Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.DOI

Impact and vulnerability analysis of IEC61850 in smartgrids using multiple HIL real-time testbeds

MARZIYEH HEMMATI[1], HARSHAVARDHAN PALAHALLI[1], (Student Member, IEEE), GIANCARLO STORTI GAJANI[1], (Senior Member, IEEE) and GIAMBATTISTA GRUOSSO[1], (Senior Member, IEEE)

[1]Dipartimento di Elettronica, Informazione e Bioingegneria, Politecnico di Milano, 20133 Milano, Italy

Corresponding author: GIAMBATTISTA GRUOSSO (e-mail: Giambattista.gruosso@polimi.it)

ABSTRACT Due to the increasing use of smart components in smart grids, interoperability among them is a crucial aspect to address. IEC61850 is a communication standard that has been already used in substations because of its instant data transfer and the ability to enable data exchange between a variety of smart energy-related digital technologies. This article studies the application of the communication protocols defined by the IEC61850 standard in Intelligent Electronic Devices (IEDs) by using a prototype testbed architecture running on a real-time digital device. The goal of this activity is to study the impact of smart simulations and the vulnerability in terms of cyber-security. This testbed includes the supervisor, the substation bus, and the process bus communication layer creating a local network exchanging data at distinct levels. Different fault protection scenarios are discussed using both physical and emulated IEDs, and the communication protocols implemented in each scenario are explained showing that additional delays are introduced.

In the first two scenarios, the operation of the testbed using physical versus emulated IEDs is analyzed and compared, ensuring the robustness of this methodology in situations where the use of a physical IED would be unfeasible. In these scenarios, the functionality and robustness of the protection mechanisms and communication protocols are confirmed.

In the third scenario vulnerability of smart grids that use IEC61850 as their primary communication protocol to data injection attacks is studied. Sniffing the local network, packets are captured and monitored. Spoofed data with the same structure are injected into the network to conduct false data injection attacks on the supervisory unit. Vulnerability to cyber attacks of the IEC61850 protocol in specific situations is shown.

INDEX TERMS Cybersecurity, Digital Twins, GOOSE, Hardware-In-the-Loop, IEC61850, Smartgrids.

I. INTRODUCTION

THe inclusion of a wide range of different components such as controllers, sensors, and actuators, has made the management of modern smart grids more complex. The coordination of Distributed Energy Resources (DERs) combined with storage systems is another necessity in the future of power generation [1]. To achieve optimal performance of all grid components, they are interconnected through a communication network, allowing control in a distributed system and a decentralized manner [2]. Using Intelligent Electric Devices (IEDs) to perform protection and control operations is one of the key points in achieving smart control of these components. Since IEDs adopt IEC61850 as standard communication protocol, they guarantee interoperability between substation devices from different vendors [3], [4]. On the other hand, the disadvantage of substations based on IEC61850 as their primary communication protocol is that cyber-security issues are indisputable. IEC61850's interconnectivity through a local network makes the substation system a suitable target for coordinated cyber-attacks only if the attacker has physical access to one of the local nodes [5].

To analyze different scenarios, full tests are conducted before implementation. These tests often cannot be done directly on the power network due to the need for real-time monitoring and control systems for appropriate decision making; improving the cyber-physical power systems [6], consisting of different communication layers, new challenges are introduced and must be addressed. To study these challenges, the availability of test benches, such as digital twins [7] of the grid, can be useful to forecast the behavior of the grid and validate algorithms and devices [8], [9].

In this work, the Hardware-in-the-loop (HIL) [10], [11] methodology is adopted to simulate the microgrid in a real-time device [12] providing a flexible base architecture for further studies and testing different scenarios. The inclusion of the communication level [13] [5] and the implementation of all three protocols of IEC61850 allowed the investigation of time delays, accuracy and cyber vulnerabilities of GOOSE, SV messages, and MMS protocols.

The motivation behind this work was to create existing communication architecture of a given substation using Typhoon hil software with the built-in IEC61850 protocols in this software instead of using co-simulators which is the common methodology in the most related literature. The implemented testbed topology (the last two scenarios using emulated IED) is shown in Fig.1.

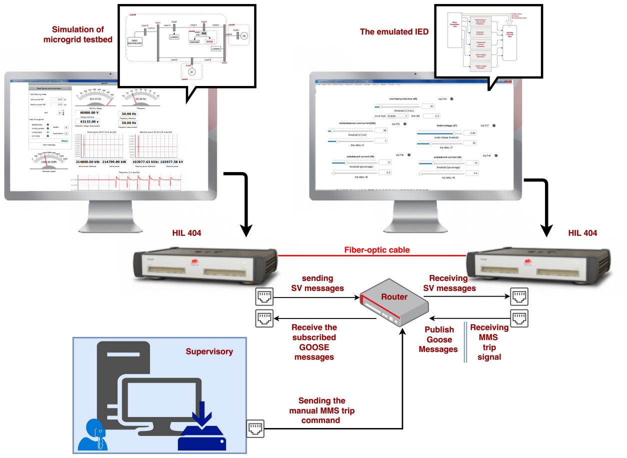

Simulation of microgrid testbed
The emulated IED
HIL 404
HIL 404
Fiber-optic cable
sending SV messages
Router
Receiving SV messages
Receive the subscribed GOOSE messages
Publish Goose Messages
Receiving MMS trip signal
Supervisory
Sending the manual MMS trip command

FIGURE 1. Physical topology of the created testbed (scenario 2 and 3)

Many aspects of microgrids are covered as contributions of this project, with three different scenarios conducted in the designed real-time testbed.The main original contributions of the work presented in this article are as follows:

- Emulation of IEDs in real-time hardware along with protection logic and its integration into the simulated smart grid network.
- Integration of the layers of the IEC61850 GOOSE, SV messages, and MMS communication protocol in the real-time electrical grid simulation.
- Test of the emulated IED's protection logic for short circuit current protection, overload protection, network unbalance tests, and analysis of the performance of our grid in these fault scenarios.
- Further use of the testbed to study the vulnerabilities of the IEC61850 communication protocol to false data injection in case of man-in-the-middle cyber security threats.

In the following, a brief review of the related literature is given in section II. Then the main body of work is presented in section III where implementation and investigation of each one of the three scenarios is shown. In the first scenario, described in III-A, **communication latency** is investigated using **physical IEDs**. Since testing coordination strategies in sophisticated networks requires multiple IEDs, in the second scenario, given in III-B, an **emulated IED**, running real-time on a HIL device, is designed so that the physical constraints associated with the characteristics of expensive physical IEDs are considered. In the third scenario, presented in III-C, **DERs** are considered in the model using the same microgrid with the inclusion of an Electric Vehicle Charging Station (EVCS) and a PV plant that substitutes one of the generators. A **man-in-the-middle** attack is performed on the network, causing the isolation of the EVCS. Finally, in Section IV, recalls the main results of this project and suggests interesting topics to consider in future studies.

II. RELATED WORKS

Recent work addresses the behavior of the power grid in an environment where cyber attacks occur, which is one of the objectives of this study. In the next section, some of them are briefly presented.

Some previous studies addressed the construction of an experimental framework to approximate the IEC61850 standard [14] [15] [16], considering physical constraints while maintaining scalability, to ease the way for more complex power grid implementations. The authors in [15], investigated complex protection coordination using the Arcteq-F215 IED. Their work redefines the relationship between primary and backup protection for microgrid protection. They employed Directional Over-Current (DOCR) [17] IEDs to achieve protection coordination without using the inverse time characteristics. The status of the direction of the fault currents is communicated between the IEDs via fast GOOSE messages. Several IEDs were used to build the presented microgrid, and further study is limited only to them. The platform they created is an offline simulation, which is not the best approach for studying communication systems.

