

# Protection and Communication Model of Intelligent Electronic Devices to Investigate Security Threats

Mohamed Faisal Elrawy<sup>1,2</sup>, Eleni Tekki<sup>1</sup>, Lenos Hadjidemetriou<sup>1</sup>, Christos Laoudias<sup>1</sup> and Maria K. Michael<sup>1,2</sup>

<sup>1</sup>KIOS Research and Innovation Center of Excellence and <sup>2</sup>Department of Electrical and Computer Engineering

University of Cyprus, 1678 Nicosia, Cyprus

Email:{*elrawy.mohamed, tekki.eleni, hadjidemetriou.lenos, laoudias.christos, mmichael*}@ucy.ac.cy

**Abstract**—Intelligent Electronic Devices (IEDs), e.g., protective relays, have a vital role for protecting power systems and substations. In modern power systems, the performance of protection schemes by IEDs can be affected by cyber-physical, communication and cybersecurity operations and thus, a holistic modeling approach is required where all the domains are properly considered. However, commercial protective relays used in the field are mainly modeled using closed-source software. Therefore, this work proposes an integrated, realistic, and flexible model of an overcurrent protective relay compatible with IEC 61850 communication standard. This open-source model integrates the behavioural interactions between the protective relays and their physical, communication and cybersecurity operations in a digital substation. A model of transmission substation is developed in MATLAB/Simulink® for validation purposes and the effect of communication operations and cybersecurity threats on the relay's physical operations is investigated according to different case studies and attack scenarios.

**Index Terms**—cybersecurity, digital substation, GOOSE protocol, IEC 61850, protective relays

## I. INTRODUCTION

THE automation of smart grid services empowers the reliability, stability, and efficiency of the electrical grid. Substation automation is one of the key services of smart grids that provides a fast response to disturbances, events and electrical faults to enhance the performance of electrical protection systems. Consequently, digital substations have been upgraded with advanced technologies, such as Intelligent Electronic Devices (IEDs), ethernet-based communications, and standardized protocols [1], [2]. In digital substations, the protective relays are implemented as IEDs compatible with the International Electrotechnical Commission (IEC) 61850 standard, which uses the Generic Object Oriented Substation Events (GOOSE) protocol as a standard communication protocol, for timely and accurate detection and isolation of electrical faults. However, the cybersecurity of these IED relays has emerged as a serious challenge due to the effects of cyber-attacks, which target these relays, that can cause infrastructure damages, cascading outages and lead to blackouts [3].

Due to the complex nature of an IED relay, the development of effective cybersecurity methods requires the knowledge of the physical, communication and cybersecurity aspects of protective relays. Therefore, an integrated model that can represent the interactions between these domains (i.e., behavioural interactions) is required to holistically describe the conditions behind the behavior of an IED relay. This way,

this behavior can be accurately modeled and the development of flexible protection schemes and effective cybersecurity methods is facilitated. Such a model can help researchers and engineers to ensure the reliability, stability, and security of digital substations. In this context, Almas et al [4]. proposed a model for Over-Current (OC) relay in SimPowerSystems (MATLAB/Simulink®), where the design is focused on the physical operation of the OC protection scheme (i.e., current measurements, trip signal, and opening time) in Hardware In the Loop (HIL) configuration without considering the communication aspects of the relay. In [5]–[7], the authors present the modeling of the communication operations of protective relays using GOOSE protocol. However, these works do not consider the effect of cybersecurity operations on the physical and communication operations of the protective relay. On the other hand, the works in [8], [9] focus on studying the cybersecurity operations of protective relay by testing different types of attacks, but without showing the behavioral interactions of relay operations on the power infrastructure.

