Hardware-in-the-Loop Implementation of the Secure SDN-Based Digital Substation

Shayan Soltani[(a)], Mehrdad Kazemtabrizi[(b)], and Innocent Kamwa[(a)]
Department of Electrical and Computer Engineering
Laval University[(a)], OPAL-RT Technologies Inc. [(b)]
Quebec City[(a)], Montréal[(b)], Canada,
shayan.soltani.1@ulaval.ca, Mehrdad.Kazemtabrizi@opal-rt.com, innocent.kamwa@gel.ulaval.ca

***Abstract*—The move toward smart and automated substations is accelerating the use of digital protection and IEC 61850-based communication. While this enhances interoperability, it also raises challenges for ensuring dependable and secure protection in highly networked environments. This paper presents a real-time cyber-physical testbed for assessing protection schemes in digital substations under both normal and adversarial conditions. The platform couples an OPAL-RT real-time simulator with SEL protective relays and Ethernet switches in a hardware-in-the-loop (HIL) setup, with IEC 61850 communications and sub-microsecond time synchronization provided by IEEE 1588 and an SEL-2488 clock. A software-defined networking (SDN) layer is used to manage traffic flows and strengthen cybersecurity against man-in-the-middle attacks. The testbed offers a high-fidelity environment to evaluate the performance, dependability, and security of protection functions, and the experimental and simulation results confirm the effectiveness of the proposed framework.**

Keywords—cyber-physical systems, digital substations, IEC 61850, protective relays, software-defined network.

I. INTRODUCTION

Substations play a crucial role in the power grid by allowing operators to monitor, manage, and ensure the safe distribution of electricity. Before 1960, control systems relied on large, hardwired relay panels, which were both expensive and susceptible to faults. This changed in the 1960s with the advent of Programmable Logic Controllers (PLCs), which replaced relay systems, significantly reducing costs and streamlining maintenance. In the 1970s, Supervisory Control and Data Acquisition (SCADA) systems were introduced, enabling remote control and improving situational awareness through the use of serial communication protocols like Modbus and IEC101 [1].

Modern intelligent electronic devices (IEDs) in substations provide extensive communication capabilities and require detailed configuration prior to deployment. Since protection systems often rely on coordination between multiple relays and communication channels, real-time testing that links physical devices with simulated power system models has become an effective method for validating relay performance and protection settings [2], [3].

In microgrids, protection strategies may rely on local measurements, digital communication networks, or external intelligent devices. One of the major challenges is creating a protection system that can dynamically coordinate cyber and physical layers as the operational state of the microgrid changes. Several co-simulation frameworks have been proposed to address this by combining power system models with communication networks. For instance, in [4], a hybrid simulation using Simulink and OMNeT++ was introduced to study interactions between electrical behavior and communication delays. In [5], Celli et al. linked OpenDDS with the NS-2 network simulator. Another study [6] utilized MATLAB SimPowerSystems and SimEvents to emulate IEC 61850-based low-voltage grids. Although these works provide valuable insight into cyber–physical integration, they mostly rely on software-based simulations and do not operate over actual communication hardware.

To address the need for practical solutions, Liao et al. [7] proposed a protection system that adapts relay settings based on real-time communication data and changing microgrid configurations. Their method utilizes digital directional relays equipped with interlocking logic to enable selective tripping. Other works [8], [9] proposed centralized protection schemes in which a supervisory controller communicates with distributed relays to modify protection characteristics according to generation and load conditions. In contrast, Han et al. [10] analyzed fault current behavior in inverter-based microgrids and developed an adaptive impedance-based method that adjusts relay settings using real-time voltage and current data in both grid-connected and islanded modes. Mahat et al. [11] showed that bidirectional power flow in inverter-dominated microgrids can lead to protection miscoordination and relay maloperation. They suggested a centralized communication-assisted system combined with Thevenin equivalent impedance estimation to detect faults and trigger the appropriate relays. Similarly, Khederzadeh [12] implemented numerical relays capable of automatically switching relay settings depending on whether the microgrid is connected to the main grid or operating in islanded mode. Li et al. [13] incorporated an energy storage unit interfaced through a DC/DC converter to stabilize voltage and improve relay sensitivity during faults; however, this method increases system cost due to limited usage of storage during normal operation. In another approach [14], authors relied on voltage disturbances detected by local modules to determine fault location and isolate the faulted section, though their system faced challenges related to detection speed and accuracy, which could affect selectivity. Table I summarizes the previous works and demonstrates their limitations.