In [18] and [19], the authors analyzed cybersecurity vulnerabilities associated with the communication protocol. The authors built real-time simulated grid testbeds and connected them to physical IEDs using Hardware-In-the-Loop (HIL) technology. The testbed used consists of three IEDs connected to a microgrid running on a Real Time Digital Simulator (RTDS). One of these IEDs receives the measurement signals of voltages and currents from the RTDS via SV messages and uses GOOSE to communicate the status. The other two are partially IEC61850 compliant, which means that they are hardwired and receive analog signals from the RTDS via power amplifiers. Although the use of HIL is one of the most suitable strategies to approach Cyber-Physical Systems (CPS), it may sacrifice other complex structures with multiple physical IEDs.

Few works considered more aspects of building an extensive testbed, such as [20]. The authors used a methodology in which some IEDs are connected to a HIL RTDS environment. In their topology, each of these physical IEDs represents 32 emulated circuit breakers. Considering the protection strategy, if a state change is approved, the relay issues the corresponding command (trip or close) to the breaker to operate. This relay also responds to signals from the Supervisory Control And Data Acquisition (SCADA) server that allowed authors to build a SCADA-training-based environment of the CPS security testbed. Their presented protection logic is executed in the RTDS instead of the physical IEDs, and this methodology allows the control center to control 64 relays through each zonal substation Remote Terminal Unit (RTU) instead of just two physical IEDs per RTU. The results of the discussed work showed that performing protection mechanisms on a RTDS did not significantly change the expected behavior of an IED. This algorithm promotes scalability of the testbed at the CPS interface layer, by allowing only one physical relay to perform multiple IED operations. This idea was used to develop the emulated IED in the second and third scenarios presented.

In [21], the authors invested in describing a man-in-the-middle cyber attack in a lap setup that includes a photovoltaic inverter. However, the inverter itself does not have IEC61850 capabilities, the MMS protocol is added using Raspberry Pi (R-Pi) hardware that performs as a gateway to connect the SCADA to the PV simulator through the inverter's inbuilt Modbus interface. Comprehensive details on the man-in-the-middle attack on MMS are presented, but the lab setup does not include other IEC61850 (GOOSE and SV) protocols.

In order to contribute to this topic, our project focuses on the aspects not fully addressed in other related works discussed in this section, introduces an emulated IED in the second scenario, and compares the working accuracy of the physical IED in the first scenario with the emulated one. In addition, distributed renewable energy sources and loads are added to the network, and an attack situation is discussed in the last scenario. This work is unique in deploying all three protocols in a scalable testbed (by introducing a generic E-IED) and analysing the communication delays related to each communication layer (substation, bay level, and process level) in an innovative way using real-time simulation with built-in IEC61850 capabilities without the use of co-simulations.

III. IMPLEMENTATION AND RESULTS

In this work, the testbed grid is selected based on the power system network presented previously in [4]. However, nominal values are modified for the test scenarios presented here. The nominal voltage of the grid is 120 kV and the working frequency 50 Hz, there are three constant power loads present in the base grid that consume 700 kW in total and two Diesel Generators (DG) whose nominal parameters are presented in table 1; the two DGs provide 600 kW of the total power while the rest is delivered from the slack node in bus13. The general design details related to the components used and the software memory assigned to each subsystem in the grid modeling are also given in [4].

TABLE 1. Nominal values for both DGs

Nominal active power (P_n)	300 kW
Nominal generator line voltage (V_{1L_n})[a]	12 kV
Nominal grid line voltage (V_{2L_n})	120 kV
Nominal frequency (F_n)	50 Hz
Nominal mechanical speed (N)	1800 rpm

[a]The ratio of the internal transformer is 10

In the following, three different scenarios are described to expand the concept of the scalability of this testbed. Each procedure practices another aspect of the designed testbed and will be built on top of the previous one.

A. FIRST SCENARIO

The first scenario is mainly concerned with incorporating physical IEDs as the hardware under test using Hardware-In-the-Loop (HIL) methodology. whose logical decisions and communication timing scenarios are examined. The IEDs used in this experiment uses IEC61850 as their communication protocol. The communication scheme in this implementation consists of all three layers: the supervisory layer, the substation, and the process bus communication layer (shown in Fig.2). This architecture is similar to the substation automation topology based on IEC61850 presented in [22] and [23] . These physical IEDs communicate with the HIL SCADA panel of the microgrid through the MMS server (supervisory layer), while they use GOOSE messages to communicate their status with each other (substation bus layer), and acquire the sample value (SV) messages that are generated, time stamped and synchronized in Merging Units (MUs) implemented inside the simulation. These MUs receive current samples from measurement instruments and then convert them to digital data packets.

The sketch of the test setup used for this scenario is shown in Fig. 3. Initially, the circuit breakers (CBs) on line (3-4) are in the closed position, and the circuit breaker on line (2-3) is in the open position so that bus3 is powered by bus4. The circuit breakers receive the trip command and status from their corresponding IEDs via a hardwired cable from the input terminals of the HIL device, and the IEDs receive the measurement signals via the Ethernet port from the MUs implemented in the microgrid.

In the event of a fault in line (3-4), only IED1, which corresponds to CB1, would detect the short-circuit current and respond to this short-circuit by issuing a trip command for instantaneous short-circuit protection. At the same time, CB2 is still in the closed position and supplies Bus3 via the other redundant lines, so that the fault continues to be supplied with power and can cause further damage to the network components.

To solve this problem, IEDs are preprogrammed to exchange protection GOOSE messages to isolate the faulty section of the network. When the faulty line is isolated, IED3

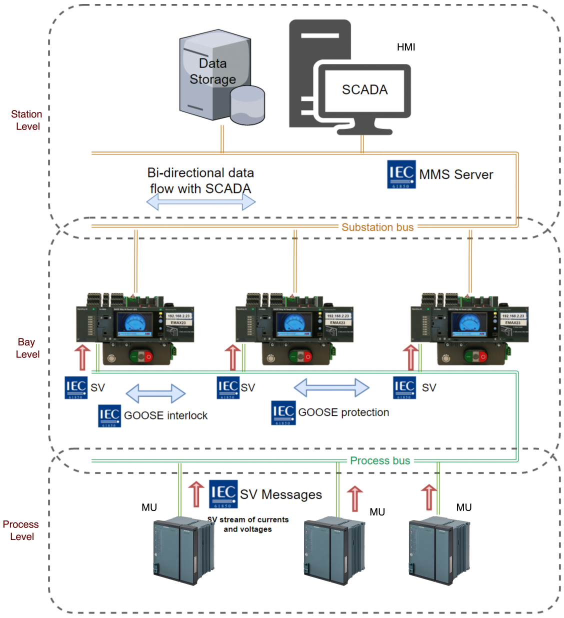


FIGURE 2. Communication layer illustration of the first scenario

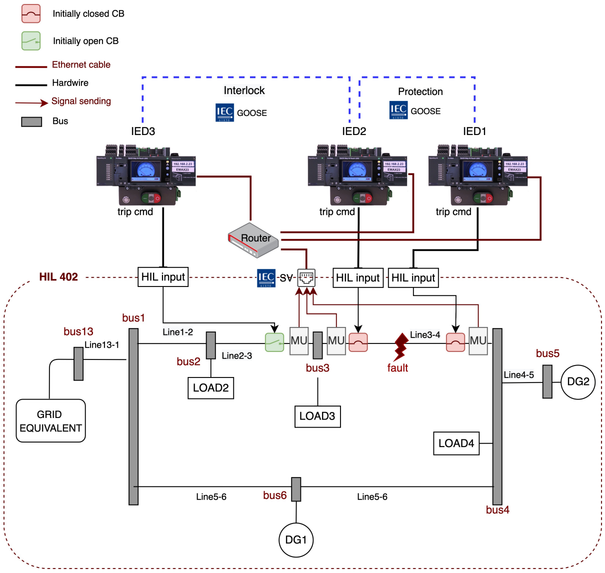


FIGURE 3. Implementation architecture of the first scenario setup

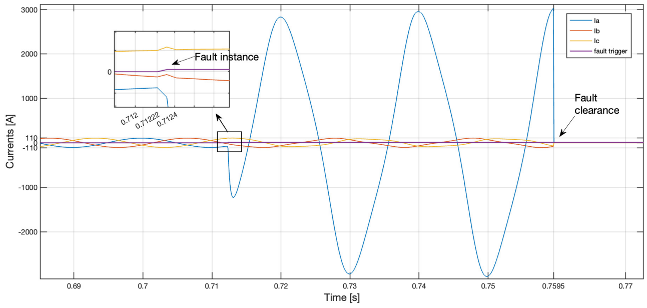


FIGURE 4. Scenario 1: the instance of injection of a single-phase fault and the decay time according to the MU connected to IED2.

sends a turn-on command to CB3 in the line (2-3) to supply power to Bus3; this way, we can ensure a seamless power supply with the shortest possible interruption time.

