This article has been accepted for publication in IEEE Transactions on Industry Applications. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIA.2026.3680372

Interoperability Assessment Framework for IEC 61850 Multivendor Digital Substations: Challenges and Recommendations

Gustav Keppler*, Andrea Bonetti†, Veit Hagenmeyer*, Ghada Elbez*
*Institute for Automation and Applied Informatics (IAI), KASTEL Security Research Labs (SRL),
Karlsruhe Institute of Technology (KIT), Germany
†Megger Sweden AB, Danderyd, Sweden
Email: gustav.keppler@kit.edu, andrea.bonetti@megger.com, veit.hagenmeyer@kit.edu, ghada.elbez@kit.edu

***Abstract*—The transition to IEC 61850-based digital substations requires robust interoperability among devices from multiple vendors. This paper presents a practical interoperability assessment framework developed and applied within an expanded multivendor laboratory environment. We address challenges including vertical and horizontal data exchange reliability, Precision Time Protocol (PTP) synchronization complexities, process interface integration using I/O boxes, and variations in vendor implementations of the IEC 61850 standard. Based on initial findings, this work details experiences gained through a two-phase engineering approach (bottom-up followed by top-down), comprehensive communication chain validation, and analysis of specific vendor behaviors, such as Report Control Block limitations and PTP handling in network switches. Although conformance testing is essential, achieving interoperability also requires meticulous configuration, targeted testing of vendor-specific nuances, and suitable network infrastructure. Ongoing standardization efforts, particularly the collaborative initiatives of IEC Technical Committees 95, 38, and 57 through the new Joint Advisory Group JAG 25, minimize these engineering and testing demands by enabling greater inherent interoperability in IEC 61850 based substations. We provide recommendations for establishing similar testbeds and executing effective interoperability assessments, aiming to streamline future deployments and enhance the reliability of digital substations.**

***Index Terms*—Digital Substation, IEC 61850, Interoperability, Functional Interoperability, Multivendor Systems, Precision Time Protocol (PTP), System Configuration Language (SCL), Conformance Testing, Laboratory Testing, Integration.**

ABBREVIATIONS

BC Boundary Clock. 7
BCU Breaker Control Unit. 9
BIED Breaker Interface Electronic Device. 9
BIOI Binary Input/Output Intelligent Electronic Device. 9

CID Configured IED Description. 7

GGIO Generic Input/Output. 7
GOOSE Generic Object Oriented System Event. 3–7

HIL Hardware-in-the-Loop. 2

ICD IED Capability Description. 7
ICT IED Configuration Tool. 4, 5, 7, 8
IDS Intrusion Detection System. 4
IED Intelligent Electronic Device. 1–9

LN Logical Node. 7

MMS Manufacturing Message Specification. 3–7
MU Merging Unit. 3–5, 7, 9

NTP Network Time Protocol. 3

P2P TC Peer-to-Peer Transparent Clock. 7
PRP Parallel Redundancy Protocol. 4, 8
PTP Precision Time Protocol. 2–8, 10

RCB Report Control Block. 5–7
RTU Remote Terminal Unit. 3, 5–7

SAMU Stand-Alone Merging Unit. 9
SCADA Supervisory Control and Data Acquisition. 3, 7
SCD Substation Configuration Description. 4–7
SCL System Configuration Language. 2, 4–7
SCT System Configuration Tool. 4, 6–8
SV Sampled Value. 3–5, 7, 8

TC Technical Committee. 9

VLAN Virtual Local Area Network. 4, 8

I. INTRODUCTION

The digitalization of electrical substations, driven by the IEC 61850 standard [1], enables advancements in grid management, including enhanced efficiency, reliability, and potential reductions in engineering and commissioning costs. Digital substations have also introduced new approaches to the management and operation of electrical grids, offering the potential for increased safety alongside these improvements [2]. IEC 61850 provides a standardized framework for communication, data modeling, and system engineering, enabling the integration of Intelligent Electronic Devices (IEDs) for protection, control, measurement, and monitoring. This standardization is essential for realizing advanced concepts like centralized

---

This work was supported by funding from the topic Engineering Secure Systems of the Helmholtz Association (HGF) and by KASTEL Security Research Labs (structure 46.23.02).

This article has been accepted for publication in IEEE Transactions on Industry Applications. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIA.2026.3680372

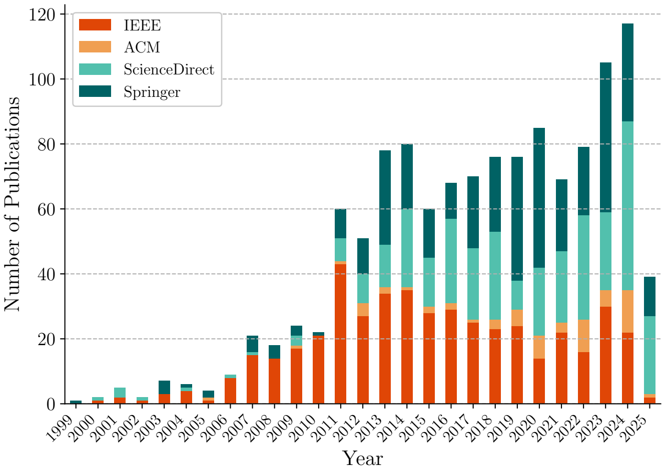


Fig. 1: Publications per year across the IEEE Xplore, ScienceDirect, ACM, and Springer databases for "IEC 61850" AND "Interoperability", showing continued research activity.

protection and control [3] and integrating substations into the broader smart grid [4], with ongoing research exploring its application in diverse contexts such as microgrid control [5] and the integration of distributed energy resources [6].

IEC 61850 digital substation devices aim for interoperability, defined as the ability of IEDs from multiple vendors to communicate and operate together. This allows utilities greater flexibility in device selection based on performance and features, thereby promoting competition and innovation. However, achieving seamless and reliable interoperability remains a practical challenge [7]. Differences in vendor interpretations of the standard, optional feature implementations, and configuration tool limitations can lead to subtle or overt communication failures, synchronization issues, particularly with Precision Time Protocol (PTP) implementations, and difficulties during commissioning [8]. These challenges emphasize the necessity for rigorous testing and validation procedures to ensure dependable data exchange among devices.

Beyond basic communication, achieving functional interoperability is critical for ensuring consistent and reliable system behavior across diverse equipment. This concept, developed through initiatives like IEC TS 60255-216-1 [9], aims to standardize the functional behavior of protection and control elements, especially during non-nominal conditions. By standardizing the behavior of protection and control functions, particularly in scenarios referred to as "non-nominal situations," the costs associated with commissioning tests can be reduced. This standardization across various scenarios not only reduces the necessity to test many behavior combinations, which are either unexpected or already accounted for through type testing by manufacturers based on standardized consensus, but also promotes consistent functionality. Consequently, not only are the commissioning tests simplified, but the technical specification also becomes less cumbersome, as many behaviors are anticipated and can be addressed simply by referencing the standard to ensure expected behavior is achieved [10]. This standardization enables the reduction of commissioning efforts by minimizing the need to test numerous vendor-specific behavioral combinations.

