ORNL/TM-2023/2921

Electrical Fault Detection, Power Quality, Distributed Energy Resource Use Cases, and Cyber Event Applications with the Cyber Grid Guard System Using Distributed Ledger Technology

Emilio C. Piesciorovsky
Gary Hahn
Raymond Borges Hink
Aaron Werth
Annabelle Lee

August 2023

OAK RIDGE National Laboratory

ORNL IS MANAGED BY UT-BATTELLE LLC FOR THE US DEPARTMENT OF ENERGY

ORNL/TM-2023/2921

Electrification and Energy Infrastructures Division

ELECTRICAL FAULT DETECTION, POWER QUALITY, DISTRIBUTED ENERGY RESOURCE USE CASES, AND CYBER EVENT APPLICATIONS WITH THE CYBER GRID GUARD SYSTEM USING DISTRIBUTED LEDGER TECHNOLOGY

Emilio C. Piesciorovsky[a]
Gary Hahn[a]
Raymond Borges Hink[a]
Aaron Werth[b]
Annabelle Lee[c]

[a]Electrification and Energy Infrastructures Division, Oak Ridge National Laboratory, One Bethel Valley Road, Oak Ridge, TN 37831, USA
[b]Cyber Resilience and Intelligence Division, Oak Ridge National Laboratory, One Bethel Valley Road, Oak Ridge, TN 37831, USA
[c]Nevermore Security LLC, 31256 Stone Canyon Rd, Evergreen, CO 80439, USA

June 2023

Prepared by
OAK RIDGE NATIONAL LABORATORY
Oak Ridge, TN 37831-6283
managed by
UT-BATTELLE LLC
for the
US DEPARTMENT OF ENERGY

CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

3LG	three line to ground
ANSI	American National Standards Institute
CGG	Cyber Grid Guard
CT	current transformer
DER	distributed energy resource
DLT	distributed ledger technology
DNP3	Distributed Network Protocol 3
EV	electric vehicle
goID	Generic Object-Oriented Substation Event device ID
GOOSE	Generic Object-Oriented Substation Event
HMI	human–machine interface
IEC	International Electrotechnical Commission
IED	intelligent electronic device
IRIG-B	inter-range instrumentation group time code B
ITC	inverse time current
LL	line to line
LLG	line to line ground
RMS	root mean square
SCADA	supervisory control and data acquisition
SEL	Schweitzer Engineering Laboratories
SLG	single line to ground
SV	smart visu
VM	virtual machine
VPP	virtual power plant

EXECUTIVE SUMMARY

Electrical utilities continue to deploy more intelligent electronic devices (IEDs) inside and outside electrical substations and are associated with distributed energy resources (DERs). The integrity and confidentiality of data from IEDs are crucial, and distributed ledger technology (DLT) could improve the resilience of microgrids by helping to make these data more secure. However, the dynamism of the penetration of customer-owned DERs and the deployment of sensors with IEDs has led to the identification of new applications using DLT that are focused on other areas, such as monitoring, operation, and management of the grid and its assets. In addition, most studies on electrical grid applications with a blockchain were validated with software simulations. Although general monitoring of power systems for using DLT could be evaluated in operational electrical grids, other DLT research applications such as defense against cyberattacks and/or electrical fault detection are unlikely to be performed in a real infrastructure because of possible risks to the network and equipment security.

This report summarizes the application of DLT within power systems, providing a secure DLT framework for collecting data from IEDs, such as power meters and protective relays, inside and outside an electrical substation and/or between two electrical utilities. In this study, the use case scenarios were created and assessed for different power system applications using DLT. The electrical fault detection for faulted phases; power quality monitoring of phase voltage magnitudes, frequency levels, and load power factor; DER use case monitoring; and cyber event applications were performed in a test bed with the Cyber Grid Guard system using DLT. The test bed used a real-time simulator with power meters and protective relays in the loop. Section 1 presents a literature review of power system applications using a blockchain at the research level. Section 2 provides the theory and equations used in this report. Section 3 describes the test bed, equipment, architecture, and electrical grid. Section 4 describes the experimental models and scenarios for the electrical fault detection, power quality, DER, and cyber event use case scenarios with the Cyber Grid Guard system using DLT. Section 5 describes the results collected from the tests based on comparing the time-stamped events of the analog signals from the IEDs, DLT computer, and real-time simulator. Section 6 discusses the results for the use case scenarios. Finally, Section 7 presents the conclusions for this report.

1. INTRODUCTION

Electrical utilities continue to deploy more types and numbers of intelligent electronic devices (IEDs), such as power meters and protective relays. As the market penetration of distributed energy resources (DERs) increases, so do measurements that rely on communications between IEDs within and outside the substation perimeter. Currently, the most popular blockchain research applications for electrical utilities are in the field of energy trading [1]. However, utilities have also employed blockchain technology to support new functions that can improve the resilience of the electrical grid [2]. Additionally, researchers are discovering grid management applications that are nontraditional in scope. Dynamic management capabilities are possible with customer-owned and customer-managed DERs and with the deployment of smart sensors with IEDs. Therefore, numerous new blockchain applications are being developed that focus on control, measurement, and protection.

The integrity and confidentiality of data and control commands between IEDs are crucial. The establishment of and reliance on communications across the utility–customer interface to enhance grid dispatch and control have created a significant threat vector for secure power system operations, such as cyber intrusion and/or communications failures. Furthermore, new scenarios include the dynamism of the energy market with the penetration of DERs and the deployment of sensors with IEDs. This opportunity introduces new players to the energy market, requiring peer-to-peer energy trading in real time [3]. Blockchain technology supports such peer-to-peer trading and thus has injected new vitality into the energy market.

The blockchain applications in the electricity sector can be classified as energy trading; wholesale markets; metering, billing, and retail markets; trading of renewable energy certificates and carbon credits; electric vehicle (EV) charging; power system cybersecurity enhancements; renewable energy certificates; and grid operation and management [4]. Based on energy trading applications, one study presented a joint operation mechanism of a distributed photovoltaic power generation market and carbon market [5]. This method modeled two chains that enabled the two markets to share data using an improved IEEE 33-bus system based on software simulation [5]. Another source presented a blockchain for transacting energy and carbon allowance in networked microgrids. Moreover, the blockchain solution algorithm consisted of column-and-constraint generation and Karush–Kuhn–Tucker conditions to solve the two-stage market optimization problems based on using an IEEE 33-bus system and an IEEE 123-bus system with a software simulation [6]. Another publication described research on a blockchain-based, peer-to-peer, transactive energy system for a community microgrid with demand response management [7]. This system used two architectures: one with the third-party agent demonstrated using the MATLAB environment and the other with the virtual agent (without the third party) implemented using a blockchain environment [7]. Another relevant blockchain application was based on cyberattack protection frameworks [8]. A distributed blockchain-based data protection framework for modern power systems against cyberattacks was developed in another source [8]; the effectiveness of this protection framework was demonstrated on the IEEE 118-bus benchmark system with a software simulation. A blockchain-based decentralized replay attack detection for large-scale power systems was based on the use of a software simulation with an IEEE 3,012-bus transmission grid [9].

Additionally, the penetration of DERs is becoming an essential part of smart grid systems and led to the formation of various aggregation mechanisms, such as virtual power plants (VPPs), enabling the use of small- and medium-scale DERs in electricity markets [10]. One publication presented a blockchain-based, decentralized VPP of small prosumers that used a public blockchain and self-enforcing smart contract to construct a VPP of prosumers to provide energy services based on smart contract algorithms [11]. Blockchain technology has also been studied in EV research applications. A smart EV charging station energy management system based on blockchain technology—which aims to protect privacy of EV users,

ensure fairness of power transactions, and meet charging demands for many EVs—was presented in one study [12]. Another study proposed an artificial intelligence–enabled, blockchain-based EV integration system in a smart grid platform [13]. This system was based on an artificial neural network for EV charge prediction, in which the EV fleet was employed as a consumer and a supplier of electrical energy within a VPP platform.

Most energy potential applications with a blockchain were based on software simulations [5–13]. Although general monitoring for blockchain applications could be evaluated in operational electrical grids, other blockchain research applications such as cyberattack defense and electrical fault detection are unlikely to be performed in operational electrical grids because of possible risks to network security, equipment failures, and energy provision. Therefore, creating a test bed with the Cyber Grid Guard (CGG) system using distributed ledger technology (DLT) is crucial for multipurpose blockchain applications. In the present study, the test bed with the CGG system was established at the US Department of Energy's Oak Ridge National Laboratory [14, 15] and enhanced with two wind farm models. This advanced electrical substation grid test bed was assessed for electrical fault detection, power quality monitoring, DER use cases, and cyber event tests, implementing the CGG system and DLT.

2. THEORY AND EQUATIONS

In this section, the theory and equations for implementing the electrical fault and power quality event detections are described. This section also presents the inverse time current (ITC) curve equations used to analyze the cyber event based on modifying the current transformer (CT) ratio of a protective relay.

2.1 ELECTRICAL FAULT EVENT DETECTION

The detection of electrical faults at the radial power lines was implemented by finding the boundaries between the minimum root mean square (RMS) current at the electrical faults and the maximum load RMS current. The threshold current to detect the electrical faults conforms to Eq. (1):

$$I_{RMS\ MIN\ FAULT} > I_{THR} > 1.3 \times I_{RMS\ MAX\ LOAD}, \tag{1}$$

where I_{THR} is the RMS current threshold measured in amps, $I_{RMS\ MAX\ LOAD}$ is the maximum current at normal operation in amps, and $I_{RMS\ MIN\ FAULT}$ is the minimum RMS electrical fault current in amps.

2.2 POWER QUALITY EVENT DETECTION

The power quality is based on assessing the voltages, frequency, and total power factor for normal operation in the power grid. The voltage limits were based on the American National Standards Institute (ANSI) C84.1 Standard [23]. Then, the service voltage limits and range B for the nominal voltage level and user load site location based on ANSI C84.1 Standard [23] were used, and the voltage boundaries to detect the under- and overvoltage situations were calculated using Eq. (2):

$$V_{NOM} \times 1.058 > V_{OVER\ ONE\ MINUTE} > V_{NOM} \times 0.95, \tag{2}$$

where V_{NOM} is the phase-to-ground nominal RMS voltage of the power grid measured in kilovolts, and $V_{OVER\ ONE\ MINUTE}$ is the phase-to-ground RMS voltage in kilovolts measured for more than 1 min to detect the voltage limits during the permanent events instead of transient states (e.g., tripped breakers, electrical faults, switched tap changers).

The limits for a 60 Hz electrical grid were calculated within a range of ±0.5% [24], and the frequency boundaries to detect the under- and overfrequency situations were calculated using Eq. (3):

$$f_{NOM} \times 1.005 > f_{OVER\ ONE\ MINUTE} > f_{NOM} \times 0.995, \tag{3}$$

where f_{NOM} is the nominal frequency (60 Hz) measured in hertz, and $f_{OVER\ ONE\ MINUTE}$ is the grid frequency in hertz measured for more than 1 min to detect the frequency limits during the permanent events instead of transient states.

The total power factor was calculated as the ratio of the total real power to the total apparent power [25]. It was estimated by using the total real and reactive power using Eq. (4):

$$PF = \frac{P}{|S|} = \frac{P}{\sqrt{Q^2 + P^2}}, \tag{4}$$

where PF is the total power factor measured from 0 to 1, P is the total real power in watts, S is the total apparent power in volt-amperes, and Q is the total reactive power in volt-amperes reactive.

If the total power factor is measured as a percentage, the maximum total power factor is 100%, and the minimum percent total power factor limit is usually between 80% and 98% [25]. With the minimum and maximum power factors limited between 0.9 (90%) and 1 (100%), the total power factor boundaries was estimated by Eq. (5):

$$PF_{MAX} > PF_{\text{OVER ONE MINUTE}} > PF_{\text{MAX}} \times 0.9, \tag{5}$$

where PF_{MAX} is the maximum total power factor measured as a percentage, and $PF_{OVER\ ONE\ MINUTE}$ is the percent total power factor measured for more than 1 min to detect the total power factor limits during the permanent events instead of transient states (e.g., tripped breakers, electrical faults, switched tap changers).

2.3 INVERSE TIME OVERCURRENT CURVE

ITC curves were used to set the relays. Based on the Schweitzer Engineering Laboratories (SEL)–451 relay [20], the inverse time overcurrent setting was based on the U3 Very ITC curves given by Eq. (6):

$$T_R = TDS \times \left(K_1 + \frac{K_2}{M^{(K_3)} - 1} \right) \times 60, \tag{6}$$

where T_R is the calculated relay time measured in cycles, TDS is the time dial setting in seconds, M is the applied multiple of pickup current, and K_1 (0.0963), K_2 (3.88), and K_3 (2) are the curve constants for the U3 Very ITC curves.

For Eq. (6), the multiple of pickup current (M) is given by Eq. (7):

$$M = \frac{I_S}{I_P} = \frac{\left(\frac{I}{CTR}\right)}{I_S}, \tag{7}$$

where M is the applied multiple of pickup current, I_S is the secondary input current measured in amperes, I_P is the relay current pickup setting in amperes, I is the primary input current in amperes, and CTR is the CT ratio.

By placing Eq. (7) in Eq. (6), the calculated relay time can be estimated by using Eq. (8) or Eq. (9).

$$T_R = TDS \times \left(0.0963 + \frac{3.88}{\left(\frac{I_S}{I_P}\right)^2 - 1} \right) \times 60, \tag{8}$$

$$T_R = TDS \times \left(0.0963 + \frac{3.88}{\left(\frac{I/CTR}{I_P}\right)^2 - 1} \right) \times 60. \tag{9}$$

To estimate the calculated relay time at an electrical fault for an overcurrent relay, Eq. (8) or Eq. (9) could be used. Whereas Eq. (8) is based on the secondary input current, Eq. (9) is based on the primary input current and the CT ratio.

3. THE ELECTRICAL SUBSTATION GRID TEST BED WITH DERs AND DLT

In this section, the electrical grid substation test bed with customer-owned DERs (wind farms) and the CGG system is described. The one-line diagram and equipment are presented in detail. The test bed architecture based on the physical layer (level 1), the protection and metering layer (level 2), the automation layer (level 3), and the control layer (level 4) is described. The three-line diagram of the electrical substation grid test bed with the customer-owned DERs (wind farms) is presented, and the CGG system is defined and described.

3.1 ONE-LINE DIAGRAM AND EQUIPMENT

A typical substation test bed with DERs and IEDs was managed for controlling and monitoring using blockchain technology. This test bed used a software model–simulated power system that performed electrical faults and cyber events. The test bed was used to determine whether the blockchain architecture was effective in controlling the utility grid and managing its assets and equipment. The one-line diagram in Figure 1 represents the design of a 34.5/12.47 kV (primary/secondary voltage) electrical substation. The electrical substation was based on a sectionalized bus configuration [16], with two power transformers and two radial feeders connected to two customer-owned DERs (wind farms), as shown in Figure 1.a. The power meters and protective relays in the rack (Figure 1.b) of the test bed were named by numbers and their locations in the power system are observed in the one-line diagram of Figure 1.a.

