STATE ESTIMATION-BASED CENTRALIZED SUBSTATION PROTECTION SCHEME

A Dissertation
Presented to
The Academic Faculty

by

Hussain Fareed Albinali

In Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy in the
School of Electrical and Computer Engineering

Georgia Institute of Technology
December, 2017

STATE ESTIMATION-BASED CENTRALIZED SUBSTATION PROTECTION SCHEME

Approved by:

Dr. Meliopoulos, A.P, Advisor
School of Electrical and Computer
Engineering
Georgia Institute of Technology

Dr. Gebraeel, Nagi Z
School of Industrial and Systems
Engineering
Georgia Institute of Technology

Dr. Wardi, Yorai
School of Electrical and Computer
Engineering
Georgia Institute of Technology

Dr. Ying, Zhang
School of Electrical and Computer
Engineering
Georgia Institute of Technology

Dr. Saeedifard, Maryam
School of Electrical and Computer
Engineering
Georgia Institute of Technology

Date Approved: [August 03, 2017]

To my beloved parents and my wife

ACKNOWLEDGEMENTS

Also, I would like to thank my family. In fact, words are powerless to express my gratitude to my parents who have drawn the road map for my success in my life since my childhood. Without my parents support, sacrifices, encouragements and inspiration, I would not be able to complete this Ph.D. So, my ultimate respect, love, thanks, and appreciation are for them. Also, I would like to thank my wife for her understanding, love, encouragement and patience which contribute significantly toward my achievements.

Last but not least, I would like to thank all my labmates. In particular, I would like to thank Dr. Thamer AlQuthami, Dr.Yonghee Lee, Dr. Fan Rui, Dr. Sun Liangyi, Dr. Yu Liu, Xie, Boqi, Vasios, Orestis, Srinivasan, Mohit, Alamri, Abdullah, and Vejdan, Seyyedmohammadsadegh. Their friendships provide countless support during my Ph.D. journey.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF SYMBOLS AND ABBREVIATIONS

AEP	American Electric Power
CID	Configured IED description
CT	Current Transformer
DSEBCPS	Dynamic State Estimation Based Centralized Protection Scheme
DSE	Dynamic State Estimation
EPRI	Electric Power Research Institute
GOOSE	Generic Object Oriented System Events
HFMCS	Hidden Failure and Monitoring and Control Scheme
HMI	Human Machine Interface
HASR	High-Availability Seamless Ring
HVDC	High Voltage Direct Current
IED	Intelligent Electronic Device
ICD	IED Capability Description
IMPACS	Integrated Modular Protection and Control System
IPACS	Integrated Protection and Control System
LN	Logical Node
MMS	Manufacturing Message Specification
NN	Neural Network
PPS	Pulse Per Second
PRP	Parallel Redundancy Protocol
PT	Potential Transformer
RSS	Relay Supervisory System

SCADA	Supervisory control and data acquisition
SCL	Substation Configuration Language
SCAQCF	State and Control Algebraic Quadratic Companion
SIPSUR	Sistema Integrado de Protección para Subestaciones Rurales'
SSD	
	System-Specification Description
SPID	Strategic Power Infrastructure Defense
WLS	Weighted Least Square

SUMMARY

Power systems are experiencing drastic changes with the introduction of renewable and customer-owned resources. These changes introduce new challenges in the protection, control, and operation of power systems. They are concurrent with utilities' efforts to boost system reliability. Such efforts are undermined by the vulnerability of protection system to hidden failures. Accordingly, it is necessary to develop new methods that can cope with new characteristics and avoid relay misoperations because of hidden failures.

In response to these challenges, relay manufacturers and researchers have proposed several protection schemes. Many of these schemes, especially those concerned with hidden failure detection, employ adaptive protection schemes to increase the security of protection systems. Adaptive protection schemes have several disadvantages. First, they do not address the issue of instrumentation channel (i.e., CT and PT) failures. Moreover, they are complex schemes because the algorithms depend on predefined contingencies. Hence, they require intensive studies to identify the behavior of each relay under various fault conditions and contingencies. Finally, adaptive schemes cannot cope with the revolutionary changes in power systems such as the introduction of renewable resources and power electronic devices. These disadvantages mandate a new philosophy which is capitalizing on technology advancement that paves the way for a paradigm shift in protection systems.

This dissertation introduces a new dynamic state estimation-based centralized protection scheme (DSEBCPS) at the substation level. This system supplements dynamic state estimation-based protection for individual zones known as "settingless relays" to

secure their operation against hidden failures. The DSEBCPS communicates with the settingless relays via the station bus and obtains essential information from each protection zone, such as phasor quantities, breakers, and disconnect status. This information is processed by the DSEBCPS to extract the substation topology and states. Specifically, the DSEBCPS performs dynamic state estimations in the quasi-dynamic domain once per cycle to detect any sort of abnormality within the substation. Upon detecting abnormalities, the DSEBCPS performs hypothesis testing to distinguish between faults and hidden failures. The DSEBCPS detects and locates hidden failures within the substation through hypothesis testing. Then, the DSEBCPS streams the estimated measurements that correspond to the detected bad measurements to the settingless relay to replace the compromised measurements. It's capability to detect hidden failures and replace the compromised measurements in real time secure settingless relays from misoperation and ensure high dependability even with the presence of hidden failures. Such capability bridges a critical gap in protection systems. The integration of the proposed scheme and the individual zone protection form a resilient protection system that is self-immunized against hidden failures. The DSEBCPS concept has been tested with numerous numerical experiments. More specifically, five cases of hidden failures were simulated: (1) PT blown fuse, (2) CT saturation, (3) CT short circuit, (4) CT reverse polarity, and (5) wrong CT ratio setting.

Critical to this work is the ability to manage data and communications between the various devices (i.e., MUs, settingless relays, and DSEBCPS) within the substation and between the substation and the control center. Therefore, this thesis includes the proposed system architecture, which specifies data management, communication protocols, and the hierarchical structure of the system. Our design for this architecture complies with IEC-

61850 standard requirements. This compatibility is achieved by using the data objects, services, and communication protocols defined in the standard. Furthermore, we highlight the long-term goals of this approach: to support the next generation of energy management systems (EMSs), where the proposed system will provide the necessary data and real-time models to the control center for performing the usual control center functions such as state estimation, optimization, and control.

CHAPTER 1.   INTRODUCTION

1.1   Background

Power systems around the world are experiencing an evolution driven by the introduction of new energy resources, particularly renewable energy resources, power electronics conversion systems, and high-voltage direct current (HVDC) transmission. According to a recent forecast, renewable energy resources will make up around 31.2% of the total world power generation by 2035 [1], [2]. Moreover, around 50% of these resources will come from wind and solar energy [1]. This massive deployment of new energy resources has already led to several changes in power system characteristics, including reduced fault current levels [3], increased dynamics, and wider-frequency variations of disturbances. Such changes impose new challenges and mandate new approaches to deal with the different aspects of the power system, one of which is the protection and control of the power system.

Another challenge faced by utility companies is to boost system reliability, a goal to which they have devoted tremendous effort. However, such efforts could be undermined by improper operations, or "misoperations," of conventional protection systems. Therefore, such misoperations must be avoided by designing a reliable protection system. This reliability is defined by two fundamental characteristics: dependability and security [4], [5]. The term *dependability* is defined in IEEE C37-100-1992 as "The facet of reliability that relates to the degree of certainty that a relay or relay system will operate correctly." This definition implies that dependability describes the ability of the relay to accurately respond to abnormalities within its protection zone in a timely manner. The term

security is defined in IEEE C37-100-1992 standard as "That facet of reliability that relates to the degree of certainty that a relay or relay system will not operate incorrectly." This definition indicates that security describes the relay's immunity to operate during a fault outside its protection zone. In fact, dependability and security are competing characteristics of any protection system because a highly dependable system might result in an insecure system, and vice versa. Accordingly, protection engineers must consider a tradeoff between dependability and security during the overall design of protection systems. Despite all the efforts exerted by protection engineers to design a reliable protection system and the development in protective devices, relay misoperations are still occurring with significant frequency. These misoperations are the reasons for approximately 10% of total power system interruptions, as reported by the North American Electric Reliability Corporation (NERC) [6]. In many cases, these misoperations lead to wide power system disturbances and even blackouts, such as the one that occurred recently in southern California [7]. To analyze these concerns in all of its regions, NERC formed the national Protection System Misoperation Task Force (PSMTF), which collects and analyzes relay operations [6]. Figure 1-1 shows recently released statistics pertaining to relay operations; around 65% of misoperations are caused by settings/logic errors, relay instrumentation channels, and communications failures. The common characteristic of these problems is that they remain hidden until they are exposed by an event in the network, such as a power fault condition [7]. This characteristic increases the complexity of the problem because it introduces several contingences into a system designed in most cases to handle only one contingency. These types of hidden failures remain a critical gap that jeopardizes the reliability of

2

protection systems. Therefore, overcoming these challenges requires a new philosophy in power system protection based on the latest developments in technology.
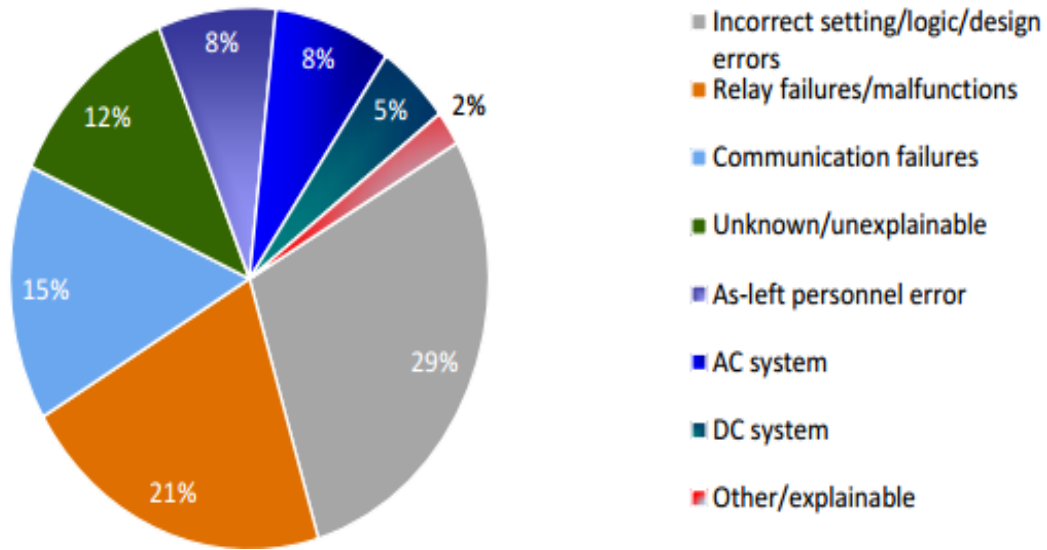
Figure 1-1 Statistics of relay misoperations [6].

Technological advancements have played a major role in paving the way for a new protection system capable of overcoming present-day challenges. Specifically, the introduction of merging units, advancements in computational capabilities and the communication infrastructure as well as availability of related standards enable the realization of centralized approaches for supervision of protective functions and self-healing and self-correction of the effects of hidden failures. The introduction of IEC 61850 provides a blueprint to allow IEDs from various manufacturers to seamlessly participate in new protection schemes. Data transfer within the substation has been standardized for any application [8], [9]. The standard introduces a new approach to interface the instrument transformers with all protection and control devices within the substation. This new approach entails separating the analog-to-digital conversion modules from the IED to

stand-alone devices called merging units (MUs). IEC 61850-9-1 defines the MU as "an interface unit that accepts multiple analogue CT/VT and binary inputs and produces multiple time synchronized serial unidirectional multi-drop digital point to point outputs to provide data communication via the logical interfaces." The separation of the D/A modules by introducing MUs facilitates the introduction of a substation-centralized protection scheme using off-the-shelf hardware [9]. Such hardware is a standard computer characterized by high computational capabilities to process massive data streaming from the MUs. Finally, this realization of the substation-centralized protection scheme will not be possible without advancement in time-synchronization technology using the precision time protocol (PTP) as per IEEE 1588-2008.

1.2   Research Objective

The evolution in power systems, the risk of relay misoperation because of hidden failures, and the technology advancement have driven us to propose a new substation-centralized protection scheme secured against hidden failures. The objective of this research is to design a dynamic state estimation-based centralized protection scheme (DSEBCPS) to increase protection system security and dependability. The DSEBCPS supervises the dynamic state estimation-based protective relays for individual zones, known as "settingless protection" [9]; detects hidden failures; and corrects compromised data resulting from hidden failures. Settingless protective relays are an emerging concept in protection that can be applied reliably to any power system device, including power electronic devices. The proposed centralized protection scheme, along with settingless relays, forms a resilient substation-centralized protection system capable of mitigating the

4

limitation in conventional protection systems, including the protection of power electronic–based systems and the capability of detecting hidden failures.

Critical to this work is the ability to manage the data and communication among various devices (MUs, settingless relays, DSEBCPS) within the substation and between the substation and the control center. Therefore, we defined the details of the system architecture, which specifies data management, communication protocols, and the hierarchical structure of the system. Currently, there are worldwide efforts to design the architecture of the digital substation, and we hope this research will make a significant contribution toward this goal.

1.3 Thesis Outline

The following chapters include the details of the DSEBCPS. Specifically, the dissertation consists of eight chapters divided as follows: Chapter 2 provides a brief review of the literature and other background information associated with the proposed research topic. Chapter 3 discusses the impact of hidden failures in different components of protection systems. The overall concept of the DSEBCPS is introduced in Chapter 4. Chapter 5 explains the mathematical formulation of every module within the DSEBCPS. In Chapter 6, we demonstrate the capability of the DSEBCPS in detecting hidden failures in real time through numerical experiments. This chapter includes the results of five cases of hidden failures: (1) PT blown fuse, (2) CT saturation, (3) CT short circuit, (4) CT reverse polarity, and (5) wrong CT ratio setting. Chapter 7 presents the proposed architectures for data management, communication with zone-level relays within the substation, and communication with the control center. This chapter introduces the proposed architecture for both grassroots installation and for an existing substation. It also highlights the long-

term goals of this architecture to support the next generation of energy management systems. Finally, Chapter 8 includes concluding remarks, contributions, and directions for future research.

CHAPTER 2.   LITERATURE SURVEY

2.1   Introduction

This chapter provides a brief review of the literature and other background information associated with the proposed research topic. We first discuss the historical development of the centralized protection scheme. Then, we introduce the adaptive scheme implementation for hidden failures application. Finally, we discuss emerging concepts that can be employed in the centralized protection scheme. More specifically, the concepts of settingless relay and pattern recognition protection schemes are highlighted.

2.2   Historical Development

The development of centralized protection schemes began in 1980 [9]. One of the earliest efforts to develop such a system was the EPRI research project RP-1359, which addressed system requirements for the substation control and protection system developed by Westinghouse Electric Cooperation [9], [10], [11]. This system is an integrated protection system for transmission-level substations, which includes line, transformer, bus, shunt reactor, and breaker failure protections. Furthermore, the system includes control functions, system restoration aid, revenue metering, and a SCADA system. Two similar systems, the integrated modular protection and control system (IMPACS) and the hybrid system, were developed by American Electric Power (AEP) and ASEA, respectively [9].

In 1992, Ontario Hydro developed the integrated protection and control system (IPACS), a computer system designed for protection, control, and monitoring [9]. It was a centralized system using a single CPU that provided a protection system for transformer

stations. It provided protection for the protection zones of typical transformer stations such as transformers, buses, and feeders. Additionally, the system provided metering and SCADA functions. It was deployed to around 56 substations. In 1994, GE and North West utility in Spain developed SIPSUR, which is a centralized protection scheme for medium voltage (MV) distribution substations. This system combined the protection schemes of two incomers, one transformer, and five feeders into a central platform [9], [12].

In 2000, a centralized protection system was developed by Vattenfalls Eldistribution in cooperation with ABB [9], [13]. The system was developed for control and protection of HVDC substations and included several conventional AC protection functions. The system was deployed at five different substations. It used the industrial computers of that time. Each computer was connected to set of I/O modules with processor cards for digital and analog input and output data.

The aforementioned systems managed to integrate both control and protection functions into microprocessor-based devices. These systems provided more monitoring and control capabilities that improved the operational aspects of the system. However, they were replicas of the legacy protection functions without additional algorithms to enhance protection-system security. Therefore, these systems were vulnerable to hidden failures, which affected their overall security.

2.3   Adaptive Scheme-Based Centralized Protection Scheme

During the last two decades, relay manufacturers and researchers have addressed some specific issues related to hidden failures. They have proposed several protection schemes that minimize the effects of hidden failures. Most of these schemes employ the

concept of adaptive protection schemes, which increase the security of protection systems [14]–[18]. Conceptually, adaptive schemes have the capability to automatically adjust the settings of the protection system according to system conditions. This type of scheme is defined in [16] as a scheme that "automatically adjusts the operating characteristics of the relay system in response to changes in power system conditions."

One example of an adaptive scheme is the blocking scheme, which can identify a faulty zone by monitoring the pickup of all relays that see the fault. Then the scheme blocks the relays not located in the faulty zone, as illustrated in Figure 2-1. The authors of [17], [19] demonstrated that the blocking signal can be sent in less than 20 ms, which is more than fast enough to block backup relays. The introduction of GOOSE messages facilitates the implementation of the blocking scheme without additional hardware requirements. The blocking scheme increases the security of the protection system by eliminating the operation of the relays outside the faulty zone. However, the system is vulnerable to hidden failures in instrumentation channels. For example, a hidden failure of a CT short circuit in CT2 in Figure 2-1 will cause the nonoperation of Relay-2 in response to a fault in its zone. Accordingly, Relay-1 will sense the fault and operate. A similar scenario will result if the setting of Relay-2 is not adequate to detect the fault. Moreover, the scheme complexity increases with the complexity of the system topology. This complexity might lead to errors in developing the overall logic of the blocking scheme.
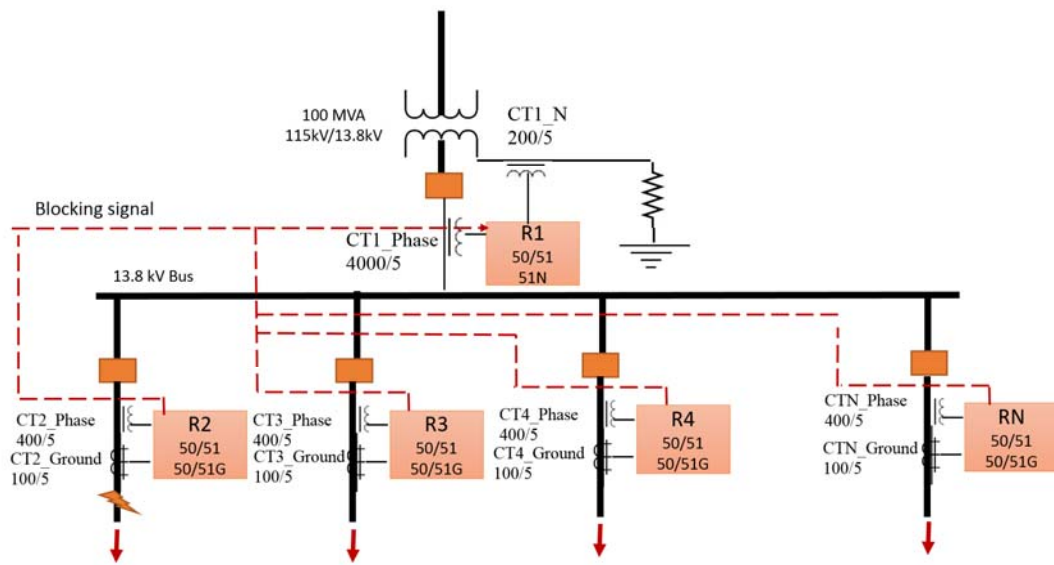
Figure 2-1 Example of blocking scheme.

A widely used adaptive scheme is the voting scheme, which capitalizes on the fact that each protection zone and its backup consist of several relays. The objective of the voting scheme is to increase the security of protection systems by involving several relays located within a protection zone to make final relay decisions [15], [17], [20], [21]. Usually, such a scheme is initiated under certain power system conditions such as heavy load conditions, which require a very secure protection system to avoid relay misoperation. A simple example of a voting scheme is shown in Figure 2.-2, which shows a transmission line with one set of protective relays used to protect the line. Typically, these relays are a differential relay (R1), distance relay (R2), and directional relay (R3). Usually, the line has another set of similar relays at each side to provide backup protection. The voting scheme implemented in this example is known as a two-out-of-three voting scheme, which demands two relays to see the fault and operate in order to initiate a trip signal and isolate the line. The initiation of the scheme depends on the system's condition, such as a heavy

load condition; otherwise, each relay operates independently [22]. These conditions need to be predefined based on comprehensive power system studies. A more advanced voting scheme with a real-time intelligent fuzzy factor has been proposed [15]. The objective of this scheme is to overcome any uncertainty in the relay's decision.

The voting scheme has several disadvantages that could jeopardize protection system security. A main disadvantage is that the relays used in the voting scheme are vulnerable to hidden failures that might cause relay misoperation. In the given example, a hidden failure in the instrumentation channel PT-1 affects the voltage inputs of relays R2 and R3 and might lead them to misoperate. Moreover, the scheme is complex and subjected to several uncertainties such as operating conditions that initiate the scheme.
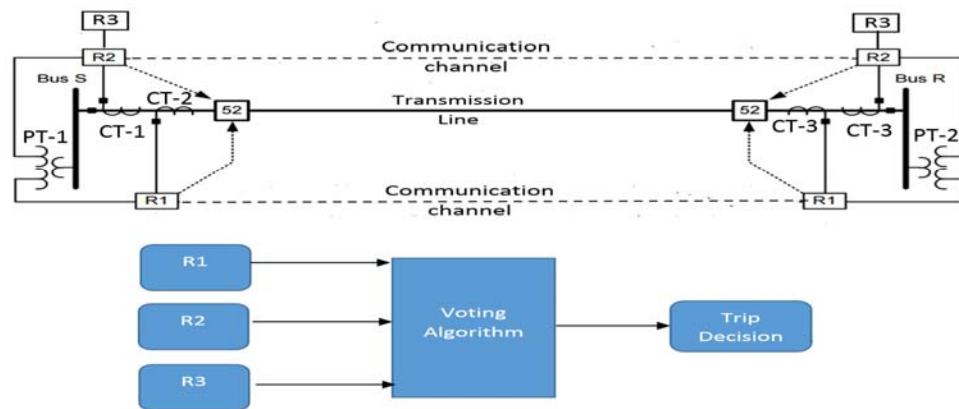
Figure 2-2 Example of voting scheme in transmission line protection.

Adaptive schemes have been employed in several centralized protection schemes. One of these systems is the strategic power infrastructure defense (SPID), a wide-area scheme that employs a multi-agent system to assess power system vulnerability and take proper defensive actions, as shown in Figure 2-3 [23]–[25]. The aim of the system is to

11

increase power system security and avoid catastrophic failures caused by the various sources of vulnerability. The key concept of this system is to secure power system through a comprehensive wide-area vulnerability assessment. SPID provides a defense against hidden failures in its protection scheme through adapting the concepts of an adaptive protection scheme. This is achieved by implementing the blocking and voting schemes described earlier. Moreover, the system can activate different setting groups within the relays as the system configuration changes.
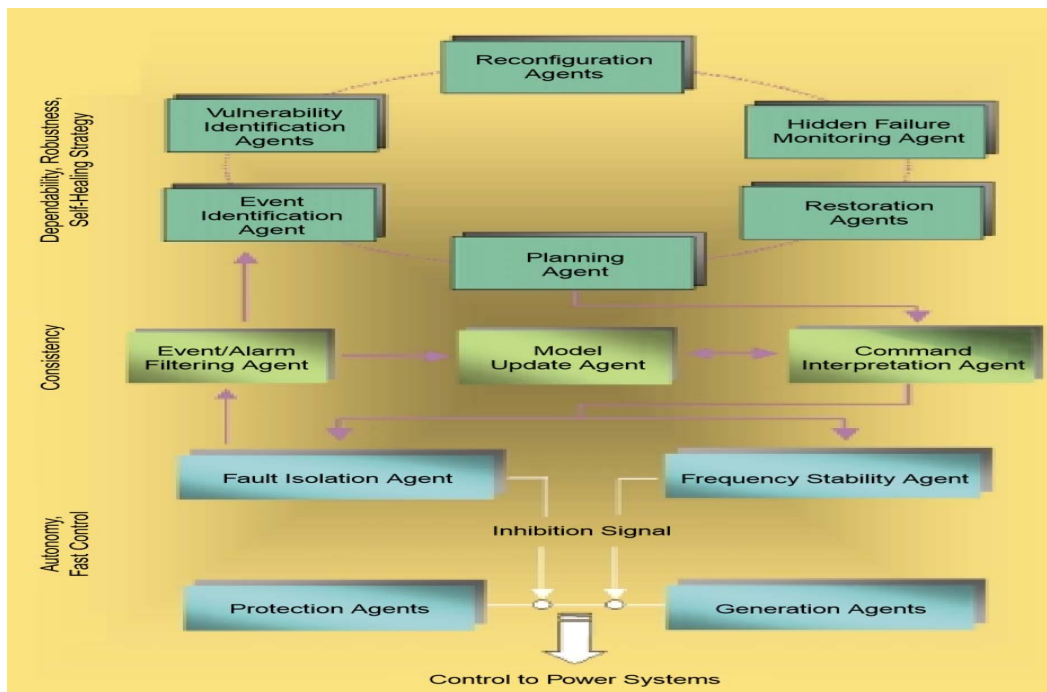
Figure 2-3 The SPID system [25].

Another centralized protection system that employs the adaptive scheme is the hidden failure and monitoring and control scheme (HFMCS) proposed in [26],[27]. It is a substation-based, wide-area system that employs a voting scheme to minimize the effect of hidden failures. This system, which monitors protection systems for hidden failure detection, aims to increase protection system security as a response to power system

vulnerability. The system architecture consists of three main modules interacting with each other, as shown in Figure 2-4. These modules are hidden failure monitoring, hidden failure control, and the misoperation tracking database. The hidden failure monitoring module allows additional controls to be initiated. It monitors the IEDs in a substation and collects the alarms related to the protection system. Moreover, it monitors power system topology to identify any stressed power system conditions. The hidden failure control module employs a voting scheme to minimize the effect of hidden failures. Upon receiving a triggering signal from hidden failure monitoring modules, it will activate the voting scheme. The misoperation tracking database module serves as a database of all hidden failures that take place within the system.
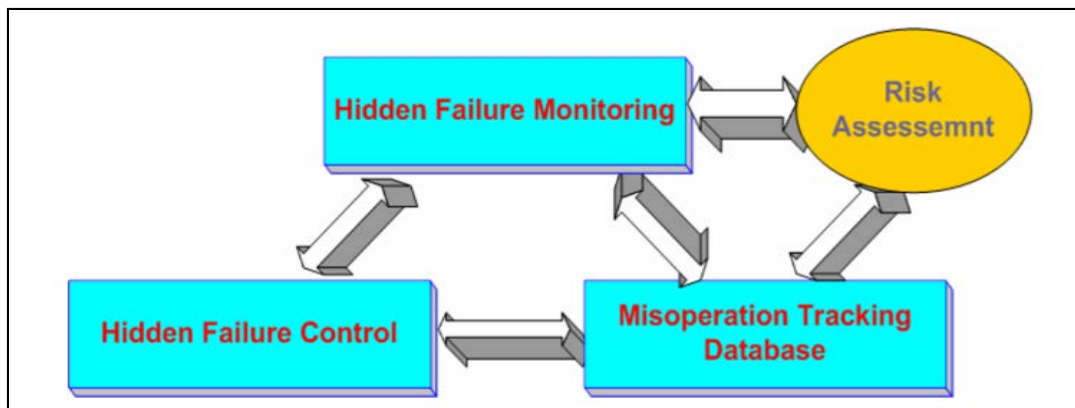
Figure 2-4 HFMCS modules [28].

Another system worth mentioning that uses the adaptive scheme is the relay supervisory system (RSS), an advanced supervisory system proposed in [29]. This system takes advantage of the latest IED technology and the newly established standard (IEC-61850) to develop a new condition-based maintenance philosophy and reduce risks from hidden failures. It supervises all the IEDs in the substations through the station and process

bus, as shown in Figure 2.5. Once the RSS receives an alarm from an IED or detects a failure, it activates the adaptive scheme.
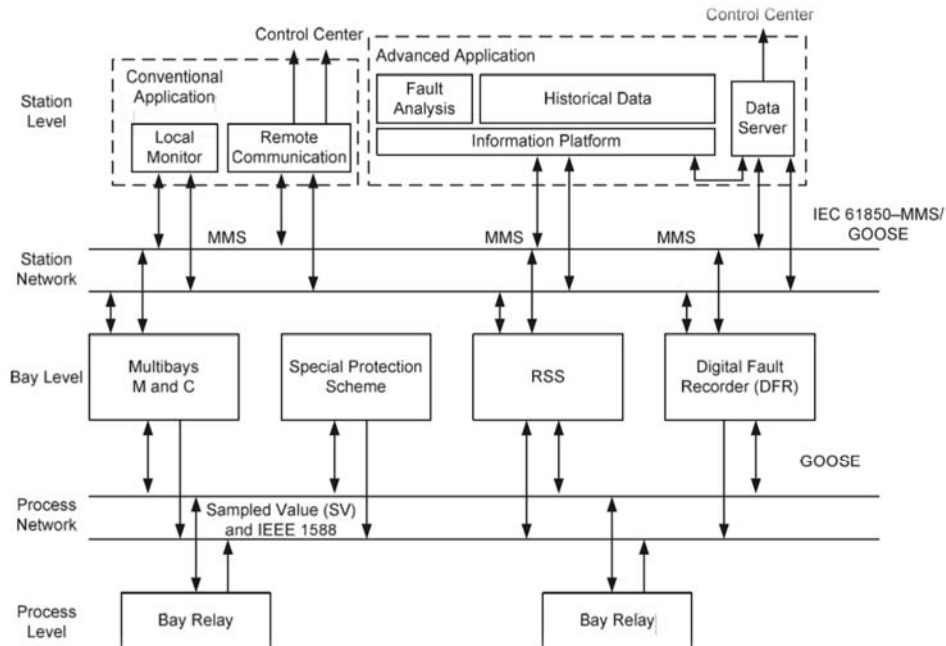
Figure 2-5 RSS architecture [29].

The aforementioned solutions are conceptual, and none has yet been deployed in an actual system due to practical considerations. These systems employ the adaptive scheme to increase the security of the protection system. However, the adaptive scheme has several drawbacks. For one, it depends on IEDs and their instrumentation channels and lacks a mechanism that verifies their accuracy. It is also contingency based, which means that its operation depends on predefined contingencies. However, because the scheme cannot handle all possible contingencies that it may encounter in an actual system, it is incomplete. Furthermore, it is extremely complex, requiring a communication system and several relays operating at the same time to confirm the final relay decision. To find the most optimal algorithm, its implementation requires intensive and comprehensive study (i.e. power flow,

short circuit, and transient analyses) beyond normal study to identify each relay's behavior at each fault condition. Finally, this scheme does not have a uniform algorithm because it mainly depends on the type and number of relays, which are system specific. Thus, the degree of complexity and the lack of standardization may be another source of hidden failures.

2.4   Emerging Concept

Recently, researchers have proposed new approaches to providing protections. This section presents two promising techniques: state estimation–based protection schemes and pattern classification–based protection schemes.

2.4.1   *State Estimation–Based Protection Schemes (Settingless Relay)*

The idea of settingless protection was inspired by the differential protection function. It requires minimal settings, and what is most important is that it does not require coordination with other protective relay functions [30]. Differential protection monitors Kirchoff's current law, which states that the sum of the currents going into a device must equal zero when the device operates normally (unfaulted). Similarly, settingless protection relays monitor all physical laws the device under protection must satisfy when it operates normally (unfaulted). This monitoring is accomplished by performing dynamic state estimation (DSE), which continuously compares the collected measurements (sampled values) to the dynamic model of the device under protection (protection zone) and provides

a quantitative assessment of how well the data fit the dynamic model [30]–[34]. DSE

quantifies the goodness of fit between the measurements and the device model by applying

the chi-square test, which calculates the probability that the measurements fit the model.

The chi-square test typically returns a probability of >80% for healthy protection zones and

<80% for a protection zone with any type of fault inside the zone [30]– [36]. Figure 2-6

shows the overall logic of DSE-based protection [37]. Given an accurate dynamic model

of the protection zone, the performance of the settingless relays is very secure and

dependable. They are immune to normal transient events or external disturbances, such as

inrush current in transformers and transient currents in capacitor banks [36]–[39].
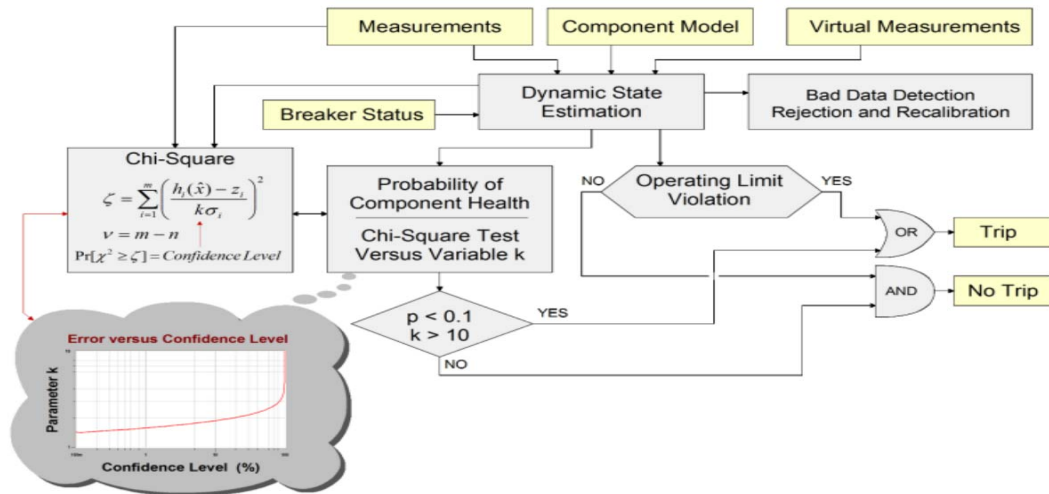
Figure 2-6 Settingless relay overall concept [37].

The settingless relays acquire the measurements of the protection zones from the

MUs via a process bus. Similarly, all relay decisions are communicated back to the

breakers via the process bus. Using MUs has the advantage of minimizing the

16

instrumentation cabling in the substation, which reduces instrumentation errors. Therefore, the accuracy of the data acquisition system depends mainly on instrumentation transformers. Moreover, the MU is characterized by a high sampling rate, a typical value being 4,800 samples/s. This sampling rate allows us to perform DSE 2,400 times per second [36]. This time performance results in detecting the fault in a small fraction of a cycle, which is superior to any existing technology. It is worthwhile to mention that the computational requirements of this proposed scheme are within the computational capabilities of modern microprocessors. The current implementation uses two cores of the processor for each protection zone in the substation, one dedicated to the execution of the DSE and the other for handling user interfaces and visualizations of the performance of the protection zone. The settingless relays for the various protection zones in a substation are integrated into a substation-centralized scheme, as illustrated in Figure 2-7.
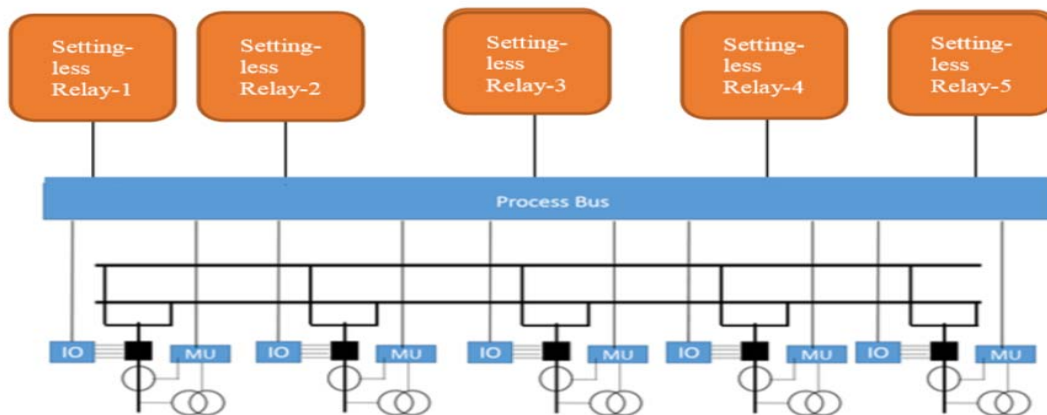
Figure 2-7 Settingless relay architecture.

The settingless relays are vulnerable to hidden failures, similar to any other relaying scheme. Such failures could affect the performance of any relay. Hence, a mechanism to detect such failures is essential for reliable protection of power system components. Figure

2-7 shows that instrumentation channels are the elements of the system most vulnerable to hidden failures. Such failures result in inaccurate measurements going to the settingless relays, which will cause misoperation. Therefore, a mechanism to detect such failures is needed for secure operation.

2.4.2   *Pattern Classification–Based Protection Schemes*

The pattern classification scheme relies mainly on the concept of translational knowledge, which is defined as "a set of procedures that allow[s] field data to be merged with models to produce better decision-making" [40]. It involves converting data to information that is mapped to different types of models. Each model fits certain applications that can be used to create knowledge to take proper control actions. For protection applications, the pattern classification uses the well-known technique of the neural network (NN)[40]–[43]. The concept of an NN-based protective relaying approach is to define a cluster of patterns through an intensive learning process of the system under investigation and match the pattern of system information (i.e., measurements) to a unique cluster, as illustrated in Figure 2-8. This process requires NN training and testing, which requires intensive analysis to characterize the system and generate the pattern clusters. Accordingly, a large number of fault and nonfault cases are required to accomplish the process of training and testing for reliable operation of the algorithm. These test cases are mainly generated from simulation to include all possible scenarios. The identification of the testing cases depends on the power system device under protection because each device in the power system has different characteristics and is subjected to different phenomena.

The technique is vulnerable to hidden failures, like any other relaying scheme. These failures could generate incorrect input data and drive the protection system to misoperate. Furthermore, the system requires intensive studies to develop predefined patterns from the collected inputs. Such requirements could result in incomplete system which is incapable of detecting all faulty conditions.
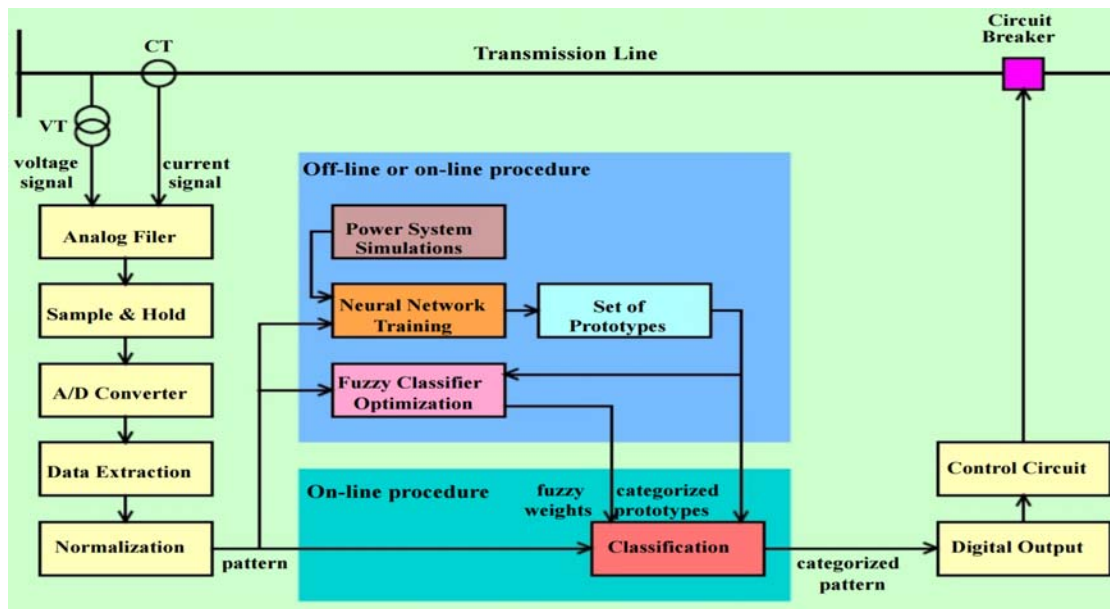
Figure 2-8 NN-based protective relaying approach [42].

2.5   Summary

The concept of a centralized protection scheme was introduced in the 1980s when several centralized protection schemes were introduced. These systems combined the conventional protection system and control functions into a central platform for more controllability. However, these systems were vulnerable to hidden failures because they were not equipped with any additional algorithms to detect such failures. To improve protection systems' security against hidden failures, adaptive protection schemes were

introduced. The adaptive scheme has the capability to automatically adjust the settings of the protection system according to system conditions. A common approach of the adaptive scheme is the voting scheme, which includes several protection relays before initiating a trip signal. In general, the adaptive scheme has several drawbacks, such as its complexity and its vulnerability to hidden failures in instrumentation channels.

The advancement in the technology enables the introduction of emerging concepts such as state estimation–based protection schemes and pattern classification–based protection schemes. The estimation-based protection scheme called a settingless relay is a model-based protection that continually monitors the consistency between the measurements and the zone model. Like the legacy protection system, the settingless relay is vulnerable to hidden failures in the instrumentation channels. Resolving such vulnerability will make the settingless relay a superior protection system in terms of security and dependability

CHAPTER 3.   HIDDEN FAILURES

3.1   Introduction

Hidden failures have been defined as "permanent defects that will cause a relay or a relay system to incorrectly and inappropriately remove a circuit element(s) as a direct consequence of another switching event" [26]. One characteristic of these problems is that they remain hidden (undetected) until an abnormal condition such as a fault occurs. During such condition, hidden failures may provide incorrect input for IEDs, which may result in misoperation and initiation of more contingencies by isolating a healthy portion of the power system. Accordingly, they might widen power system interruptions and lead to a catastrophic scenario, such as a total blackout. Therefore, hidden failures jeopardize protection system security.

A typical protection system shown in Figure 3-1 comprises protective relays, instrumentation channels, (i.e. current transformers (CTs) and potential transformers (PTs)), communication infrastructure, circuits breakers, and batteries [29]. Each component is vulnerable to hidden failures that might cause protection system misoperation. However, protective relays and instrumentation channels are more vulnerable to hidden failures because of their massive population in the substations. This chapter discusses hidden failure modes of different components and their potential impact on the protection system. It starts with protective relays vulnerability to hidden failures. Then it briefly discusses common hidden failure modes in the communication layers. Finally, hidden failure modes in the instrumentation channels are discussed.
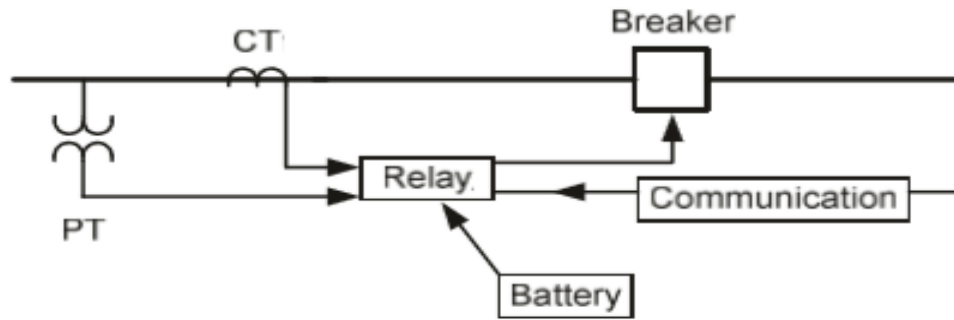
Figure 3-1 Typical protection scheme [29].

3.2   Hidden Failure Modes in Protective Relays

The protective relays are the watchdog of the power system. They are capable of processing data received from the instrumentation channels (i.e., currents and voltages measurements) and detecting abnormal conditions in the power system. These protective relays have evolved drastically over the last three decades from electromechanical-based devices to microprocessor-based devices. The microprocessor-based devices have also been developed to include communication and automation functions along with protection functions and, therefore, they are referred to as intelligent electronic devices (IEDs) [9]. Hidden failures in IEDs can be classified into three categories (a) hardware-related hidden failures, (b) setting-related hidden failures, and (c) relay logic-related hidden failures. The following paragraphs discuss each of these classes briefly [44].

Figure 3-2 shows the typical hardware structure of IEDs, which include signal conditioning to handle the transients and spikes in the signal, an analog-to-digital (A/D) converter, a processor to process the input and perform the IED functions, I/O module to receive and send digital signals, and a power supply module [45]. These components might

fail mainly because of either aging or manufacturer defects. Such failures could lead to relay misoperation by initiating a trip signal during healthy condition or relay nonoperation during faulty conditions. Most IED vendors have implemented self-testing capabilities within their IEDs [46], [47]. Such self-testing is meant to verify the condition of different components in the IED. This includes verifying that the voltage of the DC power supply is within an acceptable range, checking its ability to access the memory of the processor, and validating the A/D conversion. Upon detecting a failure through the self-check, the IED sends an alarm to the control center and deactivates itself automatically. However, the self-check process does not cover the physical I/O modules, which can fail physically (i.e., shorted) and initiate the wrong trip signal to the circuit breaker. This type of failure can't be stopped once it is initiated; nevertheless, a good maintenance program reduces the probability of its occurrence.
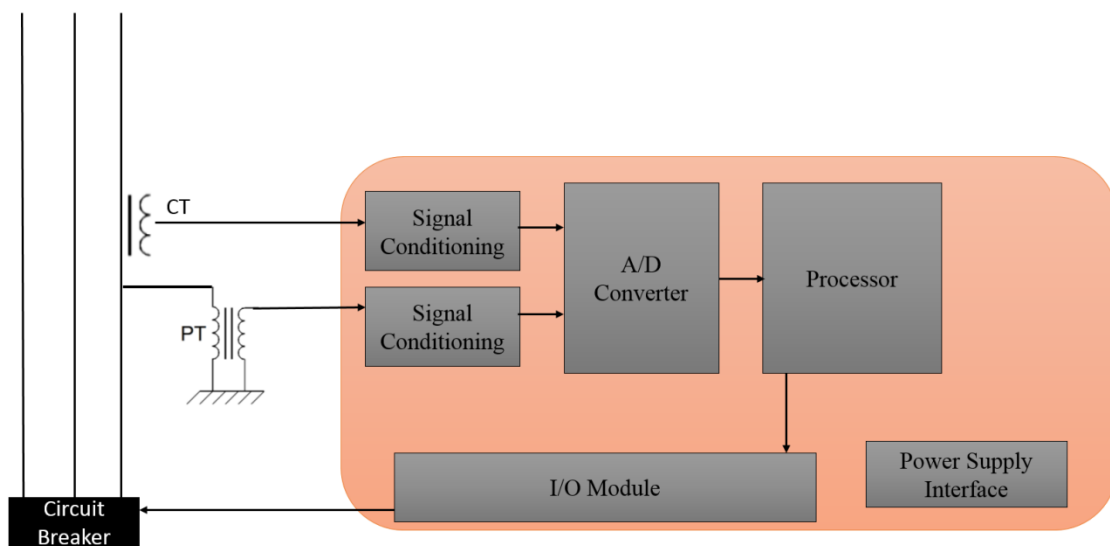
Figure 3-2 The overall structure of IEDs.

Incorrect settings or logic are the most common modes of hidden failures in IEDs, according to NERC [6]. Such failures are, in most cases, related to human factors,

represented by the protection engineers and technicians who calculate and implement the relay settings. This issue has become more observable recently as the degree of complexity in IEDs has increased because protection, control, and automation have been combined in one box. This type of hidden failure is critical because it might cause wide power system interruptions during the healthy condition of the affected zone. An example of such failures in the legacy protection system is relay miscoordination, as illustrated in Figure 3-3, which shows relay-A, located in the upper stream portion of a system, operates faster than relay-B, which is located in the downstream portion, during a fault in the relay-B zone. Accordingly, relay-A initiates a trip signal to breaker-A, which leads to power interruptions for all customers supplied by this system. To avoid the risk of relay misoperation because of incorrect relay settings and logic, many actions have been proposed such as relay settings peer reviews, more training for protection engineers, and relay setting templates standardization. Furthermore, the emerging concept of settingless relays addressed the risk of incorrect relay settings by reducing the required setting of the relay and, more importantly, eliminating the need for relay coordination.
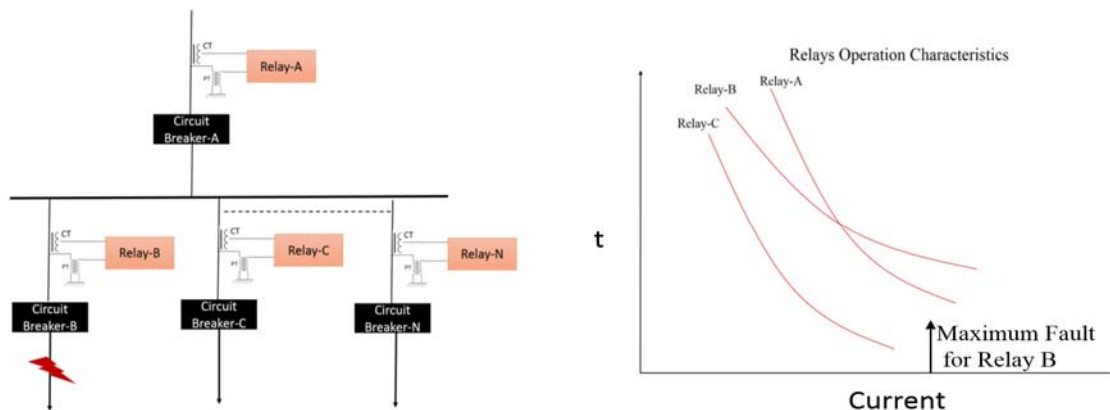
Figure 3-3 Example of relay miscoordination.