Recognizing these challenges, industry and academia utilize various methods for interoperability validation. Conformance testing laboratories assess adherence to the standard, while interoperability events, such as those organized by UCA International Users Group [11], provide platforms for multivendor testing, often revealing issues related to System Configuration Language (SCL) inconsistencies and protocol implementation nuances. Advanced testbeds employing Hardware-in-the-Loop (HIL) techniques also play a role in validating complex interactions [12]. The practical lessons learned from establishing such lab-based digital substations will also be shared later in this article.

A review of recent literature (post-2021, following Ayello et al. [13]) confirms sustained research interest (see Table I and Figure 1). Analysis of 440 papers from major databases (IEEE Xplore, ScienceDirect, ACM, Springer) yielded 11 relevant case studies focusing on practical multivendor communication after filtering for studies detailing testbed implementations or field deployments. The literature continues to emphasize interoperability benefits [14] and describes successful implementations [15]–[19]. However, persistent challenges include diverse standard interpretations, optional field usage, proprietary SCL extensions, and the need for robust testing methodologies [20]–[23]. Recent work continues to explore solutions for these issues, for instance, detailing design considerations for process bus and PTP implementations [24].

TABLE I: Number of publications from databases using specified search strings after the review by Ayello et al. [13].

Data Base	Search Strings	Search Date	# papers
IEEE Xplore	"IEC 61850" AND "Interoperability"	2021–31/3/25	96
ScienceDirect	"IEC 61850" AND "Interoperability"	2021–31/3/25	182
ACM	"IEC 61850" AND "Interoperability"	2021–31/3/25	31
Springer	"IEC 61850" AND "Interoperability"	2021–31/3/25	131

This paper extends previous work [8] by presenting a comprehensive assessment based on an expanded laboratory setup and further testing. The major contributions are:

- Application of an Interoperability Testing Framework tailored for multivendor digital substations.
- Detailed analysis of interoperability challenges in an expanded testbed, including integration of process interface devices (I/O Boxes).
- In-depth investigation of PTP synchronization issues, emphasizing the critical role of network switch capabilities.
- Identification and documentation of specific vendor implementation nuances that affect interoperability beyond standard conformance.
- Practical recommendations derived from hands-on experience for setting up similar laboratories and conducting effective interoperability testing.
- Provision of testing datasets (.pcap files) upon request to facilitate further research.

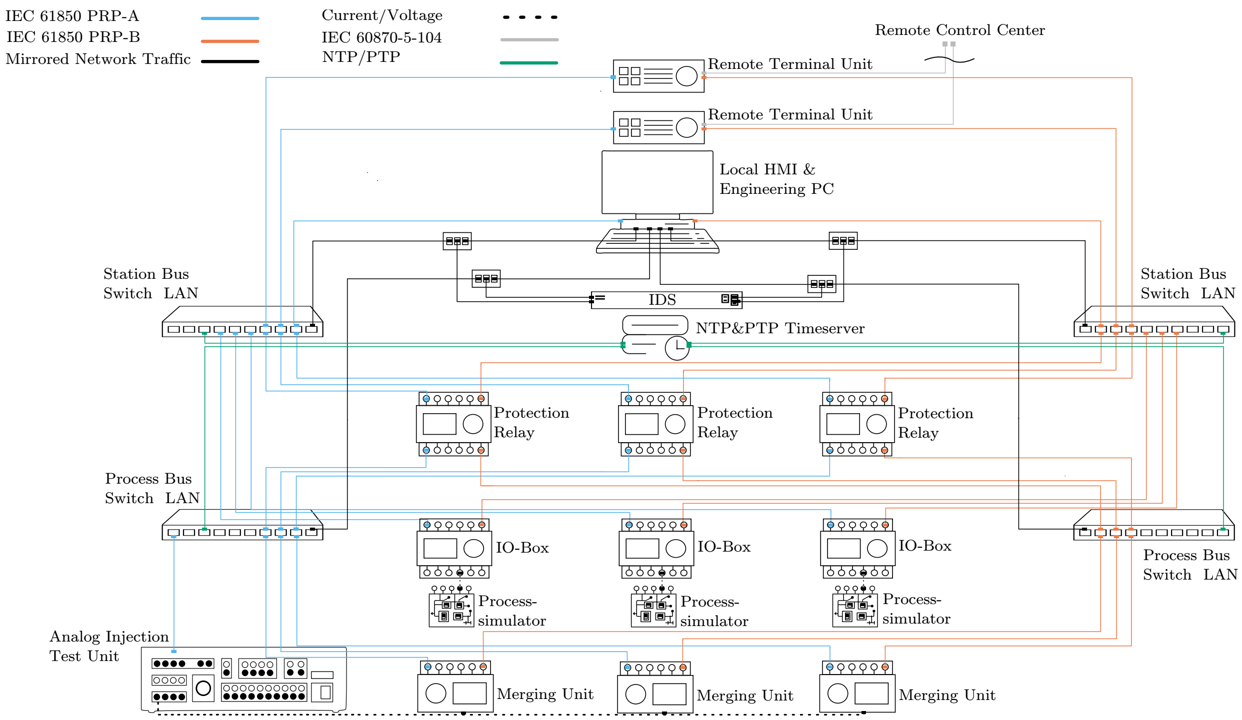


Fig. 2: Overview of the expanded multivendor substation in the KASTEL Security Lab Energy, depicting three bays and communication paths. Management network omitted for clarity.

The remainder of this paper is organized as follows: Section II describes the expanded laboratory environment and the engineering approach adopted. Section III details the interoperability testing framework and presents the results, as well as the challenges encountered. Section IV offers practical recommendations for laboratory setup and testing, drawing on our experiences and related work. Section V discusses Standardization Efforts for improved interoperability, focusing on the Joint Advisory Group JAG 25 and related initiatives. Finally, Section VI concludes the paper and outlines future research directions.

II. LABORATORY ENVIRONMENT AND ENGINEERING APPROACH

Effective interoperability assessment requires a representative test environment and a structured engineering methodology. This section details the expanded laboratory setup at the KASTEL Security Lab Energy and the two-phase engineering approach adopted.

A. *Expanded Laboratory Setup*

The laboratory emulates a digital substation environment, specifically designed for interoperability testing by integrating equipment from multiple vendors. This multivendor approach uses the IEC 61850 standard [1] to potentially reduce costs and avoid vendor lock-in, while simultaneously providing a platform to investigate interoperability challenges arising from differences in vendor implementations [8]. The setup, conceptually depicted in Figure 2, incorporates real-world equipment from major manufacturers: Schweitzer Engineering Laboratories (SEL), ABB, Siemens Energy, and General Electric.

