# A Software-Defined Networking Framework for Resilient Power Sharing in Multiple Microgrids with Hardware Implementation

Rawan A. Taha, Ahmed Aghmadi, Ahmed M. Ibrahim, Sara H. Moustafa, Student Member IEEE, and Osama A. Mohammed, Fellow IEEE

Energy Systems Research Laboratory
Florida International University
Miami, FL 33174, USA
rtaha003@fiu.edu, aaghm001@fiu.edu, aibra030@fiu.edu, smost017@fiu.edu, mohammed@fiu.edu

*Abstract*— **Cyber-physical power systems (CPPS) are reshaping electric power infrastructures by tightly coupling measuring, communication, and control with physical energy networks. Therefore, interconnected microgrid communication is pivotal, as the timely and reliable exchange of state and control signals enables selective, rapid power sharing across networked DC microgrids, reducing over-provisioning while maintaining reliability and resilience under rapid disturbances. This paper proposes a CPPS framework that integrates Software-Defined Networking (SDN) to manage flows, enforce priorities, and harden security. The SDN controller programs deterministic paths for protection and supervisory control, while a deny-by-default policy and rapid failover protect against unauthorized flows and link faults. The need for such co-design is most acute under critical pulsed load injection, which imposes steep current and voltage transients. The framework is experimentally validated on a hardware testbed of interconnected DC microgrids, demonstrating secure power sharing and maintained bus-voltage regulation under aggressive transients.**

***Index Terms-- Cyber-Physical Power Systems (CPPS), Software-Defined Networking (SDN), Networked Multi-microgrids, Pulsed load Injection, Secure Power Sharing.***

## I. Introduction

Cyber-Physical Power Systems (CPPS) emerged as electric grids grew more distributed, dynamic, and data-driven. Traditional physical architectures—built around centralized generation and slow supervisory loops—struggle with the fast variability of renewables, bidirectional power flows, and the need for fine-grained coordination among distributed energy resources and storage [1]. By tightly integrating sensing, computation, and communication with power-electronic control, CPPS enables real-time situational awareness, adaptive control, and resilient operation across transmission, distribution, and microgrids. This shift enhances efficiency and stability while laying the foundation for scalable, modular architectures, in which local controllers coordinate globally through cyber links[2].

However, this shift places greater reliance on communication infrastructures and software control planes, which introduces new points of failure and chances for attack. A single link outage, controller fault, misconfiguration, or compromised endpoint can ripple into protection maloperations and poor coordination among microgrids [3]. To counter these risks, CPPS should be engineered with security and resilience as core properties to limit exposure of critical functions, define clear trust boundaries, enforce principled access to control interfaces, segment critical paths, and plan for graceful degradation and recovery. Combined with architectural redundancy and disciplined lifecycle practices, these measures help ensure that power systems and interconnected microgrids continue operating safely even when communication links fail or adversarial conditions arise [4].

Software-Defined Networking (SDN) provides a disciplined communication backbone for CPPS and microgrids by decoupling the control plane from the data plane and centralizing policy in a programmable controller [5]. Deterministic paths can be defined for protection, control, and telemetry, then enforced network-wide with precise flow rules. Critically, SDN supports a "deny-by-default" feature where a whitelist of explicitly authorized protocols, message types, and endpoints is installed in the switches, and all other traffic is dropped. This enables the network to admit only the packets required for grid functions while blocking unsolicited, misrouted traffic or attack signals [6].

Several studies have investigated the potential of SDN using simulation-based architectures and frameworks. The authors in [7] build an SDN resiliency platform entirely on virtual machines. OpenStack hosts the controller and Open vSwitch software switches, and the study compares normal, failure, and upgraded topologies. Rerouting and monitoring are complete within a few to tens of milliseconds. The work is VM-based and does not involve physical switches or power hardware.

