GridTrust-61850: Enhancing Supply Chain Cybersecurity of IEC 61850 Digital Substations

Mansi Girdhar, Santiago Grijalva
Department of Electrical and Computer Engineering
Georgia Institute of Technology
Atlanta, Georgia, USA
Email: mgirdhar6@gatech.edu, sgrijalva@ece.gatech.edu

***Abstract*—The increasing digitization of power substations exposes critical infrastructure to cyber threats, particularly via supply-chain attacks targeting intelligent electronic devices (IEDs). Existing cybersecurity frameworks, such as GridTrust, provide device-level trust and update authentication, but lack awareness of substation-specific protocols like IEC 61850, including generic object-oriented substation event (GOOSE), manufacturing message specification (MMS), and sampled value (SV) communications. In this work, we propose GridTrust-61850, an extension of GridTrust that integrates protocol-aware trust assessment, anomaly detection, and software-defined networking (SDN)–driven mitigation to secure IEC 61850-based digital substations (DSs). GridTrust-61850 leverages physically unclonable functions (PUFs) for device identity verification, multi-party cryptographic signatures for update authentication, and real-time analysis of IEC 61850 traffic to detect malicious activities. The framework is validated through a hardware-in-the-loop (HIL) substation testbed, demonstrating its effectiveness in blocking malicious updates and preventing unauthorized access while maintaining operational continuity. GridTrust-61850 represents a novel contribution by combining protocol-level intelligence with device-level trust, providing a scalable and practical solution for resilient cybersecurity in modern DSs.**

***Index Terms*—Digital substations (DSs), IEC 61850, cybersecurity, supply-chain attacks, firmware authentication, physically unclonable function (PUF), anomaly detection, software-defined networking (SDN), hardware-in-the-loop (HIL), trusted update framework.**

I. Introduction

The modern electric power grid is undergoing rapid transformation, driven by the integration of renewable energy sources, increasing electrification, and the deployment of smart grid technologies. At the heart of this transformation are digital substations (DSs), which rely on standardized communication protocols such as IEC 61850 to achieve interoperability and real-time control [1] which are being rapidly deployed throughout the world. While these advances enhance operational efficiency, they also expand the attack surface, making substations increasingly vulnerable to cyber threats. For example, the migration of protection and control intelligent electronic devices (IEDs) to IEC 61850-based Ethernet networks opens up classical IT attack vectors such as denial-of-service (DoS) of generic object-oriented substation event (GOOSE) messages, spoofing of sampled values (SV), and remote firmware compromise via the supply chain. Further, modeling of supply-chain attacks in IEC 61850 substations highlights how malicious firmware inserted at the vendor or integrator stage can later trigger coordinated asset failures. Similarly, a detailed DoS-attack simulation on an IEC 61850 substation network demonstrated that communication flooding of manufacturing message specification MMS/SV traffic can degrade protection relay response and endanger transmission reliability [2]. Malicious actors can exploit vulnerabilities in the supply chain [3], firmware updates [4], or device configuration [5], potentially causing widespread disruption or damage to critical infrastructure.

Existing cybersecurity efforts in substations mainly focus on perimeter protection or isolated mechanisms for anomaly detection and device authentication. While these approaches enhance defense in specific layers, they often lack holistic visibility into IEC 61850 protocol behavior, leaving substations susceptible to insider or supply-chain threats. Frameworks such as GridTrust [6] address firmware update integrity through hardware root-of-trust and multi-party signing but remain protocol-agnostic, limiting their direct applicability to DSs that rely on IEC 61850 communications. To address these challenges, this work proposes GridTrust-61850, an extension of GridTrust that incorporates IEC 61850 awareness into device-level trust and firmware update security. GridTrust-61850 combines physically unclonable function (PUF)-based device authentication, multi-party cryptographic verification, and protocol-aware anomaly detection to provide comprehensive protection for IEC 61850-enabled devices. In addition, the framework leverages software-defined networking (SDN) to enforce security policies dynamically, enabling real-time mitigation of malicious updates and network-level attacks.