The components and their interactions within the IEC 61850 framework include:

- **Protection IEDs:** Central protection relays from multiple vendors, configurable with various protection functions (e.g., distance, overcurrent), form the core of the bay-level functions.
- **MUs:** Interface with an analog injection test unit to digitize simulated primary system values and transmit them as IEC 61850-9-2LE Sampled Value (SV) streams over the process bus.
- **Remote Terminal Units (RTUs):** Hardware- and Software-based RTUs act as station-level devices, collecting data from IEDs via Manufacturing Message Specification (MMS) over the station bus and mapping to other protocols like IEC 60870-5-104 for Supervisory Control and Data Acquisition (SCADA) interaction.
- **Process Interface:** Dedicated I/O boxes bridge the digital and physical domains. They receive trip commands from protection IEDs via Generic Object Oriented System Event (GOOSE) messages and interact with Switchgear Simulators (emulating circuit breakers, disconnectors, and earthing switches) via binary I/O signals, providing status feedback via GOOSE on the process bus and MMS on the station bus.
- **Time Synchronization:** A dedicated Grandmaster Clock provides a precise time reference using both IEC 61850-9-3 PTP for process bus devices and Network Time Protocol (NTP) for station bus devices. This ensures

Fig. 3: View of the KASTEL Security Lab Energy testbed racks housing (from top to bottom)network switches, multivendor IEDs, Merging Units (MUs), Intrusion Detection System (IDS).

accurate time-stamping for SV, GOOSE, and MMS report correlation.

- **Network Infrastructure:** PTP-compliant managed Ethernet switches form the communication backbone, segmenting traffic into process and station buses using Virtual Local Area Networks (VLANs). Parallel Redundancy Protocol (PRP) is employed on critical links connected to the switches to enhance network reliability. A separate management network (omitted in Figure 2 for clarity) allows device configuration.
- **Test, Measurement & Auxiliary Systems:** Includes the analog injection unit, dedicated SV/GOOSE analyzers, network taps, and analysis workstations. Additionally, auxiliary systems are integrated for network monitoring and IDS functionalities.

The complexity inherent in this multivendor setup enables the creation of a holistic network environment covering the diverse communication protocols (SV, GOOSE, MMS) and functionalities specified within the IEC 61850 standard series. While smaller than operational substations, limiting evaluations of large-scale performance and resilience, this laboratory provides a platform for investigating interoperability issues and standard conformance. The integration of dedicated process simulators for switchgear, such as those emulating circuit breakers, disconnectors, and earthing switches, significantly enhances the laboratory's capability for functional interoperability testing. While simulators don't replicate all aspects of real primary equipment, they provide a tool for testing the digital and logical aspects of systems like IEC 61850-based digital substations. Our focus remains on the communication interoperability, SCL conformity, functional logic, and system integration at the secondary system level, acknowledging that human factors and operational practices are also essential components of overall substation management.

B. *Two-Phase Engineering Approach*

To manage complexity and accelerate initial setup in a multivendor environment, a pragmatic two-phase engineering approach was employed:

Phase 1 (Bottom-Up): Focused on achieving basic communication and functionality using vendor-specific IED Configuration Tools (ICTs). Configuration was performed device-by-device, often relying on proprietary features or manual workarounds. While faster initially, this led to inconsistencies and lacked a unified system view represented by a complete Substation Configuration Description (SCD) file, with additional challenges arising from inconsistent SCL handling among the vendor configuration tools.

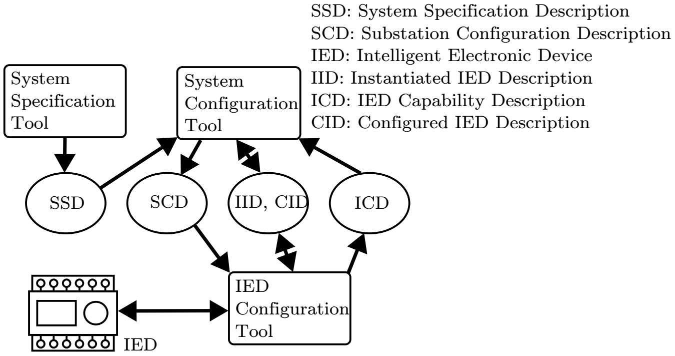


Fig. 4: Top-down engineering workflow using SCT and ICTs as defined in IEC 61850.

Phase 2 (Top-Down): Aims for a standards-compliant engineering workflow centered around a master SCD file generated and managed by a vendor-neutral System Configuration Tool

This article has been accepted for publication in IEEE Transactions on Industry Applications. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIA.2026.3680372

(SCT). The vendor ICTs is then used primarily for device-specific parameterization based on the SCD file export. This approach, depicted in Figure 4, promotes consistency, maintainability, and better adherence to the IEC 61850 engineering process. Phase 1 is largely completed, and Phase 2 is currently in progress.

C. Data Acquisition and Analysis

Systematic data acquisition and analysis are the basis for diagnosing interoperability issues. Network traffic capture using passive taps and Wireshark [25] provides raw packet data (.pcap files). Protocol analysis with IEC 61850 dissectors allows detailed inspection of SV, GOOSE, MMS, and PTP packets, essential for identifying subtle deviations or timing issues. Specialized tools like dedicated SV/GOOSE testers offer higher-level analysis and simplify conformance checks and functional testing. Device event logs provide additional context. Integrating these methods yields a comprehensive view for effective problem identification and resolution.

III. INTEROPERABILITY TESTING FRAMEWORK AND RESULTS

Based on the laboratory setup and engineering approach, an interoperability testing framework was applied. This section outlines the framework and discusses the findings and challenges encountered during testing.

A. Testing Framework Overview

The testing framework adopts an iterative approach, starting with basic connectivity and progressing towards complex functional validation, as illustrated in the diagram Figure 5.

The stages involve device setup, basic connectivity and time sync checks, integration testing (vertical: MU - Relay, Relay - RTU, IO-Box - RTU; horizontal: Relay - IO-Box), end-to-end validation, and functional testing of applications. Testing is iterative; issues trigger troubleshooting, reconfiguration, and re-testing.

B. Vertical Integration: MU-IED Communication

Testing involved injecting analog signals into MUs and verifying the reception and correct interpretation of the resulting SV streams to the protection IEDs designated for that bay. Basic SV subscription and data interpretation proved reliable with the device configuration via the vendor tools. Protection functions triggered appropriately based on received SV data during simulated fault conditions. Ensuring correct mapping of SV channels and data attributes, such as scaling factors, required verification using packet analysis tools, illustrated conceptually in Figure 6.

C. Vertical Integration: Protection Relay-RTU Communication

This focused on MMS communication, particularly Report Control Blocks (RCBs) from IEDs to RTUs and subsequent mapping to IEC 60870-5-104 within the RTU, as depicted in Figure 7. Data reporting via MMS was achieved between various IEDs and RTUs, and mapping to 104 functioned correctly after configuration.