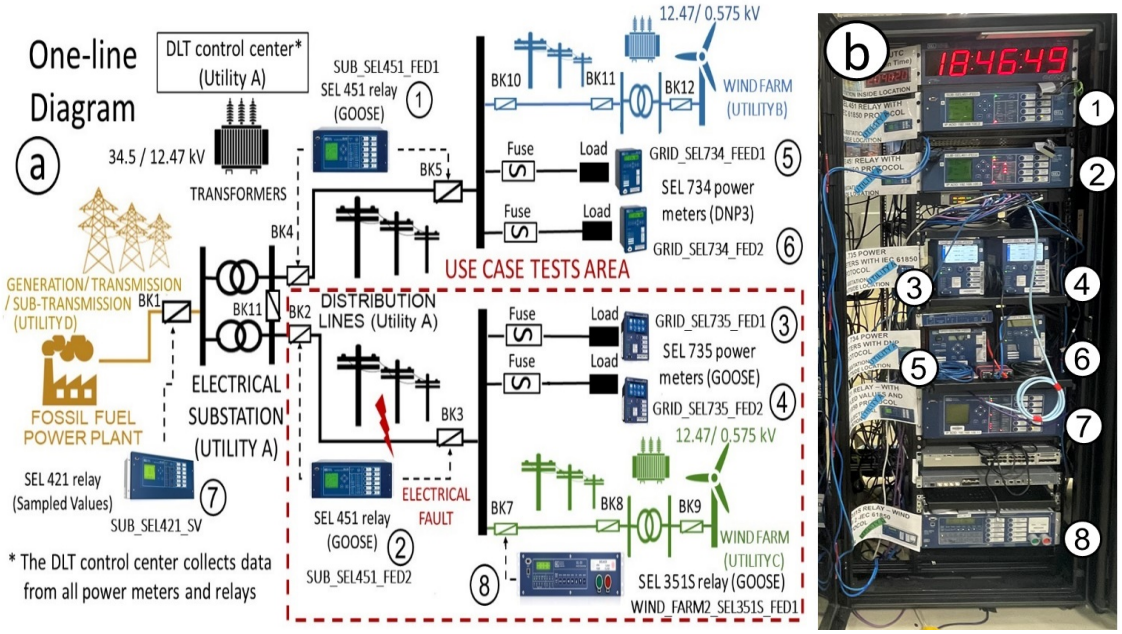

Figure 1. (a) One-line diagram and (b) equipment rack.

This one-line diagram was based on a published report [14]. Utility A included an electrical substation and distribution grid that had the control center. Utility A's electrical substation had two power transformers of 10 MVA, primary voltage of 34.5 kV, and secondary voltage of 12.47 kV. The electrical grid was a 12.47 kV power system with load feeders that are usually connected in a radial configuration; however, the load feeders could be connected to the wind farms (utilities B and C). Utilities B and C were the customer-owned DERs with six 1.5 MW wind turbines (two 9 MW wind farms), and utility D was the main energy source based on a fossil fuel power plant. In the fuses, feeders were configured at the SEL-735 [17] power meters with International Electrotechnical Commission (IEC) 61850 Generic Object-

Oriented Substation Event (GOOSE) protocol and at the SEL-734 [18] power meters with Distributed Network Protocol 3 (DNP3) protocol. The SEL-421 [19] relay at the 34.5 kV side of the electrical substation was configured with the IEC 61850 Sampled Values protocol, and the SEL-451 [20] and SEL-351S [21] relays were configured with the IEC 61850 GOOSE protocol. These protective relays measured the phase voltages and currents; real and reactive total power; total power factor; frequency; and breaker states that were collected by the control center (utility A). The tests were performed on the feeder inside the red dashed rectangle in Figure 1.a to assess the CGG system for electrical faults detection, power quality monitoring, DER use cases, and cyber event tests. In Figure 1.b, the protective relays and power meters of the one-line diagram are shown in the equipment rack. These IEDs were wired to a real-time simulator and communication devices that were connected to a synchronized-time system.

3.2 TEST BED AND ARCHITECTURE

The test bed (Figure 2) collected and recorded relevant data during the simulations. The devices (e.g., protective relays, power meters) produced data that were synchronized with a time source. The electrical substation grid test bed had six computers at desks and on racks. The computers and desk-based workstations are shown in Figure 2: the host computer (6), human–machine interface (HMI) computer (7), traffic network computer (8), and supervisory control and data acquisition (SCADA) computer (9).

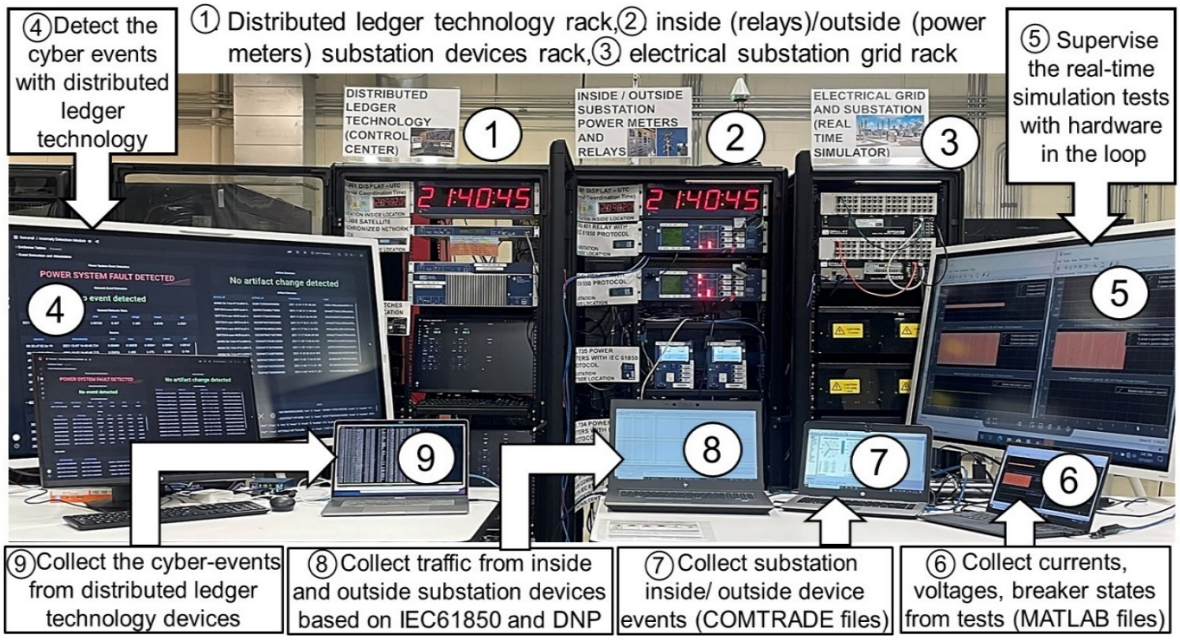

Figure 2. Electrical substation grid test bed and workstations.

Figure 3 shows the control center HMI, local substation HMI, virtual machine (VM) Blueframe, and EmSense high-speed smart visu (SV) servers/computers in the rack for the CGG system. The architecture of the electrical substation grid with customer-owned DERs (wind farms) and the CGG system for the test bed had four layers (Figure 3). The physical layer (level 1) included the power lines, breakers, transformers, feeder loads, and other power system elements that were simulated by the real-time simulator. The protection and metering layer (level 2) contained the hardware in the loop, represented by the protective relays and power meters. The automation layer (level 3) contained the remote terminal units and the Ethernet switches. The control layer (level 4) contained the supervisory control and data acquisition, HMI, and synchronized-time system for the CGG system.

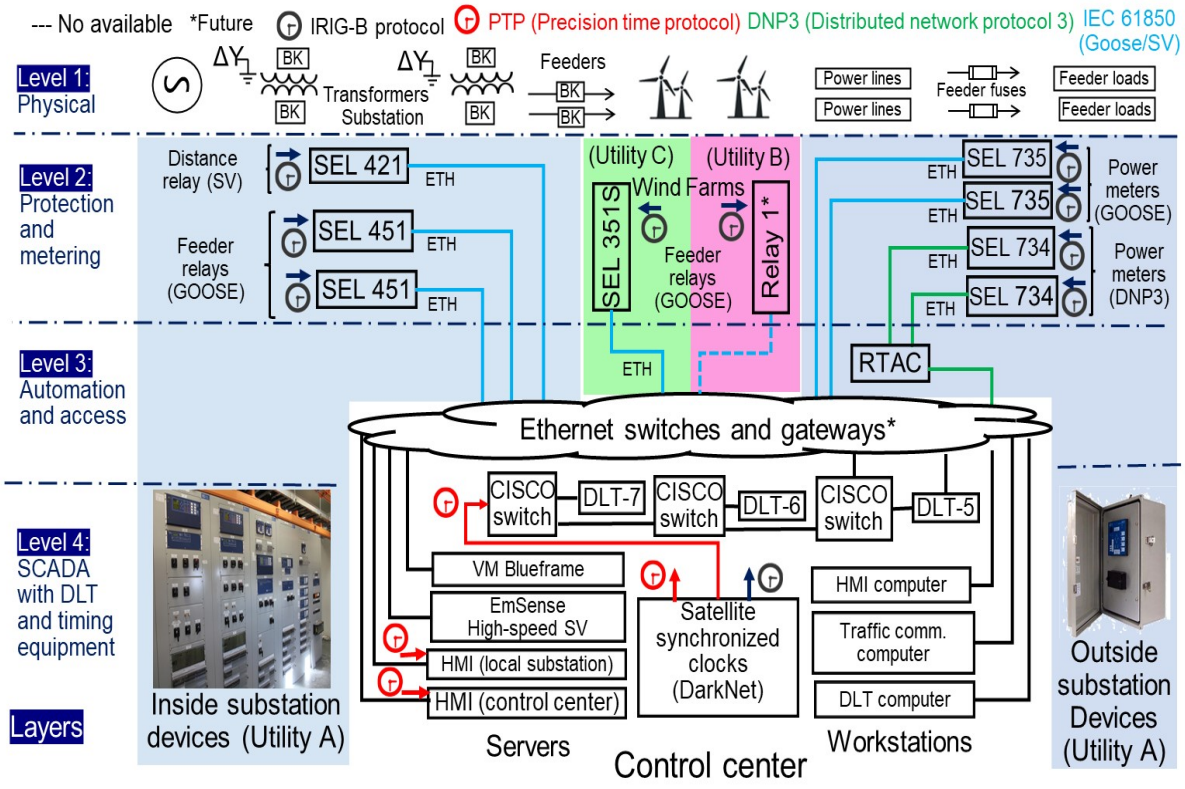

Figure 3. Architecture of the electrical substation grid test bed.

The synchronized-time protocols used in this architecture implemented the precision-time protocol and inter-range instrumentation group time code B (IRIG-B) signals. The precision-time protocol communication was implemented in the CGG system through the Ethernet network, and the IRIG-B communication was implemented at the power meters and feeder relays. The SEL-421 protective relay transmitted IEC 61850 Sampled Values messages. The SEL-451 protective relays and SEL-735 power meters transmitted IEC 61850 GOOSE messages, and the SEL-734 power meters transmitted DNP3 messages. All these message types are frequently used by electrical utilities at substations. Table 1lists the location, IP address, type of device, protocols, Ethernet port, and functions of devices installed on the test bed provided by an electrical substation grid with a customer-owned DER (wind farm) and the CGG system.

Table 1. Location, IP address, type of device, protocols, Ethernet port, and functions

Location	IP address (telnet port)	Type of device (device ID)	Protocols (messages)	Ethernet port	Functions
Inside electrical substation devices (utility A)	192.168.100.2 (23)	SEL-451 relay (SUB_SEL451 _FED1)	IEC 61850 GOOSE	5C	Measurement of currents, voltages, real and reactive three-phase power, frequency, and pole states at substation breaker feeders
	192.168.100.3 (23)	SEL-451 relay (SUB_SEL451 _FED2)	IEC 61850 GOOSE	5C	Measurement of currents, voltages, real and reactive three-phase power, frequency, and pole states at substation breaker feeders
	192.168.100.12 (23)	SEL-421 relay (SUB_SEL421 _SV)	IEC 61850 Sampled Values	5C	Measurement of currents and voltages
Outside electrical substation devices (utility A)	192.168.100.8 (23)	SEL-735 meter (SUB_SEL735 _FED1)	IEC 61850 GOOSE	1	Measurement of currents, voltages, real and reactive three-phase power, and frequency at load feeder 1 with 100 T fuses
	192.168.100.10 (23)	SEL-735 meter (SUB_SEL735 _FED2)	IEC 61850 GOOSE	1	Measurement of currents, voltages, real and reactive three-phase power, and frequency at load feeder 2 with 100 T fuses
	192.168.100.4 (23)	SEL-734 meter (SUB_SEL734 _FED1)	DNP3	1	Measurement of currents, voltages, real and reactive three-phase power, and frequency at load feeder 1 with 50 T fuses
	192.168.100.6 (23)	SEL-734 meter (SUB_SEL734 _FED2)	DNP3	1	Measurement of currents, voltages, real and reactive three-phase power, and frequency at load feeder 2 with 50 T fuses
	192.168.100.22	SEL-3530-4 RTAC	DNP3	1	Poll for DNP3 points at SEL-734 power meters
Control center (utility A)	10.0.0.141	Cisco IE3400	—	—	Ethernet switch 1 for the DLT-5
	10.0.0.142	Cisco IE3400	—	—	Ethernet switch 2 for the DLT-6
	10.0.0.143	Cisco IE3400	—	—	Ethernet switch 3 for the DLT-7
	10.0.0.144	OnLogic MC850-40	—	—	DLT device DLT-5
	10.0.0.145	OnLogic MC850-40	—	—	DLT device DLT-6
	10.0.0.146	OnLogic MC850-40	—	—	DLT device DLT-7
Wind farm (utility C)	192.168.100.20 (23)	SEL-351S relay (WIND_FAR M2_SEL351S _FED1)	IEC 61850 GOOSE	5A	Measurement of currents, voltages, power, frequency, and pole states at wind farm 2 feeder

3.3 THREE-LINE DIAGRAM

The three-line diagram was created in an RT-LAB project by using MATLAB/Simulink models to run the tests with the real-time simulator and the IEDs in the loop. The electrical substation grid (utility A) with the customer-owned wind farms (utilities B and C) is shown in Figure 4. The electrical substation (utility A) was a 34.5/12.47 kV primary/secondary voltage power system, and the wind farms (utilities C and D) were on a 0.575/12.47 kV primary/secondary voltage power system. The wind farms had doubly fed induction generator wind turbines. The wind farms of utilities C and D comprised six 1.5 MW doubly fed induction generator wind turbines each (two wind farms totaling 9 MW each). Utility A had two 34.5/12.47 kV power transformers of 10 MVA connected in parallel and two-feeder breakers of 12.47 kV that were controlled by two SEL-451 protective relays in the loop. Thus, the phase currents and voltages were collected from the feeder breaker locations. Each feeder breaker was connected to a radial power grid, with two 12.47 kV power lines connected to the feeder loads. One power line had two power loads with 50 T fuses [22], and the other power line had two power loads with 100 T fuses [22]. The phase currents and voltages for the 50T fuses were measured with the SEL-734 power meters. However, phase currents and voltages for the 100T fuses were measured with the SEL-735 power meters. Figure 1 shows the fuses and power meters.