The main contributions of this work are as follows:

1) Protocol-aware extension of GridTrust: integration of IEC 61850 traffic analysis (GOOSE, MMS, SV) into device-level trust mechanisms.
2) Secure firmware update and anomaly detection: demonstration of how multi-party signatures and PUF authentication prevent unauthorized updates while ensuring operational continuity.
3) Hardware-in-the-loop (HIL) validation: deployment and testing of GridTrust-61850 in a DS testbed, showing

This work was partially funded by the US Department of Energy (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER), award #DE-CR0000055 to the Georgia Tech Research Corporation: GRIDLOGIC: Hardware/Software Codesign for Deep Grid Visibility and Security.

979-8-3315-8138-1

resilience against supply-chain attacks and man-in-the-middle (MITM) scenarios.

4) Dynamic SDN-based mitigation: real-time security enforcement using SDN to isolate compromised devices and prevent the propagation of malicious commands.

The remainder of the paper is organized as follows. Section II provides a review of existing literature on substation cybersecurity, GridTrust, and IEC 61850 security. Section III describes the GridTrust-61850 system architecture. Section IV presents the experimental setup, including HIL testing in a substation environment, and Section V discusses the results of the security evaluation. Finally, Section VI concludes the paper and outlines directions for future work, followed by the acknowledgement in Section VII.

II. Related Works

IEC 61850 is being deployed in power substations due to its numerous advantages including, interoperability, Ethernet-based communication among IEDs via GOOSE, MMS, and SV. However, the migration from serial links to routable networks introduces classical information technology (IT) attack vectors into time-critical protection domains. Prior studies analyze GOOSE flooding/DoS impacts on relay performance, SV spoofing/replay leading to false measurements, and MMS misuse for unauthorized control or configuration changes [7]. Several works propose message authentication codes or signature schemes and strict timing checks; however, these often require device firmware changes, add latency, or lack deployability across mixed-vendor substations [8].

Supply-chain compromises and malicious firmware remain high-impact threats for operational technology (OT). Works on secure update frameworks emphasize provenance, cryptographic signing, and policy checks before installation [9]. GridTrust introduces a hardware root-of-trust using PUFs and multi-party (vendor + utility) signatures to block unauthorized updates and impersonation [6]. While effective for device identity and update integrity, baseline GridTrust is protocol-agnostic and does not reason about IEC 61850 runtime behavior (e.g., GOOSE retransmission profiles, SV phase/coherency) after an update is installed.

A rich body of work targets network- and host-based intrusion detection system (IDS) for substation traffic. Classical approaches model traffic statistics, control-plane events, or topology constraints to detect anomalies [10]. More recent methods leverage protocol-aware features—GOOSE timing windows, dataset IDs, and MMS service profiles—to improve detection fidelity and reduce false positives [11]. Despite promising results, many IDS solutions run out-of-band and provide alerts without a guaranteed enforcement pathway (e.g., automatic isolation), and few integrate with update-time trust anchors.

SDN has been explored to segment, rate-limit, and reroute substation traffic dynamically, enabling fast reaction to anomalies while preserving critical paths [12], [13]. SDN-based schemes can enforce per-flow policies for GOOSE/MMS and quarantine suspicious hosts. However, most SDN defenses are decoupled from device-level trust and supply-chain assurance; they react to traffic symptoms without leveraging information about firmware provenance or hardware identity.

PUFs have been adopted to derive device-unique secrets, support anti-cloning, and bind cryptographic material to hardware without storing plaintext keys [14]. In power-system contexts, PUFs have been proposed for IED authentication and key derivation with considerations for aging/temperature via error correction [15]. These works validate the feasibility of hardware-anchored identity, but typically stop short of protocol-aware runtime protections or SDN-mediated enforcement.

