Cyber-Resilient Service Restoration of Grid-Connected Microgrids Using ESS-based Adaptive Grid-Forming Control

Hojun Yang, Dongjun Won

Department of Electrical and Computer Engineering, Inha University

Introduction

Digital substations (DSs) built on IEC 61850 process buses, merging units, and IEDs replace hard-wired signals with Ethernet networks. This improves observability and interoperability, but expands the cyber-physical attack surface: falsified sampled value (SV) measurements or manipulated GOOSE trip messages can force circuit-breaker (CB) operation with no physical fault present.

The risk is amplified as large-capacity loads such as data centers connect directly at the 22.9 kV substation level. These loads host thousands of power-electronic devices highly sensitive to voltage and frequency, so a single cyber disturbance can escalate into wide-area instability.

Prior work focuses on prevention (message authentication) and detection (data-driven IDS), but stops at anomaly recognition. This work adds a physical-layer resilience mechanism: an ESS-based hub substation (HS/S) with an adaptive grid-forming inverter that sustains voltage and frequency during cyber-induced contingencies.

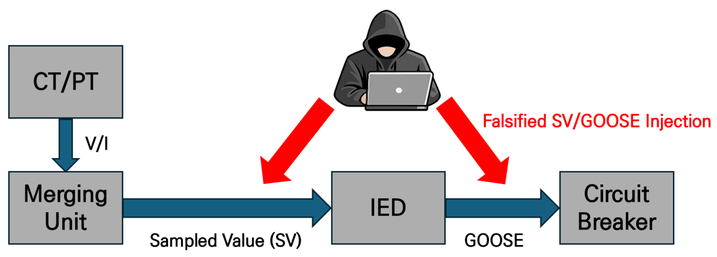


Fig 1. <SV and GOOSE Attack Structure>

Proposed Method

Cyber-Attack Model. IEC 61850 substations face two attack types: SV-based — falsified current samples make IEDs perceive a non-existent fault; and GOOSE-based — forged trip messages open CBs directly. Either path causes unintended breaker operation with no physical fault (Fig. 1).

Adaptive Grid-Forming Control. A GFMI blends a Power-Synchronization Loop (PSL) and a PLL; the phase angle θ is:

$$\theta = (1/s)[\, K_a\, G_{PSL}(s)(P^*-P) + (1-K_a)\, G_{PLL}(s)\, V_{pcc,q} + \omega_0 \,] \qquad (1)$$

A cascaded vector loop with virtual impedance feeds a PI d-q current controller:

$$V_d^* = V_{pcc,d} - \omega L_f\, I_q + (K_{pc} + K_{ic}/s)(I_d^* - I_d) \qquad (2)$$

Mode Switching. The adaptive coefficient K_a sets the operating mode:

$$K_a = 1 \ \text{(normal, PSL-dominant)} \quad | \quad K_a = 0 \ \text{(cyber-attack, PLL-dominant)} \qquad (3)$$

HS/S Restoration. An unstable grid is flagged by an IDS alarm or physical symptoms — unintended CB opening, sudden voltage sag, or large frequency deviation. The HS/S controller then sets $K_a = 0$, switching the ESS from P/Q to V/f control to establish local voltage/frequency references and restore supply within ~50 ms — without SCADA intervention.