When IED3 receives the interlock GOOSE message from IED2 confirming that the status of CB2 is Off (it is in the open position), CB3 closes. Current measurements acquired by the measurement unit in conjunction with IED1 at the time of fault occurrence are shown in Fig.4.

As shown, the fault was triggered at $0.712\,22\,\mathrm{s}$ of the captured time window and cleared at $0.7595\,\mathrm{s}$, so there is a time difference of $47.28\,\mathrm{ms}$ from the onset of the fault to the interruption. This delay until the fault is cleared corresponds to the delay caused by the digital-to-analog converters, the delay of the communication network protocol in packing and unpacking the data, the processing time of the IED to detect the fault, which can be set in the configuration of the IED in terms of priority of each type of fault detection, and also the delay of the real-time simulator in tripping the circuit breaker after the trip command received via GOOSE.

Currents measured at load3 connected to bus3 are shown in Fig.5. The fault occurred at $0.7123\,\mathrm{s}$, CB1 opens, and isolation of the faulty line is performed at $0.759\,555\,\mathrm{s}$ by opening CB2 and CB3 is turned on (with a close command from IED3 via GOOSE) to power the load at $0.786\,34\,\mathrm{s}$. Thus, the power supply to load2 is only interrupted for about $74.04\,\mathrm{ms}$ in total.

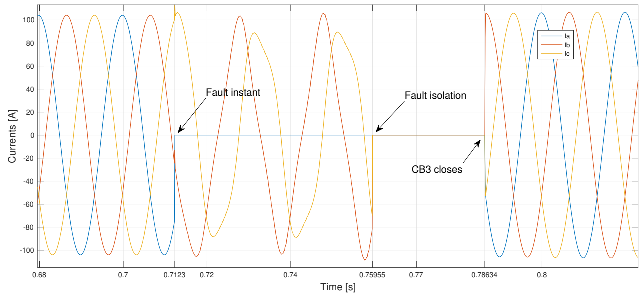


FIGURE 5. Scenario 1: Current measurements at load3 before and after the fault. Before the closure of CB3, the load current is interrupted for a small period.

In Fig.6, IED2 is taken as an example to illustrate the time delay between when the IED is tripping and when the GOOSE message is issued to update the CB status for the other IEDs. A difference of $12.7\,\mathrm{ms}$ delay in issuing the GOOSE message is shown. The communication delay for the other IEDs can also be plotted, but should be more or less the same.

B. SECOND SCENARIO

In the second scenario, instead of physical IEDs, an identical emulated IED running on a real-time device is developed and these two real-time simulators are synchronized using an optical fiber network. In this way, time signals aligned with the master HIL device can be available at the slave

This article has been accepted for publication in IEEE Access. 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/ACCESS.2022.3209698

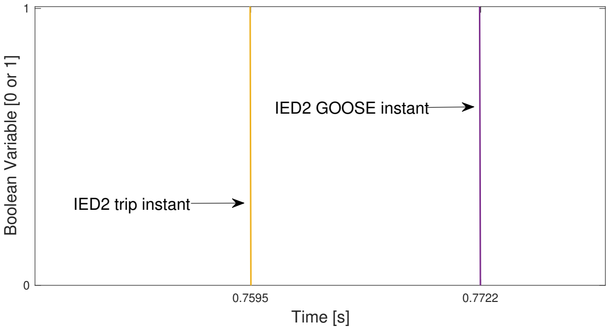


FIGURE 6. Scenario 1: the delay related to the CB status issued by IED2 via GOOSE message and the actual status directly measured of trip coil voltage present in the IED2

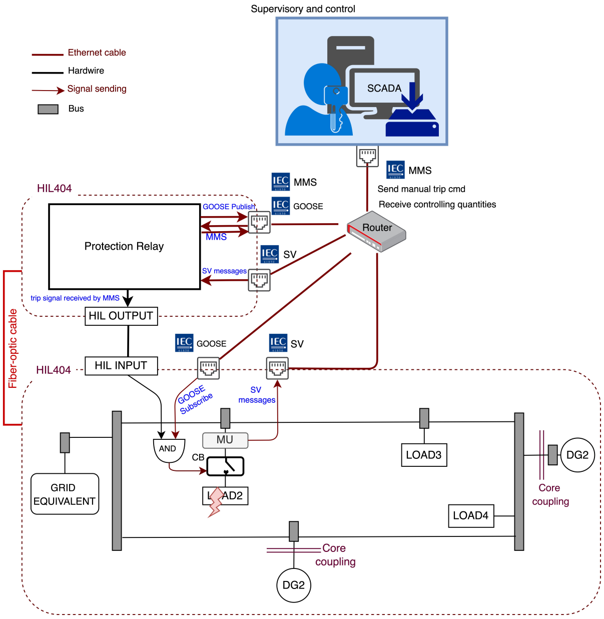


FIGURE 7. Implementation architecture of the second scenario setup

HIL device. This emulated IED allows the investigation of communication protocols, particularly IEC61850, even when no real IED device is at hand. Since the test bench is running in real-time, the challenges associated with cyber-physical systems are also present in this test setup, and the communication delay between devices can be measured as in the previous scenario. The 404 Typhoon HIL device used in this scenario can run up to 12 emulated IEDs to implement complex network configurations.

In real-world protection systems in the field (High voltage), the logic unit is usually installed far from the circuit breakers in the grid since it should be placed where the operators can access the device to change the configuration if needed. Here, to implement the scenarios as close to reality, the protection relay (logical unit of the IED) works on another HIL device and communicates with the circuit breaker implemented inside the microgrid using the communication layer created between two HIL devices. Conventionally, in the communication architecture, GOOSE is used for horizontal communication between IEDs at bay level (interlock and protection). To apply the same concept here, bay level protection signals are communicated through GOOSE. The hardwired connection between two HILs, on the other hand, is only for the sake of interconnection. By wiring the MMS command directly to the CB, it is possible to capture pure MMS delay for this study.

Here, a simple overload test scenario is presented to investigate the test bench shown in Fig.7. As shown in the sketch of the setup, the microgrid used is the same as in the first scenario, but here an overload event occurs at load 2. As mentioned above, the setup consists of two HIL devices, one of which resembles the microgrid testbed, and the other is the virtual IED. These two devices are connected via a router that resembles the gateway and demonstrates communication over the substation bus.

When the fault occurs, the emulated IED receives the sampled values of the measured currents and voltages. The emulated IED publishes a trip signal through the GOOSE publisher by comparing the measured currents with the protection setpoints. The GOOSE subscriber receives this signal inside the microgrid, and this means that one of the input signals to the logical AND became zero. As a result, the output of the logical AND is set to zero and the CB trips. The CB implemented in the microgrid responds to both the MMS pushed command from the monitoring unit and the GOOSE message command received from the IED in the event of fault detection.

