Cyber Attacks on Power System Automation and Protection and Impact Analysis

Subramaniam Rajkumar, Vetrivel; Tealane, Marko; Stefanov, Alexandru; Presekal, Alfan; Palensky, Peter

DOI
10.1109/ISGT-Europe47291.2020.9248840

Publication date
2020

Document Version
Final published version

Published in
Proceedings of 2020 IEEE PES Innovative Smart Grid Technologies Europe, ISGT-Europe 2020

2020 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe)
Virtual, October 26-28, 2020

Cyber Attacks on Power System Automation and Protection and Impact Analysis

Vetrivel Subramaniam Rajkumar*, Marko Tealane†, Alexandru Ştefanov*, Alfan Presekal*, Peter Palensky*

*Department of Electrical Sustainable Energy
Delft University of Technology
Delft, The Netherlands
v.subramaniamrajkumar@tudelft.nl

†Department of Electrical Power Engineering and Mechatronics
Talinn University of Technology
Talinn, Estonia
marko.tealane@taltech.ee

***Abstract*—Power system automation and communication standards are spearheading the power system transition towards a smart grid. IEC 61850 is one such standard, which is widely used for substation automation and protection. It enables real-time communication and data exchange between critical substation automation and protection devices within digital substations. However, IEC 61850 is not cyber secure. In this paper, we demonstrate the dangerous implications of not securing IEC 61850 standard. Cyber attacks may exploit the vulnerabilities of the Sampled Values (SV) and Generic Object-Oriented Substation Event (GOOSE) protocols of IEC 61850. The cyber attacks may be realised by injecting spoofed SV and GOOSE data frames into the substation communication network at the bay level. We demonstrate that such cyber attacks may lead to obstruction or tripping of multiple protective relays. Coordinated cyber attacks against the protection system in digital substations may cause generation and line disconnections, triggering cascading failures in the power grid. This may eventually result in a partial or complete blackout. The attack model, impact on system dynamics and cascading failures are verified experimentally through a proposed cyber-physical experimental framework that closely resembles real-world conditions within a digital substation, including Intelligent Electronic Devices (IEDs) and protection schemes. It is implemented through Hardware-in-the-Loop (HIL) simulations of commercial relays with a Real-Time Digital Simulator (RTDS).**

***Index Terms*—IEC 61850, power system protection, cyber security, cyber attacks, cascading failures, blackout**

I. Introduction

Power system automation and communication standards are spearheading the power system transition towards a smart grid. However, the increased power grid digitalization raises questions, especially with regard to, vulnerabilities and cyber secure operation of the smart grid [1], [2]. IEC 61850 is a power system communication standard used for substation automation and protection in digital substations. It enables information exchange through different communication protocols, two of which are covered in this paper. The Generic Object-Oriented Substation Event (GOOSE) and Sampled Values (SV) protocols are used to communicate substation events and measurements within a substation, respectively. Although it provides increased benefits, IEC 61850 is not cyber secure. The standard does not implement any encryption due to hard real-time requirements of trip signals for protection systems, typically in the range of 3-4 ms. This makes it highly susceptible to cyber attacks. The exploit of GOOSE protocol vulnerabilities within IEC 61850 is demonstrated in [3], [4]. It is a cause for serious concern that such cyber security vulnerabilities maybe exploited by potential attackers. Cyber attacks on power grids are a real modern-day threat. On December 23, 2015, cyber attacks were carried out on the power grid in Ukraine. Seven 110 kV and twenty-three 35 kV power substations were disconnected from the grid for hours. These attacks were the first publicly acknowledged cyber incidents to result in power outages that affected about 225,000 customers [5]. Thus, cyber security of power systems has become an important area of research [6], [7].

In related work, cyber attacks on various protections schemes, such as distance and differential protection, are discussed in [8]–[10]. Additionally, [11] proposes a mitigation measure for cyber attacks targeting distance protection through deep learning. However, in this research we focus on exploiting the vulnerabilities of the communication protocols used by relays in a digital substation and analysing the impact of such attacks on grid dynamics. Therefore, the particular attack model studied in this research is independent of the type of protection schemes used by the targeted protective relays. Earlier work on cyber security of power systems has demonstrated, how substation communication networks can be compromised in various ways [1], [12]. Cyber security exploits within the IEC 61850 standard have been widely studied and discussed in literature [12], [13]. The susceptibility of the Manufacturing Messaging Service (MMS) to session hijacking, replay attacks and packet sniffing and spoofing is shown in [14]. However, within the standard, two protocols are of major importance – GOOSE and SV. They are used to communicate critical measurements and commands within a substation in real-time. Therefore, they directly affect the protection and automation functionalities within a digital substation, making them impactful targets for cyber attacks. The various vulnerabilities and exploits of GOOSE and SV protocols are extensively discussed in [3], [4], [15], [16]. Previous work in this field has clearly established and demonstrated how IEC 61850 protocols are vulnerable to cyber attacks and may have dangerous implications on the physical power grid. However, what is found missing is the study and impact analysis of these cyber attacks on power system dynamics.

