IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received January 11, 2022, accepted January 14, 2022, date of publication January 18, 2022, date of current version January 26, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3144027

IEC 61850 Compatible OpenPLC for Cyber Attack Case Studies on Smart Substation Systems

MUHAMMAD M. ROOMI[1], (Member, IEEE), WEN SHEI ONG[1], S. M. SUHAIL HUSSAIN[2], (Member, IEEE), AND DAISUKE MASHIMA[1]

[1]Illinois at Singapore Pte. Ltd., Singapore 138602
[2]School of Computing, National University of Singapore, Singapore 119077

Corresponding author: Muhammad M. Roomi (roomi.s@adsc-create.edu.sg)

This work was supported in part by the National Research Foundation, Singapore, and the Singapore University of Technology and Design, through the National Satellite of Excellence in Design Science and Technology for Secure Critical Infrastructure, under Grant NSoE DeST-SCI2019-005; and in part by the National Research Foundation, Prime Minister's Office, Singapore, through the Campus for Research Excellence and Technological Enterprise (CREATE) Program.

ABSTRACT Programmable Logic Controllers (PLCs) are essential components for enabling remote monitoring and automated control in industrial control systems. Recently PLCs are often utilized in a modernized power grid system for implementing an additional layer of automated control, such as operation of circuit breakers under specific conditions. Thus, in order to create a software-based smart grid testbed (or 'cyber range' for cyber security experiments); emulation of the PLC is imperative. OpenPLC is a software widely used for emulating PLCs, but unfortunately it does not support IEC 61850 standard, which is the globally adopted standard for substation automation in smart power grid systems. Thus, in this paper, the enhancement of OpenPLC to support IEC 61850 protocol and information models is discussed. The performance of the implementation has been validated to corroborate its application for use cases in the smart grid paradigm. Subsequently, the implementation is demonstrated in a smart grid cyber range to evaluate the impacts of attacks and thereby, the effectiveness of security measures and robustness of PLC control logic. The implementation, named 'OpenPLC61850', is made available as an open-source project for the wider research and industry community.

INDEX TERMS Programmable logic controller, cyber security, smart grid test bed, cyber range, IEC 61850.

I. INTRODUCTION

INDUSTRIAL automation has advanced drastically from electromechanical parts and manual control of machine logic to modern electronics and automated control of machine logic. A significant contributor to this advancement is the programmable logic controller (PLC), which provides a more practical and cost-efficient solution when compared with relay logic machines [1].

PLCs are responsible for collecting sensor measurements from the physical plant and evaluating them for automated control on actuators according to the pre-programmed control logic. They are widely used for control and monitoring applications in electrical power systems. For instance, one of the newest smart grid testbeds, which is set up in Singapore, still relies on a number of PLCs for controlling generators and circuit breakers [2]. In substation systems based on the IEC 61850 standard, intelligent electronic devices (IEDs) are progressively taking over these functions. IED is an integrated microprocessor-based controller with communication and automation functionalities. PLCs in smart grid systems collect measurements and device status from such IEDs and then execute control logic. For standardizing the communication among PLCs and IEDs and achieving interoperability, different standards such as IEC 61850, DNP3, Modbus TCP/IP, etc., have been developed. Among these, IEC 61850 is the increasingly deployed one that defines comprehensive information models and communication protocols for substation automation. Therefore, it has emerged as the most popular and widely accepted standard for power utility automation [3]. In the market, there are a variety of commercial PLC products that support IEC 61850 standard [4], [5] and it is expected that such PLCs will remain operational in the power grid systems in the upcoming decades, given the lifetime and frequency of the customary updates in power grid systems.

The associate editor coordinating the review of this manuscript and approving it for publication was Salvatore Favuzza.

PLCs (along with IEDs) have become the core of smart grid control, and therefore any security breach can cause devastating damages to the entire Industrial Control Systems (ICS) [6]. For instance, Stuxnet malware tweaked PLCs to manipulate the centrifuge units of a nuclear power plant, and false data injection (FDI) attacks that attempt to mislead PLC logic within a power grid paradigm have been evaluated in [7]. Moreover, in Ukraine power plant attack in 2015 [8], malicious control commands are injected by a compromised control center, and the similar attack may target PLCs. These demonstrate the real-world risk of cyber attacks against PLCs, and thus making research into the cyber and cyber-physical security indispensable.

On the other hand, development of an environment for evaluating the impacts of cyber attacks and effectiveness of cyber security measures remains challenging. Although conducting such evaluation on a real system seems ideal, significant negative impacts stemming from interrupting the system is inevitable. To address this challenge, hardware-based testbeds that incorporate system devices are developed to glean insights into the operation of a real system. However, the limitations due to its scalability and configurability are common. In addition, high-risk attack experiments are often infeasible. Therefore, use of a software-based testbed (also called digital twin or cyber range), which is highly configurable and extensible, is a promising solution.

OpenPLC [9] is a popular open-source software to emulate the functionality of a PLC (e.g., control logic compliant to IEC 61131 standard). Research works are conducted using OpenPLC in the literature. One notable work is a low cost, open-source cyber physical system testbed called FLEP-SGS^2, which utilizes OpenPLC for relay logics [10]. However, smart grid systems support a variety of protocols which includes the most popular IEC 61850. The OpenPLC only supports traditional ICS protocols such as Modbus, and unfortunately does not support IEC 61850 standards. Therefore, using OpenPLC for software-based testbed to emulate the modernized smart grid systems was not ideal. An enhanced version of OpenPLC with IEC 61850 support ('OpenPLC61850') is published by the authors as an open-source project [11], along with technical documentation [12], [13]. The use of OpenPLC61850 can enhance the scope and capability of testbeds like FLEP-SGS^2. The previous works on OpenPLC61850 [12], [13] does not discuss the performance evaluation of the OpenPLC61850, which is vital for deployment of the enhanced version in a real-time environment. To address this gap, this paper presents the design, implementation and detailed evaluation of the OpenPLC61850. The principal objective for implementing this software is to evaluate network-based attacks (e.g., false data and command injection attacks) against PLCs. The current version of OpenPLC61850 supports IEC 61850 MMS (Manufacturing Message Specification) among other protocols defined in the standard (namely IEC 61850 GOOSE and SV), as MMS is TCP/IP-based, making it the most popular protocol utilized by PLCs for communicating with IEDs, as seen in [14]. Therefore, this paper demonstrates the variety of cyber attack scenarios that can be experimented on the OpenPLC61850. As such, the results from the impact of false data injection (FDI) and false command injection (FCI) attack through OpenPLC61850 MMS communication in a smart substation is presented in this paper.

