Coordinated Network Attacks on Microgrid Dispatch Function: An EPIC Case Study

Article · November 2022

CITATIONS
0

READS
257

4 authors, including:

Hengchuan Tan
Advanced Digital Sciences Center
20 PUBLICATIONS **177** CITATIONS
SEE PROFILE

Binbin Chen
Singapore University of Technology and Design
106 PUBLICATIONS **1,600** CITATIONS
SEE PROFILE

Coordinated Network Attacks on Microgrid Dispatch Function: An EPIC Case Study

Muhammad Ramadan Saifuddin[1], Lin Wei[2], Heng Chuan Tan[3], and Binbin Chen[1]

[1] Singapore University of Technology and Design
{muhammad_ramadan,binbin_chen}@sutd.edu.sg
[2] Singapore University of Technology and Design wei_lin@mymail.sutd.edu.sg
[3] Advanced Digital Sciences Center, Illinois at Singapore
hc.tan@adsc-create.edu.sg

Abstract. Communication network dependencies for microgrid's operations increases cybersecurity risks, where vulnerabilities found in communication protocols can be exploited for malicious intent. In this paper, we enumerate important attack techniques on multiple communication protocols and investigate their impacts on the microgrid dispatch function. We also show that an attacker can leverage multiple protocols to launch coordinated attacks that offers longer-term, stealthier, and larger adversarial impact, an advanced persistent threat. Our main contribution in this work is a detailed case study carried out on Electrical Power and Intelligent Control (EPIC) testbed located in Singapore. Through a series of experiments, we demonstrated individual protocols' vulnerability, verified their negative impacts on several microgrid's dispatch functions, and also illustrated the practicality of coordinated attacks through the manipulation of multiple protocols.

Keywords: Microgrid · Cyber-physical power system · Cybersecurity

1 Introduction

The general term "Smart Grid" implies the convergence of communications network and power system technologies to form a cyber-physical power system (CPPS). Particularly in the presence of widespread penetration of distributed energy resources (DER), e.g., solar panels, small-scaled generators, and energy storage systems, CPPS offers solutions in coordinating various DERs for operational needs, especially in the domain of improving operational efficiency, reliability, and sustainability. Over the years, smart grid deployment has shifted towards nano-structured ecosystem as a transactive hub that aggregates multiple stand-alone microgrid systems. Thus, a set of coordinated control action involving DER control and command, assets dispatch control, protection, etc., are imperative to steer a microgrid community that is sustainable and reliable; (a) it hides complexity and paves DER interoperability at the edge of the power grid, (b) it allows efficient coordination of local energy generation and usage, and

(c) it can benefit power quality and resiliency at the global transmission level, by aggregating local DERs through a dispatch control system. Hence, several microgrid research projects (e.g., the Illinois Institute of Technology campus grid [10] and the PUSPIPTEK project [9]) are developing and demonstrating new and advanced dispatch functions for microgrids. Ultimately, these microgrids must be prepared to function in a stand-alone mode (i.e, intentional islanded mode) that is cost efficient and resilient in black-start operations.

Realization in microgrid dispatch functions for islanding operation require digitization of control systems and instrument devices with network capabilities—an interconnected network architecture that interacts with the physical power system environment by utilizing communication, control, and computing resources [16]. In industrial practices, mixture of communication network standards and protocols are common because: (a) transitions are done in phases thus their CPPS implementations could be heterogeneous; (b) devices that serve different roles usually inherit and adopt different protocols; and (c) different vendors could favor different protocols. Regardless of the diversified practice for network communication standards, e.g., IEEE 1815-DNP3, IEC 61850, IEC 60870-5-104, HTTP/S, and Modbus standards, efforts are driven towards promoting system interoperability and scalability across multi-vendor devices during microgrid-forming enterprise [6]. Each of these standards provides tradeoffs between the IT/OT characteristics that involves data transportation (distance), information transfer time & latency, synchronicity & scalability, and information reliability & security.

While digitization is essential for microgrids, it also expands the attacking surface. Adversaries exploit vulnerabilities in the communication protocols or coupling layers of CPPS to corrupt industrial control and protection systems. Hence, users must take necessary steps to mitigate such vulnerabilities, e.g., IEC 62351 standard was developed to secure series of power grid protocols including IEC 60870-5 series, IEC 60870-6 series, and IEC 61850 series [15]. DNP3 can use an authentication mechanism to protect the established communication, thus countering threats such as spoofing, modification, and replay attacks [1]. IEC 60870-5-104 protocol adds an additional TLS encryption layer [14]. Despite various security controls have been proposed for these communication protocols, the real-world adoption is far from ideal. Many deployment still operates in insecure mode and many implementations have weakness [2],[7]. The Ukraine power grid attack is an example of how attackers can penetrate into a power system to cause massive disruptions [4].

In this paper, we present a case study of coordinated network attacks against islanded microgrid operations and demonstrate them on a high-fidelity power grid testbed, the Electrical Power and Intelligent Control (EPIC) testbed located in Singapore. As summarized in Table 1, we demonstrate capability in performing long-term reconnaissance operations to learn about the dispatch functions' characteristics and execute a highly synchronized, multistage attack that is stealthy in comparison to attacking a single protocol. The attack objective of our coordinated attack is no longer focused on direct power supply interruptions but rather

Table 1. Summary of cyberattacks on dispatch function requirements for Islanded operation targeting different communication protocols.

Comm. Protocol	**Attack Techniques**	**Data Flow**	**Adversarial Impact**
IEC 61850 GOOSE	DoS	IED status & sensor readings	no implication on the dispatch function requirements for Islanded operation while obvious attack traces visible on HMI.
	HSN	IED status & sensor readings	a persistent 1sec transmission delay between HSN-infected GOOSE packet and the next legitimate packet. No implication on cyber network and physical systems.
	Data Manipulation	IED status & circuit breaker position	significant impact on physical system forcing genset to stop spinning and cause CB to trip (alarm). Can be rectified by manually resetting the breaker and toggle to manual mode. But, such malicious tripping can propagates to other gensets due to overloading.
IEC 61850 MMS	MITM, FDI	IED status to PLC	significant impact on the dispatch control functions as physical system becomes unresponsive or haywire due to falsified state environment provided by IED. But, attack traces are visible on SCADA-HMI.
		sensor readings from PLC to HMI	stealthier approach as it deceives operators monitoring SCADA-HMI with malicious altercation on the true operational status of physical system,but, no operational consequences.
Modbus	MITM, FDI	command actuators	significant impact on the dispatch control function as actuator deviate from it intended operations. However, the attack traces are reflected on HMI providing information/traces.
Multiple Protocol: GOOSE, MMS, Modbus	Data Manipulation, MITM, FDI	IED trip & circuit breaker status	malicious circuit breaker tripping at PCC causes unintentional switching from grid-tied to Island and vice versa causing potential outage. But, can be easily rectified by toggling circuit breaker to manual mode.
		sensor readings, command actuator	Stealthier approach that creates long-term impact (i.e., monetary, equipment lifespan). Mask all measurement readings on SCADA-HMI and tamper the dispatch control functions (i.e, AGC).

driven towards long-term adversarial impact (i.e., monetary, equipment lifespan) that goes undetected for months of operations. We plan to open source our collected attack traces to help promote the awareness of potential attack techniques and tactics, and also to help evaluate different cyber defense solutions [13, 12].