The protection relay in the emulated IED analyzes the readings sent from MU and sends a trip command when the setpoints of a protection mechanism are violated. In this case, the GOOSE publisher in the emulated IED publishes a trip command over the Ethernet port. The GOOSE subscriber that triggers the corresponding CB subscribes to the GOOSE messages published by the relay. It triggers the CB when it receives the trip command signal. Different applications may require less frequent or more frequent status updates, which can be set accordingly. In this implementation, the execution time is set to 100 µs.

For each implemented protection mechanism, there are separate setpoints that can be set from the SCADA control panel of the emulated IED. In particular, for the overload protection (Ansi 49), which is the subject of this scenario, there are three characteristic curves to choose from in the SCADA panel (there are two other curves defined in the ANSI standard [24], which are mainly used for 60 Hz systems; therefore, they are neglected in this simulation). As shown in the $I-t$ curve (Fig.8), the relay logic unit calculates the time delay according to the selected curve for the given threshold current.

As shown in Fig. 9, the communication layer created consists of the supervisory, substation, and process bus level. The MMS pushed trip command is issued from the supervisory communication layer, it is received by the emulated IED

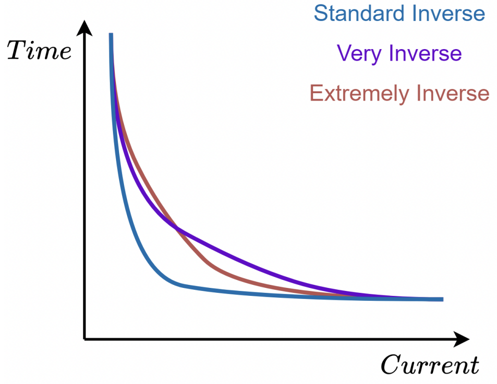


FIGURE 8. Ansi49 overload I-t curves implemented in the relay logic

located in the substation bus communication layer, then IED send this command signal to the circuit breaker located in the process bus communication layer. To mimic physical contact between the IED and the CB, the HIL output and input terminals (Hardwired communication) are used to connect the two devices and send the trip signal.

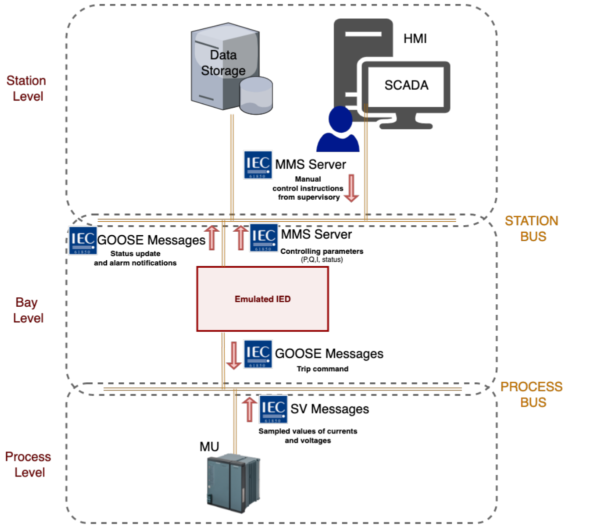


FIGURE 9. Illustration of the communication layer of the second scenario. [22]

As mentioned earlier, the CB also responds to the manual trigger command by monitoring the unit via the MMS server. The IED Explorer software installed on the SCADA device allows the supervisor to receive the quantities published by the MMS server implemented in the emulated IED. It is also possible to change the status of the IED manually in the configured direction of the MMS package `DRCC1.ST.Beh.stVal` as shown in Fig.10. This setup can be used to monitor control quantities such as active power, reactive power, apparent power, current magnitude, and angle.

Fig.11 shows the measured values sent by the IED via the MMS server from the MU connected to the CB before tripping. These data can be found in the *DataSets* directory of the `LLN0.MEASUREMETS` file, as shown in the figure.

The update frequency of the measurement can be set using the highlighted window at the top of the interface. This value only indicates the MMS packet rate captured by the monitoring unit and is independent of the execution rate set in the MMS server setup in the emulated IED.

After the circuit breaker is tripped (using GOOSE messages from the emulated IED or manually from the monitoring unit via the MMS server), the corresponding measurements received from the MMS server implemented in the emulated IED are displayed in Fig. 12.

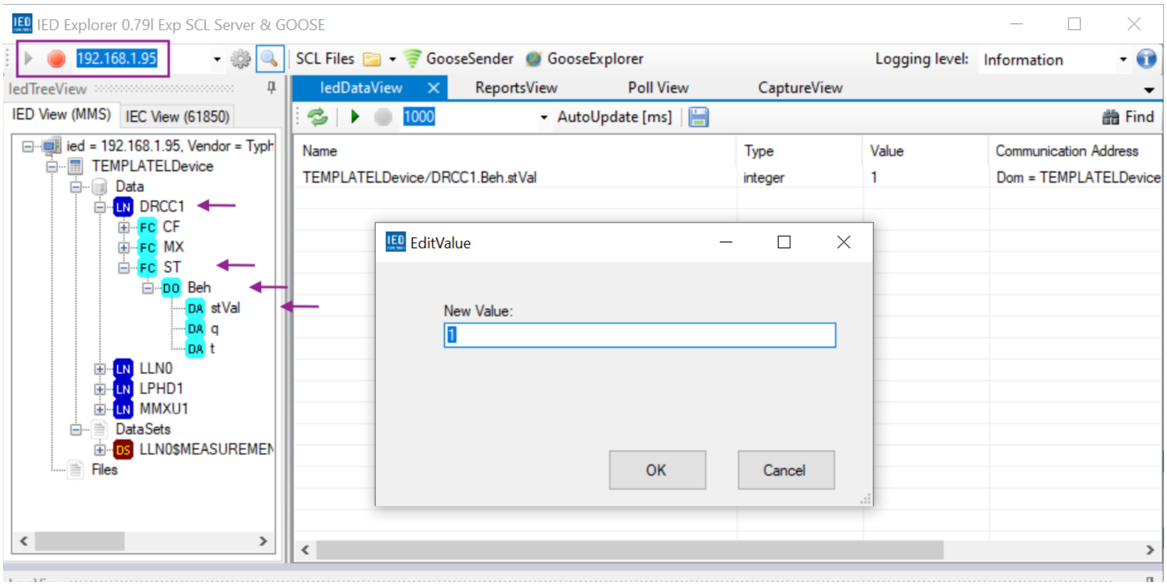
The same measurements are also collected from the simulated MU in the microgrid at the time of the MMS pushed command to capture the communication delay time. The circuit breaker was tripped upon receiving the MMS trip signal. Note that, as mentioned earlier, this signal was transmitted over a hardwired cable from the emulated IED running on the other device to the main microgrid to avoid further delays associated with GOOSE. In the enlarged window in Fig.13, you can see the MMS trigger command at time 0, represented by arrow 1, arrow 2 shows the beginning of the closure of CB, and 500 µs after sending the MMS command, the CB is fully closed, represented by arrow 3. Arrow 4 marks the time when the monitoring unit can observe the status change of CB at 900 µs after the MMS pushed command.

The time delay between the publication of the trip command through the MMS server in the supervisory communication layer and the tripping instant of the circuit breaker would indicate the MMS server communication delay (500 µs) in this experiment. When the time delay is calculated by checking the timestamp of the writing of *stVal* and comparing it with the time of the circuit breaker status change recorded by the SCADA, the additional delay of 400 µs related to the status change of CB is also considered, which shows that it is not accurate. In this experiment, the calculated time delay using the described method is 1 ms.

An unbalanced current spike and an overload event are injected into load2 to capture the results by the emulated IED protection functions. As expected, the GOOSE message published by the IED was received by the GOOSE subscriber without noticeable delays. The captured measurements for these two experiments are shown in Fig.14 and Fig.15 respectively. The time delay between the occurrence of the fault and the time of fault clearing from the acquired results is consistent with the expected time for fault clearing set by the setpoints for the time dial and threshold for the protection mechanisms under study (overload and unbalanced current). Therefore, changing the configuration of the setpoint on the SCADA control panel of the emulated IED would result in the desired time delay according to the protection strategy.