The rest of the paper is organized as follows. In Section II, related works is discussed. Section III describes the high level architecture of the original OpenPLC as well as OpenPLC61850. The memory-attribute mapping, which is needed to support IEC 61850 information model, is elaborated in Section IV, followed by the case studies to portray the impact of cyber attacks in Section VI. Finally, the paper is concluded with future research directions in Section VII.

II. RELATED WORKS

Testbeds with commercially available PLC hardware can be prohibitively expensive. Therefore, PLC simulators or emulators offer a superior alternative. PLC system simulators such as S7-PLCSIM [4] and RSLogix Emulate [15] provide the same functionality as the hardware-in-the-loop without requiring any real hardware. This is ideal for large testbeds as multiple instances of a PLC simulator can be run using a single computer. Similarly, PLC core simulators such as CORE [16] and AMICI [17] can be utilized for the integration of PLCs with supervisory control and data acquisition (SCADA) systems. Even though these simulators are cost effective, they are built based upon a single PLC program. Therefore, reprogramming is often infeasible. Yet another type is the PLC Network Simulators (Modbus Rsim [18], Modbus Slave [19]). The drawback of these network simulators is the lack of built-in control logic and therefore, they can simulate solely the application layer of network protocols.

As a solution, the aforementioned OpenPLC [9] can emulate the field devices on testbeds and offers a complete system that is compatible with IEC 61131-3. Furthermore, it provides the flexibility of reprogramming. However, OpenPLC supports only Modbus and DNP3 protocols. As an advancement of the existing OpenPLC, OpenPLC61850 was proposed [12]. The OpenPLC61850 provides the same functionality as OpenPLC with an additional support for IEC 61850 MMS based protocol. This protocol support is implemented using the open-source software libiec61850 [20], which provide server and client library using IEC 61850 MMS communication protocols.

PLCs in today's technology and industrial sector are crucial as it facilitates in automating the control process. One of the steps involved in the process is the transmission of the field devices' data to the control station. The execution of this process introduces security concerns in the operation of the system. Further, with the increased integration of internet of things (IoT) in the control sector, the ICS protocols currently cyber attack implemented lack

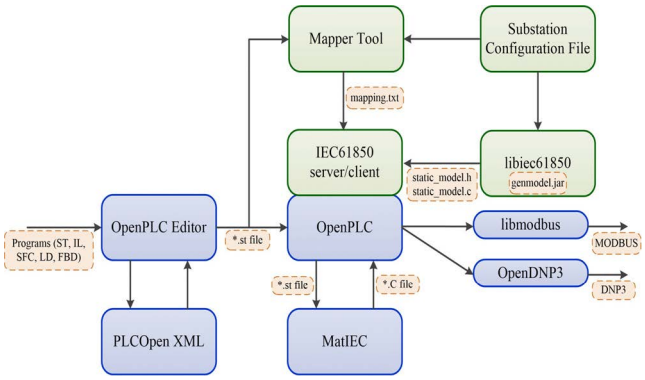


FIGURE 1. OpenPLC architecture (boxes highlighted in green color indicates the features added to existing OpenPLC).

encryption, authorization, authentication and other protection mechanisms. This paves the way for adversaries to carry out cyber attacks on SCADA and distributed control system (DCS) [6]. As PLCs lack some of the aforementioned security strategies, an adversary can manipulate the programs and instructions in PLC by solely knowing its IP address. Some of the literature works regarding the PLC vulnerability include: maliciously generating payloads of PLC [21], enabling of PLC functions through a back door [22], self-propagating worm that exists in S7-1200 [23]. Similarly, the IEDs utilizing IEC 61850 are also prone to different types of attacks including false data injection attacks [24], [25]. Several other cyber attacks have been reported in recent years [23], [26], [27]. Hence, in this paper cyber attacks are demonstrated, particularly FDI and command injection attacks, on the smart substation that utilizes OpenPLC61850 for monitoring and control.

III. ARCHITECTURE OVERVIEW

A. OPENPLC OVERVIEW

OpenPLC is an open-source environment that supports software simulation and hardware implementation on devices such as Raspberry Pi, Arduino and ESP8266 [9]. OpenPLC consists of editor, runtime and human machine interface (HMI) builder. The development environment that is used to create program is called OpenPLC editor. This editor supports program development using several IEC 61131-3 program organization units (POU) such as function block diagram (FBD), ladder diagram (LD), structured text (ST), instruction list (IL), and sequential function chart (SFC). Based on IEC 61131-3, the programs are saved as XML files and thereby, providing flexibility of project exchange with any editor that follows the PLCOpen XML standard. Once the program is created, the in-built module in editor compiles all programs into a ST file. This ST file is utilized in the OpenPLC runtime for the execution of control logics. The architecture of the OpenPLC is illustrated in Fig. 1 (highlighted in blue color).

The communication protocols supported by OpenPLC are Modbus and DNP3 SCADA protocol on default ports 502 and 20,000, respectively. Modbus protocol is implemented using libmodbus and DNP3 protocol. This support feature ensures OpenPLC compatibility with most SCADA human machine interface (HMI) compliant with these protocols.

B. OPENPLC61850: ENHANCEMENT TO SUPPORT IEC 61850

OpenPLC61850 is an extension of OpenPLC. The similarity includes the development environment that still incorporates the standardized IEC 61131-3 programming languages (FBD, LD, ST, IL, and SFC) for PLC. The difference is the addition of IEC 61850 MMS protocol to the OpenPLC software, besides the existing Modbus protocol for communication. The OpenPLC61850 provides an interface between the IEC 61850 MMS protocol and Modbus protocols. The architecture of OpenPLC61850 is depicted in Fig. 1 (highlighted in green color). IEC 61850 MMS protocol compatibility for OpenPLC is implemented by incorporating two new sub-components namely, IEC 61850 server and IEC 61850 client. The former is to accept and handle incoming IEC 61850 MMS messages and control commands transmitted by other devices, such as SCADA HMI. The latter is to send IEC 61850 messages to IEDs. According to the standard for IEC 61850 MMS protocol, the IEC 61850 server listens at port 102 by default. The multi-threaded runtime that runs the PLC program and the multiple IEC 61850 server/client is written in C++. The IEC 61850 MMS protocol in IEC 61850 server/client of OpenPLC61850 is implemented using an open-source libiec61850 library [20]. Mapper Tool is responsible for defining the mapping of IEC 61850 information model to OpenPLC's memory address. The IEC 61850 information model is defined in Substation Configuration Language (SCL) files of IEDs. The mapping ensures that the PLC logic can appropriately conduct read and write operations. The details of the mapping are elaborated in the next section.

IV. MEMORY-ATTRIBUTE MAPPING

The memory mapping between PLC program and IEC 61850 server/client is discussed in this section. Fig. 2 shows the component design and interaction of OpenPLC with the IEC 61850 server/client.