978-1-7281-7100-5/20/$31.00 ©2020 IEEE

This is extremely crucial as the implications of cyber attacks on the physical level of the grid may be devastating, causing equipment damage or even a blackout. Hence, this research seeks to address how such cyber attacks may lead to cascading events and a blackout. The key contributions of this work are as follows:

1) Investigation and demonstration of the impact of cyber attacks within a digital substation on power system dynamics. We consider typical protection schemes, i.e., distance, out of step, frequency, and voltage, implemented by IEC 61850 compliant relays. We model cyber attacks that exploit the previously demonstrated weaknesses of GOOSE and SV protocols focusing on network reconnaissance and attack execution. In this research, we build upon the proof of concept that cyber attacks against IEC 61850 can make relays trip, open circuit breakers, and cause system instability. We investigate the impact of such attacks on system dynamics and how they initiate cascading events such as line and generator disconnections, causing a blackout.
2) Experimental verification of the physical implications of cyber attacks on power system dynamics. This is achieved using a proposed cyber-physical experimental framework that closely resembles real-world conditions within a digital substation, including Intelligent Electronic Devices (IEDs) and protection schemes. It is implemented through Hardware-in-the-Loop (HIL) simulations of commercial relays with a Real-Time Digital Simulator (RTDS) that simulates the power grid. The cyber attacks on the digital substation are experimentally shown to lead to cascading failures and a partial or complete blackout.

The proposed experimental framework is a comprehensive representation of the power system and a digital substation, including both IEC 61850 GOOSE and SV protocols and operational technology components within the substation. Thus, it is a Cyber-Physical System (CPS) that can be used to develop methods and tools to analyse and defend the digital substation from cyber attacks. The focus of this paper however, is on the impact analysis of cyber attacks within a digital substation on the physical power system. The framework is used to highlight the dangerous implications of not securing the substation automation and protection functionalities within the substation. As a demonstrative example, we study a man-in-the-middle cyber attack that exploits the security vulnerabilities of the digital substation. Man-in-the-middle attack is selected because, this type of attack is vendor neutral, in comparison to a node-based attack. This enables the possibility to conduct the attack in substations with different topologies that use IEC 61850. Additionally, this attack causes significant impact on the automation and protection functionalities within a substation, as explained in [13]. The man-in-the-middle attack targets one compromised substation and is confined to its boundaries. Hence, by gaining access to the compromised substation communication network, packet sniffing and reconnaissance can be carried out. The cyber attacks may be realised by injecting spoofed SV and GOOSE data frames into the substation communication network at the bay level. This leads to blocking or tripping of protective relays in digital substations. Subsequently, it results in protection maloperation or disconnection of multiple generation and transmission lines, respectively. Hence, coordinated cyber attacks on one or more protective relays in digital substations may induce cascading failures, leading to a partial or complete blackout.

II. Power System Automation and Protection

The main objective of power system automation and protection is to ensure system stability and security. Power system protection schemes are based on multipurpose digital relays. In addition to protection functions, the digital relays can communicate with control centres, perform control actions, and log data from system events.

A. Distance Protection

The most widely used protection scheme for transmission systems is distance protection. The distance relay operates on the principle of comparing the line voltage and current to obtain their ratio. Typically, for transmission line protection, a relay's instantaneous tripping zone, i.e., zone 1, is set with a reach of 80-90% of the line impedance [17]. This corresponds to 80-90% of the physical line length. Faults beyond that point on the line, i.e., at the far end, are tripped by the next protection zone, i.e., zone 2. The second zone also includes a time delay, usually set between 150 to 400 ms. This setting is recommended to be above 120% of the line impedance, in order to provide enough safety margin for faults at the extreme ends of a transmission line [18].

B. Out of Step Protection

Out of step protection is implemented at the interface of synchronous generators with the power grid, to avoid prolonged asynchronous operation. It uses the rate of change of impedance to determine a power swing condition and the resulting out of step operation. Due to large variations in voltages and currents during an asynchronous condition, other protection functions, such as distance protection, are blocked if a power swing is detected. This is done in order to avoid maloperation of the relays. In predetermined parts of the system, out of step protection is usually set up to contain disturbances through controlled islanding of the power grid [19].

C. Frequency and Voltage Protection

If the power system is heavily loaded, then an unwanted or unforeseen trip can lead to substation voltages going out of limits for nominal system operation. In order to restore the system voltages to nominal conditions, Under Voltage Load Shedding (UVLS) schemes are employed [20]. Once the voltage drops below what is an acceptable threshold, e.g., 0.90 p.u, the protection function is activated and results in load disconnections from the grid. Typically, the load sheds occur

in percentage increments of total load demand with certain time delays, usually in the range of a few seconds. Therefore, in theory, cyber attacks on IEDs serving as protection devices within substations can result in disconnection of generators or lines. This sudden disconnection of lines or generators from the system can lead to a deficiency in generation or load, causing fluctuations in the system frequency. Subsequently, this can result in load shedding. In most power systems, an Under Frequency Load Shedding (UFLS) system is in place. Load is usually shed in multiple increments with predetermined time delays [21]. Conversely, with large load disconnections, the governors of the generators may not be fast enough to react. For this case an over frequency protection is implemented. This protection is based on a frequency-time curve depending on the type of generation units. For most types of power-plants, the immediate disconnection of the plant happens at 10% higher than nominal frequency [22]. Since cyber attacks aim at opening circuit breakers unexpectedly, they can result in load shedding and generation disconnection.