For addressing the limitations of existing solutions, this work proposes an open-source, integrated and realistic model of OC protective relay using MATLAB/Simulink®. In this model, the behavioural operations of the IED relay are integrated with the communication operations based on the GOOSE protocol. This in turn, allows for accurate and realistic investigation of cybersecurity threats emerging from the communication domain and affecting the IED protective behavior. The contributions of this work are summarized as follows:

- A model is proposed for the IED relay protection scheme behavior within the context of the communication domain based on the GOOSE protocol, including a new integrated state diagram to describe the overall operations.
- An open-source simulator based on the proposed model has been developed, to enable the investigation of power, communication and cybersecurity operations and challenges of OC relays in digital substations. The simulator is flexible and can run as a standalone software without requiring expensive field or HIL equipment, offering a cost-effective framework for researcher/engineer to validate new technologies for protective relays in substations.
- The security vulnerabilities of the OC relay model are inspected by four types of attacks targeting the Confidentiality, Integrity and Availability (CIA) of GOOSE data.

The remainder of this paper is organized as follows. Section II overviews the protective relay operations, GOOSE protocol and security vulnerabilities. The proposed model and its units are described in Section III. Section IV discusses the simulation results. Finally, conclusions are given in Section V.

## II. BACKGROUND

### A. IED for Protecting Physical Operation in Power Systems

The IEC 61850 standard was proposed for digital substations to solve interoperability and vendor-independence issues. By using this standard, all digital devices in substation are implemented as IEDs. Each IED consists of physical device, logical devices, and logical nodes. The physical device contains logical devices that aim to perform a certain high-level function (e.g., line protection) by using logical nodes, which are designed to achieve the desired protection scheme [10]. The main function of an IED that represents a protective OC relay is to protect substations from high current faults, such as Short Circuit (SC) faults. Once this IED detects a high current (current measurement exiting a certain pick-up threshold), it waits for a certain time based on the Definite Time (DT) or inverse time mechanisms and then it sends a trip command to the Circuit Breaker (CB) to open [11]. In case of CB failure, the IED sends an inter-trip command, i.e., a command sent to the backup IED to trip its CB, using GOOSE protocol which provides faster response of the backup protection.

### B. GOOSE Communication Protocol

The communication operations of the IEDs in substations are based on the GOOSE protocol to provide high-speed communication for exchanging critical information. For example, the essential events of power system protection applications, i.e., inter-trip and blocking, require strict time delivery of maximum 3 ms [12]. Therefore, the structure of the GOOSE message is designed to be directly connected with the data link layer using the CSMA/CD (Carrier Sense Multiple Access with Collision Detection) protocol. Moreover, by using the ethernet switch technology, the GOOSE protocol can implement the CSMA/CD in multicast and full duplex modes for transmitting and receiving messages to be suitable for real-time and mission-critical tasks, i.e., protection applications. Once the transmitter IED detects a new event, it can send the GOOSE message to multiple receivers at the same time [12], [13].

The GOOSE protocol is designed to retransmit the GOOSE message using two different retransmission mechanisms (i.e., steady-state retransmission and fast-retransmission mechanisms) to guarantee message reliability. The retransmission mechanisms of GOOSE protocol are based on Status number (ST) and Sequence number (SQ), where an increment of ST represents a new event and an increment of SQ represents a repetition of the same GOOSE message. For more details on these retransmission mechanisms, readers may refer to [12].

### C. Security Vulnerabilities and Threat Model

Although the GOOSE protocol is designed to provide a fast and reliable communication channel for the IEDs, exploiting

the security vulnerabilities of this protocol can threaten the physical operations of these IEDs and of the power system. Moreover, applying cybersecurity measures for securing the GOOSE protocol faces several challenges [12]. For instance, applying any encryption mechanism to this protocol is challenging due to the required strict time of 3 ms for GOOSE message delivery. Therefore, the messages are sent in plaintext format to multiple receivers at the same time. Consequently, potential attackers with access to the substation network can capture these messages and violate the CIA of GOOSE data, which threatens the protection and automation functionalities of the protective relays in the substation. In this context, a baseline cybersecurity algorithm is proposed in the IEC 62351-6 standard to protect the IEDs from cyber-attacks, such as replay and man-in-the-middle, that target GOOSE messages in substations. This cybersecurity algorithm validates the incoming GOOSE message using its ST, SQ, and the timestamp, as will be discussed in the next section. However, not all commercial protective relays have this algorithm [14].