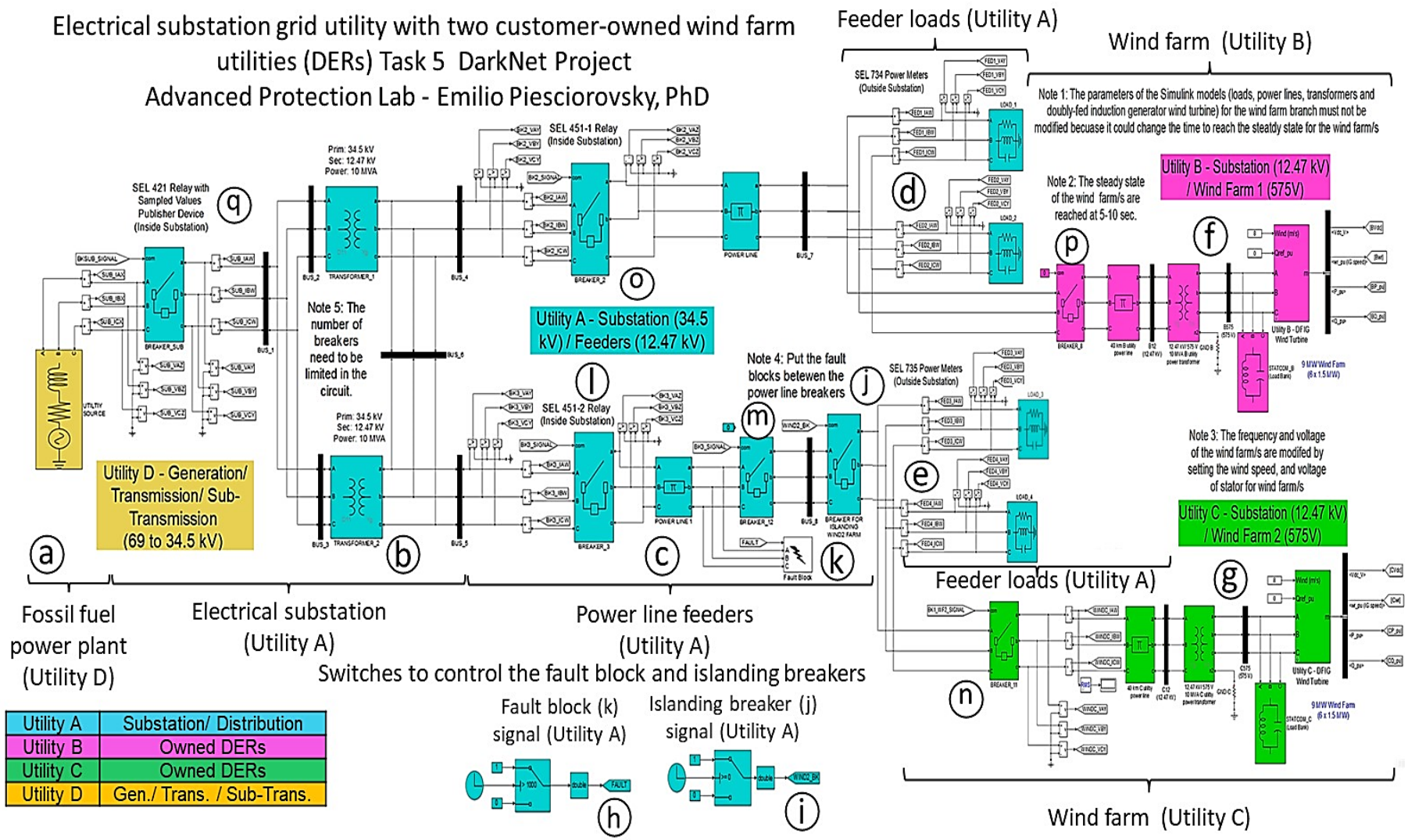

Figure 4. Three-line diagram of the electrical substation grid with customer-owned wind farms.

In Figure 4, the electrical substation grid (utility A) was connected to two DERs (utilities B and C). Utility D was represented by a fossil fuel power plant generator, transmission, and subtransmission block (Figure 4.a). Utility A consisted of the electrical substation (Figure 4.b), power line feeders (Figure 4.c), feeder loads (Figure 4.d and e), and wind farms (Figure 4.f and g). In Figure 4, the switches to control the fault block (Figure 4.h) and to operate the islanding breaker (Figure 4.i) were set before running the simulations. The breaker at the 34.5 kV side (Figure 4.q) was controlled by the SEL-421 relay, the substation feeder breakers (Figure 4.o and l) were controlled by the SEL-451 relays, and the wind farm two-feeder breaker (Figure 4.n) was controlled by the SEL-351S relay. In the load feeders (Figure 4.d and 4e), the phase voltages and currents were measured by the SEL-734 and SEL-735 power meters.

3.4 CGG SYSTEM

The CGG system is a modular software framework built on top of a data storage layer that is designed to enhance the security of electrical grid communications and device data. The modular design allows the software framework to provide diverse capabilities that can be adapted to various use cases, such as different network or communication architectures.

The CGG system architecture can be divided into two main layers, as shown in Figure 5. The data storage layer consists of an off-chain database for storing raw data and a DLT for storing cryptographic hashes. The DLT is used with a trust anchoring process, in which raw data are grouped into windows based on a period and then hashed and stored in the ledger. Using this hash reduces the amount of storage space and transaction processing required by the DLT while providing a fingerprint of the data that can be used to determine whether the data have been modified. Attestation checks are performed by rehashing the raw data and then comparing the result with the corresponding hash in the ledger. DLT features such as decentralization and tamper resistance are used to enhance the security of the collected data.

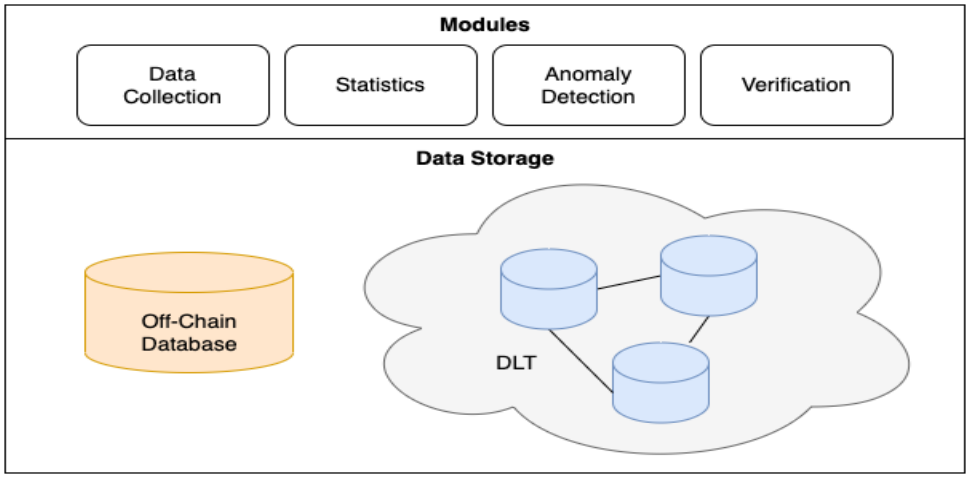

Figure 5. CGG system architecture layers.

The software modules layer of the framework provides functions that include data collection, statistics, anomaly detection, and verification. Collection of packet data from protocols such as IEC 61850 GOOSE and SV, DNP3, and Modbus is supported. Configuration artifacts and commands for IEDs are also gathered using protocols such as Telnet and File Transfer Protocol. Statistics modules generate additional statistical data based on packet payloads and network interarrival time stamps. Anomaly detection modules are used to detect cyber- or power system–related events by using the collected packets and statistics. Attestation checks are performed by using verification modules and can be triggered on periodic and random schedules or by the detection of anomalous events.

4. EXPERIMENTAL MODEL AND USE CASE SCENARIOS

In this section, the experimental model and scenarios for the electrical fault detection, power quality, DERs, and cyber event use case scenarios with a test bed using the CGG system with DLT are presented. The architecture of the CGG system based on the event, algorithm, and boundary flow diagrams is described, and the electrical fault/power quality boundary and algorithm flow diagrams are explained.

4.1 USE CASE SCENARIOS

The multipurpose electrical substation grid test bed with DLT was used to examine electrical fault detection, power quality monitoring, DER, and cyber event scenarios. These tests were performed on the feeder inside the red dashed rectangle in Figure 1.a. Table 2 lists the use case scenarios for the DLT applications on the electrical substation grid test bed.

Table 2. Use case scenarios for the DLT applications on the electrical substation grid test bed

Tests	Main situation	Test description (total simulation 100 s)
Fault detection*	LL electrical fault	The electrical fault for phase A and B located at the end of the distribution power line was set at 50 s, and the relay tripped the breaker.
Power quality*	SLG electrical fault with a nontripped breaker	The phase A to ground electrical fault at the end of the distribution power line was set at 20 s, and the relay's breaker did not trip because the trip signal circuit was disconnected (breaker failure).
DER†	Connection of grid (utility A) and wind farm (utility C) with a 3LG electrical fault at the distribution power line	The power grid (utility A) was connected with the wind farm (utility C), and a 3LG electrical fault located at the end of the distribution power line was set at 50 s. Then, the relay cleared the electrical fault, and the feeder loads were fed by the wind farm (utility C).
Cyber events*	Combined cyber event with a SLG electrical fault	The CT ratio setting of the SEL-451 relay was changed from 80 to 1 after 20 s, then a phase A to ground electrical fault located at the end of the distribution power line was set at 50 s.

*Tests without DERs (wind farms); SLG: single line to ground, LL: line to line.
†3LG: three line to ground.

The electrical fault detection test was based on identifying an overcurrent fault event. The power quality monitoring case test was based on monitoring the frequency, RMS phase voltages, and total power factor. The DER use case test was based on the connection of the power grid (utility A) and wind farm (utility C) with a three line to ground (3LG) electrical fault at the distribution power line. The cyber event test was based on a combined scenario performing an undesired relay setting with a 3LG electrical fault to study the relay's behavior and possible effect.

4.2 ARCHITECTURE AND FLOW DIAGRAMS

In this study, the architecture of the CGG system was based on the event, algorithm, and boundary flow diagrams. The event flow diagram was run in the test bed, and the algorithm flow diagrams were defined for each power system application. The boundary flow diagrams calculated the limits of the algorithms, which were performed externally. Figure 6 shows the integration of the flow diagrams for the architecture of the CGG system with DLT.

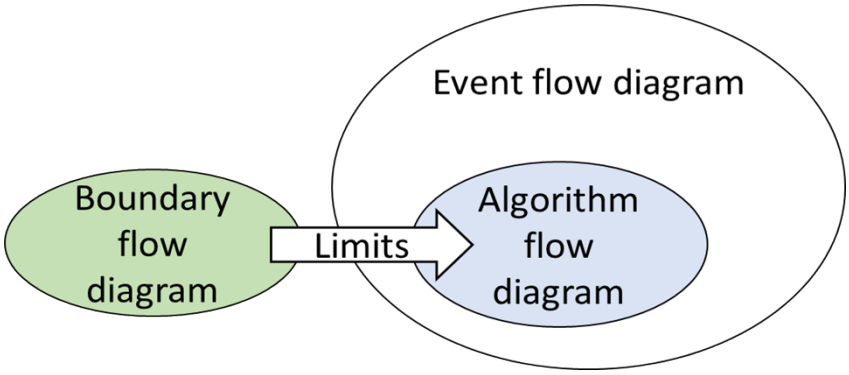

Figure 6. Architecture and flow diagrams.

4.3 EVENT FLOW DIAGRAM

In the CGG system, the DLT was used in the implementation of the monitoring systems. The DLT is a platform that uses ledgers stored on separate, connected devices in a network to ensure data accuracy and security. The three features of the DLT are the distributed nature of the ledger, the consensus mechanism, and the cryptographic mechanisms. Based on this platform, the event flow diagram (Figure 7) for the event detection module was implemented in the Python module powersys_event_detect.py of the CGG framework.

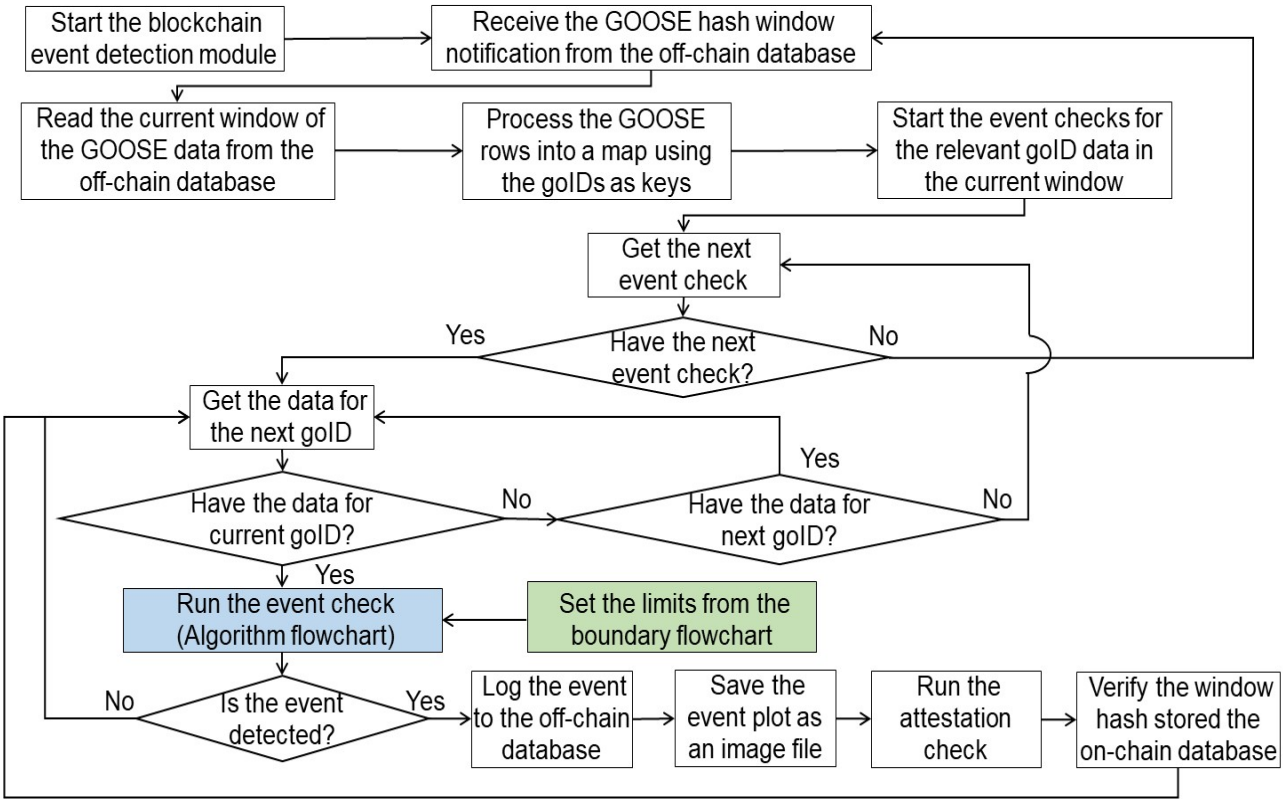

Figure 7. Event flow diagram.

