A novel methodology to validate cyberattacks and evaluate their impact on power systems using real time digital simulation

Shahbaz Hussain
Department of Electrical Engineering
Qatar University
Doha, Qatar
shahbaz.hussain@polimi.it

Atif Iqbal
Department of Electrical Engineering
Qatar University
Doha, Qatar
atif.iqbal@qu.edu.qa

Stefano Zanero
Dipartimento di Elettronica, Informazione e Bioingegneria
Politecnico di Milano
Milan, Italy
stefano.zanero@polimi.it

S. M. Suhail Hussain
Department of Computer Science, School of Computing
National University of Singapore
Singapore
suhail@comp.nus.edu.sg

Abdullatif Shikfa
School of IT and Business Management
College of the North Atlantic - Qatar
Doha, Qatar
abdullatif.shikfa@cna-qatar.edu.qa

Enrico Ragaini
Dipartimento di Elettronica, Informazione e Bioingegneria
Politecnico di Milano
Milan, Italy
enrico.ragaini@polimi.it

Rashid Alammari
Department of Electrical Engineering
Qatar University
Doha, Qatar
ralammari@qu.edu.qa

Irfan Khan*
Department of Electrical and Computer Engineering
Texas A&M University
Texas, USA
irfankhan@tamu.edu

***Abstract*—The traditional power systems are rapidly digitalized and automated for increased monitoring and control. This automation of power system communication has made it possible to monitor and control operations remotely in a plant. However, this also opens up an exploitation vector for attackers, after they gain access to the substation network. This scenario can only be investigated through an in-depth study of communication protocols and control authority concepts associated with power system. IEC 61850 has emerged as the most popular protocol for power system communication. In this paper, we investigate real-time simulation of power systems with IEC 61850 based communication, in order to devise a testbed that can be used to validate false data injection cyberattacks and evaluate their impact. Based on the results, we discuss possible countermeasures to such attacks and outline future research directions.**

Keywords— cyberattacks, false data injection, real time digital simulation, IEC 61850, communication protocols, control authority, countermeasures

I. INTRODUCTION

Nowadays, power systems are being augmented with remote monitoring and control. On the one hand, this trend makes it possible to perform operations remotely from a control center. However, on the other hand, this creates an attack surface for intruders to attack the system to achieve their malicious objectives. In modern power automation systems, protection operations are performed via the generic object oriented substation event (GOOSE) protocol, as defined in IEC 61850 [1]. However, the standardized communication and protocols increases vulnerabilities that may be exploited by cyberattackers.

In present literature, researchers are focusing on either information technology (IT) or operational technology (OT) domains to provide novel solutions to various attack scenarios. For instance, focusing on IT-based solutions, in order to ensure the integrity of the messages exchanged, there have been proposals to adopt signatures based on traditional algorithms such as Rivest–Shamir–Adleman (RSA) and elliptic curve digital signature algorithm (ECDSA) [2]. However, since the end-to-end (E2E) delays introduced are beyond the acceptable threshold of 3 ms required in protection commands triggered via GOOSE, adoption of message authentication code (MAC) algorithms [3] has been proposed in their stead. Unfortunately, one of the drawbacks of MAC algorithms is the requirement of pre-shared keys. Future research pertaining to the safe distribution of keys or proposing of new algorithms without the need for pre-shared keys can be investigated [4].

Researchers have also proposed cybersecurity solutions in the power domain (or, more generally, outside the IT domain). In such solutions, the communication signals are verified before implementation at the device end, once they reach the intelligent electronic devices (IEDs). This verification can be carried out by various methods, such as getting confirmation from neighboring IEDs [5]. This confirms the integrity of messages and rules out the case of some individual compromised IEDs. This can, once again, happen within the standard-specified time requirements.

While these efforts help secure different parts of the systems separately, it is important to analyze security systemically, in an end-to-end fashion. In order to do so, the first step is to validate cyberattacks and evaluate their impact on a practical platform in real time. As it is difficult to conduct all tests on real system to avoid downtime and damage, alternatives such as real time simulations and digital twins offer huge potential. Such digital counterparts of the physical system provide great flexibility for testing engineers and researchers to implement and analyze cyberattacks [6]. This can be achieved by a testbed with the capacity of simulating both power and communication systems and their interconnection [7]. Many such testbeds are developed to simulate a cyber-physical system in present literature [8-10]. In this work, we have developed a novel methodology to validate cyberattacks and evaluate their impact on simulated power system in real time. It is achieved by a testbed which uses open source tools such as Snort and Wireshark to modify and observe the communication packets respectively. The packets are exchanged by the network interface of real time digital environment. The common

*Corresponding author

978-1-7281-8612-2/21/$31.00 ©2021 IEEE

practice in recent works is to capture the traffic during fault and then play it back to the digital simulation for analysis. However, this testbed is capable of creating a live environment to modify the IEC 61850 based communication packets in real time due to the synergy of digital simulation, Wireshark and Snort. The work deals with the following:

1) Implementation and analysis of GOOSE protocol in real time digital simulation.
2) Modification of these communication packets to validate cyberattack in a real case scenario.
3) Discuss appropriate countermeasures to these attacks.

