

Improving the Resilience and Stability of the Power Grid through the Deployment of
Remedial Action Schemes

A Thesis

Presented in Partial Fulfilment of the Requirements for the

Degree of Master of Science

with a

Major in Electrical Engineering

in the

College of Graduate Studies

University of Idaho

by

Babatunde Oluwatobi Ajao

Major Professor: Brian K. Johnson, Ph.D.

Committee Members: Yacine Chakhchoukh, Ph.D.; Daniel Conte de Leon, Ph.D.

Department Administrator: Joseph D. Law, Ph.D.

August 2020

Authorization to Submit Thesis

This thesis of Babatunde Ajao, submitted for the degree of Master of Science with a major in Electrical Engineering and titled “Improving the Resilience and Stability of the Power Grid through the Deployment of Remedial Action Schemes,” has been reviewed in final form. Permission, as indicated by the signatures and dates given below, is now granted to submit final copies to the College of Graduate Studies for approval.

Major Professor _____ Date _____
 Brian K. Johnson, Ph.D.

Committee
 Members _____ Date _____
 Yacine Chakhchoukh, Ph.D.

_____ Date _____
 Daniel Conte de Leon, Ph.D.

Department
 Administrator _____ Date _____
 Joseph D. Law, Ph.D.

Abstract

Maintaining the stability, reliability, and most importantly, the cyber-security of the power grid is becoming more complicated as the demands placed on the power system grows steadily as do cyber threats. As the demand placed on power system increases, a modern power system is more likely to operate near its secure limit. Due to the cost implications of building more plants and transmission lines to make the power system robust, the already installed infrastructure is usually operated closer to its secure operating limits. Deployment of Remedial Action Schemes (RAS) is a viable economical alternative to maintain operational security when the construction of new infrastructure is not desirable. It is also important to ensure that the deployed RAS scheme is protected from cyber-attacks intended to make it mis-operate, whereby it would make the power grid even more vulnerable to cascading failure.

In this thesis, two RAS schemes were designed, modelled and deployed to improve the resilience, reliability and stability of the power system. The first RAS scheme is designed to improve the transient stability index of the system when critical events capable of driving the system to cascading failure occur. The second RAS scheme is designed to be immune to data measurement cyber threats. The second RAS scheme should operate correctly even in the presence of false data in the power grid. Both RAS models were deployed and tested on the WECC 179 bus test system.

Acknowledgements

There are many people that have earned my gratitude for their contribution to my time in graduate school. Firstly, I would like to thank God almighty, the author and finisher of my faith. My profound gratitude also goes to my advisor in person of Dr. Brian K. Johnson. With his consistent help, support and funding throughout my years here I was able to accomplish more than I thought possible. He has pushed me to pursue new and challenging research works and has encouraged me when difficulties inevitably arose. With his help I have gained a great deal of knowledge and confidence as an electrical engineer. In addition, my appreciation goes to Dr. Yacine Chakhchoukh and Dr. Daniel Conte de Leon for their contribution to my publication and thesis. Both of them were instrumental in the guidance of my research work.

Finally, a huge thanks goes to my beloved wife, Ruth for your love and immense support. You have been a huge pillar behind my success hitherto and I really appreciate you for this. And to my beautiful daughter Samantha, thank you for helping me recharge when I felt overwhelmed. Also to my sisters Yetunde and Titilayo, thank you for being there all these years. Mom and dad, thank you for supporting me through college and graduate school. I love you and could not have done this without your help.

Dedication

This thesis work is dedicated to my wife, Ruth, who has been a constant source of support and encouragement during the challenges of graduate school and life in general. I am truly thankful for having you in my life. And to our beautiful daughter, Samantha, you are indeed a treasure from the Lord. This work is also dedicated to my parents, Olugbenga and Tejumade Ajao, who have always loved me unconditionally and whose good examples have taught me to work hard for the things that I aspire to achieve.

Table of Contents

Authorization to Submit Thesis	ii
Abstract	iii
Acknowledgements	iv
Dedication	v
Table of Contents	vi
List of Tables	ix
List of Figures	x
1 Introduction	1
1.1 Background	1
1.2 Objectives and Contributions	3
1.3 Thesis Organization	4
2 Literature Review	5
2.1 Power System Stability	5
2.1.1 Rotor Angle Stability	6
2.1.1.1 Transient Angle Instability	6
2.1.1.2 Small Disturbance Angle Instability	7
2.1.2 Voltage Stability	7
2.1.3 Frequency Instability	8
2.2 Operating States of the Power System	8
2.3 Power System Islanding	10
2.4 Overview of Remedial Action Schemes	11

2.4.1	RAS Classification	11
2.4.1.1	Event-based Schemes	11
2.4.1.2	Parameter-based Schemes	12
2.4.1.3	Response-based Schemes	12
2.4.2	RAS Features	12
2.4.2.1	RAS Status Monitoring and Controller Logic	13
2.4.2.2	RAS Arming/Triggers	13
2.4.3	Possible Actions in RAS.....	13
2.4.4	Examples of RAS Implementation in Literature	15
2.5	Cyber-Security Issues in Power System	15
3	Implementation of Remedial Action Scheme for Transient Stability Index Improvement of Power System Island	17
3.1	Introduction	17
3.2	Deployment and Testing of RAS Model.....	19
3.2.1	Transient Stability Index.....	20
3.2.2	Events and Actions.....	21
3.2.3	RAS User-defined Model	22
3.2.4	Simulation Results.....	23
3.3	Benefit of RAS Deployment in Power Grid Island.....	25
3.4	Concluding Remarks	25
4	Implementation and Deployment of Attack-Resilient Remedial Action Schemes	27
4.1	Background and Problem Description	27
4.2	Cyber Vulnerabilities of WAMPAC	28
4.2.1	Public Network Connectivity.....	29
4.2.2	Communication Protocols	29

4.2.3	Supply Chain.....	29
4.2.4	Human Factors	30
4.3	Cyber-Security Concerns in RAS System	30
4.4	False Data Injection Attack Surface of the RAS Scheme.....	31
4.5	Proposed RAS Scheme.....	33
4.5.1	Deployment and Testing of the Proposed Robust RAS Logic.....	35
4.5.1.1	Case 1	35
4.5.1.2	Case 2	40
4.5.2	Concluding Remarks.....	41
5	Conclusions and Future Work.....	44
5.1	Conclusions	44
5.2	Contributions	45
5.3	Recommendations for Future Work	45
	References	46
	Appendix A The full results from TSAT package of DSATools for IEEE	
	179 bus system.....	52
	Appendix B Copyright Permission.....	58

List of Tables

3.1	Result of Transient Stability Index Improvement Under Different Cases	24
-----	---	----

List of Figures

2.1	Classification of Power System Stability [7]	5
2.2	The five states of an electric power system and their transitions as defined by Fink and Carlsen [14]	10
2.3	Illustration of implementation of simple RAS logic.	13
3.1	WECC 179-bus test system	20
3.2	Logic Diagram of the Implemented RAS.	22
3.3	Bus Voltage Magnitudes for Case 1 without RAS.	24
3.4	Bus Voltage Magnitudes for Case 1 with RAS.	25
4.1	Potential Cyber-Security Concerns in RAS Systems	30
4.2	RAS False Data Attack Surface.	32
4.3	Proposed RAS Logic Flow Chart.	34
4.4	Logic Diagram of the Proposed RAS Scheme Modelled in UDM for Case 1.	36
4.5	Simulation Result Showing Faulted Lines Removed but RAS Refused to Trigger Due to False Data Injection in Case 1	37
4.6	RAS Model Loaded into the Case File	38
4.7	Simulation Result: RAS Correctly Triggered When the Proposed Scheme was Implemented for Case 1	39
4.8	RAS Summary for Case 1	39
4.9	Logic Diagram of the Proposed RAS Scheme Modelled in UDM for Case 2	41
4.10	Simulation Result Showing Faulted Lines Removed but RAS Refused to Trigger Due to False Data Injection in Case 2	42
4.11	Simulation Result: RAS Correctly Triggered When the Proposed Scheme was Implemented for Case 2	43
B.1	IEEE Permission for Copying a Paper as Chapter 3 in the Thesis	58

Chapter 1: Introduction

This chapter presents the background motivation behind this research as well as the goals of the research. A brief introduction of transient stability of the power grid as well as Remedial Action Schemes will be provided. Also, the importance of deploying remedial action schemes in power grid system integrity protection is discussed to highlight the relevance of the research objectives to the power utility industry. The need to secure RAS schemes from data measurement based cyber-attacks is also briefly addressed in this chapter.

1.1 Background

The modern smart power grid is often operated closer to the maximum secure limits of transmission assets due to increases in demand for power transfer from remote non-fossil generation, limited generation options to meet this demand, as well as environmental and economic constraints on the construction of new transmission lines. Generally speaking, the power grid was designed with inherent controls to operate within acceptable and secure voltage and frequency levels in the face of various stringent disturbing conditions like generation loss, sudden load change and the occurrence of different types of faults. However, when some unexpected events or simultaneous multiple critical disturbances take place in a power grid that is already operating with limited stability margin, transmission lines and transformers in such systems are liable to being overloaded. As a result, different generator groups in the system may lose the synchronism that is vital to their proper operation. If this condition is not immediately remedied and is allowed to persist for a time frame ranging from few cycles to several minutes (depending on evolving phenomena), cascading tripping of transmission equipment can occur leading to regional collapse of the power grid.

Rotor angle instability and voltage instability are two of the most serious conditions that trigger cascading failure in the power system. An out-of-step condition that results from the loss of synchronism between two or more synchronous generators or sets of generator in the power system gives rise to angular stability problems in the grid. This condition may

result in wide fluctuation in power flow which if not curtailed in a timely manner might ultimately lead to uncontrolled system separations due to the operation of protection relays. Voltage instability on the other hand occurs when the system becomes heavily loaded and the reactive power resources approach their limit. The overloading of transmission lines typically occurs because of power imbalance in the grid following an outage. When the overloaded transmission lines are tripped, it results into further overloading of the remaining equipment, potentially resulting in cascading tripping. This sequence of events is likely to develop into larger system outage if remedial actions are not taken in a timely manner.

Remedial action schemes are one of the measures taken to mitigate the occurrence of the power system failure described above. RAS are used to mitigate the problem of instability that results from the combined loss of several major assets in a power grid that evolve too fast for human operator intervention [1]. They help guard against out-of-step conditions that may result in cascading failure or degradation of major power system equipment [2]. They are highly economical and simpler to design when compared to other alternatives like the construction of new transmission lines and power plants. Conventional protection schemes are focused on individual power system equipment like the generators, transmission lines and transformers. Equipment protection is however insufficient to provide adequate protection to the power system integrity especially with the increasing demand for regional transfer in the modern power grid [3]. If anything, traditional protection schemes can further aggravate wide area problems while trying to protect individual local equipment from abnormal operating conditions or overloading. To avert this problem, wide area information about the operating state of the power system needs to be collected and provided to the RAS scheme to be able to take appropriate correct remedial actions to mitigate cascading failure in the grid. These information are also made available to operators in the control centers. There is usually sufficient time available for operator's intervention to alleviate the system condition for certain events like thermal overloading with proper action following contingency analysis in the control center. However, to ensure quick response and maximum loadability of the

power system, RAS schemes can be designed to manage such events faster than operator actions [4]. Modern communication technologies like Supervisory Control and Data Acquisition (SCADA) and Synchrophasor Units (PMUs) have made this possible. The data and information provided by these technologies can be used to analyse the state of the power system and provide adequate remedial action in a timely manner.

With these technologies like SCADA which incorporate communication to the control center allowing connection to the control side of the substation comes the inherent vulnerability associated with cyber-attack risks. Siemens and Ponemon Institute conducted a survey on cyber threats to power utilities in 2019 [5]. Fifty-four percent of the 1,726 utility professionals surveyed (representing electric utilities around the world) expect at least one cyber-attack on their critical infrastructures within the year 2020. Hence, there is a need to provide adequate security for the power grid against cyber-attacks. The data measurement cyber threat is a focus of this thesis. If the RAS scheme is allowed to operate with falsified data, it will most likely take or fail to take actions that would drive the power grid into instability and ultimately results in cascading failure. For this reason, it is important to ensure that the RAS scheme receives data that correctly depicts the true state of the power system at any point in time. Or better-still, the RAS scheme can be developed to be robust enough to take the correct actions even in the presence of falsified data.

1.2 Objectives and Contributions

The main goal of this research is to explore the possibility of using remedial action schemes to improve the resilience and stability of the smart power grid in the face of false data injection attacks. Two RAS schemes were designed and modeled to achieve the goals set out for this research.

The objective of the first RAS model is to aid stability improvement as measured through transient stability index of the power grid. The proposed model was implemented with the help of user-defined models (UDM) in the commercial Transient Stability Assessment Tool

(TSAT) while the powerflow analysis was conducted in the Powerflow Short-circuit Analysis Tool (PSAT). These applications are packages from PowerTech's DSATools [6].

The objective of the second RAS model designed in this research is to ensure that the scheme is robust enough to take correct remediation action(s) even in the presence of falsified data when the smart grid is under data measurement cyber-attack. The same packages from DSATools were also used to design and deploy the models. Both schemes were tested and validated using the WECC 179 Bus System.

1.3 Thesis Organization

The rest of the thesis is structured as follows: Chapter 2 includes a literature review, which addresses power system stability, operating states, data measurement cyber-attacks on smart power grid and remedial action schemes.