C. THIRD SCENARIO

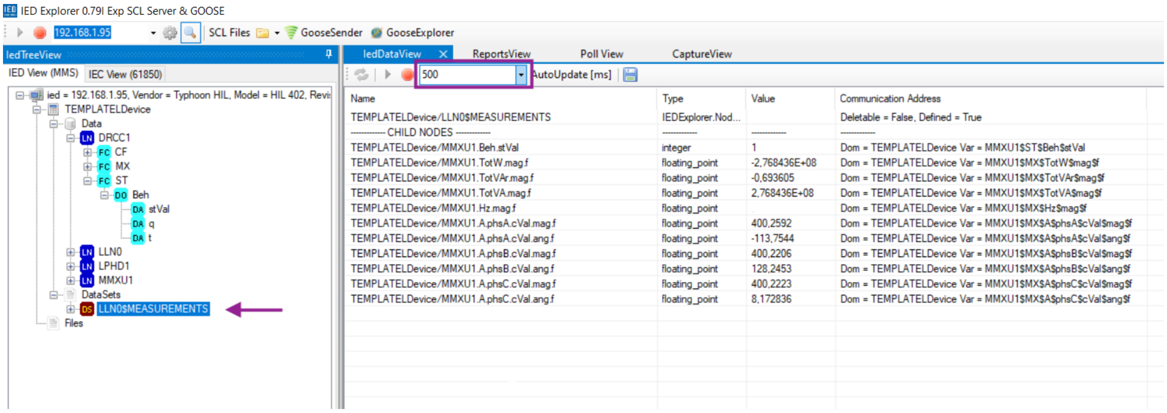
As shown in the outline of the setup in Fig.16, the base microgrid used is similar to one of the first scenarios with a different protection system and inclusion of a low voltage level Electric Vehicle Charging Station (EVCS) working at



Name	Type	Value	Communication Address
TEMPLATELDevice/DRCC1.Beh.stVal	integer	1	Dom = TEMPLATELDevice

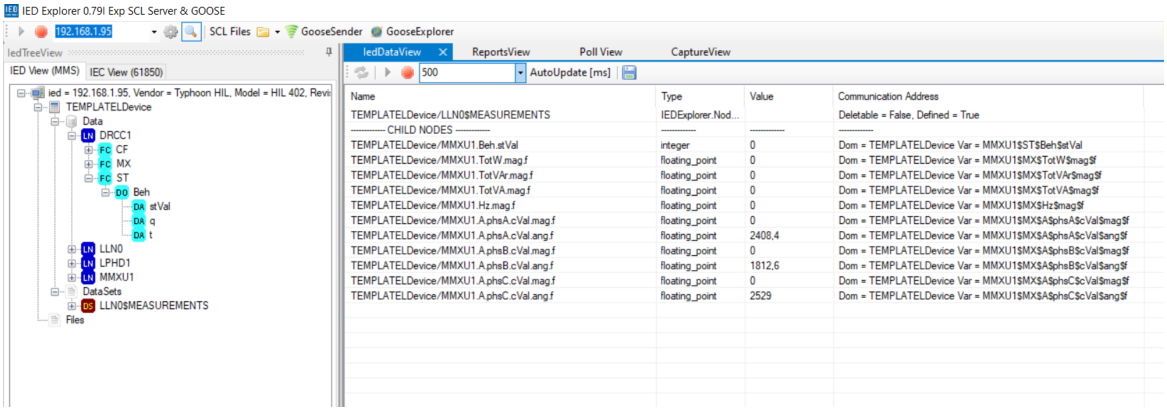
New Value: 1

FIGURE 10. Manually writing the IED status using the IED Explorer software that runs on the SCADA system via the MMS server.



Name	Type	Value	Communication Address
TEMPLATELDevice/LLN0$MEASUREMENTS	IEDExplorer.Nod...		Deletable = False, Defined = True
------------ CHILD NODES ------------	------------	------------	------------
TEMPLATELDevice/MMXU1.Beh.stVal	integer	1	Dom = TEMPLATELDevice Var = MMXU1$ST$Beh$stVal
TEMPLATELDevice/MMXU1.TotW.mag.f	floating_point	-2,768436E+08	Dom = TEMPLATELDevice Var = MMXU1$MX$TotW$mag$f
TEMPLATELDevice/MMXU1.TotVAr.mag.f	floating_point	-0,693605	Dom = TEMPLATELDevice Var = MMXU1$MX$TotVAr$mag$f
TEMPLATELDevice/MMXU1.TotVA.mag.f	floating_point	2,768436E+08	Dom = TEMPLATELDevice Var = MMXU1$MX$TotVA$mag$f
TEMPLATELDevice/MMXU1.Hz.mag.f	floating_point		Dom = TEMPLATELDevice Var = MMXU1$MX$Hz$mag$f
TEMPLATELDevice/MMXU1.A.phsA.cVal.mag.f	floating_point	400,2592	Dom = TEMPLATELDevice Var = MMXU1$MX$A$phsA$cVal$mag$f
TEMPLATELDevice/MMXU1.A.phsA.cVal.ang.f	floating_point	-113,7544	Dom = TEMPLATELDevice Var = MMXU1$MX$A$phsA$cVal$ang$f
TEMPLATELDevice/MMXU1.A.phsB.cVal.mag.f	floating_point	400,2206	Dom = TEMPLATELDevice Var = MMXU1$MX$A$phsB$cVal$mag$f
TEMPLATELDevice/MMXU1.A.phsB.cVal.ang.f	floating_point	128,2453	Dom = TEMPLATELDevice Var = MMXU1$MX$A$phsB$cVal$ang$f
TEMPLATELDevice/MMXU1.A.phsC.cVal.mag.f	floating_point	400,2223	Dom = TEMPLATELDevice Var = MMXU1$MX$A$phsC$cVal$mag$f
TEMPLATELDevice/MMXU1.A.phsC.cVal.ang.f	floating_point	8,172836	Dom = TEMPLATELDevice Var = MMXU1$MX$A$phsC$cVal$ang$f

FIGURE 11. Monitoring the measurements sent by the IED MMS server before the trip.



Name	Type	Value	Communication Address
TEMPLATELDevice/LLN0$MEASUREMENTS	IEDExplorer.Nod...		Deletable = False, Defined = True
------------ CHILD NODES ------------	------------	------------	------------
TEMPLATELDevice/MMXU1.Beh.stVal	integer	0	Dom = TEMPLATELDevice Var = MMXU1$ST$Beh$stVal
TEMPLATELDevice/MMXU1.TotW.mag.f	floating_point	0	Dom = TEMPLATELDevice Var = MMXU1$MX$TotW$mag$f
TEMPLATELDevice/MMXU1.TotVAr.mag.f	floating_point	0	Dom = TEMPLATELDevice Var = MMXU1$MX$TotVAr$mag$f
TEMPLATELDevice/MMXU1.TotVA.mag.f	floating_point	0	Dom = TEMPLATELDevice Var = MMXU1$MX$TotVA$mag$f
TEMPLATELDevice/MMXU1.Hz.mag.f	floating_point	0	Dom = TEMPLATELDevice Var = MMXU1$MX$Hz$mag$f
TEMPLATELDevice/MMXU1.A.phsA.cVal.mag.f	floating_point	0	Dom = TEMPLATELDevice Var = MMXU1$MX$A$phsA$cVal$mag$f
TEMPLATELDevice/MMXU1.A.phsA.cVal.ang.f	floating_point	2408,4	Dom = TEMPLATELDevice Var = MMXU1$MX$A$phsA$cVal$ang$f
TEMPLATELDevice/MMXU1.A.phsB.cVal.mag.f	floating_point	0	Dom = TEMPLATELDevice Var = MMXU1$MX$A$phsB$cVal$mag$f
TEMPLATELDevice/MMXU1.A.phsB.cVal.ang.f	floating_point	1812,6	Dom = TEMPLATELDevice Var = MMXU1$MX$A$phsB$cVal$ang$f
TEMPLATELDevice/MMXU1.A.phsC.cVal.mag.f	floating_point	0	Dom = TEMPLATELDevice Var = MMXU1$MX$A$phsC$cVal$mag$f
TEMPLATELDevice/MMXU1.A.phsC.cVal.ang.f	floating_point	2529	Dom = TEMPLATELDevice Var = MMXU1$MX$A$phsC$cVal$ang$f

FIGURE 12. Monitoring the measurements sent by the IED MMS server after the trip.