The paper is organized accordingly with section 2 focusing on communication protocols and control authority used for power system automation as per IEC 61850. The methodology to validate cyberattacks in real time is covered in section 3 which explains the developed testbed for implementation of attacks, the simulation and modification of GOOSE packets and finally their impact on a simple electrical system and on a standard microgrid. Section 4 discusses cybersecurity solutions and finally section 5 concludes the work with implementation of countermeasures as a future work direction.

II. IEC 61850 Protocols and Control Authority

The IEC 61850 standard was initially developed for substation automation systems and later extended to entire power utility automation systems. In IEC 61850 based automated systems, the information is exchanged among different devices and the control centre, using the following protocols and messages, as defined by the IEC 61850 standard [11]:

- GOOSE for switching signals from IEDs to circuit breakers (CBs);
- Sampled measured values (SMV) for measurement values from merging units (MU) to IEDs;
- Manufacturing message specification (MMS) to exchange measurement readings and control commands between human machine interface (HMI) and IEDs; and
- Simple network time protocols (SNTP) for time synchronization of IEDs with GPS master clock.

Circuit breakers can be tripped via GOOSE during fault or maintenance manually from process and automatically from bay, station and remote level by the operator. To grant accessibility to operators at different locations and to avoid conflicts between them, a concept called control authority is used, which designates an operator's right to switch a specific circuit breaker [12]. This implementation is based on an entity called a switch object (SO), which is a combination of three logical node (LN) instances, one each from XCBR (or XSWI), CSWI and CILO as shown in TABLE I and Fig. 1. Information flow between these LN instances are internal to the model. A SO takes the control parameters and an interlock logic as inputs. A particular SO can be mapped to a desired circuit switch in the simulation for control operations. A remote client can access the SO for control purposes using the MMS protocol as shown in TABLE II. Binding of external trip signals (published as GOOSE messages) to the corresponding circuit breaker is achieved using a generic input (GGIO LN instance), and done independently from the SO.

TABLE I. Logical node classes and control parameters as per IEC-61850

Logical Node Class (IEC 61850-7-4)	Description
XCBR	Circuit Breakers - Switches with short circuit breaking capability
XSWI	Circuit Switches - Switches without short circuit breaking capability
CSWI	Switch Controller - Control all switching conditions above process level
CILO	Interlocking Function - Enable a switching operation if interlocking conditions are met
Control Parameter	**Description**
XCBR/XSWI.Loc	Represents the status of an actual switch at the process and allows taking over the manual control authority
LLNO.MltLev	Enables for more than one originator to hold control authority at the same time
CSWI.Loc	Represents the control behaviour of the logical node (bay level)
CSWI.LocSta	Represents the switching authority at station level