Chapter 3 presents the first RAS scheme that was modeled and deployed in the power grid to improve its transient stability index. The development of the scheme and its validation under different critical events in the system are provided.

Chapter 4 proposes a second RAS scheme that is robust enough to operate correctly even in the presence of falsified data. The development, deployment and the validation of the scheme are presented.

Chapter 5 summarizes the proposed RAS models in this thesis and presents the research conclusions and the contributions. Some suggestions for future research endeavors are also provided.

Chapter 2: Literature Review

In this chapter, the essential background related to power grid stability and different operating states in the power systems are presented. A broad overview of remedial action schemes is provided including descriptions of several RAS techniques used in practice. Various types of data measurement cyber threats on the power system are also discussed in this chapter.

2.1 Power System Stability

A Power system is said to be stable if it has the capability of returning to a stable operating state following the occurrence of events which can result in abnormal operation in the power grid. Typically, there are three main subdivisions of power system stability, namely rotor angle stability, frequency stability and voltage stability [7]. Due to the non-linearity of the power system, its stability is not only affected by the severity of the disturbance, but also by the prevailing operating condition of the power network at the time of the disturbance. In line with this, the angular and voltage stability have been further subdivided into small and large disturbance stability. This classification is illustrated in Figure 2.1 [7].

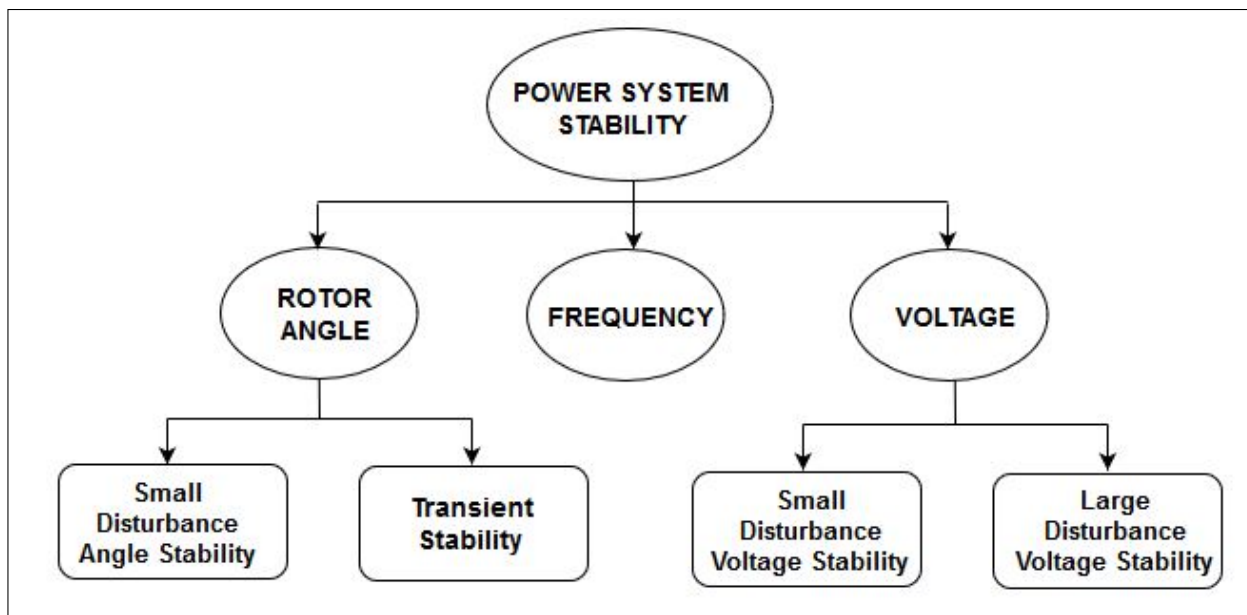


Figure 2.1: Classification of Power System Stability [7]

2.1.1 Rotor Angle Stability

Rotor angle stability is the ability of the interconnected synchronous machines running in the power system to remain in the state of synchronism [8]. The power system experiences angle, and in some cases frequency oscillations in response to disturbances that impact power balance. In the vast majority of cases these are damped oscillations due to the response of synchronous generators and their controls. In case of angle instability the oscillations continue to grow. Depending on the severity and origin of these unstable oscillations, rotor angle instability is categorized as transient angle instability or small disturbance angle instability.

2.1.1.1 Transient Angle Instability

Kundur defines transient stability as the ability of the power system to maintain synchronism when subjected to severe disturbance(s) such as loss of generation, sudden loss of large load or a fault on transmission facilities [9]. These types of disturbing events typically result in large differences in generator angles and significant changes in the power system frequency, bus voltages, and active and reactive power flows in the grid. In an unstable case this loss of synchronism may impact one single generating unit, a power plant (with multiple generators) or a region of the power network. If appropriate remedial counter actions are not taken in a timely manner, local transient instability may result in cascading failure.

Large power flows, lightly meshed networks and long distance power transport are some of the features that contribute to transient angle instability. Accordingly, tie lines and weak power system interconnections are the typical sources of transient instability. Since transient instability involves large current and voltage variations, modern fast operating protection devices may be incorrectly initiated leading to undesirable protection operations making the condition worse.

2.1.1.2 Small Disturbance Angle Instability

Small disturbance angle stability, also known as small signal stability, is a subconcept of transient angle stability, which refers to the ability of a power system to maintain synchronism under small disturbances. In this context, a disturbance is considered to be small if the equation that describes the resulting response of the system can be linearized for the purpose of analysis [9]. This kind of disturbance happen all the time due to small variations in load and generation. Small disturbance stability usually depends on the initial operating state of the power system. The instability that may result can be of two forms: i) increase in rotor angle due to lack of synchronizing torque, or ii) rotor oscillations of increasing amplitude due to lack of sufficient damping torque [7].

Small disturbance rotor angle stability problems maybe either local or global in nature. For the local issues, a very small part of the power system is involved in power instability. These are usually associated with rotor angle oscillations of a single power plant and its controls against the rest of the power system. Global issues on the other hand are caused by the interactions among large groups of generators and their controls, and have widespread effects on the power system. They involve oscillations of a group of generators in one area swinging against a group of generators in another area [9].

2.1.2 Voltage Stability

Voltage stability refers to the ability of the power grid to maintain acceptable voltages at all buses in the system under normal condition and after being subjected to disturbing event(s). The instability that may result occurs in the form of a progressive fall or rise of voltages of some buses in the power system. A possible outcome of voltage instability is loss of load in an area, or tripping of transmission lines and other elements by their protective systems leading to cascading outages [10]. The main cause of voltage instability is the inability of the power system to meet reactive power demand [9].

Voltage instability may be caused by a variety of single or multiple disturbing events. Typical initiating events may include sudden heavy load pick-up and generator tripping, especially the generators close to the loads that is supporting the voltage in that area. The power system is liable to collapse within a few seconds after the occurrence of such a disturbance if remediation actions are not taken in a timely manner.

2.1.3 Frequency Instability

Frequency stability can be described as the ability of the power system to maintain an acceptable frequency range during normal operation or after a severe disturbance. Hence, frequency instability takes place when there is a load-supply mismatch and the power system controls are unable to compensate for this mismatch before the frequency reaches an unacceptable value. Typical events that may lead to frequency instability are outages on major generating units and uncontrolled islands formation in the power system due to faults on protection misoperation.

Generally speaking, frequency instability is associated with inadequacies in equipment responses, poor coordination of control and protection equipment, or insufficient generation reserve [7]. In isolated island systems, frequency stability could be of concern for any disturbance causing a relatively significant loss of load or generation [11].

It is very important to take extra measures to limit frequency excursion when normal frequency control means fail to maintain the frequency within an acceptable range. Generators are especially sensitive to fairly minute frequency variations.

2.2 Operating States of the Power System

Rapid and sudden changes in online operating conditions of the power system is one of the challenges that threatens the reliability and resilience of the power system. Use of intermittent energy resources like wind and solar, and increased inter-regional power

transfers in the power system are some of the most pressing factors affecting the reliability of the power system. Power system blackouts and cascading failures are often due to lack of situational awareness in the power system [12]. It is then very crucial for human operators and autonomous control devices to have a true knowledge of the operating states of the power system at all time. This situational awareness can only be achieved through real-time system monitoring and precise estimation of the power system operating states and conditions from those measurements at all times.

The power system can be described using linear and nonlinear differential equations with equality and inequality constraints. The equality constraints typically corresponds to the generation and load balance while the inequality constraints have to do with the power system equipment capacity ranges like voltage and power flow limits. Under normal operating condition, the power system satisfies both the equality and inequality constraints. When the system remains in the normal operating condition even after a severe disturbance, it is because it has sufficient security margin to maintain the normal state. Security margin can be described as the range between the operating state and the boundary of unstable conditions. The system moves into an alert state if there is a decrease in the security margin, even though it still satisfies all the equality and inequality constraints [13]. This usually indicates that the system is vulnerable to failures. This means that in the event of another disturbance, referred to as a contingency, when studying potential events before this occur at least one inequality constraint will be violated [13]. If the system is subjected to more abnormalities at this point, it moves into emergency state depending on the extremity of the event. Further severe abnormalities push the system into the extremis state, where both the equality and inequality constraints are violated. Corrective actions are typically taken at this point to mitigate violation impacts. Once the corrective actions are taken, the system can be restored to pre-contingency state. This is the restorative state of the power system. The classification of the power system operating states is illustrated in Figure 2.2 [14].

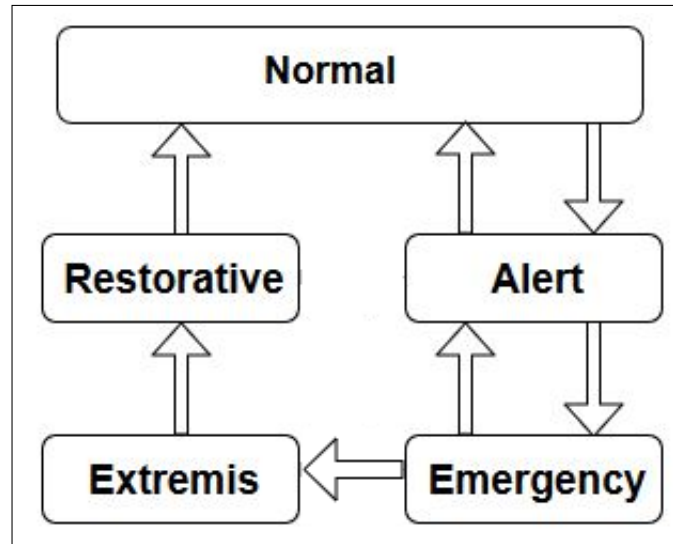


Figure 2.2: The five states of an electric power system and their transitions as defined by Fink and Carlsen [14]

In this thesis, remedial action schemes are implemented when the system is in the emergency state in order to restore a power system that is subjected to transient instability.

2.3 Power System Islanding

Power system islanding is the condition in which distributed generation becomes isolated from the electric power grid and continues to supply power to the load in the portion of the grid it remains connected to. The separation of the generation from the main grid could be intentional or unintentional. For intentional islanding, utilities typically creates power system islands to contain the negative impact of faults or cyber-attacks to certain part of the grid. This would prevent the impact of the disturbing event from propagating to other parts of the inter-connected power system. Unintentional islanding on the other hand is not pre-planned and it can result from system faults, environmental causes and equipment failure.

2.4 Overview of Remedial Action Schemes

Remedial action schemes are designed to detect predetermined system conditions that have a high probability of causing unusual stress on the power system [15]. As defined by NERC, “RAS is an automatic protection system designed to detect abnormal or predetermined system conditions, and take corrective actions other than and/or in addition to the isolation of faulted components to maintain system reliability. Such action may include changes in demand, generation (MW and MVar), or system configuration to maintain system stability, acceptable voltage, or power flow” [16].

More often than not, RAS are designed to serve specific purposes such as allow increased power transfer, mitigate overfrequency or underfrequency, provide reactive support, to limit line thermal overloads, etc. These schemes are becoming more common because they are less costly to design and implement than other alternatives such as construction of new transmission lines and power plants [2]. They can also be implemented relatively quickly and used until a long term fix is implemented. RAS supplements ordinary protection and control devices to prevent violation of the NERC reliability standards and limit the impact of extreme events [16]. They are designed to operate as autonomous or partially autonomous schemes that can take action without a human in the loop.

2.4.1 RAS Classification

One method of classifying RAS principles is by the inputs used to detect system conditions and disturbances. This classification was extracted from [17]:

2.4.1.1 Event-based Schemes

These schemes directly detect outages and/or fault events and initiate action(s) such as generator/load tripping to fully or partially mitigate the event impact. This open-loop type of control is commonly used for preventing system instabilities when necessary remedial

actions need to be applied as quickly as possible.

2.4.1.2 Parameter-based Schemes

These schemes use a sudden significant variation in the measured variables to confirm the occurrence of a critical event. This is also a form of open-loop control but with indirect event detection. The indirect method is mainly used to detect sudden changes in the measured variables which may cause instabilities, but may not be readily detected. Examples include detecting the remote switching of breakers on the remote end of lines. The measured variables may include power flow, local or remote voltage magnitudes and angles.

2.4.1.3 Response-based Schemes

These schemes monitor the response of the system during disturbances and then incorporate a closed-loop process to react to the actual system conditions. It is possible to closely calibrate the response-based scheme to the magnitude of the disturbance, although this scheme is usually not fast enough to mitigate instability following a very severe contingency. The class of scheme can, however, be implemented if a slower remedial action is acceptable. They are typically deployed for small signal cases, possibly to prevent cascading failures.