Table 2. Microgrid dispatch function overview (simplified for islanded operation only).

Elements of the Function	**Function Characterization**	**Parameters & Metrics**
DER control & command	single dispatch	P,V,Q,f meets operating requirements
	coordinated dispatch	
Load management	demand response, load prioritization & shedding, load scheduling (BESS)	balance supply-demand, freq. deviation within threshold
Dispatch control	look-up table	dynamic response, quantify performance
	optimization problem	
Voltage regulation & power quality	inverter-based volt/var control, constant freq. control	V,f, deviate within operating limit, inverter quality (THD), %flicker, rapid voltage change (RVC)
Switching device	control commands	device status
Data acquisition	sensor request/response	signal availability, measurement accuracy

2 Dispatch Function for Islanded Microgrid Operation

Consider a microgrid that consists of rooftop solar PV systems, battery energy storage systems (BESS), and two backup diesel engine-driven synchronous gensets, which is interacting with the external grid at one point, t, but, intentionally islanded at (t+1). Such automation can be well directed by a centralized microgrid controller, programmed with operating costs minimization dispatch function while considering power quality management. Before the microgrid decouples itself from the external grid (i.e., opening of circuit breaker at point of common coupling (PCC)), under steady-state condition for islanded operation, the dispatch function specifications must include [5]:

- full access to DER asset control & command, individually or collectively.
- load control management; critical, non-critical, and adjustable loads.
- optimal dispatch to satisfy operational requirements (i.e., grid-forming — gensets running in isochronous mode to maintain system inertia while inverter-based DERs operate in droop mode).
- Switching control of circuit breaker, and other switching devices.
- System reliability and power quality (i.e., voltage regulation) using inverter-based Volt/Var control.
- V/f control in grid-forming operation and synchronization for load sharing (i.e., isochronous generator & BESS).

The list of dispatch control requirements in Table 2 are interdependent of each other as they ensure operational stability during Islanded, and if any of these establishments were to fail, it can lead to a cascading tripping effect or worst, connected equipment or appliances getting severely damaged. The dispatch function generates and executes control orders (i.e., sets of commands)

to appropriate assets based on the received state information. Although the dispatch function for a Microgrid control does cover a wider range of operations that includes black start, grid-connected, re-connection from Island to grid-connected and vice versa, however, we limit our discussions to only steady-state dispatch function for Islanded Microgrid as we want to relate our attack strategies on these functional requirements (see Sec. 4 & 4.4).

3 Communication Protocols and Standards for Microgrid

Modern power grid communication technology has evolved from a serial communication architecture to an Ethernet-based network as seen in Fig. 1. Such advancement is required to support the increasing integration of diverse monitoring devices (i.e., IED, smart meters) and data-driven intelligent systems (i.e., PLC, RTU). The transition from analog to digital channels enables reliable synchronicity and scalability, allowing for data transfer over long distances. In the following, we review several communication protocols and discuss their applications in modern power grid system. Table 3 summaries the communication data flow (i.e., protocols) against different applications.

IEEE 1815 – The IEEE 1815 standard, also known as DNP3, is an open standard protocol that defines communication between process control systems. It provides a lightweight method of transferring simple data for control and data acquisition purposes. It is a polling protocol in which the master can poll the slaves for data. The slaves (i.e., outstation) can also transmit data to the master without being polled. This can occurs if there have been changes since the last poll or if certain parameters are met. Regarding security, the DNP3 protocol uses TLS encryption to protect TCP/IP channels and supports an optional secure authentication mechanism to authenticate specific requests.

IEC 61850 — The IEC 61850 standard defines the functional requirements for grid communications. The result of this standardization is the definition of data models and services that can be used to enhance process automation and device interoperability. This standardization enables devices to map power system functions to MMS, GOOSE, or SV protocols for communications.

- **MMS** is a client/server communication protocol. It utilizes the TCP/IP protocol stack to ensure reliable message delivery. It is used for time-insensitive applications such as file transfers, data management, remote control of plant operations, and remote monitoring of devices. The standard defines $\approx$ 87 MMS services to support read, write, modify, create, and delete data operations. The MMS client sends a service request to the MMS server and the server responds back with the requested data.
- **GOOSE** is a layer 2 protocol that operates over the Ethernet. It is used for fast data transfer between IEDs — mainly to provide protection relay operations. It detects faults in the system and initiates fault responses, such

as tripping the circuit breakers. Other functionalities include transmitting up-to-date information about the state of the power system, e.g., status and fault messages. Each GOOSE message contains a status number (stNum) and a sequence number (sqNum) to monitor any event change in the system. When a new event (e.g., a breaker trip signal) occurs, the stNum value will increment by 1 and sqNum will reset to 0. This is followed by a burst of transmissions to ensure that all subscribed IEDs receive the state change. If there is no event change, only sqNum is incremented. We note that the GOOSE contents are not encrypted and, thus, susceptible to poisoning attacks [8, 3].
- **SV** is an Ethernet-based protocol for sending voltage and current samples between MUs and IEDs. Each SV packet is indexed by a sample count (smpCnt) value that increments each time the MU sends a new message. Each packet contains a dataset comprising eight digitized values; 3-phase voltage with neutral and 3-phase current with neutral. Unlike GOOSE protocol, there are no re-transmissions in SV. The sending interval for SV messages depends on the sampling rate (smpRate), which according to the standard, is defined as 80 samples per cycle for basic protection and 256 samples per cycle for measurement applications. For a 50 Hz power system, the sending rate is 250μs for protection and 78.12μs for measurement.