3.3　Hidden Failure Modes in Communication Channels

In the era of the smart grid, communication systems have become an integral part of protection systems. These communication systems have massive applications, such as communication between differential relays, transfer blocking, permissive and tripping signals, and the transfer of current and voltage inputs from merging units. With such massive applications, however, communication systems could suffer from hidden failures, which might cause relay misoperations. The common hidden failure modes in communication systems include failures in communication media (i.e., fiber optic cables) and communication interfaces (i.e., routers) [48]. These failures result in the loss of information from the remote ends, which causes a loss of controllability and observability. In legacy protection systems, transmission line protection is the most vulnerable system to hidden failures in communication channels because it employs several communication-based protection schemes, such as differential scheme and a permissive overreach/underreach transfer trip scheme. These schemes rely mainly on the communication channels, and they might misoperate during communication failures. In newly emerged digital substations, the entire protection system for all protection zones in a substation relies heavily on communication. Accordingly, every protection zone is vulnerable to hidden failures in the communication channels. However, this vulnerability is captured in the design of the communication system. Such design entails redundant communication infrastructure. Subsequently, a failure in a communication channel will not impact the integrity of the protection system. Moreover, the design includes initiating an alarm to the control center whenever a communication channel is lost. These design criteria are available in both legacy and emerging protection systems.

3.4   Hidden Failure Modes in Instrumentation Channels

The instrumentation channels in protection systems consist of instrumentation transformers, instrumentation cables, and burdens. They represent the front line of the protection systems, and they act as the interphase between the primary devices (i.e., HV power system devices) and the IEDs, which require a relatively low current and voltage to operate [49], [50]. The instrumentation transformers step down the voltage and current to lower values (typically 1 or 5A for CTs and 69V for PTs). These voltages and currents are supplied to the IED through instrumentation cables. Moreover, the IEDs are equipped with A/D conversion units to convert the collected measurements to digital signals before they are processed. Recently, the A/D conversion has been separated from the IEDs with the introduction of merging units (MU), which substantially reduce the amount of instrumentation cabling [45]. Figure 3-4 shows typical instrumentation channels with and without MUs. Figure 3-4b suggests that instrument transformers are the most vulnerable elements to hidden failures in the instrumentation channels because the MUs have almost eliminated the instrumentation cables. Moreover, the loss of communication between the IEDs and the MUs results in data flow interruption, which can usually be detected by the IEDs. Also, the redundancy in the fiber optic infrastructure minimizes the risk of communication loss. Accordingly, hidden failures in the instrumentation transformers remain a gap that needs to be investigated to improve the security of the protection systems. The following subsections discuss the common modes of hidden failures in CTs and PTs as well as their impact on the legacy protection systems. Furthermore, this research focuses on these hidden failures to develop an overall scheme that can detect hidden failures and secure protections system operations.
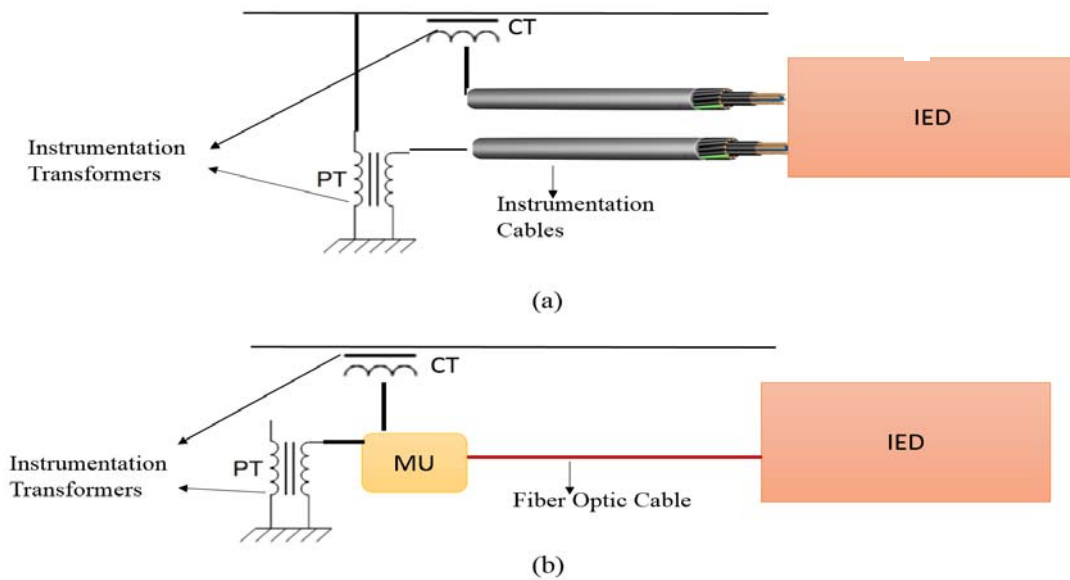
Figure 3-4 Instrumentation channels: (a) conventional; (b) recent approach with MU.

3.4.1   Hidden Failure Modes in Current Transformers

Current transformers (CTs) are instrument transformers used to measure the current waveforms of the protected zone and step them down to values that can be handled by the IEDs. They are typically based on magnetic core design and characterized by their ratio and accuracy class [51]. CT ratio is the ratio of the rated primary current to the rated secondary current, which is typically 5A or 1A. CT accuracy class defines the maximum permissible voltage that can be developed on CT burden before saturation takes place [52]. ANSI C57.13-1978 defines the following two types of CT accuracy based on the application:

- Metering accuracy class used for application that require a high degree of accuracy, such as revenue meters. An example of this class is "0.3 B 0.2," which means that

at 0.2 ohm burden and rated secondary current (i.e., 5A or 1A), the CT accuracy is 0.3% [53], [54].

- Relaying accuracy class for protection application. In this application, the relay accuracy is identified at 20 times of the rated current [53]. An example of this accuracy is "10 C 800," which means that at a standard burden and a fault current of 20 times the CT secondary rating (i.e., 100A or 20A), the CT secondary voltage that will be developed is 800V, and the accuracy of the CT at this condition is 10%. Usually, CT will saturate beyond this condition.

The CT circuits, which are shown in Figure 3-5, are vulnerable to hidden failures. Such failures will cause the IED to inaccurately read current waveform and misoperate. For this research, the CT mathematical model, which is included in Appendix 1, has been developed to simulate and analyze the following common hidden failures modes: (1) CT saturation, (2) CT short circuit, (3) wrong CT polarity, and (4) wrong CT ratio settings.
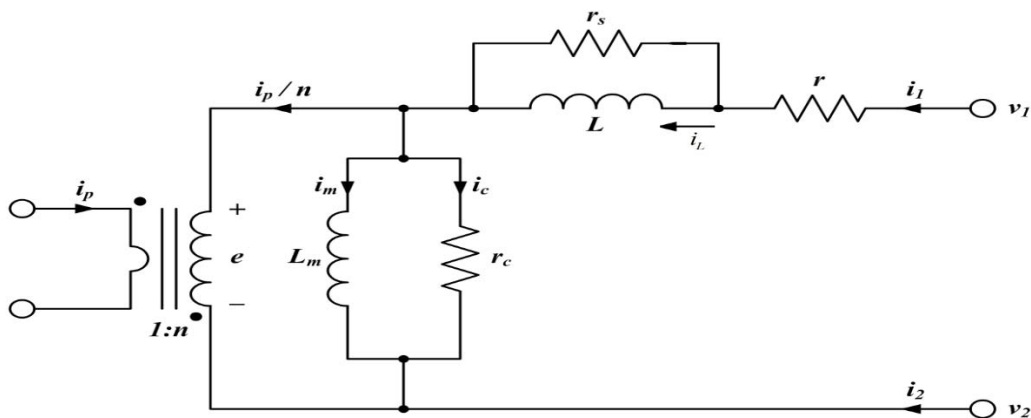
Figure 3-5 CT equivalent circuit.

3.4.1.1. CT Saturation

The CT saturation is one of the most common hidden failure modes in the CT circuit. It is caused by the nonlinear behavior of the magnetic core. The nonlinearity is depicted in the relationship between magnetizing current (i_m) and the magnetic flux density ($\lambda(t)$), as per the following relation:

$$i_m(t) = i_0 \left| \frac{\lambda(t)}{\lambda_0} \right|^n sign(\lambda(t))$$

Figure 3-6 depicts the relationship between the magnetizing curve and the secondary voltage [49], [55]. The figure shows that the relationship is linear for a secondary voltage less than the knee voltage, which is generally defined "as the voltage at which a further 10% increase in volts at the secondary side of the CT requires more than 50% increase in excitation current."[56] Moreover, the relationship becomes nonlinear when the secondary voltage exceeds the knee voltage. In the nonlinear region, the magnetization current increases substantially for a small increase in the voltage. Accordingly, the secondary current of the CT will not be a replica of the primary current. Figure 3-7 shows a typical waveform of a saturated CT, which is a distorted waveform with a lower magnitude than that of the original waveform [55].

There are four main factors that cause CT saturation; (a) high fault current, (b) high CT burden, (c) large DC offset during fault current, and (d) high percentage of remanence [56]. The high fault current and the high CT burden cause the voltage across the burden to increase substantially during the fault condition. This voltage might exceed the knee voltage and drive the CT into the saturation region. The DC offset component increases

the positive half cycles of the secondary voltage that might exceed the knee voltage. The remanence, which is also called residual flux, is the magnetic flux that remains from the previous excitation process. It will add up to the magnetic flux induced by the primary current and could push the core into the saturation region.
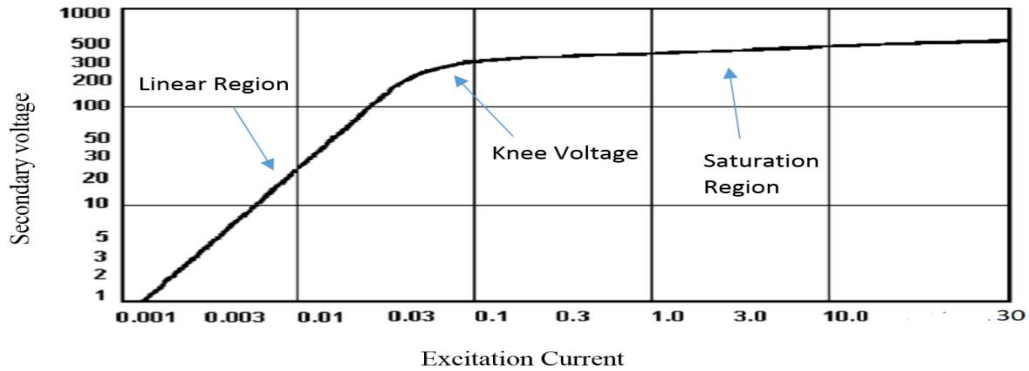
Figure 3-6 CT excitation curve [55].
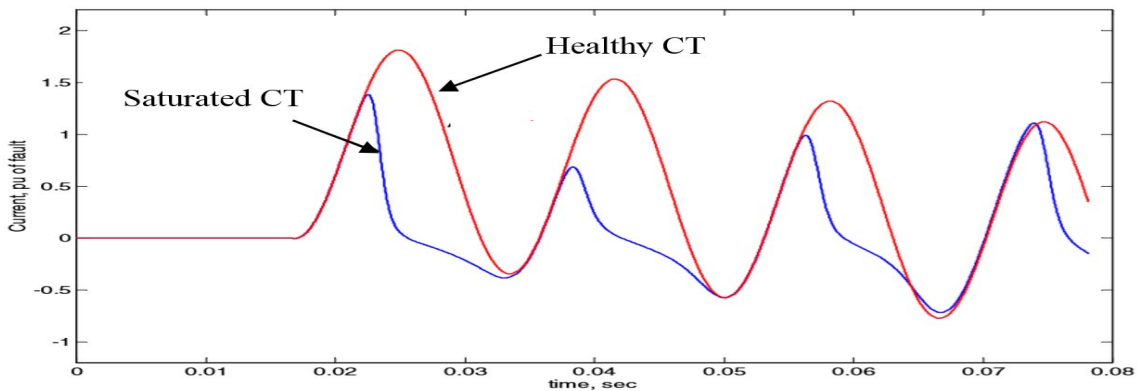
Figure 3-7 Typical waveform of a saturated CT [55].

The saturated CT results in current waveform, which does not replicate the primary current. In particular, the magnitude of the phasor quantity decreases during the CT saturation as shown in Figure 3-7. Moreover, the angle becomes leading [55], [56].

Consequently, all current-based legacy protection devices are vulnerable to misoperation during the CT saturation. For example, Figure 3-8 depicts the response of the transformer (i.e., 100 MVA, 230kV/115kV) differential relay with CT saturation in the secondary side during external ground fault at phase A on the 115 kV side. The figure shows that the CT saturation led to a substantial increase in the differential element, which causes the relay to operate and isolate a healthy transformer. This simulation assumes that there are no CT saturation detection algorithm implemented to secure the relay operation. This example of the CT saturation impact on differential relays can be extended to all types of current-based legacy protection relays. The impact can take the form of relay misoperation or relay nonoperation during an event that requires the relay to operate.
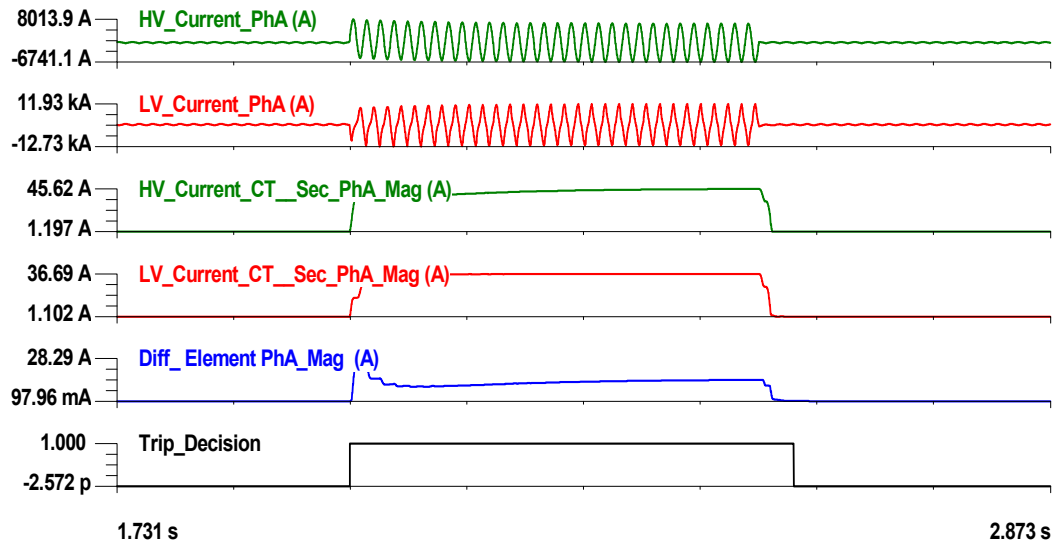
Figure 3-8 Example of the impact of CT saturation on transformer differential protection.

Researchers and relay manufactures have proposed several algorithms to detect CT saturation and inhibit relay operations [57]. Most of these algorithms detect CT saturation based on the harmonic contents in the current waveform of the saturated CT. Other

techniques have been also proposed such as wave shape identification and flux-restrained current differential relay [57]. These techniques mainly block the relay operation or desensitize the relay upon detecting saturation. Their main disadvantage is that their capability to detect the CT saturation is significantly reduced at lower levels of saturation. Additionally, these techniques are also subjected to hidden failures such as improper setting to the CT saturation algorithm. Moreover, their philosophy depends on increasing relay security in the expense of the dependability because during the detection the affected relays will be disabled or desensitized.

3.4.1.2 *CT Short Circuit*

CT short circuit takes place when the CT terminals are shorted. It may take place because of a short circuit event in the instrumentation cables of the CT resulting from a transient surge in the system or poor workmanship during the construction phase of the substation. Also, it might take place following human error during maintenance activities. In both cases, the CT terminals are shorted as shown in Figure 3-9. Consequently, the protective devices connected to the CT will not receive the actual CT secondary current. This might result in the nonoperation of some relays, such as the simple overcurrent relay, during severe fault conditions that require the relay to operate instantaneously. Also, it might cause the relay to misoperate for some relays, such as differential relays and distance relays, during external faults. Figure 3-10 shows the impact of a CT short circuit in a simple ground overcurrent relay (i.e., R2, 51/50 G) for a distribution line during a ground fault in the line. The figure shows that the relay did not operate and caused the upper stream relay (R1, 51N) to operate after a delay and isolate a larger portion of the system.
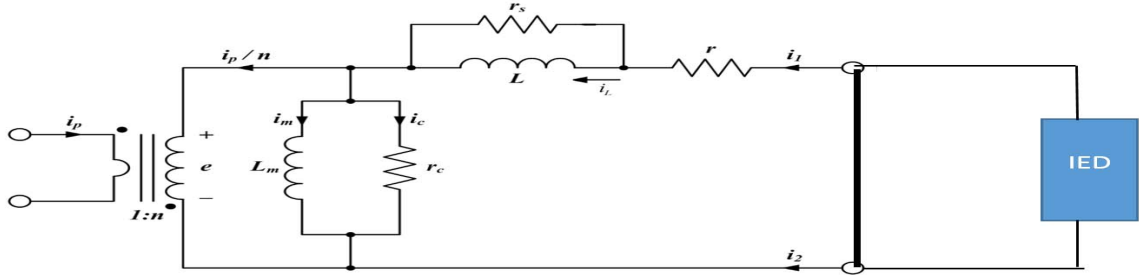
Figure 3-9 CT short circuit model.

a) One line diagram

b) Upper stream relay (R1) operation

c) Distribution line relay (R2) operation
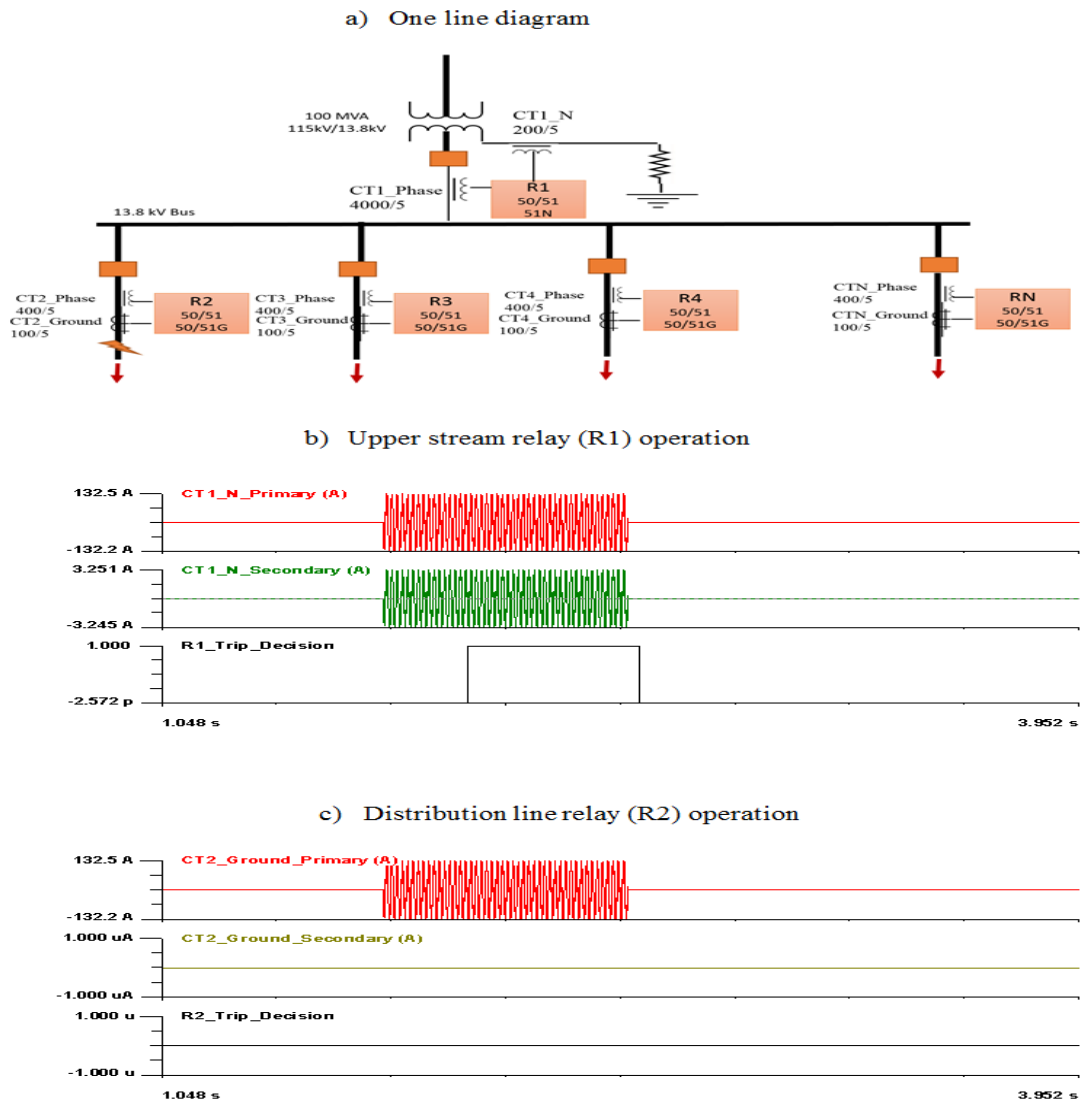
Figure 3-10 Example of the impact of a CT short circuit on overcurrent relay.

3.4.1.3. CT Reverse Polarity

The CT polarity is identified using the dot convention, as shown in Figure 3-11. This convention indicates that if the primary current flows into the dot of the primary side, then the current must flow out of the dot on the secondary side. Similarly, if the current in the primary side flows out of the dot, the current flows into the dot on the secondary side. Usually, the manufacturers use this convention through either paint marks or symbol marks (i.e., H1 and H2 for primary and X1 and X2 for secondary) to identify the polarity [58]. These markings are used to connect the CT based on the requirements of each application.
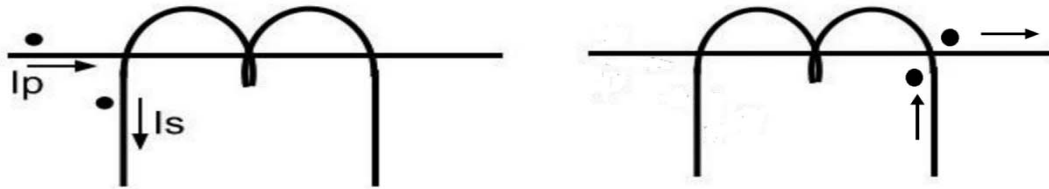
Figure 3-11 CT polarity convention.

CT reverse polarity occurs when the CT terminals are reversed in the relay terminals or in the terminal blocks, which causes the current waveform in the secondary side to be 180 degrees out of phase with the primary current. This type of hidden failure results in relay misoperation for the protective functions that are sensitive to CT polarity, such as differential relays, distance relays, and directional relays. Usually, such hidden failure takes place because of poor workmanship during maintenance or pre-commissioning activities. Also, CT reverse polarity might exist for a long time until a fault occurs in the system or an increment in the load takes place, causing the relay to misoperate.

Figure 3-12 illustrates the impact of the CT reverse polarity in the operation of the 100

MVA, 230kV/115kV transformer differential relay during an increment in the transformer

load from no load condition to 30% of its rating. In this example, the polarity of the CT in

the secondary side of the transformer is reversed. Figure 3-12 shows that the differential

element's current represents the vector sum of the primary and secondary currents read

from the CTs. Subsequently, the relay operated and initiated a trip signal to isolate the

transformer because of the reverse polarity. This example illustrates the negative impact of

hidden failures on power system operations. This impact can also be seen in the operation

of the directional relay, where CT reverse polarity will always reverse the direction of the

current and cause the relay to operate during external faults.
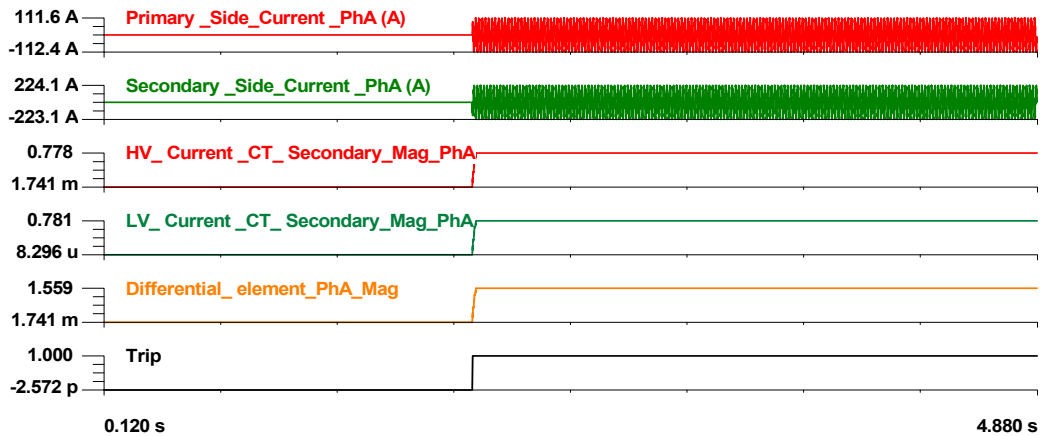
 Figure 3-12 Example of CT reverse polarity.

3.4.1.4 Wrong CT Ratio Setting

The relay requires the correct CT ratio setting to replicate the precise primary

current. The CT wrong ratio is one of the hidden failure modes that takes place during relay

setting implementation or calculation. Protection engineers might consider the wrong

35

setting of the CT ratio during the setting calculation. Also, technicians might implement the wrong CT ratio during setting implementation. In the legacy protection system, the impact of the wrongly implemented CT ratio is mainly to the wrongly calculated primary waveform, which might disturb the metering function within the relay. Also, considering the wrong CT ratio during setting calculation might result in an inaccurate setting. Consequently, the relay might either misoperate during normal condition and an external fault or not operate during an internal fault. Figure 3-13 shows an example of the calculated primary current using the wrong CT ratio for two cases (i.e., a higher ratio of 3000/5 and a lower ratio of 1000/5). In this example, the correct CT ratio is 2000/5. The example shows the difference between the calculated primary currents, considering the correct and wrong ratio could be substantial.
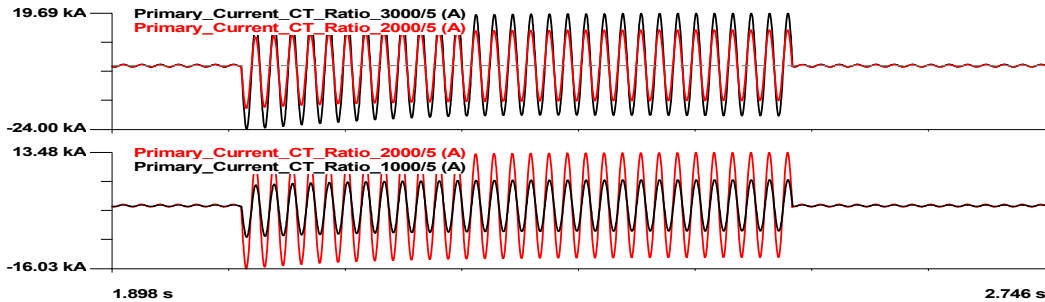
Figure 3-13 Example of the impact of using wrong CT ratio to calculate the primary current.

3.4.2   Hidden Failure Modes in Potential Transformers (PT)

Potential transformers (PT) are instrument transformers that are used to stepdown the system voltage to a level that can be handled by protective devices or meters. PTs are usually single phase transformers that are connected in three phases. The most common connection methods are Y-Y, delta-delta, and open delta, as illustrated in Figure 3-14 [59].

The selection criteria for connection methods mainly depend on the application and economic considerations. The Y-Y connection is used in the HV application more often, while the open delta connection is used more frequently in the distribution network. Delta-delta connections are less common because open delta connections are more economical with two PTs, compared with three PTs in the delta-delta connection. Moreover, delta-connected PTs are not suitable for some protection applications, such as directional overcurrent relays that need a polarizing voltage [59]. Furthermore, Delta-Y connection is used in some application especially in transmission substations.
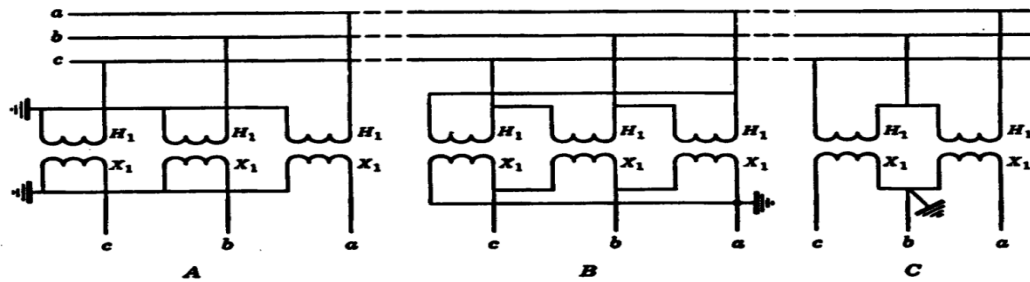
Figure 3-14 Typical connection methods for potential transformers [59].

Figure 3-15 shows the PT circuit, which consists of a primary fuse, internal winding, secondary fuses, instrumentation cable, and a burden. Every component in this circuit is subjected to hidden failures, like any component in the protection circuit. These hidden failures can result in inaccurate voltage readings in the protective devices and may cause relay misoperation. The primary and secondary fuses protect the PT circuit during abnormal conditions. These fuses get blown when the current in the PT circuit exceeds the fuse rating because of an internal fault or overload conditions. Moreover, the fuse might be blown due to under sizing, transients, or harmonic resonance [60]. Additionally, most

failures in the PT circuit will eventually lead to blown fuses. Therefore, blown fuses are considered the most common mode of hidden failures in the PT circuit. Accordingly, we have modeled the PT circuit (Appendix 2) to analyze the impact of blown fuses in the protection system. Figure 3-16 shows an example of such impact on distance relay during phase to phase faults occurred outside 115 kV transmission line with length of 25 mile. Figure 3-16c shows the mho type distance relay characteristic on the R-X diagram with two points A and B that represent the calculated impedance by distance relay phase element (i.e. phase AB) with and without the blown fuse condition, respectively. The figure shows that the blown fuse caused the calculated impedance to fall within zone 1 setting, while the actual impedance during the event was within zone 2 setting. Accordingly, the relay might misoperate during this condition.

The issue of the blown fuse was addressed by the loss of potential (LOP) scheme, which detects an unbalanced condition in the voltage measurements and compares it with the unbalanced condition in the current measurement [61]. If the unbalanced condition exists only in the voltage measurements, loss of potential, which might be caused by a blown fuse, is detected. Upon detecting such event, the affected protection schemes will be blocked. The main disadvantage of this scheme is that during fault conditions the unbalance will appear in both voltage and current measurements and accordingly the LOP will not detect the blown fuse condition.

Figure 3-15 Typical potential transformers circuit.

a) Transmission line side_1 waveform with blown fuse
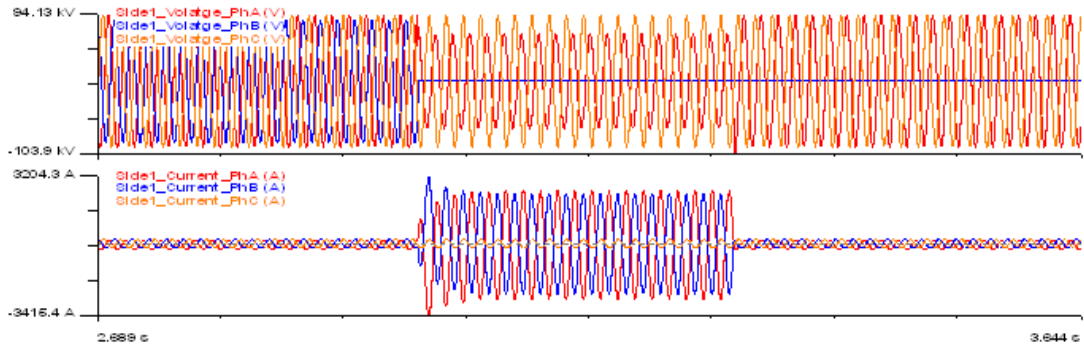
b) Transmission line side_1 waveform without blown fuse
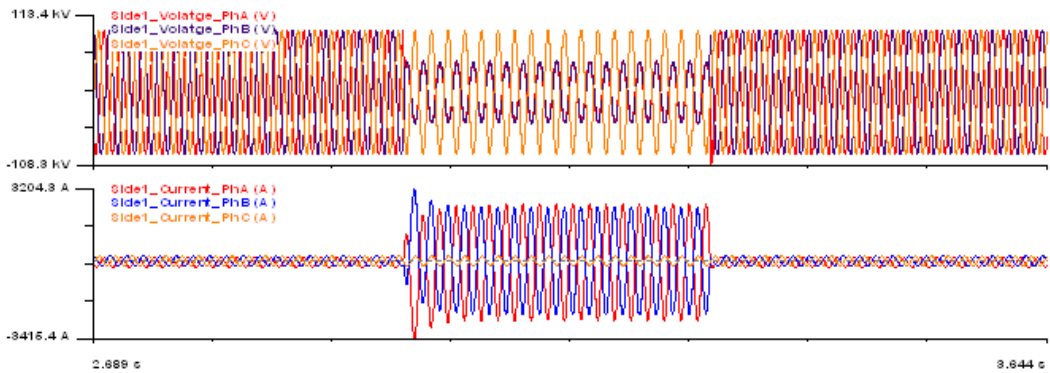
c) Blown fuse effect on distance relay (A with fuse blown and B without fuse blown)
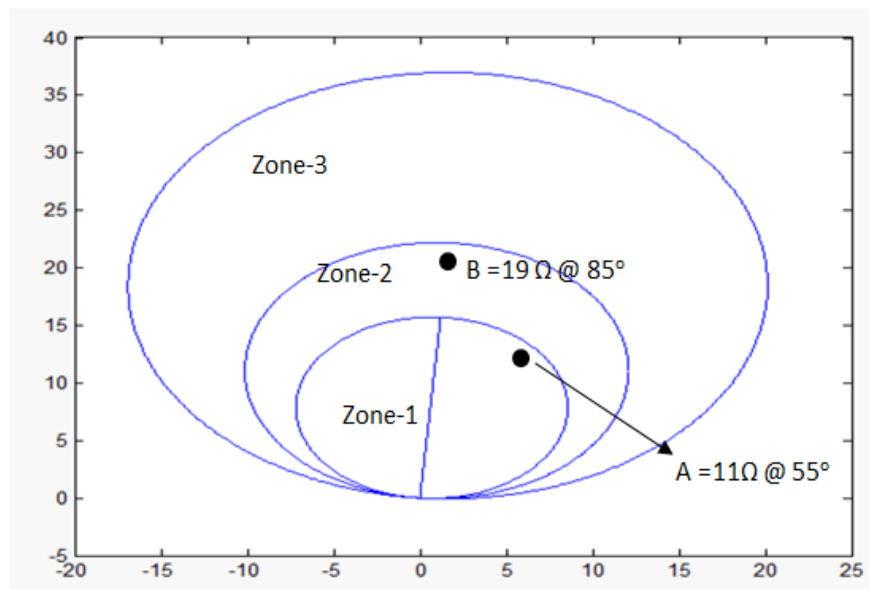
Figure 3-16 Example of the impact of PT blown fuse on distance relay.

3.5   Summary

Hidden failures in protection systems are defects that become apparent during switching and/or fault events in power system network and cause protection system to misoperate. They might widen power system interruption by isolating healthy portions of the power system. Each component in a protection system is vulnerable to hidden failures. However, the protective relays and the instrumentation channels are more vulnerable to the hidden failures due to their massive population in the substations. For the protective relays, the most common hidden failure modes are the incorrect setting and logic of the IEDs. For the instrumentation channels the most common hidden failures modes are blown fuse, CT saturation, CT short circuit, CT reverse polarity, and wrong CT ratio setting. These failures in the instrumentation channels cause the protective device to read incorrect measurement which might cause a relay misooperation or nonoperation for an external fault or an internal fault respectively.

CHAPTER 4.   PROPOSED RESEARCH

4.1   Introduction

This chapter provides an overview of the proposed dynamic sate estimation-based centralized protection scheme (DSEBCPS). The scheme name implies that it employs the dynamic state estimation approach to secure zone level protection system against hidden failure. The objective of the scheme is to continually monitor zone-level protection, detect hidden failures, and correct compromised data. We propose integrating the DSEBCPS with settingless relays to secure their operation against hidden failures. The DSEBCPS works along with the settingless relays to form a resilient protection system. We have implemented the proposed scheme in an object-oriented manner, which requires expressing the substation model and measurement model in the standard form known as the state and control algebraic quadratic companion form (SCAQCF). The substation model in the SCAQCF format is used directly by the dynamic state estimation algorithm, which is the main process in the proposed scheme.

4.2   Overall Approach

The DSEBCPS is a substation-centralized protection scheme that monitors zone-level relays (i.e., settingless protection relays) in real time to secure their operation against potential hidden failures. As depicted in Figures 4-1 and 4-2, the DSEBCPS inside the dotted frame is a second layer that monitors the operation of all settingless relays in a substation. The DSEBCPS communicates with the settingless relays via the station bus and obtains essential information from each protection zone, such as phasor quantities and breaker and disconnect status. This information is processed by the DSEBCPS to extract

the substation topology and states. Specifically, the DSEBCPS performs dynamic state estimations in the quasi-dynamic domain at sampling rate defined by the user to detect any sort of abnormality within the substation. The DSEBCPS measures the consistency between the phasor quantities obtained from the settingless relays and the quasi-dynamic model of the substation. Any inconsistency between the measurements and the model is detected by performing the chi-square test, which computes the probability that the measurements fit the model [62], [63]. We refer to this probability as the "confidence level" [64]. A high confidence level (i.e., close to 1) indicates a healthy substation; lower values indicate a faulty one. It is vital to emphasize the object-oriented approach in our implementation of the DSEBCPS. Such an approach is depicted in Figure 4-2, which shows that the scheme is built through several objects, such as a substation model, measurement model, measurement definition, and dynamic state estimation algorithm.

Upon detecting abnormalities in the substation through a low confidence level, an additional process is needed to distinguish whether this abnormality has resulted from a fault or hidden failure. For this purpose, we propose performing hypothesis testing, which entails identifying a set of suspicious measurements, removing them one at a time, and performing dynamic state estimation every time a suspicious measurement or set of suspicious measurements are removed. If the removal process reveals a high confidence level, the eliminated suspicious measurements suffer from abnormalities. Moreover, if the suspicious measurements represent a complete zone (i.e., all of them are used to model the zone), a power fault is detected in the zone. Furthermore, if the suspect measurements do not represent the whole zone, hidden failure in the suspect measurement is detected. The effectiveness of the hypothesis testing depends on the level of redundancy in

measurements. Because all protective relays (i.e., settingless relays) stream their

measurements to the DSEBCPS, the redundancy is quite high, typically 2,000% [36]. This

means that the measurements are twenty times more than the number of states describing

the operation of the substation. This high level of redundancy results in higher residuals

(the error between the estimated and measured value) for the bad data and minimizes the

possibility of bad measurements acting as leverage points [64], [65]. This property enables

fast convergence of the hypothesis testing. The DSEBCPS classifies measurements with

high residuals as suspect measurements [66]. Then it starts the removal process with the

measurement (or set of measurements) of the highest residual(s). More details about

hypothesis testing are presented in Chapter 5.

Upon detecting hidden failures, the DSEBCPS computes the sampled values

corresponding to the detected bad data to the settingless relay to replace the bad

measurements. To facilitate this process, a delay of two cycles is introduced in the

operation of the settingless relay. Upon replacing the bad measurements, the confidence

level of the zone under protection recovers from its low level. Subsequently, the relay will

not initiate a trip signal. Accordingly, the DSEBCPS increases the settingless relay's

security without jeopardizing the dependability. Figure 4-3 depicts the overall concept of

the DSEBCPS. More details about every process in the DSEBCPS are presented in Chapter

5.
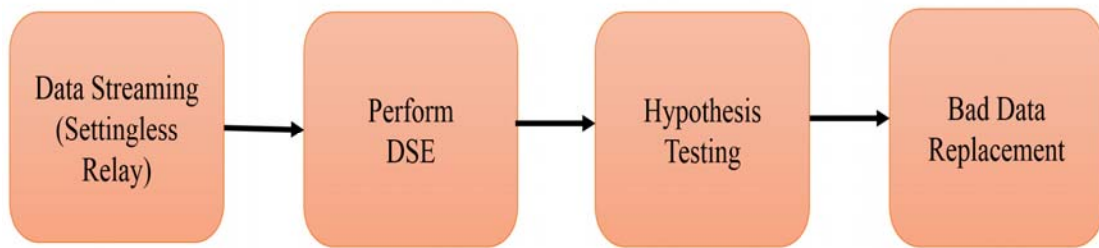
Figure 4-1 DSEBCPS overall concept.
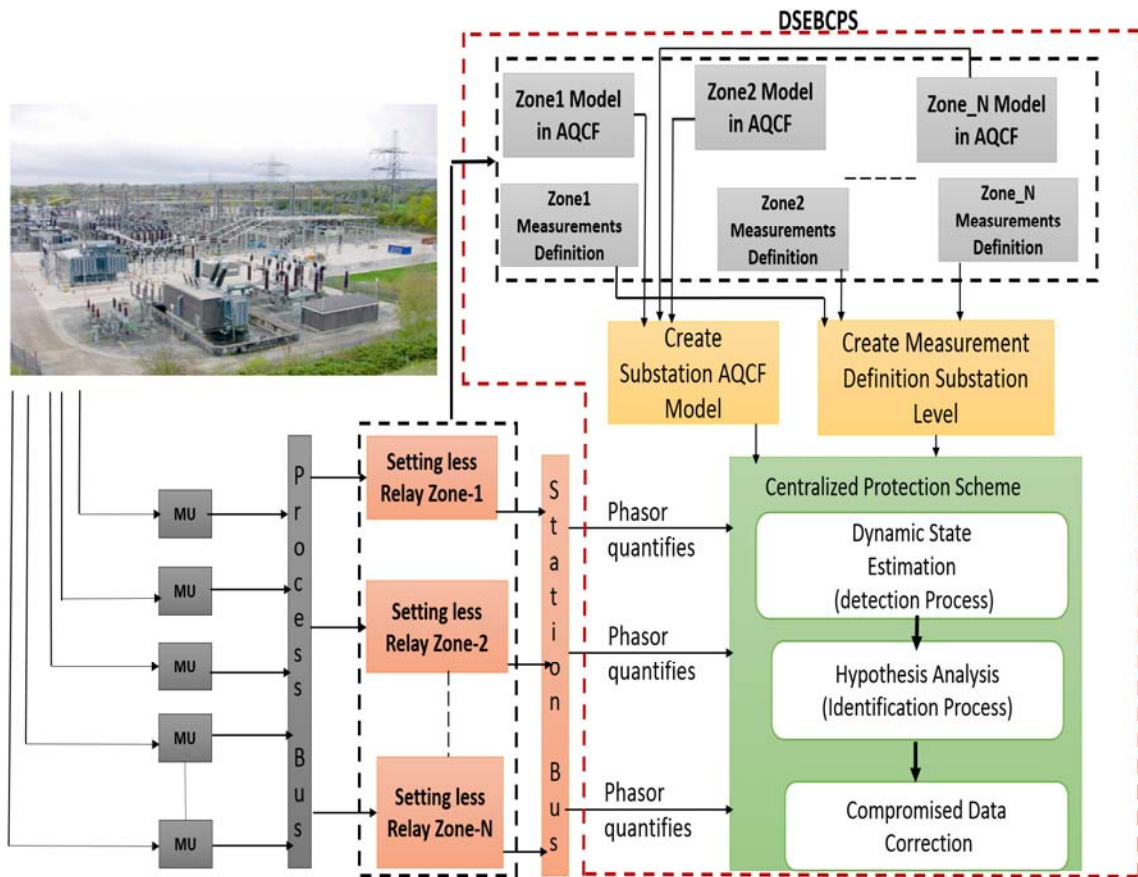
Figure 4-2 DSEBCPS overall architecture.
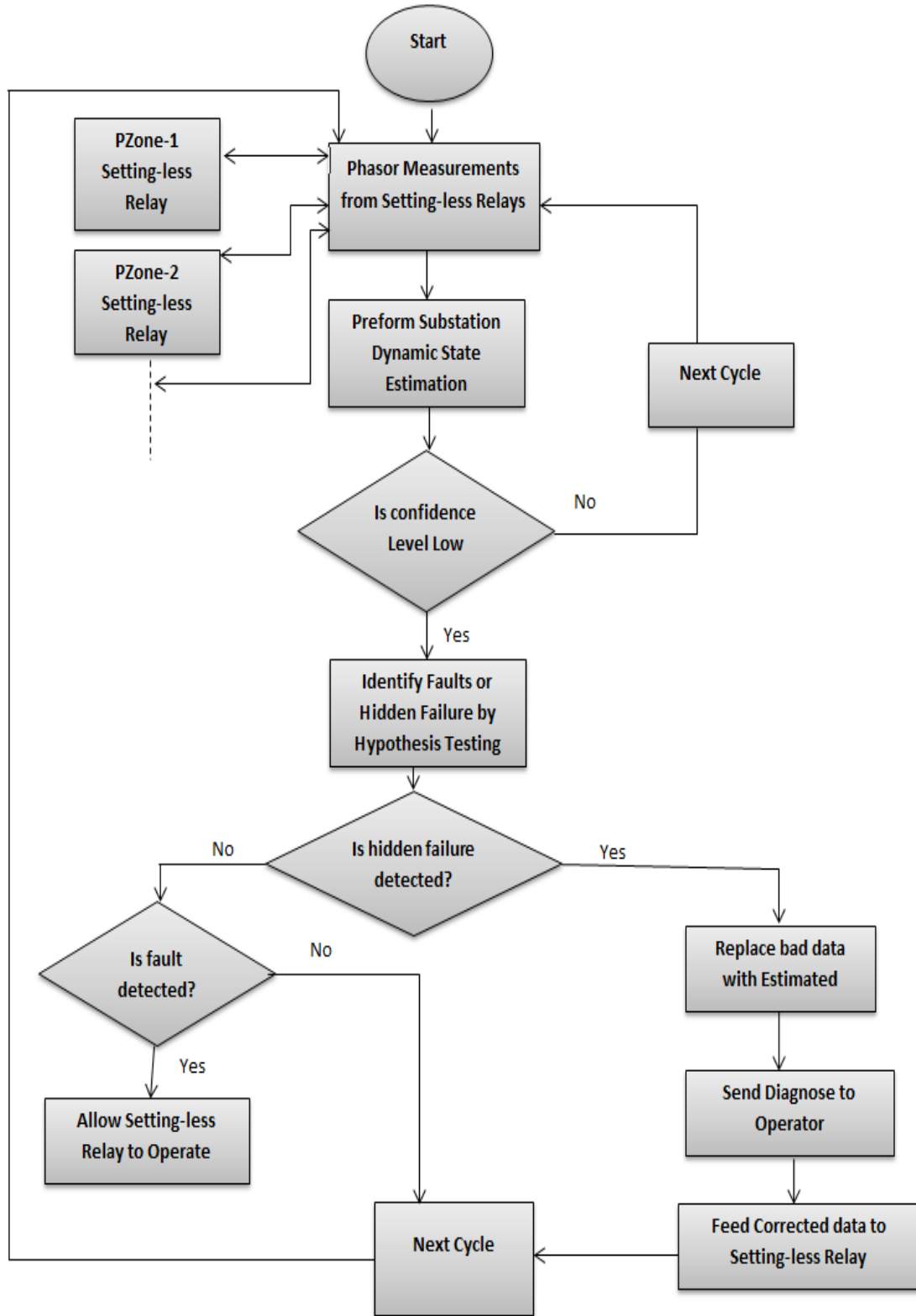
Figure 4-3 Flow chart for the DSEBCPS overall concept.

4.3   Summary

The DSEBCPS supervises the individual settingless relays to secure their operations against hidden failures. The process starts with data streaming from the settingless relay to the DSEBCPS, which processes the data by performing DSE. This process verifies the consistency between the measurements and the substation model. Upon detecting inconsistency through the chi-square test, the DSEBCPS performs hypothesis testing to detect hidden failures. Upon detecting hidden failures, the DSEBCPS initiates bad data replacement to secure the settingless relay from misoperation.

CHAPTER 5.   SUBSTATION-CENTRALIZED PROTECTION

SCHEME

5.1   Introduction

This chapter discusses the mathematical formulation of the proposed centralized protection scheme. It starts with a discussion about the object-oriented approach used in our design, then moves on to the substation and measurement models. The modeling section is followed by the formulation of the dynamic state estimation that monitors the settingless relays and detects substation abnormality. Then hypothesis testing, which is used to further classify the abnormality as a faulty zone or hidden failure, is discussed in detail. Finally, we present the process of replacing the compromised measurement.

5.2   Object-Oriented Approach

The object-oriented approach is generally employed in developing a specific application by using the object oriented paradigm, which entails dividing the application into a set of objects that interact with each other to perform the overall function. This approach has many advantages, including that it will [67]:

- Provide a unified syntax to each component of the proposed application, which supports larger-scale implementation. This advantage is depicted in our proposed DSEBCPS by defining several components: (1) substation model extraction, which reads an external file to extract the substation model; (2) measurement model development; (3) dynamic state estimation computation; (4) hypothesis testing; and

(5) bad data replacement. Each component has been designed to accommodate different substation designs.

- Simplify the interaction between the different components of the proposed application in a reliable manner. For example, in our design of the DSEBCPS, the measurement models' developments rely on the information provided by the substation model extraction module. Similarly, the dynamic state estimation computation components use the measurement models in performing DSE.

- Facilitate the expansion of the application to accommodate additional functions. For example, in our design of the DSEBCPS, every function represents an object so that any additional functions can be integrated as additional objects.

- Enable integration with other applications to perform a system-level application. For example, the DSEBCPS at every substation can be using the energy management system in the control center to perform dynamic state estimation at the system level.