2.4.2 RAS Features

RAS schemes are critical for system operators to maintain system operating limits reliably. The features of a RAS typically consist of status monitoring, controller logic and RAS arming/triggers [18].

2.4.2.1 RAS Status Monitoring and Controller Logic

RAS systems are designed to detect changes in topology or specified system conditions. Once the RAS system autonomously detects a status change in power system topology, and conditions meet the pre-determined logical requirements, the RAS scheme is armed to act when required. A simple RAS logic is presented in Figure 2.3 [19].

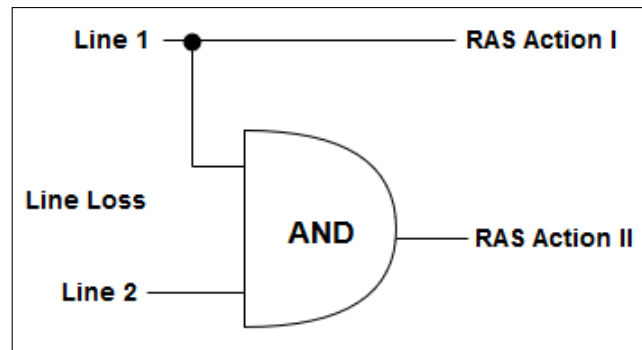


Figure 2.3: Illustration of implementation of simple RAS logic.

In this example, the loss of Line 1 will initiate RAS Action I, and the subsequent loss of Line 2 will result in the initiation of RAS Action II. The loss of Line 2 by itself will not trigger any RAS action for activation.

2.4.2.2 RAS Arming/Triggers

The RAS arming criteria are the critical arming conditions for which the RAS schemes should be prepared for action when required, while the triggering conditions are the critical conditions that initiates action(s) if the scheme is already armed [17].

2.4.3 Possible Actions in RAS

Numerous possible actions are available to improve system performance. These may include, but are not limited to [17]:

- Line tripping, possibly to create islands in extreme cases

- Generator tripping
- Generator runback
- Load tripping
- Inserting braking resistors
- Changing operating points of static VAR control units
- Capacitor and/or reactor switching

The minimum remedial action required is determined through studies that help define the boundary between acceptable and unacceptable system performance. The remedial action, in addition to this minimum level, often can result in further system performance improvements. At some higher action level, the performance standard of the system may again be violated if the system's response approaches another part of the boundary (for instance high voltage due to extra load shedding). However, some extra remediation action (safety margin) should be applied to make sure that at least the minimum action will still occur even for the worst-case credible scheme failure. Although actions above the necessary safety margin do not create new violations, they may make the scheme more expensive and increase its complexity, as well as result in a larger impact to customers (e.g. reduction of generating reserve, shedding more load than necessary) [20].

The maximum time allowable to take action will change with the type of problem for which the RAS is a solution. Short-term angular and voltage stability problems typically require the fastest response, as fast as a few cycles but usually less than one second, far faster than human operator can act. Actions to mitigate steady-state stability and slow voltage collapse problems may allow several seconds [17]. In this study, target events are chosen such that all the required remedial actions are to be triggered exactly one second following the occurrence of the RAS input contingency or event(s).

2.4.4 Examples of RAS Implementation in Literature

As RAS are becoming more widely used, an increasing number of studies have researched implementations of the schemes in the power grid. In [21], California Independent System Operator (CAISO) staff described their implementation experience with RAS. Ten RAS schemes were designed and implemented in the California ISO Energy Management System, and validated thereafter by operations engineers. They reported increments in the allowable power transfer capability after the application of RAS. The authors in [22] performed extensive study to evaluate the impact of including RAS models on transient stability study results. Their study revealed that incorporating RAS models on transient stability analysis provides a more accurate representation of the system response during changes in system operating conditions. In the same vein, implementation of RAS in power flow models for operation studies were reported in [19]. The scheme was reported to have saved time, reduced workload and also minimized error. Popat et al. discussed the need to include Remedial Action Schemes in variable transfer limit computations in [18]. Use of a RAS scheme to improve the power grid security was described in [20]. A dynamic RAS scheme using online transient stability analysis was proposed in [2]. Jenkins and Dolezilek presented a case study where a wide-area, communications-assisted RAS scheme was used to improve transmission system reliability in [23]. In summary, the aforementioned works proposed ways of improving the reliability and performance of the power system by the implementation of remedial action schemes. However, none of these works actually showed how the scheme really impacts the transient stability indices of a power system that has been intentionally divided into islands. That topic will be addressed in the Chapter 3 of this thesis.

2.5 Cyber-Security Issues in Power System

In recent years, situational awareness has become very crucial to the proper operation of the power system with the increased penetration of renewable generation. Hence, more

measurement devices have been added to better estimate the operating state of the power system with higher sampling rates. Increasingly sophisticated Energy Management Systems (EMS) being deployed by utilities to obtain higher resolution real-time estimate of the power system operation state. Despite the advent of Phasor Measurement Units (PMUs), which provide the potential for direct state measurement as well as updating measured data at a very high speed, utilities are still largely using Supervisory Control and Data Acquisition (SCADA) systems for measurement collation and to communicate central control action to substations. SCADA measurements supplemented with PMUs can tremendously improve the observability of the power system. However, the deployment of various communication technology coupled with the bridging between Operation Technology (OT) and Information Technology (IT) has left the power system vulnerable to cyber-attacks.

State estimation is used to infer the operational state of the power system from available measurements [24]. In a data measurement cyber-attack, the attacker aims to inject malicious measurements to mislead the state estimation process [25]. Also, an attacker can exploit the small errors tolerated by the state estimation algorithm to bypass the bad data detection scheme of the state estimation process [24]. If such compromised measurements are fed into the RAS controller, it could make the scheme misoperate, as the RAS system is always designed to operate only when it is required. However, RAS operation when there is no pressing stability issue in the power system can adversely affect the stability and reliability of the interconnected grid. Also, failure of a RAS to operate in a timely manner when genuine events occur can swiftly drive the power system into an extremis state. Hence it is very important to secure the RAS system from data measurement cyber-attack in order to ensure that RAS is armed and triggered by uncompromised data. If this occurs, the risk of cascading failure due to false data injection is drastically reduced and the power system becomes more reliable and secure. The second RAS scheme proposed in this thesis is able to take the correct remedial action even in the presence of false data.

Chapter 3: Implementation of Remedial Action Scheme for Transient Stability Index Improvement of Power System Island

The work in this chapter was published in the proceedings of the 2020 Innovative Smart Grid Technologies conference (ISGT 2020). The citation numbers, equations, table and sections have been updated for inclusion in this thesis and therefore differ from the published form. The original paper is available upon request [26].

3.1 Introduction

Today's utilities are becoming increasingly reliant on the extensive usage of Remedial Action Schemes (RAS) to make the power grids more stable [2]. Economic and environmental issues force modern power systems to operate within tighter margins and with less redundancy. For instance, the transmission network is experiencing increased stress daily since regulatory processes, high capital costs and right-of-way restrictions limit the possibility of new construction to ease the workload on existing infrastructure [2]. Furthermore, the proliferation of distributed renewable energy sources in the power industry has further increased the complications and complexity of operating the grid in a secure manner. The combined effects of these factors have led to an increased concern about the transient stability margins of the power grid.

Transient stability concerns result from major disturbances such as loss of a major generator, line-switching operations, faults, and large sudden load changes. Following a disturbance, synchronous machine frequencies undergo transient deviations from synchronous frequency, and machine power angle changes considerably. The objective of a transient stability study is to determine whether or not the machines will return to synchronous frequency with new steady-state power angles [27]. The time frame required to prevent the system from losing synchronism following a major contingency might only be a few tens of cycles. This highlights the immense importance of transient stability study in most power system due to the extremely short recovery window.

System operators have two transient stability enhancement actions available to them to mitigate instability of the grid after a major contingency happens; preventive control and emergency control [28]. The main purpose of the preventive measure is to modify the operating conditions (e.g. rescheduling generation) of a power system in order to make it capable of withstanding severe contingencies that could drive the grid to instability. This measure is, however, a tradeoff between security and economics. The response to severe contingency, effective preventive control actions might require impractical solutions, such as shifting generation between a number of generators [2]. The emergency control on the other hand is modeled to sense abnormal conditions and take pre-determined remedial actions to prevent the conditions from escalating to very severe disturbance in the power system. Popularly known as either RAS or Special Protection Schemes (SPS), these emergency control approaches have been extensively adopted by various utilities [15] [19] [21].

The security and reliability of the power grid has critical impact on society, hence there is a need to put certain measures in place to mitigate events that could lead to cascading blackouts in the power grid. Whenever a power system is subjected to large disturbances, such as loss of generating units or major transmission lines, and the system is approaching catastrophic failure, control actions need to be taken to limit the extent of the disturbance. Power system islanding is one of such measures that is implemented by utilities to contain severe faults, preventing the effect of the disturbing event from propagating to other areas of the power system. It is however important to ensure that islands are able to function independently until the fault and related effects in the system is cleared. A RAS scheme can be employed to ensure adequate stability of the individual islands.

RAS are designed to sense abnormal, predetermined system conditions and take corrective actions to maintain the power system's reliability and stability [17]. These schemes require numerous simulation studies during the planning phase of the implementation of the schemes. These simulations are conducted to study the behavior of the grid following the occurrence of severe disturbance(s). The outcome of these studies are used as bases for

determining the adequate remedial actions that should be triggered in order to maintain the reliability of the grid for each identified severe contingency. In this thesis, we analyze the impact of the deployment of a remedial action scheme on the transient stability index of the power system island.

3.2 Deployment and Testing of RAS Model

It is important to note that this study is not focused on the intricacies involved in the formation of islands. Instead, we want to demonstrate the impact of remedial action scheme on the transient stability index of power system islands. To achieve this aim, simulations were conducted on the WECC 179-bus test system. The Transient Stability Assessment (TSA) was performed using three packages from the DSATools; PSAT, TSAT and UDM. PSAT (Powerflow and Short-circuit Analysis Tool) is a powerflow program which was used for powerflow analysis in this paper. TSAT (Transient Stability Assessment Tool) [29] is the computation engine that was used to perform the transient stability analysis of the test system. The actual RAS logic and control was modeled using a UDM (User-Defined Model). Once the RAS logic is modeled in UDM, its file is included in the TSAT case (in the Dynamic Data section) to be used in the computations.

As shown in Figure 3.1, the 179-bus test system can be broken into five controlled islands, namely 1-A, 1-B, 1-C, 2-A and 2-B. The actual simulation and studies centered on Island 1-A only. This controlled island was isolated from the system by tripping transmission lines 83-168, 83-170, 83-172 and 81-99. The resulting controlled Island 1-A has 39 buses and 6 generators. The effectiveness of the implemented RAS scheme on the transient stability margin of the controlled island was tested off-line for all enabling and triggering conditions using a pre-defined set of contingencies.

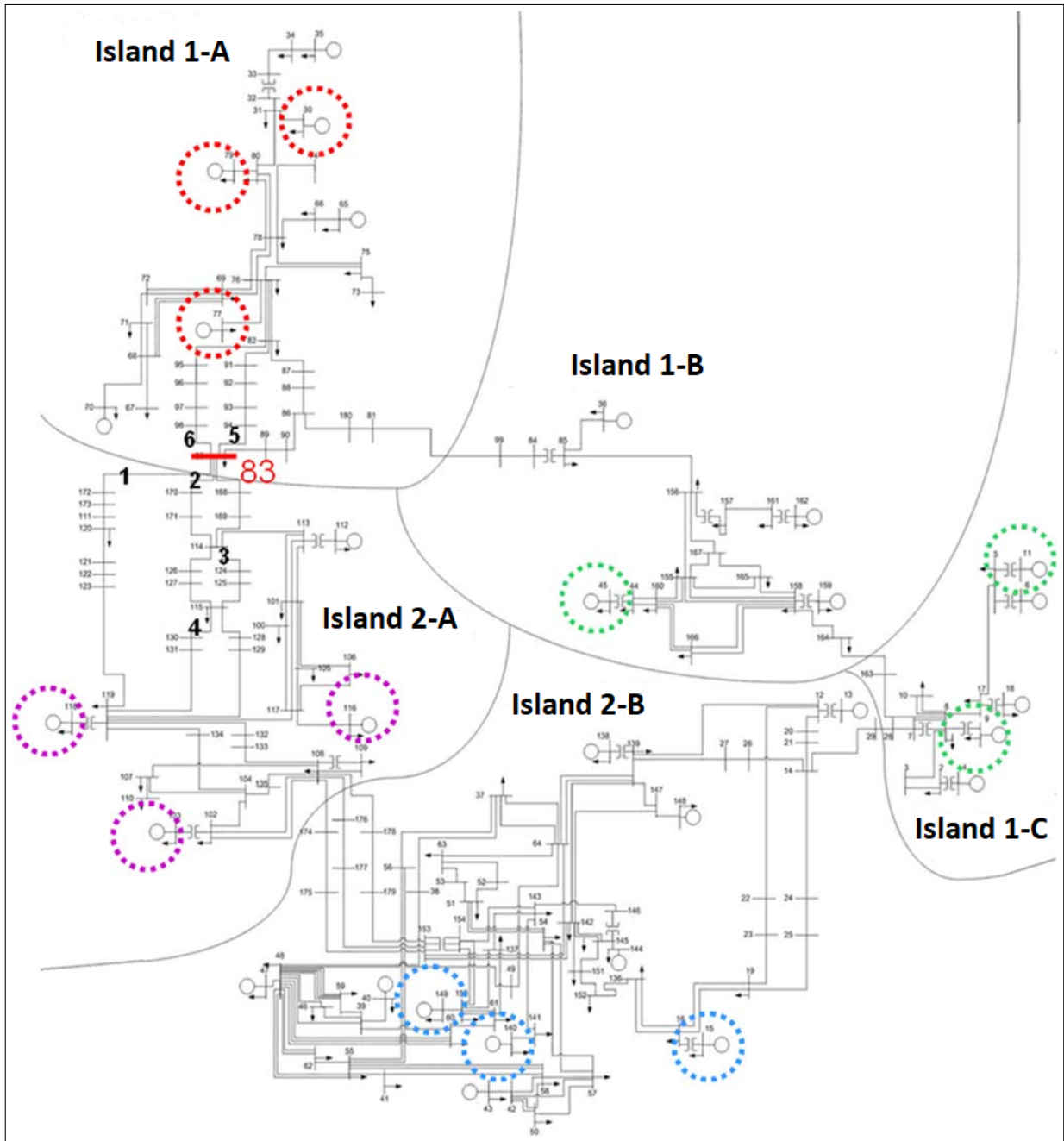


Figure 3.1: WECC 179-bus test system

3.2.1 Transient Stability Index

Time domain simulation is able to accurately determine the trajectory of a system following a severe disturbance. Utilizing TSAT, two methods are available to assess the severity of a contingency, each of which gives a transient stability index [29]; Power Swing-

based Stability Margin or Index (SM) and Power Angle-based Stability Margin or Index (AM).