Modbus is a legacy communication standard used by many power grid operators. It is well supported by many device manufacturers due to its simple message structure. The protocol is based on a master/slave architecture where one master device can poll one or more slaves to request data. The slaves cannot initiate communication with the master devices. Modbus protocols include Modbus ASCII and Modbus RTU for serial communications, and Modbus TCP/IP for Ethernet communications. The difference between Modbus ASCII and Modbus RTU lies in the way the data is encoded. Modbus ASCII encodes data using ASCII characters while Modbus RTU uses binary encoding. Thus, Modbus ASCII requires more bytes to transmit than Modbus RTU. On the other hand, Modbus TCP is a Modbus RTU packet encapsulated in TCP/IP headers to facilitate data transfer over the Ethernet networks. Despite the different encoding formats, each Modbus payload begins with a function code followed by the data value. The function code determines the types of operation (read/write) and register types. For example, function code 16 represents a write operation to multiple holding registers. A function code of value 5 represents a write single coil operation.

IEC 60870 –The IEC 60870 standard defines the functional requirements for systems used for telecontrol which are supervisory control and data acquisition. The result of this standardization is to fulfill the special requirements of communication and co-ordination between control centers which are not defined in DNP3 and IEC 61850. For instance, both IEC 60870-5-101 and IEC 60870-5-104 are used to transmit SCADA data. The difference is that IEC 60870-5-101 is

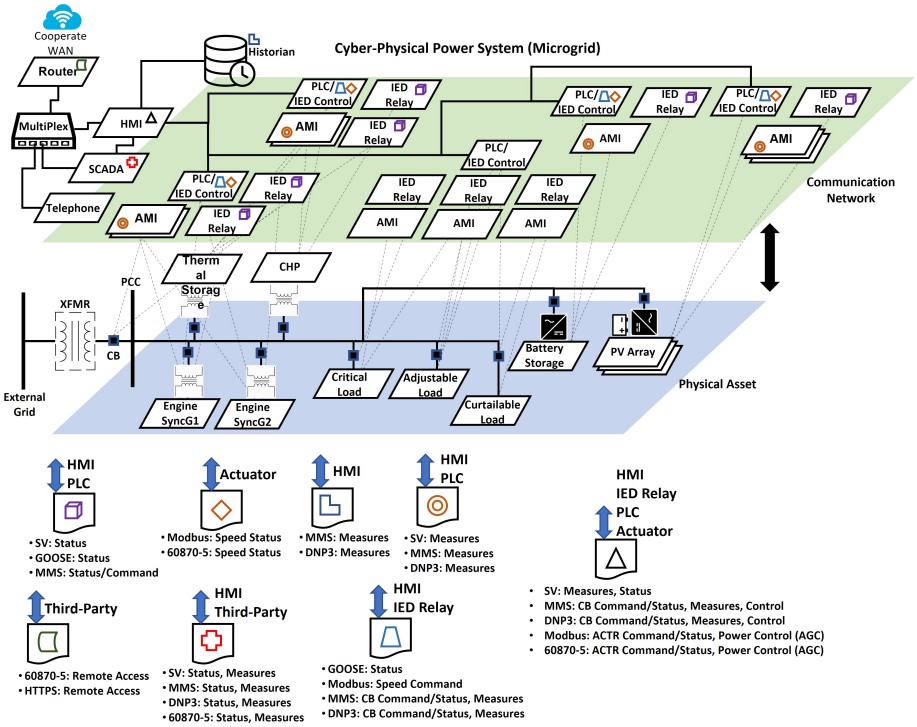

Fig. 1. The cyber-physical infrastructure of microgrid, interacting with physical devices using different communication network protocols and standards.

based on serial communication (such as RS-232, FSK based modems) while IEC 60870-5-104 is the network access for IEC 60870-5-101 using standard transport profiles. IEC 60870-5-101 supports partyline (polling, multipoint, multidrop, unbalanced) and point-to-point operation mode. IEC 60870-5-104 only supports point-to-point operation mode.

As an example, we will look into the dispatch function requirements of DER Control and Command (listed in Table 2) for islanded operation, e.g., generator synchronization and automatic generation control (AGC) involving two diesel engine-driven synchronous generators as seen in Fig. 1. We assume that the microgrid is initially operating in grid-tied mode and we want to transition its operations into islanded (stand-alone) by opening circuit breaker at PCC. The control logic is as follows:

- Ensure the the circuit breaker at PCC is at close position and monitor the exchanged power flow to determine the total demand load consumed by Microgrid.
- Calculate the total available power generation locally (i.e., generators, CHP, solar PV, BESS). If $P_{Ld} \leq P_{gen}^{max}$ then, perform Islanding. If no, proceed with load curtailment first until the criterion meets.

Table 3. Network protocols for different applications.

		Protocols						
		IEC 61850			**IEEE 1815**		**IEC 60870**	
	Secure	GOOSE	MMS	SV	DNP3		IEC	HTTPS
Applications	**Unsecure**					Mod bus	60870 -5-104	HTTP
Supervisory Control & Data Acquisition (SCADA)				X	X	X	X	
Distributed Energy Resources Management System (DERMS)			X			X		
Advance Distribution Management Systems (ADMS)				X	X			
Isochronous generator control						X	X	
Distribution automation systems (DA), integrated with substation, ADMS, or communications				X	X			
Protection communications within the substation		X		X				
Protection communications outside the substation (to another substation)		X					X	
Equipment monitoring (transformer, breaker, battery, etc.)			X		X	X		
Power quality monitoring			X	X	X	X	X	
Metering (i.e., AMI, IED)			X	X	X	X	X	
Planning & design								X
Cyber access control and monitoring								X
Third party access (remote vendors)			X					X
LAN/WAN management, monitoring and control							X	X
TCP Port		NILL	102	NILL	20000	501	2404	80 443

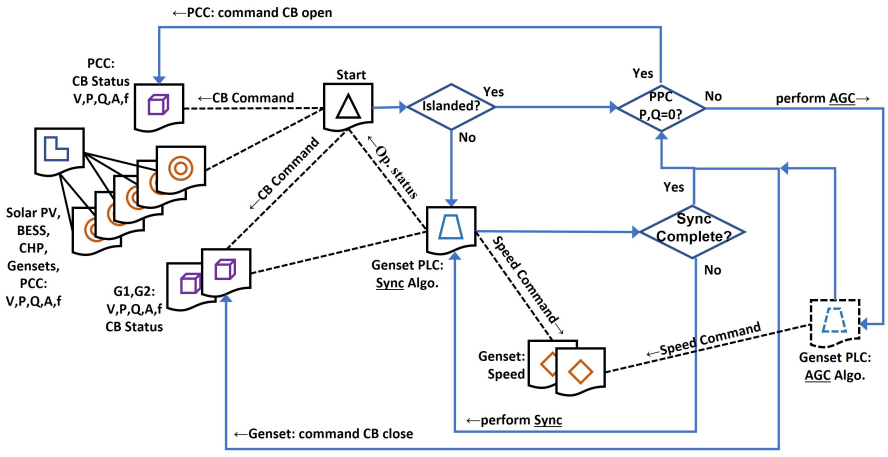

Fig. 2. Process flow of communication protocols to perform gensets synchronization and AGC based on DER control and command dispatch function, transitioning from grid-tied to islanded operation (symbols refer to Fig. 1).