The event detection module receives data by subscribing to notifications from the off-chain database about new windows of IEC 61850 GOOSE packets that were collected from the network and then stored. Each window has a corresponding SHA256 hash, which is stored in the Hyperledger Fabric DLT to

provide trust anchoring of the GOOSE data. The event detection module uses the psycopg2 library to read data from the off-chain database and standard Python libraries, and it functions to structure and check the windows of GOOSE packet data for events. First, the rows of data queried from the database are transformed into a dictionary. Each row of data represents a GOOSE packet and consists of the GOOSE device ID (goID), time stamp, and data set values. Table 3 describes the specific data set values used for checking events.

Table 3. GOOSE data set fields used in event checks

Field name	Value (unit)
magVoltagePhaseA	10-cycle average fundamental phase A voltage magnitude (V)
magVoltagePhaseB	10-cycle average fundamental phase B voltage magnitude (V)
magVoltagePhaseC	10-cycle average fundamental phase C voltage magnitude (V)
magCurrentPhaseA	10-cycle average fundamental phase A current magnitude (A)
magCurrentPhaseB	10-cycle average fundamental phase B current magnitude (A)
magCurrentPhaseC	10-cycle average fundamental phase C current magnitude (A)
magFreqHz	Measured system frequency (Hz)
magTotW	Fundamental real three-phase power (W)
magTotVAr	Fundamental reactive three-phase power (VAR)

The dictionary maps each goID to its list of rows in the current window. The GOOSE data set fields can vary by goID. The event checks are defined as tuples within a list. Each tuple contains the check label, a function to perform the check on the relevant GOOSE data set values, the check description/details string, and the event duration threshold. Each check function returns a Boolean value representing whether the GOOSE value(s) given as argument(s) represent an event (using true) or not (using false). For example, a particular check function (e.g., electrical fault detection algorithm) might check whether values of the phase current magnitude fields are greater than the current magnitude threshold value (200 A) based on Eq. (1), resulting in a true event for that value and returning the result. The event state is maintained for each goID and event check to determine when events start and stop. The event duration threshold interval is used to filter out events that do not meet the minimum duration, using a default duration of 60 s. The valid events are logged and inserted into the off-chain database and can be saved automatically as event plot image files using the Pandas, matplotlib, and Seaborn libraries. This logging is handled by a separate event plotter class that maintains custom plot settings per event check, such as *y*-limits and threshold annotations. These plots can be used to quickly analyze detected events using visual inspection. Finally, valid events trigger an attestation check of GOOSE data by comparing hashes of the current off-chain

GOOSE data with those in the ledger. In Figure 7, the blue and green blocks were set according to the power system application within the event flow diagram.

4.4 ELECTRICAL FAULT BOUNDARY AND ALGORITHM FLOW DIAGRAMS

The electrical fault boundary algorithm was created to detect the electrical faults in the power system implemented in the electrical substation grid test bed. The algorithm was based on (1) finding the range between the minimum RMS fault current and maximum load RMS current to detect the overcurrent electrical faults; (2) setting the single line to ground (SLG), line to line ground (LLG), line to line (LL), and 3LG electrical faults in the test bed to measure all electrical fault RMS currents; (3) finding the minimum electrical fault RMS current, which was calculated by implementing a power flow simulation on the electrical substation grid test bed to detect the maximum load RMS current; (4) setting the threshold value to detect the electrical faults with a value between the 1.3 × $I_{RMS\ MAX\ LOAD}$ (the maximum load RMS current) and the $I_{RMS\ MIN\ FAULT}$ (the minimum electrical fault RMS current); and (5) calculating the RMS current threshold (I_{THR}) to set the algorithm and detect the faulted phases in the electrical substation relay feeder. The electrical fault boundary (Figure 8.a) and algorithm (Figure 8.b) flow diagrams are shown here.

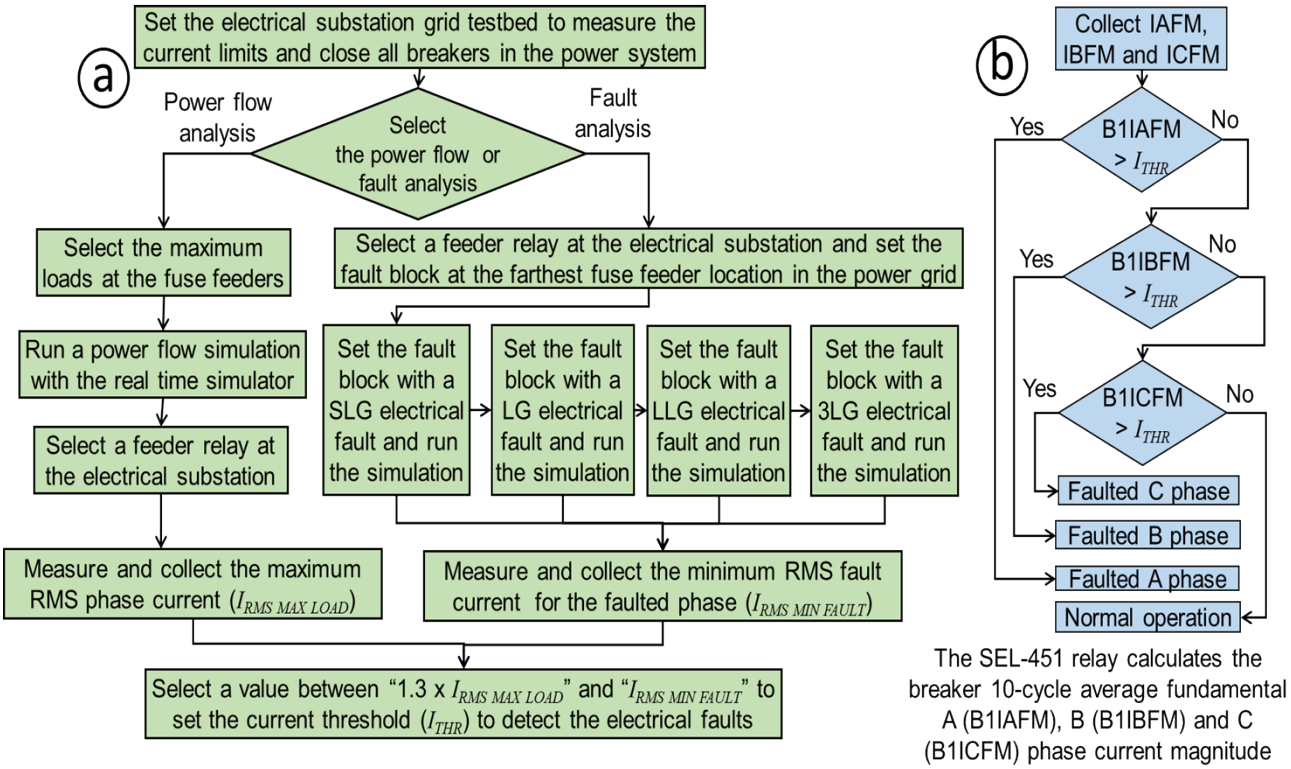

Figure 8. (a) Electrical fault boundary and (b) algorithm flow diagrams.

Based on the electrical substation grid test bed [14], the SEL-451 relays located at the electrical substation feeders had a maximum load current between 70 and 140 A, and the minimum electrical fault current was 751 A (SLG electrical fault). From Figure 8, the selected RMS current threshold was 200 A to set the algorithm for detecting the overcurrent electrical fault events.

4.5 POWER QUALITY BOUNDARY AND ALGORITHM FLOW DIAGRAMS

In the power quality application, the boundary flow diagram defines the limits for the algorithm flow diagram. Figure 9 shows the boundary flow diagrams for the power quality algorithm. This boundary flow diagram helps to calculate the voltage (Figure 9.a), frequency (Figure 9.b), and power factor (Figure 9.Figure 9c) limits. The voltage limits (Figure 9.a) were calculated based on the ANSI C84.1 Standard [23]. The voltage limits depend on the nominal voltage level and the non-load or user load site location of the selected IED.

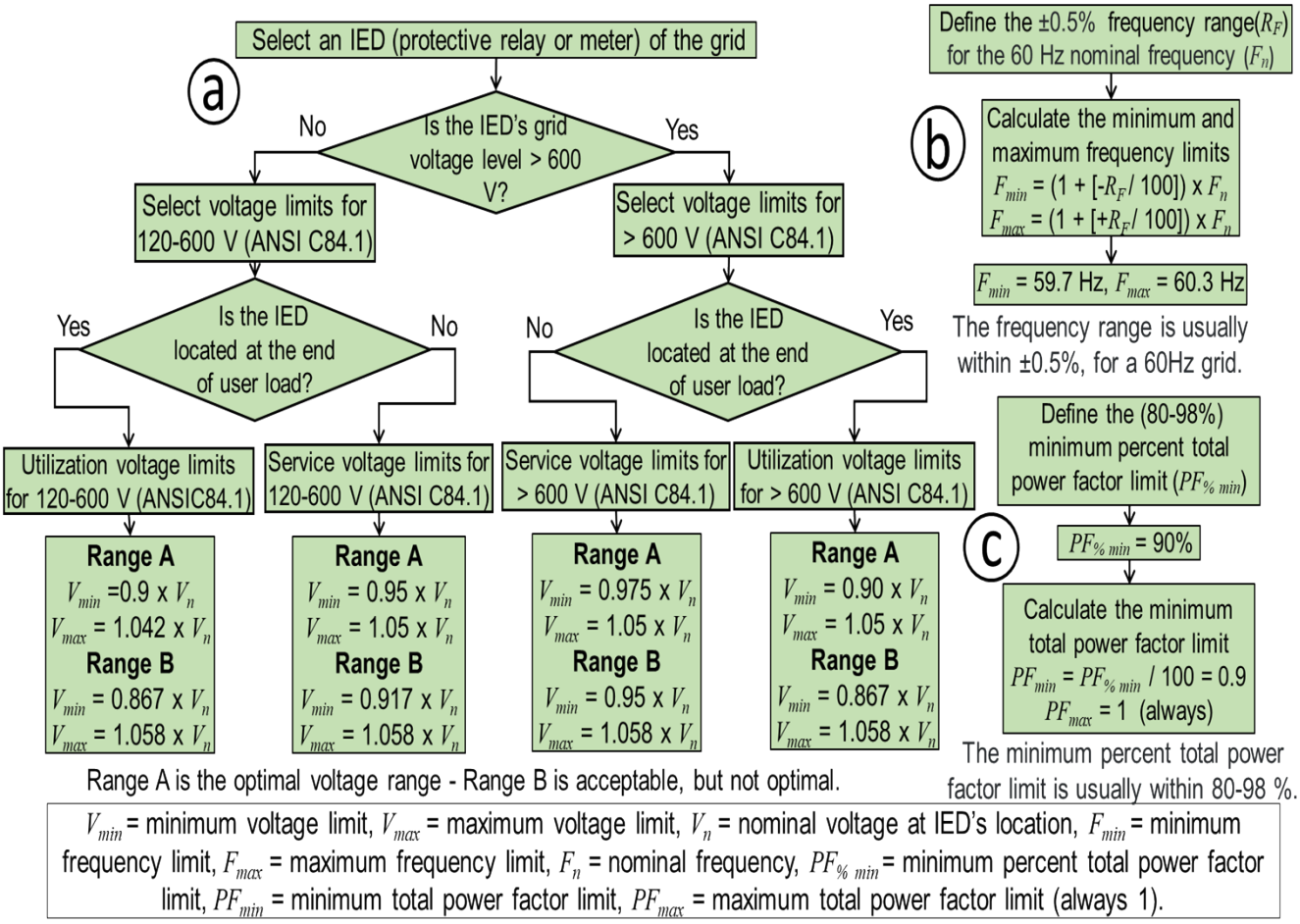

Figure 9. (a) Voltage, (b) frequency and (c) total power factor boundary flow diagrams.

In this study, the IED was a SEL-451 relay that was not located on a user load site. Then, the range B of the ANSI C84.1 service voltage limits was selected. The minimum voltage was set to 95%, and the maximum voltage was set to 105.8%. The undervoltage limit was set to 6.84 kV, and the overvoltage limit was set to 7.62 kV. For a 60 Hz electrical grid, the frequency limits (Figure 9.b) were calculated within a range of ±0.5% [24], obtaining a minimum frequency of 59.7 Hz and a maximum frequency of 60.3 Hz. For the total power factor measured as a percentage, the maximum percent total power factor was 100%, and the minimum percent total power factor limit was usually between 80% and 98% [25]. The minimum power factor was 0.9 (90%), and the maximum power factor was 1 (100%) (Figure 9.c).The power quality algorithm is shown in Figure 10. The calculated limits for the voltages, frequency, and total power factor were used in Figure 10. These power quality algorithm flow diagrams show how ethe power quality normal and abnormal situations were calculated.

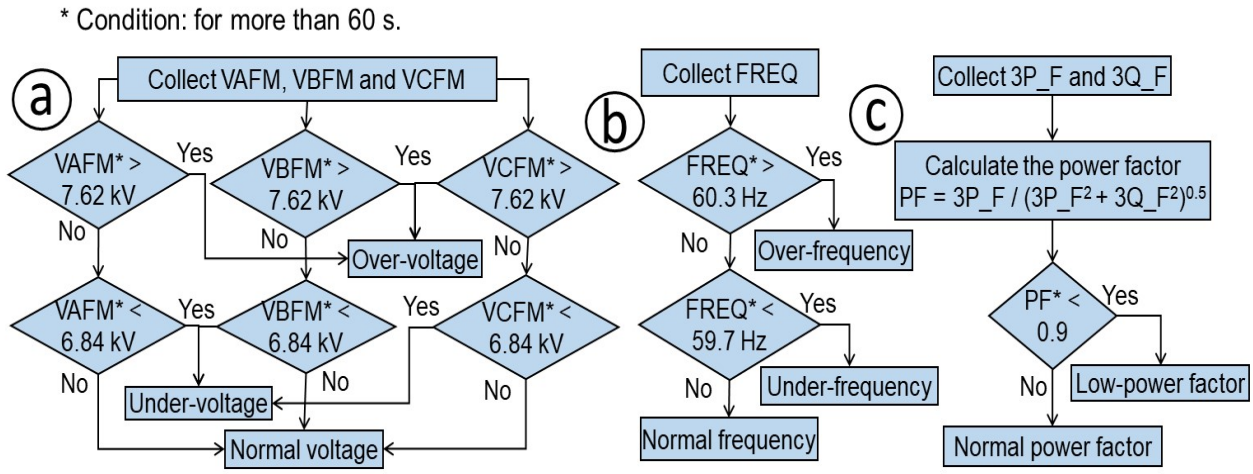

Figure 10. (a) Voltage, (b) frequency and (c) total power factor algorithm flow diagrams.