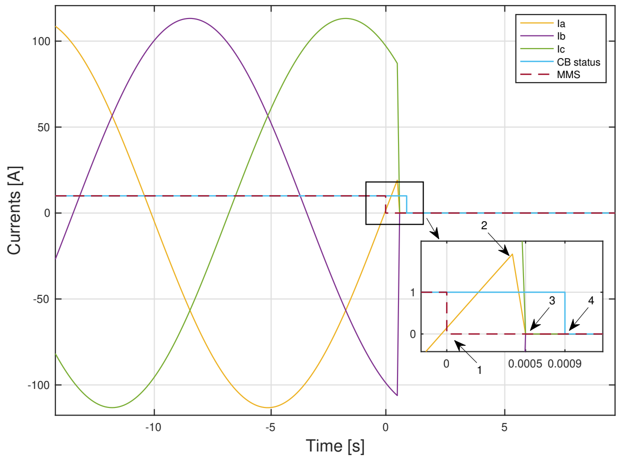


FIGURE 13. Scenario 2: time instance of the MMS pushed trip. Arrow 1: MMS trigger command, arrow 2: CB starting to trip, arrow 3: CB fully closed, arrow 4: CB status seen in the monitoring unit is changed.

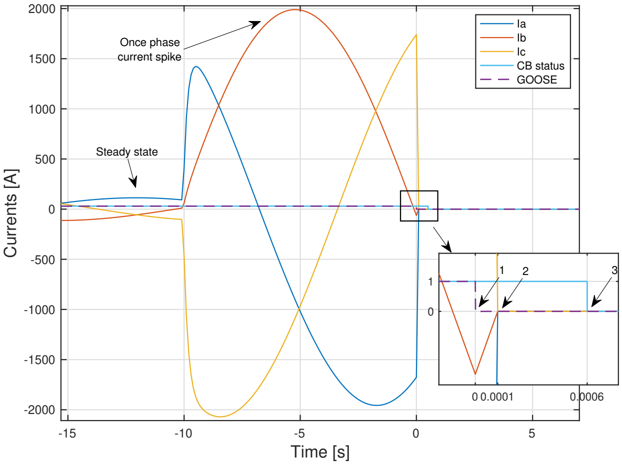


FIGURE 14. Scenario 2: Time instance of the unbalanced current spike and the clearance of unbalanced currents via GOOSE messaging. Arrow 1: GOOSE message received, arrow 2: CB fully tripped, arrow 3: CB status change initiates, arrow 4: CB status changed.

400 V. As in the previous scenario, two HIL devices are present; one of them acts as the microgrid testbed, and the other is designed to perform as an IED. The communication architecture remains the same, but the emulated IED is connected to the circuit breaker of the EVCS. This way, the created private Local Area Network (LAN) is where the charging station is located.

As in the previous scenario, the protection relay inside the emulated IED analyzes the measurements of currents and voltages, and in case of violation, sends a trip signal via GOOSE. The monitoring unit also has access to change the status of the circuit breaker in case of emergency, and this can be done as described in the previous scenario.

The monitoring unit and the created LAN communicate through MMS messages. These MMS messages are not encrypted because they are not widely spread and can only be manipulated by physical access to the network. In general,

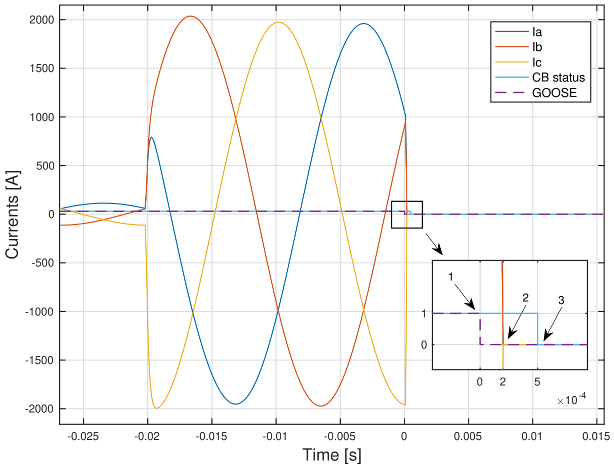


FIGURE 15. Scenario 2: time instant of the overload event and the clearance via GOOSE messaging. Arrow 1: GOOSE message received, arrow 2: CB fully tripped, arrow 3: CB status change in SCADA.

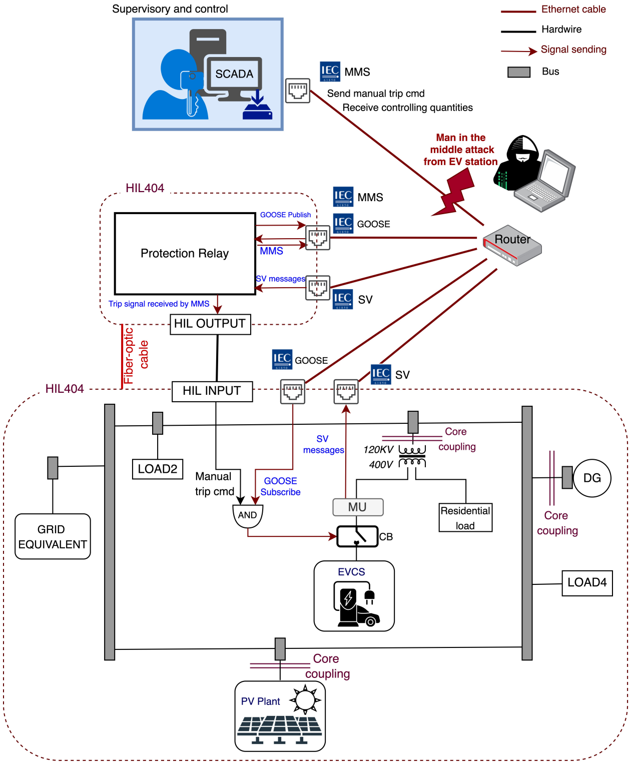


FIGURE 16. Outline of the third scenario including the communication layer.

to have physical access, the attacker would have to be able to reach the engineering site, since the IEC61850 protocol is adopted by IEDs working at higher voltage level. But in the event that this protocol is used for the EVCS, physical access can be granted to the individuals responsible for these charging stations and fewer safety protocols are adopted. In this type of situations the attacker may have the possibility to access the network easily through *social engineering* methods [25], [26].

This scenario is focused on demonstration of how cyber-attacks can be performed on this testbed. The first step is to understand the data structure of the communicated MMS messages. The information model of the E-IED is defined using the library provided by the real-time simulating device, and, for the physical IED, it is defined using the operation software provided by the manufacturer of the IED. The client model is implemented in an external PC connected to the same physical network and running IED-Explorer software [27]. Fig.17 shows the different layers of a MMS packet issued by the emulated IED. As shown, there are four Logical Nodes (LN). The measured data such as the values of powers, frequency, voltages, and currents are stored in the MMXU1 logical node, which has the same sub-layers as shown for the DRCC1 logical node.