The main contributions of this work can be summarized as follows:

- The proposed substation automation system enables secure, dependable fault detection, and minimize the load disconnection after faults. The method can speeds up of the isolation of the fault in circuit breaker failure condition, as well.
- Real-time cyber–physical protection testbed: A closed-loop hardware-in-the-loop platform is developed that couples an OPAL-RT real-time simulated substation with SEL protective relays to evaluate protection performance in IEC 61850-based digital substations.

979-8-3315-8138-1

TABLE I. COMPARISON PREVIOUS WORKS

Ref.	Contribution	Approach	Limitation
[4]	Cyber-physical system with communication delays	Simulink + OMNeT++ co-simulation	No real hardware or IEC 61850 implementation
[5]	Cyber layer integration via middleware	OpenDDS + NS-2	Purely software-based
[6]	IEC 61850 modeling in LV networks	SimPowerSystems + SimEvents	Lacks real-time relay interaction
[7]	Adaptive protection using relay communication layers	Digital directional relays + interlocking	Requires complex settings update
[8]	Central modifies relay settings via communication	Control center + distributed relays	Single-point-of-failure
[10]	Adaptive protection using real-time estimation	V–I measurements, grid/island modes	Dependent on accurate measurements
[11]	Coordination issues due to bidirectional power flow	Thevenin impedance + centralized	Communication delay risk
[12]	Self-adjusting relay settings for different modes	Numerical relays with offline settings	No real-time relay learning
[13]	Energy storage to aid protection during faults	DC/DC interfaced ESS	High cost, low use in normal state
[14]	Voltage-based fault detection and isolation	Local fault modules	Sensitive to measurement errors

- Implementation of standardized digital communication and time synchronization: IEC 61850 GOOSE and Sampled Values are configured between the simulator and physical IEDs, while IEEE 1588 and IRIG-B time protocols ensure sub-microsecond synchronization across all devices.
- Practical relay configuration for digital substations: A complete setup procedure is provided for integrating SEL relays into the digital testbed, including dataset creation, publishing/subscribing of GOOSE/SV messages, and mapping logical nodes based on IEC 61850 requirements.
- Show the role of SDN switches in the securing digital substation, rather than "plug and play" switches.
- Validation of protection reliability under different scenarios.

II. CYBER-PHISICAL FRAMEWORK

The following section explains the main components of the proposed framework in digital substation. The suggested hardware configuration can be shown in Fig. 1.

A. Real-time Simulator

The OP4510 real-time simulator from OPAL-RT is designed for electromagnetic transient studies and hardware-in-the-loop applications. It uses a multi-core Intel processor to solve power system and control system equations in real time using the RT-LAB/Hypersim environment. All processor cores are placed on a single board, allowing fast communication between tasks such as network calculations, control algorithms, and I/O processing. The simulator also includes built-in analog and digital I/O and support for IEC 61850, making it suitable for testing protection systems with real devices. In this work, five processing cores of the OP4510 are used to run the digital substation model and interface with SEL relays.

B. SEL-2488 Satellite-Synchronized Network Clock

The SEL-2488 is a satellite-synchronized clock designed for precise time distribution in digital substations. It supports IEEE 1588 Precision Time Protocol (PTP), allowing sub-microsecond synchronization over Ethernet networks. In a PTP system, the SEL-2488 operates as a master or grandmaster clock, providing the reference time to all other slave devices in the domain. It cannot function as a PTP slave. The device supports multiple PTP profiles. It can operate over Layer 2 (Ethernet/802.3) or Layer 3 using UDP. For power system applications, it includes the IEEE C37.238 Power Profile, which enforces Layer 2 communication and fixes most timing parameters to ensure interoperability and deterministic behavior. For delay compensation, the clock uses the peer-to-peer (P2P) path delay mechanism as required in the Power Profile. This method allows each device to measure the delay to its directly connected neighbor, improving timing accuracy across the network.