OpenPLC (and thus OpenPLC61850) has memory organized in the form of arrays, which is originally designed for supporting Modbus protocol [28]. The PLC program uses this memory to read/write the input/output values. To ensure the compatibility of PLC program with IEC 61850 semantics, necessary IEC 61850 data attributes need to be mapped onto specific memory addresses in the PLC memory. This obviates the need for any major changes to the components of OpenPLC. This mapping is carried out by the mapper tool. Using IEC 61850 SCL files, the mapper tool assigns PLC memory addresses with the corresponding IEC 61850 data attributes.

The ST file of PLC program and SCL files of IEC 61850 server/client are provided as the input to the mapper

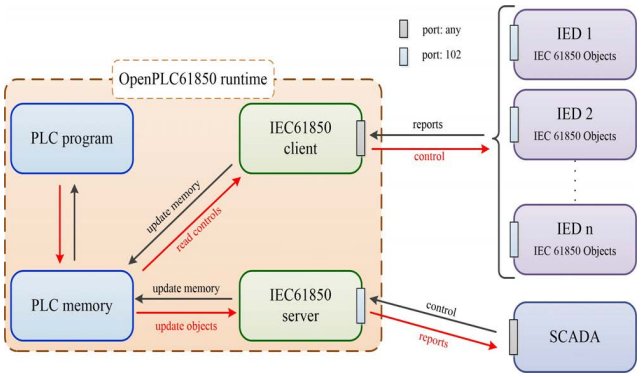


FIGURE 2. Interaction architecture between OpenPLC and IEC 61850 server/client.

TABLE 1. PLC program variables and their corresponding PLC memory address extracted from a ST file.

PLC program variable	PLC memory address	Variable Type
Line_cb_1	%QX00.1	Bool
Line_cb_2	%QX00.2	Bool
Line_cb_3	%QX00.3	Bool
Line_cb_4	%QX00.4	Bool
Line_cb_5	%QX00.5	Bool
Line_cb_6	%QX00.6	Bool
Line_cb_7	%QX00.7	Bool
Line_cb_8	%QX00.8	Bool
Line_cb_9	%QX00.9	Bool

tool. Firstly, the mapper tool extracts the PLC program variables and their corresponding PLC memory addresses using the ST file. Table 1 tabulates the PLC program variables and their corresponding PLC memory address extracted from the ST file. Secondly, the SCL files are parsed to list the private elements using the XML parser. Subsequently, the mapper tool combines these outputs to create a mapping of IEC 61850 data attributes and PLC memory addresses. An example of this mapping of OpenPLC memory to the IEC 61850 server and client variables is tabulated in Table 2. The 'CONTROL' and 'MONITOR' represents whether the data attribute is operable (i.e., whether it is read-only or writable). The output mapping files for IEC 61850 server and client differ slightly. The IEC 61850 client mapping contains additional information such as IP address, available report control blocks (RCB), and the operable IEC 61850 data objects of each IED.

Using the generated mapping, the OpenPLC61850 runtime can extract data from IEC 61850 messages received by IEC 61850 server/client and store them in the PLC memory so that the PLC program refers to the correct value. When PLC program triggers any change as the result of execution of control logic, the corresponding memory address is updated by the program, and then is parsed and processed by IEC 61850 server/client modules (Refer: Fig. 2).

V. PERFORMANCE EVALUATION

This section presents the performance evaluation in terms of computational burden for OpenPLC61850. The computational burden for the additional features in OpenPLC61850 i.e., IEC 61850 server, IEC 61850 client and memory mapping module, are evaluated. In order to evaluate the performance, communication between OpenPLC61850 and virtual IEDs (IEC 61850 MMS servers) is established. The OpenPLC61850 module and virtual IED modules are run on a device equipped with an Intel(R) Core(TM) i7-7700HQ CPU @ 2.80GHz processor and 4GB RAM. The OpenPLC61850 exchanges MMS report and control messages with the IEC 61850 client and server, respectively. The IEC 61850 client module in OpenPLC61850 reads the incoming MMS reports sent by the virtual IEDs. Similarly, the IEC 61850 client module in OpenPLC61850 transmits the MMS control messages to virtual IEDs. Table 3 tabulates the computational times for processing incoming MMS report messages and sending the MMS control messages. The processing times of MMS report and MMS control messages are measured to be below 0.16 ms and 3 ms respectively, which is acceptable and well within the 100 ms limit for low-speed messages stipulated by IEC 61850-5 standards [30]. The MMS control messages evince slightly larger delays as it includes the checking of status (i.e., if the new value matches with the current value) in the IED and subsequently, libiec61850 issues control to the respective IEDs.

Furthermore, the performance of OpenPLC61850 in handling multiple IEC 61850 server and clients is evaluated. A test scenario where OpenPLC61850 is exchanging 40 reports with IEC 61850 server and clients is considered. This test is conducted on the substation model demonstrated in [7]. For this scenario, a total of 22 IEDs (8 IEDs with 2 reports each and 4 IEDs with 1 report each) are utilized. The tests are conducted by increasing the reports exchanges from 40 reports per second to 2000 reports per second. Fig. 3 depicts the graph plotted for estimated reports per second and processed reports per second. The linearity of the graph confirms that the OpenPLC61850 performance does not deteriorate with processing high number of reports.

Additionally, in order to demonstrate that OpenPLC61850 can be utilized for realistic testbedding scenarios, one of the PLCs used in Electric Power and Intelligent Control (EPIC) [14] is configured. EPIC is a power grid testbed for conducting cyber security experiments to validate the effectiveness of cyber defense mechanisms. The testbed includes 7 IEDs and the data is reported to a single PLC, which relays communication to the SCADA HMI workstation. The IEDs implemented for the evaluation is similar to the configuration of the IEDs in the testbed. This experiment is conducted to verify whether the OpenPLC61850 can successfully process a comparable quantum of data sent from the IEDs. The difference in the implementation between the virtual and EPIC testbed is that the PLC in EPIC actively sends query message to collect measurements from IEDs

TABLE 2. Mapping between OpenPLC memory and IEC 61850 attributes.