Several challenges were encountered. Standard SCD files do not fully define the client-side (RTU) configuration, such as which reports to enable or how data should be mapped. This required supplementary configuration using spreadsheets or vendor-specific RTU tools, highlighting a limitation in the standard SCL workflow for client setup. One protection relay

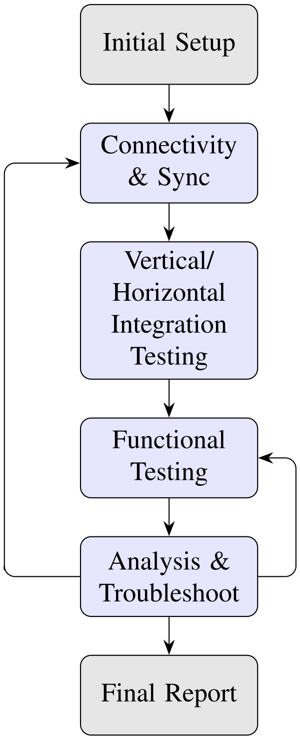


Fig. 5: Simplified Iterative Interoperability Testing Framework, showing feedback loops for re-testing after analysis.

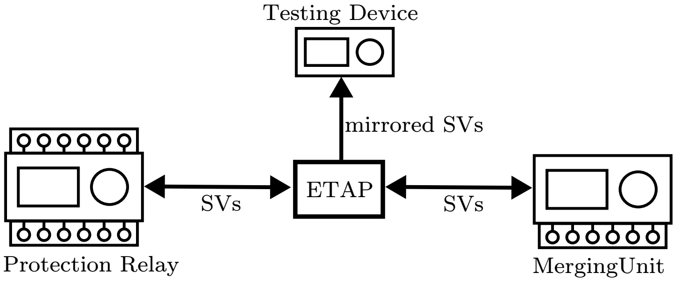


Fig. 6: Conceptual diagram for testing MU-IED communication using an injection tester and SV/GOOSE analyzer.

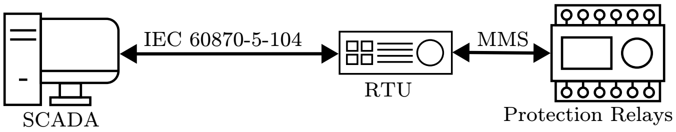


Fig. 7: Conceptual diagram of testing IED-RTU communication (MMS) and RTU-SCADA mapping (IEC 60870-5-104).

This article has been accepted for publication in IEEE Transactions on Industry Applications. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIA.2026.3680372

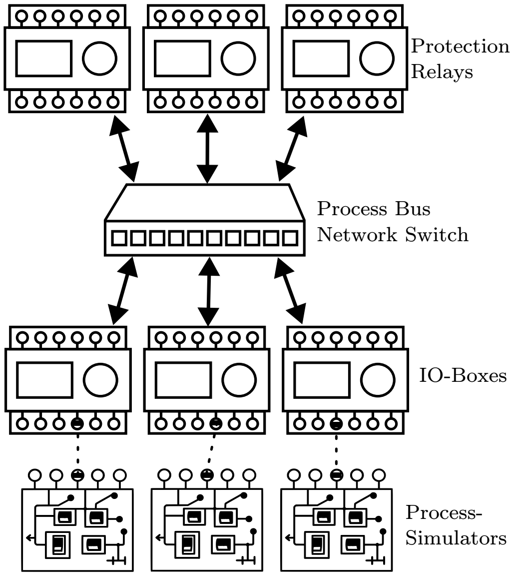
exhibited a vendor-specific MMS behavior where an RCB instance could only be exclusively enabled and utilized by a single client simultaneously, preventing concurrent subscriptions from multiple clients to the same report. If multiple clients needed the same dataset, duplicate RCBs had to be configured within the IED, deviating from the typical expectation of multi-client subscription. Furthermore, another relay required active MMS polling from the client (RTU) to retrieve data updates, rather than reporting spontaneously based on triggers, increasing network traffic and client dependency. Configuration complexities, especially during the bottom-up phase, often require manual intervention or workarounds within vendor tools. Verification of the RTU's 104 mapping was aided by tools like Fink's 104 tester [26]. These findings demonstrate how vendor-specific implementations impact interoperability.

D. Process Interface Integration

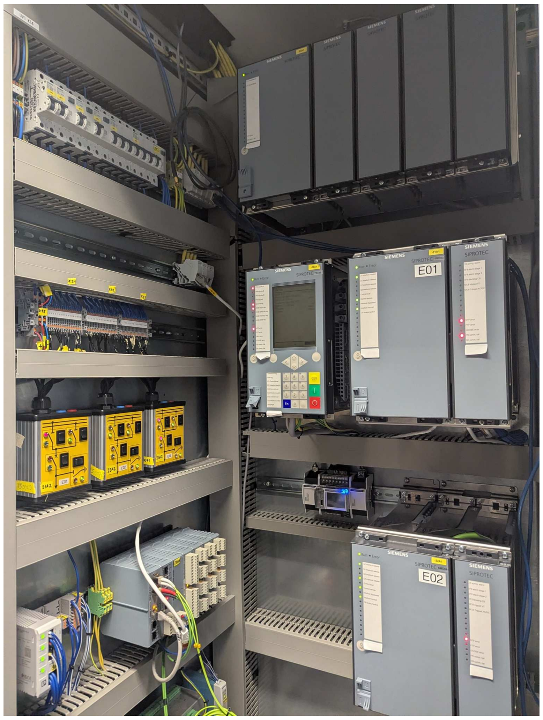
Interfacing with primary equipment was tested by integrating I/O boxes and Switchgear Simulators, such as those emulating circuit breakers, disconnectors, and earthing switches. This enhances the laboratory's capability for functional interoperability testing. While these simulators provide an abstracted representation of the primary equipment's physical behavior, they are crucial for validating the complete control loop involving protection IEDs and I/O boxes. They enable testing of sequences like trip command issuance via the process bus GOOSE, the I/O-Box's subsequent interaction with the simulated switchgear, and the feedback of the new switchgear status via GOOSE or MMS. This setup, featuring the physical I/O Boxes and Switchgear Simulators, is shown in Figure 8, while a conceptual diagram illustrating the communication flow for testing this integration is presented in Figure 8a.

Integrating the I/O-Boxes within a multivendor SCD file using a generic SCT proved challenging due to vendor-specific SCL modeling practices. Configuring the interaction purely based on the standard SCL workflow required dedicated mapping and understanding of the specific device model. Testing multivendor GOOSE between different IEDs and the I/O box demanded a specific SCL configuration of control blocks and datasets. This highlights the need for standardized modeling of process interface devices for seamless multivendor integration.

Although these simulators do not replicate the complex electro-mechanical transients or arcing phenomena of real switchgear, their ability to model discrete state changes and interact via standard binary I/O or communication protocols is sufficient for verifying the logical correctness of protection and control functions within the IEC 61850 framework. This allows for assessment of the digital communication and automation logic, which is a primary objective in these interoperability studies, without the risks and costs associated with actual high-voltage equipment.



(a) Conceptual diagram of testing Process Interface integration, showing I/O Boxes receiving GOOSE, and controlling the Switchgear Simulator.