5.3   Phasor Extraction

The DSEBCPS performs dynamic state estimation in the quasi-dynamic domain, which is the domain that neglects electrical transient phenomena and uses phasor quantities. Therefore, phasor quantities need to be computed from the sample values used in the settingless relay. These phasor quantities have been computed using Fourier series expansion, which allows us to express the sampled waveform x(t) as follows:

$$x(t) = a_1 \cos(wt) + a_2 \sin(wt) + harmonics \tag{5.1}$$

To compute the parameters a₁ and a₂ efficiently, we propose using the circular array-based algorithm as illustrated in Figure 5-1 [68]. To explain the algorithm, consider a sampled value of x(i) and two sets of circular arrays with N entries each. The entries of the circular buffers are initialized to zero. Then the process starts by computing the values y(i) and z(i) for each sampled value as follows:

$$y(i) = x(i)\cos(W_0 Ti) \tag{5.2}$$

$$z(i) = x(i)\sin(W_0 Ti) \tag{5.3}$$

where x(i) is the sampled value at sample i, W_0 is the frequency, and T is the period of the sampled waveform.

After each sample, the values of V₁(k) and V₂(k) are computed as follows:

$$V_1(k) = \sum_{i=k}^{k+N-1} y(i) \tag{5.4}$$

$$V_2(k) = \sum_{i=k}^{k+N-1} z(i) \tag{5.5}$$

For each new sample beyond the first N samples, the values V₁(k) and V₂(k) are updated as follows:

$$V_1(k) = V_1(k-1) + y(i) - y(i-N) \tag{5.6}$$

$$V_2(k) = V_2(k-1) + z(i) - z(i-N) \tag{5.7}$$

where $y(i-N)$ and $z(i-N)$ are the oldest values in the circular buffer that will be overwritten by introducing the latest values of $y(i)$ and $z(i)$.

49

Finally, the phasor values are computed as follows:

$$\tilde{x}(k) = \frac{\sqrt{2}}{N}(V_1(k) + V_2(k)) \tag{5.8}$$
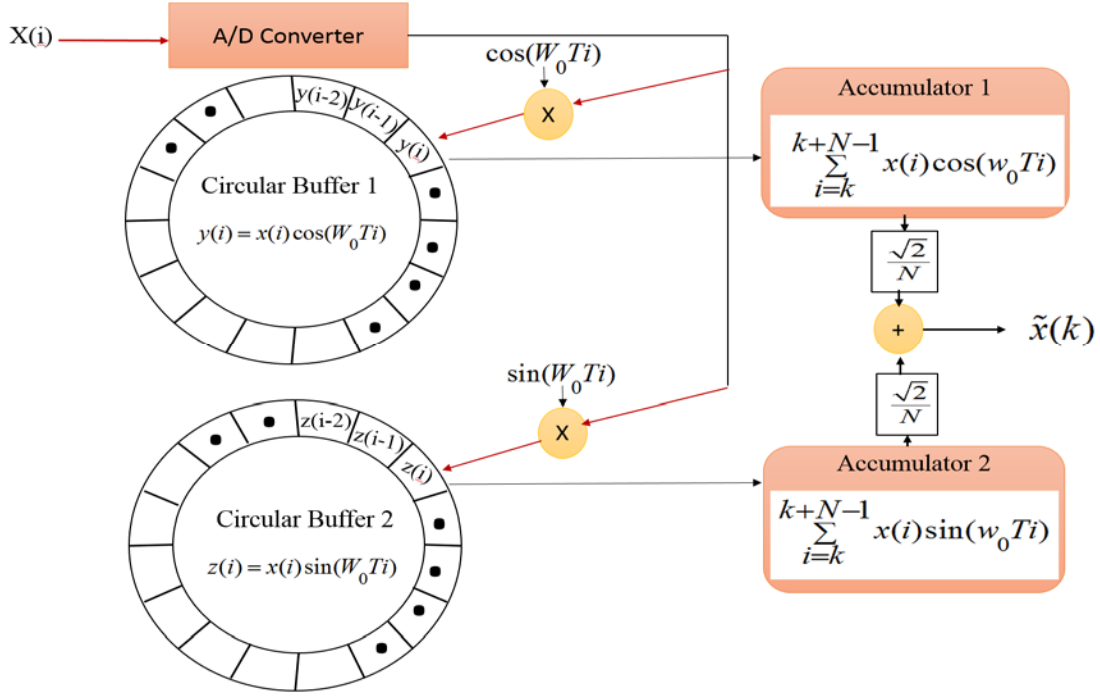
Figure 5-1 Illustration of circular buffer implementation for phasor extraction.

5.4 Substation Model

This section demonstrates the process of developing the substation quasi-dynamic model in state and control algebraic quadratic companion form (SCAQCF), which relates a set of through variables originating from the physical model of the substation to the state and control variables of the substation. The SCAQCF is a mathematical model derived from the physical model of the power system devices in the substation. Therefore, the substation model is a collection of the individual devices' models within the substation.

5.4.1 Quadratized Dynamic Model (QDM)

The first step in developing the substation model is to derive the substation physical model, which consists of a set of linear and nonlinear algebraic and differential equations. These equations are derived from the physical model of the power system devices located in the substation. The second step is to quadratize the model to reduce the nonlinearities of order to no greater than two. This step is achieved by introducing new state variables. Thus, the model consists of only linear and quadratic terms. The model in this format is referred to as the quadratized dynamic model (QDM), which has the following standard format:

$$\tilde{I}(t) = Y_{eqx1}\tilde{\mathbf{x}}(t) + Y_{equ1}\tilde{\mathbf{u}}(t) + D_{eqxd1}\frac{d\tilde{\mathbf{x}}(t)}{dt} + C_{eqc1} \tag{5.9}$$

$$0 = Y_{eqx2}\tilde{\mathbf{x}}(t) + Y_{equ2}\tilde{\mathbf{u}}(t) + D_{eqxd2}\frac{d\tilde{\mathbf{x}}(t)}{dt} + C_{eqc2} \tag{5.10}$$

$$0 = Y_{eqx3}\tilde{\mathbf{x}}(t) + \left\{ \begin{matrix} \vdots \\ \tilde{\mathbf{x}}(t)^T \left\langle F^i_{eqxx3} \right\rangle \tilde{\mathbf{x}}(t) \\ \vdots \end{matrix} \right\} + \left\{ \begin{matrix} \vdots \\ \tilde{\mathbf{u}}(t)^T \left\langle F^i_{equu3} \right\rangle \tilde{\mathbf{u}}(t) \\ \vdots \end{matrix} \right\} +$$
$$\left\{ \begin{matrix} \vdots \\ \tilde{\mathbf{u}}(t)^T \left\langle F^i_{equx3} \right\rangle \tilde{\mathbf{x}}(t) \\ \vdots \end{matrix} \right\} + C_{eqc3} \tag{5.11}$$

where $\tilde{I}(t)$ are through variables; $\tilde{x}(t)$ are the external and internal state variables of the substation model; $\tilde{u}(t)$ are control variables of the device model; Y_{eqx} is a matrix defining the coefficients of the state variables for the linear part; F_{eqxx}, F_{equu}, and F_{equx} are matrices defining the coefficients of the state variables for the quadratic part; and D_{eqxd} is a matrix defining the coefficients of the state variables for the differential part.

51

The QDM standard format has three sets of equations. The first set is composed of external equations that relate the terminal currents to the state variables. The second set is internal equations needed to satisfy the physical model of the substation and consists of only linear terms. The third set is also composed of internal equations that contain quadratic terms.

5.4.2 State and Control Algebraic Quadratic Companion Form (SCAQCF)

The third step in developing the substation model is to eliminate the differential terms through an integration process. For such a process, we propose a quadratic integration that assumes the functions of the integrated waveform vary quadratically within an integration time step, as shown in Figure 5-2 [69]. The figure illustrates that the quadratic functions are defined by three points: $x(t - h)$, x_m, and $x(t)$ within the interval $[t - h, t]$. The quadratic integration has the advantage of improving accuracy and numerical stability and minimizing numerical oscillations. The quadratic integration results in a set of SCAQCF with the following standard format:

$$
\begin{Bmatrix} \tilde{I}(t) \\ 0 \\ 0 \\ \tilde{I}(t_m) \\ 0 \\ 0 \end{Bmatrix} = Y_{eqx}\tilde{\mathbf{x}} + \begin{Bmatrix} \vdots \\ \tilde{\mathbf{x}}^T \left\langle F_{eqx}^i \right\rangle \tilde{\mathbf{x}} \\ \vdots \end{Bmatrix} + Y_{QDequ}\tilde{\mathbf{u}} + \begin{Bmatrix} \vdots \\ \tilde{\mathbf{u}}^T \left\langle F_{equ}^i \right\rangle \tilde{\mathbf{u}} \\ \vdots \end{Bmatrix} +
$$

$$
\begin{Bmatrix} \vdots \\ \tilde{\mathbf{u}}^T \left\langle F_{equx}^i \right\rangle \tilde{\mathbf{x}} \\ \vdots \end{Bmatrix} - B_{eq}
$$

(5.12)

$$
B_{eq} = -N_{eq,x}\tilde{\mathbf{x}}(t-h) - N_{eq,u}\tilde{\mathbf{u}}(t-h) - M_{eq}\tilde{I}(t-h) - K_{eq}
$$

(5.13)

where t_m is midpoint of the integration step; $[i(t), i(t_m)]$ are through variables, which are substation terminal currents that flow into the device at times t and t_m; $[x(t), x(t_m)]$ are external and internal state variables of the device model at times t and t_m; $[u(t), u(t_m)]$ are control variables of the device model at times t and t_m; Y_{eqx} is a matrix defining the coefficients of the state variables for the linear part; F_{eqx}, F_{equ}, and F_{equx} are matrices defining the coefficients of the state variables for the quadratic part; B_{eq} is a constant past history–dependent vector; N_{eqx} is a matrix defining the coefficients of the state variables associated with the last integration step; M_{eq} is a matrix defining the coefficients of the through variables associated with the last integration step; and K_{eq} is a constant vector.
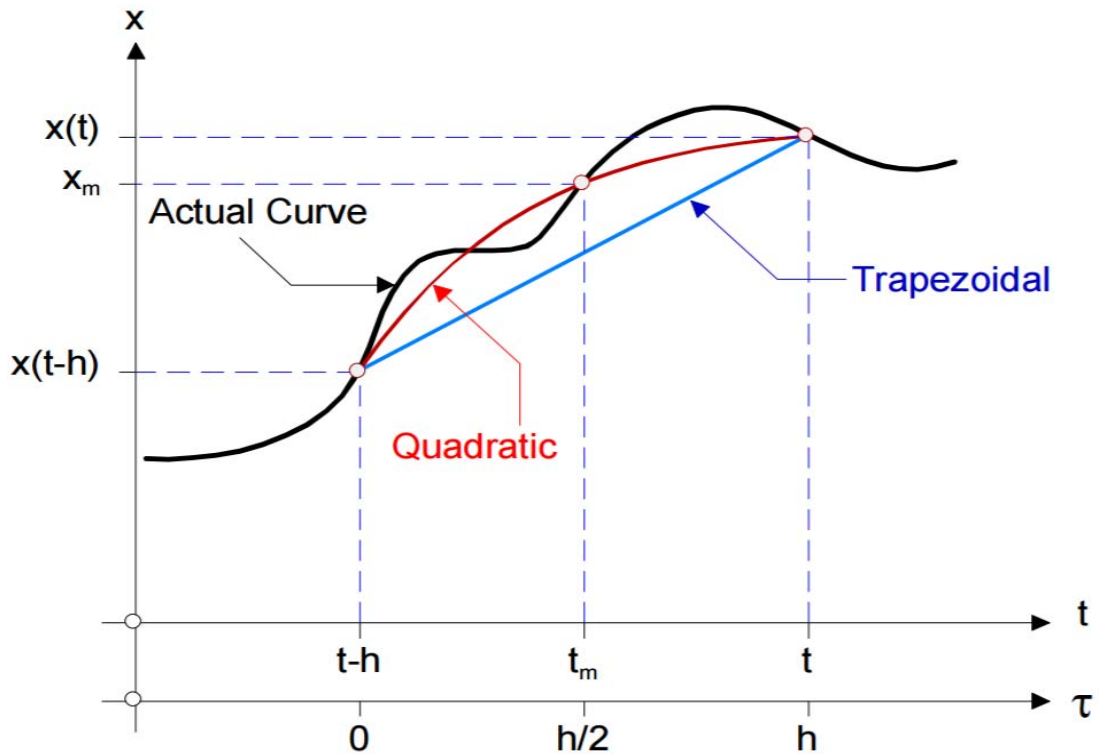
Figure 5-2 Quadratic function [69].

53

5.5 Substation Measurement SCAQCF Model

The substation model explained in the previous section is used to derive the measurements model in the SCAQCF standard. These measurements of the substation have four types:

1. Actual measurements, which are real measurements, such as voltage and current measurements, obtained from measurement devices and assigned a percentage error equal to the standard deviation of the measurement devices. Usually, these measurements, such as the current measurements, are modeled by using the corresponding equation in the substation models. Also, some of these measurements, such as the voltage measurements, are modeled directly by the state variables.

2. Derived measurements, which are derived from actual measurements, such as the neutral current of the transformer. Usually, these measurements are modeled by the corresponding equations in the substation models.

3. Pseudo measurements, which are measurements for quantities that are normally not measured, such as the voltage of the neutral. For such quantities, we can assume a certain value (i.e., zero for neutral voltages) and assign a relatively large measurement error.

4. Virtual measurements, which represent the zero value on the left-hand side of the equations. These measurements originate from the physical model of the substation. Usually, they are assigned a small percentage error.

The models for all measurements are stacked with each other to form the SCAQCF model of the measurements, which has the following standard format:

$$\tilde{\mathbf{z}} = Y_{qm,x}\tilde{\mathbf{x}} + \left\{ \begin{matrix} \vdots \\ \tilde{\mathbf{x}}^T F^i_{qm,x}\tilde{\mathbf{x}} \\ \vdots \end{matrix} \right\} + Y_{qm,u}\tilde{\mathbf{u}} + \left\{ \begin{matrix} \vdots \\ \tilde{\mathbf{u}}^T F^i_{qm,u}\tilde{\mathbf{u}} \\ \vdots \end{matrix} \right\} + \left\{ \begin{matrix} \vdots \\ \tilde{\mathbf{u}}^T F^i_{qm,ux}\tilde{\mathbf{x}} \\ \vdots \end{matrix} \right\} + C_{qm} \qquad (5.14)$$

$$C_{qm} = N_{qm,x}\tilde{\mathbf{x}}(t-h) + N_{qm,u}\tilde{\mathbf{u}}(t-h) + M_{qm}\tilde{I}(t-h) + K_{qm} \qquad (5.15)$$

where $\tilde{z}$ is the measurement quantity at times t and t_m; Y_{eqx} is a matrix defining the coefficients of the state variables for the linear part; $F_{eqx}, F_{equ},$ and F_{equx} are matrices defining the coefficients of the state variables for the quadratic part; B_{eq} is a constant past history–dependent vector; N_{eqx} is a matrix defining the coefficients of the state variables associated with the last integration step; M_{eq} is a matrix defining the coefficients of the through variables associated with the last integration step; and K_{eq} is a constant vector.

5.6 Dynamic State Estimation at Substation Level

In the proposed scheme, the dynamic state estimation method is used to compute the best estimate of the state variables for the substation. These computed states are used to calculate the estimated measurement using the substation model. The state estimation performance is analyzed through a chi-square test, which measures the goodness of fit between the measurements and the substation model. The goodness of fit is quantified by what is known as the confidence level. Therefore, a high confidence level indicates that the measurements' fit with the model and the substation is healthy. The following subsection details the process of the dynamic state estimation formulations.

5.6.1 Weighted Least-Square Method

We have used the weighted least-square method to formulate the dynamic state estimation at the substation level. This formulation is started by expressing the measurements in terms of the state variables of the substation as follows:

$$\tilde{z}_k(t) = h_k(x) + \eta = Y_{qm,x}\tilde{\mathbf{x}} + \left\{\begin{array}{c} \vdots \\ \tilde{\mathbf{x}}^T F^i_{qm,x}\tilde{\mathbf{x}} \\ \vdots \end{array}\right\} + C_{qm} + \eta \qquad (5.16)$$

where z is the measurements; x is the state variables; $Y_{qm,\,x}$ is the coefficient matrix of the linear terms; $F_{qm,x}$ is the coefficient matrix of nonlinear terms; C_{qm} is the constant term; and η is the measurement error.

Then the WLS method is formulated as an optimization problem with an objective function to minimize the error as follows [64], [65], [70]:

$$Minimize \quad J = \sum_{i=1}^{n}\left(\frac{h_i(x) - z_i}{\sigma_i}\right)^2 = \sum_{i=1}^{n} s_i^2 = \eta^T W \eta \qquad (5.17)$$

where $s_i = \frac{\eta_i}{\sigma_i}$, $W = diag\left\{\cdots,\frac{1}{\sigma_i^2},\cdots\right\}$, and σ_i is the standard deviation of the meter by which the corresponding measurement z is measured.

For the nonlinear case, the solution is given with Newton's iterative algorithm as follows:

$$x^{V+1} = x^V - (H^T W H)^{-1} H^T W (h(x^V) - z) \qquad (5.18)$$

where H is the Jacobean matrix computed as follows:

$$H = \frac{\delta h(x)}{\delta x}$$

(5.19)

For the linear case, the solution is given as follows:

$$X = (H^T W H)^{-1} H^T W (Z - C).$$

(5.20)

5.6.2   Abnormality Detection

Abnormality detection is achieved by performing the chi-square test, which calculates the goodness of fit between the measurement and the substation model. The goodness of fit is quantified by the confidence level. A high confidence level indicates a healthy substation, and a low confidence level indicates an abnormality. The chi-square test is computed as follows [64]:

$$\xi = \sum_{k=0}^{n} (\frac{h_k(x) - \tilde{Z}_k(t)}{\delta})^2$$

(5.21)

$$V = m - n$$

(5.22)

$$\Pr(\chi^2 \leq \xi) = P(\xi, V)$$

(5.23)

$$\text{Confidence level} = \Pr(\chi^2 \geq \xi) = 1 - P(\xi, V)$$

(5.24)

where the ξ variable in equation 5.21 is the summation of normalized residuals, which have a Gaussian distribution within the range of -1 to 1. The variable V in equation 5.22 represents the degree of freedom, which is the difference between the number of the measurement (m) and the number of the states (n). The term $\Pr(\chi^2 \leq \xi)$ in equation 5.23 is the chi-square probability distribution function, which is shown in Figure 5-3. It represents

the probability that the summation of the normalized residuals is out of the bounds. In fact, it is the probability that the measurements do not fit the model. Accordingly, this probability is used in equation 5.24 to compute the confidence level which is the probability that the measurements fit the substation model.
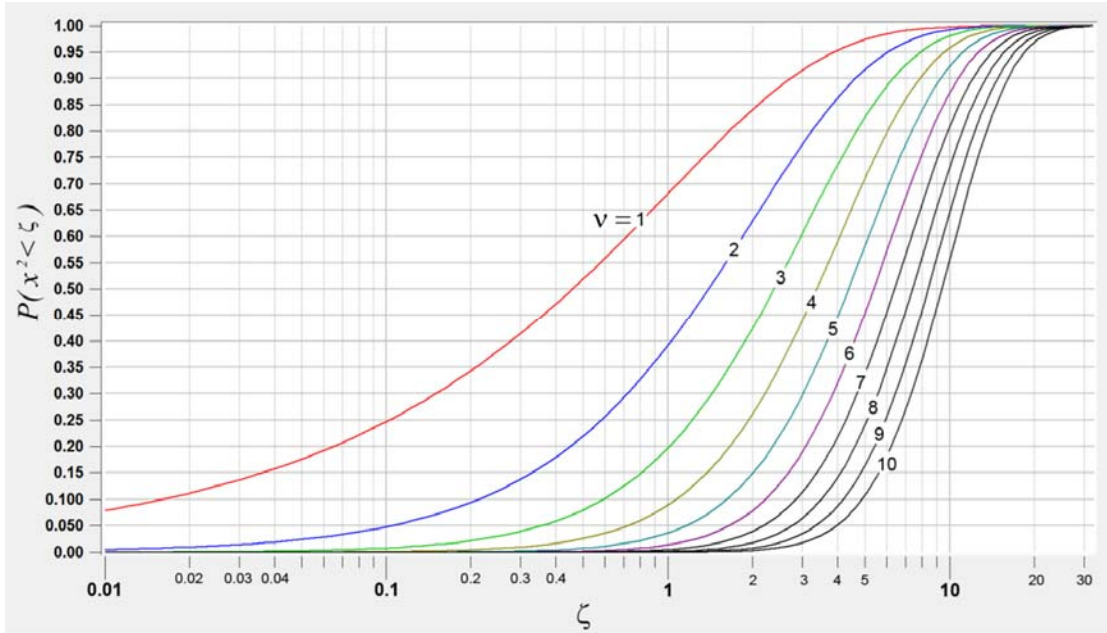
Figure 5-3 Chi-square probability distribution function [64].

5.7 Hypothesis Testing

This module is initiated when the dynamic state estimation has declared the existence of bad data (data abnormality). The objective of this module is to identify the root cause of the abnormality which is either power fault or hidden failure. In this context we have three possible cases: (1) one or more power faults exist in the substation or any of the interconnected circuits, (2) one or more hidden failures exist in the overall system (3) both faults and hidden failures exist in the substation. The probability of having two simultaneous faults or two simultaneous hidden failures within the substation is very low.

58

However two concurrent events of hidden failure and power fault in the substation are more likely to occur. Therefore, our design for this module takes into consideration two scenarios (a) single event of either hidden failure or power fault and (b) two concurrent even of both hidden failure and power fault.

To identify the type and location of the abnormality, we propose using hypothesis testing. The enabler for such approach is the high redundancy in the measurements at the substation level [36], [62]. This redundancy minimizes the possibility of leverage point. Therefore, the measurements with abnormality will always experience higher residual error than the healthy ones. Accordingly, the hypothesis testing starts by characterizing the measurements as suspect based on the values of their normalized residuals. Typically the measurements with the highest normalized residual are considered as suspicious measurements. The Normalized residual is computed during the DSE computation with:

$$nr_i = \left(\frac{h_i(\hat{x}) - z_i}{\sigma_i} \right) \tag{5.25}$$

where nr_i is the normalized residual for measurement i, $h_i(\hat{x})$ is the calculated measurement using the estimated substation states, z_i is the measurement i, and σ_i is the standard deviation of the meter error.

To classify the abnormality to either hidden failure or power fault we introduce the concept of device common mode criteria which enables grouping multiple suspicious measurements into one set if they are modeled by a single device and their normalized residuals exceed threshold of 2. There are two device common mode criteria: (1) a zone

common mode criterion which allows grouping all the measurements associated with a zone, for which settingless relay is operated, into a one set of suspicious measurements if their normalized residuals exceed 2 and (2) an instrumentation channel common mode criterion which enables grouping the measurements extracted from an instrumentation channel if their normalized residual exceed threshold of 2.

Our design considers three types of hypotheses. The first hypothesis considers bad measurements only as a result of hidden failure. This hypothesis involves selecting the measurement with the highest normalized residual and subjecting it to instrumentation channel common mode criterion to identify the associated instrumentation channel. For this particular hypothesis, we also verify the measurements associated with the instrumentation channels of the adjacent phases. If they exceed a threshold of 2, they are included in the set of the suspicious measurements. The set of suspicious measurements and the models of their instrumentation channels are removed from the measurement set and substation models respectively. Then the DSEBCPS reruns the DSE. If this process reveals high confidence level, hidden failure is detected in the instrumentation channels corresponding to the removed models and measurements. The second hypothesis is a power fault in the zone for which the settingless relay is operated. This hypothesis involves selecting the measurements with highest value of normalized residual and subjecting it to zone common mode criterion. If the residuals exceed a threshold of 2, the measurements are included in the set of the suspicious measurements. The set of suspicious measurements and the models of their zone are removed from the measurements set and substation model respectively. Then the DSEBCPS reruns the DSE. If this process reveals high confidence level power fault is detected in the zone corresponded to the removed models and

measurements. The third hypothesis is both hidden failure in an instrumentation channel and power fault in a zone. The two sets of suspicious measurements considered in the previous two hypotheses are grouped as one set of suspicious measurements. Then, this set of measurements is removed with their associated models. A successful outcome of the third hypothesis indicates a detection of both hidden failure and power fault.

Figure 5-4 depicts our proposed design for the hypothesis testing. The overall concept is to identify a suspicious measurement (i.e., the measurement with the highest normalized residual). Then, the suspicious measurement is verified for the device common mode criteria to identify the hypothesis under consideration and group suspicious measurements according to the selected hypothesis. More specifically, the instrumentation channel common mode criterion results in selecting the first type of hypothesis which is hidden failure in instrumentation channel. Furthermore, the zone common mode criterion results in selecting the second type of hypothesis which is power fault in the corresponding zone. In case of single event, the DSEBCPS selects the first or second type of hypothesis based on the device common mode criteria, removes suspicious measurements from substation measurements and the corresponding device model from substation model and reruns the DSE. High confidence level indicates a successful hypothesis and abnormality is identified based on the selected hypothesis. In case of two simultaneous events the process is summarized in the following points:

1- The DSEBCPS starts with either hypothesis type1 or type 2 based on the qualified device common mode criterion. This hypothesis will fail because of the second abnormality.

2- The DSEBCPS moves to the second hypothesis during which it verifies the normalized residual for all measurements that are not included in the removal process during the first hypothesis, picks the highest normalized residual, verifies the device common mode criteria, groups the suspicious measurements, removes suspicious measurements, and reruns the DSE. This hypothesis will fail because of the second abnormality.

3- It is important to note that if the hypothesis is not successful, the removed set of measurements must be returned to the list of the measurements.

4- The DSE moves to the third hypothesis which combines the previous two types. This hypothesis should be successful in restoring high confidence level of the substation.

5- It is important to note that during the two concurrent events the redundancy in the measurements at the substation level will guarantee the convergence of the hypothesis testing. In other words, this redundancy will enable the successful performance of the hypothesis algorithm.
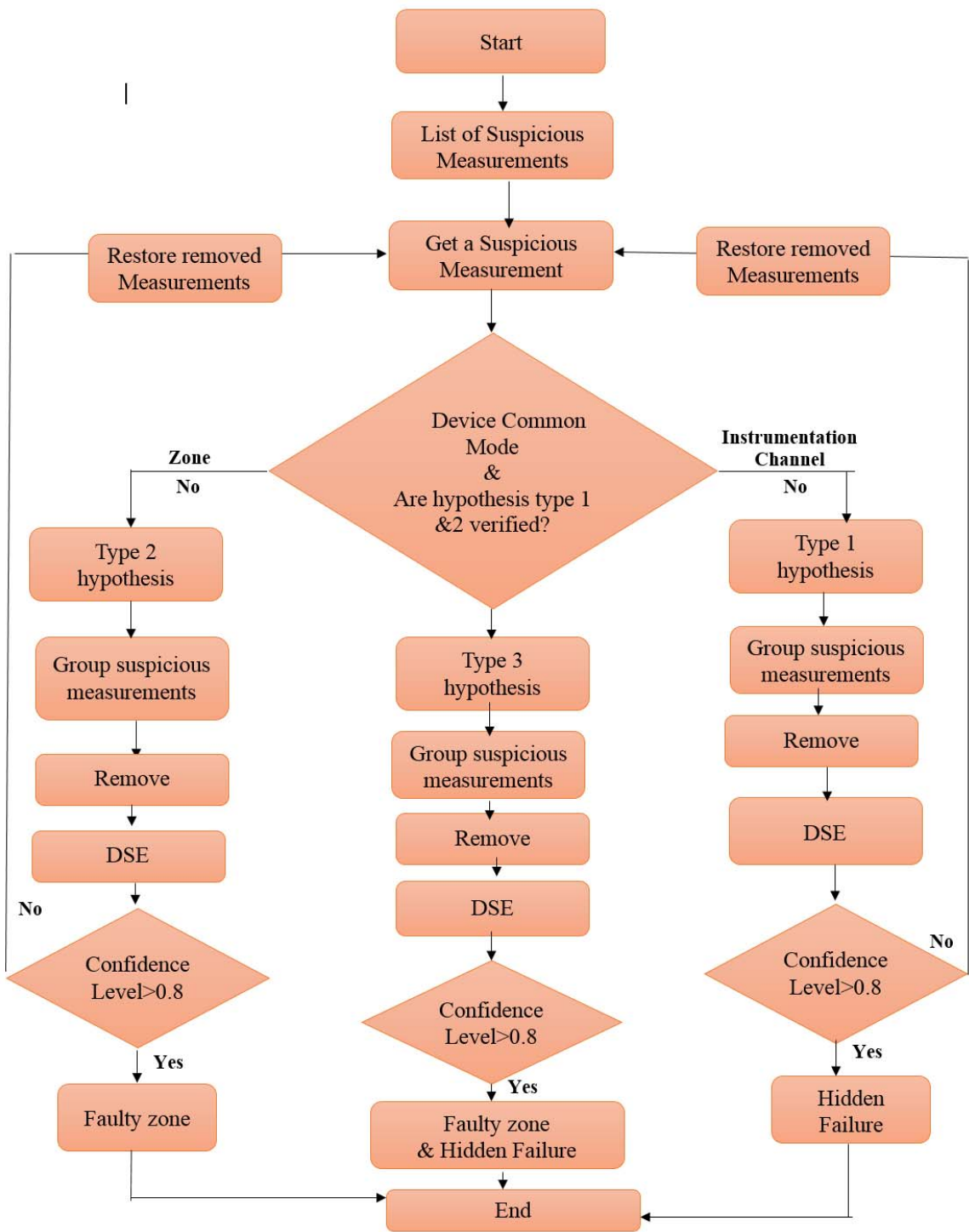
Figure 5-4 Flow chart of the hypothesis testing

5.8 Data Correction

The DSEBCPS uses the substation states to compute the estimated values of measurements using the substation models. These calculated measurements are used to compute the sampled values corresponding to the compromised measurements with the following equation:

$$X_m = A_m \cos\left(w \bullet t_m + \theta_m\right)$$

(5.26)

where X_m is the estimated signal, A_m is the estimated magnitude computed in the DSEBCPS, and θm is the estimated angle computed in the DSEBCPS.

Upon calculating the sampled values of the compromised measurements, the DSEBCPS streams these values to the corresponding position in the circular buffers of the process bus at the same rate and in sync with the merging units. Note that this data override the compromised data in the circular buffers. Then the settingless relay, which suffers from hidden failures, will be automatically using the corrected data and the operation of the settingless relay will reset accordingly. To facilitate this process, we propose introducing a delay of two cycles in the operation of the settingless relay to allow the DSEBCPS to perform the computational procedures and start replacing the compromised data, if necessary, in less than two cycles. This means that the DSEBCPS must have the computational speed to complete its tasks in about 1.75 cycles or less. The breakdown of these two cycles is illustrated in Figure 5-5.
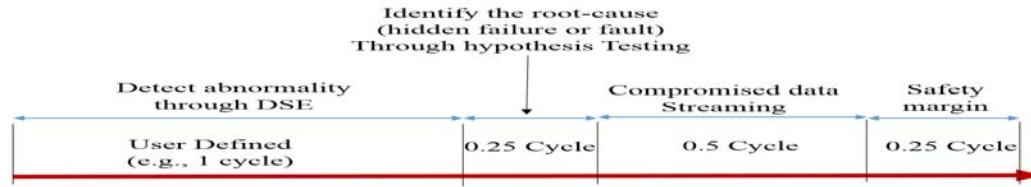
Figure 5-5 Breakdown of Time-delay for the settingless relay.

5.9   Summary

This chapter provides the theoretical details of the dynamic state estimation-based centralized protection scheme. The concept requires an accurate substation model, which is a collection of the devices' models within the substation. This model is used to derive the measurements' models, which are used in the dynamic state estimation formulation. This formulation entails defining an optimization problem with the objective to minimize the error between the actual and calculated measurements. The output of the DSE is the best estimate of the substation state variables. The DSE performance is quantified through the confidence level calculated through the chi-square test. The confidence level measures the consistency between the measurements and their models. Accordingly, if the confidence level is high, the substation is healthy; otherwise, there is an abnormality in the substation. This abnormality is further classified as a hidden failure or faulty condition through hypothesis testing. Finally, upon detecting the hidden failure, the DSEBCPS streams the calculated sampled values corresponding to the detected compromised measurements to the sample valued circular buffers at the same rate and in sync with the merging units to override the compromised measurements. This process ensures that the settingless relays will always operate with validated data. To facilitate this process and secure the settingless relay from initiating the trip signal, two cycles delay is introduced.

65

CHAPTER 6.   NUMERICAL EXPERIMENTS OF DSEBCPS

The concept of DSEBCPS is simulated for a relatively small substation which comprises five protection zones, as shown in Figures 6-1 and 6-2. The objective of this simulation is to demonstrate the concepts explained in Chapters 4 and 5 and show that the system can be implemented on a larger scale. The substation is fed by a 115 kV system via a 115 kV transmission line. The five protection zones are: (a) the 115 kV transmission line, (b) the 115 kV bus, (c) the 115kV/13.8 kV 36 MVA transformer, (d) the 13.8 kV bus, and (e) the 13.8 kV distribution line. For simplicity, Figure 6.2 shows only the instrumentation channels connected to burdens (i.e., settingless relays). This substation has a total of 202 measurements (considering real and imaginary quantities for each phase) and 38 states, resulting in a redundancy of 513%. Note the redundancy is lower than what will be experienced in a typical substation and therefore represents worse conditions from an actual substation case. We used this substation to test our concept of DSEBCPS for hidden failure detection. We tested the DSEBCPS capabilities for five types of hidden failure: (1) PT blown fuse, (2) CT saturation, (3) CT short circuit, (4) CT reverse polarity, and (5) Incorrect CT ratio setting. The simulation for each case includes the effect of the simulated hidden failure type in the settingless relays and the response of the DSEBCPS to the event.
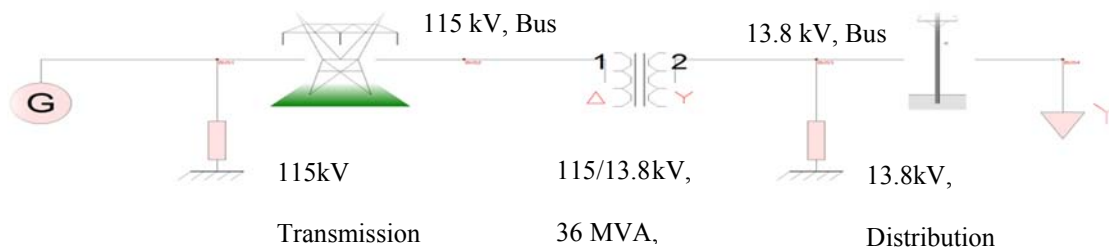
Figure 6-1 One line diagram of the substation used in the simulation.
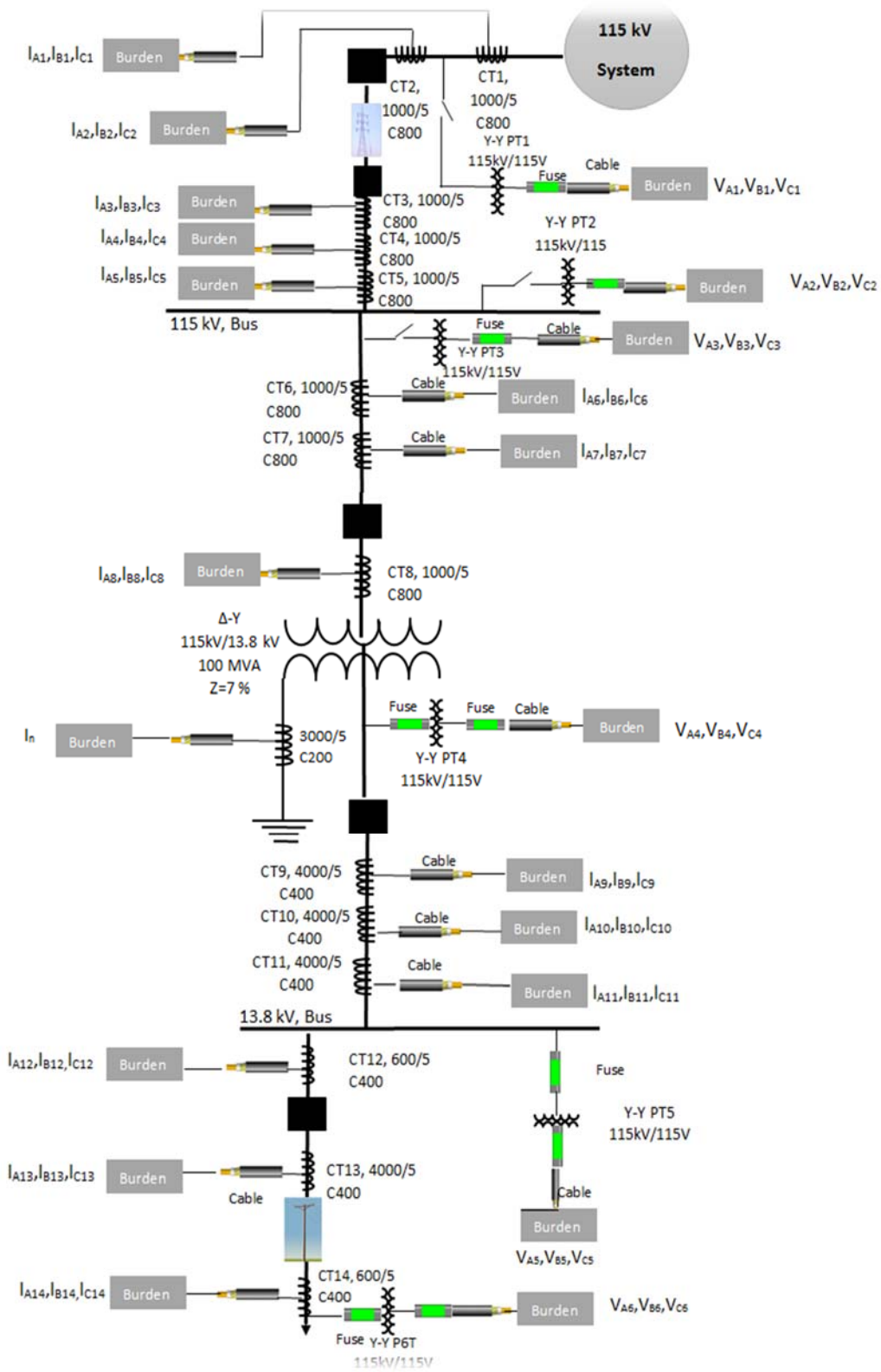
Figure 6-2 One line diagram with instrumentation channels.

6.1   Case 1: Blown Fuse

The blown fuse is one of the common hidden failure modes in the PT circuits. It is simulated by modeling the fuse as an ideal switch that opens completely when the fuse blows. The fuse of the wye-wye connected PT-4, phase A (PT-4A), which provides the settingless relays of the transformer zone with the voltage measurement of the secondary side of the transformer, was blown. This case was simulated for three scenarios: (a) single event, blown fuse of PT-4A without fault, (b) two non-simultaneous events, blown fuse of PT-4A and phase to phase fault in the distribution line, and (c) two simultaneous events, blown fuse of PT-4A and phase to phase fault in the distribution line. The objective of these three scenarios is to demonstrate the capability of DSEBCPS to distinguish between a hidden failure and a faulty zone through the hypothesis testing.

6.1.1   Case 1.1: Single Event, Blown Fuse of PT-4A without Fault

This scenario examines the effect of a single event of hidden failure on the settingless relay and the response of the DSEBCPS. The simulation period is 5 seconds. The event of the blown fuse was initiated at t=2 seconds. Furthermore, the case was initially simulated with a load of 6 MW. An additional load of 6MW was switched on at t=3 seconds and switched off at t=4 seconds. The results of the settingless relay of the transformer zone, as well as the proposed DSEBCPS, are presented below.

Settingless Relay

The waveform of the voltage measurement extracted from PT4 and recorded in the settingless relay of the transformer zone is shown in Figure 6-3. The figure clearly shows

phase A voltage experienced a significant voltage drop as a result of the blown fuse. The figure also depicts the response of the settingless relay that detected abnormal conditions and its confidence level dropped. Moreover, the relay operated accordingly and initiated a trip signal, as shown in Figure 6-3. If this operation is executed, the transformer will be tripped because of the blown fuse condition, which is not a fault in the transformer. This case clearly displays the impact of the hidden failures on the operation of the protection system and the potential negative consequences in power system operation.
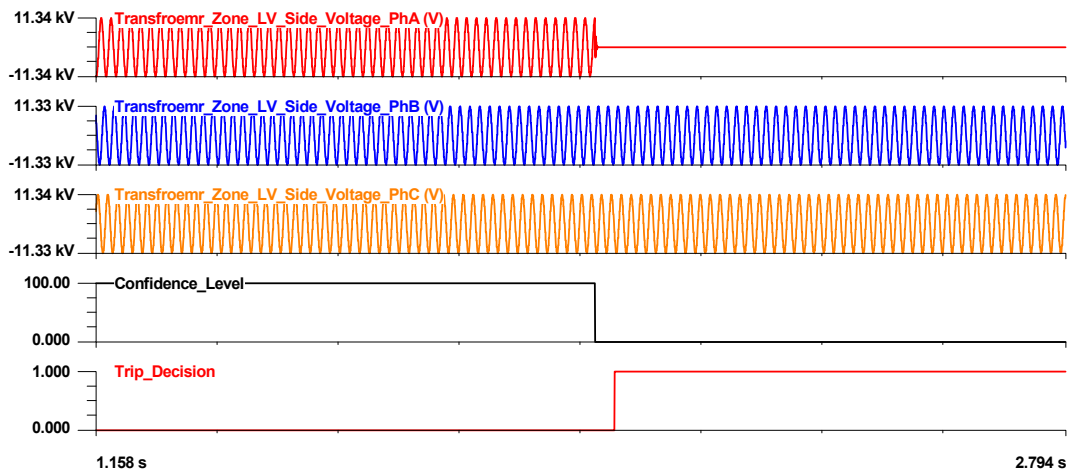
Figure 6-3 Outcome of the settingless relay of the transformer zone for case 6.1.1.

DSEBCPS

Figure 6-4 shows the phasor quantities of the events obtained from the DSEBCPS. The figure shows the voltage magnitude of phase A experienced a significant drop as a result of the blown fuse. The DSEBCPS responded immediately to the event, which caused the confidence level of the substation to drop, by initiating the hypothesis testing, summarized in Table 6-1. During the hypothesis testing the DSEBCPS scanned the values of the normalized residuals of all the measurements and selected the measurement with the

highest normalized residual as a suspicious measurement. According to Figure 6-5, measurement#66 extracted from PT-4A has the highest value of the normalized residuals. Furthermore, the device common- mode criteria verification revealed that instrumentation channel common mode criterion was satisfied. Also, verifying the adjacent phases of PT-4A revealed that they did not qualify as suspicious measurements. Thus, only the measurement of PT-4A was considered as suspicious measurement. Accordingly, the hypothesis under consideration was a hidden failure in PT4, phase A. Subsequently, all the measurements extracted from PT-4A were removed from the measurement set. The dynamic state estimation was performed again starting at time: t=2 sec. The results are shown in Figure 6-5. Note that this test indicates a high confidence level after the removal of the measurements extracted from phase A of PT-4. Moreover, as an outcome of hypothesis testing (Figure 6-5), the DSEBCPS detected a hidden failure in the substation. In this case, the DSEBCPS issued a diagnostic, inhibited temporarily the operation of the setting-less relay. Additionally, Figure 6-5 shows the DSEBCPS did not detect a faulty zone because the zone common-mode criterion was not satisfied, which indicated unfaulty substation. Subsequently, the DSEBCPS identified exactly which instrumentation channels suffered from hidden failure as shown in Figure 6-6. The figure shows that the DSEBCPS identified PT-4, phase A as the instrumentation channel suffering from hidden failure. This identification corresponds to the removed measurements. Subsequently, the DSEBCPS streamed estimated values of PT-4, phase A data to settingless relay to replace the compromised data. This case demonstrated that measurement redundancy at the substation level makes hypothesis testing quite efficient because the measurement

suffering from hidden failure experienced the highest normalized residuals and therefore placed first in the removal process.

Table 6-1 Summary of the hypothesis testing for case 6.1.1

Hypothesis #	Hypothesis under Consideration	Result
1	Hidden Failure in PT-4A	High confidence level
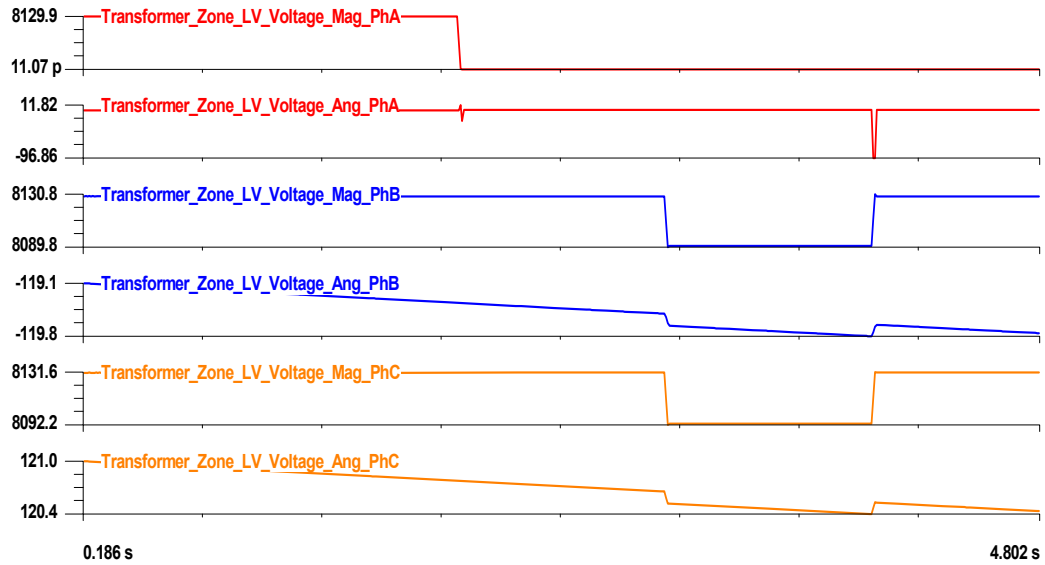
Figure 6-4 Voltage magnitude and angle from PT4 for case 6.1.1.
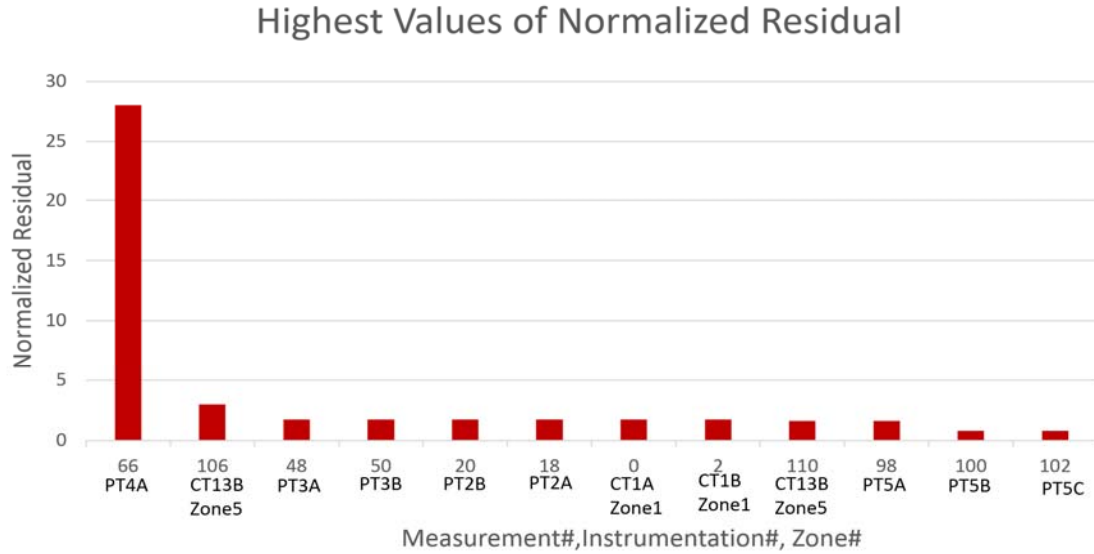
Figure 6-5 The highest values of the normalized residual for case 6.1.1.
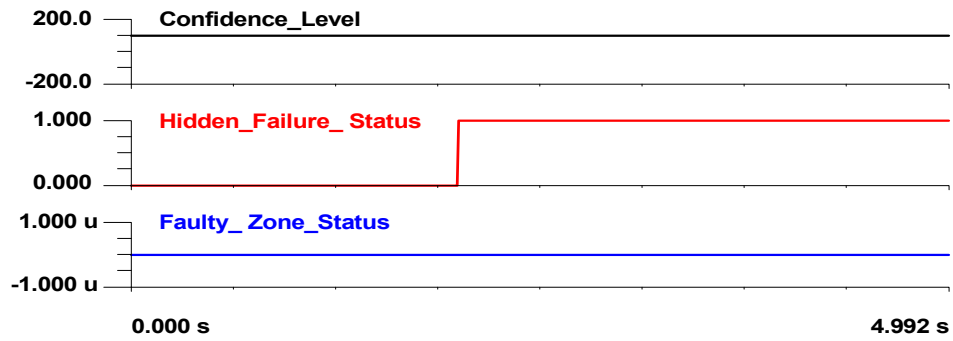
Figure 6-6 The outcome of hypothesis testing for case 6.1.1.
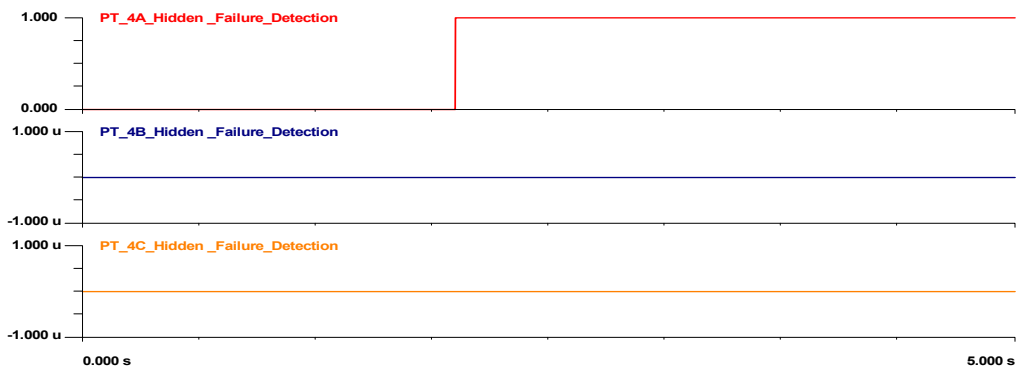
Figure 6-7 Hidden failure status in instrumentation channels for case 6.1.1

The DSEBCPS computes the substation states as an outcome of the DSE. These states are used by the DSEBCPS to compute the estimated measurements for each measurement used in performing the DSE including the removed measurements. Upon detecting hidden failure, the DSEBCPS computes the time domain waveforms using the calculated measurements, as explained in Chapter 5. The DSEBCPS streams these waveforms to the settingless relay, which suffers from the hidden failures, to override the compromised measurement. To facilitate this process a delay of 2 cycles in the settingless relay operation is introduced. This process is depicted in Figure 6-8 where the bad signal was overridden in the relay with the calculated sampled values after 2 cycles of the blown fuse initiation. Furthermore, the confidence level of the settingless relay responded to the bad data replacement and recovered from low confidence level as shown in Figure 6-8, which also shows that the trip signal was not initiated because of the 2-cycle delay introduced in the operation of the settingless relay. This process demonstrates the advantage of this scheme in maintaining high security and dependability of the protection system even with the presence of hidden failures. For this example high security was demonstrated in detecting the hidden failure, while high dependability was demonstrated by replacing the compromised data to maintain the functionality of the protection system.
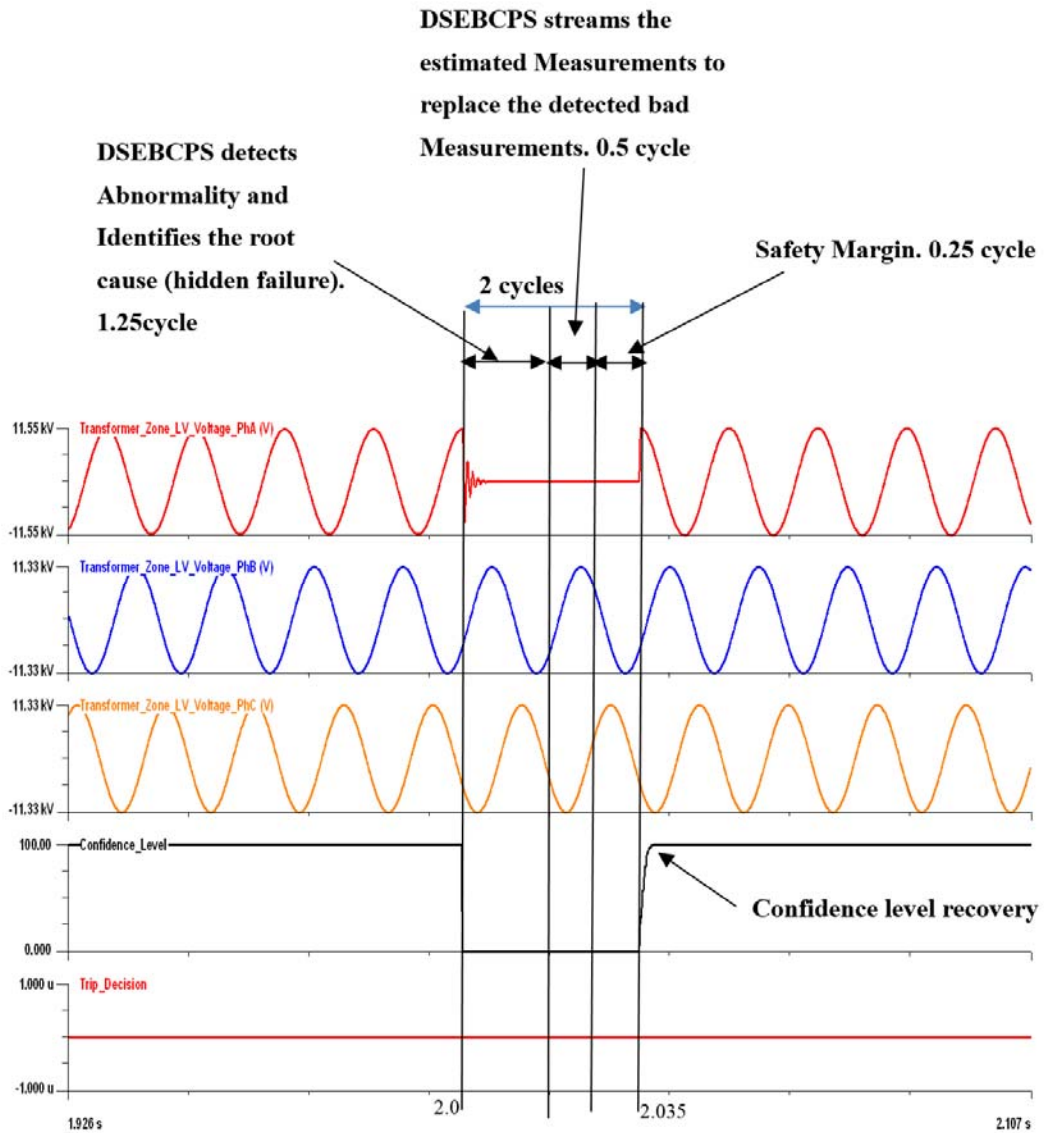
Figure 6-8 Settingless relay corrected response for case 6.1.1

6.1.2 *Case 1.2: Two Non-Concurrent Events, Blown Fuse of PT-4A and Phase to Phase*
Fault in the Distribution Line

The definition of hidden failures states that the hidden failures initiation takes place

during the switching event in the network such as load switching and fault initiation.