PLC memory address	IEC 61850 data attributes	Mapping
IEC 61850 Server Mapping		
%MD414	OpenPLC61850LD/GGIO33.AnIn1.mag.f	MONITOR OpenPLC61850LD/GGIO33.AnIn1.mag.f %MD414
%MD415	OpenPLC61850LD/GGIO34.AnIn1.mag.f	MONITOR OpenPLC61850LD/GGIO34.AnIn1.mag.f %MD415
%MD416	OpenPLC61850LD/GGIO35.AnIn1.mag.f	MONITOR OpenPLC61850LD/GGIO35.AnIn1.mag.f %MD416
%MD417	OpenPLC61850LD/GGIO36.AnIn1.mag.f	MONITOR OpenPLC61850LD/GGIO36.AnIn1.mag.f %MD417
%QX00.0	OpenPLC61850LD/GGIO37.SPC.stVal	MONITOR OpenPLC61850LD/GGIO37.SPC.stVal %QX00.0
%QX00.0	OpenPLC61850LD/GGIO37.SPC.Oper.ctlVal	CONTROL OpenPLC61850LD/GGIO37.SPC.Oper.ctlVal %QX00.0
%QX00.1	OpenPLC61850LD/GGIO38.SPC.stVal	MONITOR OpenPLC61850LD/GGIO37.SPC.stVal %QX00.1
%QX00.1	OpenPLC61850LD/GGIO38.SPC.Oper.ctlVal	CONTROL OpenPLC61850LD/GGIO37.SPC.Oper.ctlVal %QX00.1
IEC 61850 Client Mapping		
%MD0	IED0LD/GGIO1.AnIn1.mag.f	MONITOR IED0LD/GGIO1.AnIn1.mag.f %MD0
%MD400	IED0LD/GGIO2.AnIn1.mag.f	MONITOR IED0LD/GGIO2.AnIn1.mag.f %MD400
%QX00.0	IED0LD/GGIO3.SPC1.stVal	MONITOR IED0LD/GGIO3.SPC1.stVal %QX00.0
%QX00.0	IED0LD/GGIO3.SPC1.Oper.ctlVal	CONTROL IED0LD/GGIO3.SPC1.Oper.ctlVal %QX00.0
%MD10	IED1LD/GGIO1.AnIn1.mag.f	MONITOR IED1LD/GGIO1.AnIn1.mag.f %MD10
%MD410	IED1LD/GGIO2.AnIn1.mag.f	MONITOR IED1LD/GGIO2.AnIn1.mag.f %MD410
%QX00.10	IED1LD/GGIO3.SPC1.stVal	MONITOR IED1LD/GGIO3.SPC1.stVal %QX00.10
%QX00.10	IED1LD/GGIO3.SPC1.Oper.ctlVal	CONTROL IED1LD/GGIO3.SPC1.Oper.ctlVal %QX00.10

TABLE 3. Computational times for processing reports and controls.

OpenPLC61850 Action	Time
Report (reading values from IEDs)	~ 0.16ms
Control (sending commands to IEDs)	2ms – 3ms

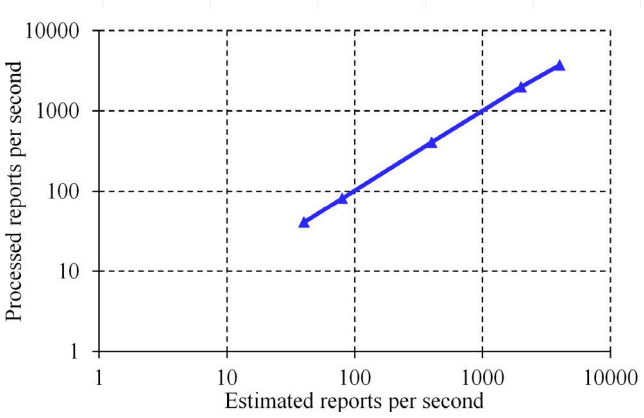


FIGURE 3. Estimated and processed reports per second.

whereas, OpenPLC61850 uses report service, through which each IED actively sends reports to the PLC at a regular interval.

The reports on each IED in the virtual testbed are configured to imitate the data points in the report and the frequency of the data collection (i.e., interval of reports) based on the EPIC testbed. The reports include 43 data points in total and the reporting interval was set to 1000 ms. Based on the conducted experiment, no packet drop or processing error was observed.

VI. CYBER ATTACK CASE STUDIES USING OPENPLC61850

While OpenPLC61850 is a general-purpose, software-based implementation of a PLC, the use of OpenPLC61850 for cyber security experiments is demonstrated in this section. Initially, the system model and the threat models that provide contextual information are explained, followed by cyber attack case studies.

A. SYSTEM DESIGN AND THREAT MODEL

The distribution-level substation system depicted in Fig. 4 is considered as the power system model in this paper. The model consists of two voltage levels, a sub-transmission voltage level of 66kV and a distribution voltage level of 11kV. Two incoming feeders (feeder1 and feeder2) in Fig. 4 represent the 66kV voltage level, which is then transformed to 11kV through transformers T1 and T2. The bus coupler breaker (CB16) remains in the open state during the normal operating condition and CB17 remains in the 'closed' state. The measurements from the field devices such as current transformers (CTs), voltage transformers (VTs), transducers and circuit breakers (CBs) are communicated to the OpenPLC through IEDs. The locations of the IEDs for measurements of different physical parameters are illustrated in Fig. 4. The assigning of logical nodes (LN) and data objects (DO) for the IEDs is tabulated in Table 4.

Cyber attacks against automation controllers in a critical infrastructure often engender severe consequences. With emerging technologies and the complexities involved, it is difficult to predict the behavior of the attacker. An attacker may infiltrate into substation network and gain access to different IEDs and PLCs in the substation network. Subsequently, the attacker is able to launch several types of

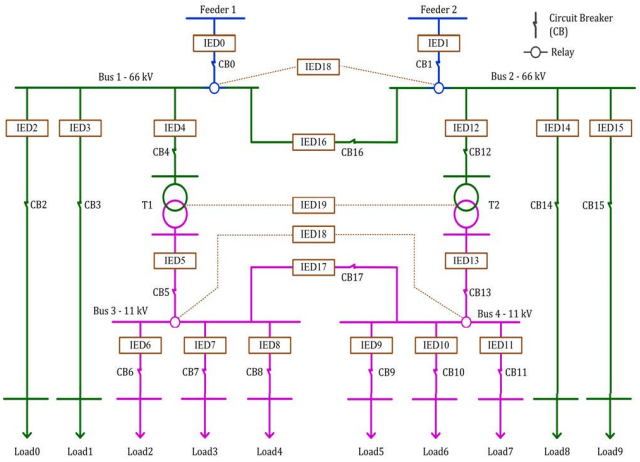


FIGURE 4. Smart substation model under study.

TABLE 4. Allocation of LNs and DOs.