D. IEC 61850

Within the IEC 61850 standard, the GOOSE protocol is used to issue tripping and blocking commands originating from protective relays in a substation. Consequently, manipulating GOOSE data can cause unwanted relay trips and opening of circuit breakers. On the other hand, the SV protocol defines the specific communication service for the exchange of sampled values. They contain direct measurements, i.e., voltages and currents from merging units. These values are sent to IEDs for utilization in protection functions. A typical rate for SV communication is 80 samples/cycle which is equivalent to 4 kHz in a 50 Hz power system. The layout of a digital substation communication network, based on IEC 61850, is shown in Fig. 1. This comprises of station, bay, and process levels. A local area network enables the communication between engineering workstations, station control systems, and communication servers with control centers. However, the focus of this paper is on the bay level where a Local Operating Network (LON) connects IEDs and enables power system automation and protection applications. A key point to be noted is that IEC 61850 traffic on the local operating network is not encrypted. This is to ensure real-time performance of protection equipment. Thus, IEC 61850-based communication is susceptible to cyber attacks [3]. Hence, the cyber attacks in this research target the GOOSE and SV protocol messages that are encapsulated as data link (Ethernet) frames and multicast on the substation LON. In this paper, IEDs refer to protection and control equipment located at the bay level and connected to the process bus. The devices at the process level are Merging Units (MUs). They are typically used for sampling and data conversion operations. The focus of this work is on digital substations that completely use IEC 61850. In this scenario, most analogue hard wiring is replaced by Ethernet or LAN connections. Thus, trip commands are sent digitally through the process bus, using the GOOSE protocol.

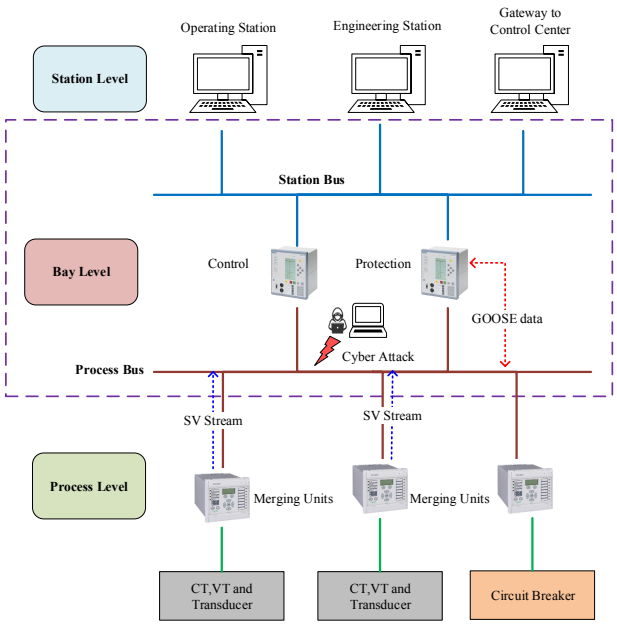


Fig. 1: Layout of digital substation communication network.

III. Cyber Attack Model on Digital Substations

The goal of a cyber attack on a digital substation is to modify, disrupt or disable a service of at least one protection, automation or control device. This raises the question of the possible means or attack vectors. To this end, physical access to the substation communication network is not always necessary [1]. The cyber attacks can be conducted remotely by exploiting backdoors to access the substation LON. This is possible through infected station control systems or engineering workstations used for relay configurations. The cyber attacks in Ukraine in 2015 and 2016 are real-world examples of such attack vectors [5], [23]. In 2016, the attack was executed by manipulating Industrial Control System (ICS) software using Crashoverride/Industroyer malware. The attackers infiltrated into the network of the Ukrainian power system operator using spam phishing techniques and malware. After infiltration, the attackers created a backdoor to maintain access to the power system IT infrastructure. The main targets of the attack were the power system communication protocols, such as IEC 101, IEC 104, IEC 61850, and Object linking and embedding for Process Control Data Access (OPC-DA). By manipulating the protocols, the attackers targeted power system equipment and consequently altered the state of the power system. This eventually led to a power outage [23]. Therefore, in this paper, the cyber attacks target an already compromised substation wherein an attacker has remote/physical access to the substation communication network.

By gaining access to the substation communication network, the attacker can cause significant disruption and abnormal functioning of equipment within the digital substation, i.e., maliciously open circuit breakers, block or disable protection

devices, or collapse the substation communication network itself. This forms the basis of cyber attack threat model on substation protection and automation investigated in this paper. This shows how malicious cyber attacks in digital substations can lead to cascading failures and a a power system blackout. Within IEC 61850, both SV and GOOSE employ a publisher-subscriber mechanism with information being communicated over the substation LON. Since IEC 61850 traffic is not encrypted, attackers may conduct a man-in-the-middle attack, with the aforementioned threat and impact. Such a cyber attack can be modelled in two stages as described below. A pseudo code was developed to conduct the SV and GOOSE man-in-the-middle cyber attacks. This is explained in the following subsections.