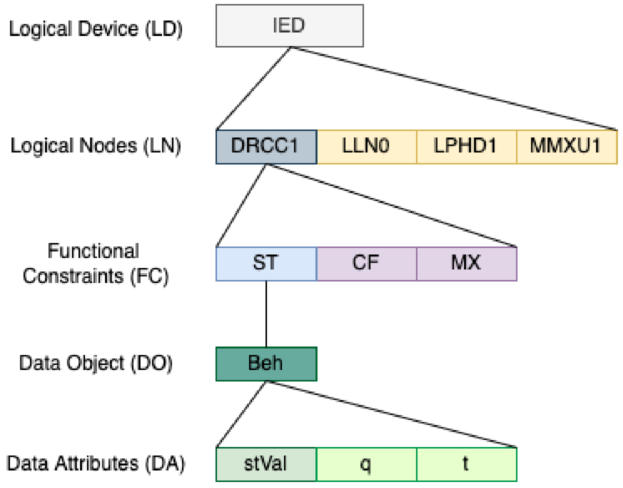


FIGURE 17. Data structure of the MMS packets communicated by the emulated IED.

As shown in Fig.16 a man-in-the-middle (MITM) attack is performed by accessing the charging station communication network. MMS packets are captured for Δt amount of time, and the monitoring values under the MMXU1 logical node can be read. Then the spoofed data is created by modifying only the status of the CB stored in the Data Attribute (DA) for all the packets captured in time Δt, and then this series of false data (Δt amount of false data) is sent to manipulate the data written by the IED in the logical node DRCC1 over and over again. In this way, the status of the CB is changed so that all the measured values by the MU are zero. However, the data that is read from the MMXU1 logical node by the monitoring unit still display healthy measurements.

The man-in-the-middle (MITM) attack is aimed at the application layer (layer 7). In the MITM attack, the goal of the attacker is to insert himself, unnoticed, between two or more communicating parties. The victims are not aware of the presence of a third party and believe they are directly in contact to each other since the attacker acts as a communication channel and relays the messages between the victims [21], [28]. In this way, the attacker has the possibility of hijacking the exchanged information and, possibly, making independent changes in the information exchanged by the victims.

The algorithm below illustrates the script written to perform this attack on the network in pseudo-code.

Algorithm: injection of spoofed MMS measurements

```
START
Captured_Messages = capture_MMXU1_messages(t)
Spoofed_Messages  = []
for MMXU1_message in Captured_Messages:
  Spoofed_Messages.add(modify_stVal(MMXU1_message))
for(i=0, i<=1000, i++):
  send_to_DRCC1(Captured_Messages)
END
```

Fig.18 displays the time instant of the attack captured directly from the MU implemented in the microgrid. As shown, after running the written algorithm, the trip command is sent to the CB and the EVCS is isolated from the grid. However, the monitoring unit receives the manipulated data that show that EVCS is still connected to the grid and is performing in a healthy state.

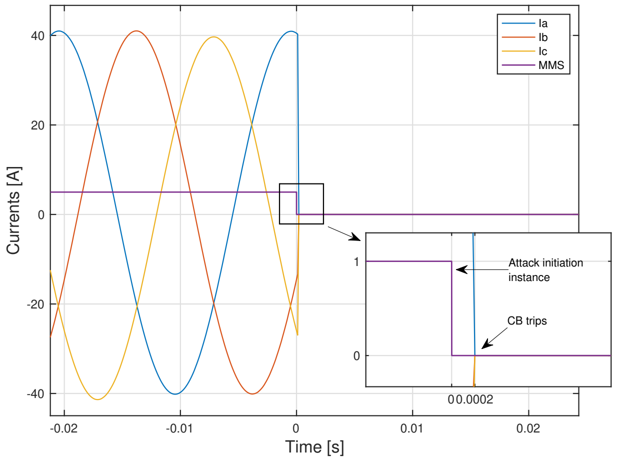


FIGURE 18. Scenario 3: time instant of the injected trip signal by the attacker and isolating the EVCS from the network

IV. CONCLUSION

Cyber-Physical Systems (CPS) are widely used as modern infrastructure to achieve faster and more reliable power grids. The IEC61850 communication protocol is one of many steps towards automated protection mechanisms that lead to smarter and more sophisticated grids. However, there are still challenges that need to be addressed, especially concerning the cyber vulnerabilities of this protocol.

The proposed test environment and the discussed scenarios contribute to analyzing the delay of the communication, the accuracy of the transmitted data, and the cybersecurity vulnerabilities of a generic IED equipped with GOOSE messages, SV messages, and the MMS server protocol of the IEC61850 standard. The experiments executed here used both physical IEDs and a designed Emulated IED. The design detail related to the protection mechanisms of this emulated IED is discussed to facilitate building complex-coordination protection networks.

The objective of creating a testbed to study scenarios for implementing protection logic in a power system was achieved. Three different scenarios were evaluated. The first scenario shows how the IEDs are coordinated to isolate the fault in a redundant microgrid using IEC61850. The simulation also captured the time delays of GOOSE messages sent and received by physical IEDs.

The second scenario proved the functionality and robustness of the designed emulated IED. In particular, an overload and an unbalanced current event are injected into the grid to analyze the behavior of the protection mechanisms of the designed emulated IED. The communication data recorded from the network created between two HIL devices show that the emulated IED design is compatible with the physical IEDs. However, the delay in message transmission (GOOSE) with respect to the physical IEDs recorded in the first scenario should be added here when approaching more time-critical scenarios. Using emulated IEDs, sending GOOSE messages between two HIL devices occurs without any visible delay. In addition, MMS servers have enabled the higher-level communication layer of the architecture. The readings collected via MMS in the monitoring unit have been shown to match the measurements captured by MU in the microgrid. Some experiments were performed with MMS servers to simulate pushed trip commands sent from the monitoring unit to the circuit breaker. The data exchange in the created local network was recorded with Wireshark software for further analysis.

The third scenario involves a man-in-the-middle cyber attack on the circuit breaker that connects the electric vehicle charging station (EVCS) to the power grid. The pseudo-code representation of the attack script is presented for a better understanding of the attack scenario. The success of the attack scenario proved the vulnerability of MMS messages in case of physical access to the communication network. The attack carried out here effectively disconnected the EVCS from the power grid without the possibility of detecting the disconnection by the monitoring unit.

The testbed setup created in this study represents a robust model of a real-time smart grid in which the controlling devices communicate with the grid via IEC61850 through the created local network. Further studies can use this platform to investigate different cyber-attack scenarios and propose effective countermeasures.

REFERENCES

[1] Yi Ding, Salvador Pineda, Preben Nyeng, Jacob Østergaard, Emil Mahler Larsen, and Qiuwei Wu. Real-time market concept architecture for ecogrid eu—a prototype for european smart grids. IEEE Transactions on Smart Grid, 4(4):2006–2016, 2013.

[2] Harshavardhan Palahalli, Enrico Ragaini, and Giambattista Gruosso. Smart grid simulation including communication network: A hardware in the loop approach. IEEE Access, 7:90171–90179, 2019.

[3] Chilton Fernandes, Samarth Borkar, and Jignesh Gohil. Testing of goose protocol of iec61850 standard in protection ied. International journal of computer applications, 93(16), 2014.

[4] Marziyeh Hemmati, Harshavardhan Palahalli, Giambattista Gruosso, and Samuele Grillo. Interoperability analysis of iec61850 protocol using an emulated ied in a hil microgrid testbed. In 2021 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), pages 152–157. IEEE, 2021.

[5] Haftu Tasew Reda, Biplob Ray, Pejman Peidaee, Adnan Anwar, Abdun Mahmood, Akhtar Kalam, and Nahina Islam. Vulnerability and impact analysis of the iec 61850 goose protocol in the smart grid. Sensors, 21(4):1554, 2021.

[6] Hamed Haggi, Meng Song, Wei Sun, et al. A review of smart grid restoration to enhance cyber-physical system resilience. 2019 IEEE Innovative Smart Grid Technologies-Asia (ISGT Asia), pages 4008–4013, 2019.