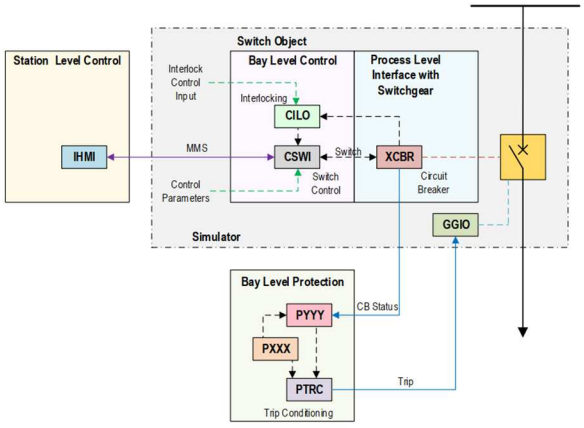

Fig. 1. Circuit breaker control based on switch object

TABLE II. Switchgear control based on control authority

Control Parameters				Control Authority at each Level			
Switch	Bay Control			Manual Control	Originator Category (OrCat)		
XCBR.Loc XSWI.Loc	LLNO.MltLev	CSWI.Loc	CSWI.LocSta	Process[1]	Bay[2]	Station[3]	Remote[3]
TRUE	FALSE	Not Applicable	Not Applicable	Always Allowed	Not Allowed	Not Allowed	Not Allowed
FALSE	FALSE	TRUE	Not Applicable	Always Allowed	Always Allowed	Not Allowed	Not Allowed
FALSE	FALSE	FALSE	TRUE	Always Allowed	Not Allowed	Always Allowed	Not Allowed
FALSE	FALSE	FALSE	FALSE	Always Allowed	Not Allowed	Not Allowed	Always Allowed
TRUE	TRUE	Not Applicable	Not Applicable	Always Allowed	Not Allowed	Not Allowed	Not Allowed
FALSE	TRUE	TRUE	Not Applicable	Always Allowed	Always Allowed	Not Allowed	Not Allowed
FALSE	TRUE	FALSE	TRUE	Always Allowed	Always Allowed	Always Allowed	Not Allowed
FALSE	TRUE	FALSE	FALSE	Always Allowed	Always Allowed	Always Allowed	Always Allowed

[1.] Current and voltage transformers (CT/VT) connected to MU
[2.] Switch controller communicating at process level with MU via SV and CB via GOOSE and MMS
[3.] Communication with switch controller via MMS

III. Methodology to Validate Cyberattacks

In order to validate cyberattacks and evaluate their impact on power system through real time simulation, we develop a testbed capable of implementing different attacks on power systems communication protocols, as well as of investigating their impact on the electrical system.

A. Testbed for implementation and modification of IEC 61850 communication

As we mentioned, IEC 61850 based automated power systems perform protection and measurement functions using GOOSE and SV protocols respectively. Based on the current and voltage sampled values sent to IEDs via SV protocol, they send control commands to circuit breakers via the GOOSE

protocol. Hence, these two protocols provide protection service over LAN in modern automated systems and their security is of paramount importance requiring special attention. If attackers get access to these communication packets, they can modify them by applying various attacks to corrupt the measurement values and protection commands. In such a scenario, operators will be potentially receiving fake data of the attacker's choice, potentially leading them to perform faulty operations. Attackers, on the other hand, can both manipulate measurement data (leading to wrong actions by the operators), or directly attack the protection commands. Keeping this into account, we implement the following steps:

1) Real time simulation of GOOSE and SV packets between IEDs,
2) We feed fake data to IEDs through the GOOSE and SV protocols, simulating a compromised IED accessed and controlled by an attacker.

We implement these steps in real time digital simulator (RTDS) [13], which provides the facility through its network interface card (GTNETx2) to implement two simulated IEDs behaving as subscriber and publisher communicating via either the GOOSE or the SV protocols. We use Wireshark, an open source tool, to observe and analyze these communication packets [14]. To modify the packets on the fly, we use a modified version of the open source tool Snort [15], which enables us to capture genuine messages to subscriber IEDs and modify them or propagate counterfeit messages. The block diagram for this testbed is shown in Fig. 2. Each GTNETx2 card has two modules, each capable of simulating one of the target protocols GOOSE and SV. The workstation on which Snort is installed captures the packets transmitted by the GTNETx2 cards, modifies them and sends them back to GTNETx2 card which is further connected to the processor simulating the designed electrical model in real time.

The objective of the laboratory testbed is to simulate different false data injection (FDI) attacks on communication protocols such as GOOSE, SV, MMS, DNP3 etc. and observe their impact on the electrical system in real time. The analysis will pave path for in depth study of various cyberattacks on power system and their appropriate countermeasures.