- Command to run the synchronous generators offline until the operating frequency is leveled with the grid (i.e., 50/60Hz).
- We perform generator synchronization with the grid by adjusting the rotating speed in real-time to align the phase angle. Once align, close the circuit breaker of the affiliated genset. Do the same process for the subsequent gensets.
- Once these gensets have successfully coupled to the grid, we launch AGC algorithm to attune the gensets' generation output (speed control) until P, Q at PCC is zero.
- Once the Microgrid assets have took full control over the demand loading and secure the power quality, open circuit breaker at PCC.

Referencing from Fig. 1, Fig. 2 illustrates the data flow process in relations to the control logic listed above.

4 Case Study: Attacks on Microgrid Dispatch Functions

Using the dispatch function provided in Table 2, e.g. DER control and command for generator synchronization and AGC (see Fig. 2), we aim to evaluate the feasibility and adversarial impacts on microgrid dispatch function. We target our attacks on several communication protocols and verify them on the Electrical Power and Intelligent Control (EPIC) testbed. EPIC [11] is a power grid testbed located in Singapore, designed for cybersecurity researchers to conduct experiments and assess effectiveness of cyber attack and defense mechanisms.

4.1 EPIC System Overview

In our experiment setup, we configured EPIC to operate similar to our dispatch function for Islanded microgrid employing; 2 Variable Speed Driver (VSD) driven generator sets, each rated at 15kVA, equipped with protection relay and remote controlled circuit breaker, a 21kVA Loadbank, and a 34kW MPPT-based PV. Both the generators operate in isochronous mode and uses synchrophasor to establish synchronization during parallel operations. Moreover, with in-built automatic generation control (AGC) capability, users can control the amount of output power generation of each gensets from SCADA.

EPIC uses the IEC 61850 MMS protocol that operates over the TCP/IP model and IEC 61850 GOOSE protocol, which is capable of obtaining responses from different parts of the system within 4msecs. It includes standard features such as standardization of data names, fast transfer of events and data storage, and device interoperability. GOOSE and MMS are used in the ring network for data transfer between IEDs and the SCADA workstation. The field bus communication among physical processes to PLCs, master PLC, and SCADA is realized through wired channels. The PLC uses Modbus TCP/IP protocol to send commands to actuators.

4.2 Attacks on IEC 61850-based Communication Protocols

Assuming that we have gained visibility on EPIC's network, we launch the attack on either GOOSE or MMS packets as seen in Fig. 3. Although the attack objectives on these protocols deemed successful, some do not imply any adversarial impact on Islanded microgrid operation and attack traces were easily identified on HMI.

GOOSE Packets The GOOSE packets in EPIC works through a publisher-subscriber mechanism on a broadcast service, thus, from SSW2, we are able to gain visibility on all connected IEDs of different network rings. We duplicate the MAC address and masquerade as legitimate IED (i.e., MIED1) and begin injecting malicious GOOSE packets into the traffic using Denial-of-Service (DoS), High Status Number (HSN), and False Data Injection (FDI) attack approach.

- **Denial-of-Service**: In DoS attack, we flood the network with malicious GOOSE packets to prevent legitimate IEDs from receiving critical messages or updates. We inject 1000 dummy GOOSE packets posing as MIED1 with *stnum* in running number sequence (but larger than the legitimate MIED1's GOOSE packet) while *sqNum* set to zero. When DoS attack was underway, we observed that all alarms associated with the protection relay coupled to MIED1 were triggered maliciously, and real-time sensor measurements of MIED1 reflected on SCADA (MMS packets) were replaced with "question mark" icon. This verifies that attack objective is successful, leaving the network lost in the flooded transmission while awaiting for a legitimate GOOSE packet from MIED1. This poses an issue when operator wants to

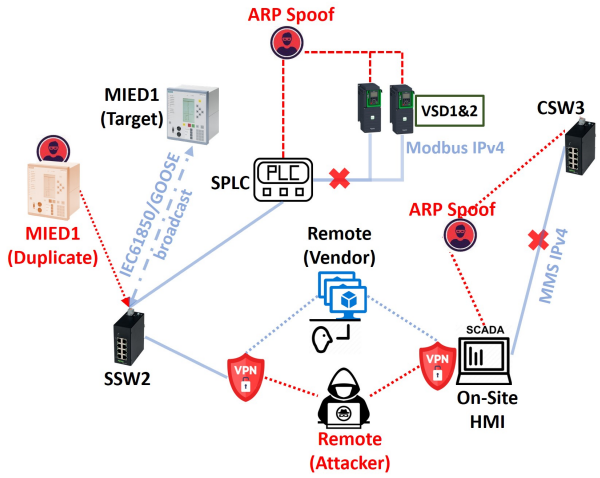

Fig. 3. Attacks on different communication protocols in IEC 61850 and Modbus. Masquerade as MIED1 to inject malicious GOOSE packets into the network, and perform MITM attack to intercept MMS and Modbus packets between user and an application and ultimately modify the packets' payload on the EPIC.

perform a manual synchronization between the incoming and running generators due to ambiguity in the phase angle differences ($\Delta\theta^{\circ}$) shown at SCADA (synchrophasor). Likewise, in the dispatch function for Islanded operation, synchronization serves as the core requirement to bring these gensets online before microgrid can decouple itself from the grid. Operating in isochronous, they provide inertia to IES and inverter-based DERs online; thus, without them, microgrid must remain grid-tied. Even if the DoS attack is launched during Islanded, where only a single genset is running and the operator intend to bring the incoming genset online to meet the high demand capacity during the next period, operator is forced to revert back into grid-tied mode and, if left unattended, the microgrid will collapse as frequency will dip and genset being overloaded.
Contrarily, in practice, the DoS attack has no implication on the microgrid's operation, e.g., successfully establishing synchronization, because; (a) the synchronization is done automatically by the PLC, (b) the PLC is able to take reference from MIED2, $\Delta\theta^{\circ}$. If EPIC is already operating in parallel mode, then, it has no impact on the system's stability and operation of AGC. In view of the attack traces, operator can identify the problem had surfaced from MIED1 as shown in SCADA. Hence, the attack objective is met but had no negative impact on grid operations.