[7] Manolya Atalay and Pelin Angin. A digital twins approach to smart grid security testing and standardization. In 2020 IEEE International Workshop on Metrology for Industry 4.0 & IoT, pages 435–440. IEEE, 2020.

[8] Pei Zhang, Fangxing Li, and Navin Bhatt. Next-generation monitoring, analysis, and control for the future smart control center. IEEE Transactions on Smart Grid, 1(2):186–192, 2010.

[9] H Palahalli, Y Huo, and G Gruosso. Real time simulation of photovoltaic system using fpga. In 2018 International Symposium on Power Electronics, Electrical Drives, Automation and Motion (SPEEDAM), pages 865–870. IEEE, 2018.

[10] H Palahalli, E Ragaini, and G Gruosso. Real-time smart microgrid simulation: The integration of communication layer in electrical simulation. In 2021 22nd IEEE International Conference on Industrial Technology (ICIT), volume 1, pages 631–636. IEEE, 2021.

[11] Ehsan Naderi and Arash Asrari. Hardware-in-the-loop experimental validation for a lab-scale microgrid targeted by cyberattacks. In 2021 9th International Conference on Smart Grid (icSmartGrid), pages 57–62. IEEE, 2021.

[12] Typhoon hil. https://www.typhoon-hil.com/. accessed Jan 2022.

[13] H Palahalli, M Hemmati, E Ragaini, and G Gruosso. Hardware in the loop simulation of the smart grid with the inclusion of iec61850 communication protocol. In IECON 2021–47th Annual Conference of the IEEE Industrial Electronics Society, pages 1–6. IEEE, 2021.

[14] SM Suhail Hussain, Shaik Mullapathi Farooq, and Taha Selim Ustun. A method for achieving confidentiality and integrity in iec 61850 goose messages. IEEE transactions on Power Delivery, 35(5):2565–2567, 2020.

[15] Jyh-Cherng Gu, Chun-Hung Liu, Jing-Min Wang, and Ming-Ta Yang. Using iec 61850 goose messages in microgrid protection. International Transactions on Electrical Energy Systems, 29(12):e12122, 2019.

[16] Zhu Yongli, Wang Dewen, Wang Yan, and Zhao Wenqing. Study on interoperable exchange of iec 61850 data model. In 2009 4th IEEE Conference on Industrial Electronics and Applications, pages 2724–2728. IEEE, 2009.

[17] Walid El-Khattam and Tarlochan S Sidhu. Resolving the impact of distributed renewable generation on directional overcurrent relay coordination: a case study. IET Renewable power generation, 3(4):415–425, 2009.

[18] Pouya Jamborsalamati, Abhinav Sadu, Ferdinanda Ponci, and Antonello Monti. A flexible hil testing platform for performance evaluation of iec 61850-based protection schemes. In 2016 IEEE Power and Energy Society General Meeting (PESGM), pages 1–5. IEEE, 2016.

[19] Vetrivel Subramaniam Rajkumar, Marko Tealane, Alexandru Ştefanov, and Peter Palensky. Cyber attacks on protective relays in digital substations and impact analysis. In 2020 8th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems, pages 1–6. IEEE, 2020.

[20] Gelli Ravikumar, Burhan Hyder, and Manimaran Govindarasu. Efficient modeling of iec-61850 logical nodes in ieds for scalability in cps security testbed. In 2020 IEEE/PES Transmission and Distribution Conference and Exposition (T&D), pages 1–5. IEEE, 2020.

[21] BooJoong Kang, Peter Maynard, Kieran McLaughlin, Sakir Sezer, Filip Andrén, Christian Seitl, Friederich Kupzog, and Thomas Strasser. Investigating cyber-physical attacks against iec 61850 photovoltaic inverter installations. In 2015 IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA), pages 1–8. IEEE, 2015.

[22] Mohammad Hasanuzzaman Shawon, SM Muyeen, Arindam Ghosh, Syed Mofizul Islam, and Murilo S Baptista. Multi-agent systems in ict enabled smart grid: A status update on technology framework and applications. IEEE Access, 7:97959–97973, 2019.

[23] Salman Mohagheghi, Jean-Charles Tournier, James Stoupis, Laurent Guise, Thierry Coste, Claus A Andersen, and Jacob Dall. Applications of iec 61850 in distribution automation. In 2011 IEEE/PES Power Systems Conference and Exposition, pages 1–9. IEEE, 2011.

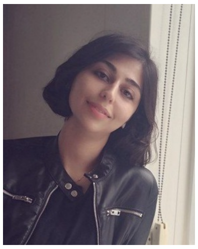
[24] IEC 60255. Inverse definite minimum time (idmt) curves. Technical report, International Organization for Standardization, 2009.

[25] Fatima Salahdine and Naima Kaabouch. Social engineering attacks: A survey. Future Internet, 11(4):89, 2019.

[26] Kwasi Boakye-Boateng, Ali A Ghorbani, and Arash Habibi Lashkari. A novel trust model in detecting final-phase attacks in substations. In 2021 18th International Conference on Privacy, Security and Trust (PST), pages 1–11. IEEE, 2021.

[27] Software to implement mms client. (Date last accessed 10-June-2022).

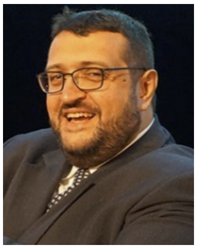
[28] Patrick Wlazlo, Abhijeet Sahu, Zeyu Mao, Hao Huang, Ana Goulart, Katherine Davis, and Saman Zonouz. Man-in-the-middle attacks and defence in a power system cyber-physical testbed. IET Cyber-Physical Systems: Theory & Applications, 6(3):164–177, 2021.



MARZIYEH HEMMATI received her Bachelor degree in Electronics Engineering from IAUCTB, Iran, in 2016, and a Masters degree in Electrical Engineering from Politecnico Di Milano, Italy, in 2021. Currently, she is working with Politecnico di Milano as a research fellow. Her research interests include real-time simulation of electrical systems, digital twins, Hardware-In-the-Loop simulation, electrical vehicles, and cyber-security of smart grids.

HARSHAVARDHAN PALAHALLI M. (Student Member, IEEE) received Bachelor degree in Electrical and Electronics Engineering from Visvesvaraya Technological University, India, in 2014, and a Masters degree in Electrical Engineering from Politecnico Di Milano, Italy, in 2018. Currently, he is in Politecnico di Milano as a Ph.D. candidate. His research interests include Probabilistic load flow, uncertainty quantification of PV and EV, Real-time simulation of electric systems, digital twins and Hardware-in-the-loop simulation.

GIANCARLO STORTI GAJANI (M'12–SM'14) received the Dr. Ing degree in electronic engineering and the Ph. D. degree in electronic systems from Politecnico di Milano in 1986, and 1991 respectively. Since 1992 he is Assistant Professor and since 2002 Associate Professor of Circuit Theory in the same University. His research interests have initially focused on the development of architectures for signal processing (in particular, for audio and music applications) and neural networks. More recently, his research interests include non linear circuits and non linear dynamics. He is a senior member of IEEE and the author of more than 90 papers in international Journals and Conferences.



GIAMBATTISTA GRUOSSO (Senior Member, IEEE) was born in 1973. He received the B.S. and M.S. degrees in electrical engineering and the Ph.D. degree in electrical engineering from the Politecnico di Torino, Italy, in 1999 and 2003, respectively. From 2002 to 2011, he was an Assistant Professor with the Department of Electronics and Informatics, Politecnico di Milano, where he has been an Associate Professor, since 2011. He is the author of more than 80 papers on Journals and conferences on the topics. He does research in electrical engineering, electronic engineering, and industrial engineering. His main research interests include electrical vehicles transportation electrification, electrical power systems optimization, simulation of electrical systems, digital twins for smart mobility, factory and city, and how they can be obtained from data.