Four types of cyber-attacks are used in the threat model in this paper, as follows. In the False Data Injection (FDI) attack, the attacker injects false information into an original message and then resends it through the Local Area Network (LAN) of the substation for affecting IEDs. In the Message Suppression (MS) attack, the attacker prevents legitimate IEDs from receiving original messages by injecting a fake message, which has a high ST value, through the LAN. In the Denial of Service (DoS) attack, the attacker injects several fake messages through the LAN to flood the traffic flow. Finally, in the replay attack, the attacker replays an original message through the LAN to deceive the IEDs.

## III. SYSTEM MODEL

### A. Overview

A transmission substation with three IEDs (i.e., definite-time OC Relays) was created in MATLAB/Simulink®, using the SimPowerSystems library components, to simulate the power system operation and to protect the system in case of SC faults on a Transmission Line (TL) or at the busbar, as shown in Fig. 1. IED1 provides primary protection for busbar faults, and backup protection for other downstream faults. IED2 and IED3 are responsible for their TL protection. Each IED decides the trip command signal ( $T_{CB}$ ) to trip its own CB and transmits four binary parameters to the other IEDs. These are Inter-trip ( $T$ ), Block ( $B$ ), Fault ( $F$ ), CB internal failure ( $CBF$ ). For Transmitting and Receiving, these parameters are subscripted with  $T$  and  $R$ , respectively. The protection scheme that is used, implies that in case of a SC fault on TL2, the IED2 should trip CB2, as it has the lowest DT setting, and block the IED1. This blocking enables discrimination for the protection approach, allowing IED2 (which is closer to the fault) to trip first without permitting the tripping of IED1 that will cause unnecessary outage to the entire substation. In the case of a busbar fault, IED1 will trip CB1 after its DT. By using small DTs for all IEDs and communication by GOOSE, the protection scheme achieves discrimination and very fast protection for both TL

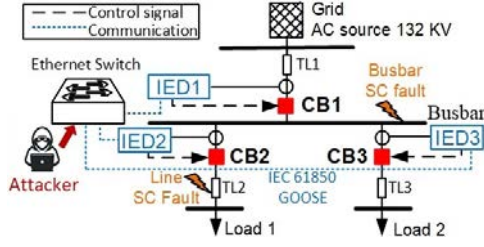


Fig. 1. Schematic diagram of the substation model.

and busbar faults, without any unnecessary disconnection of healthy parts.

The proposed model of the IED consists of a control and a communication unit, as shown in Fig. 2. The control unit is built with logical circuits that calculate the  $T_{CB}$  and the transmitted data. The communication unit converts these data into a message and vice versa to feed them back to the control unit, as they affect the decision-making of the IED.

### B. Control Unit

The control unit uses the root mean square of the measured current  $i_{rms}$  to compare it with a current pickup threshold ( $Th$ ), through an OC Detection logic circuit (OD), and set the parameter  $F_T$  equal to 1 if it detects OC fault. A parameter “Fault Check” (FC) and a parameter “wait” ( $W$ ) are also set to 1.  $FC$  indicates that the relay should wait, for Fault Checking Time (FCT), to ensure that the fault is not temporary, before sending a block ( $B_T = 1$ ).  $W$  indicates that the relay should further wait for its DT before tripping.

An IED sends a  $T_{CB}=1$  to its CB when its DT is reached, or if it receives an Inter-trip ( $T_R=1$ ).  $CBS$  represents the CB status, which equals 1 for opened CB and 0 for closed CB. A CB needs a mechanical delay (i.e.,  $CB_{delay}$ ) in order to open/close. When an IED trips its CB, it waits for  $CB_{delay}$  and for an extra time  $CB_{margin}$  to make sure, according to the CBS, if the CB has properly operated or if there is a failure (i.e.,  $CBF_T = 1$ ). In case of a failure, the IED stops the Block and sends an Inter-trip instead (i.e.,  $T_T = 1$ ).