The work presented in [8] proposes a cross-domain SDN architecture for microgrids and details a reinforcement–

This work was partially supported by NSF IUCRC and the Office of Naval Research. The authors are with the Energy Systems Research Laboratory, Florida International University, Miami, FL 33174, USA. (Corresponding author: Osama A. Mohammed, mohammed@fiu.edu)

979-8-3315-8138-1

learning–assisted control workflow that probes latency, updates paths, and learns from historical behavior. The emphasis is on the algorithm and platform concept. No physical power-hardware implementation is described, so the contribution should be viewed as a conceptual and methodological step pending hardware validation.

In [9], the authors propose an SDN design for utility communications that introduces a Prediction-based Switch Virtualization and Distribution (PSVD) scheme to balance controller load. It builds a controller-load model from CPU, memory, and traffic metrics, applies SVD-based forecasting to anticipate overload, and triggers switch migration once thresholds are exceeded. Evaluation utilizes software simulation on a lab computer, incorporating one year of operational data, a reporting controller, and processing metrics, resulting in substantial post-migration gains. However, no physical SDN switches or field hardware are tested.

The authors in [10] develop an SDN-enabled model for an interconnected multi-microgrid (IMMG) arranged in a mesh topology. It introduces an Energy Sharing Factor (ESF) to govern fair, autonomy-preserving exchanges; defines SDN application-plane modules for data collection, ESF calculation, and optimization; and formulates coupled optimization problems at two layers—the individual microgrid (MG) and the IMMG—to determine ESF values, MG class priorities, and the time-indexed sharing plan. Evaluation is purely computational: the study reports optimization outcomes and cost metrics from dataset-driven simulations, without physical microgrid hardware or real SDN switches.

Finally, the work presented in [11] implemented a co-simulation testbed. The electrical microgrid and control logic run in MATLAB/Simulink, while the communication network—OpenFlow switches with an OpenDaylight controller packaged in Docker—runs in GNS3. Synchronization occurs over UDP. Compared with OSPF, SDN converges faster and drops fewer packets. Validation targets a modified IEEE 5-bus system. The study remains a software co-simulation without physical power equipment or hardware switches.

Across these studies, the benefits of SDN for grid communications and microgrid coordination are primarily demonstrated in software. Evidence is derived from virtualized platforms utilizing OpenStack and Open vSwitch, emulated networks in Mininet or GNS3, and power-system models in MATLAB/Simulink. The key gap remains experimental evidence of SDN-based control in Operational Technology (OT) cyber-physical systems.

The main contribution of this work is a comprehensive cyber-physical hardware implementation that mirrors industrial practice, where the physical layer comprises interconnected DC microgrids with converters, storage, and pulsed load profiles. Moreover, the cyber layer is built on programmable SDN switches enforcing policy at the data plane. This integration demonstrates end-to-end secure power sharing, validating deterministic paths and whitelist-based forwarding during disturbances. The platform provides evidence of operational resilience that bridges the gap between emulated testbeds and utility-grade deployments.

## II. Proposed System Architecture

The proposed system adopts a three-layer architecture, as depicted in Figure 1. The physical layer comprises three DC microgrids, each with a distinct source: a PV emulator and a battery interfaced through DC–DC converters, and a wind emulator interfaced through an AC–DC converter. Each source is governed by a dedicated microcontroller that regulates voltage and coordinates local operation at its microgrid bus. An external pulsed load is tied to the DC bus at the point of common coupling to impose high-dynamics disturbances for evaluation. Above this, the SDN-based cyber layer interconnects the microgrids with the control layer by forwarding time-critical measurements and control commands while ingesting flow tables from the SDN controller to program the switches. These flow rules enforce a whitelist policy that permits only authorized protocols and packet types, applying default-deny handling to drop all other traffic for security purposes. The control layer hosts the multi-microgrid control center for supervisory functions and the SDN controller for centralized network management and rapid reconfiguration.

