliability control.

## V. Conclusions

This study proposed a SOC-enabled cyber-physical framework that enhances microgrid resilience by integrating SDN-based adaptive communication control, PHIL validation, and reliability-aware load management. Case studies with replay, DoS, and FDI attacks validated the framework's ability to detect and mitigate threats while maintaining critical services. The SDN controller effectively isolated malicious flows, and the reliability algorithm ensured continuous supply to priority loads. Overall, the coordinated SOC–SDN operation significantly improved detection latency, service continuity, and system stability—demonstrating a unified strategy for achieving holistic cyber-physical resilience in modern microgrids. Future work will focus on validating the proposed framework using real hardware systems in the KERI cyber-physical testbed, integrating AI-based anomaly prediction within the SOC, and extending the architecture to support coordinated protection across interconnected multi-microgrid environments

## References


[1] G. Zhang, J. Li, O. Bamisile, Y. Xing, D. Cao, and Q. Huang, "Identification and classification for multiple cyber attacks in power grids based on the deep capsule cnn," *Engineering Applications of Artificial Intelligence*, vol. 126, p. 106771, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0952197623009557

[2] S. Mogilicharla, M. Tripathy, and M. Kanabar, "Integrating cyber and physical analysis for intrusion detection in plant-level der microgrids," *IEEE Transactions on Industry Applications*, vol. 61, no. 4, pp. 5430–5444, 2025.

[3] S. R. Kasimalla, K. Park, A. Zaboli, Y. Hong, S. L. Choi, and J. Hong, "An evaluation of sustainable power system resilience in the face of severe weather conditions and climate changes: A comprehensive review of current advances," *Sustainability*, vol. 16, no. 7, 2024. [Online]. Available: https://www.mdpi.com/2071-1050/16/7/3047

[4] K. Akramul Haque, M. Massaoudi, L. Al Homoud, K. R. Davis, M. Kabalan, and H. Salamy, "Cyber-physical emulation and threat scenario simulation for enhanced microgrid resilience," *IEEE Access*, vol. 13, pp. 101 455–101 471, 2025.

[5] M. Girdhar, J. Hong, W. Su, A. Herath, and C.-C. Liu, "Sdn-based dynamic cybersecurity framework of iec-61850 communications in smart grid," in *2024 IEEE Power & Energy Society General Meeting (PESGM)*, 2024, pp. 1–5.

[6] N. Tendikov, L. Rzayeva, B. Saoud, I. Shayea, M. H. Azmi, A. Myrzatay, and M. Alnakhli, "Security information event management data acquisition and analysis methods with machine learning principles," *Results in Engineering*, vol. 22, p. 102254, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2590123024005097

[7] 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.

[8] L. Chen, X. Zhang, and F. Xiao, "A stability condition for asynchronous and aperiodic sampled-data cyber-physical systems under dos attacks," *IEEE Transactions on Industrial Cyber-Physical Systems*, vol. 3, pp. 397–407, 2025.

[9] J. Chen, A. Kemmeugne, J. Yan, M. Ghafouri, M. Kassouf, and M. Debbabi, "An sdn-based framework for cyber-physically coordinated voltage support of virtual power plants against dos attacks," *IEEE Transactions on Smart Grid*, pp. 1–1, 2025.