C. SEL-411L Relay

The SEL-411L is an advanced protection relay designed primarily for multi-terminal transmission lines and pilot protection schemes. It supports high-speed current differential protection, single- and three-pole tripping, auto-reclosing, and breaker failure protection. The relay also includes built-in synchrophasor measurement, high-resolution event recording, and fault location capabilities. In digital substation applications, the SEL-411L can receive IEC 61850-9-2 Sampled Values (SV) from merging units and exchange GOOSE messages for inter-relay communication. This allows it to operate without conventional CT/VT wiring and enables distributed protection across wide-area networks. The relay can be synchronized via IRIG-B or PTP to ensure accurate time-alignment of sampled currents and voltages during fault analysis and differential protection.

D. SEL-487E Relay

The SEL-487E is a multifunction protection and control relay intended for transformers, feeders, and busbar applications. It provides differential protection, overcurrent backup, breaker failure logic, and detailed fault reporting. Its high-accuracy metering, waveform recording, and synchrophasor data make it suitable for disturbance analysis and real-time system monitoring. In IEC 61850-based digital substations, the SEL-487E is capable of receiving SV messages over Ethernet rather than through copper-wired CTs and VTs. It also supports GOOSE messaging for fast tripping and interlocking between relays. Time synchronization is achieved via IRIG-B or IEEE 1588, ensuring precise alignment of sampled values, oscillography, and disturbance reports. This makes the relay fully compatible with process bus architectures and modern HIL/co-simulation platforms.

E. SEL-2740S / SEL-2741 SDN Switches

The SEL-2740s and SEL-2741 are SDN switches designed specifically for digital substations and time-critical power system applications. Unlike conventional Ethernet switches, they enable deterministic, real-time communication by allowing engineers to define explicit data paths and prioritize protection and control traffic. Both switches support IEC 61850 GOOSE and SV messages and are fully compatible with process bus architectures. They provide nanosecond-level time synchronization through IEEE 1588 PTP and IRIG-B inputs, making them suitable for synchronizing protection IEDs, merging units, and real-time simulators such as OPAL-RT or RTDS. The SEL-

2740S offers higher port density and is typically used in control rooms or substation cabinets, while the SEL-2741 provides a compact form factor for installation directly in field panels or process-level environments. Through centralized SDN controllers, these switches enable secure traffic engineering, cyberattack isolation, and guaranteed forwarding of critical messages such as GOOSE trips or SV streams, even under network congestion or cyber-physical attacks.

III. Designing the Experimental Framework for Cyber-Attack Analysis against Protective Relays

In this section, a typical substation is introduced and developed for testing and evaluating IEC 61850 protocol and the cyber layer of the digital substation. Fig. 1. demonstrates the integration of the typical digital substation based on IEC 61850 that simulated in HYPERSIM. The substation used for this purpose is based on an example developed during the 2019 Interoperability (IOP) conference, and further details about the substation's origin can be accessed in [15].

The substation consists of a comprehensive structure featuring two voltage levels, 230 kV and 14.4 kV, supported by two power transformers. It includes three busbars: a 230 kV BUS at the 230 kV voltage level, a Transfer BUS XF, and 14.4 kV BUS A and BUS B. The substation is organized into twelve bays, divided between the two voltage levels. At 230 kV, the bays include L1 and L2 for lines, BP for busbar protection, and TXA and TXB for transformer protection. At 14.4 kV, the bays comprise IncA and IncB (incoming), BT (tie breaker), XF (busbar XF protection), and feeders A1, A2, B1, and B2 connected to 14.4 kV BUS A and BUS B. Additionally, multiple IEDs are deployed across the bays to manage protection unit (PU), bay control unit (BCU), or both (PUBCU) depending on their type. Merging units (MU) are situated at the process level to digitize current and voltage values from instrument devices and transmit these as sampled values to the bay units.