IEDs	Measurement	IEC 61850 attributes
IED* (*-0,1,4,5, 12,13,16,17)	Line Load	IED*/LD/GGIO1/AnIn1/mag.f
	Line Loading %	IED*/LD/GGIO2/AnIn1/mag.f
	CB status	IED*/LD/GGIO3/SPC1/stVal
IED* (*-2,3,6-10, 11,14,15)	Line Load	IED*/LD/GGIO1/AnIn1/mag.f
	Line Loading %	IED*/LD/GGIO2/AnIn1/mag.f
	CB status	IED*/LD/GGIO3/SPC1/stVal
	Total Power	IED*/MEAS/MMXU/TotW/mag.f
IED18	Relay status	IED18/LD/GGIO1/SPC1/stVal
		IED18/LD/GGIO2/SPC1/stVal
		IED18/LD/GGIO3/SPC1/stVal
		IED18/LD/GGIO4/SPC1/stVal
IED19	Transformer Temperature	IED19/LD/STMP1/Tmp/mag.i
		IED19/LD/STMP2/Tmp/mag.i

injection and malware attacks in the system. In this paper two threat models are considered. In the first model, the attacker gains access to the substation network and launches FDI attacks by injecting false data through report control block MMS messages to IEC 61850 client in OpenPLC61850. Such an attack is made possible by mounting man-in-the-middle attacks on intermediate switches or TCP session hijacking. In the second model, the attacker has already gained access to the network and launches false command injection attack (FCI), by compromising or impersonating SCADA HMI. In this attack model, wo scenarios for FCI attacks are considered when SCADA is implemented with (i) IEC 61850, and (ii) Modbus protocols. Fig. 5 illustrates the threat models considered in this paper. The attacker models discussed here include: malware like CrashOverride/Industroyer [30], [31], which possess the capability to inject IEC 61850-compliant messages into the system; attacks like Ukraine power plant attack in 2015 where a legitimate SCADA HMI workstation was manipulated to emit malicious commands [32]; and recent hacking against US utility's control room [33].

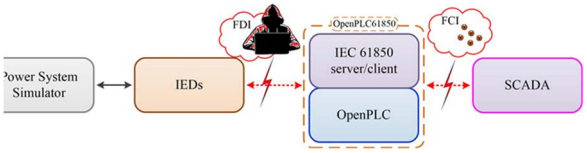


FIGURE 5. Threat model representation.

Several automation logics are implemented in the ICS [7]. In this paper, the transformer over-temperature logic is employed to demonstrate a FDI attack through tampering of the report control block in IEC 61850 MMS protocol. The FCI attack is simulated by the modification of the circuit breakers' status (CB16 and CB17 in Fig. 4) through HMI and thereby disrupting the normal operation of the system.

In order to conduct the evaluation, the physical topology of the system depicted in Fig. 4 is simulated using Pandapower. The IEDs implemented in the system are emulated using OpenPLC61850 software described earlier in this paper and the communication network topology is executed using Mininet software. All these software are run on a single Linux platform.

B. FALSE DATA INJECTION

The system considered in this paper (shown in Fig. 4) comprises of two transformers fed by two incoming feeders. The temperature of transformers T1 and T2 is monitored by IED19. The IED also compares the temperature of the transformers with the threshold values. When the temperature is greater than the threshold value, the 'threshold status' is set to 'False'; otherwise, it is set to 'True'. The IED communicates the transformer temperatures 'threshold status' as an IEC 61850 MMS message to the PLC (i.e., OpenPLC61850). Fig. 6 shows the Wireshark capture of IEC 61850 MMS message sent by IED19 to the PLC. During normal operation, the 'threshold status' values for both the transformer are 'True'.

An attacker in the network launches a FDI attack by sending a fake IEC 61850 MMS message to PLC. Such an attack is possible by 'man-in-the-middle' attack or by compromising/impersonating the IED. The attacker sets the value of 'threshold status' to 'False'. Fig. 6(b) depicts the Wireshark capture of the fake IEC 61850 MMS message sent by attacker to the PLC. The PLC, upon receiving this message, trips the transformer T1 to protect it against physical damage owing to over-temperature. Once the transformer T1 is tripped, the loads 2 to 4 are connected to T2 through CB17. This increases the loading percent on T2. IED13 monitors the load and loading percent on transformer T2. Fig. 6(c) illustrates the Wireshark capture of IEC 61850 MMS message sent by IED13. As discernible from the figure, the loading percentage of T2 is 116.39%. Due to the overloading protection logic, transformer T2 is disconnected due to the trip commands issued to the circuit breakers. This results in the complete de-energization of loads 2 to 7 as shown in

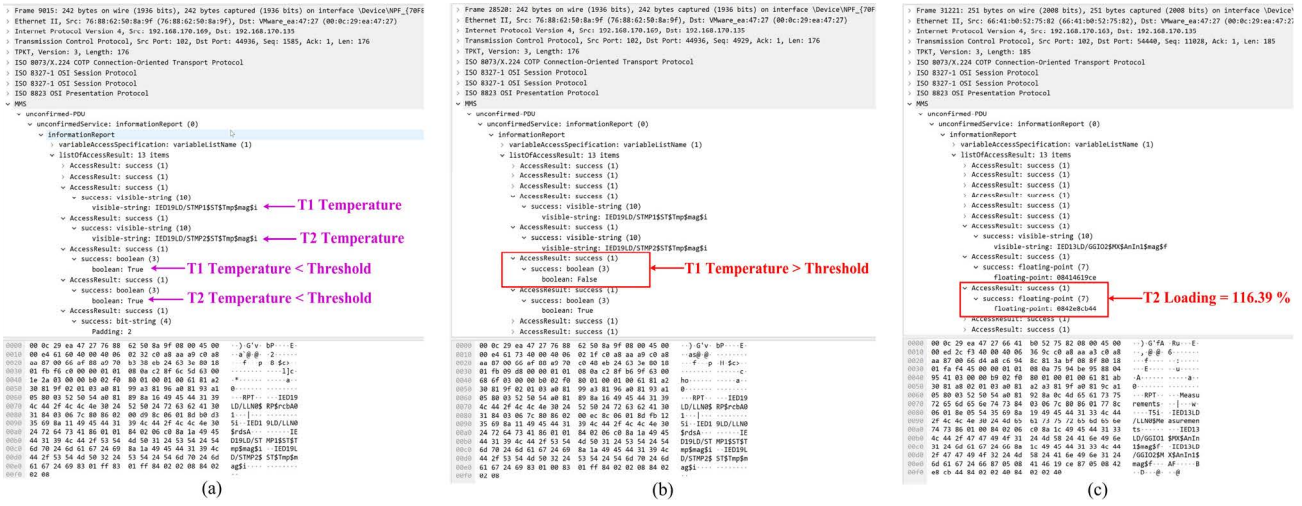


FIGURE 6. Message Exchanges between Transformers IED (IED19) and OpenPLC61850: (a) Transformers temperature is normal (b) FDI attack on T1 temperature (c) Overload on T2.

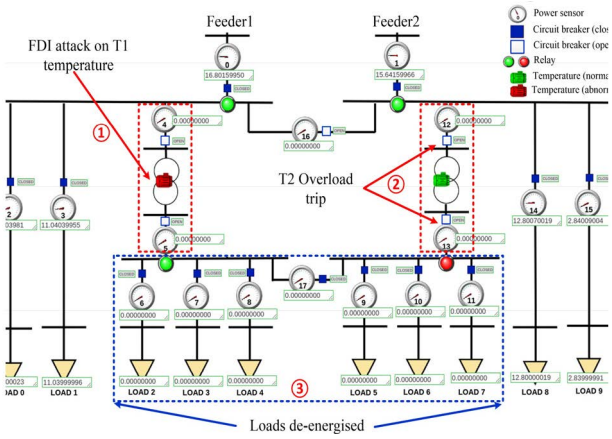


FIGURE 7. Impact of FDI attack.