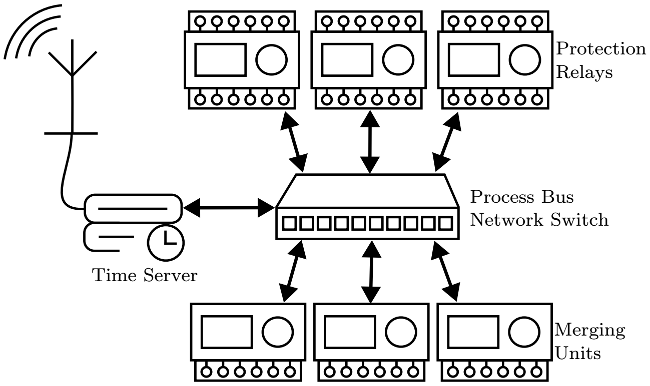
(b) Physical setup of I/O Boxes and Switchgear Simulators (yellow boxes) among other equipment in the lab.

Fig. 8: Integration of Process Interface: Conceptual diagram and physical lab setup.

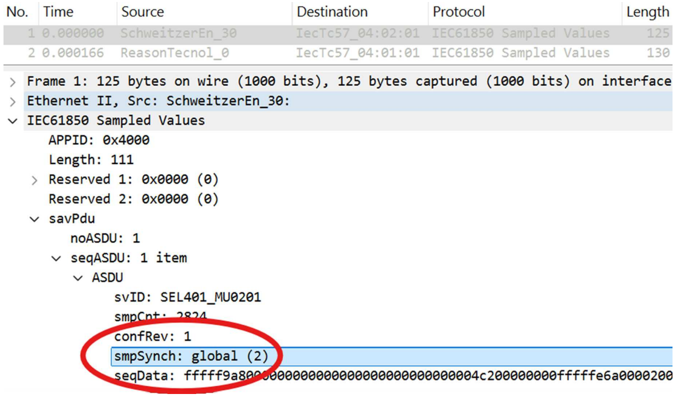
E. Precision Time Protocol Synchronization

Accurate time synchronization via PTP (IEC 61850-9-3 profile) is critical. The setup utilized a dedicated Grandmaster Clock, with devices configured as PTP slaves and PTP-aware network switches, as shown in Figure 9. With this configuration, stable synchronization was achieved across all devices, verifiable via device status and Wireshark analysis of PTP messages. A critical finding was the absolute necessity of PTP-aware switches. Initial tests with standard managed switches (lacking specific PTP support or only providing basic passthrough) resulted in unstable synchronization, frequent loss of sync, and large time offsets. This confirmed that reliable

This article has been accepted for publication in IEEE Transactions on Industry Applications. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIA.2026.3680372



(a) Conceptual diagram of PTP synchronization with a Grandmaster Clock and PTP-aware switches.



```
No.  Time       Source             Destination          Protocol                  Length
  1 0.000000   SchweitzerEn_30    IecTc57_04:02:01    IEC61850 Sampled Values     125
  2 0.000166   ReasonTecnol_0     IecTc57_04:01:01    IEC61850 Sampled Values     130

> Frame 1: 125 bytes on wire (1000 bits), 125 bytes captured (1000 bits) on interface
> Ethernet II, Src: SchweitzerEn_30:
v IEC61850 Sampled Values
    APPID: 0x4000
    Length: 111
  > Reserved 1: 0x0000 (0)
    Reserved 2: 0x0000 (0)
  v savPdu
      noASDU: 1
    v seqASDU: 1 item
      v ASDU
          svID: SEL401_MU0201
          smpCnt: 2824
          confRev: 1
          smpSynch: global (2)
          seqData: fffff9a8000000000000000000000000000004c200000000fffffe6a0000200
```

(b) Wireshark capture indicating a Merging Unit is in global PTP synchronization.

Fig. 9: PTP Synchronization: Conceptual overview and verification example.

PTP in demanding substation environments requires switches properly supporting either Boundary Clock (BC) or Peer-to-Peer Transparent Clock (P2P TC) functionality as specified in IEC 61850-9-3 and IEEE 1588. Standard ”IEC 61850 compliant” switches lacking these features may be insufficient. Consistent configuration of PTP parameters across all devices and switches also required attention, and debugging involved analyzing PTP messages and clock states.

F. End-to-End Communication Chain Validation

To ensure overall system integrity, the entire communication path from sensor (MU) to operator interface (RTU/SCADA) was tested. Analog values were injected into a MU, generating SV for a protection IED. The IED processed the SV, potentially issued a GOOSE trip, and sent data via MMS reports to an RTU. The RTU mapped the data to IEC 60870-5-104 for monitoring. This holistic test successfully verified the overall data flow and transformation across multiple devices and protocols. It proved instrumental in uncovering subtle issues, such as data type mismatches in the RTU’s 104 mapping or delays caused by inefficient MMS reporting configurations (identified in Section III-C), which might not be apparent in isolated tests. This validation provides confidence in the data integrity and timely delivery across the integrated system.

G. Vendor Implementation Variations and Adherence

Beyond explicit bugs or non-conformance, vendor choices in implementing optional features or interpreting ambiguities impact interoperability. As noted previously [8], the extensive use of the Logical Node (LN) class Generic Input/Output (GGIO) by some vendors requires reliance on vendor documentation for semantic understanding, which hinders transparency compared to the use of more specific LNs. The observed RCB single-client limitation and the MMS polling requirement are further examples of implementation choices that, while potentially compliant, create practical hurdles in multivendor systems. Minor differences in how vendor tools generate or interpret SCL files (”SCL dialects”), the use of private namespaces or handling of optional attributes, were also observed, sometimes requiring manual edits or specific tool versions for compatibility, particularly during the bottom-up phase.

H. Conformance and Tooling Considerations

The testing process highlighted distinctions related to conformance and tooling. Differentiating between interoperability issues originating in a device’s firmware, operating system, or fundamental protocol implementation versus those stemming from vendor-supplied configuration tools (ICTs or SCTs) is essential, as the root cause dictates the resolution path and responsibility. Device-inherent issues necessitate firmware updates from the device vendor, whereas tool-related problems may be addressed via configuration tool updates, workflow adjustments, or manual SCL file correction. Misattributing a tool-induced problem to a device fault leads to inefficient diagnostics and incorrect escalations. For instance, some observed interoperability problems arose from tools inadequately handling multivendor SCL scenarios, rather than from flawed device protocol implementation. The transition to a top-down engineering approach (Phase 2) particularly underscores this, as its success depends critically on the SCT’s ability to parse diverse IED Capability Description (ICD) files and generate a consistent SCD, and subsequently, on the ICTs’s capability to correctly import and process the resultant Configured IED Description (CID) file. Inconsistencies in how either tool category handles the SCL schema or vendor-specific extensions can disrupt this workflow, requiring dedicated toolchain interoperability testing. Furthermore, formal conformance tests may not cover all tool interaction scenarios, real-world configurations, vendor-specific extensions, or project-specific interaction dynamics, thus requiring dedicated laboratory testing to identify and bridge these gaps.