Moreover, the definition implies that the switching event might be concurrent or ahead of

74

time in a short time window of the hidden failure. The latter is simulated in this case with one cycle time window. The first event is a phase to phase fault at the middle of the distribution line, initiated at t=2 seconds. One cycle later, at t=2.016s seconds, the second event of blown fuse (i.e., hidden failure) was initiated by modeling the fuse as an ideal switch that opens completely when the fuse blows. Similar to the previous case, the fuse located in the primary side of the wye-wye connected PT 4, phase A, was blown. The simulation period is 5 seconds. Furthermore, the case was simulated initially with a load of 6 MW. An additional load of 6MW was switched on at t=3 seconds and switched off at t=4 seconds. The objective of this case is to test the performance of the DSEBCPS for two events in the substation. The results of settingless relay of the transformer zone, as well as the proposed DSEBCPS, are presented below.

Settingless Relay

Figures 6-9 and 6-10 show the waveforms of the event recorded in the settingless relay of the distribution line zone. Both figures show the line experienced a phase to phase fault between phases A and B. Figures 6-11 depicts the responses of the settingless relay of the distribution line zone, which detected abnormal condition and caused the confidence level of the relay to drop. Consequently, the relay operated and initiated trip signals, as shown in Figures 6-11. Moreover, Figures 6-12 shows the voltage waveforms of the secondary side of the transformer zone recorded from PT4. It clearly shows that phase A experienced a significant voltage drop as a result of the blown fuse. Additionally, the settingless relay of the transformer zone operated as demonstrated in the previous case. If these operations are executed, the transformer and the distribution line will be tripped

because of the blown fuse and phase to phase fault, respectively. The results of the former case, show settingless relay misoperation, if no correction action was inserted. On the other hand, the operation of the settingless relay of the distribution line zone was correct because of the faulty condition. This case demonstrates that hidden failures can widen the power system interruptions by including healthy zones.
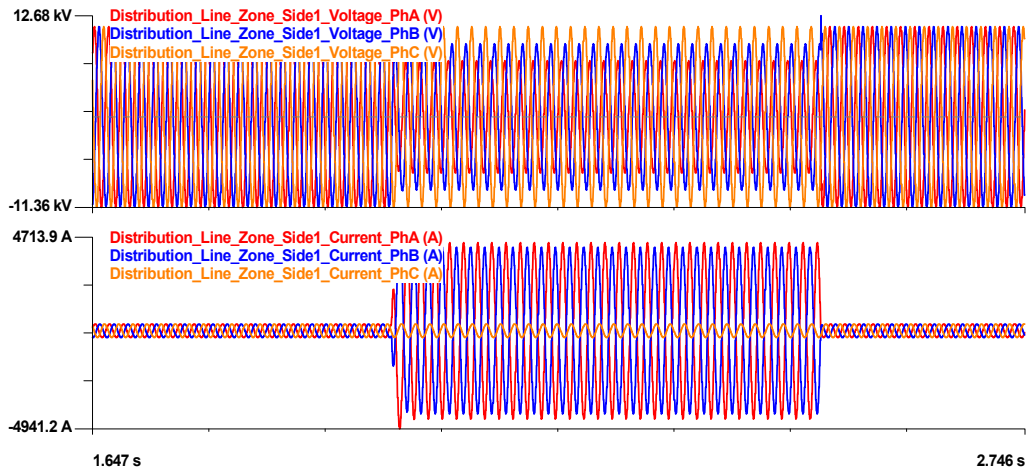
Figure 6-9 Voltage and current waveforms of distribution line zone side 1 for case 6.1.2.
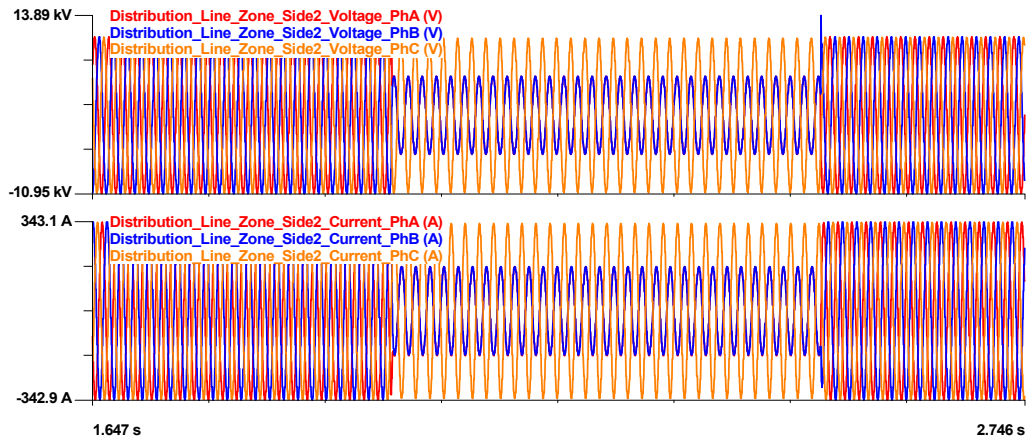
Figure 6-10 Voltage and current waveforms of distribution line zone side 2 for case 6.1.2.
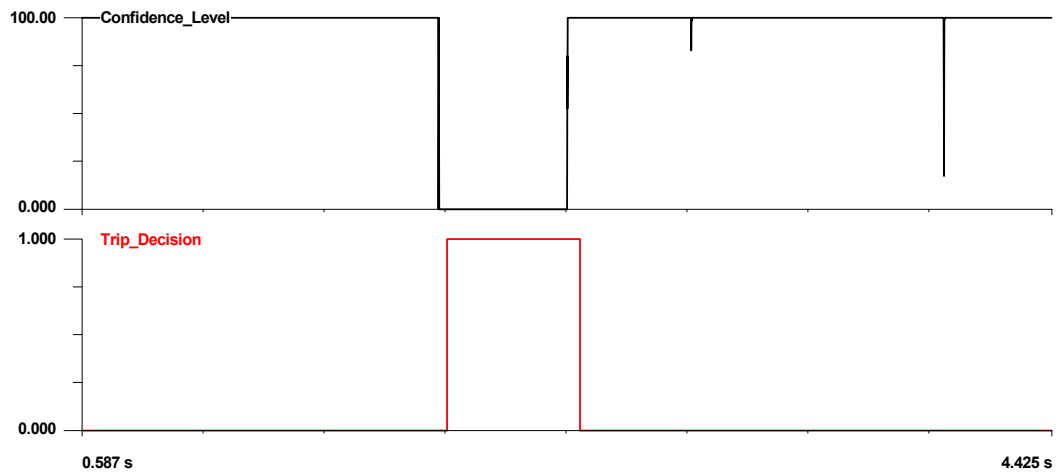
Figure 6-11 settingless relay response of the distribution line zone for case 6.1.2.
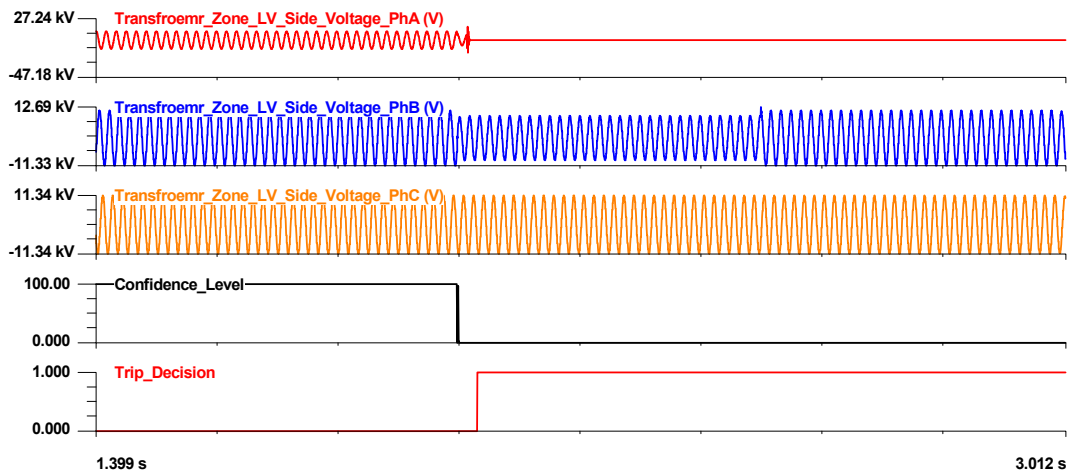
Figure 6-12 Settingless relay output of the transformer zone for case 6.1.2.

DSEBCPS

Figures 6-13 and 6-14 show the phasor quantities of the events recorded from the DSEBCPS associated with side 1 of the distribution line. The figures show the line experienced phase to phase fault between phases A and B. Moreover, Figure 6-15 shows the phasor quantities of the voltage measurements extracted from PT4. The figure clearly

shows the voltage magnitude of phase A experienced significant voltage drop because of the blown fuse. Consequently, the DSEBCPS responded to the first event at t=2s (i.e., the fault in the distribution line), which caused the confidence level of the substation to drop by initiating the hypothesis testing summarized in Table 6-2 and 6-3. During the test, the DSEBCPS scanned the values of the normalized residuals of all the measurements and extracted the highest value. According to Figure 6-16 measurement #116, extracted from CT14, phase A and modeled by the distributing line model had the highest normalized residual. The device common mode criteria verification revealed that the zone common mode criterion associated with the distribution line was satisfied because all the measurements modeled by zone 5 experienced higher value of normalized residual that exceeded the threshold of 2. Thus all the measurements of the distribution line were considered as a set of suspicious measurements. Accordingly, the hypothesis under consideration was power fault in the distribution line. Subsequently, the DSEBCPS removed these measurements from the measurement set and rerun the dynamic state estimation starting at time: t=2 sec. This process revealed high confidence level, which indicates a successful hypothesis.

One cycle later at t=2.016s, the confidence level of the substation dropped and initiated the hypothesis testing again. Figure 6-17 shows the highest set of the measurement normalized residuals computed by the DSEBCPS during the second event. The figure shows that the measurement#66 extracted from PT-4, phase A had the highest normalized residual. Verifying the device common mode criteria revealed that the instrumentation channel common mode criterion associated with only PT4, phase A was satisfied. Therefore, the hypothesis under consideration at t=2.016 was hidden failure in

PT4, phase A. Subsequently, the DSEBCPS removed all measurements extracted from PT, 4 phase A from the measurements set and rerun the DSE.

Figure 6-18 shows the outcome of the two hypotheses at t=2s and t= 2.016s. The figure shows both hypotheses were successful as indicated by high confidence level for the substation. DSEBCPS detected a faulty zone and hidden failure in the substation, as shown in Figure 6-18. Additionally, the figure shows that the phase to phase fault led the blown fuse event by one cycle, approximately. Moreover, the DSEBCPS specified which part of the substation suffered from the fault and hidden failures, as shown in Figures 6-19 and 6-20, respectively. Accordingly, DSEBCPS issued a diagnostic, inhibited temporarily the operation of the settingless relay of the transformer zone and permitted the operation of the settingless relay of the distribution line zone. This simulation shows the redundancy in the measurements makes the hypothetical testing very efficient because the measurement suffering from hidden failures was placed first in the removal process.
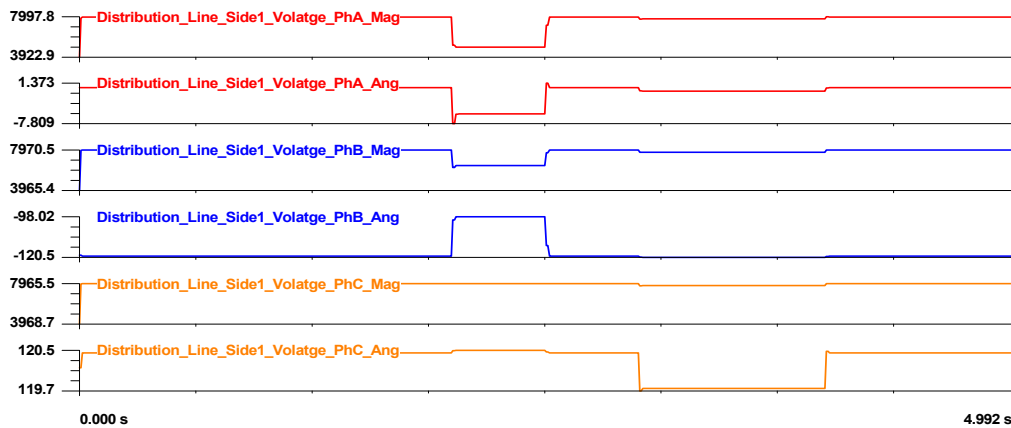
Figure 6-13 Voltage magnitude and phase angle of the distribution line side 1 for case 6.1.2.
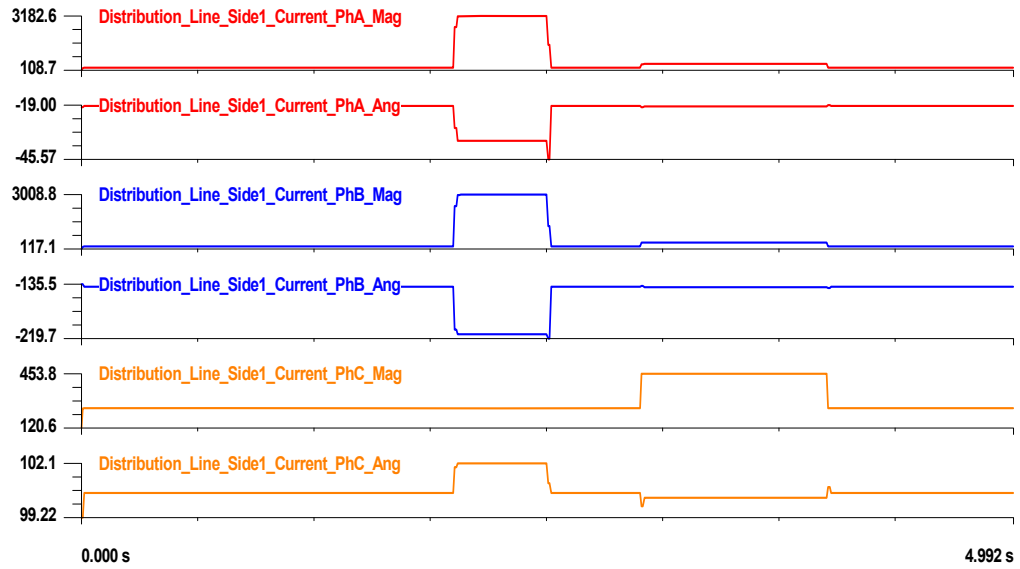
Figure 6-14 Current magnitude and phase angle of the distribution line side 1 for case 6.1.2
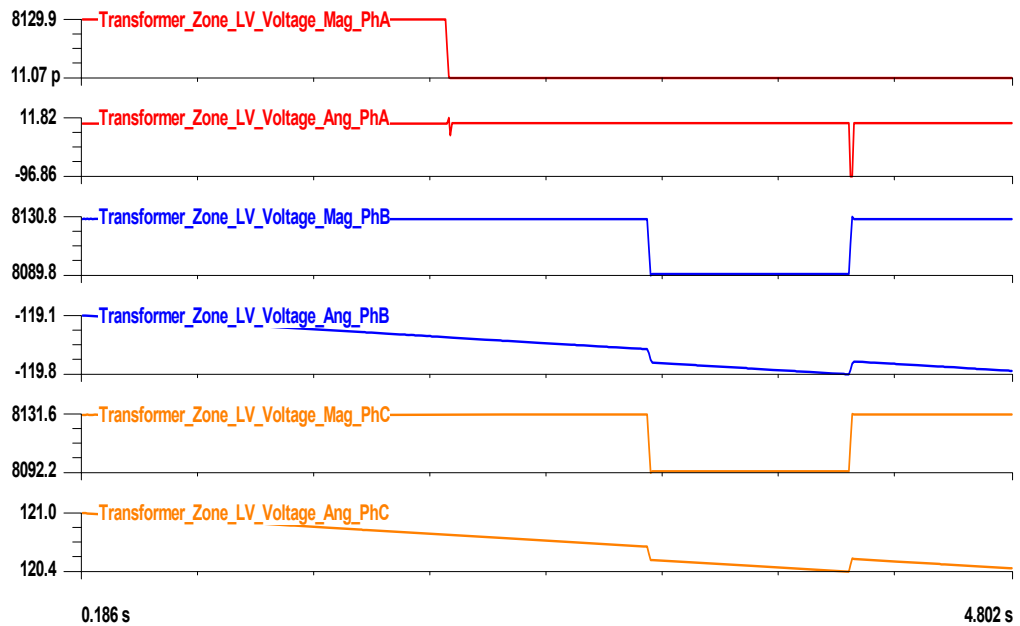
Figure 6-15 Voltage magnitude and phase angle of PT 4 for case 6.1.2.

Table 6-2 Summary of the hypothesis testing at t=2s for case 6.1.2.

Hypothesis #	Hypothesis under Consideration	Result
1	Power fault in the distribution line	High confidence level

Table 6-3 Summary of the hypothesis testing at t=2.016s for case 6.1.2.

Hypothesis #	Hypothesis under Consideration	Result
1	Hidden Failure in PT-4A	High confidence level
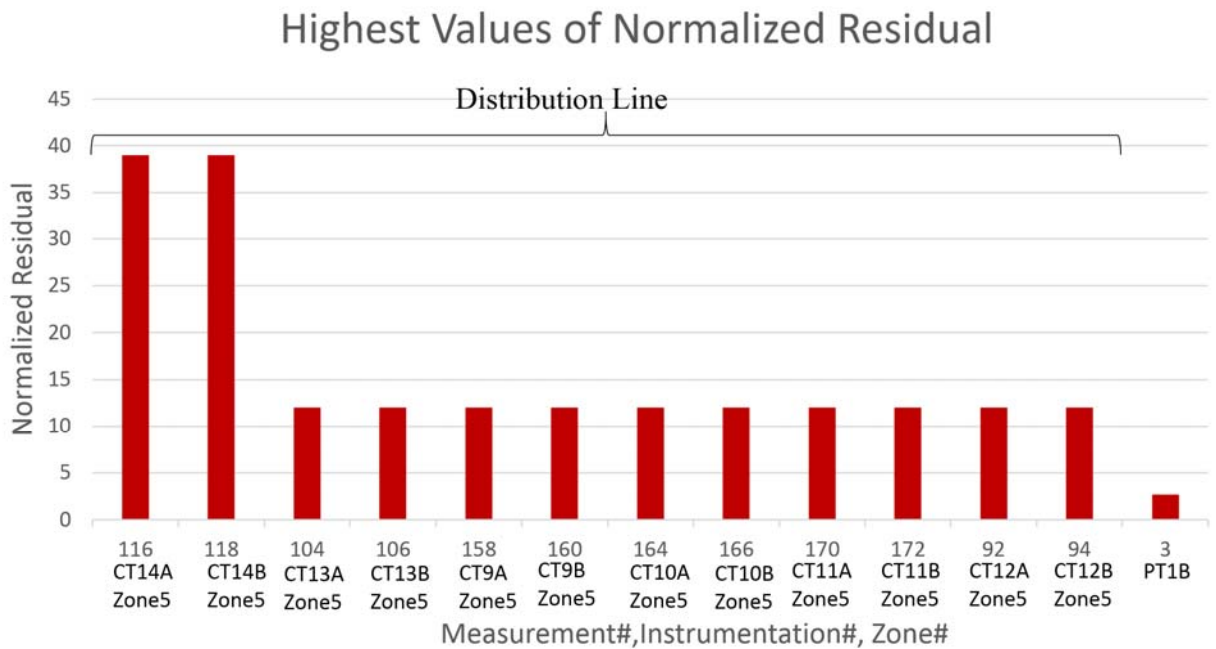
Figure 6-16 The highest values of normalized residuals during the phase to phase fault for case 6.1.2.
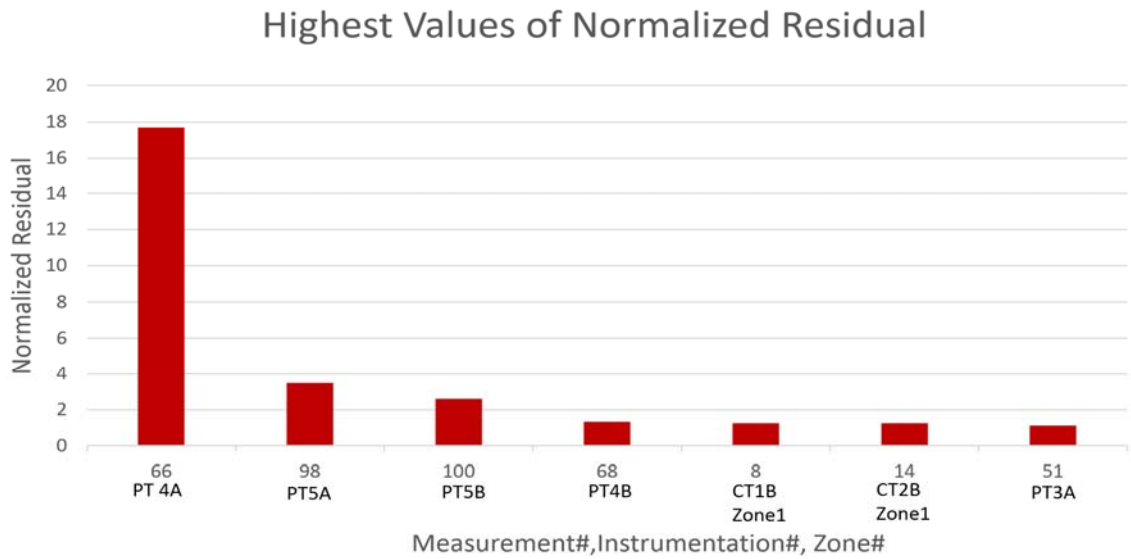
Figure 6-17 The highest values of normalized residuals during the blown fuse event for case 6.1.2.
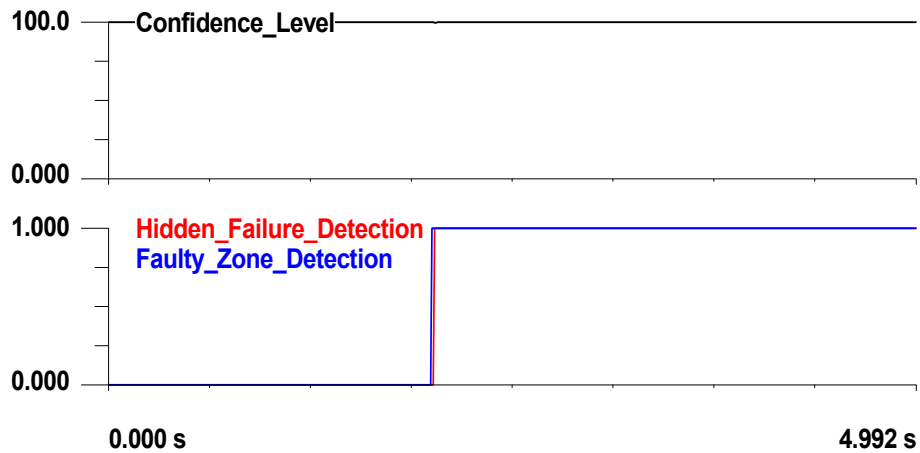
Figure 6-18 The outcome of the hypothesis testing conducted by DSEBCPS for case 6.1.2.
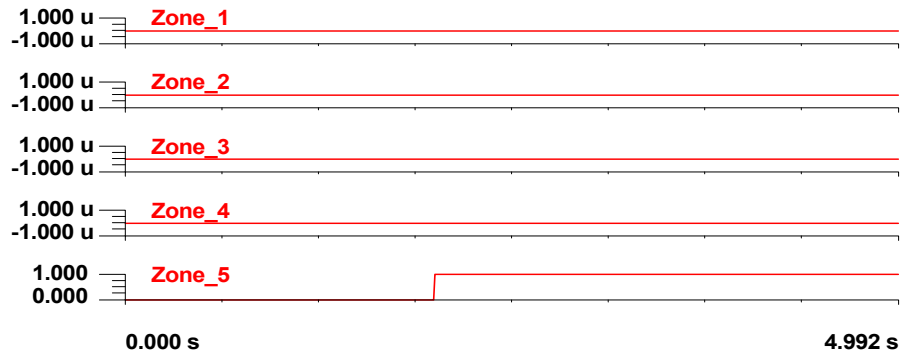
Figure 6-19 Faulty zone identification for case 6.1.2.
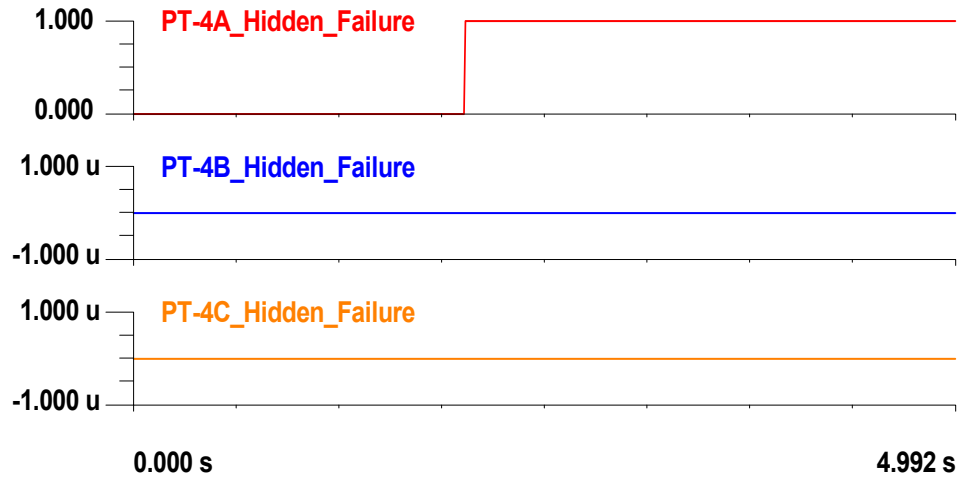
Figure 6-20 Hidden failure status in instrumentation channel for case 6.1.2

Settingless Relay Corrected Response

The DSEBCPS computed the sampled values of the compromised measurement as explained in Chapter 5. Then, it streamed these sampled values to the affected settingless relay. These waveforms overrode the compromised measurements in the affected settingless relay. This process is depicted in Figure 6-21, which shows that a bad signal

was corrected in the settingless relay of the transformer zone after 2 cycles of the blown

fuse initiation. Furthermore, the confidence level of the settingless relay responded to the

bad data replacement and recovered from a low confidence level as shown in Figure 6-21,

which also shows the trip signal was not initiated because of the 2-cycle delay introduced

in the operation of the settingless relay.
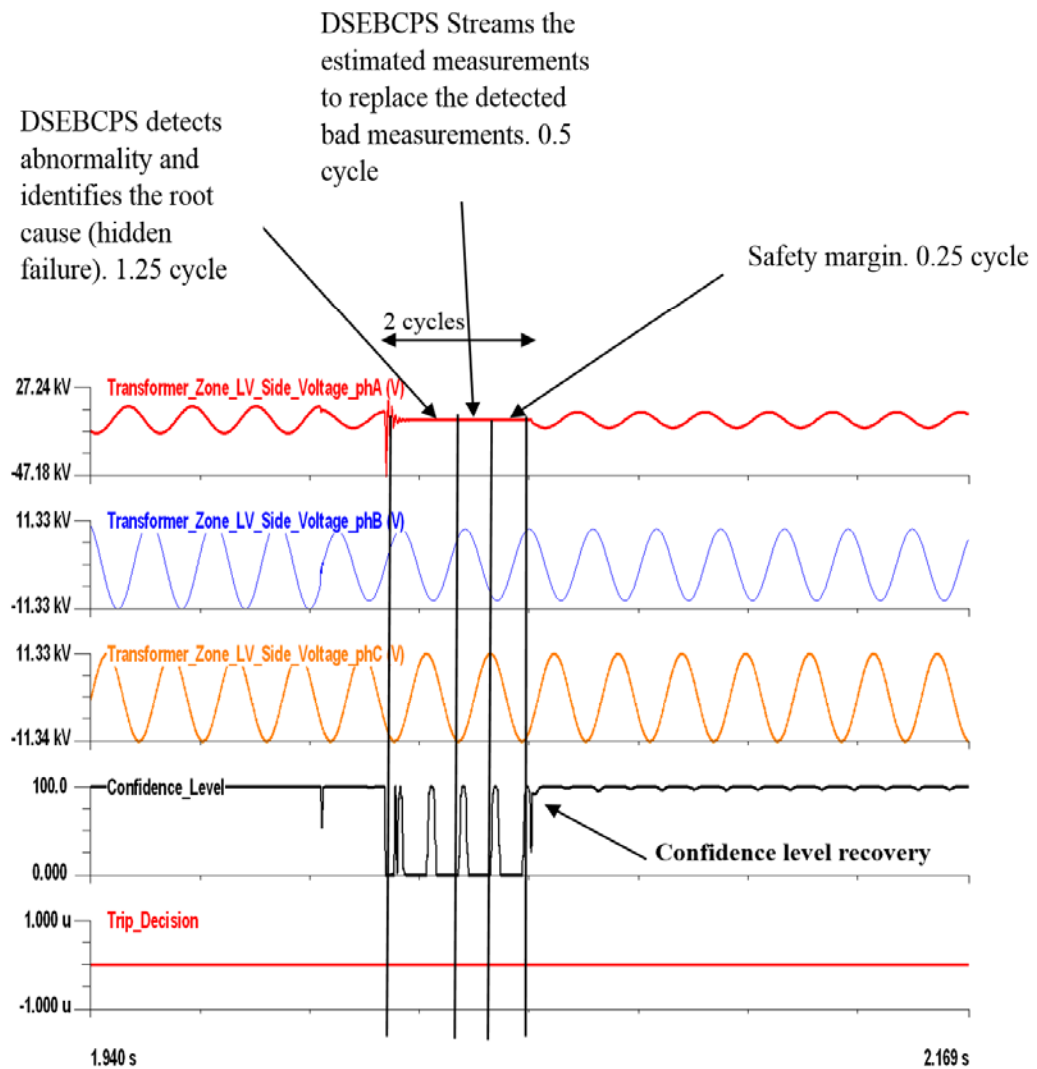
Figure 6-21 Corrected response of settingless relay of transformer zone for case 6.1.2.

6.1.3   Case-3: Two Concurrent Events, Blown Fuse of PT-4A and Phase to Phase Fault

in the Distribution Line

The two events of the previous cases were simulated concurrently of each other. The simulation period was 5 seconds. The sequence of events included the initiation of the blown fuse of PT-4A and the phase to phase fault at the middle of the distribution line at t=2 seconds; the fault was cleared at t=2.5 seconds. Furthermore, a 6 MW load was included during the simulation. Additionally, 6 MW was switched on and switched off at t=3 seconds and t=4 seconds, respectively. The objective of this case is to test the performance of the DSEBCPS for two simultaneous events in the substation. The results of the settingless relays of the transformer zone and distribution line as well as of the proposed DSEBCPS are presented below.

Settingless Relay

As with the previous two cases, the settingless relays of the transformer zone and the distribution line zone detected abnormal conditions, which caused the confidence levels of both relays to drop. Consequently, both relays initiated trip signals.

DSEBCPS

The DSEBCPS responded to both events by initiating the hypothesis testing at t=2s summarized in Table 6.4. The DSEBCPS considered three hypotheses for this case. The first hypothesis was power fault in the distribution line because the highest normalized residual was experienced by measuremnt#116 as shown in Figure 6-22. This measurements extracted from CT 14, phase A and modeled by zone-5. Also, measurement#116 satisfied

the zone common mode criterion of zone-5. Accordingly the DSEBCPS removed zone-5 measurements from the measurements set and the zone model from the substation model and rerun the DSE. The outcome of this hypothesis was low confidence level which means unsuccessful hypothesis. The second hypothesis was a hidden failure in PT4, phase A. This hypothesis was considered because the second highest normalized residual in the measurements, which were not part of the first set of suspicious measurement considered during the first hypothesis, was experienced in measurement#66 as shown in Figure 6-22. This measurement was extracted from PT-4A. Also, this measurement satisfied the instrumentation common mode criterion of PT-4A. Subsequently the DSE removed all the measurements associated with PT4, phase A and rerun the DSE. The outcome of this hypothesis was low confidence level, which means unsuccessful hypothesis. The third hypothesis combined the previous two hypotheses. It considered both power fault in the distribution line and hidden failures in PT4, phase A. Subsequently, both set of suspicious measurements associated with distribution line and PT4, phase A were removed from the measurements set and rerun the DSE. This hypothesis was successful as shown in Figure 6-23, which shows successful hypothesis testing, indicated by a high confidence level after the elimination of both set of suspicious measurements. Moreover, as an outcome of the two-level hypothesis testing, the DSEBCPS detected a faulty zone and hidden failure in the substation, as shown in Figure 6-23.The DSEBCPS specified which part of the substation suffered from the hidden failure and the fault as shown in Figures 6-24 and 6-25, respectively. Accordingly, DSEBCPS issued a diagnostic, inhibited temporarily the operation of the setting-less relay of the transformer zone and permitted the operation of the settingless relay of the distribution line zone. This simulation showed that the

redundancy in the measurements makes the hypothetical testing very efficient because the measurements suffering from abnormalities are placed first in the elimination process through the device common-mode criteria. This case demonstrated the capability of the DSEBCPS in detecting two concurrent events; hidden failures and power fault, which represents the most challenging scenario.

Table 6-4 Summary of the hypothesis testing at t=2.0s for case 6.1.3.

Hypothesis #	Hypothesis under consideration	Result
1	Power fault in distribution line	Low confidence level
2	Hidden failure in PT-4A	Low confidence level
3	Power fault in distribution line & Hidden failure in PT-4A	High confidence level
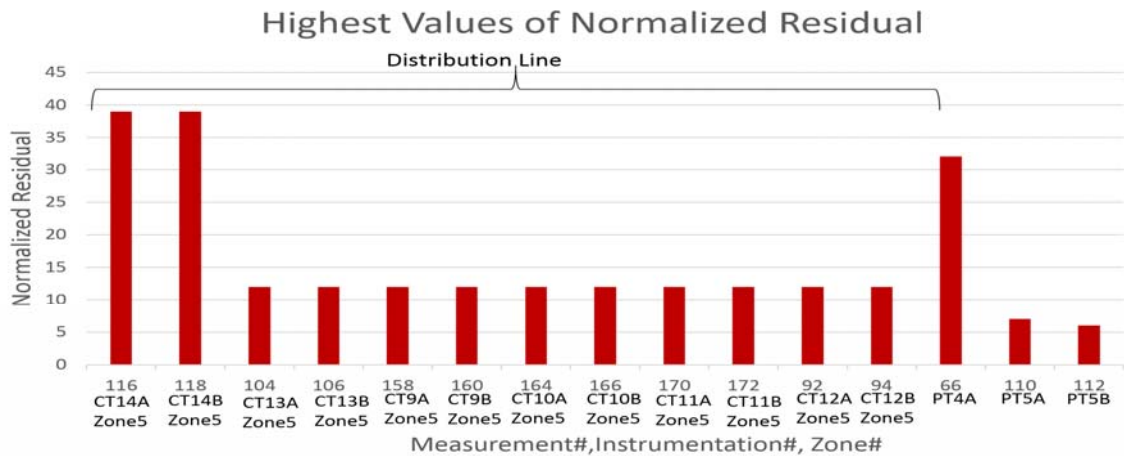
Figure 6-22 T he highest values of normalized residuals for case 6.1.3.
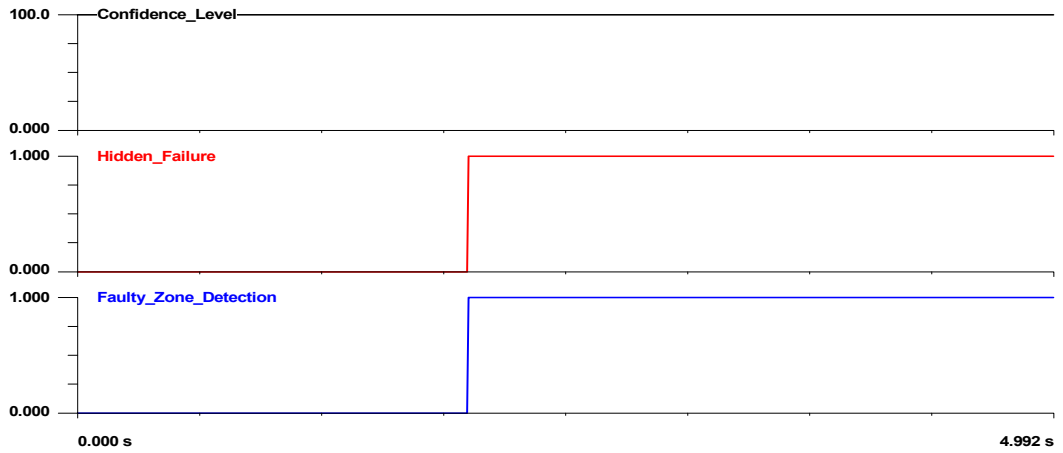
Figure 6-23 The outcome of DSEBCPS for case 6.1.3.
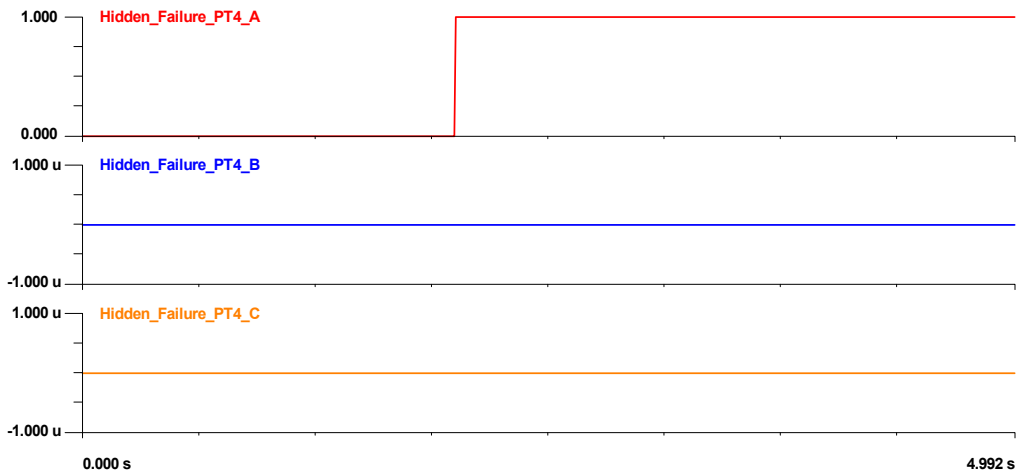
Figure 6-24 Hidden failure status in instrumentation channels for case 6.1.3.
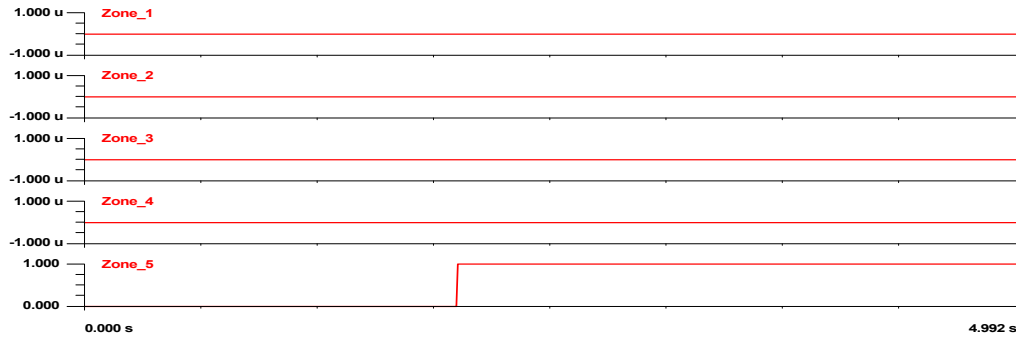
Figure 6-25 Faulty zone identification from DSEBCPS for case 6.1.3

Settingless Relay Corrected Response

As in the previous case, the estimated measurements and their time stamps are streamed to the settingless relay. This process is similar to the case depicted in Figure 6-21 of case 6.1.2.

6.2 Case2: CT Short Circuit

CT short circuit takes place when the CT terminals are shorted which results in a significant drop in the current measurement associated with the shorted CT. It is one of the critical hidden failure modes in the CT circuit that causes protection system misoperation. This case examines the responses of the setting-less relay and the DSEBCPS to this type of hidden failure in the CT circuit. Therefore, CT9, phase A, (CT-9A), which provides the setting-less relay of the transformer zone with current measurement for the secondary side of the transformer, was shorted. This type of hidden failure is modeled by shorting the CT terminals during the initiation of the event. Two cases were considered; (1) Single event of hidden failure; CT-9A short circuit and (2) Two simultaneous events of hidden failure; CT-9A short circuit and power fault in the distribution line.

6.2.1   Case 2.1: Single Event, CT-9A Short Circuit

This case examines the responses of the setting-less relay and the DSEBCPS to a single event of hidden failure. The sequence of events started at t=2s during which 6 MW load was switched on and CT 9, phase A was shorted. The simulation started initially with 6 MW load and lasted for 5s. The results of the setting-less relay, as well as the proposed DSEBCPS, for the simulated event are presented below.

Settingless Relay

Figure 6-26 shows the current waveforms recorded from CT-9A experienced a significant drop because of the CT short circuit. Moreover, the figure shows the setting-less relay responded to the event indicated by the drop in the confidence level. Accordingly, the relay initiated a trip signal to isolate the transformer. This response is a relay misoperation because no power fault exists in the system, which demonstrates the effect of the hidden failures.
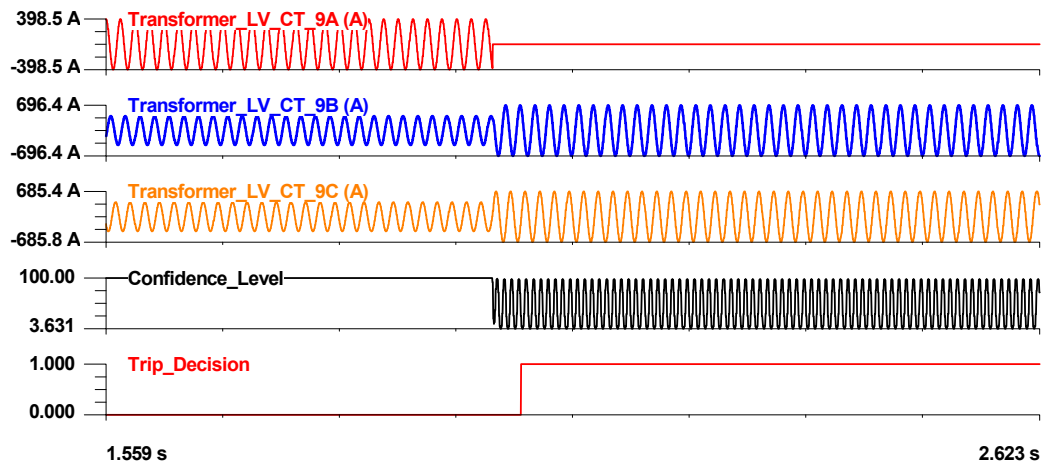
Figure 6-26 Settingless relay response for case 6.2.1

90

DSEBCPS

The DSEBCPS responded to the event by initiating the hypothesis testing, which is summarized in Table 6-5. During hypothesis testing the DSEBCPS scanned the values of the normalized residuals of all the measurements and extracted the highest value. According to Figure 6-27, measurement#72 extracted from CT-9A has the highest normalized residual. Subsequently, the DSEBCPS verified the common mode criteria, which revealed the instrumentation channel common mode criterion associated with CT-9A was satisfied. Accordingly, the hypothesis under consideration was a hidden failure in CT-9A. Therefore, all the measurements extracted from CT-9A were removed from the measurements set and the DSEBCPS re-performed the dynamic state estimation. The output of the new DSE is shown in Figure 6-28 which depicts high confidence level following the removal process that took place at t=2s. Furthermore, Figure 6-28 shows the DSEBCPS detected hidden failure because of the satisfaction of the instrumentation channel common mode criterion. Additionally, the DSEBCPS specified exactly the location of the hidden failure that corresponded to the removed measurements as shown in Figure 6-29. Accordingly, DSEBCPS issued a diagnostic, inhibited temporarily the operation of the setting-less relay of the transformer zone. It is important to note that the hypothesis testing and the re-performance of the DSE took place only for one time sample that corresponds to the initiation of the abnormality.

Table 6-5 Summary of the hypothesis testing at t=2s for case 6.2.1.