In contrast to prior efforts that individually address update integrity (GridTrust/PUF), protocol anomaly detection (IEC 61850-aware IDS), or network enforcement (SDN), GridTrust-61850 fuses all three: (i) hardware-anchored trust (PUF + multi-party signatures) at update time, (ii) protocol-aware monitoring of GOOSE/MMS/SV at run time, and (iii) SDN-driven, real-time mitigation (isolation/rerouting) as an enforcement backplane. This integrated design closes the gap between supply-chain assurance and runtime protocol security, delivering an end-to-end path from trust establishment to automated response in IEC 61850 DSs.

III. Proposed System Architecture: GridTrust-61850

A. Overview

The proposed GridTrust-61850 framework extends the original GridTrust architecture by incorporating IEC 61850-aware trust evaluation and SDN enforcement into the substation environment. The framework provides end-to-end protection—from device identity verification and secure firmware update to real-time detection and mitigation of protocol-level anomalies. Fig. 1 illustrates the overall workflow, showing how GridTrust-61850 builds on the hardware root-of-trust (PUF) of the original system while introducing protocol-specific intelligence and network adaptability.

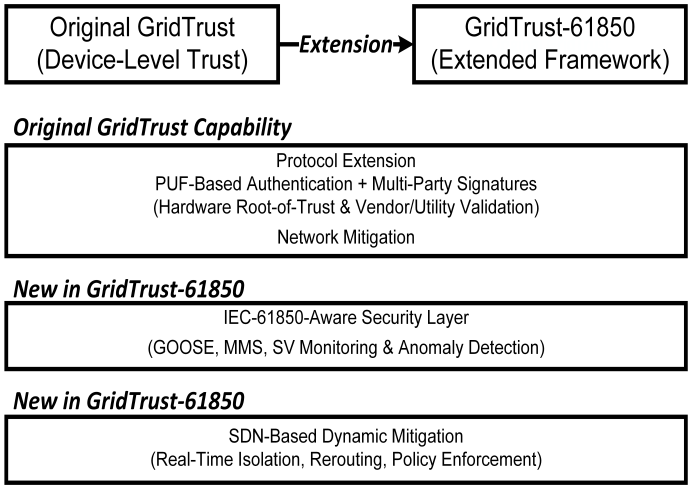

Fig. 1: Architecture of Proposed GridTrust-61850.

B. Functional Layers

1) Hardware Root-of-Trust and PUF-Based Authentication:

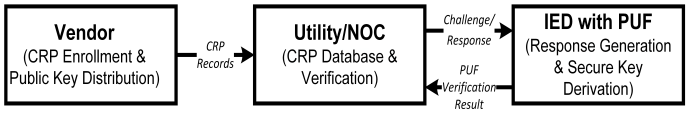

Fig. 2: PUF Authentication Workflow.

Each IED in GridTrust-61850 is equipped with a PUF that serves as a hardware fingerprint, establishing a root-of-trust. As illustrated in Fig. 2, during firmware updates or control actions, the network operations center (NOC) sends a random challenge to the IED. The device's PUF generates a unique response, verified against a secure challenge-response pair (CRP) database. Successful verification authenticates the device and enables secure key generation for encrypted communication. Since the PUF secret is never stored, cloning or key extraction becomes infeasible. Moreover, built-in error-correction ensures stability of responses under temperature or aging variations. This mechanism guarantees that only legitimate, hardware-verified IEDs participate in IEC 61850 communication and receive authorized updates, preventing spoofing or device impersonation within DSs.