– **High Status Number**: Instead of flooding the network with malicious GOOSE packets, we inject a single malicious GOOSE packet with HSN ($stNum$=5000) into the network posing as MIED1. The HSN takes precedence over any legitimate GOOSE packets coming from MIED1. In the-

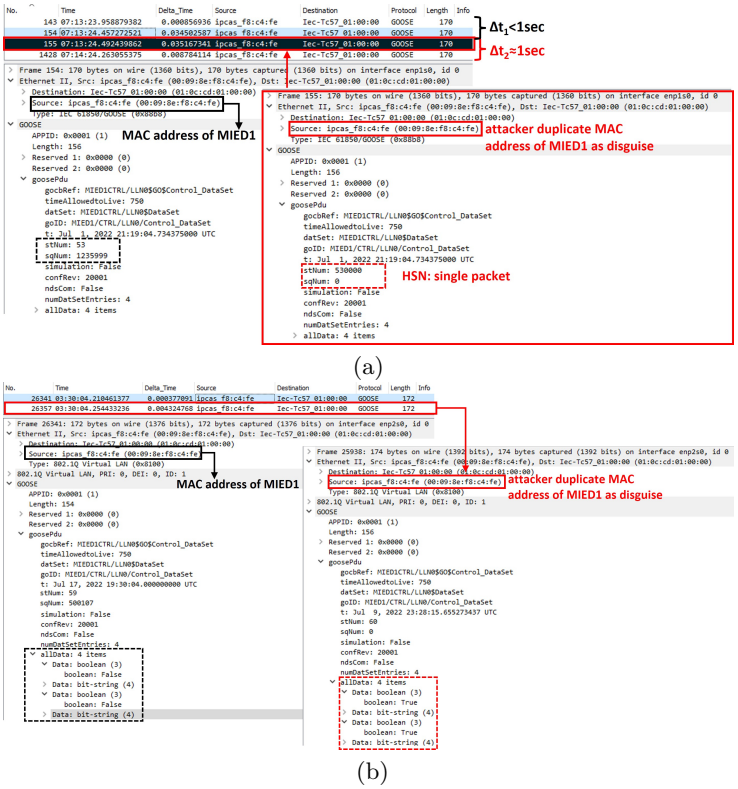

Fig. 4. Masquerade as MIED1 and inject malicious GOOSE packet into the network. (a) HSN attack introduces a delay in broadcasting GOOSE packets by injecting a single packet. (b) Modifies the GOOSE packets' payload (Boolean values) for malicious circuit breaker tripping.

ory, the network drops any MIED1's GOOSE packet with smaller $stNum$ and holds on to HSN-infected GOOSE packet the network. Hence, some researchers have reported that HSN attack offers a stealthier attack approach as compared to DoS attack and yet gained similar outcome, e.g., flooding of GOOSE packet can be easily detected visually but not for single packet injection. Contrarily, in practice, neither the network nor physical systems suffered any implication as to what we have seen in DoS attack. Legitimate GOOSE packets with lower $stNum$ from MIED1 were still picked up in the network after the HSN-infected packet as shown in Fig. 4(a). There was a persistent 1sec transmission delay between the HSN-infected GOOSE packet and the next legitimate packet whenever HSN is launched compared to a normal GOOSE packet transmission. Regardless, the HSN-infected GOOSE packet failed to achieve its attack objective and worst, had no negative impact on both the network and physical operations.

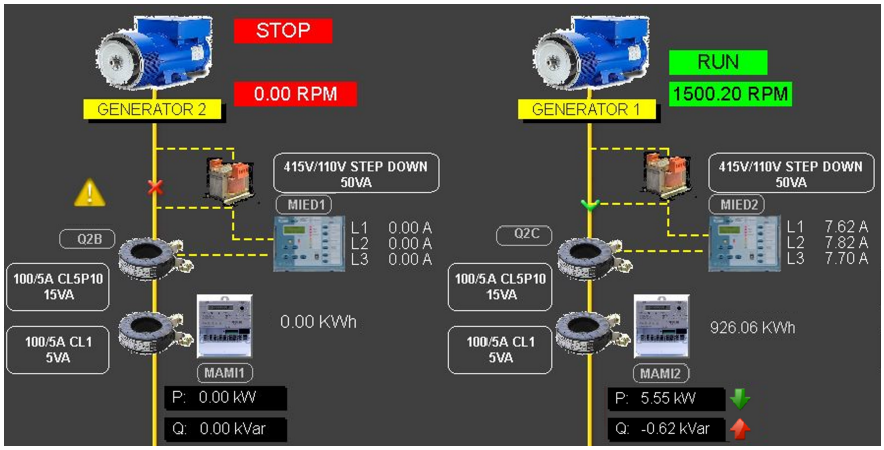

Fig. 5. Impact on EPIC under data manipulation attack, attacker posing as MIED1 and broadcast into the network indicating that Q2B is tripped and in open position.

– **Data Manipulation** In data manipulation attack, we aim to modify MIED1 GOOSE packets' payload. The payload contains two pairs of data item representing the status of circuit breaker Q2B affiliated to MIED1; trip status and mode open status. By modifying the payloads' values from False to True and injecting the packets into the network as shown in Fig. 4(b), we aim to broadcast malicious status of Q2B being tripped and in open position. We specify $stNum$ in running sequence, $sqNum$ to zero, update the timestamp to conform a legitimate GOOSE packet, and modify both the Boolean values to True. The attack generates a significant impact on the physical system as seen from Fig. 5 where Generator 2 was forced to stop spinning and an alarm "trip" is flagged. The alarm is broadcast to the speed drive controller of Generator 2 causing it to intentionally break as mandated by the protection control logic. We can expect similar adversarial impact on microgrid under the data manipulation attack on gensets' IED. Despite an eventful attack sequence, i.e, forcing Generator 2 to decoupled from the grid and leaving Generator 1 serving the demand load alone, operator can easily pinpoint the problem caused and trace the attacker's footprint. Meaning, operator can manually reset the breaker and switch to manual operation. If the alarm persist, then the problem is isolated to the circuit breaker command running in the background. However, in times where demand load capacity is high (i.e., $\mathrm{P}_L > \mathrm{P}_{G1}^{max}$) and data manipulation attack is underway, an intentional tripping can propagates towards Generator 1 as it is now overloaded.