IV. RECOMMENDATIONS FOR LABORATORY SETUP AND TESTING

Based on the experiences gained in this study and insights from related research by Sullivan et al. [27], which documented lessons from the initial design, equipment specifi-

This article has been accepted for publication in IEEE Transactions on Industry Applications. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIA.2026.3680372

cation, and setup phases, particularly regarding device compliance and the importance of training, the following recommendations are offered. These recommendations focus on establishing comprehensive interoperability assessment facilities and developing test plans for systematically evaluating multivendor digital substations and addressing specific communication and functional challenges:

- **Phased Engineering Approach:** An initial bottom-up approach is recommended for device setup and to gain a granular understanding of individual component capabilities and vendor-specific behaviors. Subsequently, a transition to a top-down, SCT-centric workflow should be planned to ensure overall system consistency, scalability, and adherence to IEC 61850 engineering processes.

  ✓ Employ a two-phase engineering approach.

- **Device Specification and Pre-Verification:** Prior to integration, detailed project requirements for IEDs must be defined. These include confirmed support for necessary communication protocols, and SV capabilities if a process bus is part of the design. A thorough review of vendor documentation and physical hardware inspection is advised to confirm compliance, including physical network port types (RJ45, fiber optic LC connectors), to mitigate integration challenges.

  ✓ Define detailed IED requirements and pre-verify hardware/documentation.

- **Network Infrastructure Planning:** The use of managed network switches with explicit support for requisite PTP profiles and redundancy protocols such as PRP is indicated. Proper network segmentation via VLANs is essential for traffic management and security. Verification that switches possess appropriate port types, or that suitable converters are planned, is necessary to accommodate all IEDs.

  ✓ Plan network with PTP/redundancy-capable switches, and correct port types.

- **Comprehensive Testing Toolkit and Data Interpretation Strategy:** IEC 61850 is a digital, standardized technology based on numerical data exchange. The fact that it is standardized is beneficial, as it enables a wide range of stakeholders to develop tools to support its testing. However, its digital nature also presents challenges, particularly for substation engineers more familiar with analog systems. In analogue systems, electrical signals are clearly structured and physically separated — for example, it is immediately obvious where voltage or current inputs for a protection relay are located. In contrast, with the digital SV approach, this information is encapsulated within data streams. A simple error in identifying or naming one of these streams can lead to confusion, as a different stream might be analyzed by mistake. Furthermore, the analogue content — voltages and currents — is conveyed through streams of numerical values (the sampled values), which can be difficult to interpret directly.
  Based on experience with the commissioning and troubleshooting of digital IEC 61850 substations since 2004 - primarily with GOOSE messages, but increasingly with SV as well - using tools from multiple vendors simultaneously is highly advisable. Each vendor presents the information differently, and examining the same data from various perspectives helps the test engineer to develop a clearer understanding of the system. This approach is particularly helpful when interpreting raw data in tools such as Wireshark, where direct insights into electrotechnical quantities are limited.

  ✓ Utilize diverse analytical tools simultaneously to aid data interpretation.

- **System-Level and Functional Interoperability Focus:** Testing should extend beyond basic communication verification to include the validation of end-to-end functional chains and application-level logic across multiple vendor devices. Comprehensive functional interoperability testing is required to ascertain that the integrated system behaves as specified under diverse operational scenarios.

  ✓ Prioritize end-to-end system validation and comprehensive functional interoperability testing.

- **Assessment of Toolchain Interoperability and Vendor Software Expertise:** Interoperability between the selected central SCT and individual vendor ICTs requires explicit verification. Investment in targeted training on vendor-specific software tools is recommended to facilitate effective system implementation, optimization, and troubleshooting.

  ✓ Verify toolchain interoperability (SCT-ICT) and vendor software proficiency through training.

V. STANDARDIZATION EFFORTS FOR ENHANCED INTEROPERABILITY: JOINT ADVISORY GROUP JAG 25

The preceding sections have detailed the interoperability challenges encountered in multivendor IEC 61850 digital substations. This section outlines ongoing standardization activities, primarily through the Joint Advisory Group JAG 25 and associated Technical Committees, that aim to enhance baseline interoperability and functional consistency, directly impacting the challenges and testing needs discussed earlier.

The Joint Advisory Group JAG 25 was established to coordinate standardization efforts related to IEC 61850 applications within and between substations. As of May 2025, the group comprises three IEC Technical Committees:

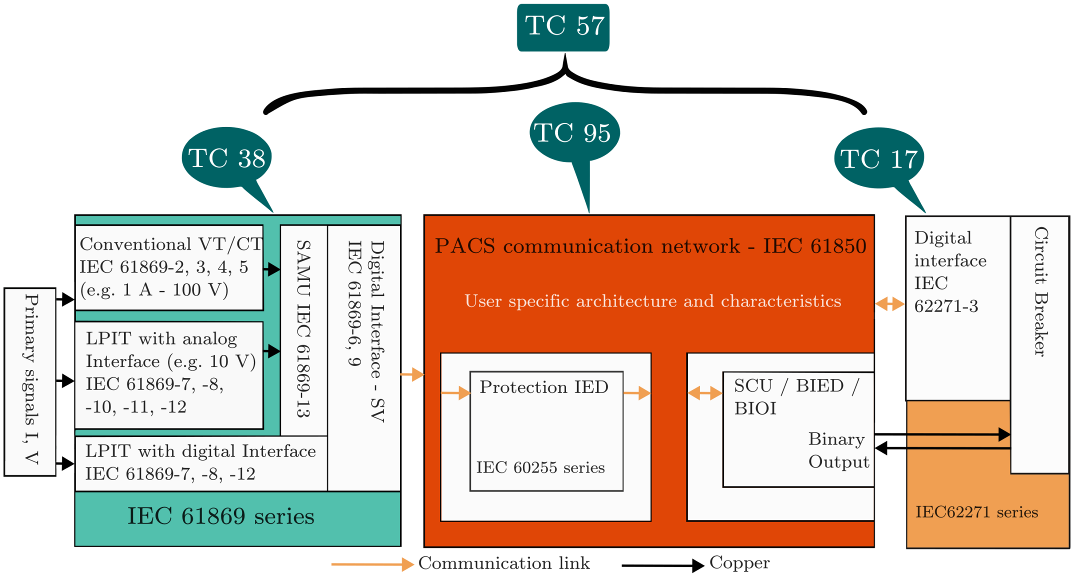


Fig. 10: Protection related elements of an IEC 61850 substation, showing their interactions, responsible IEC Technical Committees, and relevant standards.

- TC 57, responsible for the development and maintenance of the IEC 61850 standard.
- TC 38 (Instrument Transformers), which oversees standards for instrument transformers, including the merging unit functionality and stand-alone merging units Stand-Alone Merging Unit (SAMU) within the IEC 61850 framework.
- TC 95 (Measuring relays and protection equipment), responsible for standards concerning protection relays.

JAG 25 provides a cross-committee platform for coordination and information exchange on IEC 61850 implementation across substations. Participation from other committees, such as Technical Committee (TC) 17 (High-voltage switchgear and controlgear) and TC 13 (Electrical energy measurement and control), is also planned to broaden its impact.