Overvoltage occurred when the nominal voltage rose above 105.8% for more than 1 min, and undervoltage occurred when the nominal voltage dropped below 95% for more than 1 min. The frequency range was usually held within ±0.5% of 60 Hz, so the measured range frequency should have been between 59.7 and 60.3 Hz. Overfrequency occurred when the frequency dropped below 59.7 Hz for more than 1 min, and underfrequency occurred when the frequency rose above 60.3 Hz for more than 1 min. The measurement of the total power factor was based on using a range between 0.9 and 1. A low power factor occurred when it dropped below 0.9 for more than 1 min. The low power factor decreases when some inductive loads like electrical induction motors, synchronous motors, power transformers or welding transformers are connected to the electrical grid. However, a high-power factor represented by 1 is always given by a pure resistive load like incandescent lighting systems or electrical heaters.

5. RESULTS

In this section, the test results for the electrical fault detection, power quality, DER, and cyber event use case scenarios are presented. The analysis of the test results is based on comparing the time-stamped events of the analog signals from the power meters and protective relays and the digital signals from breaker states for the prefault, fault, and postfault states. These events were collected during the experiments from the protective relays, DLT computer, and real-time simulator to be analyzed in detail according to the use case scenario descriptions.

5.1 ELECTRICAL FAULT DETECTION

An LL electrical fault was simulated, and the algorithm (Figure 8.b) detected this anomaly situation by predicting the fault currents within the established limits for detecting the electrical faults. The CGG system communications successfully conveyed the protective relay information and current status. The electrical fault detection was based on performing an electrical fault test. In this case, the electrical fault boundary and algorithm flow diagrams (Figure 8) with the event flow diagrams (Figure 7) were used. The electrical fault test was represented by an LL electrical fault at the SEL-735 power meter feeder based on the circuit inside the red dashed rectangle in Figure 1.a but without the wind farm feeder. Figure 11 shows the simulated phase currents, voltages, and pole states for the SEL-451 relay and SEL-735 power meters in the electrical fault detection test.

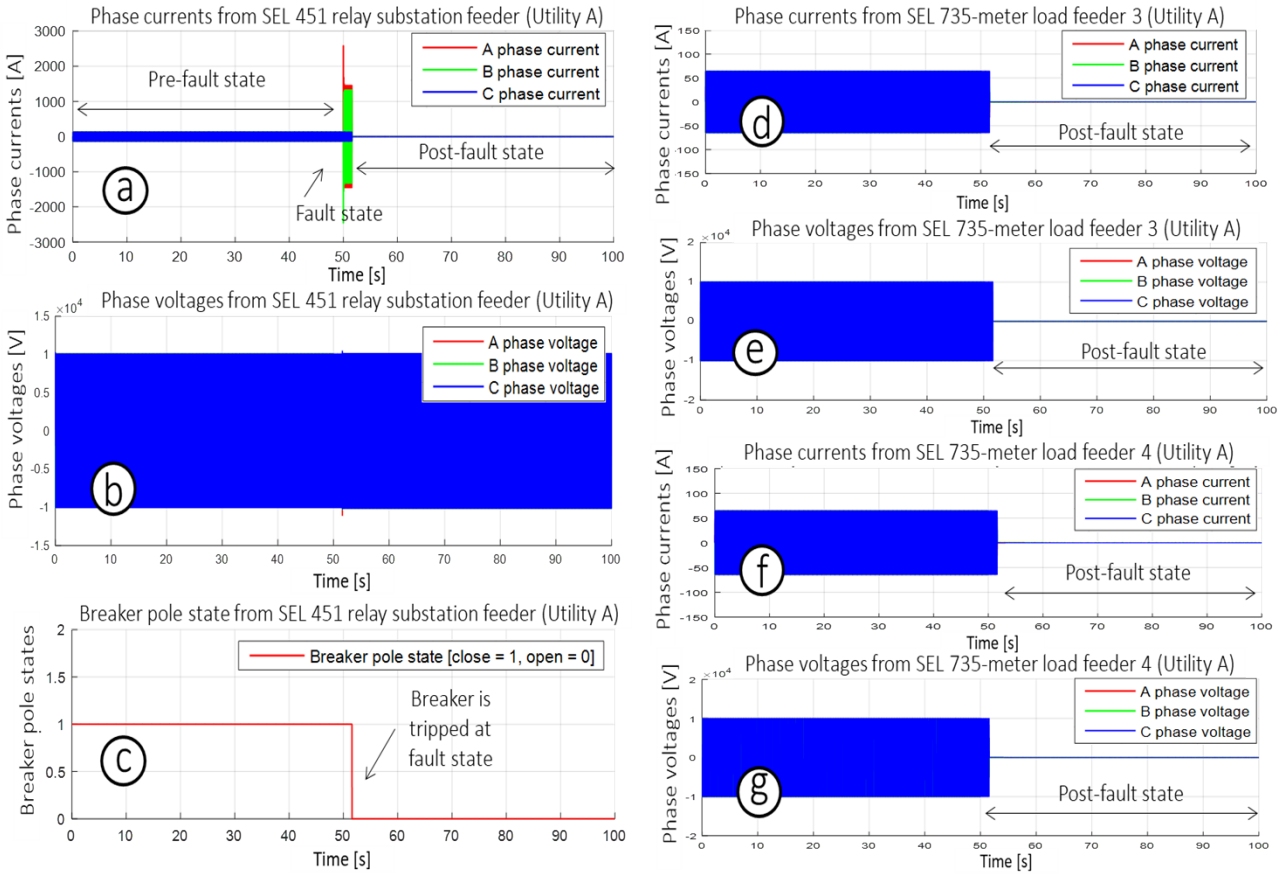

Figure 11. (a, d, f) Simulated phase currents, (b, e, g) voltages, and (c) pole states for the SEL-451 relay and SEL-735 power meters for the electrical fault detection test.

The RMS phase currents and voltages from the SEL-451 relay and SEL-735 power meters (GOOSE messages) were collected from the CGG computer system, as shown in Figure 12. During this LL electrical fault, the CGG system observed a significant increase in the currents of phases A and B for the SUB_SEL451_FED2 relay, and a threshold of 200 A (red dashed line) was used to detect the overcurrent electrical fault events (Figure 12.a). Once the phase A and B currents increased at the fault state (Figure 12.a), the CGG system computer detected the electrical fault, but the SEL-451 relay also detected the electrical fault and tripped the breaker by clearing the electrical fault. The LL electrical fault was cleared at the postfault state, and the RMS phase currents dropped to zero at the power line and load feeders (Figure 12.a, b, and c). Additionally, the SEL-735 power meters showed that the phase voltages (Figure 12.e and f) dropped to zero because the fault was cleared.

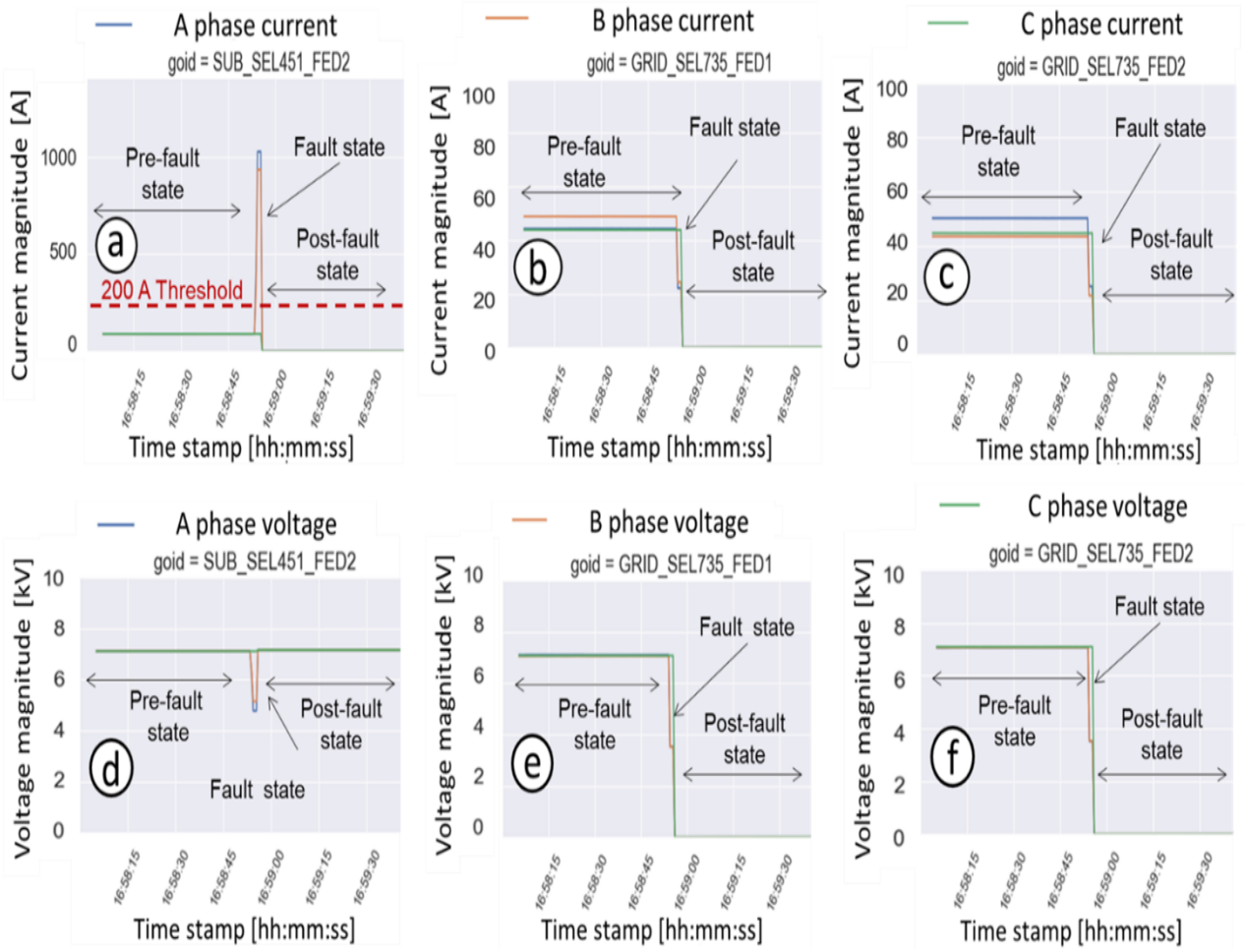

Figure 12. CGG system (a, b, c) phase RMS currents and (d, e, f) voltages of the SEL-451 relay and SEL-735 power meters for the electrical fault detection test.

Figure 13 shows the phase currents and voltages of the SEL-451 relay for the electrical fault detection test. After running the test, the event from the relay was collected to observe just one time stamp, phase currents, and voltages from the relay (Figure 13) that were matched with the time stamp, phase voltages, and currents collected from the DLT system (Figure 12.a and d). The same time stamp for the events from the relay and the DLT system proved the synchronization of the data managed with the DLT algorithms using a blockchain.

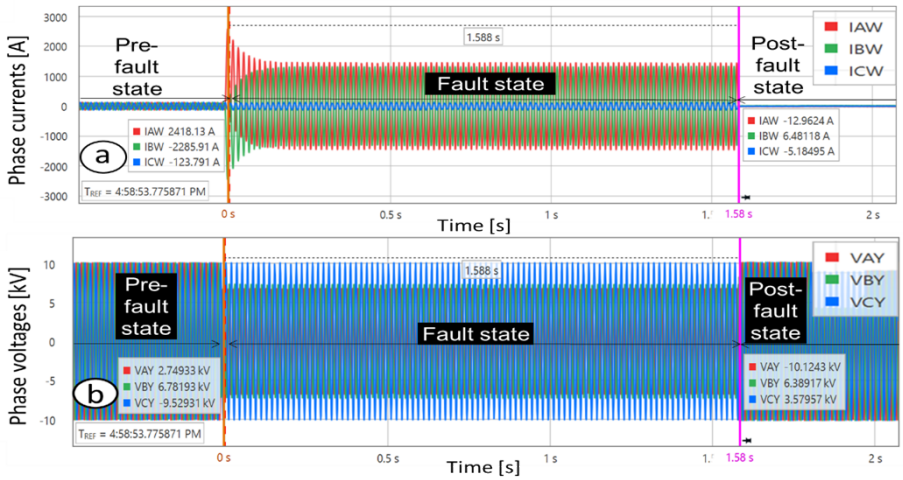

Figure 13. (a) Phase currents and (b) voltages of the SEL-451 relay for the electrical fault detection test.

5.2 POWER QUALITY MONITORING

A power quality monitoring situation was simulated, and the CGG system compared the measured voltages, frequency, and total power factor with the power quality limits by predicting the power quality situation for the electrical substation main feeder. The CGG system communications successfully conveyed the protective relay measurements. The power quality monitoring was based on performing an electrical fault with a nontripped breaker test to assess the power quality boundary (Figure 9) and algorithm (Figure 10) flow diagrams with the event flow diagram (Figure 7).

The electrical fault test was represented by an SLG electrical fault at the SEL-735 power meter feeder based on the circuit inside the red dashed rectangle in Figure 1.a but without the wind farm feeder branch. The phase A to ground electrical fault at the end of the distribution power line was set to 20 s, and the relay's breaker did not trip because the trip signal circuit was disconnected (breaker failure). This test was based on a simulation of 100 s to compare the frequency, phase voltages, and power factor within their limits for the power quality during a period greater than 60 s. Figure 14.a and c show the simulated frequency, phase voltages, and power factors for the SEL-451 relay.

The frequency, RMS phase voltages, and total power factor from the SEL-451 relay (GOOSE messages) were collected from the DLT computer system, as shown in Figure 14.d, e, f, g, and h. During the SLG electrical fault, the CGG system master node observed a significant decrease in the voltage of phase A (Figure 14.e) and total power factor (Figure 14.h) for the SUB_SEL451_FED2 relay. The voltage of the faulted phase (phase A) was below the undervoltage limit of 6.84 kV (red dashed line) in Figure 14.e, and the total power factor was below the minimum power factor limit of 0.9 (red dashed line) in Figure 14.h.