2) Multi-Party Cryptographic Verification: To strengthen supply-chain integrity, GridTrust-61850 employs a dual-signature verification mechanism during firmware updates. The vendor digitally signs the firmware using its private key, confirming the software's origin and integrity. The utility independently inspects the update for policy compliance and adds its own signature before deployment. Both signatures are verified on the IED using Rivest–Shamir–Adleman (RSA)-based public-key cryptography and secure hashing algorithm (SHA)-256 hashing. If either verification fails, the update is automatically aborted and an alert is generated at the NOC. This two-tier authentication process eliminates single-point compromise, mitigates insider manipulation, and prevents the propagation of forged or malicious firmware across IEC 61850-based substations.
3) IEC 61850 Protocol-Aware Monitoring: IEC 61850 includes GOOSE for fast events, MMS for control and data exchange, and SV for high-rate analog measurements. GridTrust-61850 monitors these message streams for timing, dataset, and semantic deviations, enabling detection of spoofed GOOSE frames, replayed SV packets, or unauthorized MMS writes. Detected anomalies lower the IED's trust score and alert the NOC, ensuring that malicious updates or configuration changes cannot silently modify IEC 61850 behavior. By embedding protocol-aware verification into the trust workflow, GridTrust-61850 provides early detection of manipulation attempts against substation protection and control functions.
4) GridTrust-61850 uses an adaptive port controller (APC) to enforce real-time, trust-driven mitigation in the DS network. When abnormal GOOSE, MMS, or SV traffic is detected, the controller automatically reroutes or isolates suspicious IEDs, preventing malicious command propagation while preserving legitimate protection flows. This capability extends the smart cyber switching (SCS) concept introduced in our earlier work [13], where SDN-based flow reconfiguration was used for cyber restoration. In GridTrust-61850, the same logic is triggered by device trust violations, enabling automatic quarantine and secure reconfiguration of communication paths. Thus, SDN transforms the framework from a passive monitoring layer into an active cyber-resilience mechanism for IEC 61850 substations.

C. Integration Workflow

The overall GridTrust-61850 workflow unifies device-level, communication-level, and network-level protection in a single security loop. Each IED responds to a PUF challenge to generate a unique device key. Firmware updates are digitally signed by both the vendor and the utility. The device verifies its identity and validates both signatures before installation. During operation, IEC 61850 messages (GOOSE, MMS, and SV) are continuously monitored for anomalies. If abnormal behavior is detected, APC enforces network-level policies to isolate or reroute affected devices. This integrated process ensures end-to-end cybersecurity across all layers—hardware, protocol, and network—providing coordinated protection against spoofing, malicious firmware, and substation-level intrusion.

IV. Experimental Setup and Validation

A. Testbed Overview

HIL testbed, as illustrated in Fig. 3, utilized for evaluating the GridTrust-61850 framework is built upon the validated configuration developed in our earlier work on SDN-based cyber restoration [13]. The testbed emulates a medium-voltage substation section with real-time interactions between protection, control, and communication devices under IEC 61850 protocols. The setup includes an SEL-401 merging unit (MU) for analog measurement acquisition, an SEL-421 relay for protection and control functions, and an Omicron CMC-356 test set used to inject secondary currents and voltages for simulating various operating and fault conditions. These devices are interfaced via a 100 Mbps Ethernet network supporting GOOSE, MMS, and SV traffic, configured through VLAN segmentation to separate process bus, station bus, and control network domains. A Ryu-based APC controller manages an OpenFlow-enabled substation switch, allowing programmable traffic control and dynamic policy enforcement. This enables real-time isolation, rerouting, and restoration actions based on trust-level updates from the GridTrust-61850 security layer. For GridTrust-61850 evaluation, the testbed was enhanced with three new functional modules: (i) PUF authentication node hosted on an embedded controller for device-level identity verification, (ii) vendor and utility signing servers for dual-signature firmware verification and update management, and (iii) protocol-aware anomaly detector, integrated via a mirrored