Pseudocode 1: Injection of spoofed IEC 61850 traffic

```
Monitor network interface;
Filter packet based on type 0x88b8 (GOOSE);
Filter packet based on type 0x88ba (SV);
Capture filtered packets as p_cap ;
i= 0, n= number of p_cap ;
src = source MAC address;
dst = destination MAC address;
while (i < n) do
    p_spoof = Get and modify payload of p_cap;
    send packet (src, dest, VLAN, p_spoof);
    i++;
end
```

A. Network Reconnaissance

The first stage of the attack model is to monitor the substation communication traffic and identify GOOSE and SV messages. The structures of a typical GOOSE and SV frame are similar as shown in Fig. 2 and 3. The common fields include, the physical link destination and source addresses, i.e., Media Access Control (MAC), tag of the Virtual Local Area Network (VLAN), type header, length of the frame, and data payload. The type headers for GOOSE and SV are distinct. Additionally, the actual data payload is different. For a typical GOOSE frame, under the data payload, the data set contains the various trips commands and breaker statuses. The status and sequence number fields, i.e., StNum and sqNum, are important from an operational perspective. In the processing algorithm of GOOSE messages, the sequence number is incremented continuously with every GOOSE message sent while the status number is fixed. Status number is changed by one in the case of an event in the relay, e.g., a relay trip, and the sequence number is reset to zero. Thus, GOOSE messages with a lower status number are discarded. Similarly, the SV frame contains the smpCnt field, which increments with every frame transmitted. The seqData holds all the instantaneous phase measurements sent to the protective relays. Due to the lack of cyber security implementations, both of these protocols are susceptible to man-in-the-middle cyber attacks. Spoofed information can be supplied to the protection IEDs to trigger or inhibit protection functions. Keeping this in mind, this paper seeks to formulate a generic model of a man-in-the-middle cyber attack, with a twofold objective. The first is to inject false SV data streams into the substation network. Secondly, the attack supplies spoofed GOOSE information to protective relays, causing them to trip. The first stage of the attack is completed by monitoring the network for the Ethernet source, destination, VLAN, and data payload of GOOSE and SV. Most importantly, the status number and sequence number field within the GOOSE data payload are noted. This information is used to develop an appropriate attack vector to execute the man-in-the-middle cyber attack.

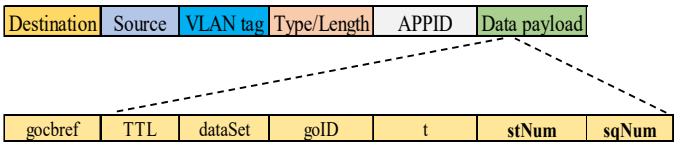


Fig. 2: Structure of GOOSE data frame.

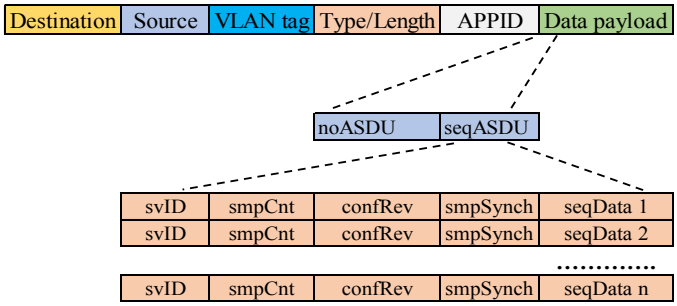


Fig. 3: Structure of SV data frame.

B. Cyber Attack Execution on Sampled Values (SV)

As discussed in Section 2.1, distance protection relies on both voltage and current measurements. There are mechanisms in IEDs to detect voltage transformer failures. It is common for the Miniature Circuit Breaker (MCB) of a voltage transformer to trip. In that case, the measured voltage is zero and IED blocks all distance protection functions. Therefore, for a cyber attack that manipulates sampled values, changing the voltage to zero might not be sufficient to make distance protection trip. However, it might be sufficient to block the protection functions of the IED such that it fails to operate during an actual fault. The cyber attack on the SV protocol in this paper focuses on inhibiting the protection functionality of the targeted relay. The network traffic is captured and filtered with key type of SV, i.e., 0x88ba. The rate of typical SV traffic is 80 samples/cycle. In the attack conducted in this paper, for each captured frame, the value of measurements sent to the IED is specifically modified, which is part of Application Specific Data Unit (ASDU). The attack is carried out by spoofing the identity of the legitimate SV data stream provider (RTDS in this case), using the information collected

from stage one. Next, we replay the spoofed frames that are completely identical to the actual SV stream, except the modified ASDU part. This modified ASDU contains spoofed data, e.g., constant data stream of zero volts, or previously observed SV data stream. This essentially creates two data streams of measurements for the IED, one with actual values from the merging unit and the other with spoofed frames. These two sets of values are unexpected for the IED. Hence, it gets blocked from further operations. The time required for the entire process from capture, modification, and spoofed data transmission is sufficient to conduct the cyber attack, as it is carried out over two stages. Traffic is captured and analysed in stage one. Stage two only focuses on the transmission of spoofed frames to the IED.

Now, when a short-circuit occurs, the IED fails to act, as it is blocked. This causes a delay in fault clearance and may set off a chain of cascading events. With the protection device being blocked, it causes other relays in the system to trip and leads to power swing situations. Consequently, out of step conditions may result, causing generators to trip. The final result of such an attack is a blackout. This type of attack can be considered as a 'sleeper cell' in the substation that will present itself at a critical moment when protection needs to operate. It is interesting to note that, manipulation of the voltage/current SV measurements can create over-voltage/over-current conditions that can result in malicious tripping of the subscribing IED. However, for such an advanced SV attack, the SV traffic should come only from the attacker and the legitimate SV traffic to the IED must somehow be rerouted. Else, the IED might get blocked from further operations due to multiple concurrent input SV streams.