The JAG 25 group officially launched with its inaugural meeting on 11 April 2025, which was hosted by Etch at KU Leuven as part of the IEC working group sessions. Figure 10 illustrates the interactions between components within an IEC 61850-based substation, highlighting their associated IEC Technical Committees and relevant standards. The figure underscores the substantial transformation of protection relays (or protection IEDs) within the context of digital substations, a shift largely driven by the IEC 61850 standard.

Historically, TC 95 (protection equipment) handled analogue-to-digital conversion in protection relays. In digital substations, this function transferred to stand-alone devices under TC 38 (instrument transformers), formalized by the IEC 61869 series, which standardizes MUs and SAMUs.

Despite these changes, the trip contact function - an essential element of protection relays - remains under the remit of TC 95. However, rather than residing within the relay itself, it has been functionally relocated to external devices such as Breaker Control Units (BCUs), Breaker Interface Electronic Devices (BIEDs), or potentially a formally standardized class known as Binary Input/Output Intelligent Electronic Devices (BIOIs). TC 95 is now tasked with defining a standard framework for these devices, ensuring consistent operation, clear functional definitions, and interoperability across digital substations.

Additionally, circuit breakers now often support direct GOOSE reception, enhancing control efficiency and potentially reducing the need for separate BIOIs. The IEC 62271-3 standard, published in 2015, is instrumental in enabling this integration, supporting the broader evolution of digital substations and the roles of protection IEDs within them.

Protection function standardization is notably advanced by TC 95/WG 2 (Protection functions with Digital Input / Output): the adoption of fully digital substations using the IEC 61850 process bus is progressing globally, with utilities advancing from pilot projects to large-scale implementations. As protection systems transition to digital inputs and outputs, IEC TC 95 has taken the lead in standardizing these functions. In 2016, TC 95 established Working Group 2 (TC 95/WG 2) to define the requirements and testing procedures for protection IEDs with digital interfaces, as part of the IEC 60255-1xx series. These protection functions utilize publisher/subscriber communication models, compliant with IEC 61850 (TC 57) and IEC 61869 (TC 38), including Sampled Values (SV) for energizing inputs and GOOSE messages for protection-related inputs and outputs. Beyond communication protocols, these functions also address critical aspects such as data quality, connection status, and time synchronization. The work of TC 95/WG 2 is central to the continued evolution of IEC 60255 standards, with the first standard in this area - IEC TS 60255-216-1, “Digital interface – General requirements and tests for protection functions using digital communication as input and output” [9] - scheduled for publication in 2025.

This article has been accepted for publication in IEEE Transactions on Industry Applications. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIA.2026.3680372

Another interesting development in standardization is IEC TS 63266:2023, published by Joint Working Group 17 — a collaboration between TC 3 (Documentation, graphical symbols, and representations) and TC 57/WG 10 (IED communication and data models). This Technical Specification defines how to represent communication flows in power utility automation, focusing on devices using IEC 61850 for at least part of their data exchange. It proposes structured tabular formats (rather than graphical models) to visualize logical data flows between devices such as merging units, switchgear IEDs, gateways, and digital fault recorders. These formats support testing, maintenance, and system understanding, especially where multiple devices communicate over IEC 61850.

Rather than a universal format, the Technical Specification offers visual representations to help users efficiently interpret and validate communication in digital substations. It complements existing standards by providing a reference-friendly and harmonized view of systems based on IEC 61850. This TS addresses the need to provide the users with a short easy-to-understand documentation to have a clear overlook of the communication structure in the substation but also related to the application. Adherence to the documentation framework proposed in the Technical Specification can mitigate errors arising from the digital nature of IEC 61850 substations, where electro-technical information is numerically encapsulated.

VI. CONCLUSION AND FUTURE WORK

This paper presented a framework and detailed findings from interoperability assessments in an expanded multivendor IEC 61850 laboratory. The work confirms that achieving reliable interoperability requires navigating challenges beyond basic standard conformance. The findings highlight the importance of PTP-compliant network infrastructure, the impact of vendor-specific implementation choices, and the necessity of validating the entire communication chain. The testing framework provided a structured methodology, and the derived recommendations offer practical guidance for similar endeavors.

Future work will focus on completing the top-down workflow transition, expanding functional interoperability testing based on IEC TS 60255-216-1, investigating the application of IEC TS 63266:2023 for representing communication flows, and incorporating cybersecurity testing within our laboratory setup. Practical testing remains essential alongside standardization efforts for successful digital substation deployment.

ACKNOWLEDGMENT

The authors thank Karlheinz Schwarz (Schwarz Consulting) for his feedback and support throughout this research.

REFERENCES

[1] IEC 61850 - Communication networks and systems for power utility automation

[2] C. Naik, T. Brzezinski, C. Bates, J. Schiller, and E. Senkowicz, “Practical Application of IEC 61850 in U.S Substations Compared to Traditional Relay Protection,” in *2024 IEEE Rural Electric Power Conference (REPC)*, pp. 46–53.

[3] C. Guibout, A. Wataré, F. Carli, A. Carbonne, K. Mourier, and T. Rudolph, “Centralized Protection and Control for Transmission System Operations: Practical Applications and Perspectives,” vol. 22, no. 3, pp. 67–78.

[4] R. Mackiewicz, “Overview of IEC 61850 and benefits,” in *2006 IEEE Power Engineering Society General Meeting*, pp. 8 pp.–.

[5] Y. Wu, F. Daraiseh, E. Ramqvist, A. Larsson, and U. Morild, “An implementation of iec 61850 for microgrid control,” in *27th International Conference on Electricity Distribution (CIRED 2023)*, vol. 2023, pp. 409–413, 2023.

[6] R. Huang, E.-K. Lee, C.-C. Chu, and R. Gadh, “Integration of iec 61850 into a distributed energy resources system in a smart green building,” in *2014 IEEE PES General Meeting — Conference Exposition*, pp. 1–5, 2014.

[7] N. Higgins, V. Vyatkin, N.-K. C. Nair, and K. Schwarz, “Distributed Power System Automation With IEC 61850, IEC 61499, and Intelligent Control,” vol. 41, no. 1, pp. 81–92.

[8] G. Keppler, A. Bonetti, S. Canbolat, A. Mumrez, V. Hagenmeyer, and G. Elbez, “Interoperability Assessment of IEC 61850 Devices in a Multivendor Digital Substation,” in *2024 6th Global Power, Energy and Communication Conference (GPECOM)*, pp. 635–640.

[9] IEC TS 60255-216-1 ED1 - Measuring relays and protection equipment - Part 216-1: Digital Interface - General Requirements and Tests for Protection Functions using digital communication as input and output

[10] V. Leitloff, A. Bonetti, H. Chen, L. Xu, S. Baumgartner, C. Bennauer, and C. Byman, “Iec tc95 wg2 – towards a standardisation of an iec 61850 based digital interface for protection functions,” in *16th International Conference on Developments in Power System Protection (DPSP 2022)*, vol. 2022, pp. 92–97, 2022.

[11] UCAIug: UCA International Users Group. (2025), Available: http://www.ucaiug.org/.

[12] A. Ağin, A. Demirören, and î Usta, “A Novel Approach for Power System Protection Simulation via the IEC 61850 Protocol,” vol. 12, pp. 107656–107669.