In the HYPERSIM model, only three bays and their respective IEDs are involved in the designed scenarios, all located on the low voltage (LV) side of the substation at 14.4 kV. HYPERSIM components are utilized to develop the internal protection logic and IEC 61850 communication sections of the IEDs, which are organized as sub-circuits. The Target I/O interface component block is used to simulate a merging unit and for general IEC 61850 data mapping to component sensors. Each piece of equipment is named to represent the name of its respective bay, such as CT1_INCA and CB_INCA. Three-phase breakers are used for circuit breakers, and three-phase current probes represent current transformers. The 14.4 kV busbars are named BUS_A, BUS_B, and TRANSFER_XF. All logical node names used in this work follow the naming conventions defined in IEC 61850-7-4.

In the digital model, three logical protection IEDs are associated with the LV bays IncA, IncB and BT. For the HIL experiments, these IEDs are implemented using a SEL-487E assigned to the BT bay and an SEL-411L that is configured as the incomer relay for either IncA or IncB, depending on the scenario. The phase currents and breaker status signals of the three bays are exported from HYPERSIM through the Target I/O interface, grouped into IEC 61850-9-2LE sampled-value datasets and GOOSE

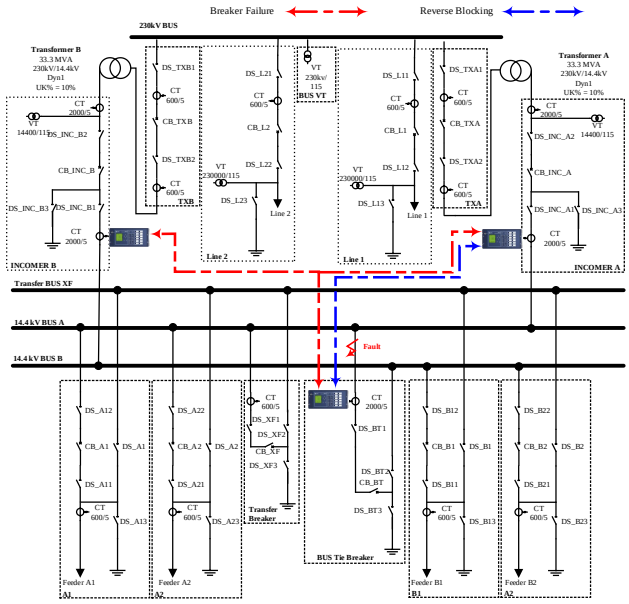

Fig. 1. Single-line-diagram of the modeled substation

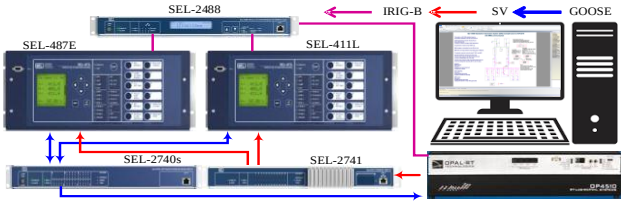

Fig. 2. OPAL/SEL HIL designed setup

control blocks, and published by the OP4510 to the process-level SDN switch. The SV streams are then subscribed to by both the BT relay and the active incomer relay, ensuring that they see a consistent view of the 14.4-kV network, while GOOSE messages from the BT relay provide reverse-blocking and breaker-failure indications that are mapped to the corresponding blocking and tripping inputs of the IncA and IncB relays. This one-to-one mapping between the bays, the logical IEDs in HYPERSIM and the physical SEL relays allows the coordination logic used in the reverse-blocking and breaker-failure scenarios of Section IV to be reproduced faithfully in the HIL platform.