After running the test, the event data from the relay were collected to observe just one time stamp, phase currents, and voltages from the relay (Figure 15). The time stamp from the relay event matched the time stamp of the events collected from the CGG computer system (Figure 14.d, e, f, g, and h). The same time stamp for the events from the relay and the CGG system proved the synchronization of the data managed with the algorithms using a blockchain.

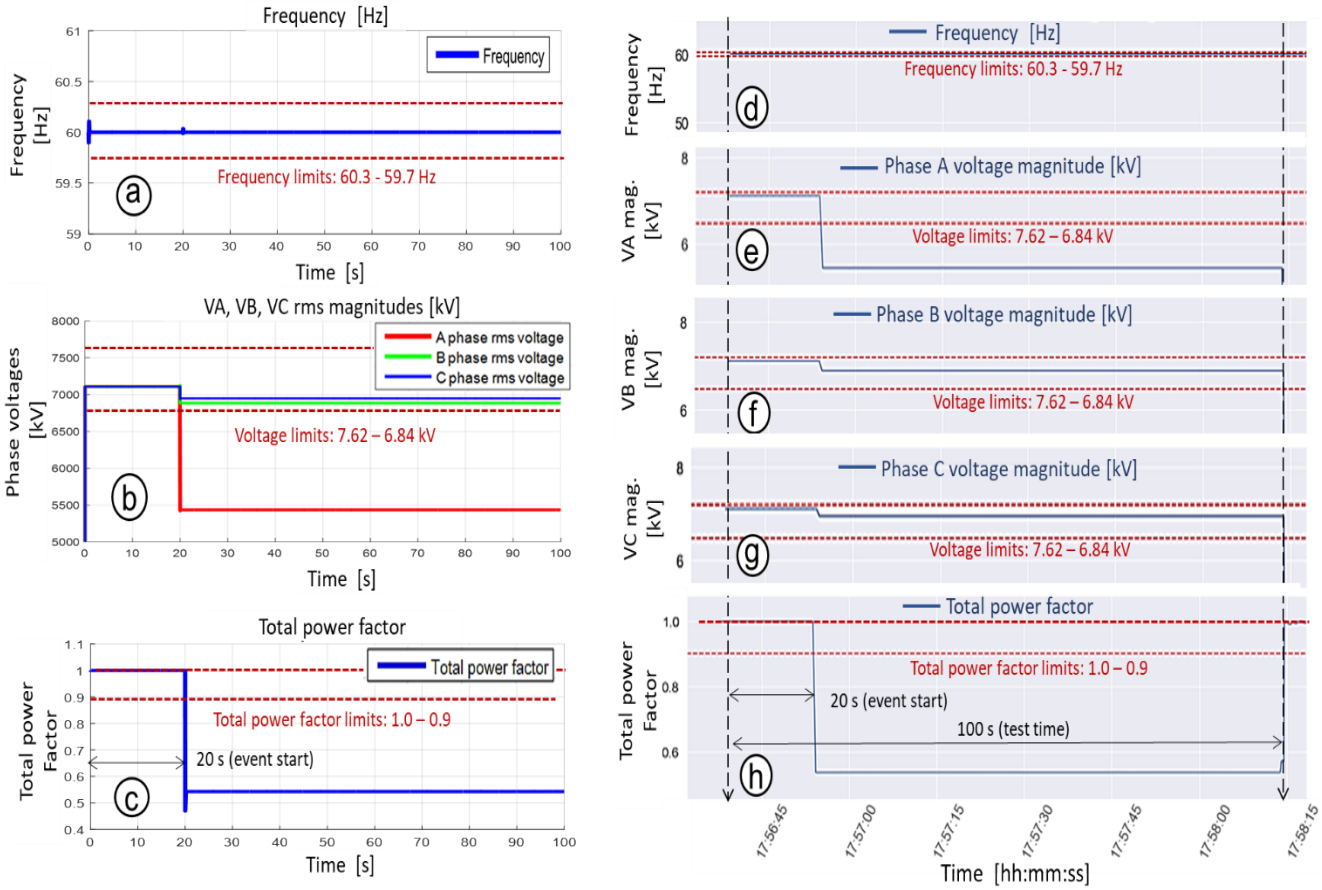

Figure 14. (a–c) Simulated and (d–h) measured CGG system frequency, phase RMS voltages, and total power factor of the SEL-451 relay for the power quality test of electrical fault without tripping.

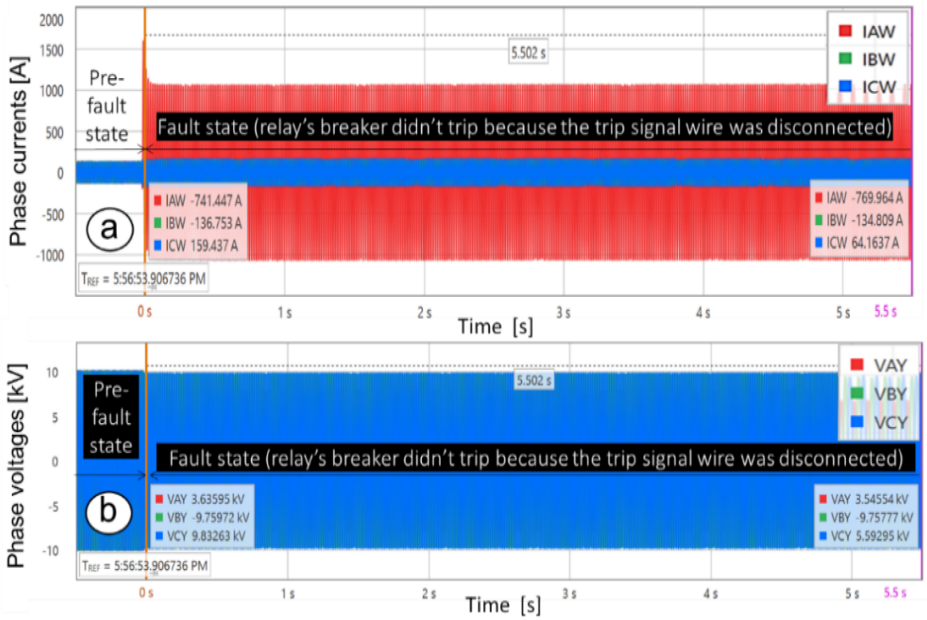

Figure 15. (a) Phase currents and (b) voltages of the SEL-451 relay event for the power quality test of electrical fault without tripping the breaker.

5.3 DER USE CASE MONITORING

A DER use case monitoring situation with an electrical fault was simulated, and the CGG system measured the voltages and currents by predicting the islanding of the customer-owned DERs (wind farm) in the electrical grid. The CGG system communications successfully conveyed the current information of the relay and power meters. The DER use case monitoring was based on simulating the connection of the grid and wind farm during an electrical fault to assess the measurements of the wind farm feeder relay (utility C) and electrical substation relay and load feeder power meters (utility A). Figure 16 shows the simulated phase currents, voltages, and pole states for the SEL-451/SEL-351 relays and SEL-735 power meters during the connection of the grid and wind farm with an electrical fault test.

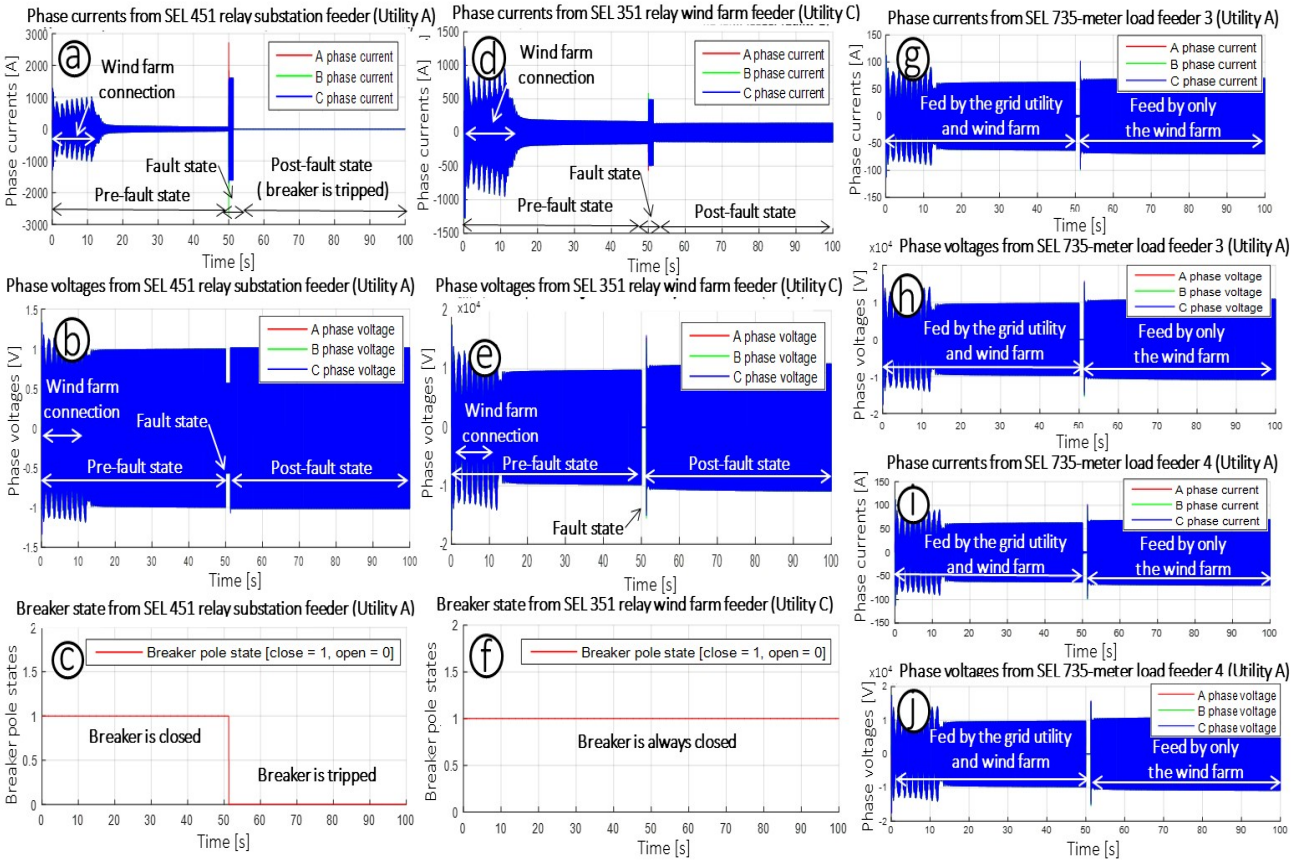

Figure 16. (a, d, g, i) Simulated phase currents, (b, e, h, j) voltages, and (c, f) pole states for the SEL-451/SEL-351 relays and SEL-735 power meters for the connection of the grid and wind farm with an electrical fault test.

The electrical fault test was represented by a 3LG electrical fault at the end of the distribution power line based on the circuit inside the red dashed rectangle in Figure 1.a with the wind farm (utility C) feeder connected. The 3LG electrical fault at the end of the distribution power line was set at 50 s, and the SEL-451 relay tripped the breakers at both sides of the distribution power line. This test was based on a simulation of 100 s; the connection of the grid and wind farm with an electrical fault test was based on assessing the DER use case scenario with the CGG system. Before running this simulation, the time switch (Figure 4.h) to control the fault block (Figure 4.k) was set at 50 s, and the time switch (Figure 4.i) to control the islanding breaker (Figure 4.j) was set at 0 s. Initially, the electrical substation (utility A) and wind farm (utility C) were connected to the load feeders. The 3LG electrical fault was cleared by the

SEL-451 relay after 50 s, and the feeder loads of the SEL-735 power meters were only fed by the wind farm (utility C).

The RMS phase currents and voltages from the SEL-451/SEL-351 relays and SEL-735 power meters (GOOSE messages) were collected from the CGG system computer, as shown in Figure 17. During the 3LG electrical fault, the CGG system master node observed a significant increase in the currents of phases A, B, and C for the SUB_SEL451_FED2 relay (Figure 17.a). Once the A, B, and C phase currents increased at the fault state (Figure 17.a), the SEL-451 relay detected the electrical fault and tripped the breakers at both sides of the power line by clearing the electrical fault. The RMS phase currents and voltages for the SEL-451 relay (utility A) are shown in Figure 17.a and b, and the RMS phase currents and voltages for the SEL-351S relay (utility C) are presented in Figure 17.c and d.

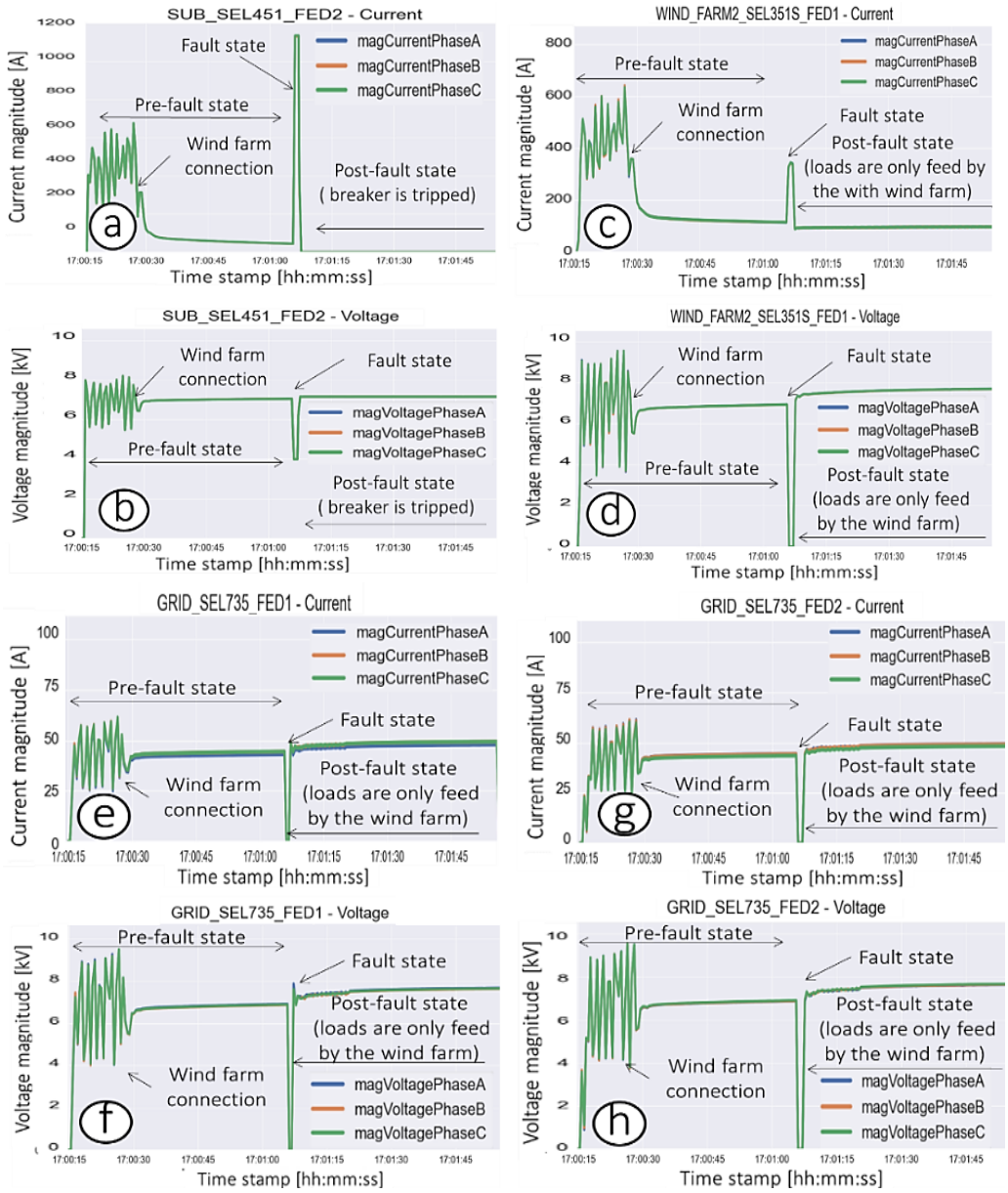

Figure 17. CGG system (a, c, e, g) RMS phase currents and (b, d, f, h) voltages from the SEL-451/SEL-351 relays and SEL-735 power meters for the connection of the grid and wind farm with an electrical fault test.