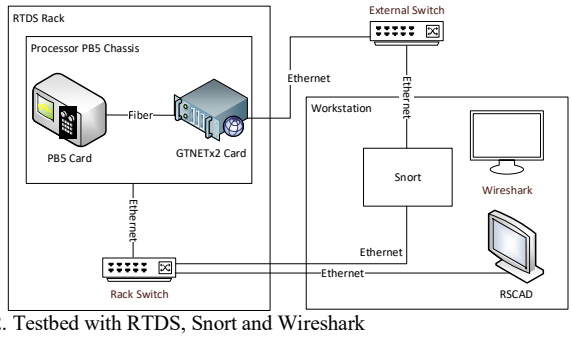

Fig. 2. Testbed with RTDS, Snort and Wireshark

B. *Simulation and modification of GOOSE packets*

The GOOSE protocol is associated with protection, which is critical, hence it has been implemented in RTDS by using the GSE component of the GTNETx2 card at both of its modules to simulate a publisher and a subscriber IED. The publisher IED sends four different types of data (X integer values, X binary values, a value composed by two bits and a floating point value) to the subscriber IED. At runtime, in a normal scenario, the data published by IED 1 is subscribed by IED 2 and vice-versa as shown in Fig. 3. We simulate a cyberattack in which the attacker captures the original GOOSE packets and manipulates them, sending counterfeit messages. In our testbed, the modification is carried out by using Snort providing it with control block (gocbRef) and data set (datSet) parameters of the original captured GOOSE packets. We show an example of this scenario in Fig. 4. In the example shown, the data published by IED 1 has been intercepted, and modified data has been forwarded to subscriber IED 2. In normal conditions, IED 1 sends the data [3 0 1 60] which is received by IED 2 as shown in Fig. 3; after the attacker's manipulation, instead, IED 2 is receiving the false data [9 1 3 22.22] injected by the attacker. The impact of this situation is significant; for instance, in case of a fault, a tripping signal would be sent by the control IED to the protection IED, instructing it to trip the circuit breaker. An attacker able to manipulate the transmission as shown in Fig. 4 would be able to prevent the protection IED from responding.

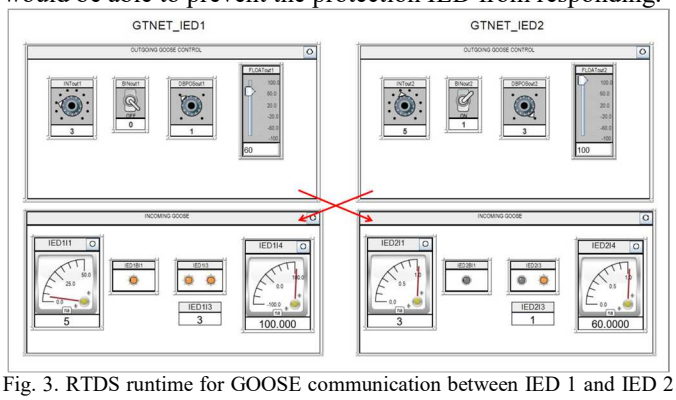

Fig. 3. RTDS runtime for GOOSE communication between IED 1 and IED 2 before the manipulation of packets by the attacker

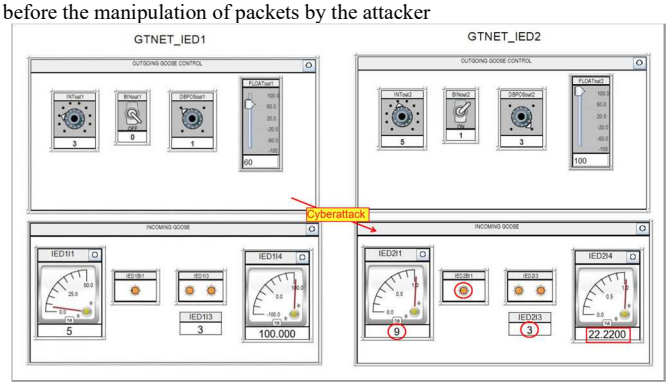

Fig. 4. RTDS runtime for GOOSE communication between IED 1 and IED 2 after the manipulation of packets by the attacker

The original and counterfeit GOOSE messages can be observed in Wireshark as shown in Fig. 5. It shows the original and modified GOOSE messages with integer data being changed from 3 to 9, boolean data is being modified from False to True and same is true for bit-string and floating point data types. As stNum and sqNum are crucial parameters in GOOSE packets from security perspective because the first (status) increments its value from 0 to 1 as soon as the broadcasting starts. The latter (sequence) initializes from 0 and keeps on incrementing with each repetition of the same message being

sent (burst mode) until another event (any change in the dataset of GOOSE packet) occurs. stNum increments its value on any new event with sqNum initialized to 0 and the broadcasting continues periodically. It can be observed that the initial original packet with status 1 and sequence 0 is captured from IED 1, modified and sent as new event to subscriber IED 2. It is reflected in its status which is updated to 2 while the sequence is reset to 0. The time stamp for original packet published by GTNETx2_GSE component is older (year 2004) and can be synchronized to current time with RTDS GTSYNC card, however we kept it as it is for the sake of easier identification of original published messages. The modified packet provided by Snort contains current timestamp (year 2020) corresponding to workstation's time clock with Snort installation.

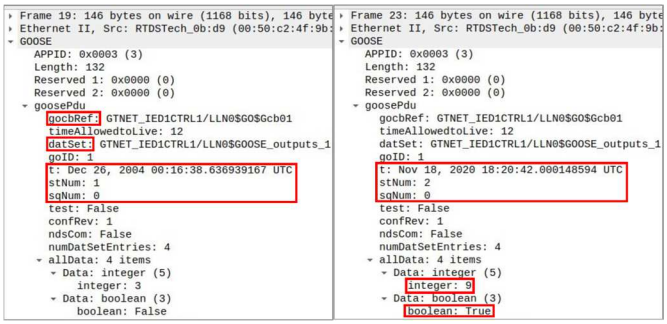

Fig. 5. Original and counterfeit GOOSE packets for IED 1 on LAN port

Since protection functions in IEC 61850 automated systems are performed by GOOSE packets, it is necessary to discuss and develop appropriate cybersecurity solutions which can secure the communication [16]. Similarly, the SV protocol and its packets can be simulated and modified. For brevity, we omit a full description of that experiment.