IV. Real-Time Validation & Discussion

To evaluate the performance of the proposed protection schemes in the prepared HIL setup (see Fig. 2), three operating scenarios are defined. Scenario 1 investigates the correct coordination between the bus-tie protection unit and the incomer relay under reverse-blocking conditions. Scenario 2 evaluates the breaker-failure logic of the bus-tie relay and the corresponding backup tripping provided by the incomer relay. Scenario 3 assesses the cyber-resiliency of the SDN-based communication network when an attacker injects spoofed SV and GOOSE messages, and verifies that the protection system continues to operate correctly under cyber-attack conditions. All the setting for overcurrent relays are modified based on [15]

A. *Scenario 1: Reverse Blocking (RB).*

In the hardware-in-the-loop setup, the 14.4 kV network is modeled in the OPAL-RT simulator, which publishes IEC 61850-9-2LE SV streams to a process-level SEL SDN switch. The SV streams are then routed and adapted to an

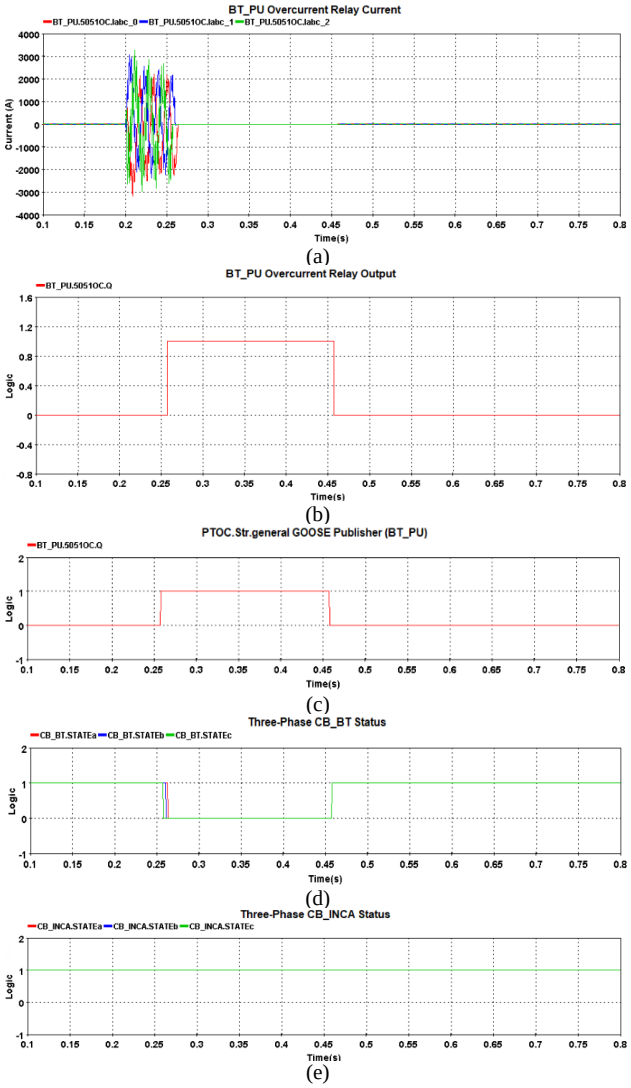

Fig. 3. HIL results for scenario 1, (a) current measurement waveforms, (b) the operation of SEL-487E, (c) published GOOSE messages from SEL-487E, (d) the status of the BT circuit breaker, (d) the status of the IncA circuit breaker.