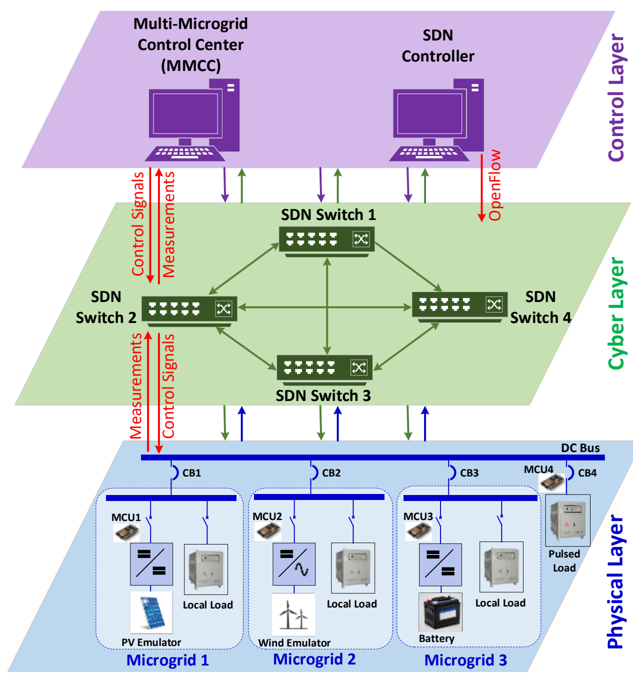



Figure 1. Proposed System Architecture

### A. *Physical Layer*

In the physical layer, Microgrid 1 (MG1) is energized by a programmable PV emulator whose output is governed by the single-diode model in (1) to replicate a solar module's I–V and P–V behavior [12],

$$I = I_{ph} - I_o\left[\exp\left(\frac{V + IR_s}{aV_t}\right) - 1\right] - \frac{V + IR_s}{R_{sh}} \qquad (1)$$

Where $I$ is the module current, $I_{ph}$ represents photocurrent, $I_o$ is the diode saturation current, $V_t$ is the thermal voltage, while $Rs$ and $Rsh$ model resistive losses. The emulator continuously updates these parameters so the terminal point voltage and current remain on the prescribed PV profile. A microcontroller executes the control loops, featuring fast inner voltage and current regulation, as well as an outer curve-enforcement loop that adjusts the DC–DC interface to maintain the microgrid bus at the commanded operating point.

Microgrid 2 (MG2) is supplied by a programmable wind emulator that reproduces the turbine–generator electromechanical behavior from a commanded wind profile using the standard model in (2) and (3),

$$P_{mech} = \frac{1}{2}\rho A C_p(\beta,\lambda) v_\omega^3 \tag{2}$$

$$\lambda = \frac{\omega_r R}{v_\omega} \tag{3}$$

Where $\rho$ is the air density, $A$ is the rotor swept area, $C_p$ is the power coefficient, which is a function of the tip-speed ratio $\lambda$ and blade pitch angle $\beta$, and $v_\omega$ is the wind speed. The emulator computes the torque reference in real time, based on the measured shaft speed and the imposed wind speed, ensuring the operating point follows the turbine's torque–speed characteristic across cut-in to rated conditions. A dedicated microcontroller executes the control loops that translate the torque reference into drive commands for the prime mover and regulates the generator interface, which is rectified through an AC–DC stage to the DC bus of MG2 [13].

Furthermore, Microgrid 3 (MG3) employs a battery energy storage system interfaced through a DC–DC converter. The converter's supervisory logic compares real-time demand against the aggregated available capacity of the PV and wind sources. When demand exceeds this capacity, the battery discharges to support the DC bus. Conversely, when surplus power is present in MG1 and MG2, the battery charges to absorb the excess. State-of-charge (SoC) limits, current and voltage protections, and inner current/voltage control loops regulate charge–discharge transitions to maintain bus stability and ensure reliable operation across load and generation variations [14]. The battery voltage model can be represented as in (4),

$$V_{bat}(t) = E_0 - k\frac{Q}{Q - \int_0^t i\,dt} + A\exp\left(-B\int_0^t i\,dt\right) \tag{4}$$

Where $E_0$ is the constant open-circuit voltage, $k$ denotes the polarization voltage, $Q$ is the nominal capacity, $A$ is the amplitude of the exponential region, $B$ is the inverse time constant of that exponential term, and $i(t)$ is the battery current.