MMS Packets We direct our attacks to modify gensets' IED MMS packets' payload to make synchronization process unresponsive on the incoming genset as shown in Fig. 3. The objective is to launch man-in-the-middle (MITM) attack and intercepts MMS packets from IEDs to PLC and modify its payload

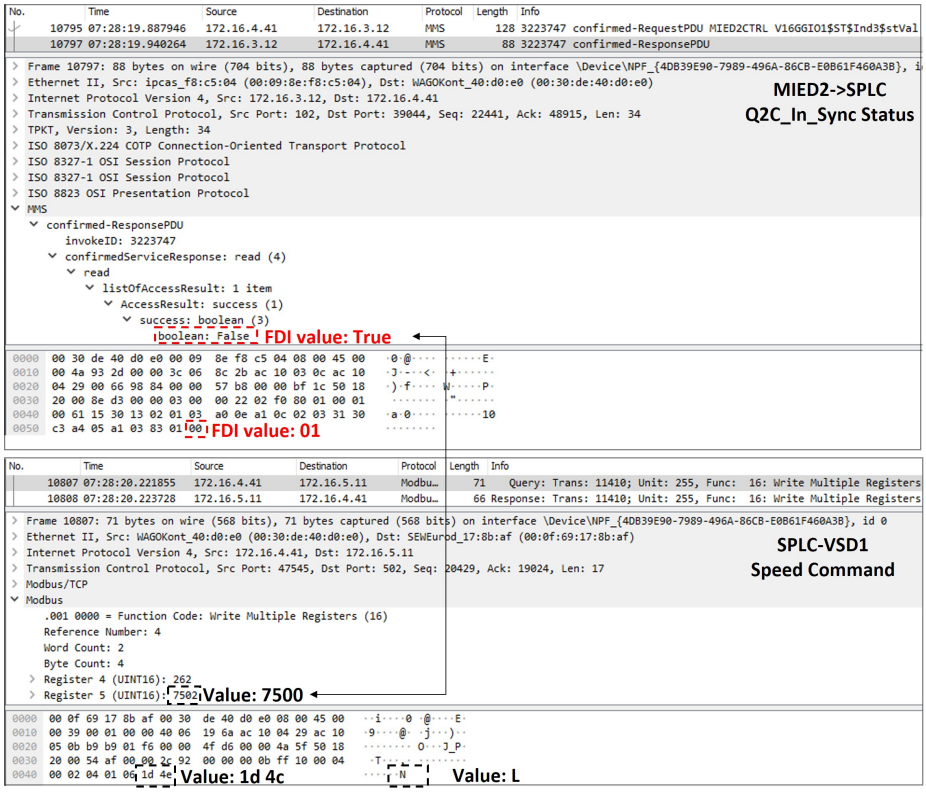

Fig. 6. Malicious insider MITM attack on MMS packet between PLC and IED1/2 and tamper MIED2 MMS's payload with false declaration on the synchronization status. TRUE at all times even before initiating synchronization.

(i.e., synchronization status) as seen in Fig. 6. Based on the control logic defined in generators' PLC, if the in-synchronization status is TRUE, it signifies that both gensets have established synchronization and there will no command change on the speed values leaving the associated circuit breaker in the open position. While, if it is False, PLC will initiate the synchronization algorithm and closes the circuit breaker once its phase angles converges with the running genset (by attuning the incoming genset's speed). This attack approach is feasible to an untrained attacker who has no prior knowledge on generator synchronization process as it exploit operational status instead of implementing physical changes to influence the status, e.g., tampering the synchronous speed during synchronization to ensure the status remains False). Moreover, pinpointing attacks on IED would be an intelligent guess for an attacker as it holds vital information on equipment status and measurements which are gold for data-driven industrial control.

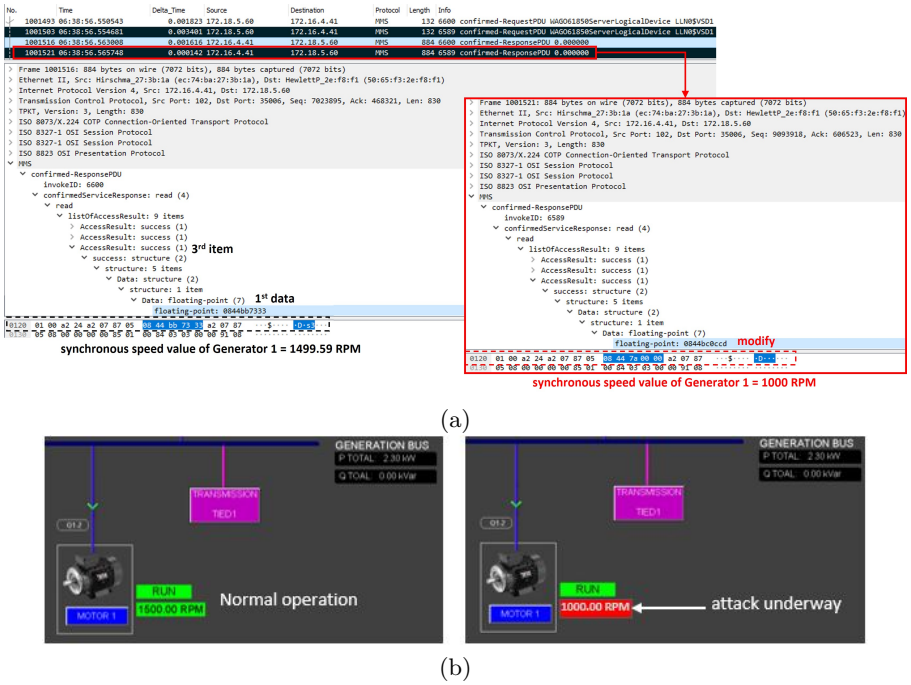

Fig. 7. Performing MITM attack on MMS packets' payload coming from PLC to HMI, modifying Generator 1's synchronous speed values away from its true values. (a) Modifying MMS packets' payload, generator speed. (b) Adversarial impact on HMI with the modified values.

Contrarily, we target our attacks on MMS packets coming from PLC to HMI as seen in Fig. 3. These packets' payload contains real-time sensor measurements of the physical systems' performances and also some remote control functionalities for microgrid operations (i.e., switching of circuit breakers and load capacity selections). Likewise, we will perform MITM attack to redirect the packets' payload for tampering, e.g., modify the SCADA's real-time synchronous generator's speed value to 1000rpm using MITM attack and mask its true values as seen in Fig. 7(a). In consequence, the modified synchronous speed value is updated on the SCADA workstation, deceiving grid operators its true operating behavior as seen in Fig. 7(b).