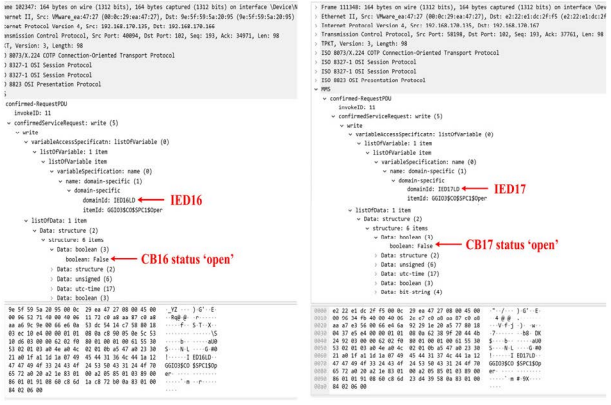


FIGURE 9. MMS Communication to IED from OpenPLC61850: (a) CB16 'open' (b) CB17 'open'.

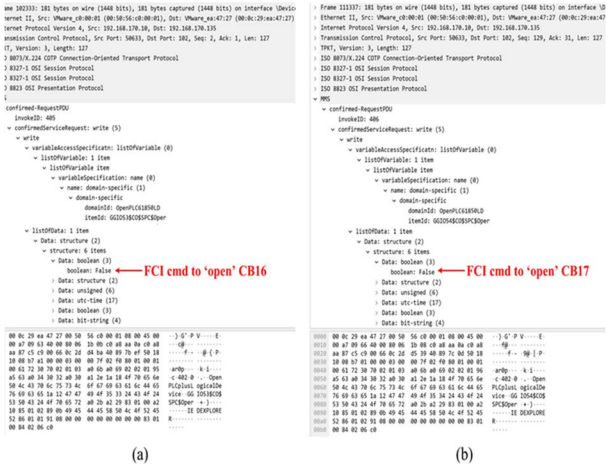


FIGURE 8. MMS communication to OpenPLC61850 server: (a) FCI to 'open' CB16 (b) FCI to 'open' CB17.

Fig. 7. By launching FDI attack on OpenPLC the attacker is able to effectively de-energize the loads 2 to 7.

C. FALSE COMMAND INJECTION

1) FCI through IEC 61850 MMS

As depicted in Fig. 4, there are two incoming feeders that are separated by a bus coupler (CB16). This coupler is normally 'open' isolating both the feeders. During situations wherein one of the feeders is rendered non-operational due to servicing, and also, when there are no faults in the bus, the bus coupler CB16 is then 'closed'. As such, the feeder in operation supplies power to the non-operational feeder's loads.

During this condition, an attacker, possibly impersonating a legitimate SCADA HMI, launches a FCI to the PLC. The malicious command to 'open' the bus couplers CB16 and CB17 is depicted in Fig. 8. This false command triggers the PLC to render the bus couplers CB16 and CB17 to be 'open'. Fig. 9 depicts the MMS communication between the PLC and IEDs. As seen in the figure, the IED attributes corresponding to the status of CB 16 (*IED16/LD/GGIO3/SPC1/stVal)* and CB 17 (*IED17/LD/GGIO3/SPC1/stVal*) are overwritten. The

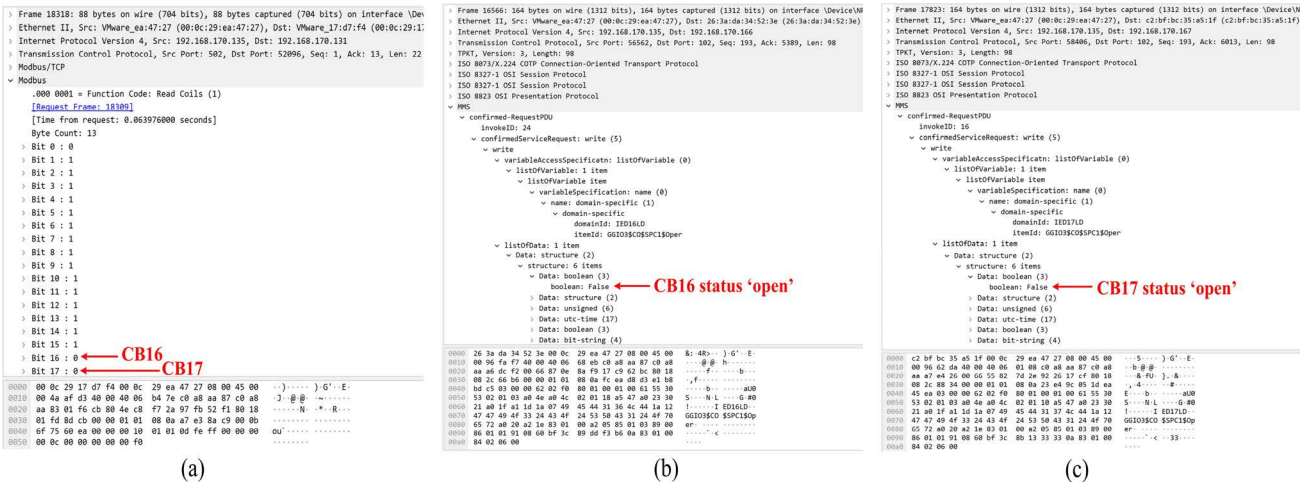


FIGURE 10. Message Exchanges between SCADA HMI and OpenPLC61850: (a) CB manipulation via Modbus (b) MMS communication to IED from OpenPLC for 'CB16' (c) MMS communication to IED from OpenPLC for 'CB17'.

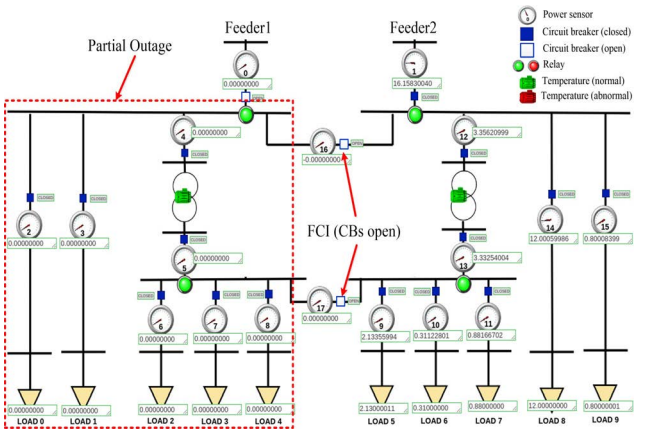


FIGURE 11. Impact of FCI attack.