Finally, each microgrid includes a local variable resistive load whose power varies with its instantaneous resistance and bus voltage. In contrast, the external disturbance is a pulsed power load (PPL) that alternates between a minimum and maximum demand with a defined period and duty cycle. Its instantaneous power can be modeled as [15]

$$P_D(t) = P_{min} + \sum_{K=0}^{N-1}(P_{max} - P_{min})\begin{bmatrix}\delta(t-KT) - \\ \delta(T-(K+D)T)\end{bmatrix} \tag{5}$$

where $P_{min}$ and $P_{max}$ are the minimum and maximum power levels, $T$ is the pulse period, $D$ is the duty cycle, $N$ is the number of pulses, and $\delta$ denotes the unit step function.

*B. Cyber Layer*

The SDN-based cyber layer interconnects all microgrid assets through a mesh of programmable SDN switches, providing path diversity and fault tolerance against link failures. Each device in the physical layer is hardwired to the switches via dedicated Ethernet links and assigned a unique IPv4 address. The SDN controller configures the data plane by installing flow entries that specify source and destination endpoints, required protocols, and permitted ports for each communication pattern, such as supervisory commands from the MMCC to the MCUs and measurement streams returning to the control layer.

These controller-defined flows implement a strict whitelist: only approved traffic is forwarded, while all other packets are blocked by default to enforce security. Figure 2 shows the resulting topology as rendered in the controller software. Communication relies on HTTP over TCP/IP to access source and MCU web interfaces and to transmit control commands from the MMCC to the field devices. A network analyzer is integrated into the fabric to monitor packet paths, throughput, and loss, ensuring continuous visibility into cyber-layer performance.

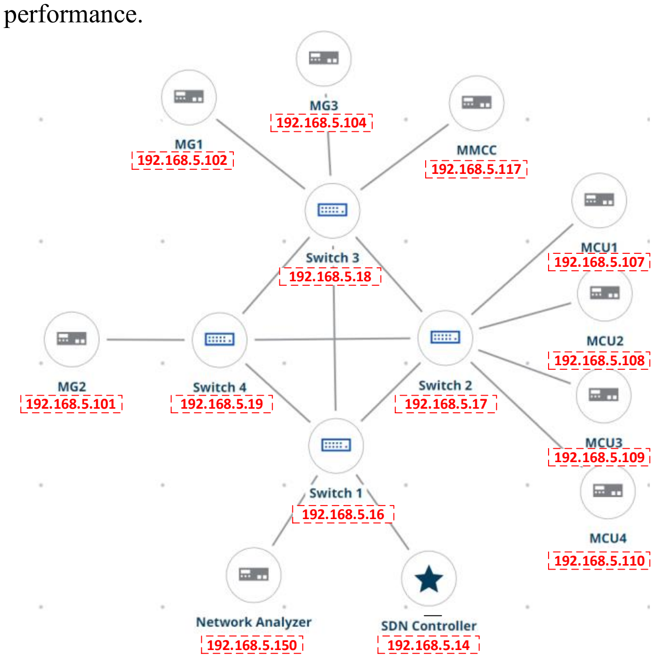


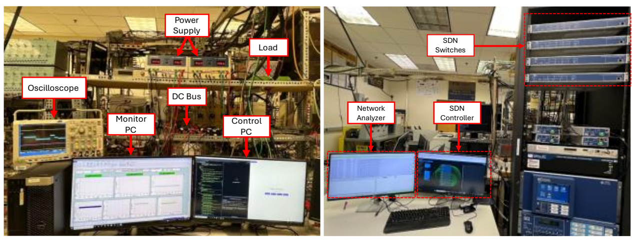

Figure 2. Network Management Topology for the Cyber Layer

*C. Control Layer*

The Multi-Microgrid Central Control (MMCC) is the supervisory layer that coordinates energy exchange and ensures system stability across interconnected microgrids. It continually collects real-time data from each microgrid, including voltage, current, generation, and state of charge (SOC), through the communication network described above. Based on this data, the MMCC utilizes optimization algorithms to balance supply and demand, schedule power flows, and mitigate disturbances such as load transients and renewable intermittency. In the event of a local imbalance or communication failure, it sends corrective commands to redistribute power. The MMCC thus ensures uninterrupted communication among decentralized controllers, enhances overall system robustness, and enables the optimal exploitation of distributed energy resources.