C. Cyber Attack Execution on GOOSE

The cyber attack on the GOOSE protocol injects spoofed GOOSE frames by using information collected from the first stage. The spoofed frames contain modified data payloads, i.e., goosepdu, that issue trip signals. These spoofed data frames also contain modified status and sequence number fields. By injecting the spoofed data into the process bus at a high rate, the tripping of protective relays is mimicked. This causes the circuit breakers to open, thereby disconnecting transmission lines. The sudden opening of the lines causes fluctuations in voltages and frequency. Thus, by injecting spoofed GOOSE frames, bus voltages and frequencies are severely affected. This may lead to triggering of UVLS or UFLS schemes in order to preserve the system stability and therefore a loss of load.

IV. Experimental Framework and Results

A. Hardware-in-the-Loop (HIL) Setup

The hardware-in-the-loop setup used to carry out the cyber attack investigations is shown in Fig. 4. IED 1 is fully IEC 61850 compliant, meaning, the relay has the capability for GOOSE messaging and uses SV for measurements. On the basis of the received SV input, it calculates fault condition and trip status, which is then communicated through GOOSE. IEDs 2 and 3 are partially IEC 61850 compliant. They are hardwired and receive analogue signals from RTDS through power amplifiers. The remaining relays are modelled and simulated on the RTDS. It is to be noted, all the physical IEDs used in this paper use GOOSE messaging for critical substation communication, i.e., trip and block commands through switched Ethernet. This is keeping in line with the concept of a digital substation that employs IEC 61850. As shown in Fig. 4, the relay data links are connected to a network switch which also has a connection to RTDS GTNET 2x card. The card is interfaced to the RTDS through an internal optic fibre connection. The card publishes sampled values to IED 1 and acts as a subscriber to the GOOSE messages from IEDs 1, 2 and 3.

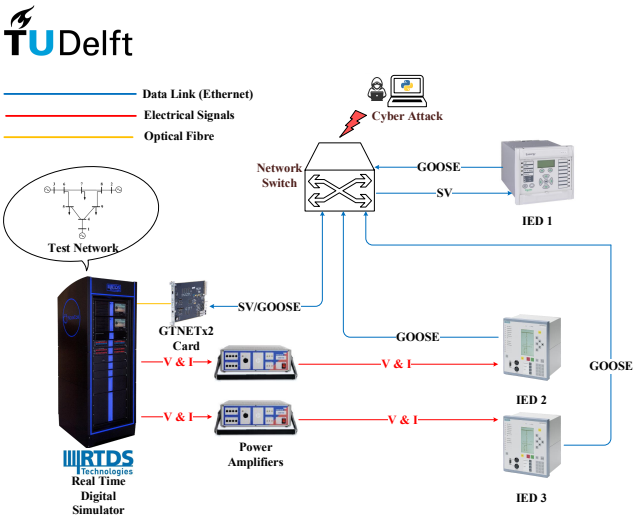


Fig. 4: HIL cyber-physical experimental framework to analyse impact of cyber attack on the power grid.

The power system model simulated on RTDS is the IEEE 9-bus system, shown in Fig. 5. As previously mentioned, IEC 61850 employs a publisher-subscriber mechanism. Under this mechanism, GOOSE and SV messages are multicast using Ethernet over the process bus. This means, one IED publishes GOOSE messages to the process bus. Other IEDs only receive messages belonging to the destination address group they are configured to subscribe to, rather than all messages. Similarly, an IED is configured to subscribe to SV measurements only from a certain merging unit publishing to the process bus. In this research, the substation process bus is represented by the network switch shown in Fig. 4. Thus, all GOOSE and SV messages are published and subscribed through the switch. To enable flexibility of connected devices, the switch is set to broadcast to all available ports, i.e., it sends packets to all connected nodes in a single broadcast domain. This is because it is not configured in secure mode. To enable this mode, flow control rules and restrictions need to be configured, which affect the flexibility and scalability of the network. Therefore, a potential cyber attacker can monitor critical substation communication traffic by gaining access to

the switch and conduct packet sniffing. Moreover, the attacker can then inject spoofed packets into the network, through the switch. This forms the basis for the cyber attacks in this paper.