C. *Tripping of circuit breaker and its electrical impact*

A circuit breaker can be tripped/reclosed by sending a boolean value of False/True respectively in GOOSE data items. Consider a simple doubly fed 3-phase system with three buses (1-3), a resistive load at bus 2, circuit breaker CB1 between bus 1 and 2 and isolator at each end as shown in Fig. 6 from the Draft (reserved for design) in RSCAD (software counterpart of RTDS) and intended to observe the electrical impact when the circuit breaker is tripped in Runtime (reserved for simulation) of RSCAD.

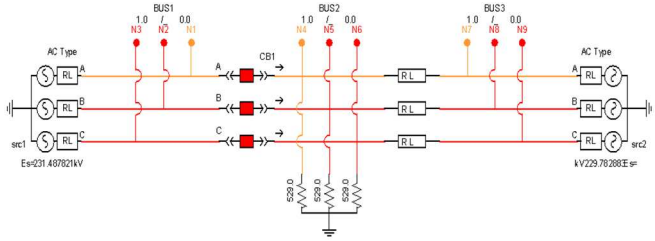

Fig. 6. 3-phase doubly fed system in RSCAD Draft with 3 buses, circuit breaker, isolators and load

The designed model in Draft is compiled and then simulated in Runtime to observe bus voltages and breaker currents. When the breaker is closed, due to load connected at bus 2, its voltage is 229.9 kV while each source bus (1 and 3) have nominal voltage of 230 kV. Fig. 7 shows sinusoidal 3-phase voltage at load bus 2 and breaker currents oscillating between [-0.7, 0.7] kA confirming the breaker is closed with current flow.

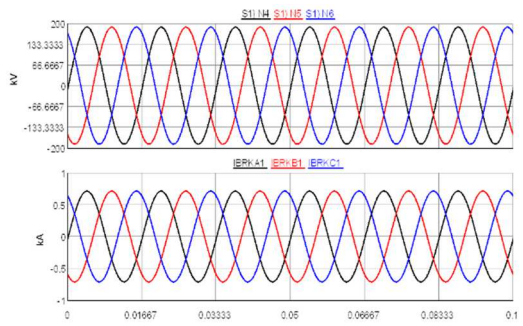

Fig. 7. 3-phase voltage at load bus 2 and 3-phase breaker current when CB is closed (ON/red)

The breaker is then tripped remotely with the GOOSE protocol which changes all the bus voltages. Source bus 1 voltage increases to 231.5 kV while source bus 2 voltage drops to 228.7 kV, both from 230 kV. Load bus voltage decreases more to 226.8 kV from 229.9 kV and this variation can damage the sensitive load components connected to this bus if appropriate protection is not applied. The same scenario can be observed by 3-phase voltage of bus 2 and breaker currents as shown in Fig. 8. The breaker currents oscillating between [-4E-7, 4E-7] reflects its opened status with minimal current flow.

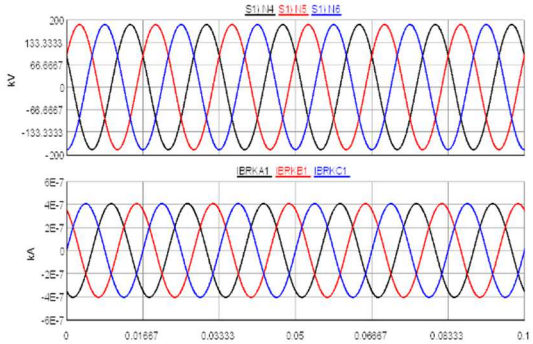

Fig. 8. 3-phase voltage at load bus 2 and 3-phase breaker currents when CB is opened (OFF/green)

D. *Impact of FDI attacks on Banshee Microgrid*

While in the previous two subsections we have showed how to simulate the modification of GOOSE packets, and the potential impact of such manipulations on a simple electrical system, the effect of modified communications on a larger, more complex electrical system can increase manifold. As an example, we will discuss impacts on a microgrid widely used as a benchmark in different studies for real time simulations of power systems known as Banshee microgrid, shown in Fig. 9 [17]. It consists of three areas fed by three radial feeders connected to the grid. The areas can be interconnected through normally opened (N.O.) tie switches and can operate under either grid connected or islanding modes. The main breaker to each area can be tripped by a simple GOOSE packet with boolean data set as False, thus initiating islanding mode. In this mode, frequency drops, if the area generation cannot adequately feeds the area load demand in isolation from the grid, further tripping or load shedding may follow. On a small scale, the various breakers inside each area can also be tripped to isolate various power components and devices to introduce disturbances in the overall system.