## III. Experimental Setup

This work focuses on the operational layer of a standalone DC microgrid and its SDN-enabled communication infrastructure. Electrical waveforms were captured using a high-speed digital oscilloscope under the control desk interface, as shown in Figure 3(a). Meanwhile, packet-level traffic was recorded in real-time using Wireshark on a dedicated network analyzer, as illustrated in Figure 3(b). By time-aligning these measurements, the setup tightly correlates power-system dynamics with network performance, empirically demonstrating how centralized SDN orchestration improves resilience, reliability, and responsiveness in DC microgrid operations. The parameters of the proposed DC networked multi-microgrid system are summarized in Table I.



(a) (b)

Figure 3. Proposed System Hardware Setup. (a) Physical Hardware Configuration, (b) SDN Communication Hardware Configuration

TABLE I. Proposed DC microgrid system ratings.

| Parameter | Value |
|---|---|
| DC Bus Rated Voltage | 60 V |
| Pulsed Load Power | 1-2.5 kW |
| **Microgrid 1** | |
| PV Emulator Power | 5 kW |
| Local Load 1 | 360-720 W |
| **Microgrid 2** | |
| Wind Emulator Power | 5 kW |
| Local Load 2 | 50-380 W |
| **Microgrid 3** | |
| Battery Rating | 12V, 100 Ah |
| Local Load 3 | 110-230 W |

## IV. Results and Discussion

### *A. Scenario 1: Normal Operation*

Scenario 1 depicts the MMG system's coordinated operation under SDN-based control. The SDN layer allows the central controller shown in Fig. 3.(a) to send generation and load setpoint commands to the local controllers, which then change the output of each microgrid as depicted in Fig. 9. In Case 1, MG3's local load drops, causing MG1 to cut its output proportionately, but MG2 remains relatively constant. In Case 2, MG2's generation is decreased to 35% of its initial capacity, and MG1 compensates by increasing its output. A further reduction in MG1's load setpoint reduces its production while maintaining MG2 at the reduced level. In Case 3, MG2's local load is reduced, bringing its net power closer to zero and driving MG1's supply to fall accordingly; meanwhile, MG3 maintains its nominal consumption.

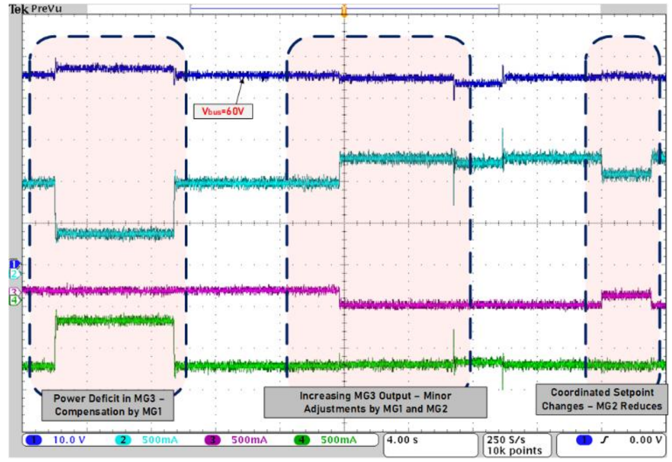



Figure. 4. DC Bus & MGs Power Sharing - Scenario 1

### *B. Scenario 2: Pulsed Load Injection*

Scenario 2 examines the MMG system's response to a series of pulsed-load steps applied to the common bus via the SDN layer, with each pulse occurring every 5 seconds. The oscilloscope recordings of the DC-bus voltage and microgrid power show the transient behavior induced by each load injection and removal. It is noted that MG3 does not share much power because the local controller prioritizes tasks to supply its local load first, while MG2 supplies more than 80% of the power due to the extra energy. These findings demonstrate that the SDN communication layer reliably coordinates rapid load changes with the microgrids' power dynamics, allowing for accurate, real-time control of pulsed load events.