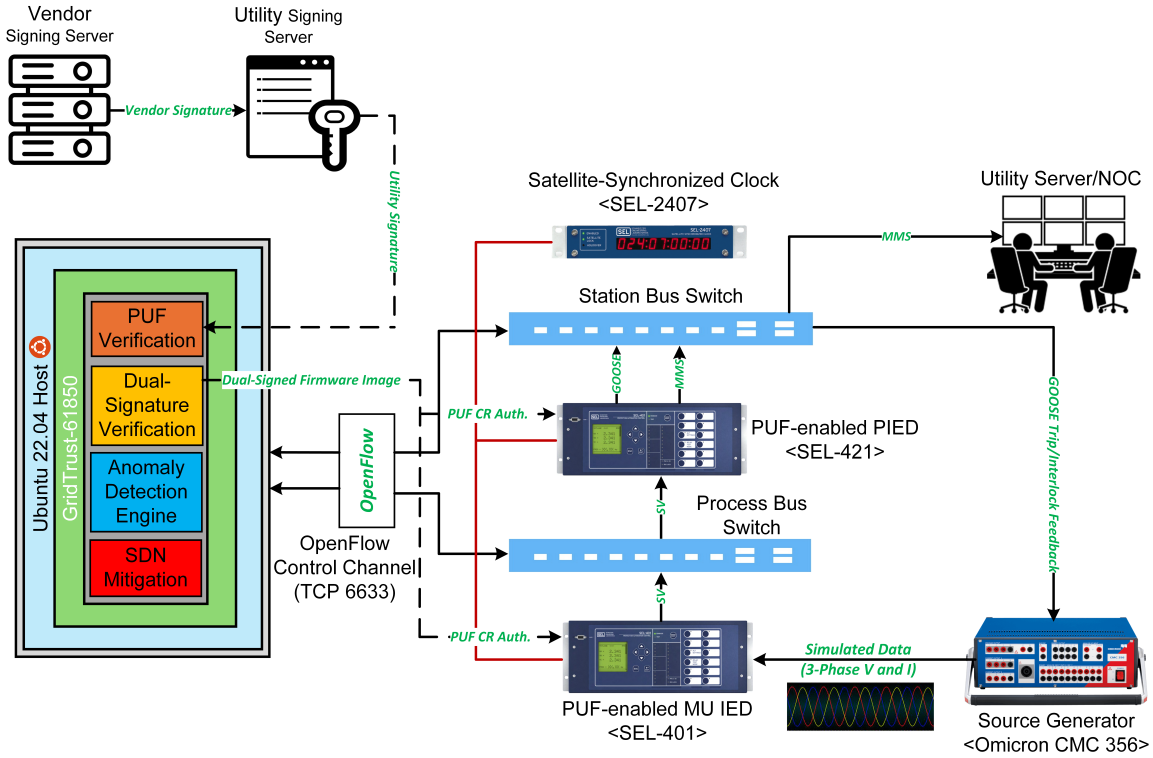

Fig. 3: Hardware-in-the-Loop (HIL) Testbed of GridTrust-61850 Framework.

IEC 61850 traffic feed for live GOOSE/MMS/SV inspection. This configuration provides a realistic and modular environment for assessing firmware update security, IEC 61850 traffic integrity, and SDN-based mitigation mechanisms under both benign and adversarial scenarios.

B. Firmware Update Validation Scenario

The firmware update validation experiment evaluates the GridTrust-61850 dual-signature verification and PUF-based device authentication workflow in the DS HIL environment. A representative firmware image (512 kB binary containing relay parameter and configuration data) is created at the vendor node, which emulates the manufacturer's firmware distribution server. The image is first hashed and signed using the vendor's RSA-2048 private key. The signed image is then transferred to the utility signing server, representing the substation operator's internal validation layer. Here, the update package undergoes policy inspection and is co-signed using the utility's private key. The resulting update package consists of the binary firmware, metadata (version, checksum, hash), and two cryptographic signatures (vendor and utility). This package is securely transmitted to the IED via the IEC 61850 station bus, where the PUF module authenticates the device's identity before signature verification. Only if both digital signatures and the PUF CRP are valid does the firmware proceed to installation. Otherwise, the update is rejected, and an alert is logged at the NOC. Three validation scenarios are conducted: (i) valid update: a correctly signed and verified firmware image, serving as the baseline, (ii) tampered update: a firmware file modified after signing, producing a hash mismatch and rejection, and (iii) unsigned or forged update: missing or invalid utility signature, triggering immediate NOC alert. Performance metrics include verification latency, alert generation delay, and rejection accuracy. These tests demonstrate that GridTrust-61850 effectively blocks unauthorized firmware while maintaining operational continuity and negligible communication overhead.