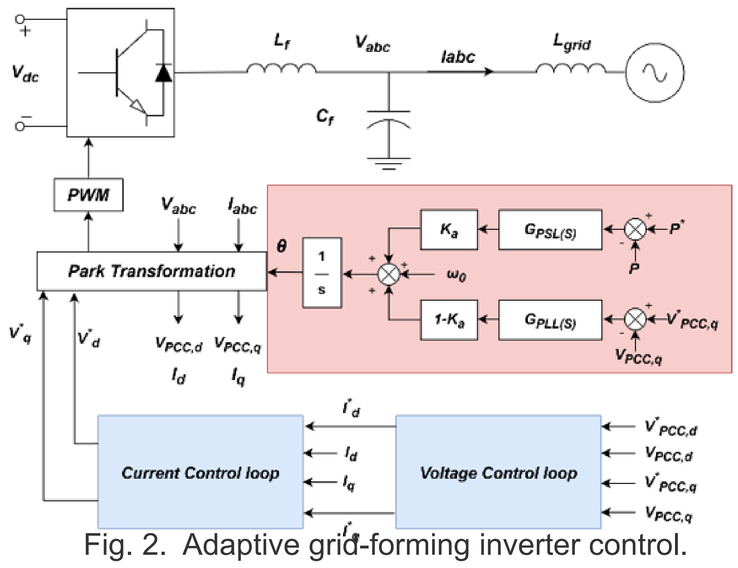


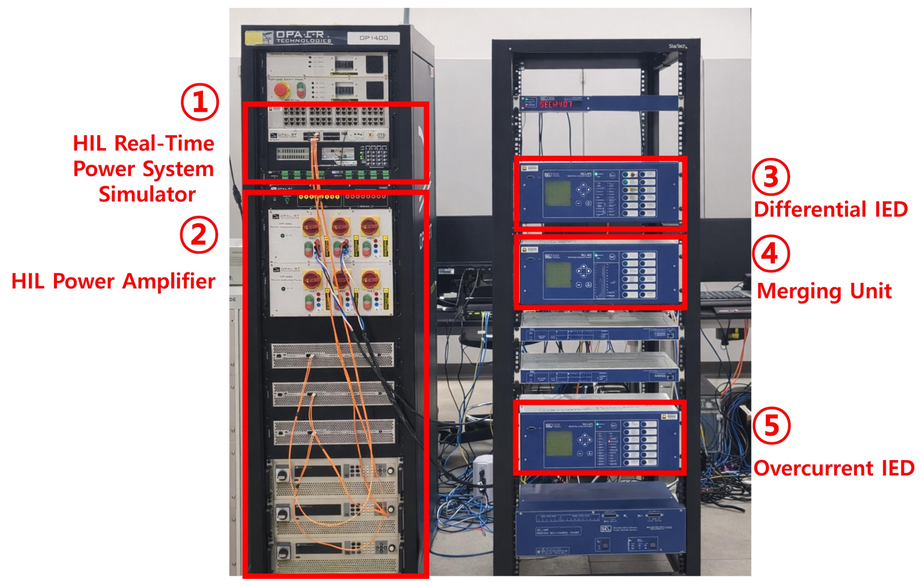
Fig. 2. Adaptive grid-forming inverter control.

Key Contributions

1. A physical recovery framework based on an ESS hub substation (HS/S) that sustains stable voltage and frequency during cyber-attacks — beyond communication-layer defenses.
2. An adaptive grid-forming inverter (GFMI) operating mode: a grid-connected ESS hub in normal operation that transitions to an independent voltage source — a recovery node — under attack.
3. A real-time OPAL-RT HILS testbed with actual IEC 61850 SV/GOOSE injection, validating the framework under realistic cyber-physical conditions.

Positioning: vs. prior prevention / detection work, this is the first Resilience · ESS-assisted · Physical-layer response.