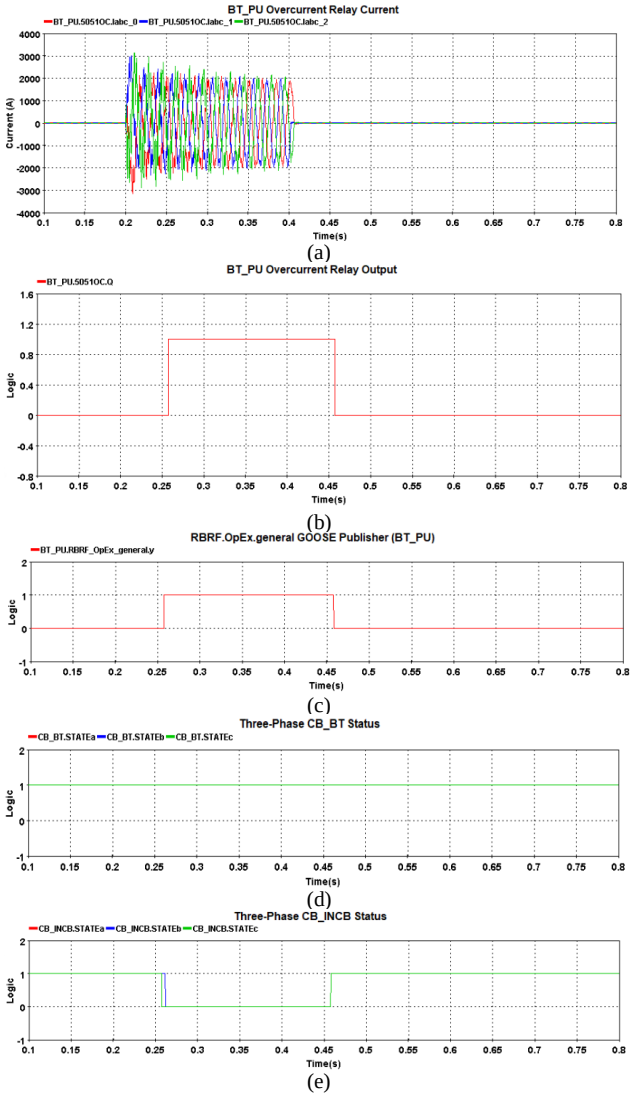

Fig. 4. HIL results for scenario 2, (a) current measurement waveforms, (b) the operation of SEL-487E, (c) published GOOSE messages from SEL-487E, (d) the status of the BT circuit breaker, (d) the status of the IncA circuit breaker.

SEL-487E configured as the tie-bay relay (BT) and an SEL-411L configured as the IncA. A three-phase fault is applied at the BT bay at t = 0.2 s and maintained for 200 ms. Both SEL relays measure the fault through the SV stream, but the SEL-487E is designated as the primary protection. After its intentional delay (≈0.05 s), the SEL-487E issues a trip to the tie breaker and publishes a reverse-blocking GOOSE message via a second SDN switch. This GOOSE is received by the SEL-411L, which asserts its blocking logic and inhibits tripping of the IncA breaker even though it sees the same fault current. Oscillography from the SEL-487E and SEL-411L, along with SV/GOOSE captures at the SEL SDN switches, confirm that the tie breaker opens while the incomer remains closed, demonstrating correct and fully selective operation of the reverse-blocking scheme with real devices, as shown in Fig. 3.

B. Scenario 2 – Breaker Failure (BF).

The same HIL platform is used to validate the breaker-failure scheme. The OPAL-RT simulator publishes IEC 61850-9-2LE sampled values (SV) to the first SEL SDN switch, which forwards them to the SEL-487E configured as the tie-bay relay (BT) and to an SEL-411L configured as the incomer relay at bay IncB. A three-phase fault is applied at the BT bay at t = 0.2 s. The SEL-487E detects the fault through the SV stream and issues a primary trip command according to its 0.05 s intentional delay. In this breaker-failure test, however, the tie breaker is forced to "fail," i.e., it does not open despite receiving the trip signal. The breaker-failure element in the SEL-487E then picks up and publishes a GOOSE message containing breaker failure signal via the second SEL SDN switch. The SEL-411L at IncB subscribes to this GOOSE, interprets it as a breaker-failure backup request, and trips its associated incomer breaker at around t = 0.25 s, thereby isolating the faulted section from the healthy busbar while the tie breaker remains closed, as shown in Fig. 4.. Event reports and GOOSE/SV captures confirm correct primary and backup operation without mis-trips.