Boolean value representing the status of the CBs is changed to 'False' and thereby, the CBs are 'open'.

2) FCI THROUGH MODBUS TCP

OpenPLC61850 can support Modbus protocol for interacting with traditional SCADA HMI system, like the original OpenPLC, while interacting with IEDs via IEC 61850 MMS. In this section, the use of OpenPLC61850 between a Modbus-based SCADA HMI and an IEC 61850 based substation system is presented and the attack against OpenPLC through Modbus communication is demonstrated.

The Modbus and MMS communications between the SCADA HMI (ScadaBR), PLC (OpenPLC61850), and target IEDs are depicted in Fig. 10. In Fig. 10(a), Bit 0 to Bit 16 represents the status of the CB in the system. When receiving the Modbus message, the PLC maps the information onto the memory address, which is then processed by IEC 61850 client module in the PLC in order to send out the corresponding IEC 61850 MMS messages to the target IEDs. The updated status is then reported back to the SCADA HMI. During normal operation of system, the CB status for feeder1 is '1' (i.e., CB0 is 'closed'), bus coupler 16 status is '0' (i.e., CB16 is 'open') and bus coupler 17 is '1' (i.e., CB17 is 'closed').

Assuming that the attacker injects false Modbus TCP messages from SCADA HMI to OpenPLC to 'open' the CB16 and CB17, the reflection of the status change of CB16 and CB17 to '0' is demonstrated in Fig. 10(a). Once the attack has been launched, the false command received by the OpenPLC is fed to corresponding IEDs (in this case IED16 and IED17) through IEC 61850 MMS protocol. Fig. 10(b) & (c) depicts the MMS communication between OpenPLC and IED16 & IED 17, respectively.

The status change of the manipulated circuit breakers is then communicated to the PLC via IEC 61850 MMS and then sent to the SCADA HMI via Modbus. The consequence of the FCI attack through HMI is shown in Fig. 11. As depicted, feeder1 CB is 'open' due to servicing, and CB16 and CB17 status are 'open' due to the false injection of the command through HMI. In this case, the loads that are usually fed by feeder1 (load 0 to load 4) are de-energized, resulting in partial outage.

VII. CONCLUSION

In order to develop a virtual, cyber security-testing platform (also known as cyber range) that emulates modernized substation systems, the widely-used open-source software (OpenPLC) is enhanced to support IEC 61850 standard. The enhanced software, named OpenPLC61850, allows us to demonstrate cyber attack against PLCs, such as false data/command injection attacks. The current version supports only IEC 61850 MMS protocols as it is the principal protocol used by PLC to interact with IEDs in a substation. OpenPLC61850 has been published as an open-source project [11], [12] to further its applications and functionalities by other researchers.

Furthermore, the FDI attack on the MMS report control block messages to manipulate the transformer temperature that led to disruption in the normal operation of the system was demonstrated. Additionally, FCI attack through HMI and falsely triggering the CB status that led to partial outage in the system was demonstrated. Cyber security measures to ensure secured exchange of power system messages using IEC 61850, according to IEC 62351 standards [25] will be included as a part of forthcoming research.

As aforementioned, the current version supports only the principal protocol (IEC 61850 MMS) that is used for PLC to interact with IEDs in a substation. However, IEC 61850 standard also defines other protocols, such as IEC 61850 GOOSE and SV, and this implementation is part of our future work. Subsequently, the aim is to provide support for cybersecurity measures for IEC 61850 message exchanges according to the IEC 62351 standard [25].