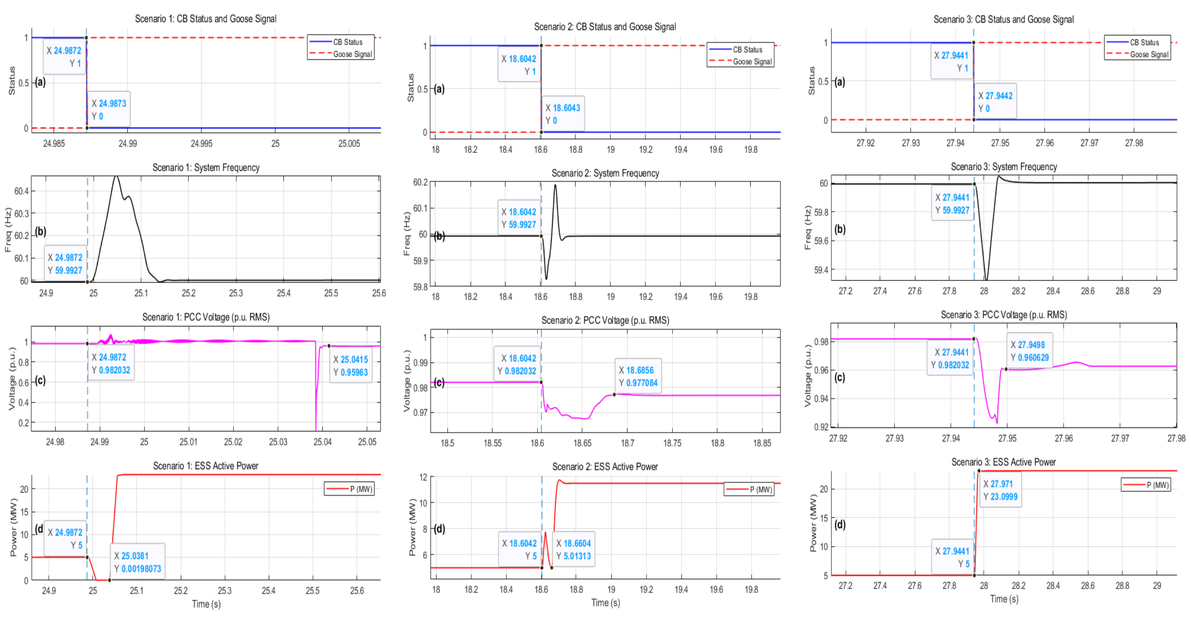
HILS Testbed & Setup



Closed-loop OPAL-RT real-time HILS with physical IEC 61850 SV / GOOSE injection:

- OPAL-RT simulator + power amplifier + merging unit + protection IEDs
- System: 154 / 22.9 kV digital substation, double-busbar
- ESS: 25 MW / 50 MWh via adaptive GFMI; P_{ref} = 5 MW
- Total load 24 MW; standby feeder closes in ≈ 50 ms

Case Study Results



Scenario 1 — Load-side CB

- Forged GOOSE trips load-side CB at t ≈ 24.99 s
- Frequency spikes to 60.4 Hz; PCC voltage dips to 0.2 p.u. during P/Q→V/f transition
- ESS ramps 5 → 24 MW, supplying the entire disconnected load; V & f restored in ≈ 50 ms

Scenario 2 — One substation

- Forged GOOSE opens one transformer-side CB at t ≈ 18.60 s
- Double-busbar keeps partial grid support; frequency 60 ± 0.2 Hz, voltage holds at 0.977 p.u.
- ESS provides partial 12 MW support — output scaled to contingency severity

Scenario 3 — Two substations

- Both transformer CBs trip → full upstream isolation at t ≈ 27.94 s
- Frequency drops to 59.4 Hz; voltage falls to 0.92 p.u., recovers to 0.96 p.u.
- ESS enters V/f mode at 23 MW, acting as the islanded grid-forming source

Conclusion

Cyber-induced CB malfunctions can cause voltage collapse and service interruption with no physical fault. The proposed ESS-based adaptive grid-forming framework restored stable voltage and frequency across all three attack scenarios.

- Severity depends on resulting network topology, not the attack type — SV and GOOSE manipulations yield identical CB patterns.
- By switching P/Q → V/f control, the ESS acts as a grid-forming source, restoring references within ~50 ms even under full substation isolation.
- Detection / communication-layer countermeasures alone are insufficient; physical-layer ESS support is essential.

Future Work: dynamically tune K_a between 0 and 1 from real-time grid conditions and disturbance severity for optimized synchronization damping and smoother restoration.

IPSL
Inha Univ. Power System Lab