4.3 EPIC Modbus Communication Network

In this section, we direct our attacks on the Modbus communication coming from PLC to actuators as seen from Fig. 3. The objective is to launch MITM attack to redirect those Modbus packets containing gensets' synchronous speed values commanding individual VSDs and perform FDI attack to modify their payloads.

To a trained attacker who has knowledge on generator synchronization process, tampering of these synchronous speed values not only hinders the synchronization process but also derail the AGC performances causing negative economic standpoint and destabilizes the grid's operating frequency beyond the threshold limits. In this attack sequence, we aim to create a non-responsive synchronization process between the running and incoming genset.

Synchronization of gensets is governed by a closed-loop speed controller that commands incoming genset's VSD to ramp-up or -down until the phase angle differences between both gensets is less than $\pm 1°$, e.g., PLC commands VSD1 (Generator 1) to spin at 1500.4rpm (or 7502 sent via a Modbus) until the phase angle aligns with Generator 2. Once achieved, immediately, Generator 1's circuit breaker (Q2C) will close and the user-defined AGC algorithm takes over the speed controller. Moreover, ordering of these gensets' synchronous speed values must not deviate by more than 1rpm to avoid introducing unintentional frequency swelling or dipping (± 1%Hz). Fig. 8(c) illustrates the synchronization control sequences during normal operation followed by a balanced AGC (i.e., 50%-50%).

However, when FDI attack is underway, e.g., assigning Generator 1 speed command constant at 1500rpm (Modbus command 7500) as seen in Fig. 8(a), $|\Delta\theta°|$ failed to converge thus leaving Q2C to remain open. This forces Generator 2 to serve the total load capacity alone, raising the concern that it could overload as demand capacity reaches its peak at (t+1.) Alternatively, we can alternate high/low speed values to render unstable $|\Delta\theta°|$ profile (oscillating), but, exploiting these values can easily trigger bad data detection in state estimation.

Although FDI attack has little impact on the microgrid's stability (i.e., healthy frequency/voltage levels), from economical viewpoint, it hampers the ability to achieve optimal unit-commitment for economic dispatch. Even so, the implications can get serious when the attack is strategically launched during peak demand periods where incoming gensets are needed online to share the load capacities and maintain frequency levels at nominal. Seen from Fig. 8(b), at tail end of the graph, it shows that an overloading alarm is flagged (>9.5kVA) on Generator 2 when the load capacity increases to 10kW as compared to a successful synchronization where gensets are operating at 50% loading.

4.4 Coordinated Attacks Targeting Multiple Protocols

From the case studies learned in Sec. 4.2-4.3, we aim to formulate a stealthier attacks on EPIC by targeting different combination of communication protocols, coordinated attacks. We define stealthy as the act of deceiving the grid operators comprehending from what is shown on the HMI versus the true operations of the physical systems. The attack objective is driven towards long-term adversarial impact during Islanded operation, e.g., to incur high operating costs and depreciate equipment lifespan exponentially. We point the attack vectors on the communication protocols of several dispatch control functions and synchronize the attack on; DER control and command (synchronization of isochronous

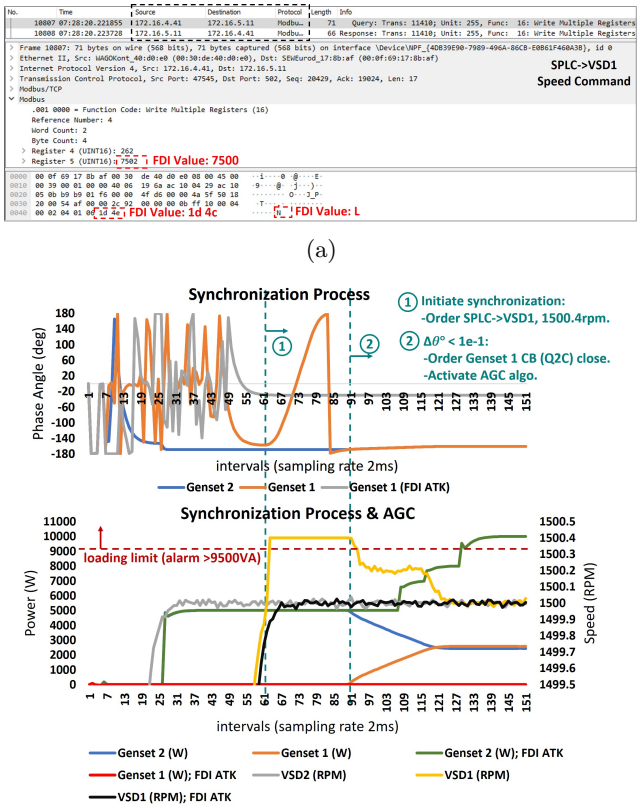

Fig. 8. Malicious insider MITM attack on Modbus packet between PLC and VSDs. (a) Tampering the Modbus packets' payload (i.e., synchronous speed) of incoming genset to cease the synchronization process. (b) Comparative profiles of gensets' power generation capacities, phase angles differences, and speed command, under attacking and non-attacking scenarios during the synchronization process.

generators), dispatch control (AGC), and switching device (circuit breaker at PCC).

Procedure 1 guides attackers in gaining the initial state operation of the microgrid, e.g., grid-tied, islanded. Once appreciated, attacker can program to raise an alert whenever the microgrid is transitioning between grid-connected mode and islanded mode. Assuming the microgrid is transitioning from grid-tied to islanded mode and gensets are in the process of synchronizing (isochronous generators), attacker proceeds to execute stealthy attack on DER control and command. We aim to cease the synchronization process forcing microgrid to remain grid-tied. We tamper the speed command from PLC to gensets' VSDs (actuator) with large values which then forces synchrophasor unable to converge.

However, we need to strategically attune the tampered speed values within the operating frequency threshold ($\pm$0.5Hz) as not to render obvious anomaly that could potentially trip the genset due to overspeed.

Procedure 1 *Stealthy attack on DER control and command.*

Step 1: *Perform reconnaissance on the following packets:*

- *Modbus packets: speed command and status.*
- *MMS packets: synchronization status.*
- *circuit breaker located at PCC.*

Step 2: *modify speed command values to actuators by increasing it speed within the operating frequency limit.*

Step 3: *Update speed measurements on HMI with dummy values by displaying nominal operating synchronous speed value.*

Procedure 2 guides attackers in executing stealthy attack on dispatch control (AGC). Upon establishing synchronization and Microgrid is operating in Islanded mode, we intent to force one of the two gensets to operate near its rated operating power limit without intentionally tripping it. To achieve this, we tamper the AGC settings of a single genset, i.e., assigning to its maximum loading without causing reverse power on other generators, constantly stressing the targeted genset to cover high percentage of demand loading. Such operation also causes negative implication on the economic dispatch (minimization of operating costs). However, on HMI, the sensor measurement are in accordance to the user-defined AGC.