C. Cyber Attack Condition

In IEC 61850-based substation OT networks, SDN enhances security and cyber-resilience by replacing "plug-and-play" Ethernet switching with centrally engineered, flow-based forwarding. In a conventional Layer-2 VLAN, switches rely on dynamic MAC learning, STP/RSTP, and

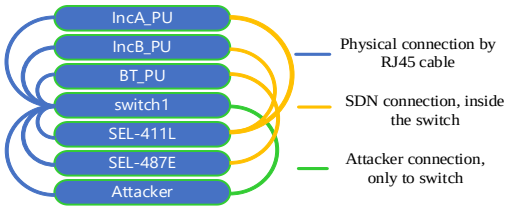

Fig. 5. Cyber-physical connection based on SDN switches

flooding of ARP/ICMP/multicast traffic, which leaves the network exposed to man-in-the-middle attacks and broadcast flooding. As a result, an adversary connecting to any open port in the same VLAN can inject forged GOOSE/SV frames that may trigger false trips or denial of service, since these messages are neither authenticated nor tightly constrained by the network. [16].

SDN replaces this "plug-and-play" model by separating the control and data planes and using an OpenFlow controller to pre-install whitelisted flow rules in each OT switch. These rules match on selected L1–L4 fields and explicitly define output ports, so the network operates in a deny-by-default mode where unsolicited ARP, spoofed multicast, or unknown DNP3 traffic is dropped at the first hop and GOOSE/SV streams are forwarded only to legitimate subscribers. SDN traffic engineering also enables hardware fast-failover groups, allowing switches to switch locally to backup paths within microseconds after a link failure, avoiding STP/RSTP re-convergence delays and maintaining protection performance [16].

To evaluate the behaviour of the SDN switches under cyber-attack conditions, the two previous scenarios are re-simulated in the presence of an attacker who has access to the switches and injects spoofed SV and GOOSE messages, following the attack model in [17]. As shown in Fig. 5, data flows between the attacker's port and the IEDs are not pre-configured in the SDN controller, the relays do not accept any of the spoofed GOOSE or SV messages. It is also worth noting that the attacker cannot manipulate the GOOSE messages received by the OP4510, because the corresponding traffic path between the attacker and the real-time simulator is likewise not defined.

V. Conclusion & Future Works

In this paper, a real-time cyber–physical testbed for IEC 61850-based digital substations was developed and experimentally validated using an OP4510 simulator, SEL-411L and SEL-487E protective relays, an SEL-2488 satellite clock, and SEL-2740S/2741 SDN switches. The platform faithfully reproduces the UCA international user **g**roup IOP2019 substation topology, implements GOOSE and sampled-value communication between the simulated process and physical IEDs, and achieves sub-microsecond time alignment through the IRIG-B synchronization protocol. Three representative scenarios were studied: reverse blocking between the bus-tie relay and the incomer, breaker-failure backup tripping, and a cyber-attack case in which an adversary injects spoofed GOOSE and SV frames into the OT network. The HIL results show that the proposed protection schemes operate selectively and dependably under normal and breaker-failure conditions, and that the SDN-based communication fabric successfully enforces a deny-by-default policy, blocking unauthorized traffic from the attacker and preserving correct fault-clearing behaviour. These findings confirm that SDN-enabled digital substations, when combined with realistic HIL validation, provide a practical path toward secure, interoperable, and testable protection systems. Future work will extend the framework to additional bays and protection functions, consider richer attack vectors (e.g., coordinated DoS and topology poisoning), and investigate the integration of cybersecurity guidelines from IEC 61850 and IEC 61850 and test the security of microgrid control and protection applications within the same HIL environment.

References

[1] J. C. Lozano, K. Koneru, N. Ortiz, and A. A. Cardenas, "Digital substations and iec 61850: A primer," *IEEE Communications Magazine*, vol. 61, no. 6, pp. 28-34, 2023.

[2] H. F. Habib, N. Fawzy, and S. Brahma, "Performance testing and assessment of protection scheme using real-time hardware-in-the-loop and IEC 61850 standard," *IEEE Transactions on Industry Applications*, vol. 57, no. 5, pp. 4569-4578, 2021.