REFERENCES

[1] P. E. Moody and R. E. Morley, *The Technology Machine: How Manufacturing Will Work in the Year 2020*. New York, NY, USA: Simon and Schuster, 2001.
[2] A. Siddiqi, N. O. Tippenhauer, D. Mashima, and B. Chen, "On practical threat scenario testing in an electric power ICS testbed," in *Proc. 4th ACM Workshop Cyber-Physical Syst. Secur.*, May 2018, pp. 15–21.
[3] M. A. Aftab, S. M. S. Hussain, I. Ali, and T. S. Ustun, "IEC 61850 based substation automation system: A survey," *Int. J. Electr. Power Energy Syst.*, vol. 120, Sep. 2020, Art. no. 106008.
[4] Siemens. *SIMATIC S7-PLCSIM Software for SIMATIC Controllers*. Accessed: Aug. 20, 2021. [Online]. Available: http://w3.siemens.com/mcms/simatic-controller-software/en/step7/simatic-s7-plcsim/pages/default.aspx
[5] BECKHOFF. *TwinCAT PLC IEC 61850 Server*. Accessed: Dec. 31, 2021. [Online]. Available: https://www.beckhoff.com/zh-sg/products/automation/twincat/tsxxxx-twincat-2-supplements/ts6511.html
[6] X. Pan, Z. Wang, and Y. Sun, "Review of PLC security issues in industrial control system," *J. Cybersecur.*, vol. 2, no. 2, p. 69, 2020.
[7] M. M. Roomi, P. P. Biswas, D. Mashima, Y. Fan, and E.-C. Chang, "False data injection cyber range of modernized substation system," in *Proc. IEEE Int. Conf. Commun., Control, Comput. Technol. Smart Grids (SmartGridComm)*, Nov. 2020, pp. 1–7.
[8] K. Zetter. (2016). *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid*. Accessed: Jun. 7, 2017. [Online]. Available: http://www.wired.com/2016/03/insidecunning-unprecedented-hack-ukraines-power-grid/
[9] T. Alves and T. Morris, "OpenPLC: An IEC 61,131–3 compliant open source industrial controller for cyber security research," *Comput. Secur.*, vol. 78, pp. 364–379, Sep. 2018.
[10] C. Konstantinou, M. Sazos, and M. Maniatakos, "FLEP-SGS2: A flexible and low-cost evaluation platform for smart grid systems security," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. (ISGT)*, Feb. 2019, pp. 1–5.
[11] *OpenPLC61850*. Accessed: Dec. 20, 2021. [Online]. Available: https://github.com/smartgridadsc/OpenPLC61850
[12] M. M. Roomi, W. S. Ong, D. Mashima, and S. M. S. Hussain. (Jun. 2021). *OpenPLC61850: An IEC 61850 compatible OpenPLC for Smart Grid Research*. [Online]. Available: https://www.techrxiv.org/articles/preprint/OpenPLC61850_An_IEC_61850_compatible_OpenPLC_for_Smart_Grid_Research/14845062/1
[13] M. M. Roomi, W. S. Ong, D. Mashima, and S. M. S. Hussain, "OpenPLC61850: An IEC 61850 MMS compatible OpenPLC for smart grid research," *SoftwareX*, vol. 17, Jan. 2022, Art. no. 100917.
[14] *iTrust*. Accessed: Dec. 21, 2021. [Online]. Available: https://itrust.sutd.edu.sg/testbeds/electric-powerintelligent-control-epic/
[15] Rockwell. *Studio 5000 Logix Emulate*. Accessed: Aug. 20, 2021. [Online]. Available: https://www.rockwellautomation.com/rockwellsoftware/products/studio5000-logix-emulate.page
[16] U. S. Naval Research Lab. *Common Open Research Emulator (CORE)*. Accessed: Jan. 21, 2022. [Online]. Available: https://www.nrl.navy.mil/Our-Work/Areas-of-Research/Information-Technology/NCS/CORE/
[17] B. Genge, C. Siaterlis, and M. Hohenadel, "AMICI: An assessment platform for multi-domain security experimentation on critical infrastructures," in *Critical Information Infrastructures Security*. Cham, Switzerland: Springer, 2013, pp. 228–239.
[18] *Modbus PLC Simulator*. Accessed: Aug. 21, 2021. [Online]. Available: http://www.plcsimulator.org/
[19] M. Tools. *Modbus Slave Simulator*. Accessed: Aug. 21, 2021. [Online]. Available: http://www.modbustools.com/modbus_slave.html
[20] *libIEC61850*. Accessed: Dec. 11, 2021. [Online]. Available: https://libiec61850.com/libiec61850/
[21] S. E. McLaughlin, "On dynamic malware payloads aimed at programmable logic controllers," in *Proc. HotSec*, Aug. 2011, pp. 1–6.
[22] J. Klick, S. Lau, D. Marzin, J.-O. Malchow, and V. Roth, "Internet-facing PLCs—A new back orifice," *Blackhat USA*, pp. 22–26, Aug. 2015.
[23] R. Spenneberg, M. Brüggemann, and H. Schwartke, "PLC-blaster: A worm living solely in the PLC," in *Proc. Black Hat Asia*, vol. 16, 2016, pp. 1–16.
[24] M. Chlela, G. Joos, M. Kassouf, and Y. Brissette, "Real-time testing platform for microgrid controllers against false data injection cybersecurity attacks," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Jul. 2016, pp. 1–5.
[25] S. M. S. Hussain, T. S. Ustun, and A. Kalam, "A review of IEC 62351 security mechanisms for IEC 61850 message exchanges," *IEEE Trans. Ind. Informat.*, vol. 16, no. 9, pp. 5643–5654, Sep. 2020.
[26] S. E. McLaughlin, "On dynamic malware payloads aimed at programmable logic controllers," in *Proc. HotSec*, 2011, pp. 1–6.
[27] Q. Tan, G. Yue, J. Shi, X. Wang, B. Fang, and Z. Tian, "Toward a comprehensive insight into the eclipse attacks of tor hidden services," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1584–1593, Apr. 2019.
[28] T. Alves, *OpenPLC*. Accessed: Jan. 20, 2021. [Online]. Available: https://www.openplcproject.com/reference/modbus/
[29] P. CODE, "Communication networks and systems in substations—Part 5: Communication requirements for functions and device models," ed., 2003.
[30] (2017). *CrashOverride Malware*. Accessed: Aug. 18, 2017. [Online]. Available: https://www.us-cert.gov/ncas/alerts/TA17-163A
[31] (2017). *CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations*. Accessed: Aug. 18, 2017. [Online]. Available: https://dragos.com/blog/crashoverride/CrashOverride-01.pdf
[32] D. U. Case, "Analysis of the cyber attack on the Ukrainian power grid," Electricity Information Sharing and Analysis Center (E-ISAC), vol. 388, 2016.
[33] R. Smith. *Russian Hackers Reach U.S. Utility Control Rooms, Homeland Security Officials Say*. Accessed: Sep. 29, 2021. [Online]. Available: https://www.wsj.com/articles/russianhackers-reach-u-s-utility-control-rooms-homeland-security-officialssay-1532388110

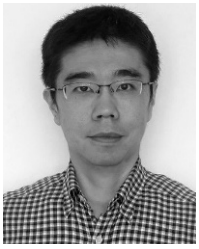
MUHAMMAD M. ROOMI (Member, IEEE) received the B.E. degree in electronics and electronics engineering from Anna University affiliated college (N.I.C.E), Tamil Nadu, India, in 2008, and the M.Sc. and Ph.D. degrees in power engineering from Nanyang Technological University, Singapore, in 2011 and 2016, respectively.

From 2017 to 2018, he was a Research Fellow with the Energy Research Institute @ Nanyang Technological University. In 2019, he joined the Singapore University of Technology and Design, Singapore, as a Research Fellow I. He is currently working as a Research Scientist with Illinois at Singapore Pte Ltd. The aim is to design an automated framework for generating cyber-physical range for smart grids. His research interests include cyber security for smart grids, power electronic converters, series compensators for distribution systems, and IEC 61850 standards for electric power systems.

WEN SHEI ONG received the B.Comp. degree in computer science from the National University of Singapore, Singapore, in 2021. He is currently working as a Software Engineer at the Advanced Digital Sciences Centre, Illinois at Singapore Pte Ltd. His research interests include software engineering and cybersecurity.

S. M. SUHAIL HUSSAIN (Member, IEEE) received the Ph.D. degree in electrical engineering from Jamia Millia Islamia (a Central University), New Delhi, India, in 2018.

He is currently a Senior Research Fellow with the Department of Computer Science, National University of Singapore (NUS), Singapore. Prior to that, he was a AIST Postdoctoral Researcher at the Fukushima Renewable Energy Institute, AIST (FREA), Koriyama, Japan, from 2018 to 2020. His research interests include power system communication, cyber security in power systems, substation automation systems, IEC 61850 standards, electric vehicle integration, and smart grid. He was a recipient of the IEEE Standards Education Grant approved by the IEEE Standards Education Committee for implementing project and submitting a student application paper in 2014–2015. He was a Guest Editor of the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS.



DAISUKE MASHIMA received the Ph.D. degree in computer science from the Georgia Institute of Technology, in 2012.

He is currently a Senior Research Scientist at Illinois at Singapore Pte Ltd. He is also affiliated with the University of Illinois at Urbana–Champaign, USA, as a Research Affiliate, as well as the National University of Singapore as an Adjunct Assistant Professor. He has been leading multiple government-funded research projects in smart grid security. His research interests include cyber security, privacy, and digital twinning of cyber-physical systems and industrial control systems, with particular emphasis on smart power grid systems. He was a recipient of the Best Paper Award at IEEE SmartGridComm 2014 and the Best Reviewer Award of the IEEE TRANSACTIONS ON SMART GRID (PES) in 2019.