Fig. 2 describes the logic of the control unit, which uses the measured parameters (i.e., blue colored) and the received parameters (i.e., green colored), to calculate the transmitted parameters (i.e., red colored) that are combined with other measurement data to form the GOOSE data payload (i.e.,  $P_T$ ). The message coming from the communication unit (i.e.,  $M_R$ ) is processed by a baseline Cyber-security algorithm based on the standard IEC 62351-6, which discards any received message that has the same or lower ST number, or an older timestamp than the previous message. Then, a Selection algorithm is used, whose logic depends on the protection scheme. For example, the “Block” or “Inter-trip” messages coming from the upstream relay (IED1) are ignored by the feeder relays (IED2 and IED3) but not vice versa.

### C. Communication Unit

The communication unit of each IED is modeled using Simulink® messages and SimEvents®. It consists of a GOOSE

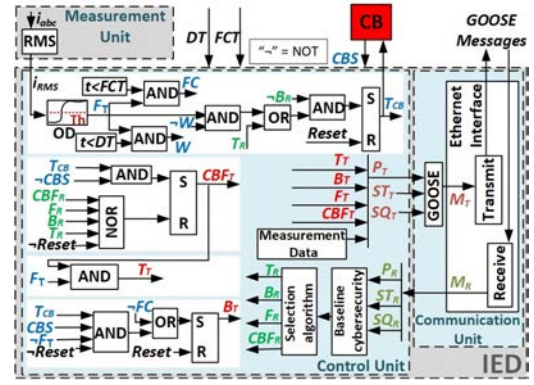


Fig. 2. The proposed model of the OC protective relay in digital substation.

block for messaging and an ethernet interface block, which uses the full duplex multicast CSMA/CD protocol, to control the interaction between the IED and the ethernet communication network. The GOOSE block decides when a GOOSE message will be sent, based on the detection of an event. For this model, six events were developed, which are defined by specific combinations of the  $T_T$ ,  $B_T$ ,  $F_T$  and  $CBF_T$  parameters. The six events are defined as Normal, Fault, Block, Fault Cleared, Inter-trip and CB failure. The GOOSE block receives the payload  $P_T$  from the control unit and when an event is detected, the ( $ST$ ) increases by one, triggering the transmission of the new message. Otherwise, the  $ST$  number remains unchanged while the  $SQ$  number increases by one, triggering the re-transmission of the same message. The transmitted data  $P_T$  along with  $ST_T$  and  $SQ_T$  are converted to a message  $M_T$  to be used by the ethernet interface block.

The ethernet interface block applies the full duplex CSMA/CD protocol by using two discrete-event chart blocks labeled Transmit and Receive, for packet frame transmission and reception, respectively. The transmit block converts the GOOSE message to an ethernet Media Access Control (MAC) frame by attaching ethernet-specific attributes to the message, such as the multicast destination address, which represents the group of the relays that will receive this message according to the protection scheme. The ethernet switch receives the GOOSE message from any IED and then multicasts it (i.e., sends the message to all the other IEDs that share the same multicast destination address). The Receive block takes these received messages  $M_R$  and drive them to the control unit.

### D. Integrated State Diagram Model

The behavior of the IEDs depends on their status, which is a result of the interaction between their physical and communication operations. These behavioural operations have been expressed using a state diagram, as depicted in Fig. 3. The diagram includes five different states (S1-S5) describing the possible conditions of an IED. Each state has an input, which acts like a trigger for the state transition, and an output, which is a GOOSE message of the associated GOOSE event. An input is expressed as a series of binary values consisting of the physical parameters  $T_D$ ,  $CBS$ ,  $F_T$ ,  $W$ ,  $FC$  and the



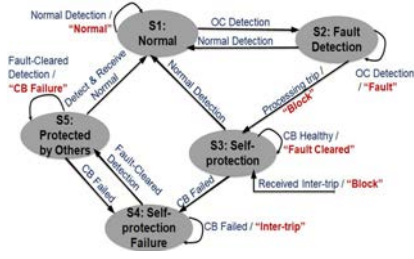


Fig. 3. The state diagram representing the behavior of the IED.

received communication parameters  $T_R$ ,  $B_R$ ,  $F_R$ ,  $CBF_R$ . Based on specific combinations of these binary values, the IEDs change their state, following the arrowed lines.