In the Power Angle-based Stability Index adopted in this paper, the transient stability index is defined for each island in the system as shown in equation (3-1):

$$\eta = \frac{360 - \delta_m}{360 + \delta_m} \times 100 \quad (3.1)$$

Where δ_m is the maximum angle separation of any two generators in the island in degrees at the same instant in time in the post-fault response. Depending on the severity of a disturbing event and the operating condition of a power system, the power swing that results from the fault can cause δ_m to be greater than 360 degrees, thereby resulting into a negative η value. Thus, if $\eta > 0$ the power system is said to be in a stable condition. However if $\eta \leq 0$ the power system is in an unstable condition.

3.2.2 Events and Actions

The events or contingencies that can result in action by the implemented RAS scheme are the loss of one or two critical components from the service. These events could result in power system instability and overloading of neighboring transmission lines. The control actions the RAS can take are the following:

- Trip generator unit
- Load shedding

Anderson and LeReverend conducted a world-wide survey on industry experience with special protection schemes in 1996 [15]. Out of a total of 111 schemes reported by 49 utilities from 17 different countries, generation tripping was the most utilized RAS action implemented, accounting for about 21.6% of the available RAS action options. Load shedding was reported to be the second most implemented RAS action (10.8% of the most common

RAS action scheme). This prompted the decision to use these two broadly used RAS action in our study.

In this study, contingency analysis was conducted in TSAT to identify the events that can result in the overloading of the neighboring transmission lines and cause transient instability of the controlled island under consideration. An outage on any of these identified critical components triggers the RAS scheme action as shown in Figure 3.2.

3.2.3 RAS User-defined Model

This scheme is designed to be armed by the formation of the island, so it was already enabled for these studies. The triggering conditions for this implementation are shown in the UDM model in Figure 3.2.

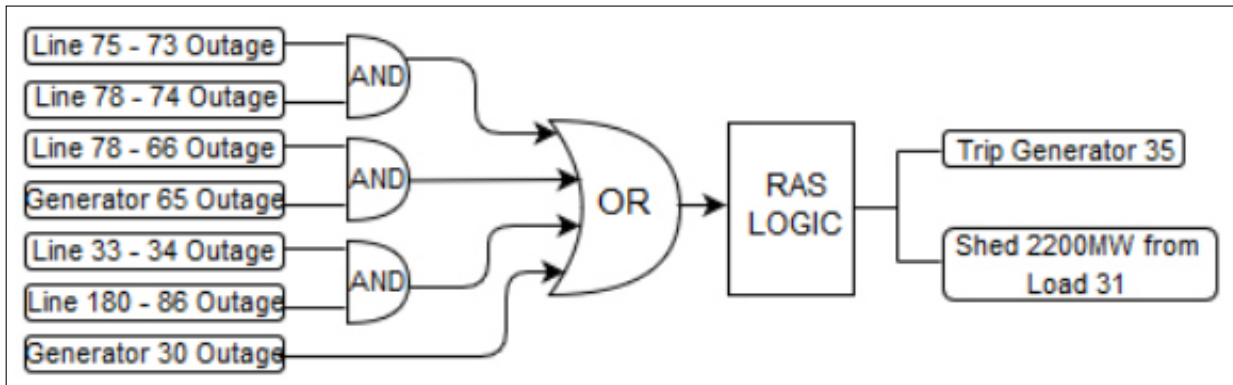


Figure 3.2: Logic Diagram of the Implemented RAS.

For this RAS scheme, all the actions should take place instantaneously, which is within the transient stability analysis time frame. Figure 3.2 highlights the required input signals and the pre-defined remedial actions. After designing the logic diagram, the scheme was built using the UDM Editor graphical interface. The UDM file is then included in the dynamic data section of the TSAT model.

Following the extensive contingency analysis studies, the generator at bus 35 was identified as the one whose rotor angle deviated the most following the occurrence of the pre-defined disturbances. For this reason, this generator was selected to be tripped as a remediation ac-

tion. Also, 2200 MW of the load at bus 31 is simultaneously shed to maintain stability of the controlled island.

3.2.4 Simulation Results

To test the functionality of the RAS scheme, contingencies were simulated on the identified critical components listed in Figure 3.2, first without including the RAS file in the simulation. Three phase faults that lasted for 1 second were introduced on transmission lines 75-73 and 78-74, to simulate a N - 2 contingency. It was assumed that the faults lasted that long due to a combined cyber-physical attack that prevented the protection devices from tripping within their normal response time of few cycles. We observed that the transient stability index of the controlled island gave a negative value; -5%. Consequently, the generators in the island experienced out of step conditions as they lost synchronism due to the instability. As shown in Figure 3.3, the bus voltages fell well below the set threshold of 0.9 per unit (pu). It is clear that the island is unstable and is on the verge of collapse if adequate remedial actions are not taken for these long lasting 3-phase faults.

To demonstrate how RAS scheme improves the transient stability index of the power system island, we applied the RAS logic discussed in Subsection 3.2.3. This was achieved by including the UDM RAS model's file in the TSAT case file of the contingencies under consideration. The scheme was set up to be triggered at exactly one second following the occurrence of the event.

There was a significant improvement in the transient stability index of the power system when the RAS scheme was deployed. The calculated transient stability margin was 60%, against the -5% that was observed prior to the deployment of the RAS scheme.

As can be observed in Figure 3.4, RAS deployment ensured that the bus voltage threshold was not violated despite the presence of the severe disturbances in the controlled island. To confirm the effectiveness of RAS in improving the transient stability index of the controlled island, we considered three more cases in which 3-phase faults were introduced on different

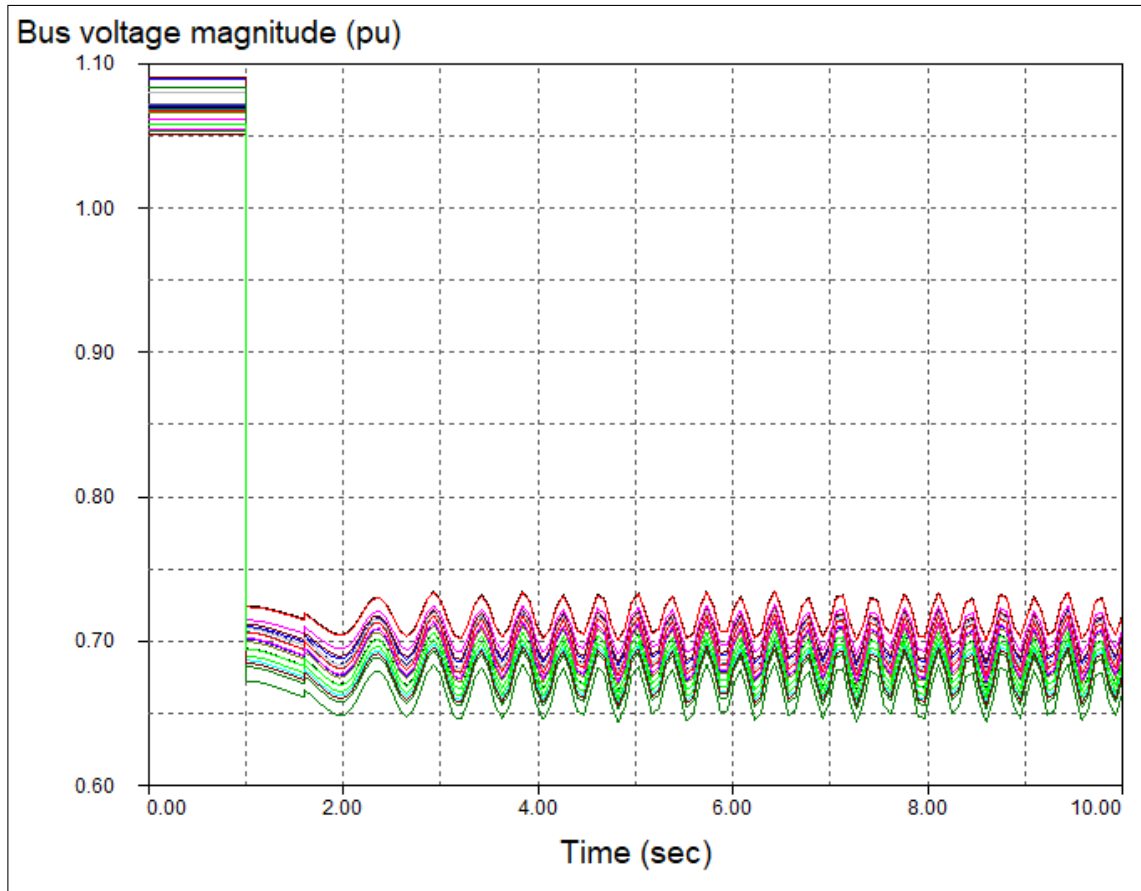


Figure 3.3: Bus Voltage Magnitudes for Case 1 without RAS.

critical components of the island. As shown in Table 3.1, RAS deployment was able to enhance the resilience of the island by improving its transient stability index.

Table 3.1: Result of Transient Stability Index Improvement Under Different Cases

Transient Stability Index Improvement by RAS Deployment			
Cases	Contingencies	Without RAS	With RAS
Case 1	Line 75-73 and Line 78-74	-5%	60%
Case 2	Line 78-66 and Gen 65	-91%	82%
Case 3	Line 33-34 and Line 180-86	-93%	81%
Case 4	Generator 30	-51%	79%

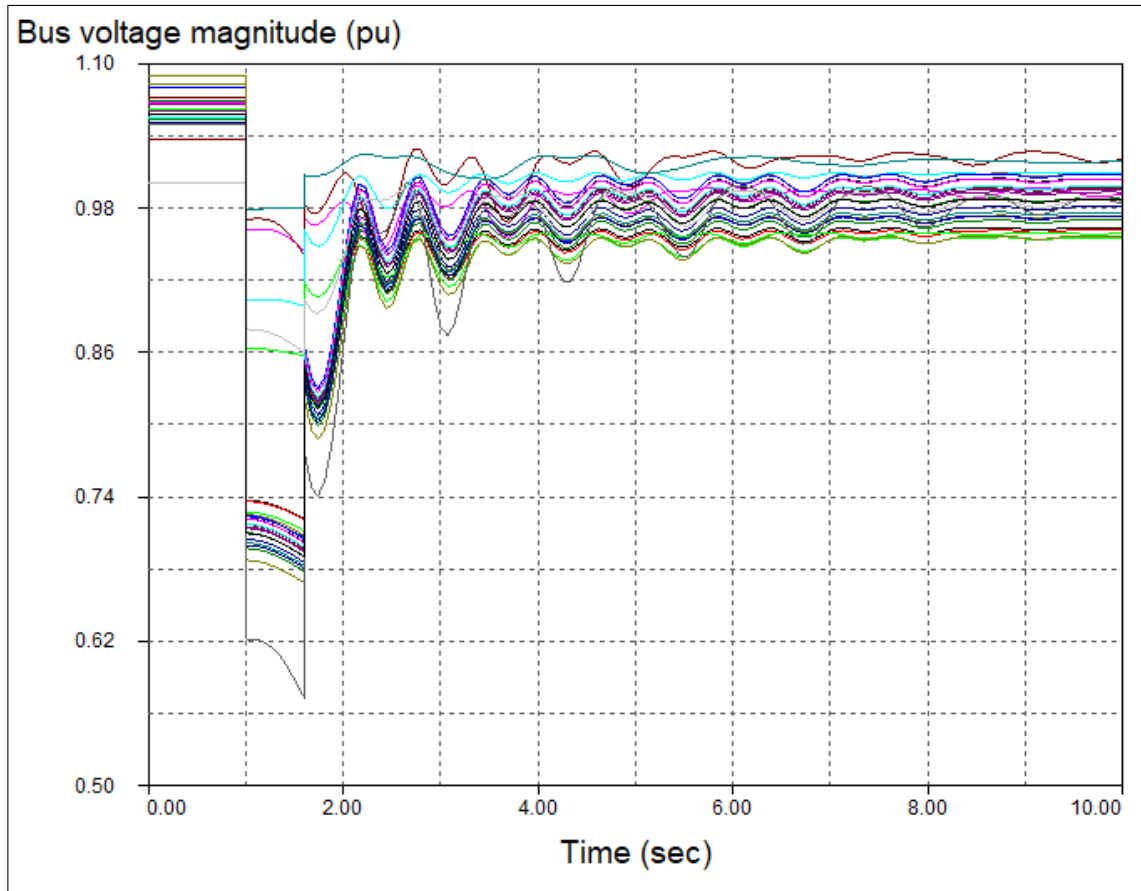


Figure 3.4: Bus Voltage Magnitudes for Case 1 with RAS.