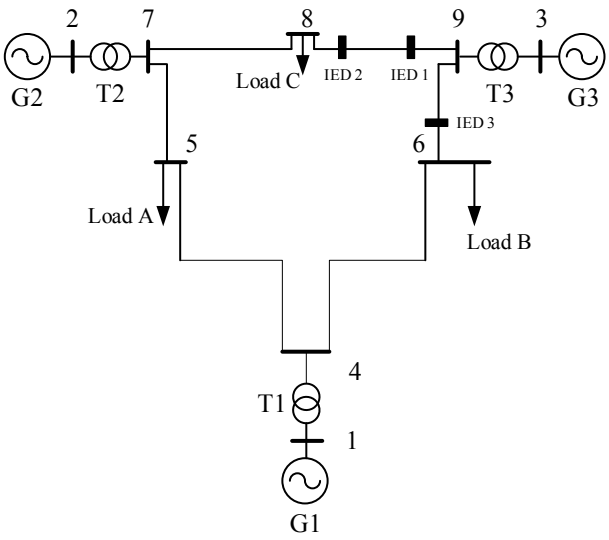


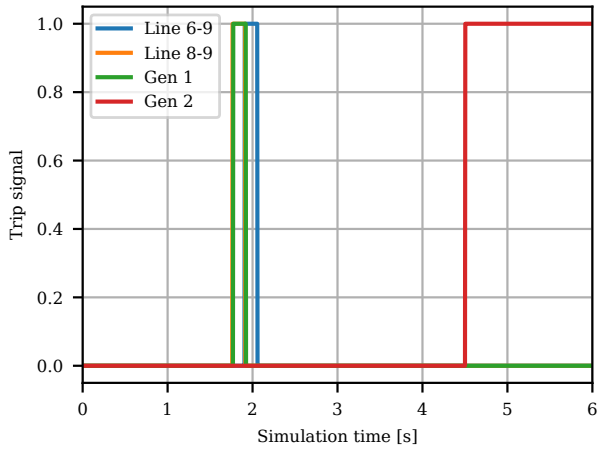
Fig. 5: IEEE 9-bus test system.

The proposed cyber attack model in this paper is generic and can be carried out in two stages using a wide range of tools. We use a well-known communication network tool, i.e., Wireshark, to carry out stage one, i.e., network reconnaissance. Wireshark is run on a separate host machine, which is connected to the network switch. The network interface of this host machine is set to 'promiscuous' mode in Wireshark. This enables all the network traffic through the switch to be monitored and inspected on the host machine. The data collected from this stage is used in a python script, based on the Scapy networking library. Scapy is a packet manipulation tool for computer networks that enables the crafting of spoofed data packets/frames. With access to the network switch, the script executes the man-in-the-middle cyber attack by injecting spoofed SV and GOOSE data streams directly into the substation communication network. The spoofed SV data streams cause the blocking of protection equipment. This prevents its normal operation during faults. On the other hand, the spoofed GOOSE frames compromise multiple IEDs, causing them to trip and open circuit breakers.

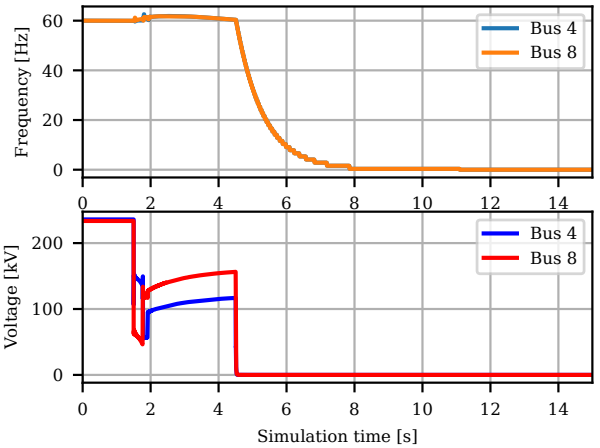
It is interesting to point out, the cyber-physical experimental framework can also be used to carry out cyber security investigations. It can be integrated with cyber security defence and mitigation techniques by implementing Intrusion Detection and Prevention Systems (IDPS) for application in digital substations. Furthermore, the use of commercial protection devices enables evaluation of the cyber security standards applicable to IEC 61850, such as IEC 62351-6. For example, testing of Hash-based Message Authentication Codes (HMAC) to be used by IEDs within the substation to guarantee message authenticity and integrity, which is mandated by the latest edition of the IEC 61850 standard. Hence, this opens up many possible avenues for future research into cyber security of digital substations.

B. Impact of SV cyber attack on IEEE 9-bus system

The cyber attack on IED 1 forces the device to block its protection functions. During normal operation, in the case of a fault on the transmission line 8-9, at bus 9, the fault is cleared in ca. 80 ms. However, with IED 1 being blocked, the fault is not cleared on time. As a result, IED 2 trips line 8-9 first, followed by an out of step protection trip on G1, switching the generator off from the network, as seen in Fig. 6a. The fault is then cleared by the second zone of distance protection of IED 3 located on line 6-9, which acts as a backup for blocked IED 2. Now, the system is extremely unstable and the only remaining generator, i.e., G2, cannot supply all loads. Finally, G2 is also disconnected due to an under-voltage state. Therefore, the cyber attack induces cascading failures, which lead to a blackout. Fig. 6b shows the voltage and frequency dropping to zero. Therefore, by compromising only one IED, the cyber attack leads to a blackout.



(a) Trip signals due to cyber attack.



(b) Frequency and voltage after cyber attack.

Fig. 6: Impact of SV cyber attack on system parameters.

C. Impact of GOOSE attack on IEEE 9-bus system

The second cyber attack involves the malicious opening of circuit breakers in the substation at bus 7. This attack sends spoofed GOOSE data streams to three compromised IEDs in the substation. As a result of the attack, G2 and lines 7-5 and 7-8 are disconnected. The frequency drops below admissible limits as shown in Fig. 7. This causes under frequency load shedding to take place around 5s simulation time. After three steps of load shedding, at approximately 7.5s, the system frequency starts to recover. It eventually settles to a value lesser than the nominal frequency of 60 Hz. Thus, the cyber attack results in a load shed of 90 MW, which is equivalent to a partial blackout.