Hypothesis #	Hypothesis Under Consideration	Result
1	Hidden Failure in CT-9A	High confidence level
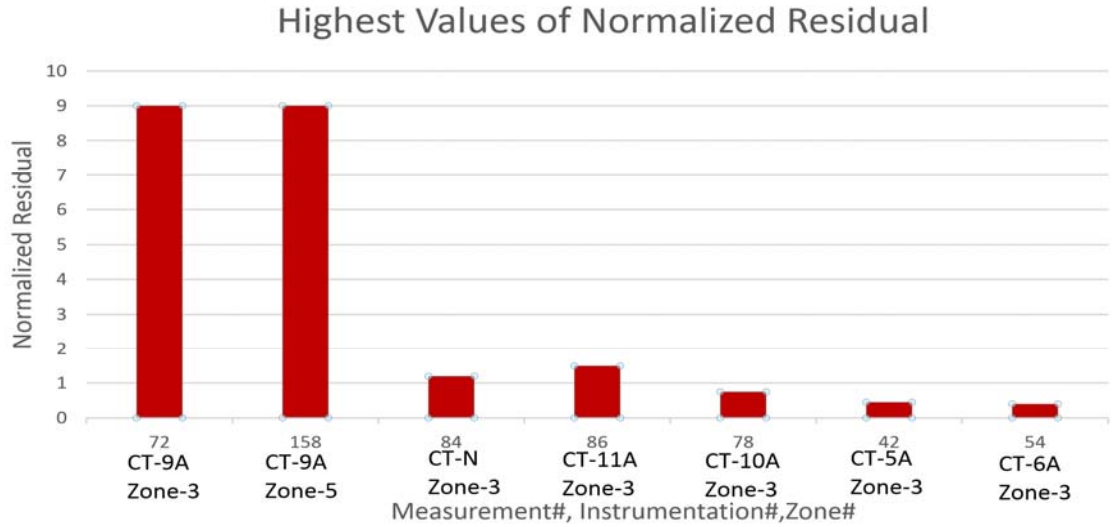
Figure 6-27 Highest values of normalized residual for case 6.2.1
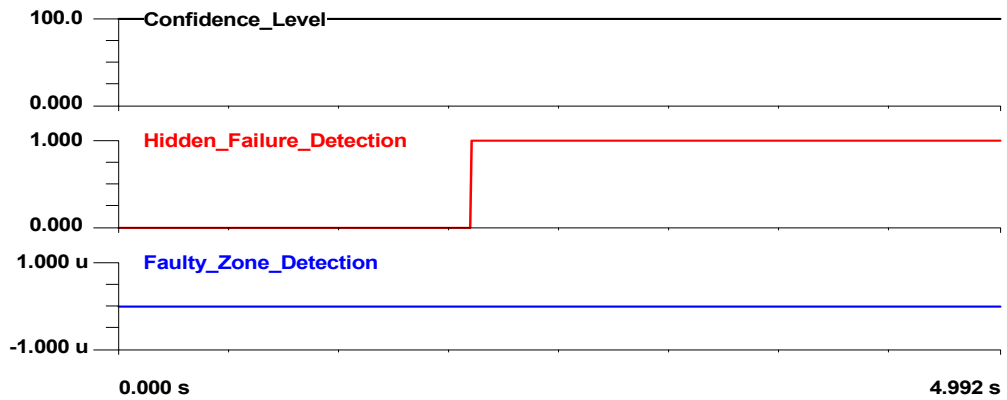
Figure 6-28 The DSEBCPS results for case 6.2.1.
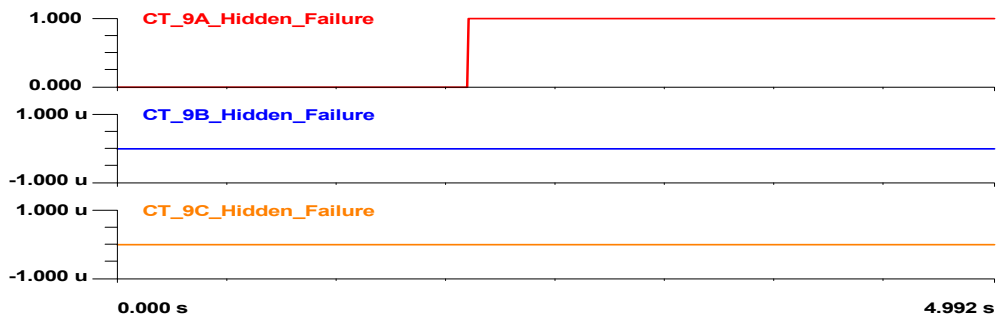
Figure 6-29 Hidden failures identification for case 6.2.1.

Corrected Settingless Response

Figure 6-30 shows the corrected response of the setting-less relay. This figure shows that the detected bad signal from CT-9 was overridden by the calculated measurements computed in the DSEBCPS. These calculated sampled values corresponding to the bad signal were streamed from the DSEBCPS to the setting-less relay with their time stamps to override the compromised measurement. Furthermore, the confidence level of the setting-less relay responded to the replacement of the bad data and recovered to a high level, as shown in Figure 6-30, which also shows that the trip signal was not initiated because of the two-cycle delay introduced in the operation of the setting-less relay.

Figure 6-30 Settingless relay corrected response for case 6.2.1

6.2.2   Case 2.2: Concurrent Events, CT-9A Short Circuit and Power Fault

This scenario tests the response of the DSEBCPS for two concurrent events, CT short circuit in CT9, phase A and phase to phase fault in the 13.8 kV feeder. Both events were initiated simultaneously at t=2s. Moreover, the fault was cleared at 2.5s. The simulation was started with load of 12 MW and lasted for 5s. The response of both settingless relays and DSEBCPS are presented below

Settingless Relay

Figure 6-31 shows the settingless relay of the transformer zone. Moreover, the figure shows that the relay responded to the event of CT short circuit as indicated by the drop in the confidence level. Subsequently, the relay initiated a trip signal to isolate the transformer zone. Furthermore, the response of the setting-less relay for the distribution line is depicted in Figure 6-32, which shows that the relay responded to the phase to phase fault and initiated a trip signal. Therefore, this scenario resulted in the tripping of two zones (i.e., the transformer and the distribution line). If the relays' operations are executed, the transformer and the distribution line will be tripped because of the CT short circuit and phase to phase fault, respectively. The former case results in isolating the transformer because of the CT short circuit, which is not a faulty condition.
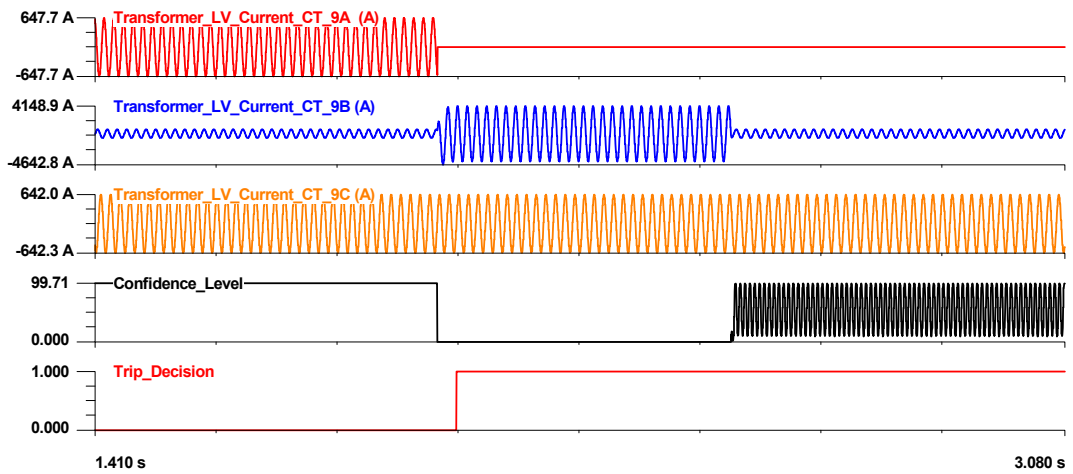
Figure 6-31 Settingless relay output of transformer zone for case 6.2.2
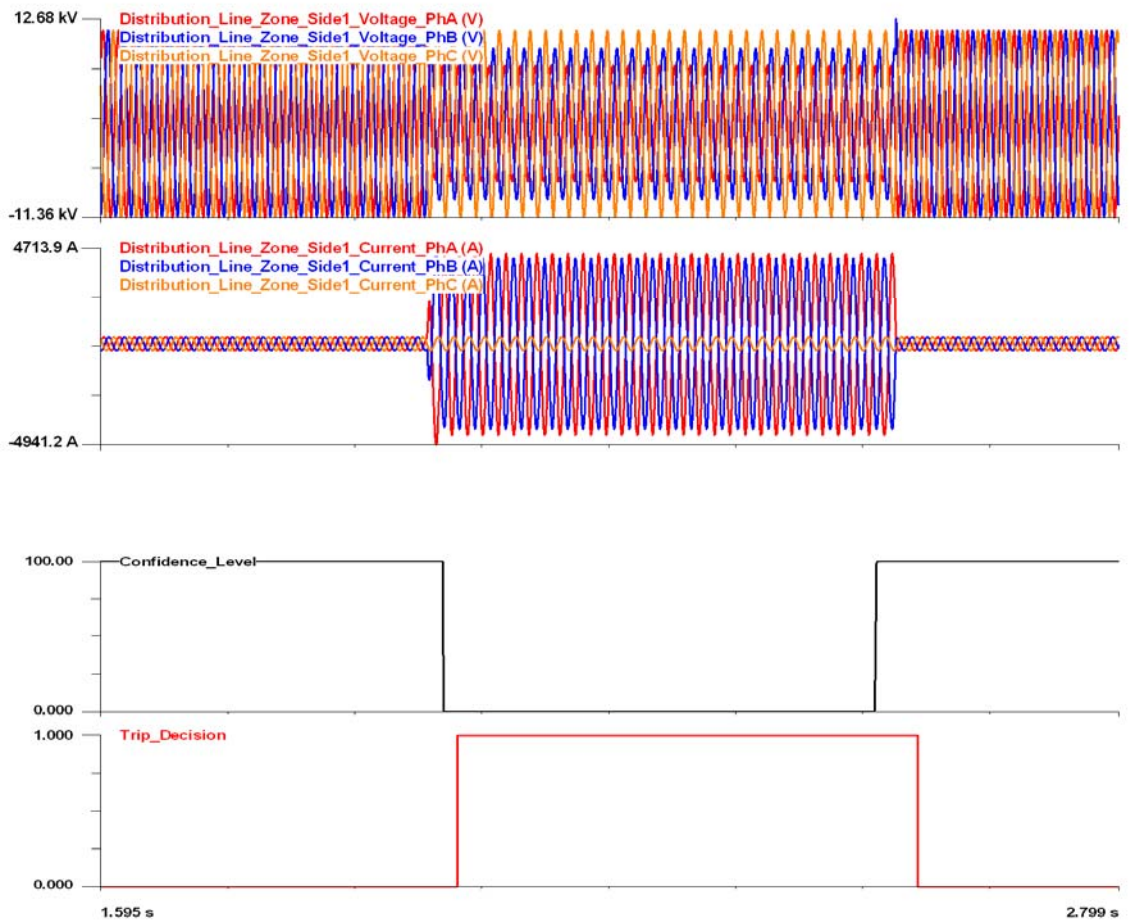
Figure 6-32 Settingless relay output of distribution line zone for case 6.2.2

95

DSEBCPS

The phasor quantities of the current waveform recorded from CT-9 are shown in Figure 6-33. The figure clearly shows that the current magnitude of phase A experienced a significant drop because of the CT short circuit condition. The DSEBCPS responded to the event by initiating the hypothesis testing summarized in Table 6-6. The table shows three hypotheses were considered because of the two simultaneous events. The first two hypotheses considered only one device (i.e., full zone or instrumentation channel) during the removal process, which all failed to achieve high confidence level. On the other hand, the third hypothesis was successful. This hypothesis was power fault in the distribution line and hidden failure in CT-9A. The process started by selecting the measurement with the highest normalized residual and verifying the device common mode criteria. According to Figure 6-34 measurement#92 extracted from CT-12A and modeled by the zone-5 had the highest normalized residual. This measurement satisfied the device common mode criterion associated with zone 5 and therefore, all the measurements modeled by zone 5 were selected as first set of the suspicious measurements. Then, the measurement with the second highest normalized residual value, which was not part of the first set of suspicious measurements, was selected as second suspicious measurement and subjected to common mode criteria. According to Figure 6-34, this measurement was measurement #72 which satisfied the instrumentation channels common mode criterion associated with CT9, phase A. Therefore, the third hypothesis under consideration was a fault in the distribution feeder and a hidden failure in CT9, phase A which both were considered in the previous two hypotheses. Hence, the DSEBCPS removed all the measurements and the models associated with these devices. This removal process results in high confidence level, which

indicates a successful hypothesis. Figure 6-35 depicts the result of the DSEBCPS, which shows both fault and hidden failure were detected as a result of the two level hypothesis testing. Additionally, the DSEBCPS located the portions of the system that suffer from the abnormalities as shown in Figures 6-36 and 6-37.
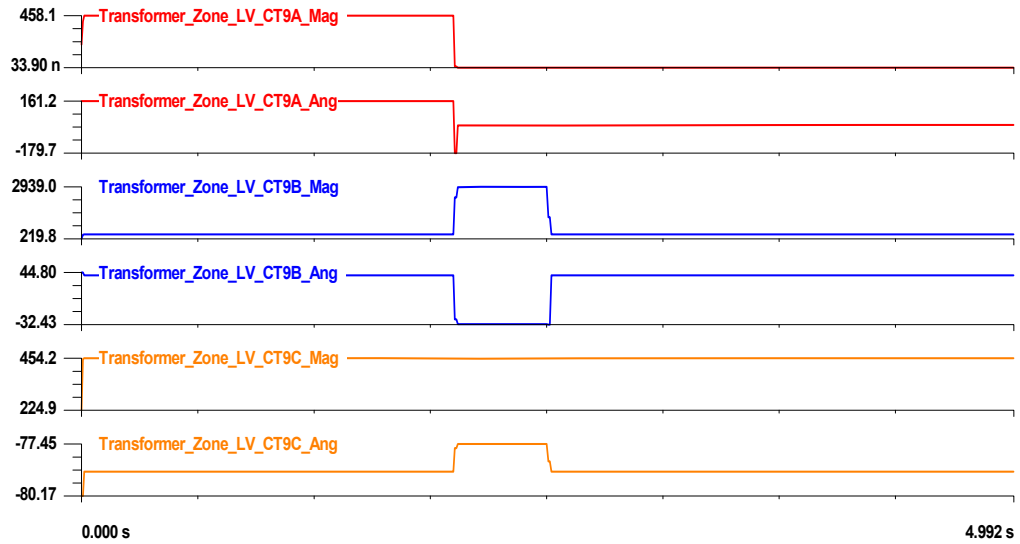
Figure 6-33 Current Phasor quantities from CT 9 of transformer Zone for case 6.2.2.

Table 6-6 Summary of the hypothesis testing at t=2.0s for case 6.2.2.

Hypothesis #	Hypothesis	Result
1	Power fault in distribution line	Low confidence level
2	Hidden failure in CT-9A	Low confidence level
3	Power fault in distribution line & Hidden failure in C9-9A	High confidence level
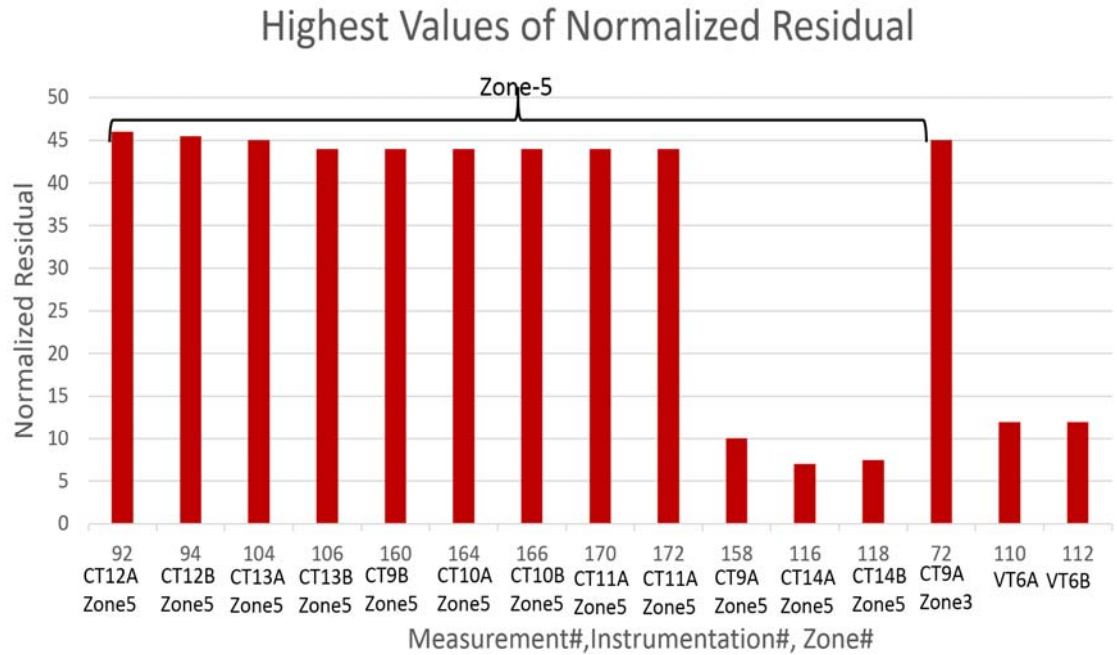
Figure 6-34 The highest values of the normalized residual for case 6.2.2.
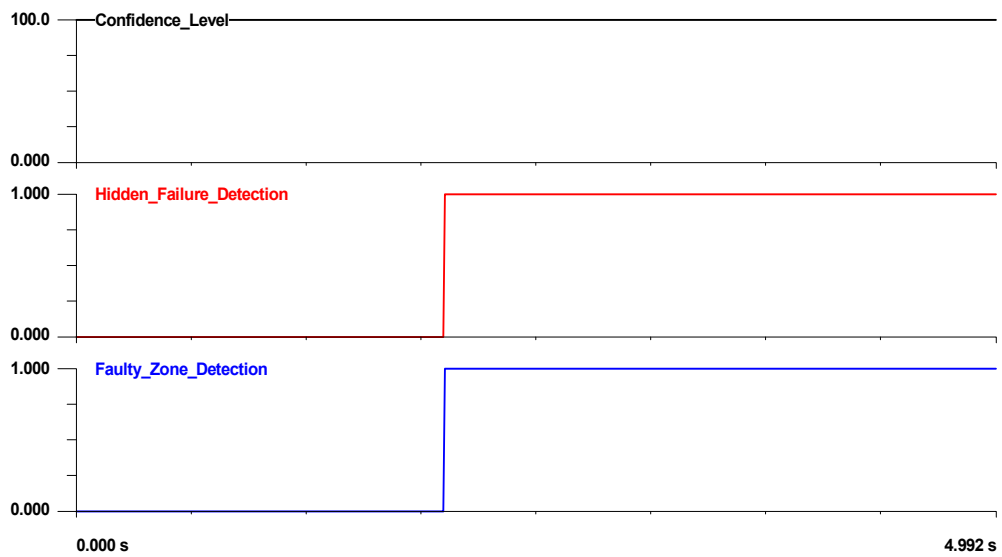
Figure 6-35 The outcome of DSEBCPS for case 6.2.2
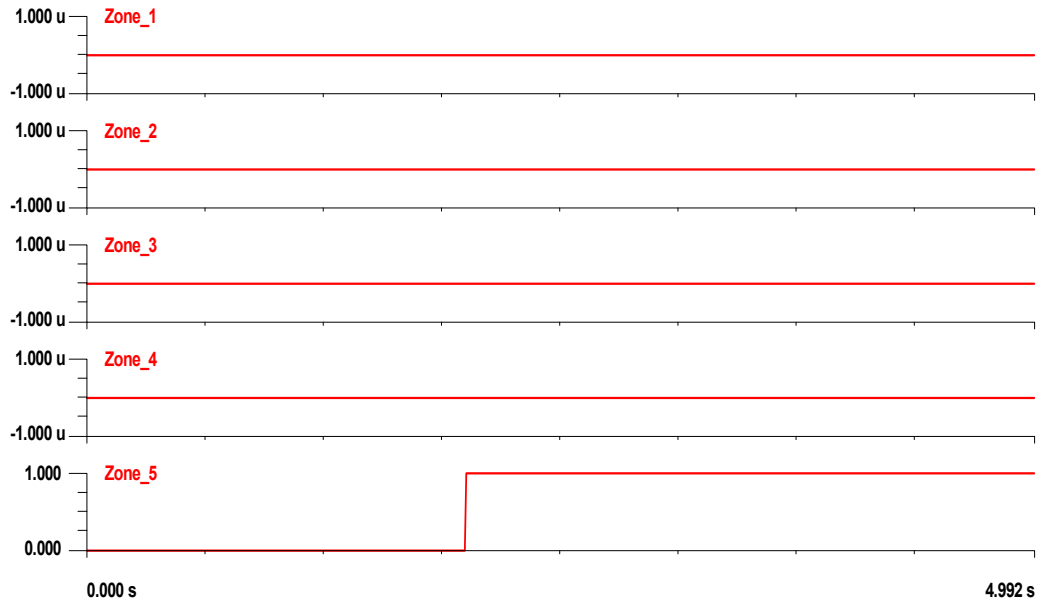
Figure 6-36 Faulty zone status for case 6.2.2
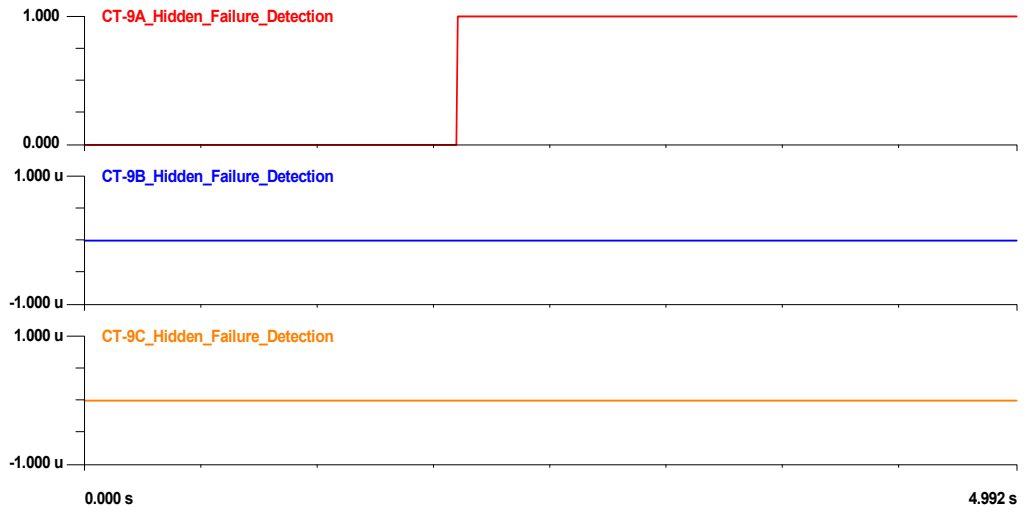
Figure 6-37 Hidden failure status for case 6.2.2.

Settingless Relay Corrected Response

Figure 6-38 shows the corrected response of the setting-less relay. This figure shows that the detected bad signal from CT-9 has been replaced by the calculated measurement computed in the DSEBCPS as explained in Chapter 5. The calculated sampled values are streamed from the DSBCPS to the settingless relay with their time stamps to override the compromised measurements in the settingless relay. Furthermore, the confidence level of the setting-less relay responded to the replacement of the bad data and recovered to a high level, as shown in Figure 6-38, which also shows that the trip signal was not initiated because of the two-cycle delay introduced in the operation of the setting-less relay.
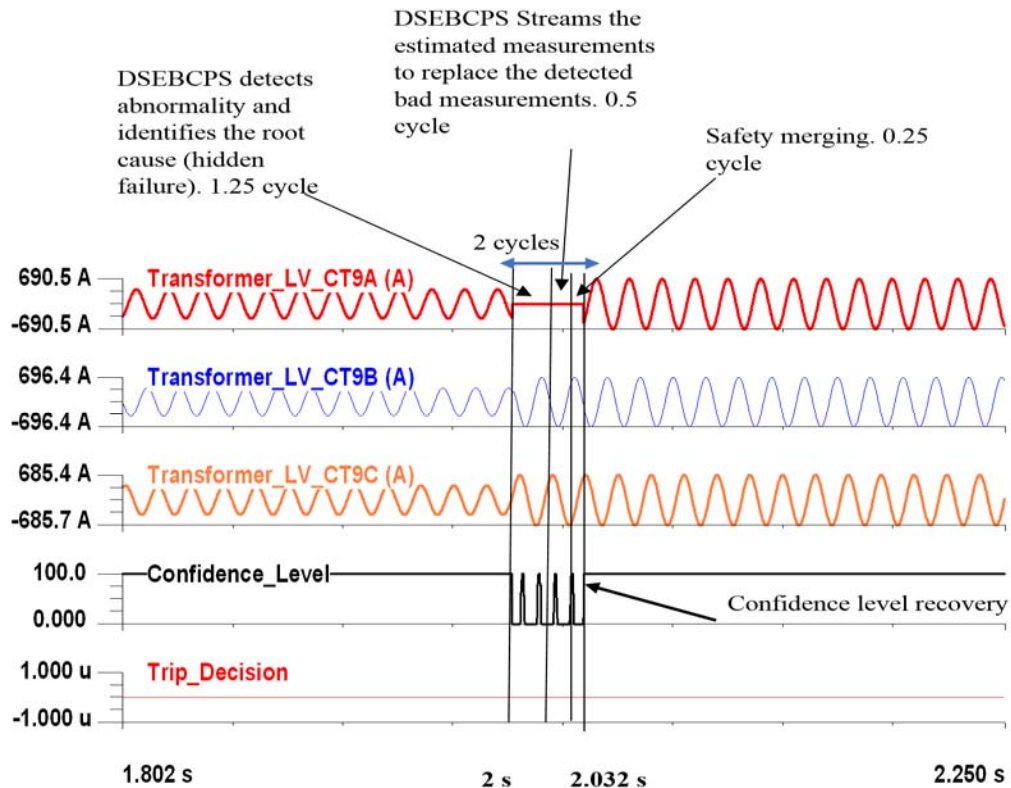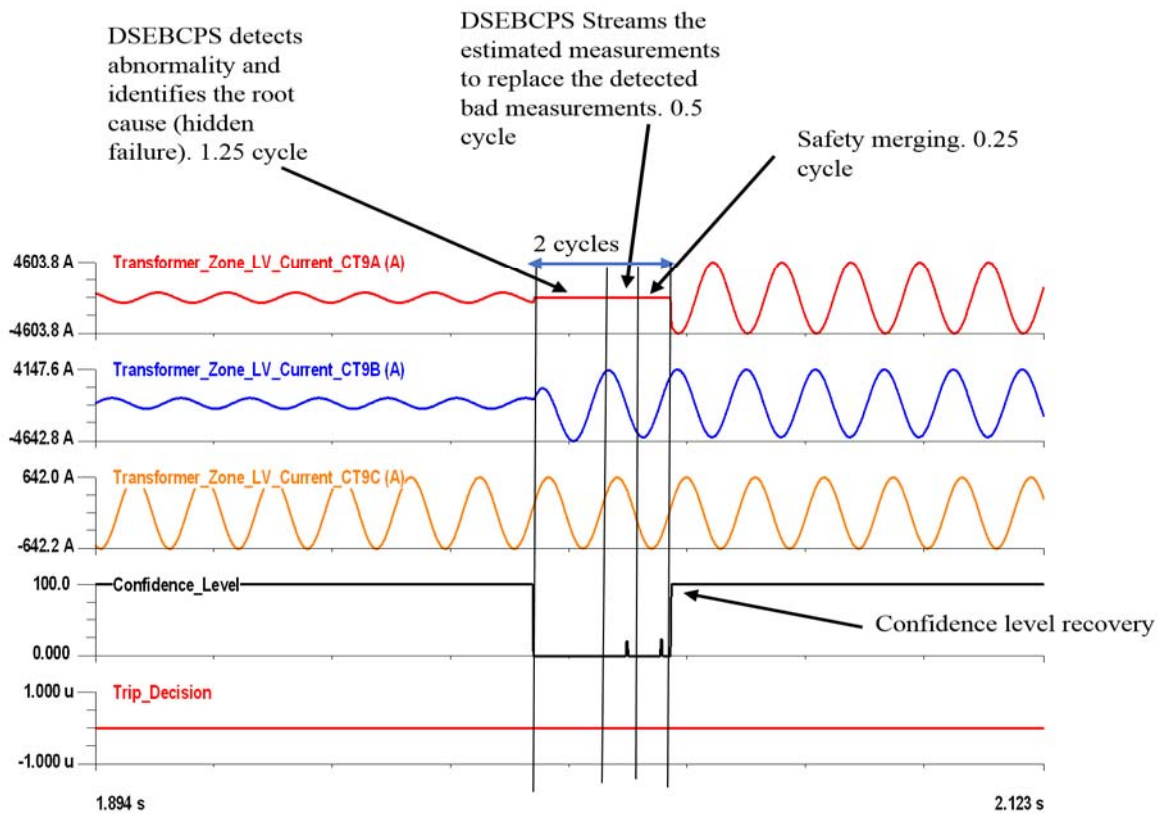

Figure 6-38 Corrected response of settingless relay of transformer zone for case 6.2.2.

6.3   Case 3: CT Saturation

CT saturation is one of the common hidden failure modes that might cause relay misoperation. This mode of hidden failure is modeled and simulated to test the response of the settingless relay and the DSEBCPS. specifically, CT-3, phases A and B, which provide the settingless relay of the transmission line zone with the current measurement, were modeled to saturate during phase to phase fault in the primary side of the transformer. The model entailed increasing the CT burden to a higher level that drives the CT to saturate during fault condition. Moreover, we increased the short circuit level of the source to drive a higher short-circuit current. The sequence of events started by initiating phase to phase fault inside the transformer at t=1.5 seconds; the fault was cleared at around t=2 seconds. The case was simulated during a no-load condition. The performance of the settingless relay for the transformer zone, as well as the proposed DSEBCPS, is presented below.

Settingless Relay

Figure 6-39 shows the current waveforms of the primary side of the transformer depicted from the settingless relay of the transformer zone. It shows that the transformer zone experienced phase to phase fault between phase A and phase B. Moreover, Figure 6-39 depicts the relay operations for this event, which shows that the confidence level of the relay dropped and the trip signal was initiated. This operation is correct, given the fault within the transformer zone. Figures 6-40 and 6-41 show the output of the settingless relays of the transmission line zone. Both figures show that the current waveforms of CT3, phase A and phase B are distorted because of the CT saturation. The response of the settingless relay depends on whether the CT model was included in the overall zone model.

In the event the CT model is not included, the relay will operate and initiate a trip signal as shown in Figure 6-40, because the saturated wave violates the overall transmission line model. This action is considered as a relay misoperation because of hidden failure. However, if the CT model is included with the zone models, the relay will not operate as shown in Figure 6-41; this is because the CT model captures the saturation condition.
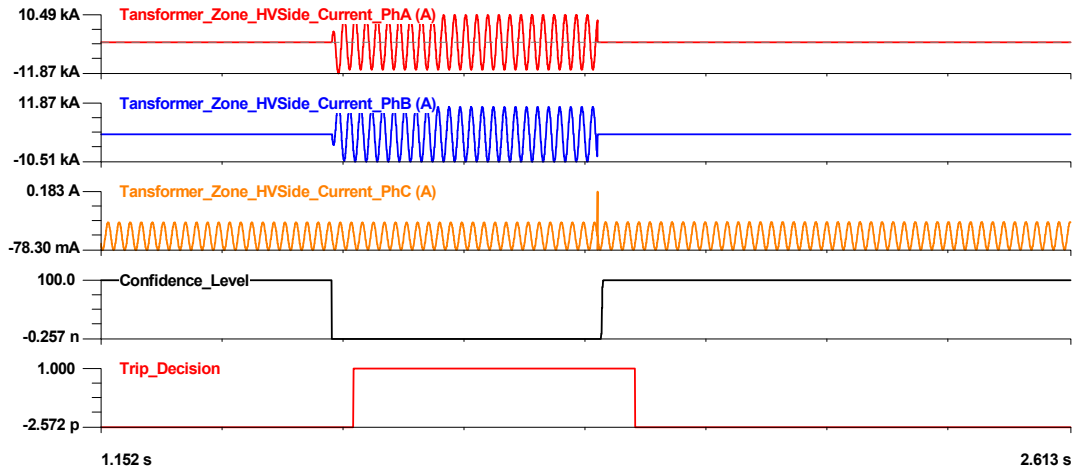
Figure 6-39 The outcome of the settingless relay of the transformcer zone for case 6.3.
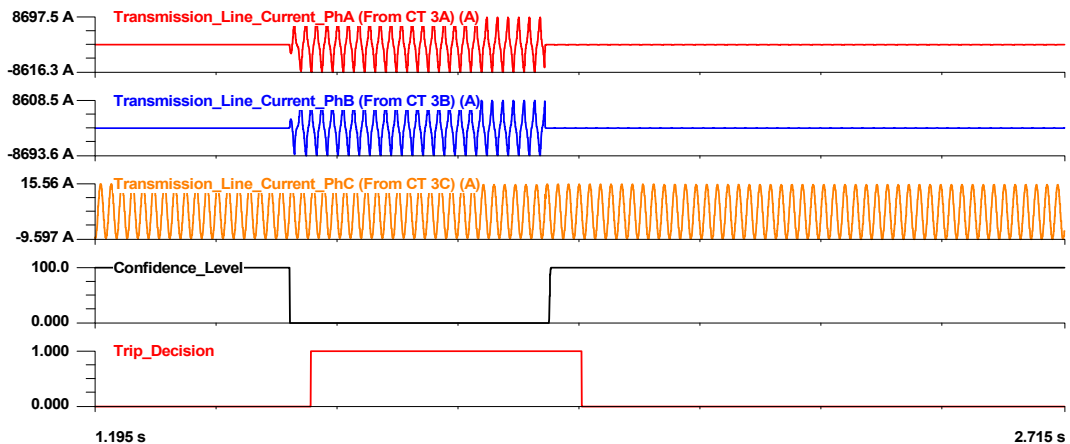
Figure 6-40 The outcome of the settingless relay of the transmission line without the CT model for case 6.3.
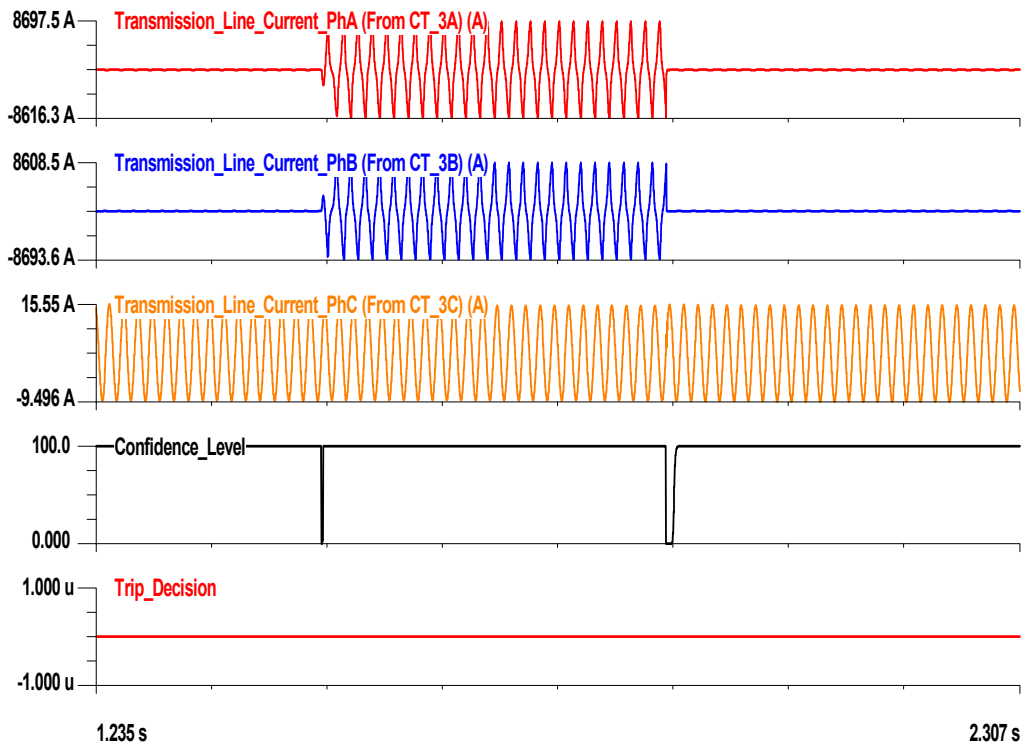
Figure 6-41 The outcome of the settingless relay of the transmission line with CT model for case 6.3.

DSEBCPS

Figure 6-42 depicts the phasor quantities of the current measurement of the primary side of the transformer, clearly showing that the transformer experienced phase to phase fault in the primary side of the transformer. Moreover, Figure 6-42 shows the phasor quantities of the current measurement extracted from CT-3. There is a notable reduction in the current magnitude of phase A and phase B because of the CT saturation.

The DSEBCPS responded to both events by initiating the hypothesis testing summarized in Table-7. There were three hypotheses under consideration. The first two considered a single event of either hidden failure or power fault, which both failed to restore

high confidence level of the substation. The third hypothesis combined the previous two hypotheses by considering both power fault in the transformer and hidden failure in CT 3A and B. The selection of these two hypotheses was based on the values of the normalized residuals. As shown in Figure 6-44, measurement#42 experienced the highest normalized residual. This measurement satisfied the transformer common mode criterion and therefore, all transformer measurements were grouped as a set of suspicious measurements. Furthermore, measurement #25 experienced the second highest normalized residual of the measurements that was not included in the first set of suspicious measurements. These measurements satisfied the instrumentation channel common mode criterion of CT3 phases A and B. Accordingly all measurements extracted from CT3A and CT3B were grouped as a second set of suspicious measurements. Subsequently, The DSEBCPS removed both set of suspicious measurements from the measurements set and rerun the DSE. This hypothesis was successful as indicated by the high confidence level of the substation as shown in Figure 6-45. Moreover, as an outcome of the two-level hypothesis testing, the DSEBCPS detected a faulty zone and hidden failure in the substation as shown in Figure 6-45. Furthermore, the DSEBCPS specified which part of the substation suffered from hidden failures and the fault as shown in Figures 6-46 and 6-47, respectively. This simulation also shows that the redundancy in the measurements makes two-level hypothesis testing very efficient because the measurements that display abnormalities experienced the highest normalized residuals which placed them first in the removal process.

Table 6-7 Summary of the hypothesis testing at t=1.5s for case 6.3.

Hypothesis #	Hypothesis under consideration	Result
1	Power fault in Transformer	Low confidence level
2	Hidden failure in CT-3A and 3B	Low confidence level
3	Power fault in Transformer & Hidden failure in C3-A and 3B	High confidence level
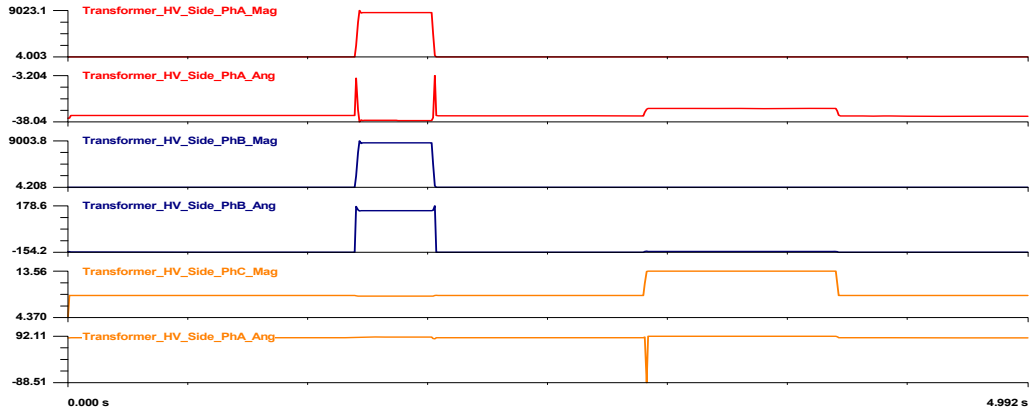
Figure 6-42 Current phasor quantities of the primary side of the transformer for case 6.3.
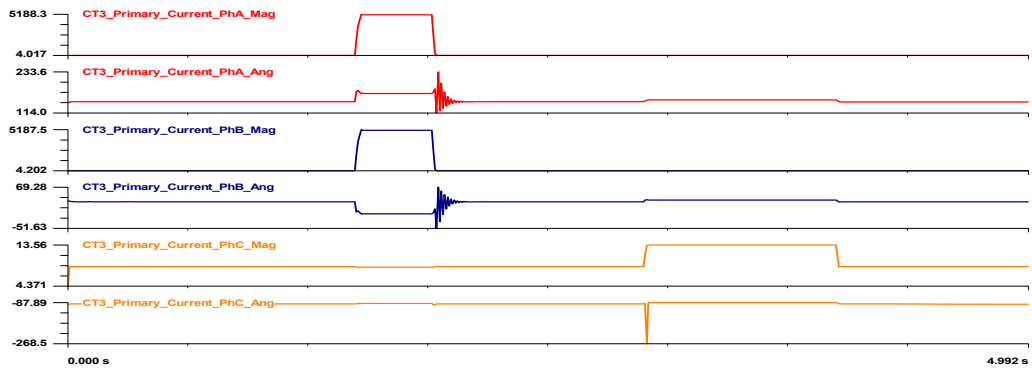
Figure 6-43 Current phasor quantities of the calculated primary side of CT-3 for case 6.3
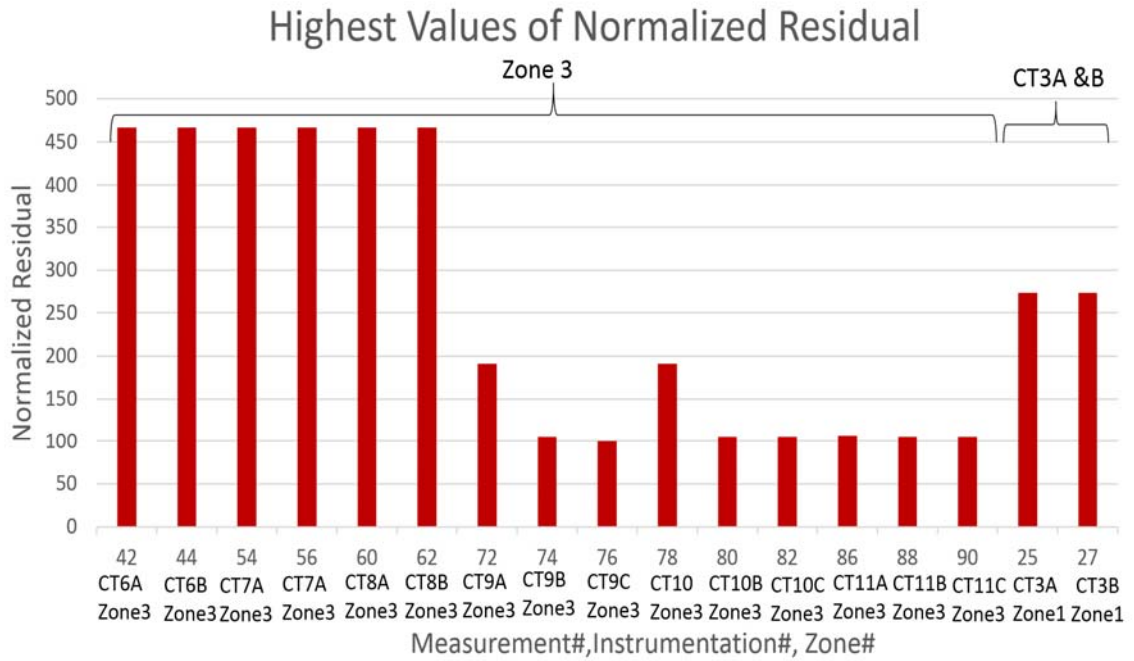
Figure 6-44 The highest values of the normalized residual for case 6.3
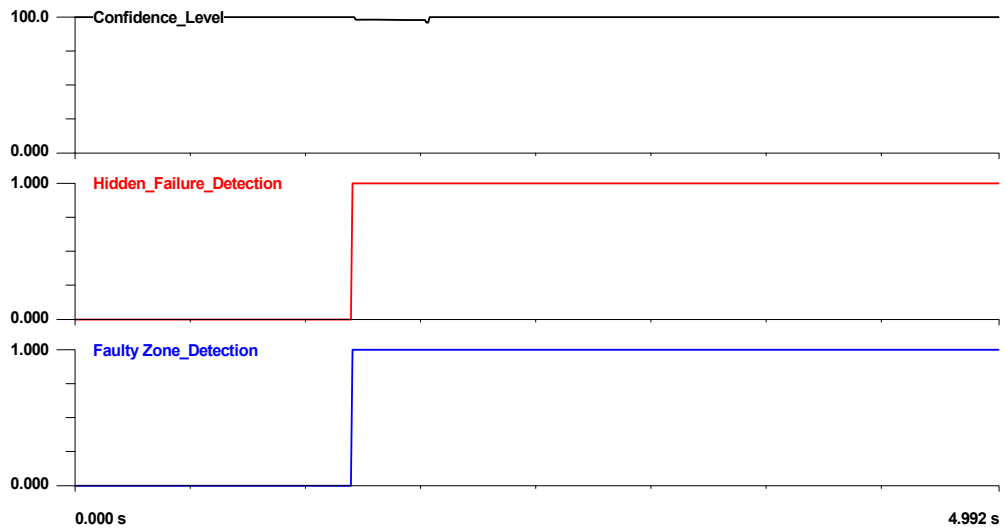
Figure 6-45 The outcome of DSEBCPS for case 6.3
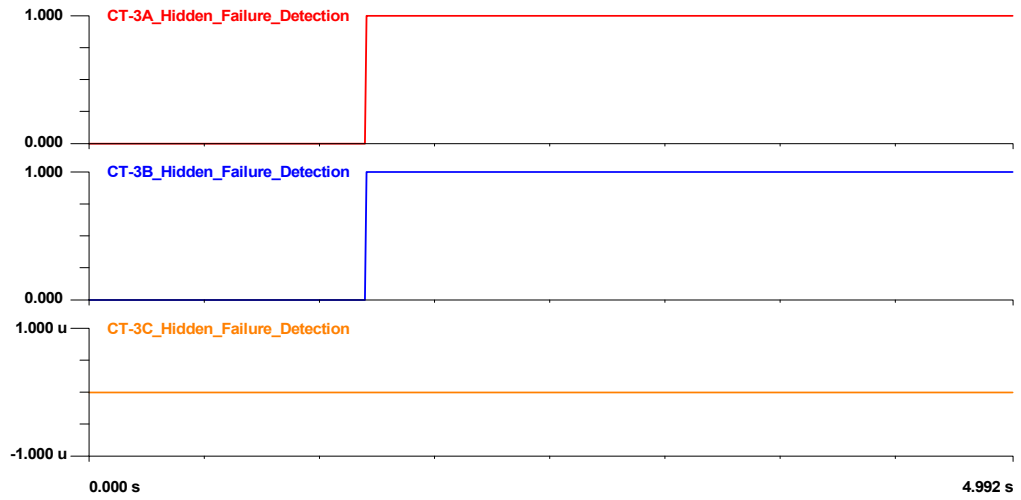
Figure 6-46 Hidden failure detection for case 6.3.
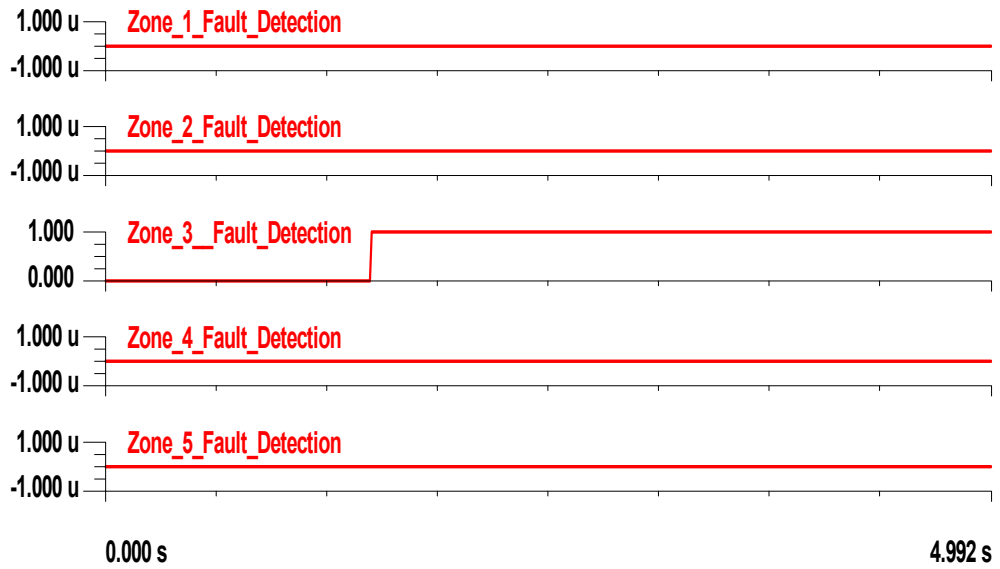
Figure 6-47 Faulty zone detection for case 6.3.