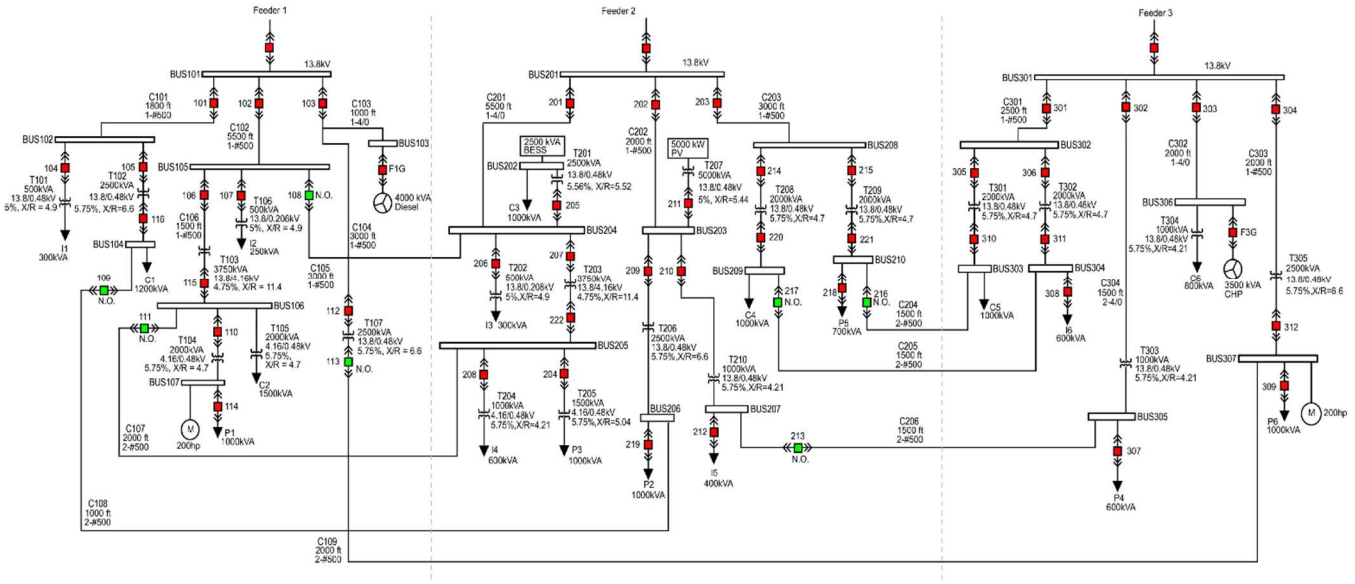

Fig. 9. Runtime single line diagram of Banshee microgrid

The generation assets in the three areas include 4 MVA diesel in area 1 and 3.5 MVA natural gas fired combined heat and power (CHP) in area 3, both are based on governor, exciter and synchronous generator model. Area 2 has 5 MVA photovoltaic (PV) with 2.5 MVA battery energy storage system (BESS) based on average value model for converter. The system contains the following components:

- Transformers: with primary voltage level of 13.8 kV stepping down to 4.16 kV, 480 V and 208 V secondary voltage levels.
- Loads: Dynamic aggregated ones (categorized into critical, priority and interruptible) and motor loads (induction motor driving 200 horsepower (hp) chiller compressor).
- Cables: modelled with series resistance-inductance (RL) impedances.
- Circuit breakers: including synchro-check capability for main incomers (3 areas) used to connect each area to the grid. All these breakers including in each area can be controlled by external trip/reclose signals or manual push buttons in Runtime of RSCAD.

This system provides the opportunity to investigate islanding scenarios. The objective in islanding any area is to observe if generation can keep up with the load demand inside that area for frequency stability. After islanding, if the frequency drops, there are controls in place in each area which will shed the interruptible loads in stages proceeding to priority loads if required. The operating points of generation assets may also change in case of islanding, particularly BESS in area 2 shifts to VF mode from PQ mode. Fig. 10 shows the difference in steps 1 to 5 observed after islanding between areas with conventional generation (area 1 and area 3) and renewable generation (area 2). After islanding an area by tripping the main incoming breaker, the frequency drops and the area struggles to achieve the nominal frequency. In areas 1 and 3, it is achieved by shedding the interruptible loads such as I2 in area 1, the sources also shifts to new operating points and finally the rotating phasors at the top of each diagram represents the mismatch of voltage frequency between grid and the area. In area 3, the battery starts providing power to the area which changes its operating points and also avoids tripping of interruptible loads such as I3 in area 2.