Table I summarizes the inputs and the outputs of the state diagram, where the symbol “-” indicates that it doesn't matter. Based on the logic of the control unit, there are eight possible inputs for the state diagram. S1 represents the normal condition. S2 is for the OC detection and the waiting of the  $FCT$ . The transition to S3 represents the discrimination by blocking other IEDs. S3 represents the waiting for the DT, the tripping command and the CB failure check. The loop of S3 represents an opened CB and fault isolation. S4 is for a failed CB that needs backup protection. Finally, S5 represents a failed CB after a backup protection has been provided. The Received Inter-trip input is an asynchronous external signal that takes the state of the IED directly to S3.

#### IV. SIMULATION RESULTS AND DISCUSSION

The proposed holistic model for IEDs is developed in MATLAB/Simulink using a discrete-time solver and is able to capture the power, communication and security aspects of a digital substation. For the simulation tests, three different cases are used; Case 1 for a TL2 SC Fault with all the CBs healthy, Case 2 with a failure in CB2 and Case 3 for a busbar SC fault and healthy CBs. The following values are used for all cases:  $DT2 = DT3 = 0.1$  s and  $DT1 = 0.104$  s,  $FCT = 0.05$  s.

##### A. Physical and Communication Operations

The results for Case 1 are depicted in Fig. 4, where the physical and power operation is presented by the parameters  $T_{CB}$ ,  $CBS$  and  $i_{RMS}$ , and the communication operation by the transmitted parameters, for both IED1 and IED2. The timeline boxes explain the behavior of the IEDs at different

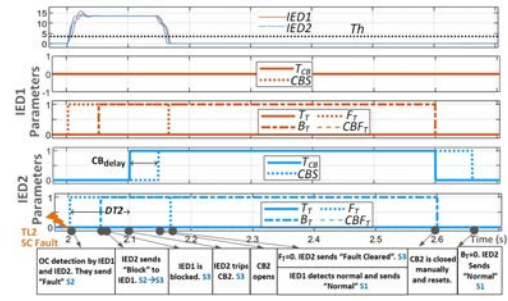


Fig. 4. Simulation results of Case 1 considering IED1 and IED2 operations.

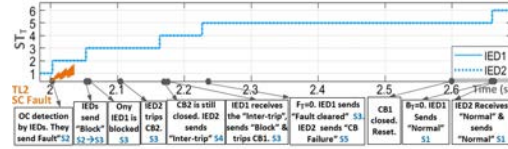


Fig. 5. Simulation results of Case 2, with ST number of IED1 and IED2.

operation times. As expected, the IED2, blocks the IED1 and trips the CB2 after  $DT2$ . The “Block” from IED2 prevents the unnecessary tripping of other CBs (e.g., CB1) and thus, the fault is timely cleared by the closer to the fault IED.

Case 2 is presented in Fig. 5. The graph shows the  $ST$  number of the IED1 and IED2, indicating the times they transmit a new message. Due to the failed  $CB2$ , communication is used to inter-trip the  $CB1$  for fast backup protection. The IED1 trips  $CB1$  before its  $DT1$ , resulting to the clearing of the fault. Similarly, Case 3 is depicted in Fig. 6. The busbar SC fault is detected by IED1 only thus the  $CB1$  is tripped and opens. The use of small  $DTs$  provides fast protection from faults near the source, contrary to conventional protection schemes that gradually increase upstream  $DTs$ .

##### B. Cybersecurity and Network Operations

For studying the cybersecurity operations, four types of cyber-attacks were tested. An attacker is modeled inside the substation, and interferes into the LAN while spoofing the MAC addresses of all the IEDs. The effect of FDI attack is tested on Case 1, where the attacker sends a fake “Inter-trip” message with  $ST_T=4$ . Based on the baseline cybersecurity algorithm, when the IEDs receive the  $ST_R = 4$ , they immediately accept this message and ignore any other with  $ST_R \leq 4$ .