Settingless Relay Corrected Response

Similar to the previous cases, the DSEBCPS streamed the calculated sampled values corresponding to the detected bad signals to the settingless relay of the transmission line zone to override the bad signals. This process is depicted in Figure 6-48.
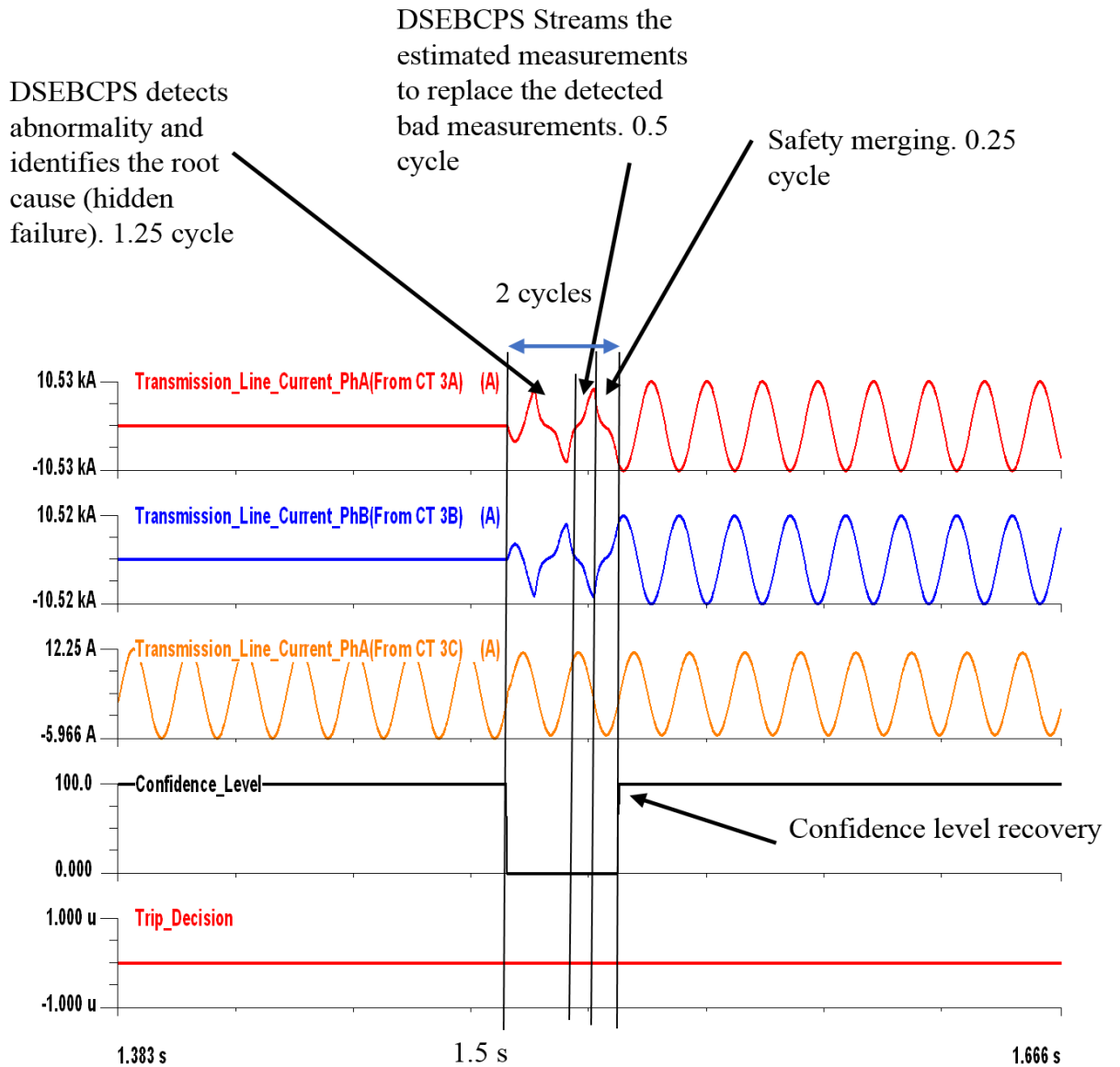
Figure 6-48. Corrected response of settingless relay of transmission line zone for case 6.3.

6.4 Case4: CT Reverse Polarity

CT reverse polarity is one type of hidden failures in the CT circuit. Typically, this event occurs following pre-commissioning activities for a new substation or maintenance activities for an existing substation. In either case, the problem remains hidden following the energization until the affected zone is loaded. This case simulates the CT reverse polarity to analyze the response of both the setting-less relay and the DSEBCPS. Specifically, we modeled CT-10 phases A, B, and C, which provide the setting-less relay of the transformer zone with the current measurements, with reverse polarity by swapping the terminals of each CT at the relay terminals. The sequence of events starts with energizing the substation at t=0 s with no load. Then, the transformer is loaded with 15 MW at t=3 s. The response of the settingless relay and the DSEBCPS is presented below.

Settingless Relay

Figure 6-49 shows the current waveforms of the secondary side of the transformer depicted from the setting-less relay of the transformer zone. The figure shows 180 degree-phase shift between the current waveforms extracted from CT 9 (i.e., the healthy CT) and CT 10 because of the reverse polarity. Figure 6-49 also depicts the setting-less relay operation for this event, which shows that the relay operated and initiated a trip signal to isolate the transformer. This response is a relay misoperation because of the hidden failure. This case demonstrated the negative consequences of the hidden failure in power system operation, which requires a proper action.
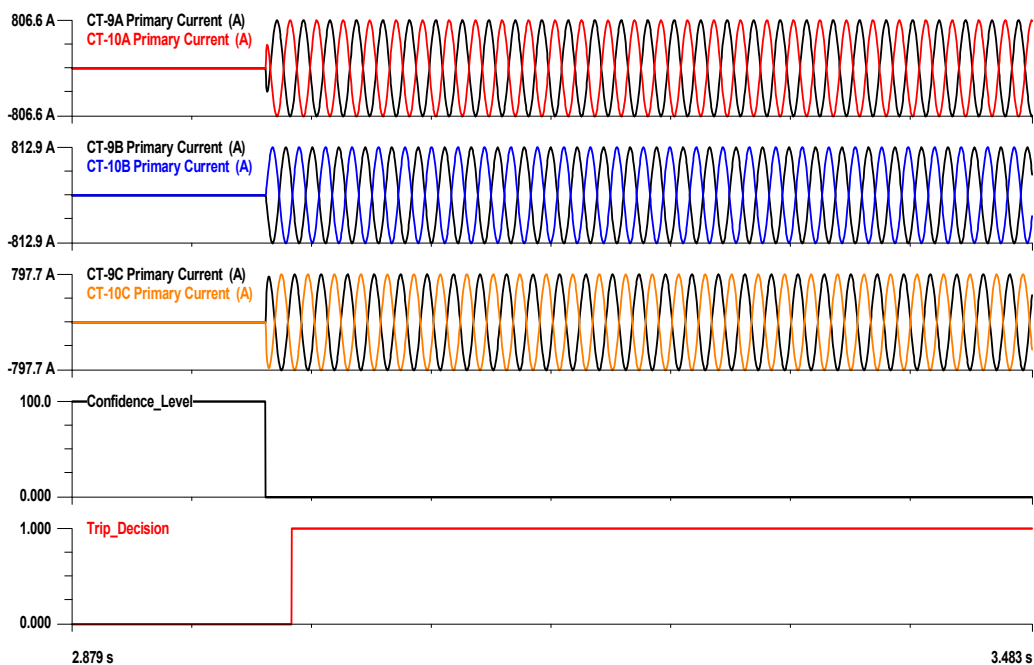
Figure 6-49 The outcome of the settingless relay of the transformer zone for case 6.4.

DSEBCPS

Figure 6-50 shows the angles of the current waveforms extracted from CT-10 compared to the angles of current waveforms extracted from CT-9. The DSEBCPS responded to the event of the hidden failure by initiating hypothesis testing summarized in Table 6-8. During such testing the DSEBCPS verified the values of the normalized residuals of the measurements and extracted the highest value. According to Figure 6-51, measurement #78, extracted from CT-10 phase A experienced the highest normalized residual. This measurement was subjected to device common mode criteria verification, which revealed the instrumentation channel common mode criterion associated with CT-10, phases A, B, and C was satisfied. Accordingly the hypothesis under consideration was hidden failures in CT-10 phases A, B and C. Subsequently all measurement extracted from these

110

instrumentation channels were grouped as suspicious measurements and removed from the measurements set. The DSEBCPS rerun the DSE which revealed high confidence level as shown in Figure 6-52. This indicates a successful hypothesis. Accordingly, the DSEBCPS detected hidden failures within the substation and did not detect any faulty zones. Additionally, the DSEBCPS precisely identified the instrumentation channels that suffer from the hidden failures, as shown in Figure 6-53. This case demonstrates the advantage of redundancy in the measurements, which makes the hypothesis testing very efficient by placing the detected faulty measurements first during the removal process.
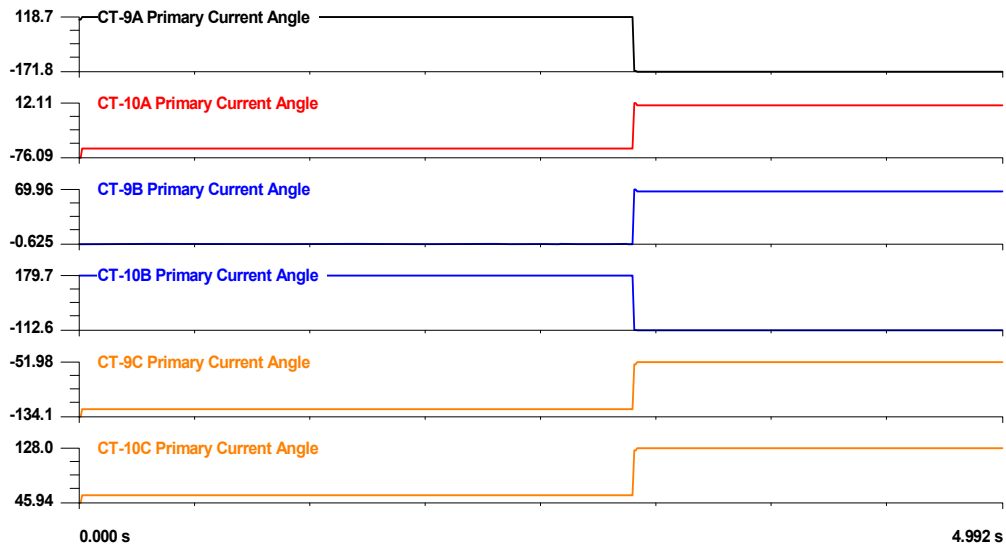
Figure 6-50 Angles of the current waveform extratced from CT9 and CT 10 for case 6.4

Table 6-8 Summary of the hypothesis testing at t=3s for case 6.4.

Hypothesis #	Hypothesis under consideration	Result
1	Hidden Failure in CT-10A,B and C	High confidence level
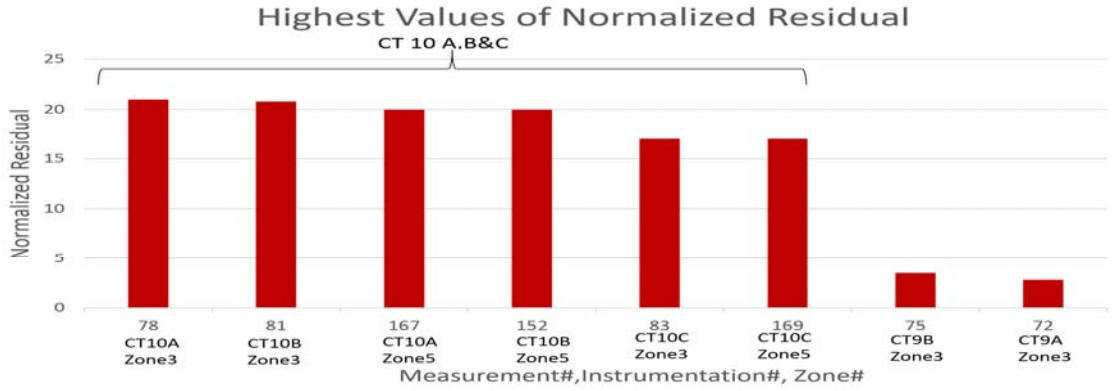
Figure 6-51 The highest values of the normalized residual for case 6.4
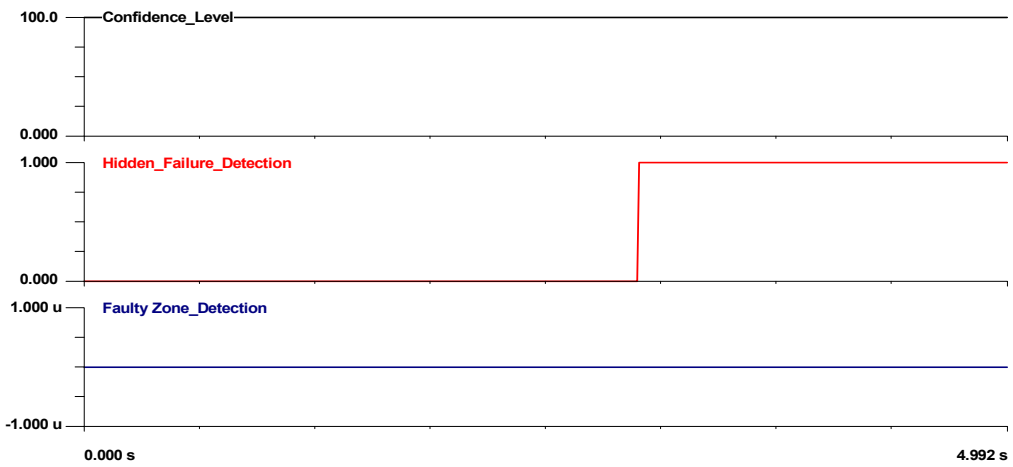
Figure 6-52 The outcome of DSEBCPS for case 6.4.
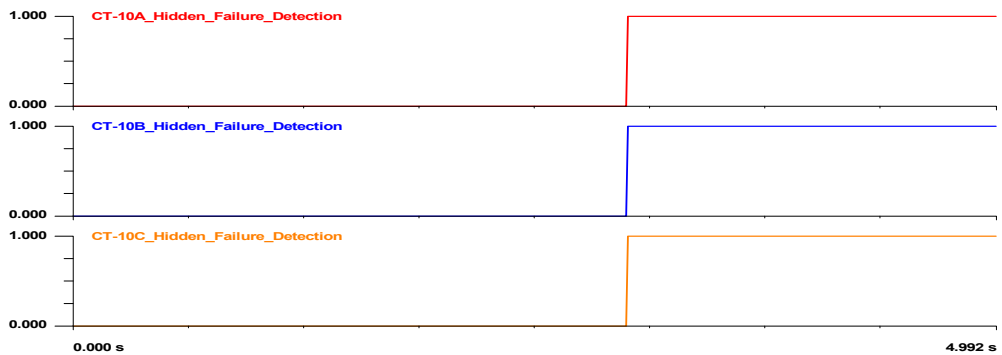
Figure 6-53 Hidden failure detections for case 6.4

Corrected Response of Settingless Relay

Similar to the previous cases, the detected bad waveform in the settingless relay were overridden by calculated sampled values computed in the DSEBCPS and streamed to the settingless relay as shown in Figure 6-54. This process results in confidence level recovery which eliminates the initiation of the trip signal.
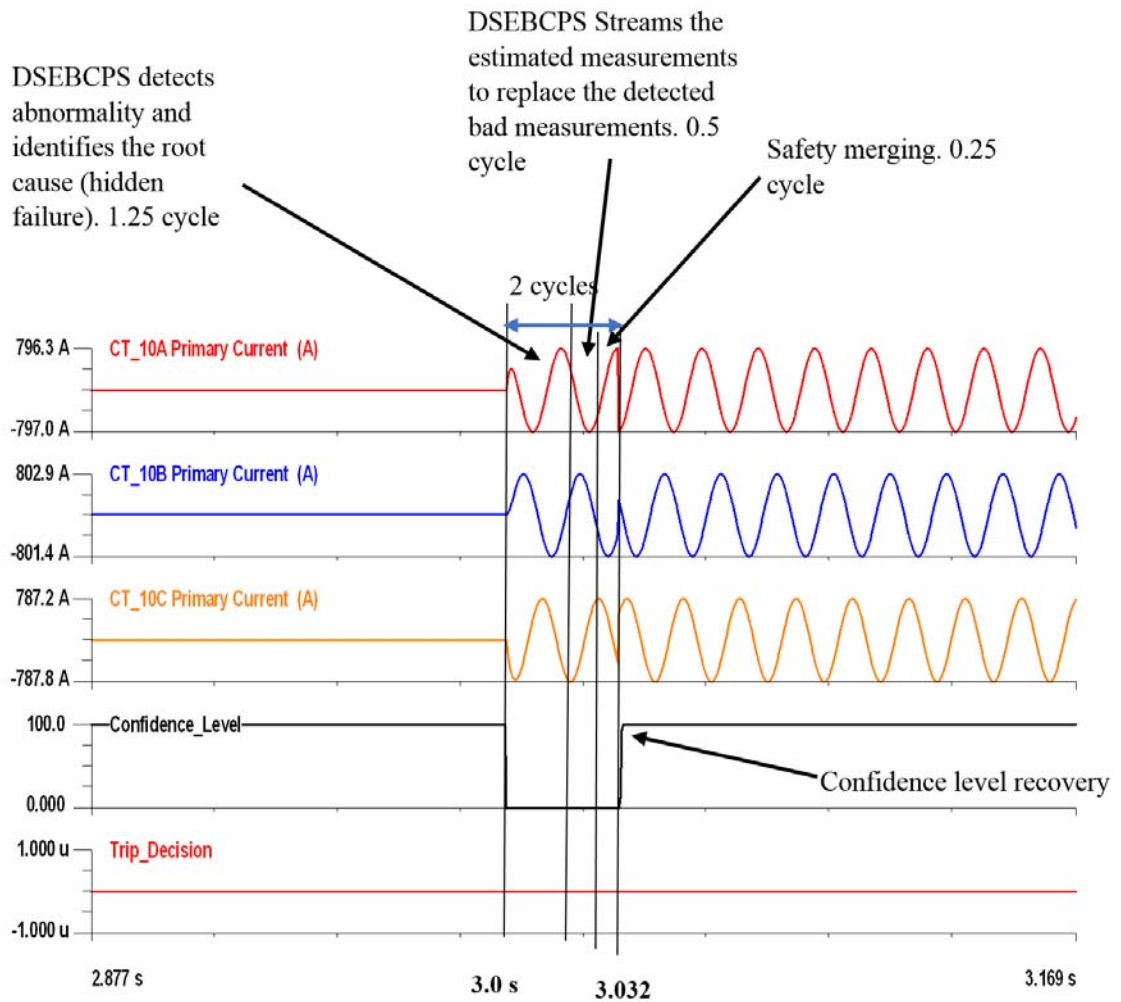
Figure 6-54 Corrected response of settingless relay of transformer zone for case 6.4.

6.5 Case5: CT Incorrect Ratio Settings

Another common hidden failure that could affect protection system operation is the incorrect CT ratio setting. It is usually a protection engineer's responsibility to provide the relay setting, which includes the CT ratio. Therefore, if the engineer sets the ratio incorrectly or the technician implements it in the relay inaccurately, the relay will have the incorrect setting. Subsequently, the settingless relay will read the incorrect primary current values and might misoperate. Generally, this event occurs following pre-commissioning activities for a new substation or maintenance activities for an existing substation. In both cases, the problem remains hidden following the energization until the affected zone starts to be loaded. This case examines the effect of the wrong CT ratio setting in the settingless relays and DSEBCPS. More specifically, the ratio associated with CT-10, phases A, B, and C, which provide the settingless relay of the transformer zone with the current measurements, is set to 1000/5 instead of 4000/5 (i.e., the correct ratio). The sequence of events starts by energizing the substation at t=0 seconds with no load. Then, the transformer is loaded with 15 MW at t=3 seconds. The results of the settingless relays of the transformer zone, as well as the proposed DSEBCPS, are presented below.

Settingless Relay

Figure 6-55 shows the current waveforms of the secondary side of the transformer seen in the settingless relay of the transformer zone. It shows a drop in the current measurement of CT-10 compared to CT-9 because of the wrong CT ratio. Figure 6-55 also depicts the settingless relay operation for this event, which shows that the relay operated

114

and initiated a trip signal to isolate the transformer. This response is a relay misoperation because there was no faulty condition in the transformer.
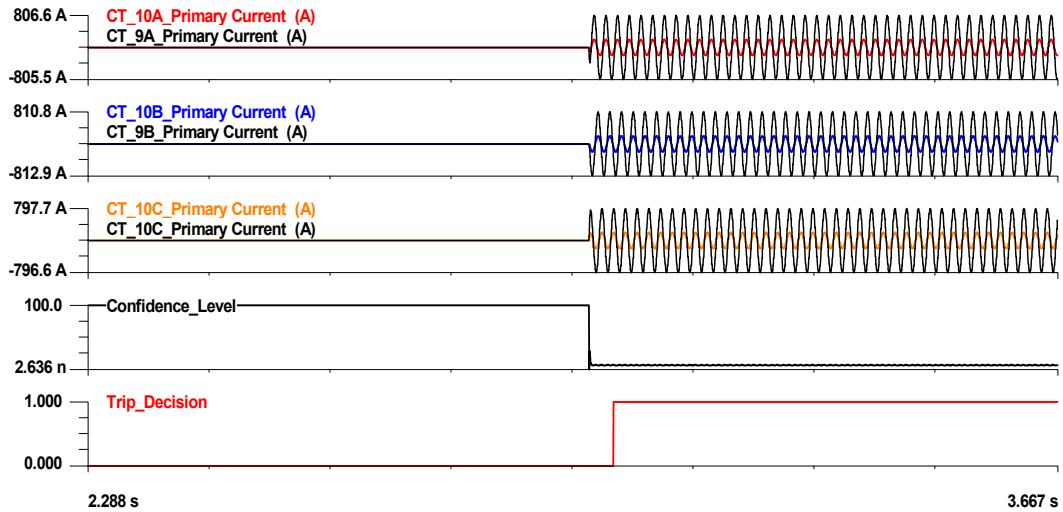
Figure 6-55 The outcome of the settingless relay of the transformer zone for case 6.5.

DSEBCPS

Figure 6-56 shows the magnitude of the phasor currents extracted from CT-9 and CT-10. The figure clearly shows the reduction in the current magnitude seen by the DSEBCPS because of the wrong CT ratio. This event caused the confidence level of the substation to drop. Therefore, DSEBCPS initiated hypothesis testing (Table 6-9), during which the DSEBCPS verified the values of the normalized residuals of all the measurements and extracted the highest value. According to Figure 6-57, the measurement #81 extracted from CT-10, phase B has the highest normalized residual. Hence, the DSEBCPS selected this measurement as suspicious measurement and subjected it to device common-mode criterion. For this case, the instrumentation channel common mode criterion associated with CT-10, phases A, B and C was satisfied. Therefore, the hypothesis

under consideration was hidden failure in CT-10, phases A, B and C. Subsequently, the DSEBCPS removed all the measurements extracted from CT10 and rerun the DSE. Figure 6-58 shows that this hypothesis was successful and resulted in a high confidence level. Moreover, The DSEBCPS managed to detect hidden failures within the substation and did not detect a faulty zone. Additionally, the DSEBCPS identified the instrumentation channels that suffer from the hidden failures, which is CT-10 as shown in Figure 6-59. As in the previous cases, we see the advantage of the redundancy at the substation level in making the hypothesis testing very efficient.
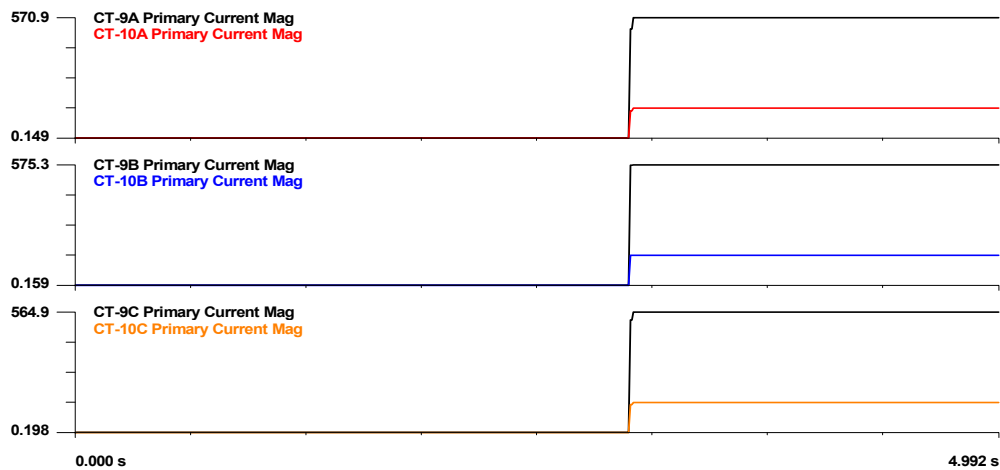
Figure 6-56 Magnitudes of the current phasor quantities of CT9 and CT 10 for case 6.5.

Table 6-9 Summary of the hypothesis testing at t=3 s for case 6.5

Hypothesis #	Hypothesis under consideration	Result
1	Hidden Failure in CT-10A,B and C	High confidence level
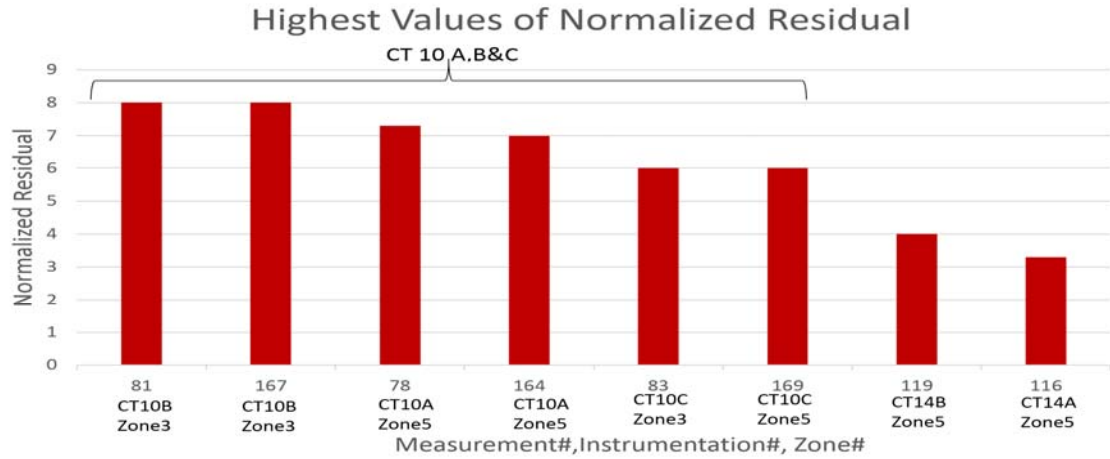
Figure 6-57 The highest values of the normalized residual for case 6.5.
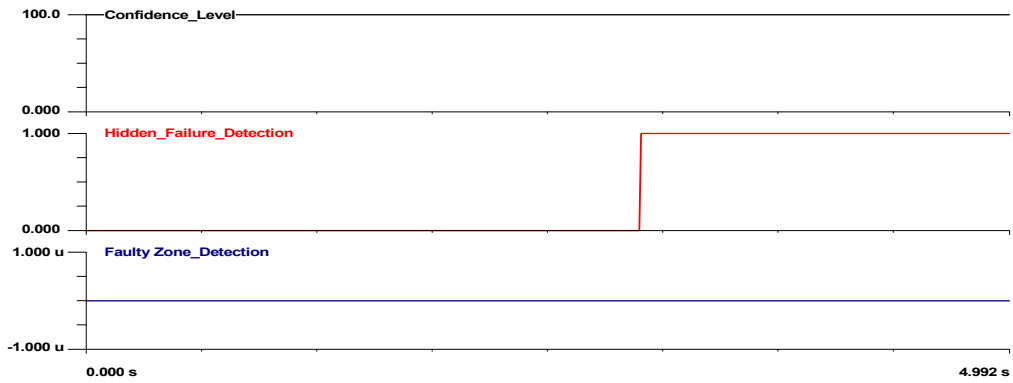
Figure 6-58 The outcome of DSEBCPS for case 6.5.
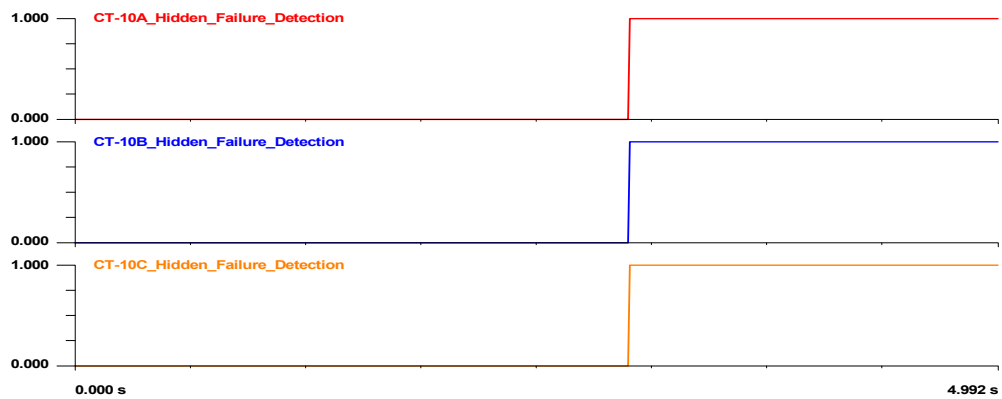
Figure 6-59 Hidden failure detections from DSEBCPS for case 6.5.

117

Corrected Response of Settingless Relay

Similar to the previous cases, the response of the settingless relay is corrected by replacing the detected bad measurements, as shown in Figure 6-60. The DSEBCPS streamed the calculated sampled values corresponding to the bad signal to override the bad measurements in the settingless relay of the transformer zone. Accordingly the confidence level recovered and the relay did not initiate the trip signal.
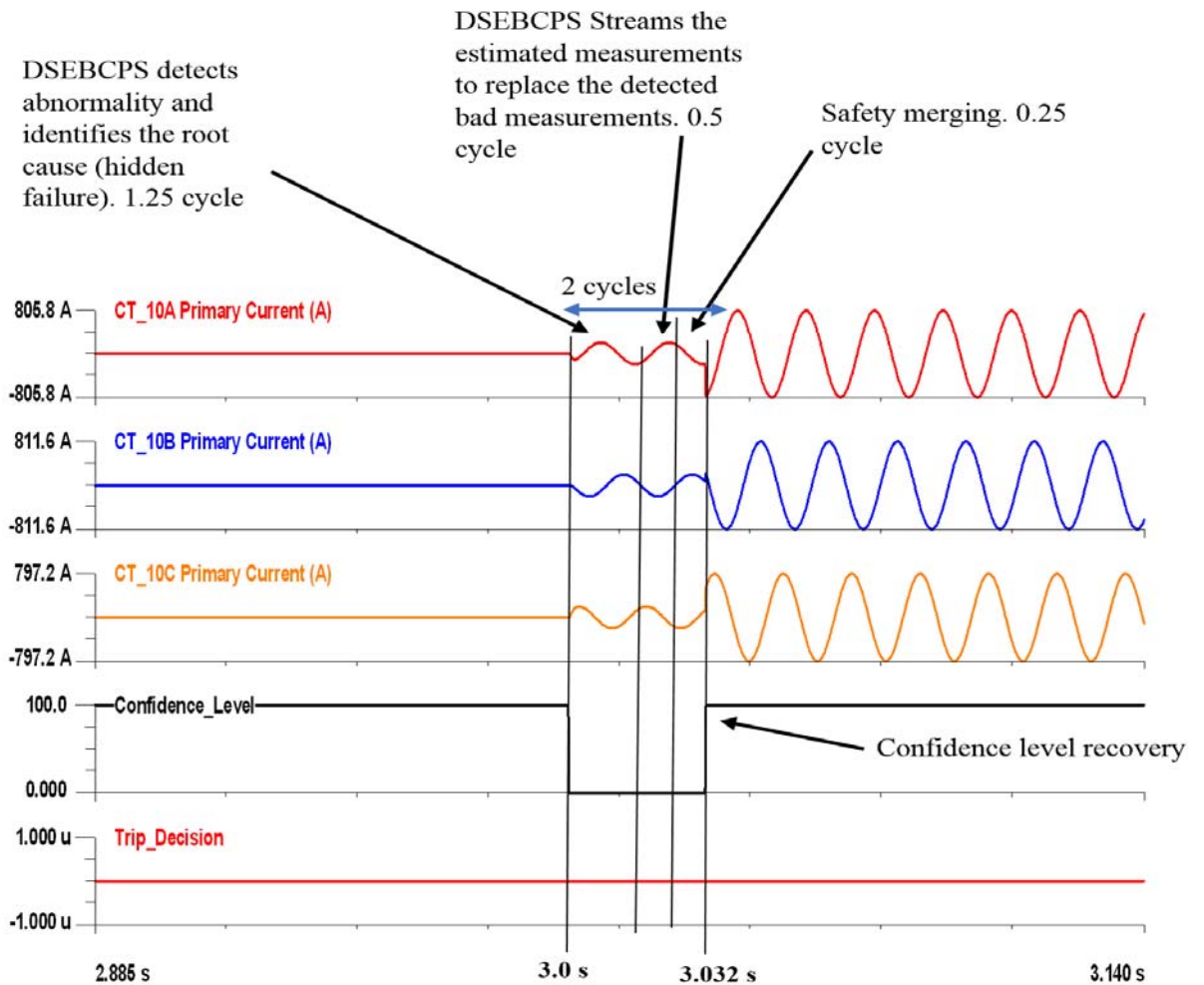
Figure 6-60 Corrected response of settingless relay of transformer zone for case 6.5.

6.6　Summary

This chapter demonstrated the capability of the DSEBCPS to detect hidden failures in real time. Moreover, it shows the capability of the DSEBCPS to secure the settingless relay operation during hidden failures while maintaining high degree of dependability. Five cases of hidden failures were simulated: (1) PT blown fuse, (2) CT saturation, (3) CT short circuit, (4) CT reverse polarity, and (5) Wrong CT ratio setting. The DSEBCPS managed to detect the hidden failure for each case and identified the instrumentation channels that suffer from the hidden failures. Additionally, the simulation cases demonstrated the DSEBCPS capacity to distinguish between hidden failures and power faults through the hypothesis testing. Furthermore, the cases show the advantage of high redundancy in the measurements at the substation level, which makes hypothesis testing quite efficient because the suspicious measurements always experience the highest normalized residual. This characteristic eliminates the possibility of leverage points and places the suspicious measurements first in the removal process for the bad data.

CHAPTER 7.   SYSTEM ARCHITECTURE

7.1   Introduction

Critical to this work is the ability to manage data and communications between the various devices (i.e., merging units, settingless relays and DSEBCPS) within the substation and also between the substation and the control center. We define the details of the system architecture, which specifies data management, communication protocols, and the hierarchical structure of the system. Figure 4-2 in Chapter 4 depicts conceptually the top view of the architecture, which shows that the system consists of the following three layers of communication: (1) the communication between merging units (MUs) and settingless relays through the process bus, (2) the communication between settingless relays and DSEBCPS through the station bus, and (3) the communication between DSEBCPS and the control center through the station bus. This chapter explains the details of our proposed design for each layer and how the layers interact with one another to form the overall system architecture. Our design for this architecture complies with IEC-61850 standard requirements. We achieve this compatibility by using the data objects, services, and communication protocols defined in the standard. The implementation of IEC 61850 permits interoperability between products from different vendors, which enables seamless migration to our proposed scheme within existing substations [1]. Furthermore, this chapter sheds light on this approach's long-term goals: to support the next generation of energy management systems (EMS), where the proposed system will provide the necessary data and real-time models to the control center for performing the usual control center functions, including state estimation, optimization, and control.

7.2   IEC 61850 Overview

The main objective of IEC 61850 is to standardize data communication within the substation [7], [71]. The overall concept of IEC 61850 uses abstract modeling and virtualization approaches [7], [71], [72]. Abstract modeling entails creating abstract definitions of data items/objects and services that are independent of the communication protocol [7], [73], [74]. Data modeling, which is performed using an object-oriented approach, consists of logical nodes (LNs) that represent functions or equipment that exchange data [7], [75]. Abstract services are services that act on the data to read, write, issue control commands, receive alarms, and manage audit logs [76], [77]. IEC 61850-7-1 explains virtualization as a tool "that provides a view of those aspects of a real device that are of interest for the information exchange with other devices." Figure 7-1 illustrates this concept, showing that the real devices on the right-hand side are modeled virtually as LNs [71]. Furthermore, the standard defines communication protocols to map the abstract models of data and services for data transfer between interfaces. Several protocols satisfy the application requirements in terms of performance and technicality. Finally, the standard specifies a configuration tool to put each individual part of the system together. This configuration is implemented using XML-based Substation Configuration Language (SCL), which provides the topology of the entire system in the context of IEC 61850 [78]. The standard's advantage is that it provides a uniform communication mechanism within the substation that every IED vendor is obligated to follow. Therefore, utilities enjoy interoperable IEDs regardless of their manufacturer, which saves a significant amount of time, cost, and effort in dealing with the system. Moreover, the standard provides the flexibility to accommodate new applications as they evolve or are introduced to the market.
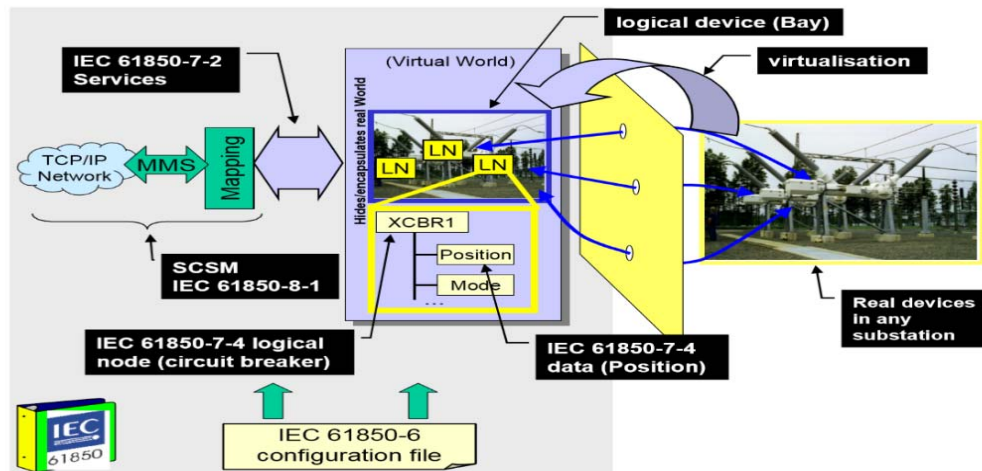
Figure 7-1 IEC 61850 virtual modeling approach [71].

7.2.1 Abstract Data and Service Modeling in IEC 61850 Context

The modeling process starts by introducing a virtual representation of a physical device through a logical device [7]. The physical device, which may contain several logical devices, is an actual device connected to the network and typically defined by its network address. Furthermore, each logical device contains one or more LNs that represent a set of data and services associated with a power system function [73], [75], [79]. The LNs are grouped according to the nature of the data and function of each LN. Therefore, the names of LNs begin with a character that represents their group; for example, the LNs for automatic control start with the letter "A" [75]. Additionally, each LN contains several data elements, each of which is assigned a unique name specified in the standard. An example of an LN and its data elements is an XCBR LN, which is used to model a circuit breaker. Its data elements include Loc to indicate remote or local operation, OpCnt to indicate operations count, Pos to indicate position status, a BlkOpn block to indicate open commands, a BlkCls block to indicate close commands, and CBOpCap for the circuit breaker operating capability [75]. These data elements belong to common data classes

122

(CDCs) specified in IEC 61850-7-3. The CDC describes the nature and structure of the data within the LN [73], [80]. The specified CDCs are, for example, controllable status information, controllable analog set point information, status settings, and analog settings. Each CDC has a defined name and a set of data attributes; the data attributes are simply the data elements, such as the status of the breaker. Figure 7-2 shows the overall data modeling approach.
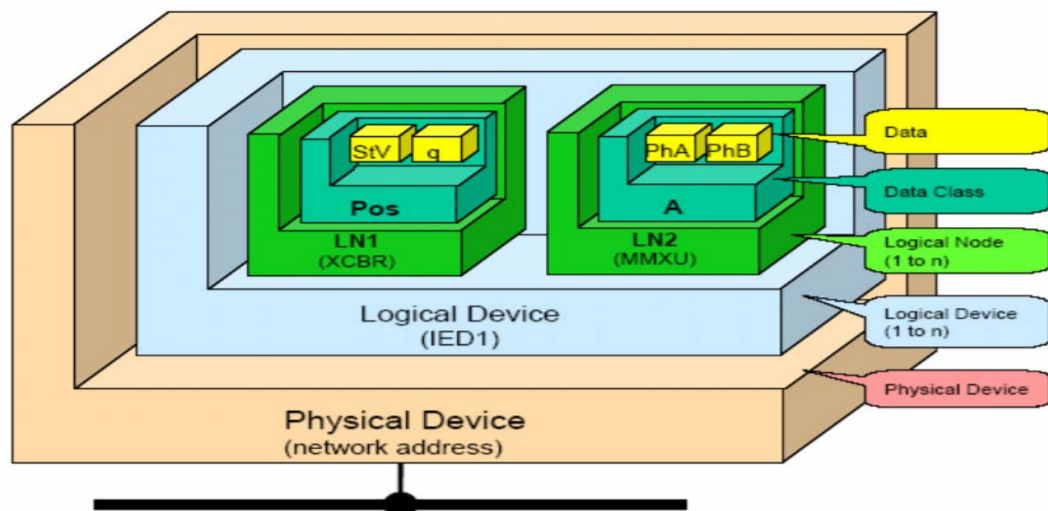
Figure 7-2 IEC 61850 data modeling [73].

Data is communicated between different LNs within the substation by abstract services defined in IEC 61850, part 7.3. Figure 7-3 shows a top view of communication using these services [74].
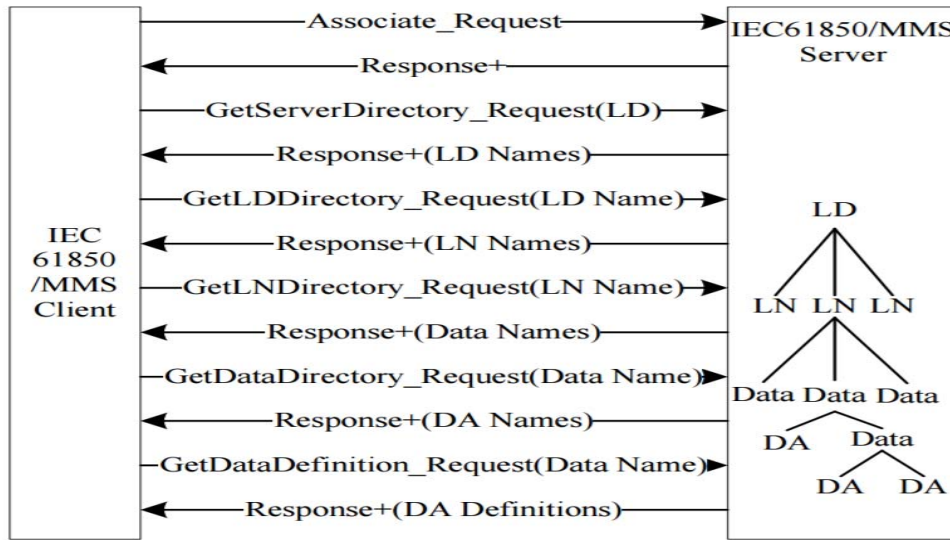
Figure 7-3 IEC 61850 abstract services acting on data models [74].

7.2.2 *Communication Protocols*

The abstract data models and services defined in IEC 61850 can be mapped to several communication protocols defined in IEC 61850-8-1 and depicted in Figure 7-4 [81]. Furthermore, Figure 7-5 shows the performance requirement for each application. In general, the standard defines two types of communication mechanisms. The first type is a client/server-based mechanism typically used for HMI and SCADA applications [82]. The second type is peer-to-peer communication, which is typically used for fast data transfer between IEDs and MUs [7]. This type is based on a publisher–subscriber mechanism that uses a multicast transmission approach. An example implementation used the following three communication protocols to transmit data through the aforementioned mechanisms:

1. The MMS protocol is used for client/server communication, which runs over TCP/IP or OSI networks [7], [73]. Thus, it functions with IP addresses through routers. Typically, an MMS client, such as SCADA, sends a request for an explicit

data element to the MMS server, which is usually an IED, specified through its IP address. The server responds to the request by returning the specified data to the client defined by its IP address. This protocol relies on the TCP protocol to verify data delivery.

2. GOOSE messages capitalize on the multicast functionality, provided by Ethernet switches, that allows simultaneous communication with several IEDs [72], [83]. Thus, they operate on the publisher/subscriber principle. GOOSE communication transmits a fast event-driven signal such as a trip signal, which is not cyclic in nature [7]. Typically, an IED or MU sends a GOOSE message with the variables of the events that need to be communicated. Because of the messages' multicast nature, the destination does not acknowledge delivery [72]. Therefore, to guarantee delivery, the same GOOSE message is resent several times. Moreover, to verify the virtual connectivity between source and destination, a cyclic GOOSE message is sent at a low rate of T0 specified by the user [7]. In most cases, GOOSE messages are applied directly to Ethernet switches (i.e., LAN) [7]. Subsequently, they are identified by their source MAC addresses. Moreover, GOOSE messages are not routable and cannot cross the routers.

3. The sampled values protocol, as specified in IEC 61850-9-2, is used to communicate analog values (current and voltage) from unconventional sensors or MUs to the IEDs [84], [85]. Like GOOSE, this protocol capitalizes on the multicast functionality provided by Ethernet switches. Moreover, the messages are identified by their MAC addresses and are communicated periodically at high frequencies after being digitalized [1]. The standard (i.e., 61859-9-2LE) specifies a sampling

period of 250 and 208.3 μs for 50 and 60 Hz systems, respectively, for protection

and most applications as well as a higher rate for metering and power quality.
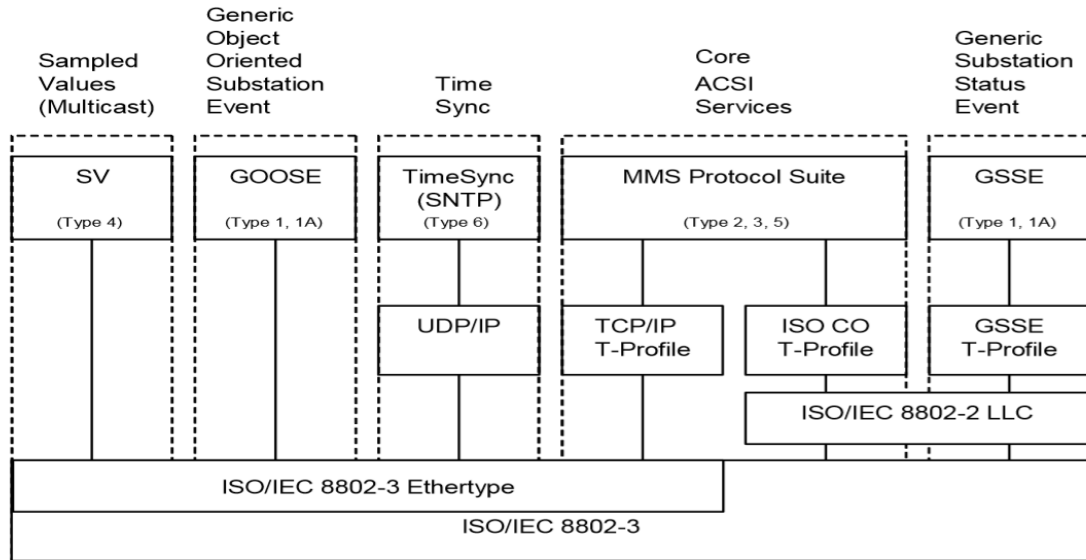
Figure 7-4 IEC 61850 communication protocols [81].

TABLE I
IEC 61850 MESSAGE TYPES AND PERFORMANCES

Type	Applications	Performance Class	Requirements (Transmission Time)
1A	Fast Messages (Trip)	P1	10 ms
		P2/P3	3 ms
1B	Fast Messages (Other)	P1	100 ms
		P2/P3	20 ms
2	Medium Speed		100 ms
3	Low Speed		500 ms
4	Raw Data	P1	10 ms
		P2/P3	3 ms
5	File Transfer		$\geq$1000 ms
6	Time Synchronization		(Accuracy)

Figure 7-5 IEC 61850 performance requirement [7].

The standard also specifies a configuration tool, XML-based Substation

Configuration Language (SCL) [78]. There are four different configuration files:

1. A system-specification description (SSD) file that includes project information and the substation one-line diagram.

2. An IED capability description (ICD) file that defines the LNs and services within an IED.

3. A substation configuration description (SCD) file that details the connectivity and data transfer between the IEDs within the substation.

4. A configured IED description (CID) file that is used to configure the IED with its intended function.

7.2.3 IEC 61850 Substation Architecture

Figure 7-6 shows a typical IEC 61850 substation architecture consisting of two main layers [7], [73]. The first layer is the "process bus," where data from MUs are collected and transmitted to the IEDs. The MUs collect the analog and digital data from the switchyard, convert the analog data to digital signals, and transmit all the data in digital format to the process bus [84]. Physically, the process bus consists of redundant fiber-optic cables connected to a redundant Ethernet switch [7]. To eliminate network congestion in the process bus, both virtual LAN (VLAN) and priority tagging are used [72]. The communication protocols used in the process bus are SV for analog signals and GOOSE for status and control signals. Therefore, the multicast communication mechanism is used. Furthermore, a timing signal (IEEE 1588) is available at the process bus connected to the MUs, and data are time-tagged accordingly.

The second layer in the architecture is the station bus through which data transfer takes place among and between IEDs, SCADA, and HMI. The communication protocols

used in the station bus are GOOSE for communication between IEDs and MMS for communication with SCADA and HMI [7], [72], [82]. Furthermore, a timing signal is available at the station bus, and data are time-tagged accordingly [2].
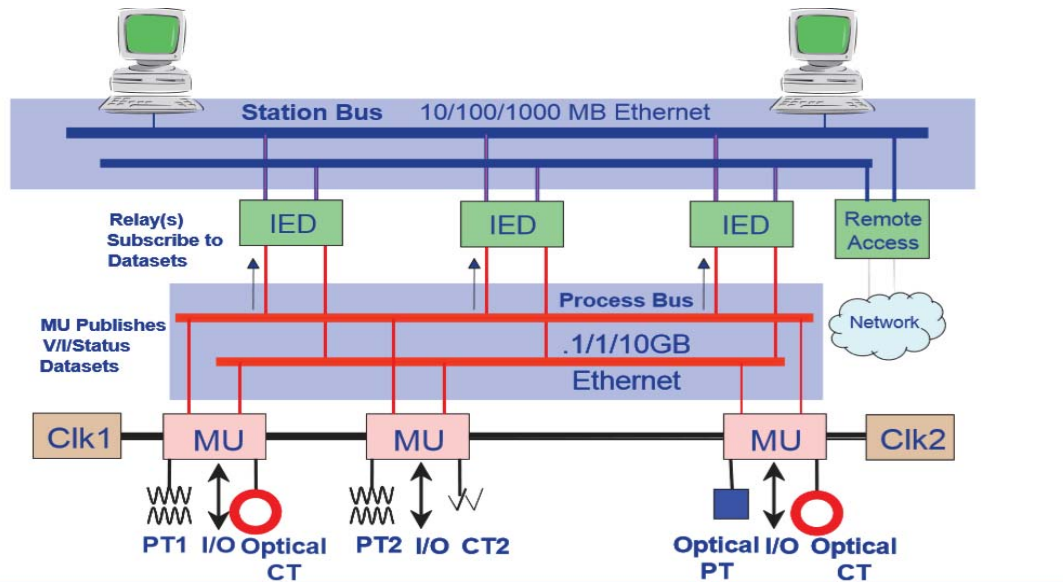
Figure 7-6 IEC 61850 substation architecture [7].