3.3 Benefit of RAS Deployment in Power Grid Island

Based on the results presented in Section 3.2.4, it is clear that the implementation of RAS in power system controlled island makes the grid more robust and resilient as the island is able to operate independently in a stable condition following a severe disturbance in the grid.

3.4 Concluding Remarks

Severe disturbances in a power system can result in the formation of undesirable islanding. On the other hand, controlled islanding is one of the measures taken to avert wide-spread impact of faults in the power system network. Therefore it is important to put certain

measures in place to ensure the sustainability of the individual islands so that they can function independently. Generation-load balance must be sustained in the islands to ascertain its stability. In this study, we have demonstrated how the deployment of RAS scheme can improve the transient stability index of the island thereby making it more resilient. With RAS scheme implementation, there is no need for operator intervention as the scheme is automatically triggered once the predetermined contingencies occur. Hence, the scheme is able to operate faster to maintain the stability of the power system island.

Chapter 4: Implementation and Deployment of Attack-Resilient Remedial Action Schemes

In this chapter, a hybrid RAS scheme (comprises of both event-based and parameter-based schemes) which is attack-resilient is proposed. The scheme is designed to be robust enough to take the correct remedial action(s) in the face of measurement cyber-attack. Impact analysis of data measurement cyber-attack on the operations of RAS scheme will be assessed before the deployment and validation of the attack-resilient RAS scheme. The scheme is tested and validated on the same controlled island introduced in Chapter 3. Simulation results are presented to demonstrate the effectiveness of the proposed scheme.

4.1 Background and Problem Description

Cyber-attacks have become a serious concern worldwide in the energy sector. As reported by the Department of Homeland Security, about 40% of the total critical infrastructure cyber incidents occurred in the energy sector between 2009 and 2014 [30]. One of the first highly publicized large-scale cyber-attacks on power system occurred in Ukraine in December 23, 2015 leaving well over 80,000 customers without power supply for several hours. It took Ukraine utilities months to recover from this attack [31]. The cyber vulnerability of the power system has been on the increase due to a number of modernizations taking place in substation operations [32]. The ability of cyber-attacks to cause physical damage on the power system as demonstrated in [33] has further raised the concern of power system operators on the impact of such attacks on the security and reliability of the power system.

Wide-area monitoring, protection and control (WAMPAC) uses system-wide information and sends selected data to specific remote locations. Real-time synchrophasor measurements for voltage and current phasors of the power system are provided by phasor measurement units which are time synchronized by the global position system (GPS). These real-time measurements provide real-time visibility of the power system dynamics, thereby complementing the traditional SCADA measurements [34]. The use of PMUs of-

fers significant advantages over SCADA as it provides, fast, precise and time-synchronized measurements from which the voltage and current phasors can be obtained directly. These measurements are typically reported at a high rate up to 60 times per second [35]. Due to the availability of these PMU measurements, they are being considered in various applications which includes automatic generation control (AGC), state estimation, contingency analysis, economic dispatch, remedial action scheme (RAS), and many other applications [36]. The RAS scheme as focused on in this thesis uses a number of remedial actions to ensure the stability of the power system. Among some of the common actions include generation tripping, load shedding, under frequency load shedding, VAR compensation, etc.

Due to the complexity and inter-connectivity of the power system, most of the applications listed above use communication systems to interact with each other. This adds more vulnerability to the power system to cyber-attacks [34]. Some of the cyber-attacks that can compromise the wide-area operations of the power system include man-in-the-middle attacks, denial of service attacks, malware infections, eavesdropping, intrusions and false data injection attacks [37] [38]. Hence, it is important to implement and deploy RAS schemes that are able to withstand malicious endeavors such as cyber-attacks on complex and interconnected cyber-physical systems such as the power system.

4.2 Cyber Vulnerabilities of WAMPAC

When the initial WAMPAC schemes were proposed over two decades ago, cyber-security was not a major concern at the time. When the digital WAMPAC solutions based on Information and Communication Technology (ICT) started to evolve, vendors and stakeholders only focused on maximizing the numerous potentials of the new technology to improve the availability and reliability of these functions, without really considering the potential cyber vulnerabilities they pose to the power system. Hence, most of the legacy WAMPAC functions in today's power industry lack the required security mechanism, making them vulnerable to cyber-attacks.

4.2.1 Public Network Connectivity

Physical segregation of the Information Technology (IT) and Operational Technology (OT) is often costly and inconvenient to implement [39]. To offset this cost implication, it is not uncommon for utilities to leverage publicly available network (internet) to achieve the required data/measurement transmissions involved in WAMPAC [39]. The overlap between the OT and IT networks can be exploited by an attacker to gain access to some critical OT functions. Once adversaries are able to gain access to the OT network, they are able to access sensitive data, alter measurements or control algorithms, and even manipulate the settings of actuators (as was the case in the first Ukraine attack).

4.2.2 Communication Protocols

Most of the protocols used for communication both within the modern substation and between substations like Modbus, IEC 61850 and DNP3 do not have sufficient inherent security measures. The lack of adequate data encryption and authentication make these protocols susceptible to cyber-attacks in which the attacker could alter, intercept or spoof data in transmission. The adversary could also exploit this vulnerabilities to launch data integrity attack purposely to cause protective devices or systems to malfunction by sending false data/measurement to control systems such as RAS.

4.2.3 Supply Chain

The vulnerabilities embedded in supply chain is another factor that could present an adversary the opportunity to carry out cyber-attacks on the power system. As observed by Federal Energy Regulatory Commission (FERC), cyber supply chain risk may stem from the insertion of counterfeits, unauthorized production, tampering, insertion of malicious software and hardware, and poor manufacturing and developmental processes [40]. It is possible for even the well designed products to have malicious components introduced in the supply

chain, and this might be very difficult to identify before deployment [41].

4.2.4 Human Factors

The issue of human factors can not be over-emphasized when considering cyber vulnerability of the WAMPAC. Often time, human employees turns out to be the most vulnerable link in the cyber-security chain of the power system [42]. Disgruntled employees might directly or indirectly cause great damage since they may possess the privilege to access critical settings, data or measurement in the WAMPAC system.

4.3 Cyber-Security Concerns in RAS System

As described in Section 4.2, there are a number of factors that have rendered WAMPAC applications in power system vulnerable to cyber-attacks. RAS schemes are one of the most widely used protection methods in WAMPAC applications and are also affected by these vulnerabilities. The heavy reliance of RAS schemes on communication exposes them to potential devastating cyber-attacks.

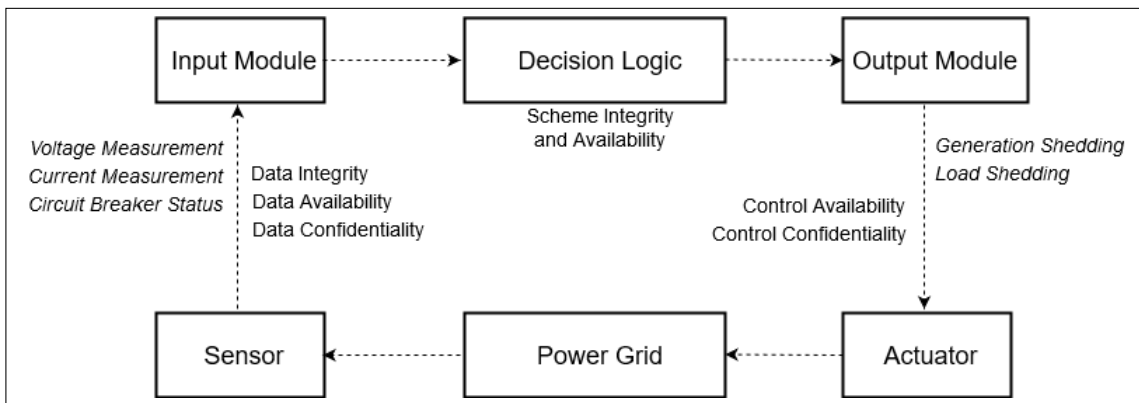


Figure 4.1: Potential Cyber-Security Concerns in RAS Systems

Figure 4.1 illustrates the communication channels and steps in the process that can potentially be exploited by an adversary to attack the RAS system. Various sensors are deployed in substations to take raw data like voltage and current measurements together

with the open/close status of circuit breakers. The input module shown in the figure converts those raw data into the format required by the RAS logic controller. The communication channel between the sensors and the input module could create an avenue for a man-in-the-middle attack. This could impact the integrity, availability and confidentiality of the data if an attacker is able to compromise the communication link. In a more severe scenario, an adversary with enough expertise and sufficient information about the topology of both the OT network and external IT network of a power system can also hack into the RAS logic controller. Once the controller is compromised, the attacker can either trigger a denial of service attack or change the pre-configured logic in the controller in such a way that the RAS system takes action that would lead to cascading failure in the power system. The communication link between the output module of the RAS system and the actuators in the substations is another avenue through which an adversary can attack the RAS scheme. Control command availability and confidentiality can be compromised in event of a man-in-the-middle attack. The attacker can either cause a denial of service or alter the commands issued by the output module of the RAS scheme.

4.4 False Data Injection Attack Surface of the RAS Scheme

The sensors, controllers, actuators and the measurements are the obvious targets of cyber-attacks on a power system. As illustrated in Section 4.3, once a power system component is compromised, the attacker can inject false data with the aim of triggering the RAS controller to take a wrong action. The adversary can also cause denial of service in which the data and measurements needed by the RAS controller to function will be unavailable when required.

The false data injection attack surface and the flow chart of a typical RAS system are shown in Figure 4.2. As illustrated in the figure, the communication channels, RAS logic controller, wide area network (internet), sensors and the actuators are all attack surfaces that the adversary can exploit. The reason false data injection attacks are of particular concern in RAS systems is that the misoperation of a scheme is capable of having far-reaching impacts

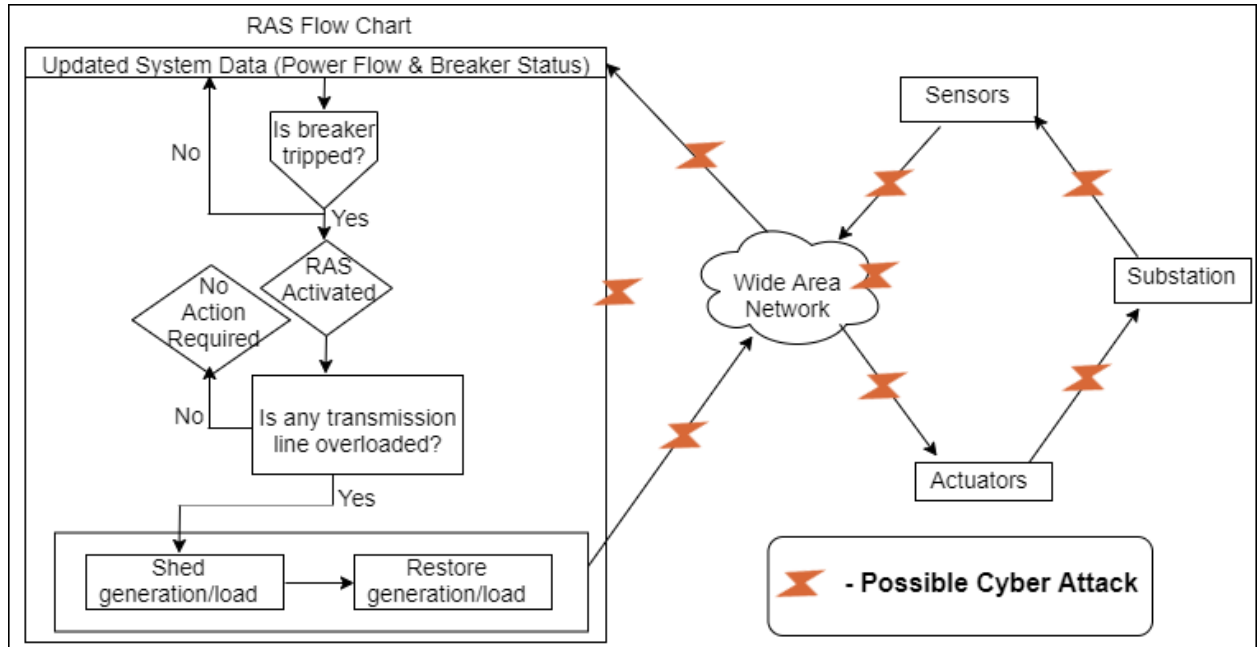


Figure 4.2: RAS False Data Attack Surface.

on the stability of the power system. For instance, an attacker can inject false data into the updates communicated to the RAS controller purposely to cause the failure of the RAS system to operate when it should (i.e. false negative). On the other hand, the attack can also be devised in such a way that it prompts an action from the RAS scheme when such actions are not required (i.e. false positive). The action or inaction of the RAS system due to the injection of false data can potentially result in cascading failure in the power system.