Procedure 2 *Stealthy attack on dispatch control during Islanded.*

Step 1: *Perform reconnaissance on the following packets:*

- *Modbus packets: speed command and status.*
- *MMS packets: speed value measurement, generator output power and maximum loading threshold, load capacity.*
- *GOOSE packet: CB status;*

Step 2: *Update sensor measurements on HMI with dummy values:*

- *compute the total active and reactive power of gensets.*
- *compute the desired output power of each gensets based on user-specified AGC settings.*
- *Inject computed power generation measurements into HMI.*

Step 3: *modify the AGC in the background, ramping up the synchronous speed without causing reverse power on the other genset. Disable the generator's maximum loading threshold*

Procedure 3 guides attackers in executing stealthy attack on circuit breaker at PCC. We aim to deny transitional operation from Islanded to grid-tied mode by tampering the IED status of PCC. In consequence, option to initiate grid-tied transition is unabled on HMI unless switching it to manual operation and may imply to operator that the circuit breaker is faulty in automation mode and will need replacement.

Procedure 3 *Stealthy attack on circuit breaker switching event*

Step 1: *Perform reconnaissance on GOOSE packet, CB status.*
Step 2: *Update CB status at PCC to trip and always in open position.*

5 Conclusion

In this paper, we provided detailed case study on applying attack techniques to target the individual and multiple communication protocols used on the EPIC testbed. We studied the impacts of these attacks on the microgrid dispatch function. We show that the EPIC testbed has security vulnerabilities that attackers can leverage to disrupt operations or even cause physical damage.

Acknowledgment

This research is supported in part by the National Research Foundation, Singapore, under its National Satellite of Excellence Programme "Design Science and Technology for Secure Critical Infrastructure" (Award Number: NSoE_DeST-SCI2019-0008 and NSoE_DeST-SCI2021TG-0003), and in part by the National Research Foundation, Prime Minister's Office, Singapore under its Campus for Research Excellence and Technological Enterprise (CREATE) programme, and in part by the SUTD Start-up Research Grant (SRG Award No: SRG ISTD 2020 157). Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not reflect the views of National Research Foundation, Singapore.

References

1. Amoah, R., Camtepe, S., Foo, E.: Securing DNP3 broadcast communications in SCADA systems. IEEE Transactions on Industrial Informatics **12**(4), 1474–1485 (2016)
2. Biswas, P.P., Li, Y., Tan, H.C., Mashima, D., Chen, B.: An Attack-Trace Generating Toolchain for Cybersecurity Study of IEC61850 based Substations. In: 2020 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm). pp. 1–7. IEEE (2020)

3. Biswas, P.P., Tan, H.C., Zhu, Q., Li, Y., Mashima, D., Chen, B.: A synthesized dataset for cybersecurity study of iec 61850 based substation. In: 2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm). pp. 1–7. IEEE (2019)
4. Case, D.U.: Analysis of the cyber attack on the Ukrainian power grid. Electricity Information Sharing and Analysis Center (E-ISAC) **388**, 1–29 (2016)
5. IEEE Standard for the Specification of Microgrid Controllers. IEEE Std 2030.7-2017 pp. 1–43 (2018). https://doi.org/10.1109/IEEESTD.2018.8340204
6. IEEE Recommended Practice for Network Communication in Electric Power Substations. IEEE Std 1615-2019 (Revision of IEEE Std 1615-2007) pp. 1–140 (2019). https://doi.org/10.1109/IEEESTD.2019.8894229
7. Khodabakhsh, A., Yayilgan, S.Y., Houmb, S.H., Hurzuk, N., Foros, J., Istad, M.: Cyber-security gaps in a digital substation: From sensors to SCADA. In: 2020 9th Mediterranean Conference on Embedded Computing (MECO). pp. 1–4. IEEE (2020)
8. Kush, N.S., Ahmed, E., Branagan, M., Foo, E.: Poisoned goose: Exploiting the goose protocol. In: Proceedings of the Twelfth Australasian Information Security Conference (AISC 2014)[Conferences in Research and Practice in Information Technology, Volume 149]. pp. 17–22. Australian Computer Society (2014)
9. Nurdiana, E., Riza, R., Ifanda, I., Basharah, A.A.: Performance of 10 kWp PV Rooftop System Based on Smart Grid in Energy Building PUSPIPTEK. In: 2019 International Conference on Sustainable Energy Engineering and Application (ICSEEA). pp. 193–200. IEEE (2019)
10. Shahidehpour, M., Gong, W., Lopata, M., Bahramirad, S., Paaso, A., Zhang, C.: Transforming a National Historic Landmark Into a Green Nanogrid: The Case of Crown Hall. IEEE Electrification Magazine **8**(4), 20–35 (2020)
11. Siaterlis, C., Genge, B., Hohenadel, M.: EPIC: A testbed for scientifically rigorous cyber-physical security experimentation. IEEE Transactions on Emerging Topics in Computing **1**(2), 319–330 (2013)
12. Tan, H.C., Cheh, C., Chen, B.: CoToRu: Automatic Generation of Network Intrusion Detection Rules from Code. In: IEEE INFOCOM 2022-IEEE Conference on Computer Communications. pp. 720–729. IEEE (2022)
13. Tan, H.C., Cheh, C., Chen, B., Mashima, D.: Tabulating cybersecurity solutions for substations: Towards pragmatic design and planning. In: 2019 IEEE Innovative Smart Grid Technologies-Asia (ISGT Asia). pp. 1018–1023. IEEE (2019)
14. Todeschini, M.G., Dondossola, G.: Securing IEC 60870-5-104 communications following IEC 62351 standard: lab tests and results. In: 2020 AEIT International Annual Conference (AEIT). pp. 1–6. IEEE (2020)
15. Ustun, T.S., Hussain, S.S.: IEC 62351-4 security implementations for IEC 61850 MMS messages. IEEE Access **8**, 123979–123985 (2020)
16. Vu, T.V., Nguyen, B.L., Cheng, Z., Chow, M.Y., Zhang, B.: Cyber-physical microgrids: Toward future resilient communities. IEEE Industrial Electronics Magazine **14**(3), 4–17 (2020)