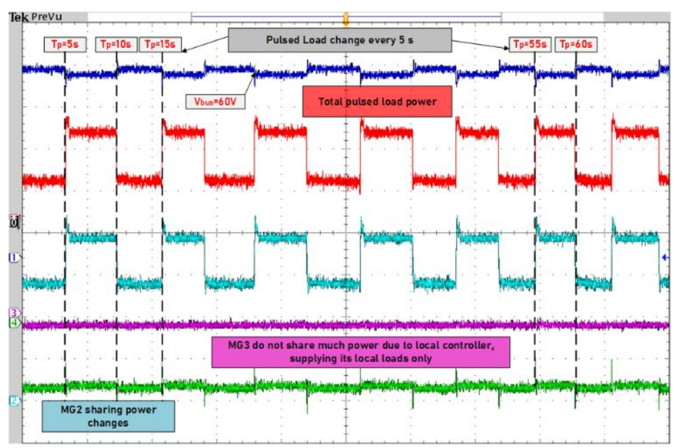



Figure. 5. DC Bus & MGs Power Sharing - Scenario 2

Figure 6 shows the decrypted packet captures, which depict control exchanges between the central controller and the local controllers. The research reveals a consistent sequence of request-acknowledgement transactions with no latency buildup. During load-step events, packet frequency dramatically increases, coinciding with reported surges in bus current. The strong correlation between communication timestamps and electrical responses supports the SDN layer's reliable and deterministic performance, ensuring effective real-time coordination. Overall, our findings show that the SDN-

979-8-3315-8138-1

based control infrastructure maintains timing precision and communication dependability during rapid, pulsed-load operations.

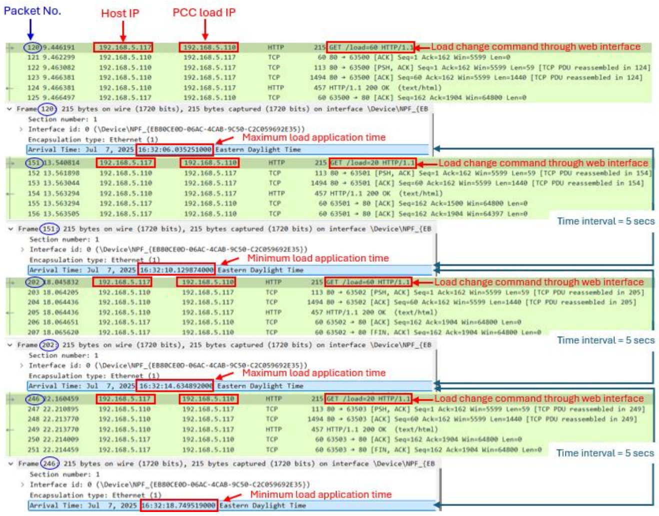



Figure. 6. SDN-based packet communication during pulsed-load events

## V. CONCLUSION

In conclusion, this experimentally implemented cyber-physical framework for networked DC microgrids demonstrates that integrating Software-Defined Networking as the communication layer establishes a robust cyber plane with deterministic, controller-programmed flows, deny-by-default protection against undefined traffic, and rapid, reliable messaging during critical pulsed-load events; collectively, these features enable secure power sharing and sustained bus-voltage regulation under steep transients, validating the proposed co-design for resilient, responsive multi-microgrid operation.

## ACKNOWLEDGMENT

The authors acknowledge the support of the Schweitzer Engineering Laboratories (SEL) for the technical discussions and for providing the needed SDN hardware.

## REFERENCES

[1] R. Arghandeh, A. Von Meier, L. Mehrmanesh, and L. Mili, "On the definition of cyber-physical resilience in power systems," *Renewable and Sustainable Energy Reviews*, vol. 58, pp. 1060–1069, May 2016, doi: 10.1016/J.RSER.2015.12.193.

[2] K. Zhang, Y. Shi, S. Karnouskos, T. Sauter, H. Fang, and A. W. Colombo, "Advancements in Industrial Cyber-Physical Systems: An Overview and Perspectives," Jan. 01, 2023, *IEEE Computer Society*. doi: 10.1109/TII.2022.3199481.