Finally, this architecture supports remote network access through the station bus. Accordingly, an authorized client can access a wide range of information. Such clients could be local HMI, a control center, maintenance technician, or protection engineer [82].

7.2.4   Time Synchronization

Time synchronization is crucial for data communication between different devices within the substation. To reflect the power system operating states, these data are synchronized to a common time reference [86], [87]. The standard time reference currently used for most applications, including power systems, is coordinated universal time (UTC), which can be obtained through GPS satellite clock receivers [88]. Time synchronization is achievable through a dedicated timing system using a separate cabling system, as Figure

7-7 shows, or through the network used for substation automation, as Figure 7-8 shows [86], [87]. The former often uses one pulse per second (1-PPS) and the IRIG-B time code as time synchronization techniques, which both satisfy ± 1 µs accuracy [87]. The substation automation network can use the network time protocol (NTP) and the newly established IEEE 1588v2 protocol for applications that require time synchronization accuracy of ± 1 ms and ± 1 µs, respectively [87]. IEEE 1588v2 is expected to dominate in the near future because it has the advantage of using the local area network and providing high synchronization accuracy [86]–[88].
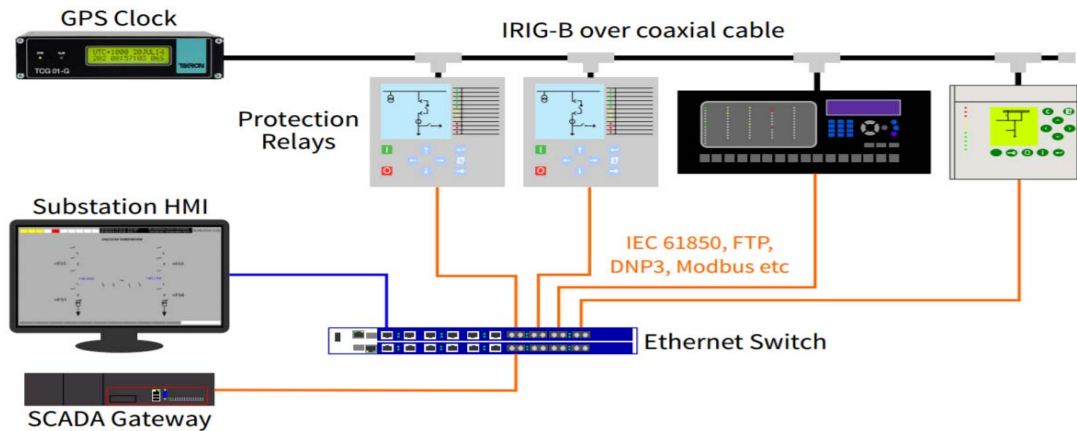
Figure 7-7 Separate timing and communication networks in a substation [87].
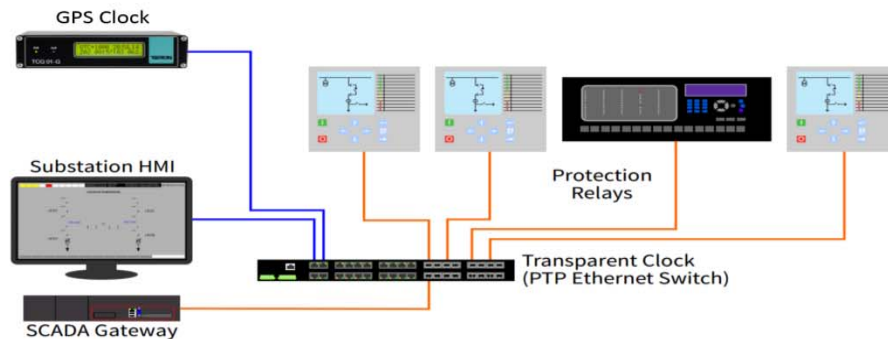
Figure 7-8 Network topology for NTP and IEEE 1588v2 time synchronization [87].

7.3 DSEBCPS System Architecture for Grassroots Installations

This section introduces our proposed architecture for the DSEBCPS considering grassroots installations, which means that the limitations of existing installations do not constrain the architecture. Figure 7-9 depicts the proposed architecture, showing that continuous data streaming in the process bus and station bus is key to the scheme's reliable operation. The figure shows that data flow starts from the MU and telemetry data interface and proceeds to the settingless relays through the process bus, which consists of data concentrators and a set of Ethernet switches. This data are sampled values streamed at a rate of 4,800 samples/s for 60 Hz systems or 4,000 samples/s for 50 Hz systems. Such streaming at this rate from every measurement tool in the substation results in a huge set of data that requires special management. Therefore, the following subsections detail data management at the process bus. Furthermore, at the station bus, phasor quantities, which are computed in the settingless relays and transmitted from the remote substation through the telemetry data interface, are streamed to DSEBCPS at a rate of 1 sample/cycle through the station bus. Such data streaming of the phasor quantities from every IED is unique at the station bus. The following subsections also detail this process. Our architectural design proposes separating the process bus and the station bus into two separate networks because of the massive data traffic in the process bus. Additionally, a critical element for this architecture's successful operation is time synchronization for the data, without which the settingless relay and DSEBCPS cannot operate reliably. Therefore, the entire architecture is based on GPS-synchronized measurements using the IEEE 1588v2 protocol, which sends a timing signal for both the process bus connected to the MUs and the station bus connected to the IEDs. All data are time-tagged accordingly.
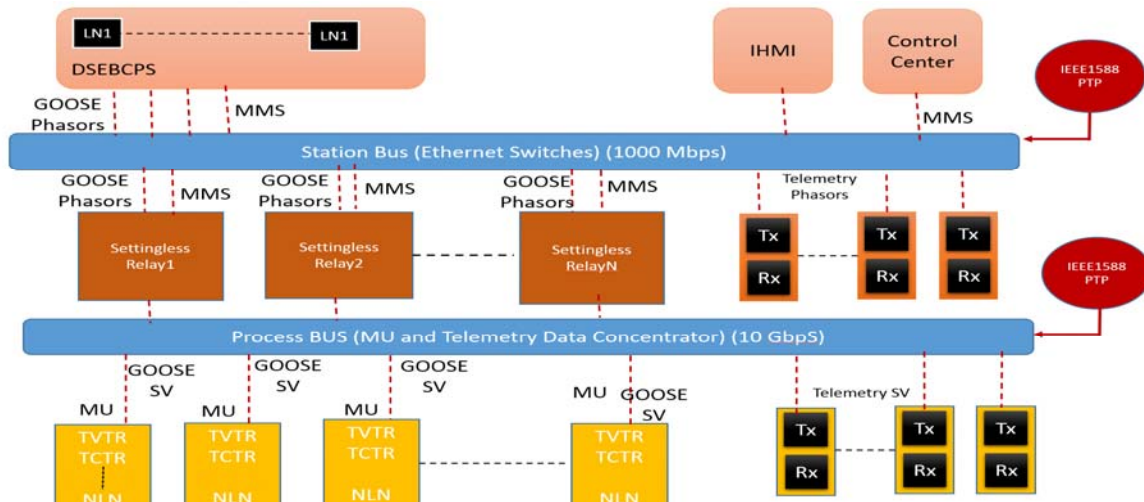
Figure 7-9 Overall system architecture.

7.3.1   Process Bus

The process bus carries data traffic in the form of sampled values originating from MUs or unconventional instrumentation channels. Figure 7-10 shows our proposed design for the process bus. The design consists of three main elements: (1) network topology, (2) data concentrator, and (3) time synchronization.

7.3.1.1   Network Topology

The process bus facilitates data flow from MUs to IEDs. Therefore, the process bus topology must ensure a reliable data flow to avoid unnecessary data interruption. The criteria for network topology selection are data recovery requirements and network bandwidth requirements [89], [90]. The data recovery requirements for the process bus have already been specified by IEC technical committee 57 (TC57) working group 10 (WG10) to be zero time [91]. Zero time means that the recovery process must take place within the time of one sampling period. This requirement indicates that the process bus cannot afford data flow interruption. The bandwidth consumption during normal operation

for each MU is estimated to be up to 5 Mbps for the protection applications [89]. Therefore, the network backbone of the process bus must be designed to accommodate the total bandwidth consumption associated with data streaming from all MUs in the substation. For example, if the substation contains 100 MUs, the total bandwidth consumption is 500 Mbps. Accordingly, the selection of the Ethernet switches must be sized accordingly to the total bandwidth.

Considering the two criteria highlighted above, IEC 61850-9-2 explicitly specifies two topologies that satisfy the data recovery requirements [85], [91], [92]. The first topology is the high-availability seamless ring (HASR), which simply connects each element in the network in a ring topology. This configuration is not practical for process buses in big substations with massive numbers of MUs because of the limitation in the bandwidth capacity. Consequently, HASR cannot accommodate data traffic for large substations. The second topology specified in IEC 61850-9-2 is the parallel redundancy protocol (PRP), which simply duplicates the infrastructure for the network backbone. This entails creating two separate local area networks (i.e., LAN_A and LAN_B). These two networks are used simultaneously to carry data traffic streaming from each MU. Accordingly, the destinations (i.e., the IEDs) receive duplicate data from both networks when they are healthy. Therefore, a duplicate detection mechanism must be implemented to phase out one set of the duplicate information [91]. The PRP consists of the network backbone, which is a set of Ethernet switches connected to each other, and network branches (i.e., MUs and IEDs). The size of the network backbone from a data perspective depends on the size of the Ethernet switches, which are available up to 1 Tbps. Thus, the PRP can fit perfectly into a larger substation because it can accommodate massive data

traffic without any limitations. Moreover, the redundancy in the PRP topology ensures reliable and uninterrupted data flow, which is extremely important for power system protection applications.

Our design for the process bus, depicted in Figure 7-10, adapts the PRP topology. We have introduced a data concentrator into the design as part of the network backbone. The function of the data concentrator is to receive data streaming from MUs, align them, generate time stamps, and stream them again to IEDs (i.e., settingless relays). In this topology, duplicated set of data are streamed from each MU and telemetry data interface to the data concentrators in LAN_A and LAN_B through Ethernet switches. The data concentrators process the data and stream them to the settingless relays through another set of Ethernet switches as data packets for each relay. The design is fully redundant as per the PRP topology structure, where each element in the backbone network is duplicated, including the data concentrator. The design does not include any single point of failure. Accordingly, each settingless relay is equipped with a duplicate data detection mechanism to handle redundant data streams. Moreover, the selection of the Ethernet switches must be engineered properly according to the expected data traffic in the substation, which depends primarily on the number of MUs and telemetry data interfaces. It is important to note that each settingless relay consists of several LNs to facilitate the required functions; for example, each relay will include an LN that represents DSE functions. Similarly, MUs consist of several LNs, such as TCTR for current measurements and TVTR for voltage measurements. Accordingly, the data transfer will take place between these LNs.
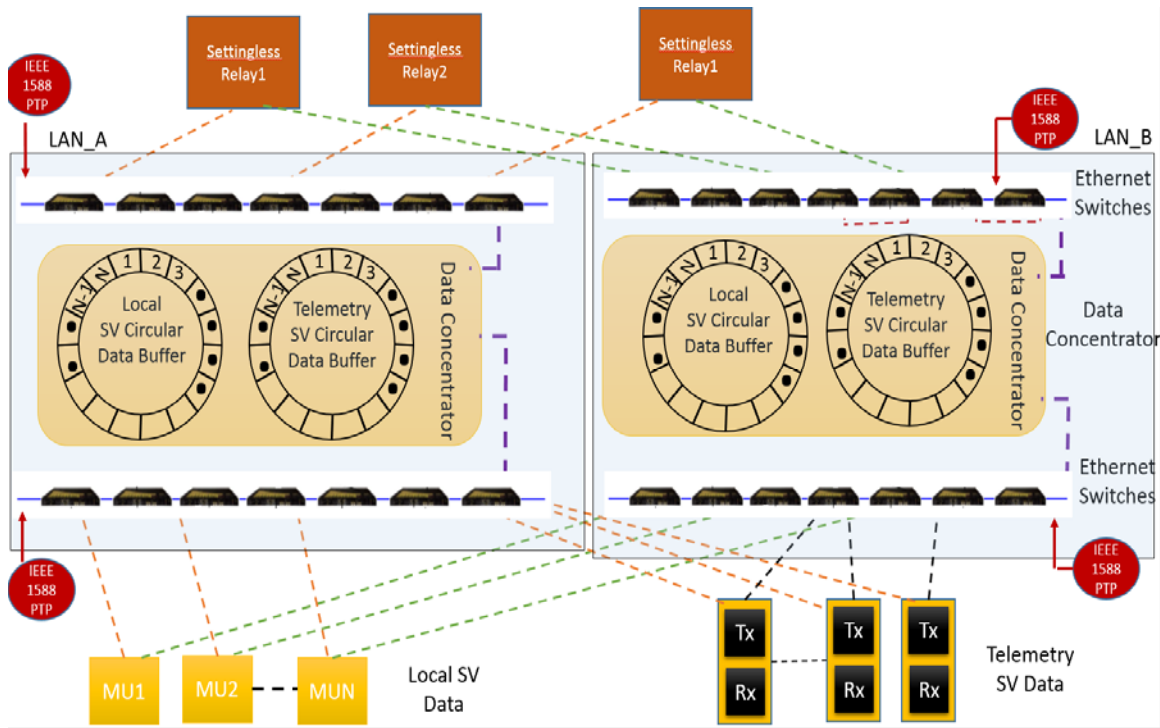
Figure 7-10 Process bus topology for grassroots installation.

7.3.1.2   <u>Data Concentrator</u>

Accurate data streaming is extremely important for reliable operation of both settingless relays and DSEBCPS. Consequently, in our design of the system architecture, we have introduced a data concentrator, which is a device that collects data streaming from MUs and telemetry interfaces, aligns, and streams them again as data packets to individual IEDs. Accordingly, each IED receives its corresponding data packet, which is ready for final processing. Each data concentrator includes two interfaces: an MU data interface and an elementary data interface. These are separated because the telemetry data's remotely communicated destination is transmitted through different communication channels. This could impose additional challenges in handling such data. Moreover, as Figure 7-10 shows, we propose including two concentrators in the substation to satisfy the PRP topology's

redundancy requirement. Each data concentrator is capable of performing the required functions independently.

The data concentrator's main task is to aggregate data from different sources. This task could be undermined by data latency if it is not handled properly [93]–[95]. Data latency is the time difference between data creation at a source and data processing at a destination. The main sources of the data latency is the time required to transmit the data through switches as well as transmit the data over fiber-optic cable. This time depends on the switch design as well as the distance the data must travel between the source and the destination. Figure 7-11 depicts the different components that could affect the latency time and shows that each node within the communication path increases the latency time [93]. Moreover, this time is magnified for the telemetry data because they are traveling across long distances and pass through several communication channels. Furthermore, the Ethernet port in the data concentrator must be properly sized to handle the massive data streaming from the substation and avoid further latency time.

There is a very important distinction here: SVs are time tagged as they come out of the MU in the Data concentrators. Telemetry SV are time tagged at the source. If these two things happen, latency can be tolerated and it will not cause problems. The data concentrator task is to time align the data. This distinction justifies the separation in handling the SV and telemetry data
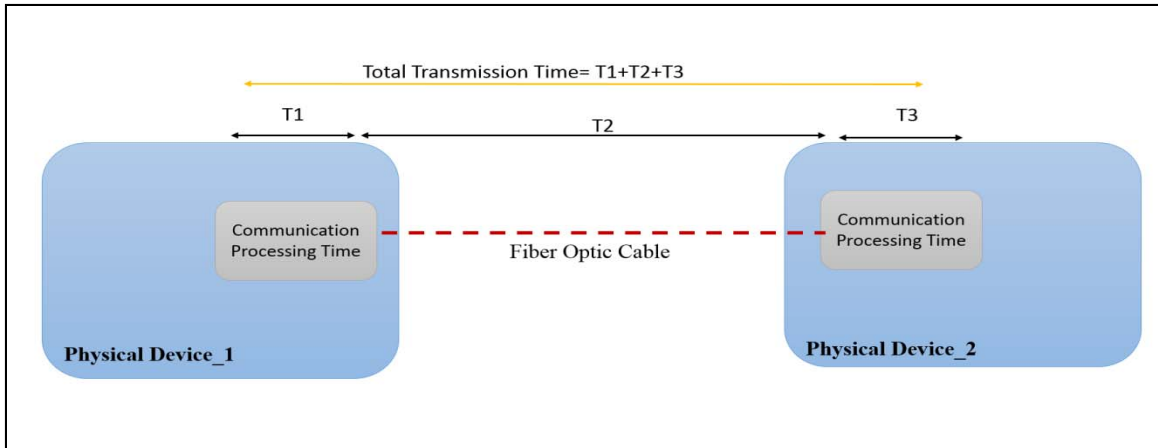
Figure 7-11 Latency time illustration.

The issue of latency is network related and cannot be avoided. However, we must deal with it to ensure reliable operation of the settingless relays. Thus, we propose aggregating the data into a circular buffer with a maximum waiting time for each sample that should be more than the maximum latency time. The circular buffer is designed to handle a specific amount of data at each time tag. The process is depicted in Figure 7-12, which shows that when the last piece of data within a specific time tag has arrived, or when the maximum waiting time has elapsed, the data are aligned, tagged in a timely manner, and placed in the output channel. The data in the output channel are grouped into data packets based on the final destination. This process also justifies the separation of the telemetry data interface into a separate circular buffer because of the expected longer latency time and different time tagging mechanism. When the data concentrator does not receive all the expected measurements, they will be considered missing data. Moreover, if the data are received after the waiting time, they will be discarded. The data in the output channel includes data aggregated from both circular buffers. This process of data aggregation introduces the data concentrator's latency, which needs to be considered in the overall performance of the system.
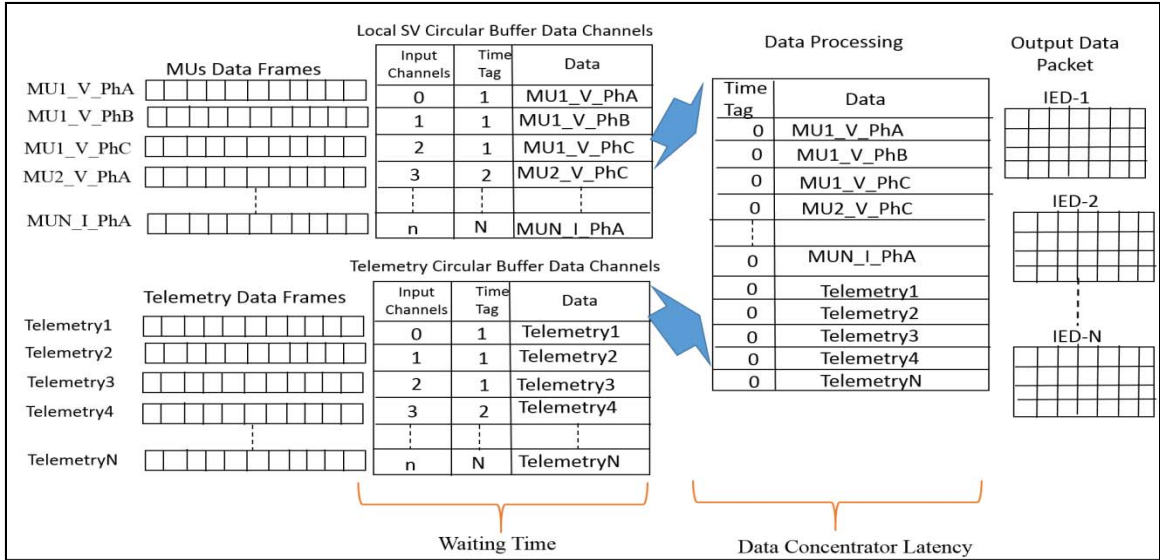
Figure 7-12 Data aggregation in the circular buffer.

The circular buffers in the data concentrators have a limited storage capacity for the aggregated data from MUs and telemetry data interfaces. This storage capacity specifies the buffer size, which is dependent on maximum expected latency. Accordingly, the buffer size is critical and must be calculated properly to avoid important data losses. The chosen size must allow a significant margin for the processing time of the data concentrator in addition to the waiting time. Data concentrator design must also take input capacity into consideration. This capacity is defined as the capability to successfully process measurements without increasing the concentrator latency [93]. Input capacity is very important because of the enormous number of input measurements at the substation level. Therefore, the input capacity must be sized properly based on the size of the data streaming at the substation level.

7.3.1.3   Time Synchronization

Time synchronization is critical for reliable operation of both settingless relays and centralized protection schemes. The required timing accuracy for such applications is less than 1 μs. Accordingly, we propose using the IEEE 1588v2 time synchronization standard known as the precision time protocol. This protocol operates through a data network and can achieve time accuracy of less than 1 μs. This section offers more details about the overall concept of the protocol and its implementation requirements.

IEEE 1588v2 is a time synchronization protocol that uses a data network and accomplish timing accuracy of less than 1 μs [87], [88], [96]. The synchronization network consists of a master clock and a set of slave clocks. Each slave clock is synchronized to the master clock so that both clocks provide exactly the same time. This master–slave IEEE 1588v2 synchronization network consists of the following three types of clock based on the location of the clock in the network [87], [96]:

1.   An ordinary clock, which is a clock located in an end device, such as an IED. It can act as both master and slave clock.

2.   A boundary clock, which is a clock located in the interface between two subnetworks. It will act as a slave clock for the upstream network and master clock for the downstream network.

3.   A transparent clock is an intermediate layer (i.e., Network Bridge or switch) between the master and slave clocks. It has the ability to measure the residence time of an IEEE 1588v2 message within the clock and the delay of the link to the destination (i.e., the slave clock).

The first step in the 1588v2 synchronization process is to identify the type of each clock in the network and then establish the master–slave hierarchy. The best master clock algorithm is used to identify the most suitable clock in the network as the master clock [27]. Furthermore, the algorithm defines the state of each clock as either master or slave. Subsequently, the master clock port will stream IEEE 1588 messages to the network. This process is clarified in Figure 7-13, which shows the time difference between the master and slave clocks, denoted by Δt_1 [96]. This time is measured by sending IEEE 1588 messages (i.e., data packet A) from the master clock through the Ethernet network to the slave clocks. The master clock records the time when data packet was sent, denoted by t_1. The data packet propagates in the network and reaches the slave clock after a propagation delay denoted by Δt_2. When the slave clock receives the data packet, it generates timestamp t_2. Thus, the relationship between t_1 and t_2 is expressed as the following:

$$t_2 = t_1 + \Delta t_2 - \Delta t_1 \tag{7.1}$$

Similarly, the slave clock sends back IEEE 1588 messages (i.e., data packet B) with timestamp t_3 at the slave clock. This data packet reaches the master clock after a propagation delay of Δt_2. When the master clock receives this data packet, it generates a timestamp of t_4. Therefore, the relationship between t_3 and t_4 is expressed as the following:

$$t_4 = t_3 + \Delta t_1 + \Delta t_2 \tag{7.2}$$

139

The timestamps at the master clock (i.e., t_1 and t_4) are sent to the slave clock and are used along with the slave clock's timestamps (i.e., t_2 and t_3) to calculate Δt_1 as follows:

$$\Delta t_1 = \frac{t_1 - t_2 - t_3 + t_4}{2} \tag{7.3}$$

The slave clock uses Δt_1 to correct its internal time to synchronize with the master clock. This process becomes more involved with the introduction of transparent clocks, which introduce additional propagation delay that must be considered.
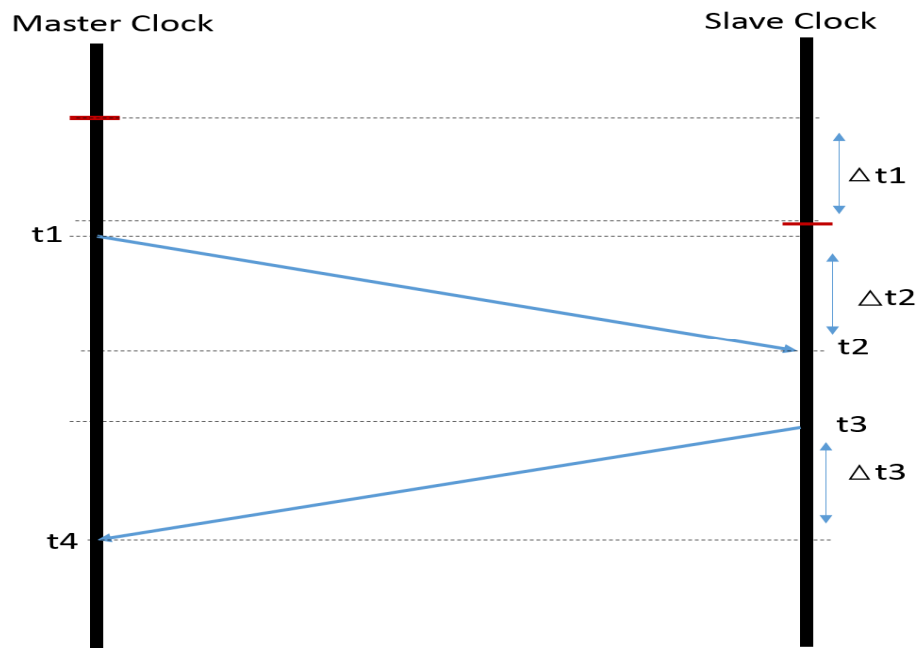
Figure 7-13 Illustration of the master–slave clock operation principle.

The time synchronization process is used to timely align the sampled values in the MUs and create time stamp for each sample in the process bus. The MUs align the data by establishing a 1-second sampling window that starts at the beginning of each second. During this period the MU uses a counter that counts the number of samples per second. It

is initialized with 0 and incremented by one. At the end of the second, it sets back to 0. This process is repeated every second to continually align the sampled values streamed to the process bus. The data concentrator in the process bus receives the data streams from the MU and establishes the time stamp for each sample using the sampling rate and the sample value count.

7.3.2 Station Bus

The station bus facilitates data exchange between settingless relays and DSEBCPS. This includes phasor quantities streaming from settingless relays to DSEBCPS at a sampling rate specified by the end user. Moreover, upon detecting hidden failure the DSEBCPS streams the calculated sampled values corresponding to the compromised data to the settingless relay, which suffers from hidden failures, at a rate and in sync with the MUs to override the compromised measurements. Furthermore, GOOSE message exchanges between the IED and DSEBCPS takes place in the station bus. These GOOSE messages include but are not limited to breaker status, disconnect status, settingless relays operation status, and DSEBCPS permissive signal to settingless relays.

Continuous phasor quantities streaming is critical for reliable operation of DSEBCPS. Thus, station bus topology must insure a reliable data flow to avoid unnecessary data interruption. As in the case of the process bus, the criteria for network topology are data recovery requirements and network bandwidth requirements[88]-[90]. The data recovery requirement for the station bus for our application is zero time. We impose this requirement to enable the DSEBCPS to have continuous supervision of the settingless relays through continuous DSE performance in the quasi-domain. This

requirement indicates that the station bus cannot afford data flow interruption. The size of the network bandwidth depends on the rate of the data flow, which is smaller than that of the process bus. According to the mentioned criteria, we propose to use the Parallel Redundancy Protocol (PRP), which simply duplicates the network backbone infrastructure. This entails creating two separate local area networks (i.e., LAN_A and LAN_B), as Figure 7-14 shows. These two networks are used simultaneously to carry data from each IED to DSEBCPS, which receives duplicated data from both networks when they are healthy. Therefore, a duplicate detection mechanism must be implemented to phase out one of the duplicated data [91]. Similar to the process bus, the PRP consists of a network backbone, which is a set of Ethernet switches connected with each other, and network branches (i.e., IEDs and DSEBCPS). The size of the network backbone from the data perspective depends on the size of the Ethernet switches, which depends on the amount of data exchanged.

Figure 7-14 shows phasor quantities streaming from settingless relays and telemetry interfaces to DSEBCPS. In this design, we have incorporated the data concentrator within the DSEBCPS. Therefore, the data concentrator in the station bus is considered a function in the DSEBCPS. The concept of the data concentrator is identical to that of the process bus. It is important to note that the DSE function within the DSEBCPS is considered for this design as a logical node. The degree of redundancy can be extended to the DSEBCPS hardware by considering two separate DSEBCPS devices (i.e., computers). This option is left to the end user to decide. Finally, time synchronization at the station bus is achieved by using PTP as per IEEE1588v2.
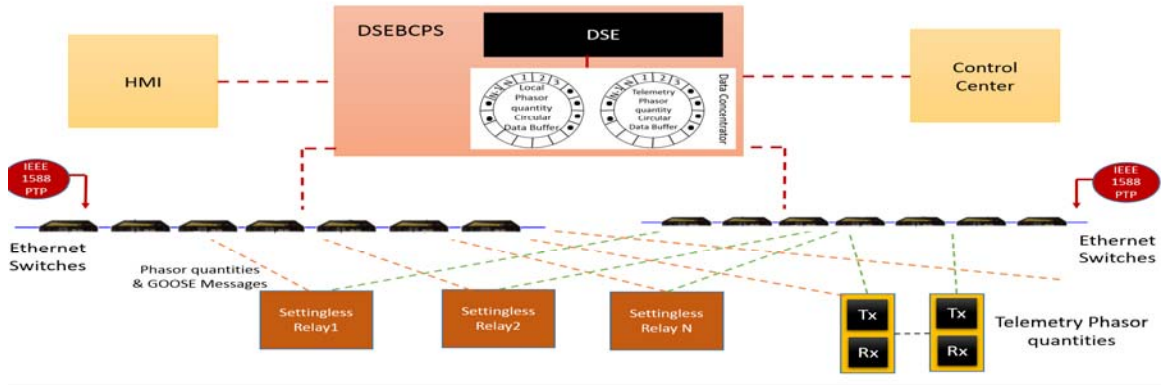
Figure 7-14 Station bus topology.

7.4 DSEBCPS System Architecture for Existing Installations

This section discusses the deployment of the DSEBCPS in existing substations, including legacy protection relays. Moreover, the substation could include settingless relays as primary protection for some zones or in parallel with the legacy protection relays. Therefore, this setup forms a conventional substation, which includes digital technology deployed in part of the substation. Conventional substations with legacy protection have always used copper cable wiring to transfer signals between the primary equipment, such as circuit breakers, instrumentation channels, and legacy protection relays. For digital technologies, data transfer takes place through communication networks as per IEC 61850 requirements. This setup of a conventional substation supplemented with digital technology is expected to dominate in the short term. Therefore, defining the architecture of such a substation will pave the way for smooth migration toward deploying both settingless relays and DSEBCPS and adapting the digital substation technology.

The proposed architecture is depicted in Figure 7-15, which shows that the instrumentation channels at the switchyard are connected through hardwires to the legacy

protection relays. Additionally, the settingless relays receive sampled values streaming

from MUs and telemetry data interfaces at a rate of 4800 sample/s through the process bus,

which will be created to facilitate such data transfer. Moreover, phasor quantities are

streaming from the settingless relays and telemetry interfaces to the DSEBCPS at the rate

of one sample/cycle. The legacy protection relays could participate in the phasor quantity

streaming if they have such streaming capabilities. Moreover, GOOSE messages are

transferred between the MU and settingless relays through the process bus and between the

legacy protection relays and DSEBCPS through the station bus. Finally, the entire

architecture is based on GPS-synchronized measurements using the IEEE 1588v2 protocol.
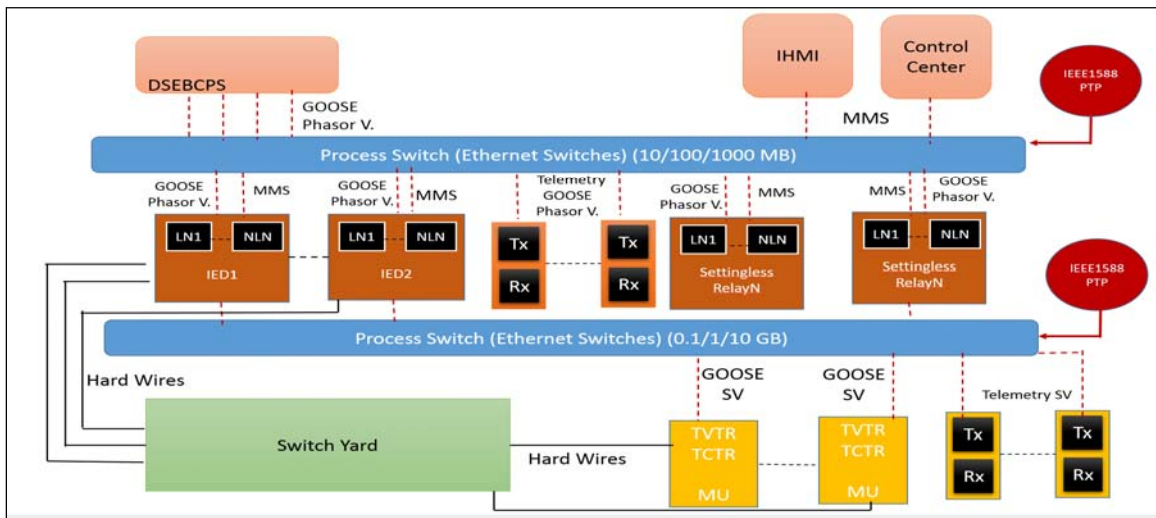
Figure 7-15 Overall system architecture of existing substation.

The process bus in this application for existing substations facilitates

communication between the settingless relays and MUs. It is identical to the process bus

explained in the previous section for the grass-root implementation. For the station bus we

suggest introducing a dedicated new portion for data streaming to the DSEBCPS, as Figure

7-16 shows. This new portion is connected with the existing station bus to communicate

the phasor quantities from the legacy protection relays, which have such capabilities, to the

DSEBCPS. This design could require reinforcement to the existing part to accommodate

the new data streaming. Several design options are available for the station bus in an

existing substation, depending on the end users' requirements.
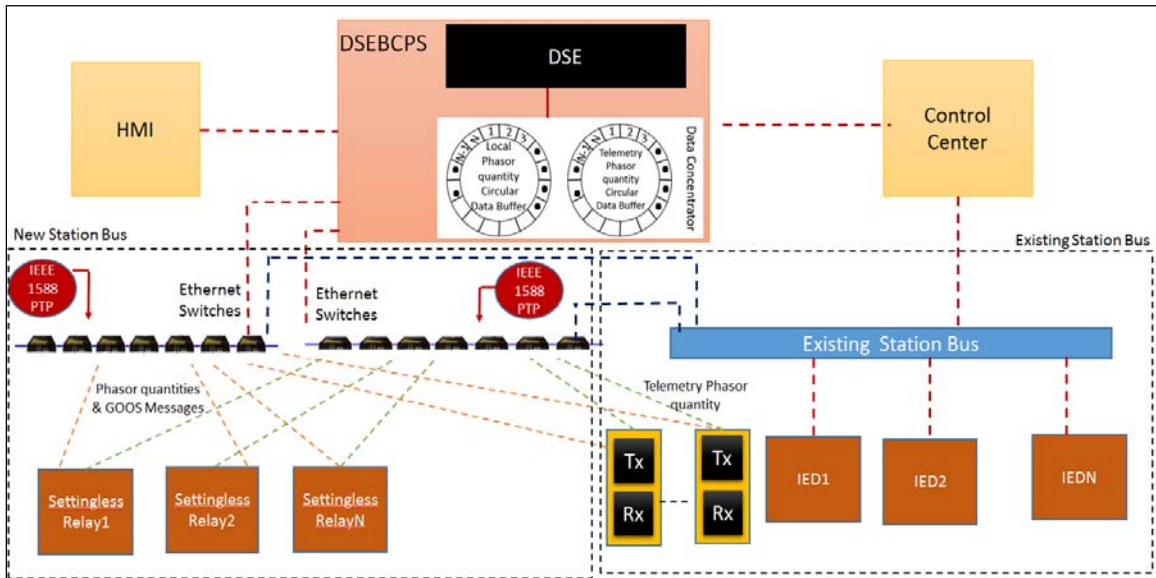
Figure 7-16 Proposed station bus topology for existing substation.

7.5   Future Energy Management Systems

The advancement in power systems and the introduction of new resources, which involve

new operational challenges, necessitate more capable control centers for reliable operation.

Decision making in the future grid requires innovative approaches to overcome existing

limitations. These approaches include advanced data management, sophisticated analytics

capabilities, and massive computational capabilities. Our proposed DSEBCPS and its

architecture provide the required infrastructure at the substation level for future energy

management systems. The DSEBCPS makes enormous measurement data available on a

central platform that can be streamed to the control center. Moreover, the availability of

the accurate substation model within the DSEBCPS, which can be sent to the control centers, provides opportunities for real-time applications such as contingency analysis before executing switching scenarios. These capabilities make the control centers more effective in decision making and ensure a reliable and cost-effective operation for power system networks.

The future EMSs use a distributed state estimation, the DSEBCPS, as a source of data acquisition and substation models to support all required applications. Specifically, each substation sends its real-time model through the DSEBCPS to the EMS whenever the substation topology is changed or a new device is introduced, which are not frequent events. Therefore, the process of synthesizing the substation model does not require continuous processing, which drastically decreases throughput requirements for the communication network. Additionally, the estimated substation states phasor quantities computed by the DSEBCPS are available to be sent to EMS once every cycle and can be streamed to the EMS at this rate or at a different rate based on communication infrastructure capabilities and the application's requirements. Along with the estimated phasor quantities, the DSEBCPS can send several sets of substation alarms that can be used to develop awareness about substation conditions and activate any security measurements to ensure reliable operation.

Furthermore, the EMS uses the states of each substation to compute the system states in real time. These states can be used in many applications associated with economical and secure power system operation, as Figure 7-17 shows. In computing the system states, the EMS combines substation models to represent the entire system model. Then the phasor quantities of substations' states are used to compute the system states. The

availability of the system models and the system data, which are synchronized through a GPS clock, makes this process straightforward. Furthermore, this process is computed in the quasi-dynamic domain, which means the data obtained from the DSEBCPS can be used without further processing. Finally, the DSEBCPS paves the way for advanced EMS capable of performing several applications for a resilient power system and overcoming the challenges of operating the future grid.
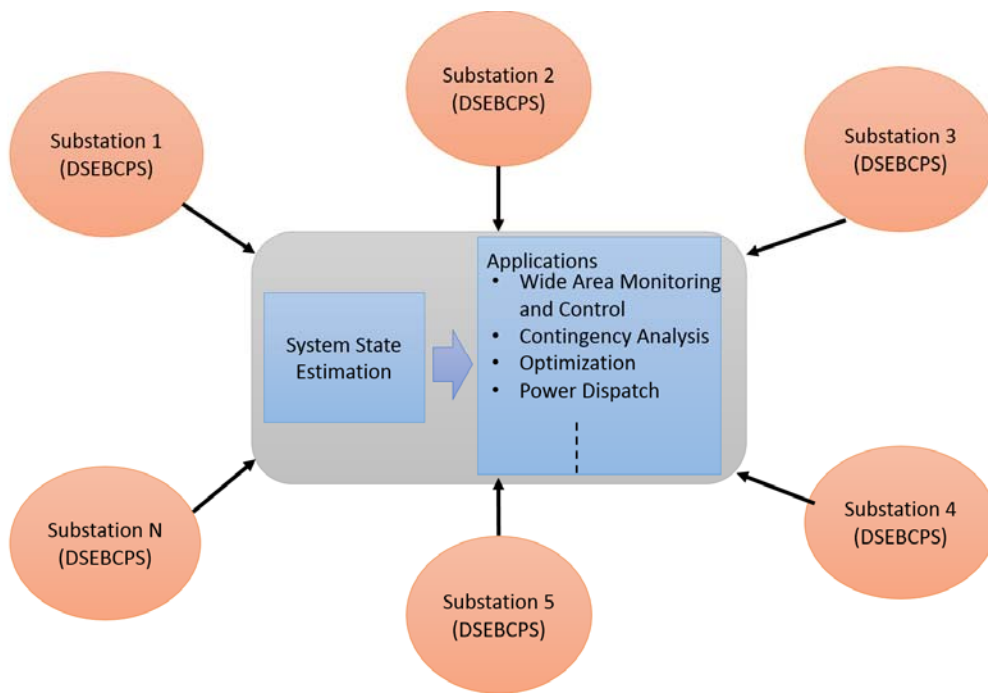
Figure 7-17 Future energy management system.

7.6 Cybersecurity

We envision the proposed DEBCPS and its architecture as an important step toward a seamless transition to digital substations. The digital substation represents a new cyber infrastructure paradigm for the power grid. As for any cyber infrastructure, cybersecurity arises as a critical risk that could undermine this architecture's advantages. The enormous

number of electronic devices (i.e., DSEBCPS and settingless relays) interconnected via communication networks at the system level multiplies such risk. These devices represent the heart of power system operation, which cannot afford malfunctions resulting from cyber-attacks on the system. Accordingly, this issue jeopardizes power system operation reliability and security; such an attack would subject the system to a catastrophic scenario such as a total blackout or infrastructure damage. The most critical attacks for a digital substation include (a) malicious modification of control data, such as the settings of the protection system, operation parameters and others and (b) insertion of malicious commands that would cause the power system to misoperate [97]–[99]. Therefore, researchers have given cybersecurity much attention. In general, any cybersecurity solution has two main requirements: attack detection and efficient communication protocol maintenance [98], [99]. The former includes continually monitoring network traffic to identify abnormal conditions resulting from attacks. This can be achieved through an authentication process for every command to verify its legitimacy. The second important requirement entails that any proposed solution does not affect the efficiency of the communication protocol. This requirement is critical because most digital substation applications are time sensitive, which requires an efficient communication protocol. Accordingly, researchers have proposed several solutions such as access control, trusted computing, and authentication and intrusion detection [99], [100]. Research into more effective solution is ongoing.

7.7 Summary

This chapter discussed our design to the architecture of the proposed DCEBCPS. This architecture is based on IEC 61850, which permits interoperability between products

from different vendors. The proposed architecture for grassroots installation entails separating the station bus and process bus into two separate networks, each of which was designed using the parallel redundancy protocol (PRP) topology, which duplicates the infrastructure for the network backbone and provides full redundancy. Moreover, the entire architecture is based on GPS-synchronized measurements using the IEEE 1588v2 protocol, which sends a timing signal for both the process bus connected to the MUs and the station bus connected to the IEDs. All data are time-tagged accordingly. Additionally, the architecture of the DSEBCPS in existing substations, which includes legacy protection relays, paves the way for smooth migration to the proposed system. The proposed architecture provides the necessary infrastructure for the next generation of energy management systems by providing the necessary data and real-time models to the control center to perform the usual control center functions, such as state estimation, optimization, and control. Finally, cybersecurity arises as critical risk that could undermine the proposed system's advantages. This risk requires more attention from researchers and experts to develop a reliable solution.

CHAPTER 8. CONCLUSIONS, CONTRIBUTIONS, AND FUTURE WORK

8.1 Conclusion

The power system is experiencing revolutionary changes driven by the introduction of customer-owned and renewable energy resources. These resources introduce significant changes in power system characteristics. These changes impose new challenges for every aspect of the power system, one of which is protection. These challenges are concurrent with utilities' efforts to boost system reliability. Such efforts are undermined by protection system vulnerability to hidden failures, which are defects that become apparent during a switching event in the power system network and cause the protection system to misoperate. They might widen the power system interruption by isolating a healthy portion of the power system. Each component in the protection system is vulnerable to such failures. Furthermore, technology advancements pave the way for introducing a new protection system to overcome the aforementioned challenges. Employing these technologies in developing new approaches results in protection systems able to cope with the new changes in the power system, detect hidden failures, and avoid misoperations.

Toward that goal, we developed a dynamic state estimation-based centralized protection scheme (DSEBCPS) to secure the protection system of a substation against hidden failures. The DSEBCPS supervises all the individual protection zone relays within a substation, detects and identifies hidden failures, and corrects the compromised data. We have employed the dynamic state estimation to detect any substation abnormality. Once an abnormality has been detected, hypothesis testing is employed to distinguish between

hidden failure(s) and power fault(s). The high level of redundancy in the measurements at the substation level eliminates the possibility of leverage points which enables highly efficient hypothesis testing. During hidden failure detection, the scheme activates a data correction module to replace compromised data with valid data. We have tested the DSEBCPS with numerous numerical experiments that demonstrated the capabilities of the proposed DSEBCPS. They showed that the scheme exploits the huge redundancy in measurements at the substation level that makes hypothesis testing quite efficient. Also, it can be concluded from the numerical examples that the scheme is capable of detecting other types of hidden failures in the instrumentation channels. The research proposed the integration of DSEBCPS with the newly emerged concept of settingless relays to ensure its secure and dependable operation even in the presence of hidden failures. The concept of DSEBCPS can be easily applied with legacy protection zone relays. Whether a substation is equipped with legacy-protective relays or settingless relays, the DSEBCPS closes a critical gap in protection systems, namely securing the operation of relays in the case of hidden failures while maintaining high dependability. The integration of the proposed scheme and the individual zone protection schemes forms a resilient protection system that is self-immunized against hidden failures.

Moreover, we have proposed an IEC 61850-based architecture of the DSEBCPS with a high degree of redundancy at every layer. The architecture entails separating the process bus and the station bus into two separate local networks. We proposed a PRP topology for the process and station buses to satisfy the criterion of "zero time" data recovery. Furthermore, we introduced data concentrators at both the station and process buses. The data concentrators aggregate data from different sources and overcome the challenge of

data latency. Moreover, the entire architecture is based on GPS-synchronized measurements using the IEEE 1588v2 protocol. All data are accordingly time tagged. Furthermore, the proposed architecture provides the necessary infrastructure for the next generation of energy management systems. This mission is achieved by providing the necessary data and real-time models to the control center to perform the usual control center functions, such as state estimation, optimization, and control. Finally, cybersecurity arises as a critical risk that could undermine the advantage of the proposed system. This risk requires more attention from researchers and experts to develop a reliable solution.

8.2   Contributions

The present thesis has made the following contributions:

- A new substation-centralized protection scheme based on dynamic state estimation (DSE). The new scheme is implemented in an object-oriented manner that makes it comprehensive and applicable for any substation. It monitors the whole substation through its measurements collected from the individual protection zones and uses these measurements to perform dynamic state estimation for the whole substation. The proposed scheme is capable of detecting abnormalities within the substation in a secure, dependable, and timely manner.

- The proposed scheme is capable of detecting hidden failures in the individual protection zone via hypothesis testing. This capability bridges a critical gap in protection systems that causes numerous misoperations.

- The integration of the proposed scheme and individual zone protection form a resilient protection system self-immunized against hidden failures.

- The proposed architecture is IEC-61850 compliant. It is aligned with worldwide efforts to design the architecture of the digital substation, and we hope that our work will make a significant contribution toward this goal.

8.3 Future Research Directions

The DSEBCPS performs DSE at the substation level using all the available measurements at the substation and the substation model, which consists of the model of different devices within the substation. This modeling approach can be enhanced by including the model of the instrumentation channels along with the main devices. The advantage of such a step is to increase the accuracy of the DSE by eliminating the error generated by considering an ideal instrumentation channel. This step will increase the computational burden of the DSEBCPS. Therefore, a thorough evaluation of the most optimal approach to include the models of instrumentation channels is needed.

Furthermore, we have proposed in the DSEBCPS a data correction module that streams the calculated sampled values corresponding to the detected bad measurements to the sample value circular buffers to override the compromised measurements. The scheme ensures that all settingless relays use validated data. In its present implementation, this process may be affected by the harmonic components and transient conditions in the system which might affect the settingless relay response. Therefore, the settingless relay response can be enhanced by including the harmonic components of the waveforms in performing the DSE. Furthermore using the time-dynamic domain for the centralized protection scheme instead of the quasi-dynamic domain will eliminate the aforementioned limitations. Such enhancements will increase the accuracy of the DSE. However, they will also increase

the computational burden of the DSEBCPS and increase data traffic in the station bus. Accordingly, this process needs to be evaluated in terms of feasibility and the need for such enhancements.

We envision the proposed DSEBCPS and its architecture as an important step toward a seamless transition to the digital substation. This involves a dramatic increase in the cyber infrastructure in the substations and eventually in the power system. This makes the system vulnerable to cyberattacks. The proposed dynamic state estimation-based method in this dissertation can be employed to detect cyberattacks. More specifically, the DSE algorithm and hypothesis testing can be used to (a) detect data attacks in real time and (b) develop a command authentication method to detect maliciously inserted commands. Such a technique needs to be developed further and assisted with faster-than-real-time simulation for command authentication, which involves three steps: (1) command capturing (i.e., intrusion), (2) impact evaluation of the captured commands through performing the DSE and hypothesis testing, and (3) command authentication or command blocking.

DSEBCPS and its architecture can be used as the base for a future energy management system where the proposed system will provide the necessary data and real-time models to the control center for performing the usual control center functions, such as state estimation, optimization, and control. The EMS uses the substation model and states obtained from the DSEBCPS of each substation to compute the system states in real time. These states can be used in many applications associated with a power system's economic and secure operation. A detailed framework for such EMS needs to be developed and detailed.

PAPERS RESULTED FROM THE RESEARCH OF THIS

THESIS

1   H. F. Albinali and A. P. Meliopoulos, "A Centralized Substation Protection Scheme that detects hidden failures," *2016 IEEE Power and Energy Society General Meeting (PESGM)*, Boston, MA, 2016, pp. 1-5.