As the Banshee microgrid is a perfect fit for power system studies such as islanding scenarios in real time which is carried out by remotely tripping area breakers with modified GOOSE packets in our case, the same system can be extended to study the effects of other remote cyberattacks on a standard electrical system. For example, an attacker can corrupt load shedding controls or prioritize specific distributed energy resources (DERs) by applying FDI attack between Aggregator (an equipment responsible for communication with DERs and optimization to provide economical energy from them) and DERs to create monopoly for selling electricity. Another scenario can be a Denial of Service (DoS) attack on the Aggregator to block available power information from DERs, resulting in overloading of generation assets for extended periods of time, leading to their damage or failure.

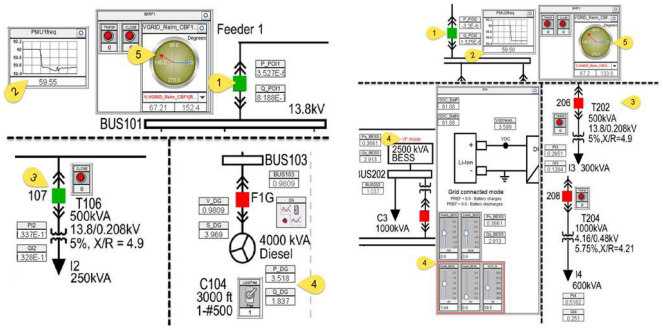

Fig. 10. Islanding Area 1 or Area 3 vs. Area 2

IV. Discussion on Cybersecurity Solutions

In automated power systems, an attacker will first target the power system network to breach the electronic boundary of the

targeted system. The next point of attack will be the devices and data flowing in between them. In order to enhance cybersecurity, various defense mechanisms such as zoning (physical or network) of power system, securing communication protocols as per IEC 62351, intruder detection system (IDS) based on statistics, machine learning (ML) [18] with integration of artificial intelligence (AI) [19], remote attestation (software or hardware based), deception technology such as honeypots and incident response (basically damage control after the attack) can be deployed by weighing in their advantages and demerits [20]. Machine learning techniques and algorithms provide efficient results when applied to network traffic for anomaly detection [21]. Considering this global scenario, we define three main categories of countermeasures to handle the cyberattacks as following:

- *IT solutions:* These solutions mostly deal with the security of communication data flowing between devices in a power utility system. Different encryption algorithms and security measures can be applied in this category to ensure confidentiality, integrity and availability of communication data [22]. RSA, ECSDA and MAC algorithms are prime examples which can be employed on power system communication such as GOOSE and SV packets to secure the data. These common algorithms have their merits and drawbacks and novel methods can be developed based on the principles underlying in them.
- *OT solutions:* These solutions rely on security at device level. For example, the critical instructions being received by IEDs can be authenticated by security filters implemented inside their firmware. An example of such a security measure is to get confirmation from neighboring IEDs to verify that the command being received is genuine and should be implemented or not. An interesting direction can be to deploy ML techniques such as decision tree, Bayesian networks, clustering, Naive Bayes and neural networks to secure the integrity of IED network [23]. However, these methods should not violate the stringent time requirements such as of 3 ms in GOOSE.
- *Hybrid solutions:* The solutions are designed to provide combined security of devices and data in automated power system. They are based on a combination of IT and OT solutions to provide a global and robust cybersecurity system such as IDS [24] or intruder prevention system (IPS) to the cyberattacks by securing both the devices and the communication in between them.

V. Conclusion

In this work, a methodology to validate cyberattacks and evaluate their impact on power systems is established with the help of a testbed focusing on GOOSE, the most critical protocol utilized for implementing protection. The protocol has been implemented and modified GOOSE messages have been sent to a simulated electrical system in order to observe its impact. This allowed us to investigate the electrical effects and discuss broad categories of countermeasures. Based on this validation of cyberattacks, their impact on power systems and brief discussion on possible countermeasures, future work will deal with developing a novel solution to secure devices and communications inside automated power systems, while fulfilling the strict performance requirements for these environments.

References

[1] 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, p. 106008, 2020.

[2] T. S. Ustun, S. M. Farooq, and S. S. Hussain, "A novel approach for mitigation of replay and masquerade attacks in smartgrids using IEC 61850 standard," *IEEE Access,* vol. 7, pp. 156044-156053, 2019.