TABLE I  
THE INPUT AND OUTPUT PARAMETERS OF THE STATE DIAGRAM.

Inputs	Input parameters									Outputs	Output parameters			
	$T_{CB}$	$CBS$	$F_T$	$W$	$FC$	$T_R$	$B_R$	$F_R$	$CBF_R$		$T_T$	$B_T$	$F_T$	$CBF_T$
Normal detection	0	0	0	0	0	0	—	—	—	“Normal”	0	0	0	0
Detect & Received Normal	0	0	0	0	0	0	0	0	0	“Normal”	0	0	0	0
OC Detection	0	0	1	1	1	0	—	—	—	“Fault”	0	0	1	0
Processing Trip	0	0	1	1	0	0	—	—	—	“Block”	0	1	1	0
CB Healthy	1	1	0	0	0	—	—	—	—	“Fault Cleared”	0	1	0	0
CB Failed	1	0	1	0	0	—	—	—	—	“Inter-trip”	1	0	1	1
Fault-Cleared Detection	1	0	0	0	0	—	—	—	—	“CB Failure”	0	0	0	1
Received Inter-trip	—	—	1	—	—	1	0	0	0	“Block”	0	1	1	0

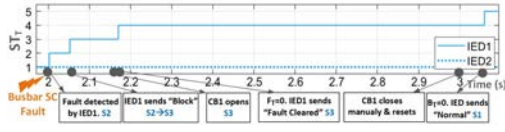


Fig. 6. Simulation results of Case 3, with ST number of IED1 and IED2.

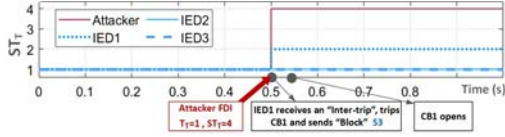


Fig. 7. Simulation results of Case 1 during an FDI attack.

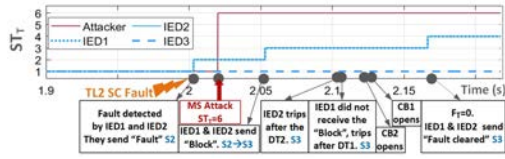


Fig. 8. Simulation results of Case 1 during an MS attack.

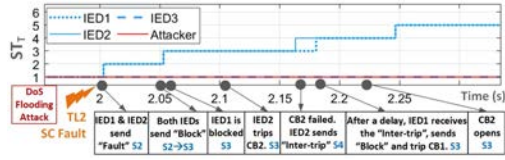


Fig. 9. Simulation results of Case 2 during a DoS Flooding attack.

The results are shown in Fig. 7, where the IED1 trips CB1 without detecting OC nor receiving legitimate "Inter-trip".

The effect of MS attack is tested on Case 1, where the attacker injects a message with  $ST_T=6$ . As shown in Fig. 8, the IED1 rejects the "Block" messages with  $ST_R=3$ , as it has already received the fake  $ST_R=6$ . Therefore, the CB1 trips as well, without considering the block command from downstream relay causing an undesired outage of the entire substation. The effect of the DoS flooding attack was tested on Case 2, as illustrated in Fig. 9. The massive transmission to the switch causes a delay in communication of some messages. Thus, IED1 does not receive the "Inter-trip" on time and remains blocked for longer than normal, causing a delay for the remaining operation, e.g., fault clearing. Finally, the replay attack does not affect the operation of the IEDs, due to the baseline cybersecurity algorithm in the control unit. However, this algorithm is not effective for the other attack types.

To study the effect of the network on the communication operations, network delays and network packet errors were applied on Case 1 and Case 2. A constant 3 ms network delay and a variable network delay (i.e, 0-3 ms), were tested separately. Additionally, network packet errors of 1%, 5% and 10% for each IED were applied, The results showed a delay in communication, compared to normal operation; however, all the important messages are delivered because of the retransmission mechanisms used by GOOSE protocol.