The RMS phase currents and voltages from the load feeders for the SEL-735 power meters are plotted in Figure 17.e and h. The transient state (approximately 10 s) to connect the wind farm was also observed, as shown in Figure 17. During the 3LG electrical fault, the SEL-451 relay cleared the electrical fault, and the RMS phase currents dropped to zero at the postfault state (Figure 17.a). Then, after clearing the electrical fault, the SEL-735 power meter loads were only fed by the wind farm feeder (utility C), as shown in Figure 17.e and g. The phase currents flowing through the breaker were controlled by the SEL-351S relay (Figure 17.c) because this breaker was kept closed. After the test, the event from the relay was collected to observe just one time stamp, phase currents, and voltages from the SEL-451 relay (Figure 18). The phase currents, voltages, and time stamp from the relay event matched those of the events collected from the CGG system computer (Figure 17). The same time stamp for the events from the protective relay and the CGG system proved the synchronization of the data managed with the algorithms.

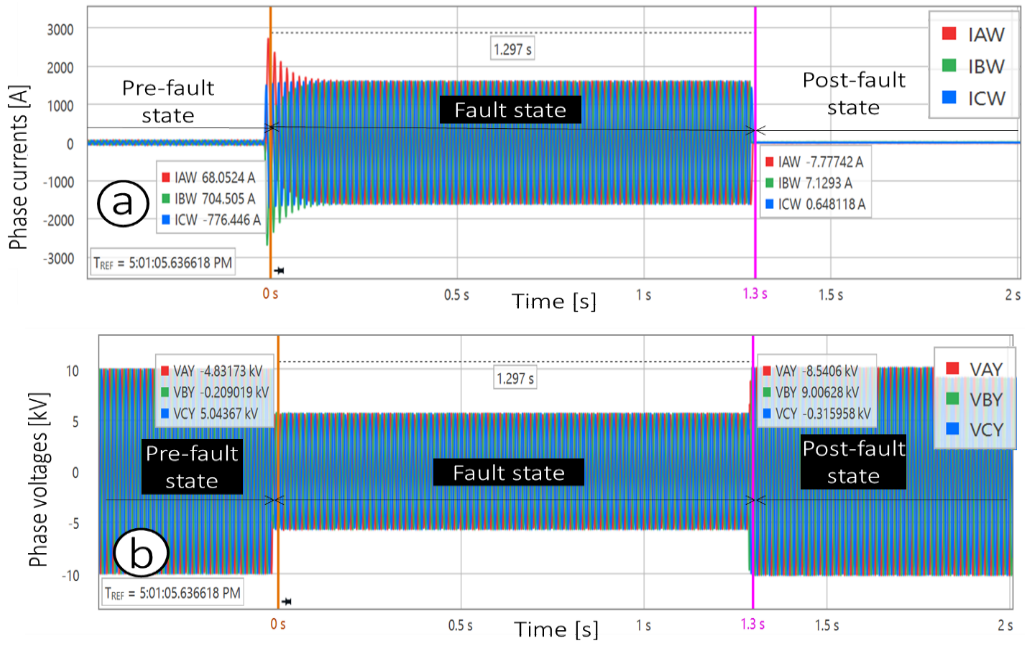

Figure 18. (a) Phase currents and (b) voltages for the SEL-451 relay event for the connection of the grid and wind farm with an electrical fault test.

5.4 CYBER EVENT MONITORING

A cyber event monitoring situation was simulated, and the CGG system measured the voltages and currents from the relay and power meters. The CGG communications successfully conveyed the relay and power meter information and current status. The cyber event monitoring test was based on detecting relay setting changes by monitoring the SEL-451 relay with the CGG system and studying the relay's behavior in cyber events.

The electrical fault test was represented by an SLG electrical fault at the end of the distribution power line based on the circuit inside the red dashed rectangle in Figure 1.a but without the wind farm feeder. In this case, the test was based on a combined cyber and electrical fault event. The test was represented by phase A to ground electrical fault at the 100 T fuse feeder, and the cyber event was the change of the CT ratio setting for the SEL-451 relay. The test was based on a simulation of 100 s, and the SLG electrical fault was set at 50 s. Figure 19 shows the simulated phase currents, voltages, and pole states of the SEL-451 relay and SEL-735 power meters for the combined cyber event and electrical fault test.

The RMS phase currents and voltages from the SEL-451 relay and SEL-735 power meters (GOOSE messages) were collected from the CGG computer system, as shown in Figure 20. Before the application of the SLG electrical fault, the CT ratio of the SUB_SEL451_FED2 relay was changed from 80 to 1. From the CGG system, the measured RMS phase currents decreased drastically (Figure 20.a) at the prefault state. The electrical fault affecting phase A was performed at 50 s, and the CGG system observed a nonsignificant increase in the current of phase A for the SEL-45 relay (Figure 20.a) at the fault state. This situation occurred because the CT ratio of the SEL-451 relay was modified. However, the relay tripped the breaker because the relay time for the SEL-451 relay did not depend on the CT ratio setting. The relay tripping behavior was based on Eq. (8) instead of Eq. (9). Once the phase A current increased at the fault state, the SEL-451 relay detected it and tripped the breaker. Then, the RMS phase currents from the relay dropped to zero at the postfault state (Figure 20.a). The nominal phase voltages from the relay were measured at the postfault state (Figure 20.d). Additionally, the CGG system enabled the assessment of the RMS phase currents and voltages for the SEL-735 power meters (Figure 20.b, c, e, and f).

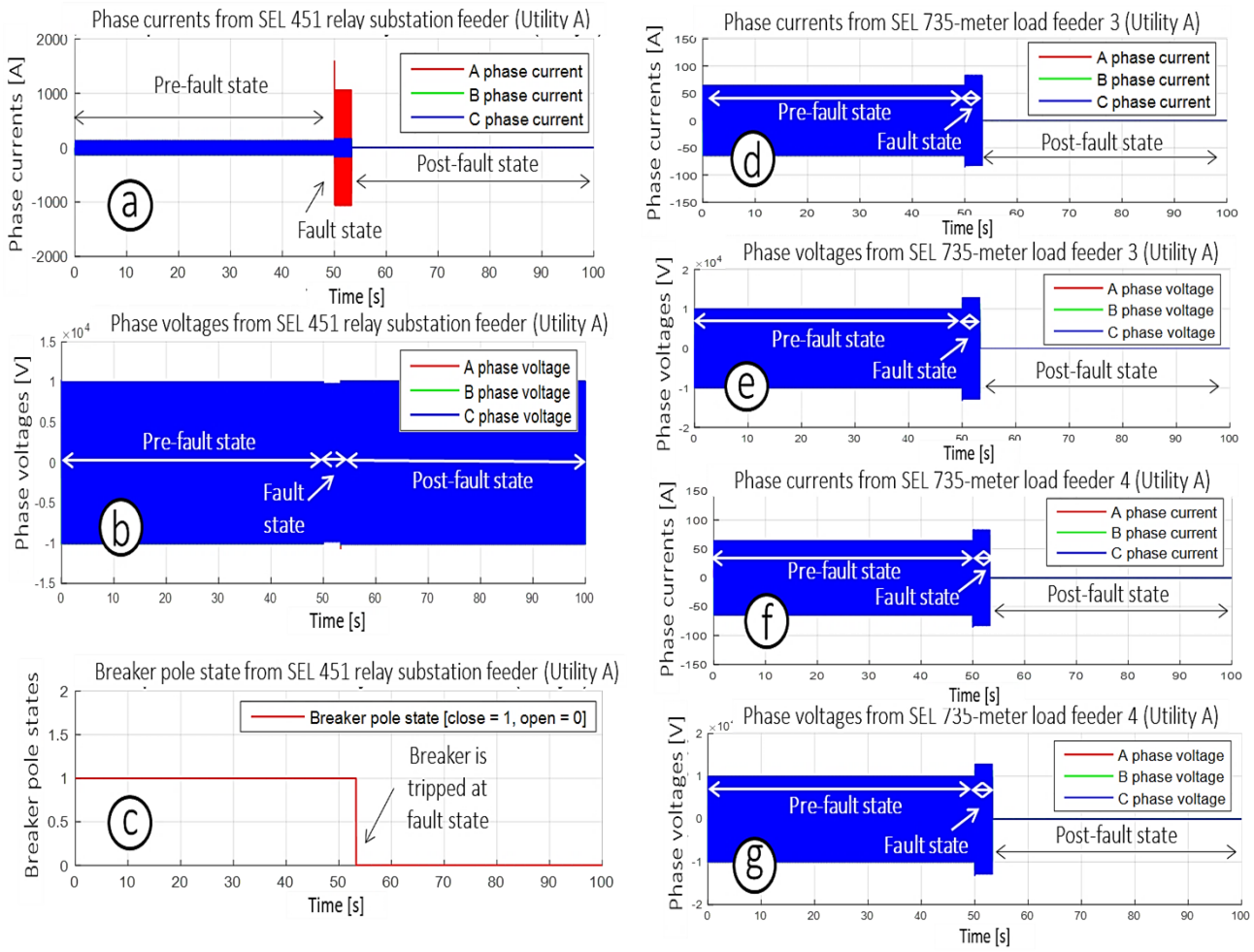

Figure 19. (a, d, f) Simulated phase currents, (b, e, g) voltages, and (c) pole states of SEL-451 relay and SEL-735 power meters for the combined CT ratio setting change with an electrical fault test.

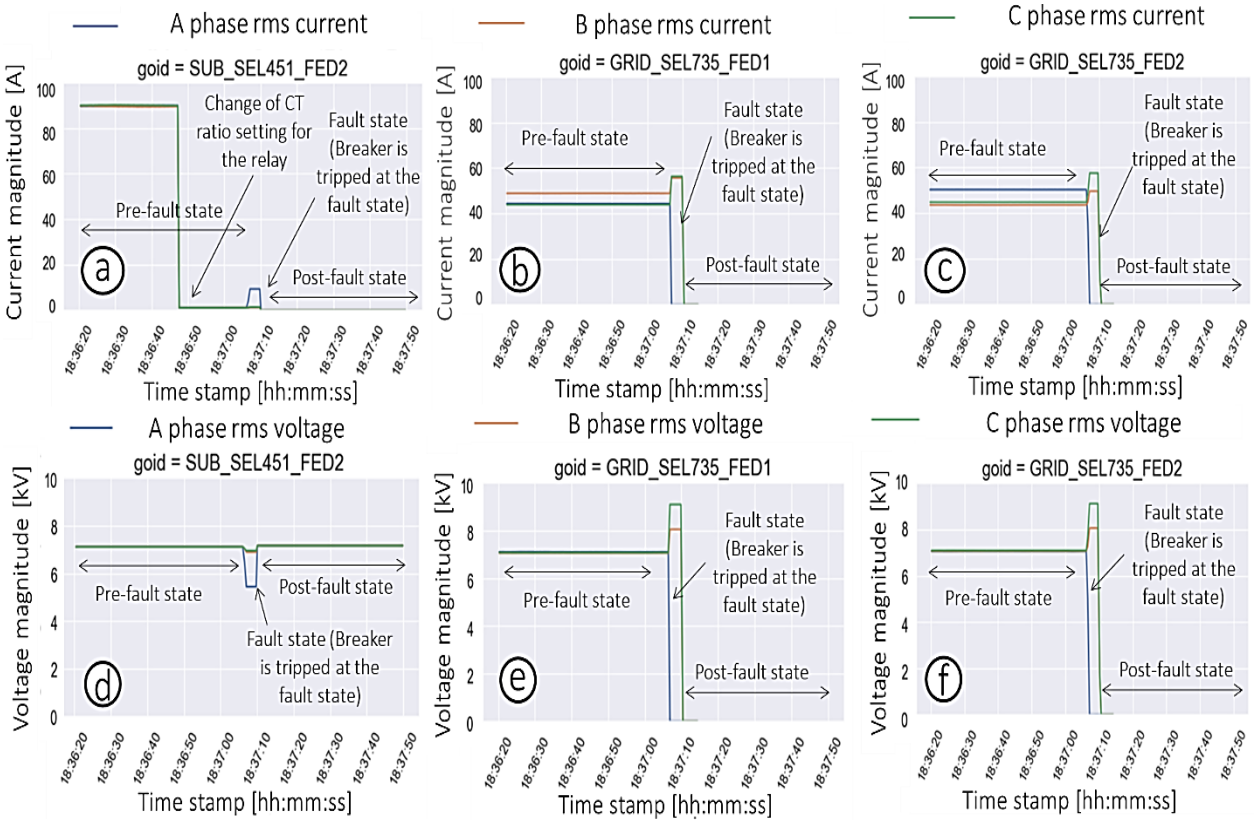

Figure 20. CGG system (a–c) phase RMS currents and (d–f) voltages from the SEL-451 relay.

6. DISCUSSION

In this section, the test results of the electrical fault detection, power quality, DER, and cyber event use case scenarios are discussed. The plots from the previous section are evaluated and discussed. The implementation of DLT in the electrical fault detection algorithm is discussed and compared with other protection functions that could trigger the breakers using protective relays. The power quality monitoring based on measuring the phase voltage magnitudes, frequency levels, and load power factor for more than 1 min is discussed. The DER use case scenario based on monitoring the connection of the electrical grid and wind farm with an electrical fault at the distribution power line is discussed. Finally, the monitoring of the combined cyber event with an electrical fault by using an incorrect CT ratio value is discussed, analyzing how it could affect the behavior of the protective relay's measurement and protection functions.