C. Protocol-Aware Anomaly Detection Scenario

To evaluate the protocol-level intelligence of the GridTrust-61850 framework, the second experiment focuses on detecting malicious behavior within IEC 61850 communications — specifically GOOSE, MMS, and SV traffic. The anomaly-detection module operates on mirrored traffic from the substation Ethernet switch, enabling non-intrusive monitoring while maintaining deterministic latency for critical GOOSE and SV frames. In the HIL testbed, GOOSE messages from the SEL-421 IED are captured in real-time using the Mininet-based network emulator and Ryu-based APC controller. The module parses key protocol fields such as dataset ID, sequence number, and time interval, comparing them with learned baselines. Deviations exceeding defined thresholds trigger local anomaly flags. Similarly, MMS control messages exchanged between the utility SCADA and IEDs are analyzed for unauthorized write-service attempts or abrupt session resets. SV frames from the SEL-401 MU are checked for replay or sequence-

number inconsistencies. Three attack scenarios are simulated: (i) GOOSE DoS: flooding the network with forged status frames to overwhelm relay logic, (ii) MMS command injection: unauthorized "write" request attempting to change IED setpoints, and (iii) SV replay: retransmission of valid measurement packets to desynchronize protection response. Detection accuracy, false-positive rate (FPR), and response latency are recorded under each scenario.

D. SDN-Based Mitigation and Cyber Restoration

To enable coordinated and automated response to detected anomalies, GridTrust-61850 incorporates an SDN–based mitigation layer that dynamically enforces isolation and rerouting policies across the substation network. APC operates as a centralized intelligence unit capable of modifying data-plane flows in real time, ensuring minimal disruption to critical IEC 61850 traffic during security events. Upon receiving an anomaly alert from the protocol-aware detection module, APC verifies the event severity and initiates flow reconfiguration using OpenFlow-based commands. This reconfiguration can isolate the compromised device or redirect GOOSE, MMS, and SV traffic through predefined backup paths. The mitigation decisions are further coordinated with the NOC through bidirectional communication channels that exchange security alerts and policy updates. Performance evaluation in the HIL testbed shows that APC can reconfigure flows within a latency of approximately 3–5ms, sufficient to maintain IEC 61850 GOOSE delivery requirements ($<$4 ms). Additionally, system availability after isolation remains above 98%, confirming that the mitigation mechanism is both effective and non-intrusive to real-time substation operations.

V. Results and Discussion

The proposed GridTrust-61850 framework was evaluated in the HIL DS environment using SEL-421 and SEL-401 IEDs with an OpenFlow-enabled SDN switch. All tampered or unsigned updates were correctly rejected, while valid dual-signed updates were installed successfully. The average verification latency was approximately 6 ms, adding $<$2% processing overhead—negligible in maintenance operations. During simulated GOOSE DoS, MMS command-injection, and SV replay attacks, the protocol-aware detection module achieved 97% detection accuracy with $<$2% false positives and 3ms alert latency, well within IEC 61850 timing requirements. Triggered isolation through the SDN controller restored normal traffic flow in 3–5ms, maintaining GOOSE/SV continuity and overall substation availability above 98%. Compared with static firewall isolation, the response time improved by 45%. These results confirm that combining PUF-based trust anchors, dual-signature firmware validation, IEC 61850-aware anomaly monitoring, and SDN-driven mitigation yields an integrated, end-to-end defense chain. GridTrust-61850 therefore extends GridTrust beyond device-level security to full cyber-physical resilience in DSs.