A sample of a typical RAS flow chart is shown on the left in Figure 4.2. The logic operation starts as soon as the RAS controller receives system data update from the power system. In this instance, the controller checks the status of the breaker to start with. If the update received indicates that the breaker is not tripped, no action is taken by the controller. But if the breaker is tripped, the RAS controller is immediately armed (activated). The logic then checks the state of loading on each transmission lines being monitored. No action will be taken if the preset load limit of any of the lines is not exceeded. However, the scheme is triggered into action once any of the transmission lines exceed its limit. The required amount of load and/or generation determined during pre-fault powerflow studies and contingency

analysis are shed accordingly to restore generation-load balance in the power system.

4.5 Proposed RAS Scheme

The example of RAS logic explained in Section 4.4 is vulnerable to false data cyber-attack in which the scheme can be tricked into believing there is a change in the status of the breakers in the substation. An adversary with sufficient information about the topology of the power grid can send a false status update to the RAS controller to achieve this. As illustrated in the RAS flow chart in Figure 4.2, the RAS controller is activated once the status of the breaker changes to "tripped". If the falsified update sent by the adversary indicates that the breaker has been tripped and the RAS controllers triggers the preset remedial actions, the power system can experience cascading failure depending on the severity of the action taken or the prevailing operating condition of the power system. However, for the attacker to achieve this aim, they must also be able to send false data regarding the loading conditions of the neighboring transmission lines as well. For the scenarios under consideration in this study, the adversary is assumed to have enough knowledge about the topology of the grid and has the ability to send falsified data regarding the loading conditions of the transmission lines. On the other hand, the adversary can also devise the attack in such a way that it creates a false negative condition, in which the RAS scheme would fail to operate when there is genuine event on one of the critical transmission lines in the power system. The latter is the primary aim of the attack considered in this study. The attacker is able to achieve this by sending an update which indicates that the breakers are not tripped when there is an actual outage on one or more critical components of the power grid.

In order to make the RAS logic described false data-resilient, the conditions that must be fulfilled to trigger any action from RAS scheme must be made a little bit more complicated. The dynamics and response of the neighboring transmission lines following an outage event(s) on a critical power grid component are used to verify the validity of

the breaker status update communicated to the RAS controller. To achieve this, several simulations were carried out using a number of severe contingencies. For each contingency analysis case conducted, the data obtained from the power flow of the grid were recorded and analyzed to devise a more robust control logic for the RAS controller. The RAS system will only operate when the conditions of the neighboring transmission lines are in conformity with values in a range obtained from the pre-fault contingency analysis conducted.

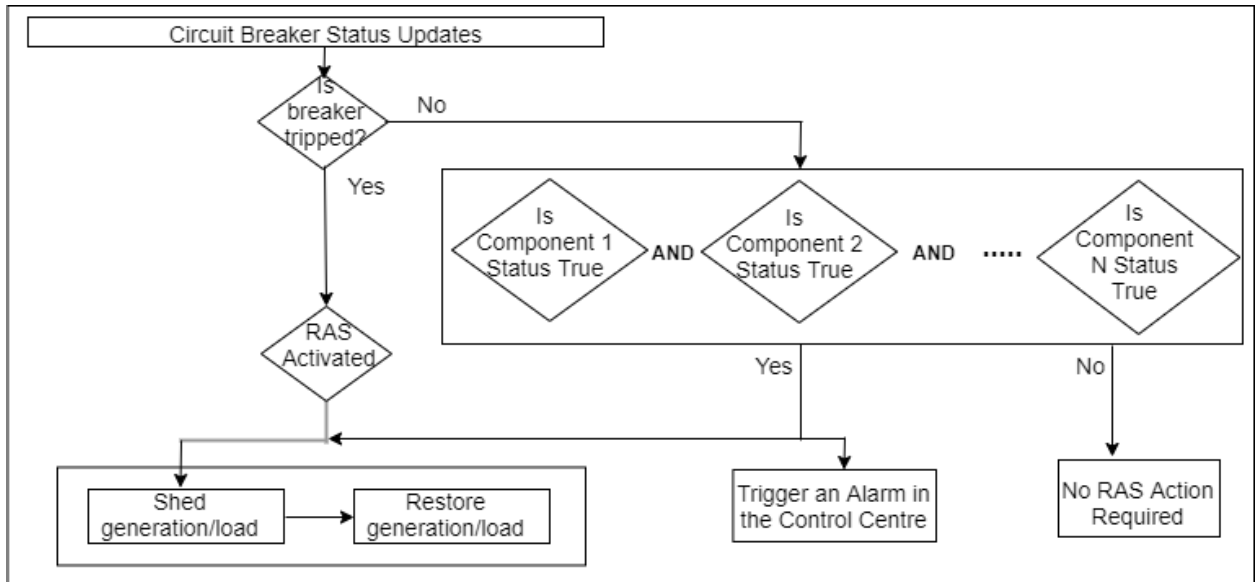


Figure 4.3: Proposed RAS Logic Flow Chart.

The flow chart of the proposed RAS logic is shown in Figure 4.3. The scheme is designed to mitigate the ability of an adversary to mask a genuine disturbing event, creating a false negative condition which would normally prevent the scheme from triggering when it actually should. This is achieved by verifying the status update communicated to the RAS controller using physics-based data to ascertain that there is no outage on any of the monitored critical transmission lines. As illustrated in the figure, the RAS controller is no longer triggered by the status of the breaker only (i.e. event-based scheme), but also by the dynamics of the transmission lines close to the fault location (i.e. parameter-based). Hence, the proposed scheme uses hybrid RAS logic since it incorporates both event-based and parameter-based schemes. The scheme operates normally if a "tripped" status

update is received by shedding the preset quantity of generation and/or load. On the other hand, if the update received indicates that the breaker is not tripped, the scheme verifies this update by checking the conditions of the neighboring transmission lines (verification parameters). If the physical conditions of all the neighboring components correspond to the results obtained during the pre-fault contingency analysis conducted for the particular event under consideration, then there is an actual outage. The scheme triggers the preset remedial action and also triggers an alarm in the control center to alert operators about potential measurement cyber-attack on the power system. However, if at least one of the verification parameter status inputs is false, this signifies that there really is no outage on the monitored transmission lines and no RAS action is required. This modification makes it difficult for the adversary to conduct a successful false data attack since more measurements will have to be compromised to trick the RAS scheme into misoperation. This scheme however requires extensive contingency analysis to gather the required data for the RAS logic and it is more efficient for smaller systems.

4.5.1 Deployment and Testing of the Proposed Robust RAS Logic

The simulations were conducted on the same power system island described in Chapter 3. The proposed RAS scheme was tested and validated using two of the four critical events identified in the previous chapter. UDM package of the DSATools was again used for the RAS modelling and it was deployed in the TSAT package. False status updates were mimicked in the model by tweaking the scaling factor of the input received by the RAS controller.

4.5.1.1 Case 1

In the first case considered, the aim of the adversary is to mask a N - 2 event (outages on line 75 - 73 and line 78 - 74) in the power system. If the RAS scheme is not triggered in a timely manner, this event can potentially lead to cascading failure in the grid. As shown in Figure 4.4, the active power of the generator in Bus 77 was scaled down to mimick a false

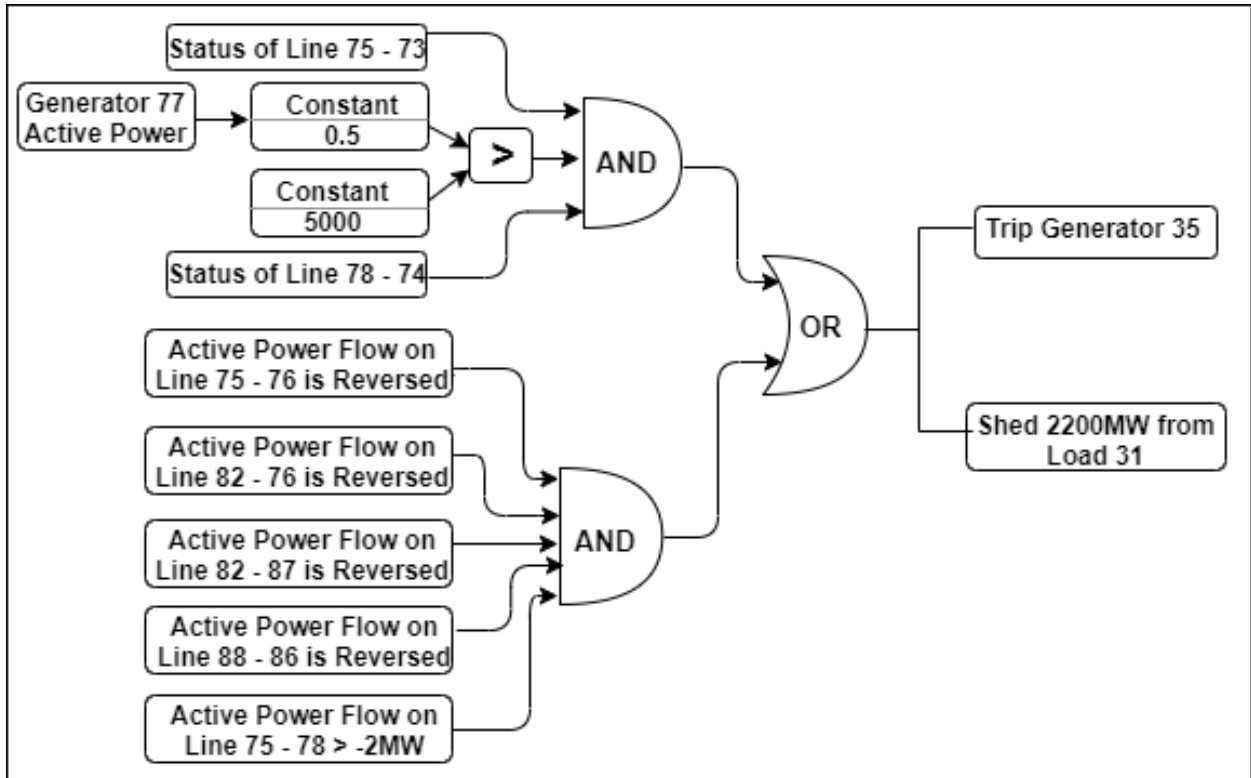


Figure 4.4: Logic Diagram of the Proposed RAS Scheme Modelled in UDM for Case 1.

data input. Five parameters (verification parameters) are also included in the input of the RAS scheme to verify the genuity of the status update communicated to the RAS controller. These verification parameters are consistent with the $N - 2$ event under consideration. Even if the attacker succeeds in communicating false data masking the $N - 2$ event to prevent the scheme from operating, the scheme would still identify the condition by checking the logic result of the five verification inputs. Increasing the required RAS input this way decreases the chances of false negative condition an attacker can induce through the introduction of false data to mask a genuine attack. And it should be noted that the verification parameters are data coming from different substations, so the adversary will have to gain unauthorized access into all the substations in order to succeed in injecting false data that would cause the RAS scheme to mis-operate. There is still vulnerability if an attacker has penetrated the system deeply, but such an attacker would also be capable of causing more severe problems on the system beyond the RAS scheme.

To confirm that the false negative condition created by the false data would cause the RAS controller to misoperate, the model was first designed without the verification inputs (similar to the RAS model described in Chapter 3). When the simulation was carried out, the RAS scheme failed to trigger despite the occurrence of genuine outages on the monitored transmission lines as shown in Figure 4.5. As can be observed in the highlighted portion of the figure, the RAS scheme was not triggered and the powerflow analysis continued following the occurrence of the fault. This is due to the presence of false data in the input communicated to the RAS controller. The power system becomes unstable as illustrated in the simulation results discussed in Chapter 3.

```

SWITCHING ACTION : AT TIME      1.000 SECONDS - ADMITTANCE ADDED
  BUS :          75 GARRISON      500.
  AMOUNT : G =    0.00000 B = -1998.16003 P.U.
SWITCHING ACTION : AT TIME      1.000 SECONDS - ADMITTANCE ADDED
  BUS :          73 COLSTRP       500.
  AMOUNT : G =    8.92294 B =  -68.19757 P.U.
SWITCHING ACTION : AT TIME      1.000 SECONDS - LINE REMOVED
  FROM BUS :     73 COLSTRP       500.
  TO BUS :       75 GARRISON      500.
  CKT : 1
SWITCHING ACTION : AT TIME      1.000 SECONDS - ADMITTANCE ADDED
  BUS :          78 HANFORD       500.
  AMOUNT : G =    0.00000 B = -1999.07239 P.U.
SWITCHING ACTION : AT TIME      1.000 SECONDS - ADMITTANCE ADDED
  BUS :          74 COULEE        500.
  AMOUNT : G =    2.63187 B =  -47.26116 P.U.
SWITCHING ACTION : AT TIME      1.000 SECONDS - LINE REMOVED
  FROM BUS :     78 HANFORD       500.
  TO BUS :       74 COULEE        500.
  CKT : 1
1.050      36 BRIDGER2      22.0   1   0.50
1.100      36 BRIDGER2      22.0   1   1.01
1.150      79 NORTH G3     20.0   1   1.47
1.200      79 NORTH G3     20.0   1   1.93

```

Figure 4.5: Simulation Result Showing Faulted Lines Removed but RAS Refused to Trigger Due to False Data Injection in Case 1

As discussed earlier, the RAS scheme can be made more robust to reduce the chances of false negative condition due to false data by including verification parameters in the input module of the RAS controller as shown in Figure 4.4. The verification parameters were ob-

```

##### SCENARIO    1 - Attack-Resilient RAS Scheme #####

SYSTEM DESCRIPTIONS AND TITLES
=====

POWERFLOW FILE NAME
-----
C:\Users\COMPUTER\Desktop\RAS Simulations\179.pfb

DYNAMIC DATA FILE NAMES
-----
C:\Users\COMPUTER\Desktop\RAS Simulations\wecc179.dyr
C:\Users\COMPUTER\Desktop\RAS Simulations\RAS2.dat

STUDY TITLES
-----
Attack-Resilient RAS Scheme

```

Figure 4.6: RAS Model Loaded into the Case File

tained by performing intensive contingency analysis studies. These verification parameters (which represent the dynamics and response of the system to the fault) are only consistent with the N - 2 event under consideration. Following the introduction of faults on the transmission lines under consideration (Lines 75 - 73 and 78 - 74) and subsequent tripping, it was observed that the active power flow on some of the neighboring transmission lines reversed. The active power flow on the transmission line 75 - 78 increased as well resulting in an overload condition. All these parameters were selected to serve as the verification parameters for the RAS scheme. The occurrence of all of these conditions at the same time is peculiar to the disturbing event under consideration.