6.1 ANALYSIS OF USE CASE SCENARIOS

The CGG system monitored the overcurrent electrical fault detection test satisfactorily. However, in terms of DLT, the transaction latency that represents the time it takes for a sent transaction to be available for query from the ledger is crucial. Additionally, the time could be affected by variables that are specific to certain configurations, such as the target throughput given by transactions per second. The DLT is capable of low latency—less than 1,000 ms for 10 transactions per second [26]—but would still not be appropriate for power system protection functions to trip breakers at fault states because the transfer time for the trip command in GOOSE messages must be 3 ms [27]. Even if the CGG system could meet this timing requirement, not enough time would be left to account for other computational overhead (e.g., preparing transaction, network jitter). Therefore, the CGG system could be used for detecting electrical faults but not for tripping the breakers at the fault states. Protective relays usually use their internal settings to trip the breakers without supervision.

The CGG system monitored the frequency, phase voltages, and power factor. The power quality test was satisfactorily performed. Because the RMS phase voltages must be measured for at least 60 s for power quality monitoring [28], the communications delay time or latency [26] should not affect the power quality monitoring, and the CGG system could satisfactorily perform this function. Additionally, frequency monitoring in load shedding, wind farms, and capacitor bank applications could be implemented with the CGG system to detect over- and underfrequency situations.

The CGG system monitored the RMS phase currents and voltages at the DER use case based on performing the connection of the grid and wind farm with an electrical fault; the test was performed satisfactorily. The application of the CGG system to electrical distribution utilities with customer-owned wind farms is another important area to explore because it could be applied to smart energy trade and interconnection contracts between electrical utilities and DERs by using new DLT applications to improve the security between different actors. Additionally, the application of adaptive protection settings with CGG systems could be used to confirm the selected setting groups of protective relays between different electrical utilities.

The CGG system performed the cyber event test satisfactorily. In the combined cyber event and electrical fault test, when the CT ratio was modified by an incorrect value, the measured current magnitude decreased, but it did not affect the tripping of the overcurrent relay at the fault state because the relay tripped the breaker. The behavior of the SEL-451 relay demonstrated that the relay time was calculated by Eq. (8), and an incorrect setting of the CT ratio could affect the measurements but not the tripping behavior at the fault state. This behavior would be a great advantage if an engineer set an incorrect CT ratio because of human error; the relay would affect the phase current measurements but not the overcurrent protection functions. The test bed demonstrated good performance to assess the protective relay's behavior for cyber events (or cybersecurity events).

The functional integrity of the CGG system that used DLT is necessary for secure power system operations. In many previous published studies, electrical grid applications with DLT were assessed with software simulation tools that did not use real IEDs. Although the monitoring of normal operation in blockchain applications could be evaluated in real electrical grids, other blockchain research applications such as cyberattacks and electrical fault detection are not likely to be performed in operational infrastructures. In evaluating IEDs on this electrical substation grid test bed with DERs and the CGG system, multiple advanced research applications and risks related to network security, equipment failures, electrical hazards, and energy blackouts could be tested and evaluated. Using real power meters and protective relays with electrical substation protocols is critical to properly assess the proposed algorithms in the CGG system.

7. CONCLUSIONS

An advanced multipurpose electrical substation grid test bed with DERs and the CGG system using DLT was created and is presented in this report. Instead of using a simulation software for validating blockchain applications (without hardware in the loop), this advanced test bed had a real-time simulator with power meters and protective relays in the loop. The test bed had wired power meters and protective relays, and it represents an electrical substation grid with inside and outside IEDs and customer-owned DERs (wind farms). In this study, the use case scenarios were focused on using power meters and protective relays with GOOSE messages and an external timing source for synchronizing the collected data for the power system applications.

The CGG system was used for applications focused on electrical fault detection, power quality monitoring, DER, and cyber event use case scenarios. The electrical fault detection and power quality algorithms for the CGG system were assessed by comparing the test results from the real-time simulation source, CGG system, and protective relays. The DER use case was assessed by collecting the measured data from the CGG system. The combined cyber event with an electrical fault use case enabled a study of the behavior of the protective relay—observing the effects on the measurement and protection functions—based on using an incorrect CT ratio setting or on a possible cyberattack scenario that could have a similar effect on the protective relay.

This test bed used a blockchain platform for performing use case scenarios with electrical faults and/or cyber events (or possible cyberattacks) that are unlikely to be performed in a real infrastructure because of possible risks related to the network and equipment security. Additionally, this test bed was based on using the same time stamp for the collected events from the protective relay and the CGG system, which demonstrated satisfactory synchronization of the data managed with the algorithms.

In future work, the electrical substation grid test bed with DERs and the CGG system will be used in other applications. For example, it will be used in an adaptive protection setting group system with DLT and smart contracts between two electrical utilities, which will have a common point of measurement for a protective relay, and the system will be used to integrate an electrical substation grid utility with customer-owned DERs. The application of a blockchain and smart contracts between electrical utilities will improve the security and operability between customer-owned DERs using wind and/or solar farms.

8. REFERENCES

[1] M. Foti and M. Vavalis, "What blockchain can do for power grids?" *Blockchain: Res. Appl.* 2(1): 1–14, 2021.

[2] S. Banks, S. Kim, M. Neposchlan, N. Velez, K. J. Duncan, J. James, A. S. Leger, and D. Hawthorne, "Blockchain for Power Grids 2019," *SoutheastCon*, Huntsville, Alabama, April 11–14, 2019, 1–5.

[3] O. Jogunola, M. Hammoudeh, K. Anoh, and B. Adebisi, "Distributed Ledger Technologies for Peer-to-Peer Energy Trading," *2020 IEEE Electric Power and Energy Conference*, Edmonton, Alberta, Canada, November 9–10, 2020, 1–6.

[4] M. Nour, J. P. Chaves-Ávila, and A. Sánchez-Miralles, "Review of Blockchain Potential Applications in the Electricity Sector and Challenges for Large Scale Adoption," *IEEE Access* 10, 47384–47418, 2022.

[5] H. He et al., "Joint Operation Mechanism of Distributed Photovoltaic Power Generation Market and Carbon Market Based on Cross-Chain Trading Technology," *IEEE Access* 8, 66116–66130, 2020.

[6] M. Yan et al., "Blockchain for Transacting Energy and Carbon Allowance in Networked Microgrids," *IEEE Trans. Smart Grid* 12(6), 4702–4714, 2021.

[7] H. R. Bokkisam, S. Singh, R. M. Acharya, and M. P. Selvan, "Blockchain-based peer-to-peer transactive energy system for community microgrid with demand response management," *CSEE J. Power Energy Syst.* 8(1), 198–211, 2022.

[8] G. Liang, S. R. Weller, F. Luo, J. Zhao, and Z. Y. Dong, "Distributed Blockchain-Based Data Protection Framework for Modern Power Systems Against Cyber Attacks," *IEEE Trans. Smart Grid* 10(3), 3162–3173, 2019.

[9] P. Ramanan, D. Li, and N. Gebraeel, "Blockchain-Based Decentralized Replay Attack Detection for Large-Scale Power Systems," *IEEE Trans. Syst., Man, Cybern.: Syst.* 52(8), 4727–4739, 2022.

[10] A. Mnatsakanyan, H. Albeshr, A. Al Marzooqi, and E. Bilbao, "Blockchain-Integrated Virtual Power Plant Demonstration," *2020 2nd International Conference on Smart Power and Internet Energy Systems*, Bangkok, Thailand, 2022, 172–175.

[11] T. Cioara, M, Antal, V. T. Mihailescu, C. D. Antal, I. M. Anghel, and D. Mitrea, "Blockchain-Based Decentralized Virtual Power Plants of Small Prosumers," *IEEE Access* 9, 29490–29504, 2021.

[12] Y. J. Lin, Y. C. Chen, J. Y. Zheng, D. W. Shao, D. Chu, and H. T. Yang, "Blockchain-Based Intelligent Charging Station Management System Platform," *IEEE Access* 10, 101936–101956, 2022.

[13] Z. Wang, M. Ogbodo, H. Huang, C. Qiu, M. Hisada, and A. B. Abdallah, "AEBIS: AI-Enabled Blockchain-Based Electric Vehicle Integration System for Power Management in Smart Grid Platform," *IEEE Access* 8, 226409–226421, 2020.

[14] E. C. Piesciorovsky, R. Borges Hink, A. Werth, G. Hahn, A. Lee, J. Richards, and Y. Polsky, *Assessment of the Electrical Substation-Grid Test Bed with Inside/Outside Devices and Distributed Ledger*, ORNL/TM-2022/1840, Oak Ridge, Tennessee, Oak Ridge National Laboratory, 1–87, 2022.

[15] G. Hahn, A. Werth, E. C. Piesciorovsky, W. Monday, Y. Polsky, A. Lee, and R. Borges Hink, *Oak Ridge National Laboratory Pilot Demonstration of an Attestation and Anomaly Detection*

Framework using Distributed Ledger Technology for Power Grid Infrastructure, ORNL/TM-2022/2527, Oak Ridge, Tennessee, Oak Ridge National Laboratory, 1–56, 2022.

[16] C. Edvard, "Six common bus configurations in substations up to 354 kV," Electrical Engineering Portal, March 18, 2019 (accessed March 10, 2023), https://electrical-engineering-portal.com/bus-configurations-substations-345-kv.

[17] Schweitzer Engineering Laboratories Inc., *SEL-735 Power Quality and Revenue Meter Instruction Manual* (accessed March 10, 2023), https://selinc.com/products/735/docs/.

[18] Schweitzer Engineering Laboratories Inc., *SEL-734 Advanced Metering System Instruction Manual* (accessed March 10, 2023), https://selinc.com/products/734/docs/.

[19] Schweitzer Engineering Laboratories Inc., *SEL-421-4, -5 Protection, Automation, and Control System Instruction Manual* (accessed March 10, 2023), https://selinc.com/products/421/docs/.

[20] Schweitzer Engineering Laboratories Inc., *SEL-451-5 Protection, Automation, and Bay Control System and SEL-400 Series Relays Instruction Manual* (accessed March 10, 2023), https://selinc.com/products/451/docs/.

[21] Schweitzer Engineering Laboratories Inc., *SEL-351S Protection System Instruction Manual* (accessed March 10, 2023), https://selinc.com/products/351S/docs/.

[22] S&C Electric Company, "Positrol® Fuse Links" (accessed March 10, 2023), https://www.sandc.com/en/products--services/products/positrol-fuse-links/#Construction.

[23] ANSI, "ANSI C84.1 Electric Power Systems and Equipment—Voltage Ranges" (accessed March 10, 2023), http://www.powerqualityworld.com/2011/04/ansi-c84-1-voltage-ratings-60-hertz.html.

[24] Wholesale Electricity Spot Market (WESM), *WESM Manual: System Security and Reliability Guidelines*, 2021 (accessed March 10, 2023), https://www.wesm.ph/downloads/download/TWFya2V0IFJlcG9ydHM=/MTUxNQ==.

[25] DTE Energy, "Electric Choice Understanding Power Factor" (accessed March 10, 2023), https://www.dteenergy.com/content/dam/dteenergy/deg/website/business/service-request/electric/electric-choice/powerFactor.pdf.

[26] J. Dreyer, M. Fischer, and R. Tönjes, "Performance Analysis of Hyperledger Fabric 2.0 Blockchain Platform," *Proceedings of the Workshop on Cloud Continuum Services for Smart IoT Systems*, 32–38, 2020, https://doi.org/10.1145/3417310.3431398.

[27] M. van Rensburg, D. Dolezilek, and J. Dearien, "Case Study: Using IEC 61850 Network Engineering Guideline Test Procedures to Diagnose and Analyze Ethernet Network Installations," *PAC World Africa Conference*, Johannesburg, South Africa, November 12–13, 2015.

[28] Duke Energy, "Power Quality Disturbances, Undervoltage/Overvoltage" (accessed March 10, 2023), https://www.duke-energy.com/energy-education/power-quality/definitions.

APPENDIX A. CODES FOR ALGHORITMS

APPENDIX A.1. ELECTRICAL FAULTED PHASE ANOMALLY DETECTION CODE

----continue up----

```
    def detect_electrical_faults(self, goose_data: dict) -> List[EventDetails]:
        """Returns the first faulted phase event for each phase in the current window for each goID."""
        current_threshold_a = 200.0

        events = []

        for goid in self._relay_goids:
            # skip if no window data for goid
            if goid not in goose_data or (
                goid in goose_data and len(goose_data[goid]) == 0
            ):
                continue

            phase_a_start = None
            phase_b_start = None
            phase_c_start = None

            for row in goose_data[goid]:
                if not phase_a_start and row[self._relay_field_name_to_index("magCurrentPhaseA")] >
current_threshold_a:
                    phase_a_start = row[1]
                if not phase_b_start and row[self._relay_field_name_to_index("magCurrentPhaseB")] >
current_threshold_a:
                    phase_b_start = row[1]
                if not phase_c_start and row[self._relay_field_name_to_index("magCurrentPhaseC")] >
current_threshold_a:
                    phase_c_start = row[1]

                if all([phase_a_start, phase_b_start, phase_c_start]):
                    break

            if phase_a_start:
                events. Append(EventDetails(phase_a_start, phase_a_start, goid,
"electrical_fault_phaseA", f"Electrical fault detected in window for phase A starting at
{phase_a_start}"))
            if phase_b_start:
                events.append(EventDetails(phase_b_start, phase_b_start, goid,
"electrical_fault_phaseB", f"Electrical fault detected in window for phase B starting at
{phase_b_start}"))
            if phase_c_start:
                events.append(EventDetails(phase_c_start, phase_c_start, goid,
"electrical_fault_phaseC", f"Electrical fault detected in window for phase C starting at
{phase_c_start}"))

        return events
```

----continue down----

Figure A-1. Code of electrical faulted phase anomaly detection.

----continue up----

```
def power_factor(magTotW: float, magTotVAr: float) -> float:
    """Returns the power factor for the given values."""
    return magTotW / ((magTotW**2 + magTotVAr**2) ** 0.5)


def is_low_power_factor(magTotW: float, magTotVAr: float) -> bool:
    """Returns true if the power factor is low for the given values."""
    power_factor_threshold = 0.9

    return (power_factor(magTotW, magTotVAr)) < power_factor_threshold


def is_over_voltage(mag_voltage: float) -> bool:
    """Returns true if the given voltage is over the threshold."""
    over_threshold_kv = 7.62

    return mag_voltage > over_threshold_kv


def is_under_voltage(mag_voltage: float) -> bool:
    """Returns true if the given voltage is under the threshold."""
    under_threshold_kv = 6.84

    return mag_voltage < under_threshold_kv


def is_over_freq(mag_freq: float) -> bool:
    """Returns true if the given frequency is over the threshold."""
    over_threshold_hz = 60.3

    return mag_freq > over_threshold_hz


def is_under_freq(mag_freq: float) -> bool:
    """Returns true if the given frequency is under the threshold."""
    under_threshold_hz = 59.7

    return mag_freq < under_threshold_hz
```

----continue down----

Figure A-2. Code of power quality detection.