2   H. Albinali, A. P. Meliopoulos, G. Cokkinides, and P. Myrda "Hidden failures detection and correction via substation wide dynamic state estimation," *presented at the PAC World Americas Conference*, Raleigh, NC, USA, pp. 1–6, 2016.

3   H. F. Albinali, A. P. Meliopoulos, and C. Vournas," Dynamic State Estimation-Based Centralized Protection Scheme" 12thIEEE Power and Energy Society PowerTech Conference, Manchester, UK, 2017, pp. 1-6.

4   H. Albinali, A. P. Meliopoulos, G. Cokkinides, and P. Myrda, and E. Farantatos "Update on Dynamic State Estimation Based Centralized Protection Scheme to Detect Hidden Failure," *presented at the PAC World Americas Conference*, Wroclaw, Poland, pp. 1–6, 2017.

5   H. F. Albinali and A. P. Meliopoulos, " Hidden Failure Detection via Dynamic State Estimation in Substation Protection Systems," *Accepted Saudi Arabia Smart Grid Conference,* Jeddah, KSA, 2017, pp. 1-6.

6   H. Albinali and A. P. Meliopoulos, "Substation Level-Wide Area Monitoring Via Dynamic State Estimation Based Protection Schemes," *Submitted to ISGT, Asia Conference*, Auckland, New Zealand, pp. 1–5, 2017.

7   H. Albinali and A. P. Meliopoulos, "Resilient Protection System through Centralized Substation Protection," *Submitted to IEEE Transactions on Power Delivery*.

8   A. P. Meliopoulos, G. Cokkinides, H. Albinali, and P. Myrda "Condition Monitoring of IEDs and IED Instrumentation via Centralized Substation Protection and Control" at the PAC World Magazine.

APPENDIX A.   CURRENT TRANSFORMER

A.1   Introduction

This Appendix presents the time domain single-phase current transformer model. The equivalent circuit of a current transformer is illustrated in Figure A-1.
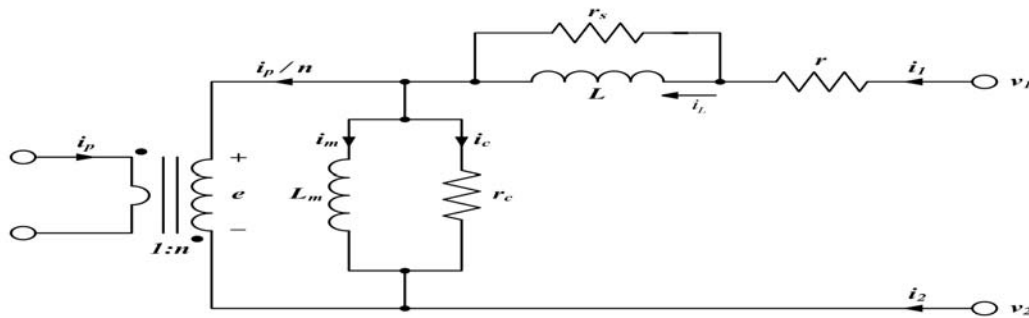
Figure A-1 CT Equivalent Circuit

The user interface and parameter settings of CT model is shown in Figure A-2.
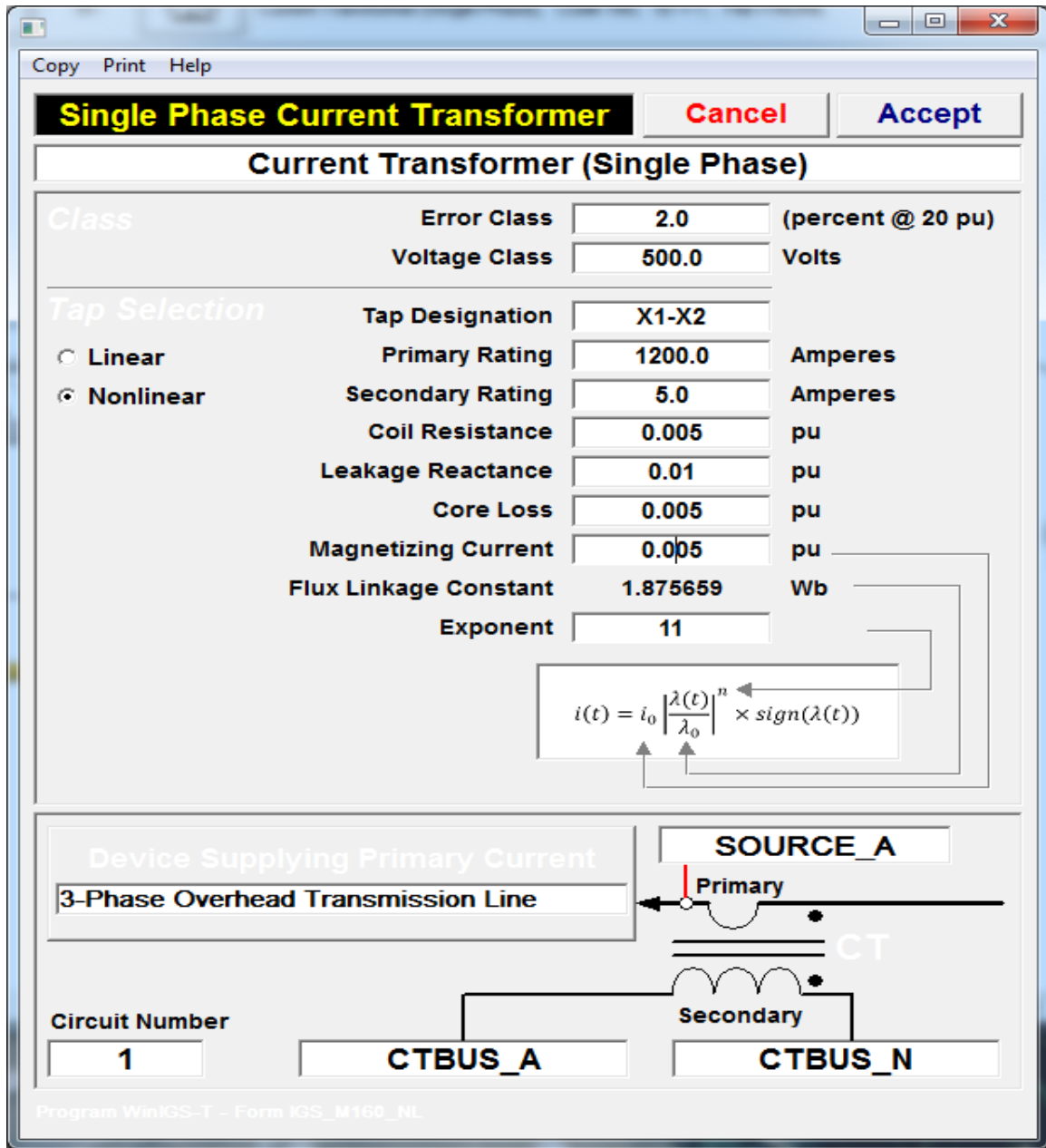
Figure A-2 User interface and parameters of a Current Transformer

A.2 Time Domain Model

A.2.1 Compact Form

Circuit analysis yields the following equations:

$$i_1(t) = i_L(t) + g_s L \frac{di_L(t)}{dt} \tag{A.1}$$

$$i_2(t) = -i_L(t) - g_s L \frac{di_L(t)}{dt} \tag{A.2}$$

$$0 = v_1(t) - v_2(t) - e(t) - L\frac{di_L(t)}{dt} - r\left(i_L(t) + g_s L\frac{di_L(t)}{dt}\right) \tag{A.3}$$

$$0 = e(t) - \frac{d\lambda(t)}{dt} \tag{A.4}$$

$$0 = i_L(t) + g_s L\frac{di_L(t)}{dt} - \frac{1}{r_c}e(t) - i_m(t) - \frac{1}{N}i_p(t) \tag{A.5}$$

For linear case

$$0 = i_m(t) - \frac{1}{L_m}\lambda(t) \tag{A.6a}$$

For nonlinear case

$$0 = i_m(t) - i_0 \left|\frac{\lambda(t)}{\lambda_0}\right|^n sign(\lambda(t)) \tag{A.6b}$$

There are six equations and six state variables:

$$I = [i_1, i_2, 0, 0, 0, 0]$$

$$X = \left[v_1, v_2, i_L, e, \lambda, i_m\right]$$

A.2.2 Quadratized Model

The model is quadratized by introducing additional internal state variables, so that the nth exponent is replaced by equations of at most quadratic degree. Since the exact degree

of nonlinearity is not known until the user specifies it, the model performs automatic quadratization of the equations. A special procedure is used, so that the model is quadratized using the minimum number of additional internal states, while also maintaining the scarcity of the resulting equations. The methodology is based on expressing the exponent in binary form. The binary representation provides all the information about the number of new variables and equations that need to be introduced and about the form of the equations (products of new variables). The procedure is described later. Following this procedure the model can be converted into the standard quadratized form:

$$i_1(t) = i_L(t) + g_s Lz(t) \tag{A.7}$$

$$i_2(t) = -i_L(t) - g_s Lz(t) \tag{A.8}$$

$$0 = z(t) - \frac{dL(t)}{dt} \tag{A.9}$$

$$0 = e(t) - \frac{d\lambda(t)}{dt} \tag{A.10}$$

$$0 = v_1(t) - v_2(t) - e(t) - Lz(t) - r(i_L(t) + g_s Lz(t)) \tag{A.11}$$

$$0 = i_L(t) + g_s Lz(t) - \frac{1}{r_c} e(t) - i_m(t) - \frac{1}{N} i_p(t) \tag{A.12}$$

For linear case:

$$0 = i_m(t) - \frac{1}{L_m} \lambda(t) \tag{A.13a}$$

For nonlinear case:

$$0 = i_m(t) - i_0 \cdot y_m(t) \cdot \left[sign(\lambda\,(t))\right]^{n+1} \qquad\qquad\qquad \text{(A.13b)}$$

$$0 = y_1(t) - \frac{\lambda\,(t)^2}{\lambda_0^{\,2}} \qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{(A.13b+1)}$$

$$0 = y_2(t) - y_1(t)^2 \qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{(A.13b+2)}$$

$$0 = y_{m1+1}(t) - y_{i1}(t) \cdot y_{j1}(t) \qquad\qquad\qquad\qquad\qquad \text{(A.13b+m1+1)}$$

$$0 = y_{m1+2}(t) - y_{m1+1}(t) \cdot y_{j2}(t) \qquad\qquad\qquad\qquad\; \text{(A.13b+m1+2)}$$

… …

… …

$$\begin{cases} 0 = y_m(t) - y_{m-1}(t) \cdot y_{jm2}(t) & ,if\ n\ even \\[2mm] 0 = y_m(t) - y_{m-1}(t) \cdot \dfrac{\lambda\,(t)}{\lambda_0} & ,if\ n\ odd \end{cases} \qquad\qquad \text{(A.13b+m)}$$

There are $7 + m$ equations and $7 + m$ state variables:

$$I = [i_1, i_2, 0, 0, 0, 0 \dots, 0]$$

$$X = \left[v_1, v_2, i_L, z, e,\ \lambda, i_m, y_1 \dots y_m\right]$$

Based on the above formulation, the number of additional internal states and equations m is computed as follows:

$$m = m_1 + m_2$$

where

$$m_1 = \text{int}(\log_2(n))$$

$m_2 = (\#\text{ of ones in the binary representation of }n) - 1$

Given the exponent = 5, the mathematical expression of the time domain quadratized device model is:

$$i(t) = Y_{eqx1}\mathbf{x}(t) + Y_{equ1}\mathbf{u}(t) + D_{eqxd1}\frac{d\mathbf{x}(t)}{dt} + C_{eqc1}$$

$$0 = Y_{eqx2}\mathbf{x}(t) + Y_{equ2}\mathbf{u}(t) + D_{eqxd2}\frac{d\mathbf{x}(t)}{dt} + C_{eqc2}$$

$$0 = Y_{eqx3}\mathbf{x}(t) + Y_{equ3}\mathbf{u}(t) + \left\{ \begin{matrix} \vdots \\ \mathbf{x}(t)^T \left\langle F^i_{eqxx3} \right\rangle \mathbf{x}(t) \\ \vdots \end{matrix} \right\} + \left\{ \begin{matrix} \vdots \\ \mathbf{u}(t)^T \left\langle F^i_{equu3} \right\rangle \mathbf{u}(t) \\ \vdots \end{matrix} \right\} + \left\{ \begin{matrix} \vdots \\ \mathbf{u}(t)^T \left\langle F^i_{equx3} \right\rangle \mathbf{x}(t) \\ \vdots \end{matrix} \right\} + C_{feqc3}$$

$$Y_{eqx1} = \begin{bmatrix} 0 & 0 & 1 & g_s L & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & -g_s L & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$Y_{eqx2} = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & -1 & -r & -L - g_s Lr & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & g_s L & -\dfrac{1}{r_c} & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & i_0 \end{bmatrix}$$

$$D_{eqxd2} = \begin{bmatrix} 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$C_{eqc2} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ \dfrac{1}{N}i_p \\ 0 \end{bmatrix}$$

$$Y_{eqx3} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$F_{eqxx3}^0 [5][5] = -\frac{1}{\lambda_0^2}$$

$$F_{eqxx3}^1 [7][7] = -1$$

$$F_{eqxx3}^2 [5][8] = -\frac{1}{\lambda_0}$$

Other matrices are zero

A.2.3   SCAQCF Model

The differential equations in above model are integrated with the quadratic integration method and the equations that are algebraic are sufficed to be written at times t and t_m. The SCAQCF model yields the following model.

The standard time domain SCAQCF device model is:

$$\begin{Bmatrix} i(t) \\ 0 \\ 0 \\ i(t_m) \\ 0 \\ 0 \end{Bmatrix} = Y_{eqx}\mathbf{x} + Y_{equ}\mathbf{u} + \begin{Bmatrix} \vdots \\ \mathbf{x}^T \left\langle F_{eqx}^i \right\rangle \mathbf{x} \\ \vdots \end{Bmatrix} + \begin{Bmatrix} \vdots \\ \mathbf{u}^T \left\langle F_{equ}^i \right\rangle \mathbf{u} \\ \vdots \end{Bmatrix} + \begin{Bmatrix} \vdots \\ \mathbf{u}^T \left\langle F_{equx}^i \right\rangle \mathbf{x} \\ \vdots \end{Bmatrix} - B_{eq}$$

$$B_{eq} = -N_{eqx}\mathbf{x}(t-h) - N_{equ}\mathbf{u}(t-h) - M_{eq}i(t-h) - K_{eq}$$

Where

$$Y_{eqx} = \begin{bmatrix} \dfrac{4}{h}D_{eqxd1} + Y_{eqx1} & -\dfrac{8}{h}D_{eqxd1} \\[2ex] D_{eqxd2} + \dfrac{h}{6}Y_{eqx2} & \dfrac{2h}{3}Y_{eqx2} \\[2ex] Y_{eqx3} & 0 \\[2ex] \dfrac{1}{2h}D_{eqxd1} & \dfrac{2}{h}D_{eqxd1} + Y_{eqx1} \\[2ex] -\dfrac{h}{24}Y_{eqx2} & D_{eqxd2} + \dfrac{h}{3}Y_{eqx2} \\[2ex] 0 & Y_{eqx3} \end{bmatrix}$$

$$Y_{equ} = \begin{bmatrix} Y_{equ1} & 0 \\[2ex] \dfrac{h}{6}Y_{equ2} & \dfrac{2h}{3}Y_{equ2} \\[2ex] Y_{equ3} & 0 \\[2ex] 0 & Y_{equ1} \\[2ex] -\dfrac{h}{24}Y_{equ2} & \dfrac{h}{3}Y_{equ2} \\[2ex] 0 & Y_{equ3} \end{bmatrix}$$

$$F_{eqx} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ F_{eqxx3} & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & Y_{eqxx3} \end{bmatrix}$$

$$F_{equ} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ F_{equu3} & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & F_{equu3} \end{bmatrix}$$

$$F_{equx} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ F_{equx3} & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & F_{equx3} \end{bmatrix}$$

$$N_{eqx} = \begin{bmatrix} -Y_{eqx1} + \dfrac{4}{h} D_{eqxd1} \\[2ex] \dfrac{h}{6} Y_{eqx2} - D_{eqxd1} \\[2ex] 0 \\[2ex] \dfrac{1}{2} Y_{eqx1} - \dfrac{5}{2h} D_{eqxd1} \\[2ex] \dfrac{5h}{24} Y_{eqx2} - D_{eqxd1} \\[2ex] 0 \end{bmatrix}$$

$$N_{equ} = \begin{bmatrix} -Y_{equ1} \\ \dfrac{h}{6}Y_{equ2} \\ 0 \\ \dfrac{1}{2}Y_{equ1} \\ \dfrac{5h}{24}Y_{equ2} \\ 0 \end{bmatrix}$$

$$M_{eq} = \begin{bmatrix} I_{size(i(t))} \\ 0 \\ 0 \\ \dfrac{1}{2}I_{size(i(t))} \\ 0 \\ 0 \end{bmatrix}$$

$$K_{eq} = \begin{bmatrix} 0 \\ hC_{eqc2} \\ C_{eqc3} \\ \dfrac{3}{2}C_{eqc1} \\ \dfrac{1}{2}hC_{eqc1} \\ C_{eqc3} \end{bmatrix}$$

APPENDIX B.   POTENTIAL TRANSFORMER

B.1   Introduction

This appendix presents the time domain model for single-phase potential transformer. The equivalent circuit of a potential transformer is illustrated in Figure B-1.
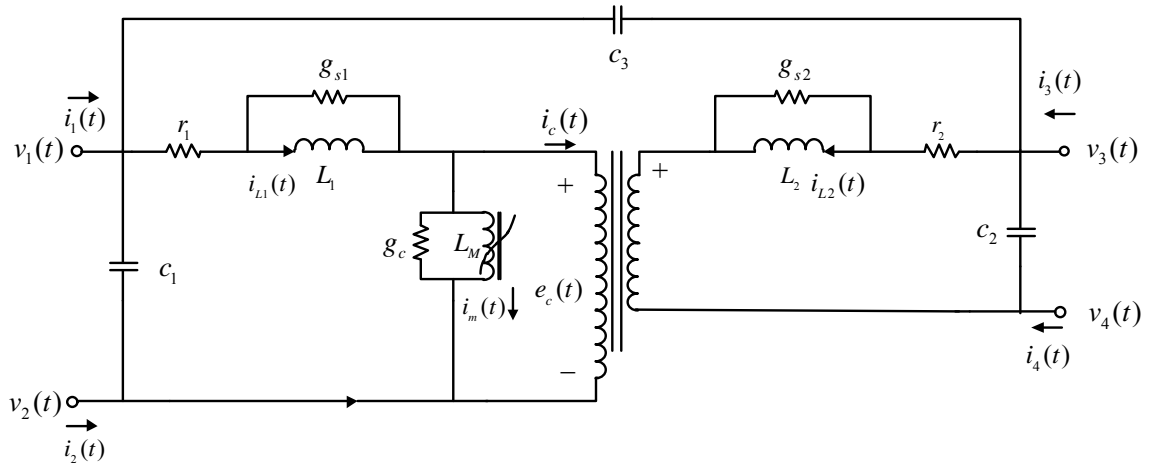
Figure B-1 PT Equivalent Circuit

where h is the integration time step, and resistance g_s stabilizes the numerical integration. The value is

$$g_s = \frac{h}{5L}$$

B.1

The user interface and parameter settings of PT model is shown in Figure 2.

Figure B-2 User interface and parameters of a potential Transformer

B.2. Time Domain Model

B.2.1. Compact Form

Circuit analysis yields the following equations:

$$i_1(t) = i_{L1}(t) + g_s L_1 \frac{di_{L1}(t)}{dt} + C_1 \frac{dV_1(t) - dV_2(t)}{dt} + C_3 \frac{dV_1(t) - dV_3(t)}{dt} \tag{B.2}$$

$$i_2(t) = -i_{L1}(t) - g_s L_1 \frac{di_{L1}(t)}{dt} - C_1 \frac{dV_1(t) - dV_2(t)}{dt} \tag{B.3}$$

$$i_3(t) = i_{L2}(t) + g_s L_2 \frac{di_{L2}(t)}{dt} + C_2 \frac{dV_3(t) - dV_4(t)}{dt} + C_3 \frac{dV_3(t) - dV_1(t)}{dt} \tag{B.4}$$

$$i_4(t) = -i_{L2}(t) - g_s L_2 \frac{di_{L2}(t)}{dt} - C_2 \frac{dV_3(t) - dV_4(t)}{dt} \tag{B.5}$$

$$0 = v_1(t) - v_2(t) - e(t) - L_1 \frac{di_{L1}(t)}{dt} - r_1 \left(i_{L1}(t) + g_s L_1 \frac{di_{L1}(t)}{dt} \right) \tag{B.6}$$

$$0 = v_3(t) - v_4(t) - \frac{1}{N} e(t) - L_2 \frac{di_{L2}(t)}{dt} - r_2 \left(i_{L2}(t) + g_s L_2 \frac{di_{L2}(t)}{dt} \right) \tag{B.7}$$

$$0 = e(t) - \frac{d\lambda(t)}{dt} \tag{B.7}$$

$$0 = i_{L1}(t) + g_s L_1 \frac{di_{L1}(t)}{dt} - i_c(t) - i_m(t) - g_c e(t) \tag{B.9}$$

$$0 = Ni_c(t) + i_{L2}(t) + g_s L_2 \frac{di_{L2}(t)}{dt} \tag{B.10}$$

For linear case:

$$0 = i_m(t) - \frac{1}{L_m} \lambda(t) \tag{B.11a}$$

For nonlinear case:

$$0 = i_m(t) - i_0 \left| \frac{\lambda(t)}{\lambda_0} \right|^n sign(\lambda(t)) \tag{B.11b}$$

There are 10 equations and 10 state variables:

$$I(t) = [i_1(t), i_2(t), i_3(t), i_4(t), 0, 0, 0, 0, 0, 0]$$

$$X(t) = [v_1(t), v_2(t), v_3(t), v_4(t), i_{L1}(t), i_{L2}(t), e(t), \lambda(t), i_c(t), i_m(t)]$$

B.2.1   Quadratized Form

The model is quadratized by introducing additional internal state variables, so that the nth exponent is replaced by equations of at most quadratic degree. Since the exact degree of nonlinearity is not known until the user specifies it, the model performs automatic quadratization of the equations. A special procedure is used, so that the model is quadratized using the minimum number of additional internal states, while also maintaining the scarcity of the resulting equations. The methodology is based on expressing the exponent in binary form. The binary representation provides all the information about the number of new variables and equations that need to be introduced and about the form of the equations (products of new variables). The procedure is described later. Following this procedure the model can be converted into the standard quadratized form:

$$i_1(t) = i_{L1}(t) + g_s L_1 z_5(t) + C_1(z_1(t) - z_2(t)) + C_3(z_1(t) - z_3(t)) \qquad \text{(B.12)}$$

$$i_2(t) = -i_{L1}(t) - g_s L_1 z_5(t) - C_1(z_1(t) - z_2(t)) \qquad \text{(B.13)}$$

$$i_3(t) = i_{L2}(t) + g_s L_2 z_6(t) + C_2(z_3(t) - z_4(t)) + C_3(z_3(t) - z_1(t)) \qquad \text{(B.14)}$$

$$i_4(t) = -i_{L2}(t) - g_s L_2 z_6(t) - C_2(z_3(t) - z_4(t)) \qquad \text{(B.15)}$$

$$0 = z_1(t) - \frac{dV_1(t)}{dt} \qquad \text{(B.16)}$$

$$0 = z_2(t) - \frac{dV_2(t)}{dt} \qquad \text{(B.17)}$$

$$0 = z_3(t) - \frac{dV_3(t)}{dt} \qquad \text{(B.18)}$$

$$0 = z_4(t) - \frac{dV_4(t)}{dt} \qquad \text{(B.19)}$$

$$0 = z_5(t) - \frac{di_{L1}(t)}{dt} \qquad \text{(B.20)}$$

$$0 = z_6(t) - \frac{di_{L2}(t)}{dt} \qquad \text{(B.21)}$$

$$0 = e(t) - \frac{d\lambda(t)}{dt} \qquad \text{(B.22)}$$

$$0 = v_1(t) - v_2(t) - e(t) - L_1 z_5(t) - r_1\big(i_{L1}(t) + g_s L_1 z_5(t)\big) \tag{B.23}$$

$$0 = v_3(t) - v_4(t) - \frac{1}{N} e(t) - L_2 z_6(t) - r_2\big(i_{L2}(t) + g_s L_2 z_6(t)\big) \tag{B.24}$$

$$0 = i_{L1}(t) + g_s L_1 z_5(t) - i_c(t) - i_m(t) - g_c e(t) \tag{B.25}$$

$$0 = N i_c(t) + i_{L2}(t) + g_s L_2 z_6(t) \tag{B.26}$$

For linear case:

$$0 = i_m(t) - \frac{1}{L_m} \lambda(t) \tag{B.27a}$$

For nonlinear case:

$$0 = i_m(t) - i_0 \cdot y_m(t) \cdot \big[sign(\lambda(t))\big]^{n+1} \tag{B.27b}$$

$$0 = y_1(t) - \frac{\lambda(t)^2}{\lambda_0^2} \tag{B.28}$$

$$0 = y_2(t) - y_1(t)^2 \tag{B.29}$$

… …

… …

$$0 = y_{m1}(t) - y_{m1-1}(t)^2 \tag{B.29b+m1}$$

$$0 = y_{m1+1}(t) - y_{i1}(t) \cdot y_{j1}(t) \tag{B.29b+m1+1}$$

$$0 = y_{m1+2}(t) - y_{m1+1}(t) \cdot y_{j2}(t) \tag{B.29b+m1+2}$$

......

......

$$\begin{cases} 0 = y_m(t) - y_{m-1}(t) \cdot y_{jm2}(t) & ,if\ n\ even \\ 0 = y_m(t) - y_{m-1}(t) \cdot \dfrac{\lambda\,(t)}{\lambda_0} & ,if\ n\ odd \end{cases} \tag{B.29b+m}$$

There are $16 + m$ equations and $16 + m$ state variables:

$$I(t) = [i_1(t), i_2(t), i_3(t), i_4(t), 0, 0, \dots, 0, 0]$$

$$X(t) = \begin{bmatrix} v_1(t), v_2(t), v_3(t), v_4(t), i_{L1}(t), i_{L2}(t), z_1(t), z_2(t), \\ z_3(t), z_4(t), z_5(t), z_6(t), e(t), \lambda(t), i_c(t), i_m(t), y_1(t), \dots, y_m(t) \end{bmatrix}$$

where m is computed as explained in Appendix A

B.2.3   SCAQCF Model

The differential equations in above model are integrated with the quadratic integration method and the equations that are algebraic are sufficed to be written at times t and t_m. The SCAQCF model yields the following model.

The standard time domain SCAQCF device model is:

172

$$
\begin{Bmatrix} i(t) \\ 0 \\ 0 \\ i(t_m) \\ 0 \\ 0 \end{Bmatrix} = Y_{eqx}\mathbf{x} + Y_{equ}\mathbf{u} + \left\{ \begin{matrix} \vdots \\ \mathbf{x}^T \left\langle F_{eqx}^i \right\rangle \mathbf{x} \\ \vdots \end{matrix} \right\} + \left\{ \begin{matrix} \vdots \\ \mathbf{u}^T \left\langle F_{equ}^i \right\rangle \mathbf{u} \\ \vdots \end{matrix} \right\} + \left\{ \begin{matrix} \vdots \\ \mathbf{u}^T \left\langle F_{equx}^i \right\rangle \mathbf{x} \\ \vdots \end{matrix} \right\} - B_{eq}
$$

$$
B_{eq} = -N_{eqx}\mathbf{x}(t-h) - N_{equ}\mathbf{u}(t-h) - M_{eq}i(t-h) - K_{eq}
$$

Where

$$
Y_{eqx} = \begin{bmatrix} \dfrac{4}{h}D_{eqxd1} + Y_{eqx1} & -\dfrac{8}{h}D_{eqxd1} \\[2ex] D_{eqxd2} + \dfrac{h}{6}Y_{eqx2} & \dfrac{2h}{3}Y_{eqx2} \\[2ex] Y_{eqx3} & 0 \\[2ex] \dfrac{1}{2h}D_{eqxd1} & \dfrac{2}{h}D_{eqxd1} + Y_{eqx1} \\[2ex] -\dfrac{h}{24}Y_{eqx2} & D_{eqxd2} + \dfrac{h}{3}Y_{eqx2} \\[2ex] 0 & Y_{eqx3} \end{bmatrix}
$$

$$
Y_{equ} = \begin{bmatrix} Y_{equ1} & 0 \\[2ex] \dfrac{h}{6}Y_{equ2} & \dfrac{2h}{3}Y_{equ2} \\[2ex] Y_{equ3} & 0 \\[2ex] 0 & Y_{equ1} \\[2ex] -\dfrac{h}{24}Y_{equ2} & \dfrac{h}{3}Y_{equ2} \\[2ex] 0 & Y_{equ3} \end{bmatrix}
$$

$$F_{eqx} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ F_{eqxx3} & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & Y_{eqxx3} \end{bmatrix}$$

$$F_{equ} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ F_{equu3} & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & F_{equu3} \end{bmatrix}$$

$$F_{equx} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ F_{equx3} & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & F_{equx3} \end{bmatrix}$$

$$N_{eqx} = \begin{bmatrix} -Y_{eqx1} + \dfrac{4}{h} D_{eqxd1} \\[2ex] \dfrac{h}{6} Y_{eqx2} - D_{eqxd1} \\[2ex] 0 \\[2ex] \dfrac{1}{2} Y_{eqx1} - \dfrac{5}{2h} D_{eqxd1} \\[2ex] \dfrac{5h}{24} Y_{eqx2} - D_{eqxd1} \\[2ex] 0 \end{bmatrix}$$

$$N_{equ} = \begin{bmatrix} -Y_{equ1} \\[2ex] \dfrac{h}{6} Y_{equ2} \\[2ex] 0 \\[2ex] \dfrac{1}{2} Y_{equ1} \\[2ex] \dfrac{5h}{24} Y_{equ2} \\[2ex] 0 \end{bmatrix}$$

$$M_{eq} = \begin{bmatrix} I_{size(i(t))} \\[2ex] 0 \\[2ex] 0 \\[2ex] \dfrac{1}{2} I_{size(i(t))} \\[2ex] 0 \\[2ex] 0 \end{bmatrix}$$

$$K_{eq} = \begin{bmatrix} 0 \\ hC_{eqc2} \\ C_{eqc3} \\ \dfrac{3}{2}C_{eqc1} \\ \dfrac{1}{2}hC_{eqc1} \\ C_{eqc3} \end{bmatrix}$$

REFERENCES

[1]   C. Lins, L.E. Williamson, S. Leitner, and S. Teske, "10 years of renewable energy progress," REN21 Secretariat, Paris, France, 2014.

[2]   "The future of the global power sector preparing for emerging opportunities and threats," Deloitte, London, 2015

[3]   R. Li, C. Booth, A. Dyśko, A. Roscoe, H. Urdal and J. Zhu, "Protection challenges in future converter dominated power systems: Demonstration through simulation and hardware tests," *International Conference on Renewable Power Generation (RPG 2015)*, Beijing, 2015, pp. 1-6. I

[4]   *IEEE Standard Definitions for Power Switchgear,* IEEE Standard C37.100 ,1992.

[5]   NERC System Protection and Control Subcommittee, "Reliability Fundamentals of System Protection," NERC, 2010

[6]   Protection System Misoperation Task Force, "Misoperations report," NERC Planning Committee, 2014.

[7]   H. F. Albinali and A. P. Meliopoulos, "A Centralized Substation Protection Scheme that detects hidden failures," *2016 IEEE Power and Energy Society General Meeting (PESGM)*, Boston, MA, 2016, pp. 1-5.

[8]   R. E. Mackiewicz, "Overview of IEC 61850 and Benefits," *2006 IEEE PES Power Systems Conference and Exposition*, Atlanta, GA, 2006, pp. 623-630.

[9]   S., Brahma. "Advancements in centralized protection and control within a substation, "*IEEE Transactions on Power Delivery*, vol. 31, no. 4, pp. 1945–1952, Aug. 2016.

[10] WG K15, "Advancements in centralized protection and control within a substation," IEEE Power System Relaying Committee, 2015

[11] S. L. Nilsson, D. F. Koenig, E. A. Udren, B. J. Allguren and K. P. Lau, "Pros and Cons of Integrating Protection and Control in Transmission Substations," in *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-104, no. 5, pp. 1207-1224, May 1985.

[12] E. Bondia, E. Suarez and F. Cobelo, "Integrated protection and control digital system

for rural substations," *1989 Fourth International Conference on Developments in Power Protection*, Edinburgh, 1989, pp. 113-115.

[13] P. Norberg, A. Fogelberg., and A. Johnsson, "Field experiences from using PC software for protection and control of AC substations," *presented at the CIGRE General Session*, Paris, France, 2006, pp. B3–208.

[14] Mohd Aifaa bin Mohd Arif, "Adaptive Protection and Control for Wide-Area Blackout Prevention," PhD Dissertation, Imperial College London, 2014.

[15] J. Huang, "Adaptive wide area protection of power systems," PhD Dissertation, Iowa State University, 2004.

[16] "Feasibility of adaptive protection and control," in *Power Delivery, IEEE Transactions*, vol. 8, no. 3, pp. 975–983, Jul. 1993.

[17] N. Thomas., L Chen-Ching, and H. Michael, "Adaptation of relay operations in real time," presented at the 15th PSCC, Liege, 2005.

[18] A.Y. Abdelaziz, H.E. Talaat, A.I Nosseir, and , A.H. Ammar, "An adaptive protection scheme for optimal coordination of overcurrent relays," *Electric Power Systems Research*, vol. 61, no. 1, pp. 1–9, Feb. 2002.

[19] B. Kasztenny, and F. Fischer, "Advanced Protection, Automation, and Control Functions," presented at the 1st Annual Protection, Automation and Control World Conference, 2010.

[20] M. Thomas, "Implementation of the Security-Dependability Adaptive Voting Scheme," MSC Dissertation, Virginia Polytechnic Institute and State University, Blacksburg, 2011.

[21] B. Zaremski, "The Advancement of Adaptive Relaying in Power Systems Protection," MSC Dissertation, Virginia Polytechnic Institute and State University, Blacksburg, 2012.

[22] GE Multilin, "Transmission Line Protection Principles." https://www.gegridsolutions.com/multilin/journals/issues/PCJ_2007-12.pdf

[23] Liu, C., "Strategic power infrastructure defense (SPID): a wide area protection and control system," *IEEE/PES Transmission and Distribution Conference and Exhibition*, 2002, pp. 500-502 vol.1.

[24] Hao Li, G. W. Rosenwald, J. Jung and Chen-ching Liu, "Strategic Power Infrastructure Defense," in *Proceedings of the IEEE*, vol. 93, no. 5, pp. 918-933, May 2005.

[25] Chen-Ching Liu, Juhwan Jung, G. T. Heydt, V. Vittal and A. G. Phadke, "The strategic power infrastructure defense (SPID) system. A conceptual design," in *IEEE Control Systems*, vol. 20, no. 4, pp. 40-52, Aug. 2000.

[26] S. Tamronglak, S. H. Horowitz, A. G. Phadke and J. S. Thorp, "Anatomy of power system blackouts: preventive relaying strategies," in *IEEE Transactions on Power Delivery*, vol. 11, no. 2, pp. 708-715, Apr 1996.

[27] A. G. Phadke and J. S. Thorp, "Expose hidden failures to prevent cascading outages [in power systems]," in *IEEE Computer Applications in Power*, vol. 9, no. 3, pp. 20-23, Jul 1996.

[28] Q. Qiu,, "Risk assessment of power system catastrophic failures and hidden failure monitoring & control system," PhD Dissertation, Virginia Polytechnic Institute and State University, 2003.

[29] X. Gao, J. S. Thorp and D. Hou, "Case studies: Designing protection systems that minimize potential hidden failures," *2013 66th Annual Conference for Protective Relay Engineers*, College Station, TX, 2013, pp. 384-393.

[30] A. P. S. Meliopoulos *et al*., "Dynamic State Estimation-Based Protection: Status and Promise," in *IEEE Transactions on Power Delivery*, vol. 32, no. 1, pp. 320-330, Feb. 2017.

[31] R. Fan, A. P. S. Meliopoulos, G. J. Cokkinides, L. Sun and Yu Liu, "Dynamic state estimation-based protection of power transformers," *2015 IEEE Power & Energy Society General Meeting*, Denver, CO, 2015, pp. 1-5.

[32] Yu Liu, A. P. Sakis Meliopoulos, Rui Fan and Liangyi Sun, "Dynamic State Estimation based protection of microgrid circuits," *2015 IEEE Power & Energy Society General Meeting*, Denver, CO, 2015, pp. 1-5.

[33] Z. Tan, "Dynamic State Estimation Based Transmission Line Protection," PhD Dissertation, Georgia Institute of Technology, Atlanta, 2016.

[34] L. Sun, R. Fan, A. P. S. Meliopoulos, Y. Liu and Z. Tan, "Capacitor bank protection via constraint WLS dynamic state estimation method (CWLS-DSE)," *2016 North American Power Symposium (NAPS)*, Denver, CO, 2016, pp. 1-6.

[35] Y. Liu, A. P. Meliopoulos, L. Sun and R. Fan, "Dynamic state estimation based protection of mutually coupled transmission lines," in *CSEE Journal of Power and Energy Systems*, vol. 2, no. 4, pp. 6-14, December 2016.

[36] A. P. Meliopoulos, et al., "Integration & automation: From protection to advanced energy management systems," *in Bulk Power System Dynamics and Control-IX Optimization, Security and Control of the Emerging Power Grid (IREP)*, 2013 IREP Symposium, 2013, pp. 1–11.

[37] R. Fan, A. P. S. Meliopoulos, L. Sun, Z. Tan and Y. Liu, "Transformer inter-turn faults detection by dynamic state estimation method," *2016 North American Power Symposium (NAPS)*, Denver, CO, 2016, pp. 1-6.

[38] R. Fan, "TRANSFORMER PROTECTION BASED ON DYNAMIC STATE ESTIMATION," PhD Dissertation, Georgia Institute of Technology, Atlanta, 2016.

[39] A. P. S. Meliopoulos, G. J. Cokkinides, Z. Tan, S. Choi, Y. Lee and P. Myrda, "Setting-Less Protection: Feasibility Study," *2013 46th Hawaii International Conference on System Sciences*, Wailea, HI, USA, 2013, pp. 2345-2353.

[40] M. Kezunovic, "Translational Knowledge: From Collecting Data to Making Decisions in a Smart Grid," in *Proceedings of the IEEE*, vol. 99, no. 6, pp. 977-997, June 2011.

[41] S. Vasilic,, and M. Kezunovic, "Fuzzy ART neural network algorithm for classifying the power system faults," in *IEEE Transactions on Power Delivery*, vol. 20, no. 2, pp. 1306-1314, April 2005.

[42] S. Vasilic, "Fuzzy neural network pattern recognition algorithm for classification of the events in power system networks," PhD Dissertation, Texas A&M University, College Station, Texas, USA, 2004.

[43] S. Vasilic, and M. Kezunovic, "An improved neural network algorithm for classifying the transmission line faults," *2002 IEEE Power Engineering Society Winter Meeting. Conference Proceedings (Cat. No.02CH37309)*, 2002, pp. 918-923 vol.2.

[44] Y. Cheng, X. Chen, J. Ren, X. Xuan, and X. Li, "Study on hidden failure of relay protection in power system,"*2013 IEEE International Conference on Cyber Technology in Automation, Control and Intelligent Systems*, Nanjing, 2013, pp. 434-439.

[45] A. P. Meliopoulos, G. J. Cokkinide, "Power System Relaying, An Introduction," in

Power System Relaying: Theory and Applications, Ch.1, unpublished.

[46] E.O.Schweitzer, B. Morris, and D. Costello, "Monitoring the Health of SEL Relays." .SEL, Pullman, WA, AN2012-01, 2012.

[47] E. Murat, "The watchdog : a main component in the protection scheme," Schneider-Electric, watchdog_sepam_05, 2005.

[48] System Protection and Control Working Group, "Relay Communication Misoperations," SPP, Little Rock, AR, SPP-White Paper, 2014.

[49] L. G. Hewitson ,M. Brown, and R. Balakrishnan, "Instrument transformers," in *Practical Power System Protection*,1st ed, Newnes, 2004, ch.6., sec. 6.4, pp. 54–65.

[50] Paul M. Anderson, "Protection Measurements and Controls," in *Power System Protection* , 1, Wiley-IEEE Press, 1999,ch.2., pp.1330-

[51] H.J.Altuve, N. Fischer, G. Benmouyal, and D. Finney, "Sizing Current Transformers for Line Protection Applications," *presented at the 67th Annual Georgia Tech Protective Relaying Conference*, Atlanta, 2013.

[52] Relay Work Group, "Relaying Current Transformer Application," WECC, Salt Lake City, Utah, White Paper, 2014.

[53] EEE Standard Requirements for Instrument Transformers," in *IEEE Std C57.13-1993(R2003) (Revision of IEEE Std C57.13-1978* , vol., no., pp.i-73, 2003.

[54] "Instrument Transformer Basic Technical Information and Application," GE Digital Energy.

[55] B. Kasztenny, J. Mazereeuw, and K. Jones, "CT Saturation in Industrial Applications – Analysis and Application Guidelines," GE Multlin.

[56] Z. Xu, M. Proctor, I. Voloh, and M. Lara, "CT saturation tolerance for 87L applications," *presented at the 2015 68th Annual Conference for Protective Relay Engineers,* College Station, 2015.

[57] B. E. Lee, J. Lee, S. H. Won, B. Lee, P.A. Crossley, and Y. C. Kang, "Saturation Detection-Based Blocking Scheme for Transformer Differential Protection," *energies*, vol. 7., pp. 4571-4587, 2014.

[58] IEEE Guide for the Application of Current Transformers Used for Protective Relaying Purposes," in *IEEE Unapproved Draft Std PC37.110/D911Oct 07* , vol., no., pp., 2007

[59] "Voltage TRANSFORMERS," GE

[60] Y. Cao, and P. Shao, "PT 10kV high-voltage fuse bus causes and solutions," *2011 International Conference on Advanced Power System Automation and Protection*, Beijing, 2011, pp. 1643-1645.

[61] Line Protection Subcommittee Working Group D-7, "Loss of ac Voltage Considerations for Line Protection," Line Protection Subcommittee of the IEEE Power Engineering Society, Power System Relaying Committee.

[62] H. F. Albinali, A. P. Meliopoulos and C. Vournas, "Dynamic state estimation-based centralized protection scheme," *2017 IEEE Manchester PowerTech*, Manchester, United Kingdom, 2017, pp. 1-6.

[63] S. M. David, "Chi_square test," Purdue University.

[64] A. P. Meliopoulos, "Operating State Estimation," in Power System Modeling, Analysis and Control, Ch.7 unpublished.

[65] A. Ali and G. E. Antonio, "Bad data detection and identification," *in Power System State Estimation: Theory and Implementation*, 2nd ed., vol. 3. J. Peters, Ed. New York: McGraw-Hill, pp. 15–67, 1964.

[66] H. Albinali, A. P. Meliopoulos, G. Cokkinides, and P. Myrda "Hidden failures detection and correction via substation wide dynamic state estimation," *presented at the PAC World Americas Conference*, Raleigh, NC, USA, pp. 1–6, 2016.

[67] T. Alquthami, "A SMART HOUSE ENERGY MANAGEMENT SYSTEM," PhD Dissertation, Georgia Institute of Technology, 2015.

[68] A. P. Meliopoulos and G. J. Cokkinide, "Basic Concepts," in *Power System Relaying: Theory and Applications*, Ch.2, unpublished.

[69] A. P. Meliopoulos, G. J. Cokkinides, and G. Stefopoulos,"Quadratic Integration Method", *Proceedings of the 2005 International Power System Transients Conference (IPST 2005)*, Montreal, Canada, June 19-23, 2005.

[70] A. Mukhtar, "Weighted Least Square Estimation" in Electric *Power System State Estimation*, 1st ed. Artech House, 2012.

[71] Communication networks and systems for power utility automation – Part 7-1: Basic communication structure - Principles and models, IEC Standard 61850-7-1, Ed. 2, Mar., 2010.

[72] D. Hou, and D. Dolezilek, "IEC 61850 – What it can and cannot offer to traditional protection schemes," *Presented at the 1st Annual Protection, Automation and Control World Conference*, 2010.

[73] R. Mackiewicz and H. Falk, "Insight in IEC 61850: What is it?" Presentation, 2012.

[74] Zhu Yongli, Wang Dewen, Wang Yan and Zhao Wenqing, "Study on interoperable exchange of IEC 61850 data model," *2009 4th IEEE Conference on Industrial Electronics and Applications*, Xi'an, 2009, pp. 2724-2728.

[75] Communication networks and systems for power utility automation – Part 7-4: Basic communication structure – Compatible logical node classes and data object classes, IEC Standard 61850-7-4, Ed. 2, Mar. 2010.

[76] Communication networks and systems for power utility automation – Part 7-2: Basic information and communication structure - Abstract communication service interface (ACSI), IEC Standard 61850-7-2, Ed. 2, Mar. 2010.

[77] "IEC 61850 information model concepts and update for distributed energy resources (DER) use cases and functions," A white paper ,Smart Grid Interoperability Panel (SGIP), Wakefield, MA , October 2015.

[78] Communication networks and systems for power utility automation – Part 6: Configuration description language for communication in electrical substations related to IEDs, IEC Standard 61850-6, Ed. 2, Mar. 2010.

[79] P. Terwiesch, C. Rytoft, E. M. Hugo, H. Bawa, P. Reinhardt, and Moglestue, A., "Special Report IEC 61850," ABB, Baden, Switzerland.

[80] C. R. Ozansoy, A. Zayegh and A. Kalam, "Object Modeling of Data and DataSets in the International Standard IEC 61850," in *IEEE Transactions on Power Delivery*, vol. 24, no. 3, pp. 1140-1147, July 2009.

[81] Communication networks and systems for power utility automation – Part 8-1: Specific Communication Service Mapping (SCSM) – Mappings to MMS, IEC Standard 61850-8-1, Ed. 2, Mar. 2010.

[82] Ryan L. O'Fallon, Dean A. Klas, Timothy Tibbals, and Saurabh Shah "IEC 61850 MMS SCADA Network Optimization for IEDs," *Presented at Rockwell Automation*

on the Move, Spokane, WA.

[83] K. P. Brand, "IEC 61850 as backbone for smart PAC systems," in *CSEE Journal of Power and Energy Systems*, vol. 2, no. 4, pp. 15-22, December 2016.

[84] D. M. E. Ingram, P. Schaub, R. R. Taylor and D. A. Campbell, "Performance Analysis of IEC 61850 Sampled Value Process Bus Networks," in *IEEE Transactions on Industrial Informatics*, vol. 9, no. 3, pp. 1445-1454, Aug. 2013.

[85] Communication networks and systems for power utility automation – Part 9-2: Specific Communication Service Mapping (SCSM) – Sampled values, IEC Standard 61850-9-2, Ed. 2, Mar. 2010.

[86] D. Ingram, and B. Smellie, "Solving Electrical Substation Timing Problems." Tekron Whitepaper, October 2014.

[87] P. A. Crossley, H. Guo and Z. Ma, "Time synchronization for transmission substations using GPS and IEEE 1588," in *CSEE Journal of Power and Energy Systems*, vol. 2, no. 3, pp. 91-99, Sept. 2016.

[88] K. Behrendt, and K. Fodero, "The perfect time: An examination of time-synchronization techniques," *presented at the 32nd Annual Western Protective Relay Conference*, 2005.

[89] J. McGhee and M. Goraj, "Smart High Voltage Substation Based on IEC 61850 Process Bus and IEEE 1588 Time Synchronization," *2010 First IEEE International Conference on Smart Grid Communications*, Gaithersburg, MD, 2010, pp. 489-494.

[90] H. Kirrmann, P. Rietmann, and S. Kunsman, "Network redundancy using IEC 62439," *PAC World*, Autumn 2008.

[91] H. Kirrmann, "Seamless redundancy", In ABB Review: Special Report IEC 61850, August 2010.

[92] C. Wester, M. Adamiak and J. Vico, "IEC61850 protocol - practical applications in industrial facilities," *2011 IEEE Industry Applications Society Annual Meeting*, Orlando, FL, 2011, pp. 1-7.

[93] H. A. Retty, "Evaluation and standardizing of phasor data concentrators," MSc Dissertation, Virginia Polytechnic Institute and State University, 2013.

[94] Power System Relaying Committee, "IEEE Guide for phasor data concentrator

requirements for power system protection, control, and monitoring," 2013.

[95] M. Kanabar, M. G. Adamiak and J. Rodrigues, "Optimizing Wide Area Measurement System architectures with advancements in Phasor Data Concentrators (PDCs)," *2013 IEEE Power & Energy Society General Meeting*, Vancouver, BC, 2013, pp. 1-5.

[96] B. Baumgartner, C. Riesch, and M. Rudigier, "IEEE 1588/PTP: The future of time synchronization in the electric power industry," OMICRON electronics GmbH, Klaus, Austria,

[97] S. Meliopoulos, G. Cokkinides, R. Fan, L. Sun and B. Cui, "Command authentication via faster than real time simulation," *2016 IEEE Power and Energy Society General Meeting (PESGM)*, Boston, MA, 2016, pp. 1-5.

[98] S. Meliopoulos, G. Cokkinides, R. Beyah, S. Walters and P. Myrda, "Cyber Security and Operational Reliability," *2015 48th Hawaii International Conference on System Sciences*, Kauai, HI, 2015, pp. 2655-2663.

[99] W. Wenye, L. Zhuo, "Cyber security in the Smart Grid: Survey and challenges," *Computer Networks*, vol. 57, no. 2, April 2013, Pages 1344–1371.

[100] A. P. S. Meliopoulos, G. Cokkinides, R. Fan and L. Sun, "Data Attack Detection and Command Authentication via Cyber-Physical Comodeling," in *IEEE Design & Test*, vol. 34, no. 4, pp. 34-43, Aug. 2017.