[13] M. Ayello and Y. Lopes, “Interoperability based on IEC 61850 standard: Systematic literature review, certification method proposal, and case study,” vol. 220, p. 109355.

[14] J. C. Lozano, K. Koneru, N. Ortiz, and A. A. Cardenas, “Digital Substations and IEC 61850: A Primer,” vol. 61, no. 6, pp. 28–34.

[15] G. Elbez, G. Sánchez, S. Canbolat, S. Corallo, C. Fruböse, F. Lanzinger, N. Kellerer, G. Keppler, F. Neumeister, B. Beckert, A. Koziolek, M. Zitterbart, and V. Hagenmeyer, “Insights and lessons learned from a realistic smart grid testbed for cybersecurity research,” in *Proceedings of the 16th ACM International Conference on Future Energy Systems*, ACM, 2025.

[16] E. Y. Song and K. B. Lee, “Hardware-In-The-Loop (HIL) Simulation-based Interoperability Testing Method of Smart Sensors in Smart Grids,” in *2024 IEEE 7th International Conference on Industrial Cyber-Physical Systems (ICPS)*, pp. 1–6.

[17] L. O. Sullivan and M. O. Donovan, “Design of a Lab-Based Digital Substation using the IEC 61850 Standard: Lessons Learned,” in *2024 59th International Universities Power Engineering Conference (UPEC)*, pp. 1–6.

[18] M. Rodriguez, J. Lazaro, U. Bidarte, J. Jimenez, and A. Astarloa, “A Fixed-Latency Architecture to Secure GOOSE and Sampled Value Messages in Substation Systems,” vol. 9, pp. 51646–51658.

[19] A. Cristina Aleixo, R. Dias Jorge, F. Gomes, L. Antunes, J. P. Barraca, R. Carvalho, M. Antunes, D. Gomes, C. Gouveia, A. Carrapatoso, E. Alves, J. Andrade, L. Gonçalves, F. Falcão, B. Pinho, and L. Pires, “Challenges and considerations for the design and implementation of a centralized protection and control solution for MV networks,” in *27th International Conference on Electricity Distribution (CIRED 2023)*, pp. 3328–3332, Institution of Engineering and Technology.

[20] V. Leitloff, F. Fousseret, G. Duverbecq, T. Machkour, Y. Leloup, G. Baron, and T. Michel, “Interoperability challenges for a digitally interfaced functional protection chain,” in *16th International Conference on Developments in Power System Protection (DPSP 2022)*, pp. 86–91, Institution of Engineering and Technology.

[21] Y.-Y. Park, S.-K. Kim, B.-T. Jang, N.-D. Kim, W.-J. Kim, and N.-H. Lee, “Development of the Testing Automation System for verifying interoperability of Digital Substation,” in *2022 6th International Conference on Electric Power Equipment - Switching Technology (ICEPE-ST)*, pp. 363–366, IEEE.

[22] N.-H. Lee, W.-J. Kim, N.-D. Kim, S.-K. Kim, B.-T. Jang, and Y.-Y. Park, “Construction of the Interoperability Test-bed for IEC 61850 based Digital Substation,” in *2022 6th International Conference on Electric*

This article has been accepted for publication in IEEE Transactions on Industry Applications. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIA.2026.3680372

Power Equipment - Switching Technology (ICEPE-ST), pp. 359–362, IEEE.

[23] G. Silva, M. C. Marques, P. Dias, H. Melo, C. Fortunato, A. Pereira, H. Barbosa, and E. Abrantes, "Testing iec 61850 in multi-vendor substation automation system," in *CIRED 2021 - The 26th International Conference and Exhibition on Electricity Distribution*, pp. 1410–1415, Institution of Engineering and Technology.

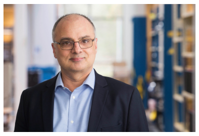
[24] R. Sully, L. Townsend, and S. Dayabhai, "Design considerations of implementing process bus and ptp along an iec 61850-based main line traction power system," in *17th International Conference on Developments in Power System Protection (DPSP 2024)*, vol. 2024, pp. 349–355, 2024.

[25] Wireshark. (2025), Available: https://www.wireshark.org/.

[26] Fink WinPP Protokollsimulator. (2025), Available: https://www.ipcomm.de/product/FinkWinPP/de/sheet.html.

[27] L. O. Sullivan and M. O. Donovan, "Design of a lab-based digital substation using the iec 61850 standard: Lessons learned," in *2024 59th International Universities Power Engineering Conference (UPEC)*, pp. 1–6, 2024.

Gustav Keppler received the M.Sc. degree in mechanical engineering from the Karlsruhe Institute of Technology (KIT), Karlsruhe, Germany, in 2023. He is currently a Research Associate with the Institute for Automation and Applied Informatics (IAI), KIT, working within the Secure Energy Systems (SES) group and KASTEL Security Research Labs. His research interests include the application of Large Language Models (LLMs) for critical infrastructure cybersecurity, threat modeling for secure energy systems, as well as the interoperability and security of IEC 61850 digital substations.



Andrea Bonetti (M'24) received the M.Sc. degree in Electrotechnical Engineering from Sapienza University of Rome, Italy. He has more than 30 years of experience in power system protection and IEC 61850 applications. He has worked with Megger Sweden AB, Hitachi Energy (formerly ABB), and as a consultant in protection engineering. His fields of interest include IEC 61850 standardization, digital substation testing, and relay protection. He is Chair of IEC TC 95 "Measuring Relays and Protection Equipment" and Vice Chair of IEEE PAR 3416. He has lectured at the Royal Institute of Technology (KTH), Stockholm, since 2008, taught professional courses at Lernia University and STF in Sweden, and trained over 2,000 engineers worldwide. Mr. Bonetti received the IEC 1906 Award in 2013 and holds two patents related to IEC 61850 testing algorithms.

Veit Hagenmeyer is Professor of energy informatics with the Faculty of Informatics, and the Director of the Institute for Automation and Applied Informatics, Karlsruhe Institute of Technology, Karlsruhe, Germany. He received the Ph.D. degree from Université Paris XI, Paris, France in 2002. His research interests include modeling, optimization and control of sector integrated energy systems, machine-learning based forecasting of uncertain demand and production in energy systems mainly driven by renewables, and integrated cyber-security of such systems. His email address is veit.hagenmeyer@kit.edu.

Ghada Elbez (Member, IEEE) received the M.Sc. degree in electrical engineering and computer science from the Ecole Polytechnique de Lille, France, in 2016, and the Ph.D. degree from the Informatics Faculty, Karlsruhe Institute of Technology (KIT), Germany, in 2022. She is the Head of the Secure Energy Systems Research Group, KIT, where she is also a Coordinator of the KASTEL Security Lab Energy, Institute for Automation and Applied Informatics. Her research interests include cybersecurity of energy systems, defense mechanisms for early detection of attacks, and security standards. She serves as a reviewer and the chair in different IEEE and ACM conferences. She actively contributes to some German standardization groups within VDI/VDE on the topics of cyber-security in energy systems.