## V. CONCLUSIONS

The proposed model successfully presents the physical, communication and cybersecurity operations of an IED relay, whose behavior is following the proposed state diagram. The small definite times and the communication through GOOSE protocol provide fast and effective fault protection. The cybersecurity investigation of the relay shows that the normal operation of the relay is affected by different cyber-attacks. Therefore, as a future work, this model can be used to study the behavior of the relay under different conditions and be integrated with cybersecurity mitigation approaches and technologies. The proposed model will be uploaded to an open repository, upon the final acceptance of the paper.

## ACKNOWLEDGMENT

This work was partially supported by the European Union's Horizon 2020 research and innovation programme under grant agreement No 101016912 (ELECTRON), and by the European Union's Horizon 2020 research and innovation programme under grant agreement No 739551 (KIOS CoE -TEAMING) and from the Republic of Cyprus through the Deputy Ministry of Research, Innovation and Digital Policy.

## REFERENCES

- [1] S. Kumar, A. Abu-Siada, N. Das, and S. Islam, "Toward a substation automation system based on IEC 61850," *Electronics*, vol. 10, no. 3, pp. 1–16, 2021.
- [2] J. Hong, R. F. Nuqui, A. Kondabathini, D. Ishchenko, and A. Martin, "Cyber attack resilient distance protection and circuit breaker control for digital substations," *IEEE Trans. on Industrial Informatics*, vol. 15, no. 7, pp. 4332–4341, 2019.
- [3] A. Ameli, K. A. Saleh, A. Kirakosyan, E. F. El-Saadany, and M. M. A. Salama, "An intrusion detection method for line current differential relays in medium-voltage dc microgrids," *IEEE Trans. on Information Forensics and Security*, vol. 15, pp. 3580–3594, 2020.
- [4] M. S. Almas, R. Leelarui, and L. Vanfretti, "Over-current relay model implementation for real time simulation & hardware-in-the-loop (HIL) validation," in *Proc. IECON*, 2012, pp. 4789–4796.
- [5] H. León, C. Montez, M. Stemmer, and F. Vasques, "Simulation models for IEC 61850 communication in electrical substations using GOOSE and SMV time-critical messages," in *Proc. IEEE WFCS*, 2016, pp. 1–8.
- [6] D. A. Postoiu, C. Bulac, I. Trîștiu, B. Camachi, and N. Anton, "Modelling and implementation of single line diagram data in IEC 61850 environment," in *Proc. IEEE SAMI*, 2021, pp. 71–76.
- [7] A. A. Memon and K. Kauhaniemi, "Real-time hardware-in-the-loop testing of IEC 61850 GOOSE-based logically selective adaptive protection of AC microgrid," *IEEE Access*, vol. 9, pp. 154 612–154 639, 2021.
- [8] E. Tebekaemi and D. Wijesekera, "Designing an IEC 61850 based power distribution substation simulation/emulation testbed for cyber-physical security studies," in *Proc. CYBER*, 2016, pp. 41–49.
- [9] P. P. Biswas, H. C. Tan, Q. Zhu, Y. Li, D. Mashima, and B. Chen, "A synthesized dataset for cybersecurity study of IEC 61850 based substation," in *Proc. IEEE SmartGridComm*, 2019, pp. 1–7.
- [10] M. A. Aftab, S. S. Hussain, I. Ali, and T. S. Ustun, "IEC 61850 based substation automation system: A survey," *International Journal of Electrical Power & Energy Systems*, vol. 120, pp. 1–16, 2020.
- [11] M. I. Awaad and Z. E. Afifi, "Over-current protection in transmission systems using analog and digital relays - case study and comparison," in *Proc. IEEE MEPCON*, 2021, pp. 156–163.
- [12] M. F. Elrawy, L. Hadjidemetriou, C. Laoudias, and M. K. Michael, "Light-weight and robust network intrusion detection for cyber-attacks in digital substations," in *Proc. IEEE ISGT Asia*, 2021, pp. 1–5.
- [13] I. Xyngi and M. Popov, "IEC61850 overview - where protection meets communication," in *Proc. IET DPSP*, 2010, pp. 1–5.
- [14] M. El 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, 2016.