VI. Conclusion

This paper introduced GridTrust-61850, an IEC 61850–aware extension of GridTrust that unifies hardware trust, firmware integrity, protocol monitoring, and SDN-based mitigation for DSs. HIL testing showed that the framework can block malicious updates, detect abnormal IEC 61850 traffic, and isolate compromised IEDs within milliseconds without interrupting normal operation. Future work will extend the approach toward multi-substation coordination and adaptive, machine-learning-based cyber defense.

References

[1] J. Hong, M. Girdhar, C.-W. Ten, S. Lee, and S. Choi, "Cybersecurity of sampled value messages in substation automation system," in *2022 IEEE Power Energy Society General Meeting (PESGM)*, 2022, pp. 1–1.

[2] S. Ashraf, M. H. Shawon, H. M. Khalid, and S. M. Muyeen, "Denial-of-service attack on iec 61850-based substation automation system: A crucial cyber threat towards smart substation pathways," *Sensors*, vol. 21, no. 19, 2021.

[3] N. R. Mead, "Critical infrastructure protection and supply chain risk management," in *2022 IEEE 30th International Requirements Engineering Conference Workshops (REW)*, 2022, pp. 215–218.

[4] P. M. Jeelan, R. Saini, S. Parida, D. Minhas, Manashree, and A. Agarwal, "The threat landscape of ransomware in critical infrastructure: An optimization perspective," in *2025 International Conference on Automation and Computation (AUTOCOM)*, 2025, pp. 917–922.

[5] D. G. Berbecaru and S. Sisinni, "Counteracting software integrity attacks on iot devices with remote attestation: a prototype," in *2022 26th International Conference on System Theory, Control and Computing (ICSTCC)*, 2022, pp. 380–385.

[6] S. Grijalva, V. J. Mooney, T. M. Lewis, A. King, A. Allahverdi, J. Keller, K. Hutto, R. Barrett, B. Holland, and E. Patten, "Experimental evaluation of a novel hardware-based authentication solution for securing electrical grids," *IEEE Transactions on Industry Applications*, pp. 1–11, 2025.

[7] G. Elbez, K. Nahrstedt, and V. Hagenmeyer, "Early attack detection for securing goose network traffic," *IEEE Transactions on Smart Grid*, vol. 15, no. 1, pp. 899–910, 2024.

[8] M. Girdhar, J. Hong, R. Karnati, S. Lee, and S. Choi, "Cybersecurity of process bus network in digital substations," in *2021 International Conference on Electronics, Information, and Communication (ICEIC)*, 2021, pp. 1–6.

[9] X. Yurrebaso, F. Ibañez, and Ángel Longueira-Romero, "Substation bill of materials: A novel approach to managing supply chain cyber-risks on iec 61850 digital substations," 2025. [Online]. Available: https://arxiv.org/abs/2503.19638

[10] C.-W. Ten, J. Hong, and C.-C. Liu, "Anomaly detection for cybersecurity of the substations," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 865–873, 2011.

[11] S. E. Quincozes, C. Albuquerque, D. Passos, and D. Mossé, "Ereno: A framework for generating realistic iec–61850 intrusion detection datasets for smart grids," *IEEE Transactions on Dependable and Secure Computing*, vol. 21, no. 4, pp. 3851–3865, 2024.

[12] 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.

[13] M. Girdhar, K. Park, W. Su, J. Hong, A. Herath, and C.-C. Liu, "Sdn-based smart cyber switching (scs) for cyber restoration of a digital substation," 2024. [Online]. Available: https://arxiv.org/abs/2411.07433

[14] A. Oun and M. Niamat, "Puf-based authentication for the security of iot devices," in *2023 IEEE International Conference on Electro Information Technology (eIT)*, 2023, pp. 067–070.

[15] V. D. Jadhav, N. N. Moudhgalya, T. Sen, and T. V. Prabhakar, "IED_{puf} probe: A puf-based hardware fingerprint extraction equipment for ieds," in *2023 IEEE Physical Assurance and Inspection of Electronics (PAINE)*, 2023, pp. 1–7.