The RAS scheme will only be triggered when all the parameters specified in Figure 4.4 are true. Hence, even if the circuit breaker status update communicated to the RAS controller has been compromised, the verification parameters ensure that the RAS scheme takes the appropriate corrective action in a timely manner. The logic shown in Figure 4.4 was designed and loaded into the test case as shown in Figure 4.6. The result of this simulation


```

SWITCHING ACTION : AT TIME      1.000 SECONDS - ADMITTANCE ADDED
  BUS :      75 GARRISON      500.
  AMOUNT : G =      0.00000 B = -1998.16003 P.U.
SWITCHING ACTION : AT TIME      1.000 SECONDS - ADMITTANCE ADDED
  BUS :      73 COLSTRP      500.
  AMOUNT : G =      8.92294 B =  -68.19757 P.U.
SWITCHING ACTION : AT TIME      1.000 SECONDS - LINE REMOVED
  FROM BUS :      73 COLSTRP      500.
  TO BUS :      75 GARRISON      500.
  CKT : 1
SWITCHING ACTION : AT TIME      1.000 SECONDS - ADMITTANCE ADDED
  BUS :      78 HANFORD      500.
  AMOUNT : G =      0.00000 B = -1999.07239 P.U.
SWITCHING ACTION : AT TIME      1.000 SECONDS - ADMITTANCE ADDED
  BUS :      74 COULEE      500.
  AMOUNT : G =      2.63187 B =  -47.26116 P.U.
SWITCHING ACTION : AT TIME      1.000 SECONDS - LINE REMOVED
  FROM BUS :      78 HANFORD      500.
  TO BUS :      74 COULEE      500.
  CKT : 1
SWITCHING ACTION : AT TIME      1.000 SECONDS - LOAD SHED
  BUS :      31 CANADA      500.
  SHUNT% =      0.00000 PLOAD% =  50.00000 QLOAD% =  50.00000
  LOAD SHED :  2200.000 MW      500.000 MVAR      SPS LOAD SHEDING
SWITCHING ACTION : AT TIME      1.000 SECONDS - GENERATOR DISCONNECTED
  GENERATOR :      35 CMAIN GM      20.0 ID : 1
  EQ. NAME:
  1.050      36 BRIDGER2      22.0      1      0.50
  1.100      36 BRIDGER2      22.0      1      1.01
  1.150      79 NORTH G3      20.0      1      1.50
  1.200      79 NORTH G3      20.0      1      1.97

```

Figure 4.7: Simulation Result: RAS Correctly Triggered When the Proposed Scheme was Implemented for Case 1

SPS ACTION REPORT									
BUS 1	BUS 2	ID	SID	MODEL	BLOCK	ACTION	STATUS	TIME (S)	DESCRIPTION
		1		SPSUDM	BLK1	trip_generator	TRIPPED	1.000	RAS
		1		SPSUDM	BLK4	trip_load	TRIPPED	1.000	RAS
SYSTEM LOAD SUMMARY TABLE AT THE END OF SIMULATION RUN									
TOTAL LOAD		TOTAL LOAD SHED		REMAINING LOAD					
MW	MX	MW	MX	MW	MX				
60785.41	15351.25	675.00	450.00	60110.41	14901.25				
SYSTEM GENERATION SUMMARY TABLE AT THE END OF SIMULATION RUN									
TOTAL GENERATION		TOTAL GENERATION SHED							
MW	MX	MW	MX						
61411.45	12333.65	4480.00	1150.38						

Figure 4.8: RAS Summary for Case 1

is illustrated in Figure 4.7 (the highlighted portion of the figure) where the RAS controller was able to trigger the pre-defined remedial actions (shedding of half of the load on Bus 31

and the generator on Bus 35 was tripped, which are highlighted) even in the presence of compromised status update. For the attacker to conduct a false data attack that leads to false negative condition in the power system, they must have full knowledge of all of the preset verification parameters and must also be able to inject false data to compromise all of the parameters. It is obvious that the addition of these verification parameters to the input module of the RAS scheme has made the scheme more robust and attack-resilient. A summary of the remedial actions triggered by the RAS controller is highlighted in Figure 4.8.

4.5.1.2 Case 2

Another N - 2 event was conducted for a second case, to confirm the effectiveness of the proposed RAS control logic. For this case, faults were introduced into transmission lines 33 - 34 and 180 - 86. As discussed in Chapter 3, if this event is allowed to linger in the power system, it could lead to cascading failure. Hence the RAS logic is designed to react in a timely manner to mitigate system failure. In this case, the aim of the adversary is to create a false negative condition in the power system by communicating false data to the RAS controller. The proposed RAS scheme design shown in Figure 4.9 is meant to mitigate this vulnerability.

The case study was first conducted by using the typical event-based RAS scheme as described in Chapter 3 without including the verification parameters. The adversary is able to compromise the measurements of the monitored transmission lines communicated to the RAS controller. As illustrated in Figure 4.10, it was observed that the RAS scheme refused to trigger despite the occurrence of disturbing events that requires instant remediation action. The power system becomes unstable as a result of this RAS mis-operation.

The proposed scheme that utilizes both event-based and parameter-based RAS logic was designed as shown in Figure 4.9, and subsequently loaded into the test case. The parameters used in the scheme were obtained based on results from contingency analysis.

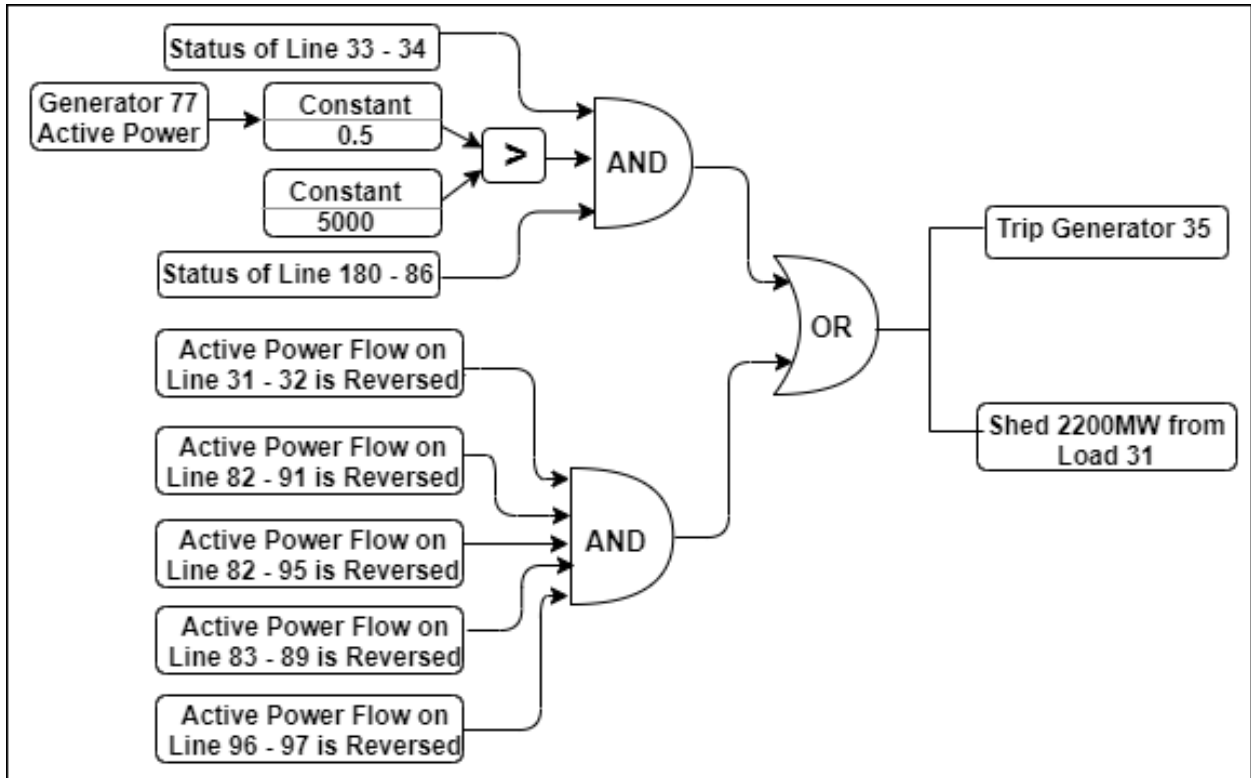


Figure 4.9: Logic Diagram of the Proposed RAS Scheme Modelled in UDM for Case 2

These parameters are consistent with the N - 2 event under consideration. Hence, even if the breaker status update is compromised by an adversary to create a false negative condition, this robust scheme will still trigger the correct actions as long as the stipulated verification parameters are consistent with the pre-fault contingency analysis results. As shown in Figure 4.11, the RAS controller was activated despite the false data update communicated to the scheme.

4.5.2 Concluding Remarks

Proper operation of the RAS scheme is key to the stability of the power grid, because its mis-operation can have a far reaching negative impact. The RAS scheme relies on the measurement input it receives from the substation to perform appropriately. If an adversary is able to successfully inject false data into the measurements supplied to the RAS controller, the scheme will most likely fail to operate correctly. The RAS scheme modelled in this chapter

```

SWITCHING ACTION : AT TIME      1.000 SECONDS - ADMITTANCE ADDED
  BUS :          33 CA230TO      230.
  AMOUNT : G =      0.00000 B = -1999.59998 P.U.
SWITCHING ACTION : AT TIME      1.000 SECONDS - ADMITTANCE ADDED
  BUS :          34 CA230       230.
  AMOUNT : G =      4.95050 B =   -49.10495 P.U.
SWITCHING ACTION : AT TIME      1.000 SECONDS - LINE REMOVED
  FROM BUS :      34 CA230       230.
  TO BUS :        33 CA230TO     230.
  CKT : 1
SWITCHING ACTION : AT TIME      1.000 SECONDS - ADMITTANCE ADDED
  BUS :          180 BURNS2      500.
  AMOUNT : G =      0.00000 B = -1998.89648 P.U.
SWITCHING ACTION : AT TIME      1.000 SECONDS - ADMITTANCE ADDED
  BUS :          86 SUMMER L     500.
  AMOUNT : G =      2.16082 B =   -40.92611 P.U.
SWITCHING ACTION : AT TIME      1.000 SECONDS - LINE REMOVED
  FROM BUS :      180 BURNS2     500.
  TO BUS :        86 SUMMER L    500.
  CKT : 1
1.050      36 BRIDGER2      22.0   1   0.50
1.100      36 BRIDGER2      22.0   1   1.01
1.150      36 BRIDGER2      22.0   1   1.44