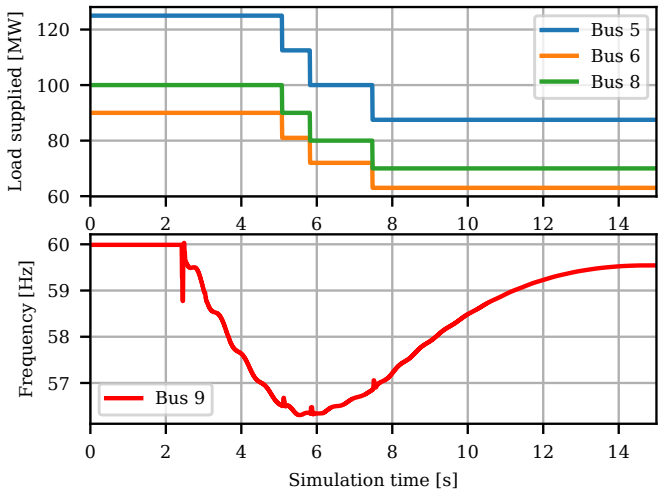


Fig. 7: Impact of GOOSE cyber attack on system parameters.

V. Conclusions and Recommendations

This paper presents the dangerous implications of not securing IEC 61850 standard used for power substation automation and protection. Man-in-the-middle cyber attacks are demonstrated to achieve protective relay blocking and malicious opening of circuit breakers in the power system. The attacks cause cascading failures, leading to a partial or complete blackout. This is validated using the proposed HIL experimental framework consisting of commercial relays and RTDS.

The IEC 62351-6 standard addresses security for protocols described within IEC 61850. It proposes an additional field to the GOOSE and SV data payloads for security-relevant information. This field contains an RSA (Rivest-Shamir-Adleman) based digital signature to ensure the integrity of the Protocol Data Unit (PDU). With this measure, the sending IED is clearly identified and it becomes impossible to manipulate the message contents. Similarly, the standard also recommends using a Message Authentication Code (MAC) to generate a hash code using a Secure Hash Algorithm-256 bit (SHA-256) for the GOOSE and SV messages to check the integrity of the packets. The GOOSE/SV publisher calculates a HMAC value and appends it to the message that is then sent to the subscriber. The subscriber re-calculates a new value of the HMAC code based on the received message and a secret key. This second value is then compared to the one appended in the received GOOSE message. Thus, the authenticity of the sent messages and identity of the associated publisher is clearly verified. However, the suggested use of the digital signatures based on RSA and HMAC algorithms for providing authenticity and integrity of messages make them unsuitable for applications where a 4 ms or lower response time is strictly required. This is because RSA and SHA based encryption and decryption are computationally demanding. Furthermore, the standard does not provide any information about the certificates related to the RSA keys used for signing extended PDUs. Also, the use of RSA and HMAC based authentication keys for IEDs requires a key management infrastructure within the digital substation. Consequently, these security mechanisms have not yet gained widespread use.

The cyber attack model in this paper targets the IEC 61850 GOOSE and SV protocols. The design of intrusion detection and prevention systems for such cyber attacks on digital substations is reported in [24], [25]. Both the works discuss methods to block protection equipment in the scenario of a cyber intrusion, to negate the effects of the cyber attack. Thus, by applying such measures, similar attacks as discussed in this paper may be detected and their damage minimised. However, these detectors or tools are not commercially available alongside protection devices, nor have they been implemented in the field. An increase in power grid digitalization and adoption of the IEC 61850 standard requires more attention on cyber security in order to ensure the resilience of future cyber-physical energy systems.

Acknowledgment

This work is part of the Designing Systems for Informed Resilience Engineering (DeSIRE) program of the 4TU Centre for Resilience Engineering (4TU.RE). DeSIRE is funded by the 4TU-program High Tech for a Sustainable Future (HTSF). 4TU is the federation of the four technical universities in The Netherlands, i.e., Delft University of Technology, Eindhoven University of Technology, University of Twente, and Wageningen University and Research. This work has also been supported by SA Archimedes Foundation Kristjan Jaak scholarship for study periods abroad, grant no. 16-3.5/1470.

References

[1] C. C. Liu, A. Stefanov, J. Hong, and P. Panciatici, "Intruders in the grid," *IEEE Power and Energy Magazine*, vol. 10, no. 1, pp. 58–66, Jan–Feb 2012.

[2] G. Ericsson, "Cyber Security and Power System Communication," *IEEE Trans Power Delivery*, vol. 25, no. 3, pp. 1501–1507, Jul 2010.

[3] J. Hoyos, M. Dehus, and T. X. Brown, "Exploiting the GOOSE protocol: A practical attack on cyber-infrastructure," in *in Proc 2012 IEEE Globecom Workshops*, Anaheim, CA, Dec 2012, pp. 1508–1513.

[4] T. A. Youssef, M. E. Hariri, N. Bugay, and O. A. Mohammed, "IEC 61850: Technology standards and cyber-threats," in *Proc IEEE Int Conf on Environment and Electrical Engineering (EEEIC)*, Florence, Jun 2016, pp. 1–6.