[3] S. Li *et al.*, "Accelerated and Online Electromagnetic Transient Simulations: Key for Swift and Accurate Stability Analysis in Large-Scale Low-Inertia Power Systems," *IEEE Power and Energy Magazine*, vol. 22, no. 2, pp. 110-118, 2024.

[4] A. N. Albagli, D. M. Falcão, and J. F. de Rezende, "Smart grid framework co-simulation using HLA architecture," *Electric Power Systems Research*, vol. 130, pp. 22-33, 2016.

[5] G. Celli, P. A. Pegoraro, F. Pilo, G. Pisano, and S. Sulis, "DMS cyber-physical simulation for assessing the impact of state estimation and communication media in smart grid operation," *IEEE Transactions on Power Systems*, vol. 29, no. 5, pp. 2436-2446, 2014.

[6] E. Sharma *et al.*, "Co-simulation of a low-voltage utility grid controlled over IEC 61850 protocol," in *2015 5th International Conference on Electric Utility Deregulation and Restructuring and Power Technologies (DRPT)*, 2015: IEEE, pp. 2365-2372.

[7] B. Liao, J. Cheng, and G. Ren, "Microgrid adaptive current instantaneous trip protection," in *2019 IEEE innovative smart grid technologies-asia (ISGT asia)*, 2019: IEEE, pp. 2074-2078.

[8] T. S. Ustun, C. Ozansoy, and A. Ustun, "Fault current coefficient and time delay assignment for microgrid protection system with central protection unit," *IEEE Transactions on power systems*, vol. 28, no. 2, pp. 598-606, 2012.

[9] T. S. Ustun and R. H. Khan, "Multiterminal hybrid protection of microgrids over wireless communications network," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2493-2500, 2015.

[10] Y. Han, X. Hu, and D. Zhang, "Study of adaptive fault current algorithm for microgrid dominated by inverter based distributed generators," in *The 2nd International Symposium on Power Electronics for Distributed Generation Systems*, 2010: IEEE, pp. 852-854.

[11] P. Mahat *et al.*, "A simple adaptive overcurrent protection of distribution systems with distributed generation," *IEEE Transactions on smart grid*, vol. 2, no. 3, pp. 428-437, 2011.

[12] M. Khederzadeh, "Adaptive setting of protective relays in microgrids in grid-connected and autonomous operation," in *11th IET International Conference on Developments in Power Systems Protection (DPSP 2012)*, 2012: IET, pp. 1-4.

[13] M. Li, Y. Xue, M. Ni, and X. Li, "Modeling and hybrid calculation architecture for cyber physical power systems," *IEEE Access*, vol. 8, pp. 138251-138263, 2020.

[14] S. Balasreedharan and S. Thangavel, "An adaptive fault identification scheme for DC microgrid using event based classification," in *2016 3rd International Conference on Advanced Computing and Communication Systems (ICACCS)*, 2016, vol. 1: IEEE, pp. 1-7.

[15] "Examples | IEC 61850 Substation Automation System (SAS) with MMS." OPAL-RT Technologies. https://opal-rt.atlassian.net/wiki/spaces/PDOCHS/pages/150208994/Examples+IEC+61850+Substation+Automation+System+SAS+with+MMS.

[16] H. M. Mustafa, S. Basumallik, R. Fetsick, and A. Srivastava, "Using sdn to enhance cyber resiliency in iec 61850-based substation ot networks," in *2023 IEEE International Conference on Energy Technologies for Future Grids (ETFG)*, 2023: IEEE, pp. 1-6.

[17] S. Soltani, M. Mottaghizadeh, A. Hussain, and I. Kamwa, "Cyber-Attack Detection on Distance Relays for Parallel Transmission Lines in Digital Substations," in *2025 IEEE Power & Energy Society General Meeting (PESGM)*, 27-31 July 2025 2025, pp. 1-5, doi: 10.1109/PESGM52009.2025.11225656.