[3] J. P. A. Yaacoub, O. Salman, H. N. Noura, N. Kaaniche, A. Chehab, and M. Malli, "Cyber-physical systems security: Limitations, issues and future trends," *Microprocess Microsyst*, vol. 77, Sep. 2020, doi: 10.1016/j.micpro.2020.103201.

[4] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-Physical Systems Security - A Survey," *IEEE Internet Things J*, vol. 4, no. 6, pp. 1802–1831, Dec. 2017, doi: 10.1109/JIOT.2017.2703172.

[5] M. Priyadarsini and P. Bera, "Software defined networking architecture, traffic management, security, and placement: A survey," *Computer Networks*, vol. 192, p. 108047, Jun. 2021, doi: 10.1016/J.COMNET.2021.108047.

[6] Y. Maleh, Y. Qasmaoui, K. El Gholami, Y. Sadqi, and S. Mounir, "A comprehensive survey on SDN security: threats, mitigations, and future directions," *J Reliab Intell Environ*, vol. 9, no. 2, pp. 201–239, Jun. 2023, doi: 10.1007/S40860-022-00171-8/FIGURES/12.

[7] S. Al-Rubaye, E. Kadhum, Q. Ni, and A. Anpalagan, "Industrial Internet of Things Driven by SDN Platform for Smart Grid Resiliency," *IEEE Internet Things J*, vol. 6, no. 1, pp. 267–277, Feb. 2019, doi: 10.1109/JIOT.2017.2734903.

[8] J. Dai, Z. Dai, and V. L. L. 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, Mar. 2025, doi: 10.1109/ticps. 2025.3548006.

[9] J. Song, Y. Zhang, and Q. Wang, "Research on Power Communication Data Network System and Key Technologies Based on SDN Architecture," in *Proceedings of 2022 IEEE 4th International Conference on Civil Aviation Safety and Information Technology, ICCASIT 2022*, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 850–855. doi: 10.1109/ICCASIT55263.2022.9987022.

[10] R. H. M. Zargar and M. H. Yaghmaee, "Energy exchange cooperative model in SDN-based interconnected multi-microgrids," *Sustainable Energy, Grids and Networks*, vol. 27, Sep. 2021, doi: 10.1016/j.segan.2021.100491.

[11] R. E. Perez Guzman, M. Rivera, P. W. Wheeler, G. Mirzaeva, E. E. Espinosa, and J. A. Rohten, "Microgrid Power Sharing Framework for Software Defined Networking and Cybersecurity Analysis," *IEEE Access*, vol. 10, pp. 111389–111405, 2022, doi: 10.1109/ACCESS.2022.3215434.

[12] A. Aghmadi, H. Hussein, and O. A. Mohammed, "Enhancing Energy Management System for a Hybrid Wind Solar Battery Based Standalone Microgrid," *Proceedings - 2023 IEEE International Conference on Environment and Electrical Engineering and 2023 IEEE Industrial and Commercial Power Systems Europe, EEEIC / I and CPS Europe 2023*, 2023, doi: 10.1109/EEEIC/ICPSEUROPE57605.2023.10194769.

[13] S. Y. Lu, L. Wang, T. M. Lo, and A. V. Prokhorov, "Integration of Wind Power and Wave Power Generation Systems Using a DC Microgrid," *IEEE Trans Ind Appl*, vol. 51, no. 4, pp. 2753–2761, Jul. 2015, doi: 10.1109/TIA.2014.2367102.

[14] T. R. Oliveira, W. W. A. Gonçalves Silva, and P. F. Donoso-Garcia, "Distributed secondary level control for energy storage management in DC microgrids," *IEEE Trans Smart Grid*, vol. 8, no. 6, pp. 2597–2607, Nov. 2017, doi: 10.1109/TSG.2016.2531503.

[15] A. Aghmadi, O. Ali, and O. A. Mohammed, "Stability Enhancement of DC Microgrid Operation Involving Hybrid Energy Storage and Pulsed Loads," *IEEE Transactions on Consumer Electronics*, vol. 71, no. 2, pp. 3204–3217, 2025, doi: 10.1109/TCE.2025.3545309.