[5] D. E. Whitehead, K. Owens, D. Gammel, and J. Smith, "Ukraine cyber-induced power outage: Analysis and practical mitigation strategies," in *Proc Annual Conf for Protective Relay Engineers (CPRE)*, College Station, TX, Apr 2017, pp. 1–8.

[6] R. Liu, C. Vellaithurai, S. S. Biswas, T. T. Gamage, and A. K. Srivastava, "Analyzing the cyber-physical impact of cyber events on the power grid," *IEEE Trans Smart Grid*, vol. 6, no. 5, pp. 2444–2453, Sep 2015.

[7] K. Pan, P. Palensky, and P. M. Esfahani, "From static to dynamic anomaly detection with application to power system cyber security," *IEEE Trans Power Systems*, vol. 35, no. 2, pp. 1584–1596, Mar 2020.

[8] A. A. Jahromi, A. Kemmeugne, D. Kundur, and A. Haddadi, "Cyber-physical attacks targeting communication-assisted protection schemes," *IEEE Trans Power Systems*, vol. 35, no. 1, pp. 440–450, Jan 2020.

[9] A. Ameli, A. Hooshyar, and E. F. El-Saadany, "Development of a cyber-resilient line current differential relay," *IEEE Trans Industrial Informatics*, vol. 15, no. 1, pp. 305–318, Jan 2019.

[10] X. Liu, M. Shahidehpour, Z. Li, X. Liu, Y. Cao, and Z. Li, "Power system risk assessment in cyber attacks considering the role of protection systems," *IEEE Trans Smart Grid*, vol. 8, no. 2, pp. 572–580, Mar 2017.

[11] Y. M. Khaw, A. A. Jahromi, A. Mohammadreza F. M., D. Kundur, S. Sanner, and M. Kassouf, "Preventing false tripping cyberattacks against distance relays: A deep learning approach," in *Proc IEEE Int Conf on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, Beijing, Oct 2019, pp. 1–6.

[12] Y. Yang, H. T. Jiang, K. McLaughlin, L. Gao, Y. B. Yuan, W. Huang, and S. Sezer, "Cybersecurity test-bed for IEC 61850 based smart substations," in *Proc IEEE Power Energy Society General Meeting*, Denver, CO, Jul 2015, pp. 1–5.

[13] M. Kabir-Querrec, S. Mocanu, J. Thiriet, and E. Savary, "A Test bed dedicated to the Study of Vulnerabilities in IEC 61850 Power Utility Automation Networks," in *Proc IEEE Int Conf on Emerging Technologies and Factory Automation (ETFA)*, Berlin, Sep 2016, pp. 1–4.

[14] O. Khaled, A. Marín, F. Almenares, P. Arias, and D. Díaz, "Analysis of Secure TCP/IP Profile in 61850 Based Substation Automation System for Smart Grids," *Int Journal of Distributed Sensor Networks*, vol. 12, no. 4, pp. 1–11, Apr 2016.

[15] M. E. Hariri, T. Youssef, and O. Mohammed, "On the Implementation of the IEC 61850 Standard: Will Different Manufacturer Devices Behave Similarly under Identical Conditions?" *Electronics*, vol. 5, no. 4, pp. 1–13, May 2016.

[16] N. Kush, E. Ahmed, M. Branagan, and E. Foo, "Poisoned GOOSE: Exploiting the GOOSE Protocol," in *Proc Australasian Information Security Conf*, Auckland, Jan 2014, pp. 17–22.

[17] P. M. Anderson, *Power System Protection*. New York: McGraw-Hill, IEEE Press, 1999.

[18] A. Apostolov, "Modeling of multifunctional distance protection IEDs," in *Proc Int Conf on Developments in Power System Protection (DPSP 2010)*, Manchester, Apr 2010, pp. 1–5.

[19] D. A. Tziouvaras and Daqing Hou, "Out-of-step protection fundamentals and advancements," in *Proc Annual Conf for Protective Relay Engineers, 2004*, College Station, TX, Apr 2004, pp. 282–307.

[20] C. Mozina, "Undervoltage load shedding," in *Proc Power Systems Conf: Advanced Metering, Protection, Control, Communication, and Distributed Resources*, Clemson, SC, Mar 2007, pp. 39–54.

[21] V. Chuvychin, A. Sauhats, V. Strelkovs, and E. Antonovs, *Under-Frequency Load Shedding System*. Berlin, Heidelberg: Springer, 2014, pp. 349–367. [Online]. Available: https://doi.org/10.1007/978-3-642-53848-3_18

[22] "IEEE Guide for Abnormal Frequency Protection for Power Generating Plants," *IEEE Std C37.106-2003*, pp. 1–40, Feb 2004.

[23] R. Lee, M. Assante, and T. Conway, "Analysis of the Cyber Attack on the Ukrainian power grid," *Electricity Information Sharing and Analysis Center (E-ISAC) Tech Report*, pp. 1–26, Mar 2016. [Online]. Available: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

[24] J. Hong and C. Liu, "Intelligent Electronic Devices With Collaborative Intrusion Detection Systems," *IEEE Trans Smart Grid*, vol. 10, no. 1, pp. 271–281, Jan 2019.

[25] D. Ishchenko and R. Nuqui, "Secure Communication of Intelligent Electronic Devices in Digital Substations," in *Proc IEEE Transmission and Distribution Conf and Exposition (T&D)*, Denver, CO, Apr 2018, pp. 1–5.