[3] S. S. Hussain, S. M. Farooq, and T. S. Ustun, "Analysis and implementation of message authentication code (MAC) algorithms for GOOSE message security," *IEEE Access,* vol. 7, pp. 80980-80984, 2019.

[4] S. S. Hussain, T. S. Ustun, and A. Kalam, "A review of IEC 62351 security mechanisms for IEC 61850 message exchanges," *IEEE Transactions on Industrial Informatics,* 2019.

[5] 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 Transactions on Industrial Informatics,* vol. 15, pp. 4332-4341, 2018.

[6] C. Devanarayana, Y. Zhang, and R. Kuffel, "Testing Cyber Security of Power Systems on a Real Time Digital Simulator," in *2019 IEEE 8th International Conference on Advanced Power System Automation and Protection (APAP)*, 2019, pp. 1166-1170.

[7] C.-C. Sun, A. Hahn, and C.-C. Liu, "Cyber security of a power grid: State-of-the-art," *International Journal of Electrical Power & Energy Systems,* vol. 99, pp. 45-56, 2018.

[8] C.-C. Sun, J. Hong, and C.-C. Liu, "A co-simulation environment for integrated cyber and power systems," in *2015 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2015, pp. 133-138.

[9] A. Ashok, S. Krishnaswamy, and M. Govindarasu, "PowerCyber: A remotely accessible testbed for Cyber Physical security of the Smart Grid," in *2016 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, 2016, pp. 1-5.

[10] M. M. S. Khan, A. Palomino, J. Brugman, J. Giraldo, S. K. Kasera, and M. Parvania, "The Cyberphysical Power System Resilience Testbed: Architecture and Applications," *Computer,* vol. 53, pp. 44-54, 2020.

[11] P. Matoušek, "Description of IEC 61850 communication," in *Technical Report*, ed: Brno University of Technology, 2018.

[12] D. R. Gurusinghe, S. Kariyawasam, and D. S. Ouellette, "Testing of Switchgear Operation in an IEC 61850 based SAS using a Real-Time Simulator," *PAC World Conference,* 2018.

[13] R. Kuffel, J. Giesbrecht, T. Maguire, R. Wierckx, and P. McLaren, "RTDS-a fully digital power system simulator operating in real time," in *Proceedings 1995 International Conference on Energy Management and Power Delivery EMPD'95*, 1995, pp. 498-503.

[14] V. Ndatinya, Z. Xiao, V. R. Manepalli, K. Meng, and Y. Xiao, "Network forensics analysis using Wireshark," *International Journal of Security and Networks,* vol. 10, pp. 91-106, 2015.

[15] C. Devanarayana, "Inline Packet Modifier using Snort, RTDS Technologies," Available at: <https://github.com/chamara84/snort-2.9_RTDS> [Accessed on: 11/2020].

[16] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," *Computer Networks,* vol. 169, p. 107094, 2020.

[17] C. Jegues, "Banshee Microgrid Sample Case," *RTDS Technologies,* Nov. 2019.

[18] P. Kreimel, O. Eigner, F. Mercaldo, A. Santone, and P. Tavolato, "Anomaly detection in substation networks," *Journal of Information Security and Applications,* vol. 54, p. 102527, 2020.

[19] S. Bhamidipati, K. J. Kim, H. Sun, and P. V. Orlik, "Artificial-Intelligence-Based Distributed Belief Propagation and Recurrent Neural Network Algorithm for Wide-Area Monitoring Systems," *IEEE Network,* vol. 34, pp. 64-72, 2020.

[20] H. C. Tan, C. Cheh, B. Chen, and D. Mashima, "Tabulating cybersecurity solutions for substations: Towards pragmatic design and planning," in *2019 IEEE Innovative Smart Grid Technologies-Asia (ISGT Asia)*, 2019, pp. 1018-1023.

[21] S. Soni and B. Bhushan, "Use of Machine Learning algorithms for designing efficient cyber security solutions," in *2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)*, 2019, pp. 1496-1501.

[22] S. S. Hussain, S. M. Farooq, and T. S. Ustun, "A Method for Achieving Confidentiality and Integrity in IEC 61850 GOOSE Messages," *IEEE Transactions on Power Delivery,* 2020.

[23] D. Wang, X. Wang, Y. Zhang, and L. Jin, "Detection of power grid disturbances and cyber-attacks based on machine learning," *Journal of Information Security and Applications,* vol. 46, pp. 42-52, 2019.

[24] J. Hong and C.-C. Liu, "Intelligent electronic devices with collaborative intrusion detection systems," *IEEE Transactions on Smart Grid,* vol. 10, pp. 271-281, 2017.