```

Figure 4.10: Simulation Result Showing Faulted Lines Removed but RAS Refused to Trigger Due to False Data Injection in Case 2

is designed to be attack-resilient because it is able to take the correct remedial actions in the presence of moderate amounts of false data.

```

SWITCHING ACTION : AT TIME      1.000 SECONDS - ADMITTANCE ADDED
  BUS :          33 CA230TO      230.
  AMOUNT : G =      0.00000 B = -1999.59998 P.U.
SWITCHING ACTION : AT TIME      1.000 SECONDS - ADMITTANCE ADDED
  BUS :          34 CA230       230.
  AMOUNT : G =      4.95050 B =  -49.10495 P.U.
SWITCHING ACTION : AT TIME      1.000 SECONDS - LINE REMOVED
  FROM BUS :      34 CA230      230.
  TO BUS :        33 CA230TO    230.
  CKT : 1
SWITCHING ACTION : AT TIME      1.000 SECONDS - ADMITTANCE ADDED
  BUS :          180 BURNS2      500.
  AMOUNT : G =      0.00000 B = -1998.89648 P.U.
SWITCHING ACTION : AT TIME      1.000 SECONDS - ADMITTANCE ADDED
  BUS :          86 SUMMER L     500.
  AMOUNT : G =      2.16082 B =  -40.92611 P.U.
SWITCHING ACTION : AT TIME      1.000 SECONDS - LINE REMOVED
  FROM BUS :      180 BURNS2    500.
  TO BUS :        86 SUMMER L   500.
  CKT : 1
SWITCHING ACTION : AT TIME      1.000 SECONDS - LOAD SHED
  BUS :          31 CANADA       500.
  SHUNT% =      0.00000 PLOAD% =  50.00000 QLOAD% =  50.00000
  LOAD SHED :   2200.000 MW      500.000 MVAR      SPS LOAD SHEDING
SWITCHING ACTION : AT TIME      1.000 SECONDS - GENERATOR DISCONNECTED
  GENERATOR :    35 CMAIN GM     20.0 ID : 1
EQ. NAME:
  1.050      36 BRIDGER2      22.0  1  0.50
  1.100      36 BRIDGER2      22.0  1  1.01
  1.150      36 BRIDGER2      22.0  1  1.44
  1.200      36 BRIDGER2      22.0  1  1.78
  1.250      36 BRIDGER2      22.0  1  2.17
  1.300      36 BRIDGER2      22.0  1  2.56
  1.350      36 BRIDGER2      22.0  1  2.95
  1.400      36 BRIDGER2      22.0  1  3.34
  1.450      36 BRIDGER2      22.0  1  3.73
  1.500      36 BRIDGER2      22.0  1  4.12
  1.550      36 BRIDGER2      22.0  1  4.51
  1.600      36 BRIDGER2      22.0  1  4.90
  1.650      36 BRIDGER2      22.0  1  5.29
  1.700      36 BRIDGER2      22.0  1  5.68
  1.750      36 BRIDGER2      22.0  1  6.07
  1.800      36 BRIDGER2      22.0  1  6.46
  1.850      36 BRIDGER2      22.0  1  6.85
  1.900      36 BRIDGER2      22.0  1  7.24
  1.950      36 BRIDGER2      22.0  1  7.63
  2.000      36 BRIDGER2      22.0  1  8.02
  2.050      36 BRIDGER2      22.0  1  8.41
  2.100      36 BRIDGER2      22.0  1  8.80
  2.150      36 BRIDGER2      22.0  1  9.19
  2.200      36 BRIDGER2      22.0  1  9.58
  2.250      36 BRIDGER2      22.0  1  9.97
  2.300      36 BRIDGER2      22.0  1  10.36
  2.350      36 BRIDGER2      22.0  1  10.75
  2.400      36 BRIDGER2      22.0  1  11.14
  2.450      36 BRIDGER2      22.0  1  11.53
  2.500      36 BRIDGER2      22.0  1  11.92
  2.550      36 BRIDGER2      22.0  1  12.31
  2.600      36 BRIDGER2      22.0  1  12.70
  2.650      36 BRIDGER2      22.0  1  13.09
  2.700      36 BRIDGER2      22.0  1  13.48
  2.750      36 BRIDGER2      22.0  1  13.87
  2.800      36 BRIDGER2      22.0  1  14.26
  2.850      36 BRIDGER2      22.0  1  14.65
  2.900      36 BRIDGER2      22.0  1  15.04
  2.950      36 BRIDGER2      22.0  1  15.43
  3.000      36 BRIDGER2      22.0  1  15.82
  3.050      36 BRIDGER2      22.0  1  16.21
  3.100      36 BRIDGER2      22.0  1  16.60
  3.150      36 BRIDGER2      22.0  1  16.99
  3.200      36 BRIDGER2      22.0  1  17.38
  3.250      36 BRIDGER2      22.0  1  17.77
  3.300      36 BRIDGER2      22.0  1  18.16
  3.350      36 BRIDGER2      22.0  1  18.55
  3.400      36 BRIDGER2      22.0  1  18.94
  3.450      36 BRIDGER2      22.0  1  19.33
  3.500      36 BRIDGER2      22.0  1  19.72
  3.550      36 BRIDGER2      22.0  1  20.11
  3.600      36 BRIDGER2      22.0  1  20.50
  3.650      36 BRIDGER2      22.0  1  20.89
  3.700      36 BRIDGER2      22.0  1  21.28
  3.750      36 BRIDGER2      22.0  1  21.67
  3.800      36 BRIDGER2      22.0  1  22.06
  3.850      36 BRIDGER2      22.0  1  22.45
  3.900      36 BRIDGER2      22.0  1  22.84
  3.950      36 BRIDGER2      22.0  1  23.23
  4.000      36 BRIDGER2      22.0  1  23.62
  4.050      36 BRIDGER2      22.0  1  24.01
  4.100      36 BRIDGER2      22.0  1  24.40
  4.150      36 BRIDGER2      22.0  1  24.79
  4.200      36 BRIDGER2      22.0  1  25.18
  4.250      36 BRIDGER2      22.0  1  25.57
  4.300      36 BRIDGER2      22.0  1  25.96
  4.350      36 BRIDGER2      22.0  1  26.35
  4.400      36 BRIDGER2      22.0  1  26.74
  4.450      36 BRIDGER2      22.0  1  27.13
  4.500      36 BRIDGER2      22.0  1  27.52
  4.550      36 BRIDGER2      22.0  1  27.91
  4.600      36 BRIDGER2      22.0  1  28.30
  4.650      36 BRIDGER2      22.0  1  28.69
  4.700      36 BRIDGER2      22.0  1  29.08
  4.750      36 BRIDGER2      22.0  1  29.47
  4.800      36 BRIDGER2      22.0  1  29.86
  4.850      36 BRIDGER2      22.0  1  30.25
  4.900      36 BRIDGER2      22.0  1  30.64
  4.950      36 BRIDGER2      22.0  1  31.03
  5.000      36 BRIDGER2      22.0  1  31.42
  5.050      36 BRIDGER2      22.0  1  31.81
  5.100      36 BRIDGER2      22.0  1  32.20
  5.150      36 BRIDGER2      22.0  1  32.59
  5.200      36 BRIDGER2      22.0  1  32.98
  5.250      36 BRIDGER2      22.0  1  33.37
  5.300      36 BRIDGER2      22.0  1  33.76
  5.350      36 BRIDGER2      22.0  1  34.15
  5.400      36 BRIDGER2      22.0  1  34.54
  5.450      36 BRIDGER2      22.0  1  34.93
  5.500      36 BRIDGER2      22.0  1  35.32
  5.550      36 BRIDGER2      22.0  1  35.71
  5.600      36 BRIDGER2      22.0  1  36.10
  5.650      36 BRIDGER2      22.0  1  36.49
  5.700      36 BRIDGER2      22.0  1  36.88
  5.750      36 BRIDGER2      22.0  1  37.27
  5.800      36 BRIDGER2      22.0  1  37.66
  5.850      36 BRIDGER2      22.0  1  38.05
  5.900      36 BRIDGER2      22.0  1  38.44
  5.950      36 BRIDGER2      22.0  1  38.83
  6.000      36 BRIDGER2      22.0  1  39.22
  6.050      36 BRIDGER2      22.0  1  39.61
  6.100      36 BRIDGER2      22.0  1  40.00
  6.150      36 BRIDGER2      22.0  1  40.39
  6.200      36 BRIDGER2      22.0  1  40.78
  6.250      36 BRIDGER2      22.0  1  41.17
  6.300      36 BRIDGER2      22.0  1  41.56
  6.350      36 BRIDGER2      22.0  1  41.95
  6.400      36 BRIDGER2      22.0  1  42.34
  6.450      36 BRIDGER2      22.0  1  42.73
  6.500      36 BRIDGER2      22.0  1  43.12
  6.550      36 BRIDGER2      22.0  1  43.51
  6.600      36 BRIDGER2      22.0  1  43.90
  6.650      36 BRIDGER2      22.0  1  44.29
  6.700      36 BRIDGER2      22.0  1  44.68
  6.750      36 BRIDGER2      22.0  1  45.07
  6.800      36 BRIDGER2      22.0  1  45.46
  6.850      36 BRIDGER2      22.0  1  45.85
  6.900      36 BRIDGER2      22.0  1  46.24
  6.950      36 BRIDGER2      22.0  1  46.63
  7.000      36 BRIDGER2      22.0  1  47.02
  7.050      36 BRIDGER2      22.0  1  47.41
  7.100      36 BRIDGER2      22.0  1  47.80
  7.150      36 BRIDGER2      22.0  1  48.19
  7.200      36 BRIDGER2      22.0  1  48.58
  7.250      36 BRIDGER2      22.0  1  48.97
  7.300      36 BRIDGER2      22.0  1  49.36
  7.350      36 BRIDGER2      22.0  1  49.75
  7.400      36 BRIDGER2      22.0  1  50.14
  7.450      36 BRIDGER2      22.0  1  50.53
  7.500      36 BRIDGER2      22.0  1  50.92
  7.550      36 BRIDGER2      22.0  1  51.31
  7.600      36 BRIDGER2      22.0  1  51.70
  7.650      36 BRIDGER2      22.0  1  52.09
  7.700      36 BRIDGER2      22.0  1  52.48
  7.750      36 BRIDGER2      22.0  1  52.87
  7.800      36 BRIDGER2      22.0  1  53.26
  7.850      36 BRIDGER2      22.0  1  53.65
  7.900      36 BRIDGER2      22.0  1  54.04
  7.950      36 BRIDGER2      22.0  1  54.43
  8.000      36 BRIDGER2      22.0  1  54.82
  8.050      36 BRIDGER2      22.0  1  55.21
  8.100      36 BRIDGER2      22.0  1  55.60
  8.150      36 BRIDGER2      22.0  1  55.99
  8.200      36 BRIDGER2      22.0  1  56.38
  8.250      36 BRIDGER2      22.0  1  56.77
  8.300      36 BRIDGER2      22.0  1  57.16
  8.350      36 BRIDGER2      22.0  1  57.55
  8.400      36 BRIDGER2      22.0  1  57.94
  8.450      36 BRIDGER2      22.0  1  58.33
  8.500      36 BRIDGER2      22.0  1  58.72
  8.550      36 BRIDGER2      22.0  1  59.11
  8.600      36 BRIDGER2      22.0  1  59.50
  8.650      36 BRIDGER2      22.0  1  59.89
  8.700      36 BRIDGER2      22.0  1  60.28
  8.750      36 BRIDGER2      22.0  1  60.67
  8.800      36 BRIDGER2      22.0  1  61.06
  8.850      36 BRIDGER2      22.0  1  61.45
  8.900      36 BRIDGER2      22.0  1  61.84
  8.950      36 BRIDGER2      22.0  1  62.23
  9.000      36 BRIDGER2      22.0  1  62.62
  9.050      36 BRIDGER2      22.0  1  63.01
  9.100      36 BRIDGER2      22.0  1  63.40
  9.150      36 BRIDGER2      22.0  1  63.79
  9.200      36 BRIDGER2      22.0  1  64.18
  9.250      36 BRIDGER2      22.0  1  64.57
  9.300      36 BRIDGER2      22.0  1  64.96
  9.350      36 BRIDGER2      22.0  1  65.35
  9.400      36 BRIDGER2      22.0  1  65.74
  9.450      36 BRIDGER2      22.0  1  66.13
  9.500      36 BRIDGER2      22.0  1  66.52
  9.550      36 BRIDGER2      22.0  1  66.91
  9.600      36 BRIDGER2      22.0  1  67.30
  9.650      36 BRIDGER2      22.0  1  67.69
  9.700      36 BRIDGER2      22.0  1  68.08
  9.750      36 BRIDGER2      22.0  1  68.47
  9.800      36 BRIDGER2      22.0  1  68.86
  9.850      36 BRIDGER2      22.0  1  69.25
  9.900      36 BRIDGER2      22.0  1  69.64
  9.950      36 BRIDGER2      22.0  1  70.03
  10.000     36 BRIDGER2      22.0  1  70.42
  10.050     36 BRIDGER2      22.0  1  70.81
  10.100     36 BRIDGER2      22.0  1  71.20
  10.150     36 BRIDGER2      22.0  1  71.59
  10.200     36 BRIDGER2      22.0  1  71.98
  10.250     36 BRIDGER2      22.0  1  72.37
  10.300     36 BRIDGER2      22.0  1  72.76
  10.350     36 BRIDGER2      22.0  1  73.15
  10.400     36 BRIDGER2      22.0  1  73.54
  10.450     36 BRIDGER2      22.0  1  73.93
  10.500     36 BRIDGER2      22.0  1  74.32
  10.550     36 BRIDGER2      22.0  1  74.71
  10.600     36 BRIDGER2      22.0  1  75.10
  10.650     36 BRIDGER2      22.0  1  75.49
  10.700     36 BRIDGER2      22.0  1  75.88
  10.750     36 BRIDGER2      22.0  1  76.27
  10.800     36 BRIDGER2      22.0  1  76.66
  10.850     36 BRIDGER2      22.0  1  77.05
  10.900     36 BRIDGER2      22.0  1  77.44
  10.950     36 BRIDGER2      22.0  1  77.83
  11.000     36 BRIDGER2      22.0  1  78.22
  11.050     36 BRIDGER2      22.0  1  78.61
  11.100     36 BRIDGER2      22.0  1  79.00
  11.150     36 BRIDGER2      22.0  1  79.39
  11.200     36 BRIDGER2      22.0  1  79.78
  11.250     36 BRIDGER2      22.0  1  80.17
  11.300     36 BRIDGER2      22.0  1  80.56
  11.350     36 BRIDGER2      22.0  1  80.95
  11.400     36 BRIDGER2      22.0  1  81.34
  11.450     36 BRIDGER2      22.0  1  81.73
  11.500     36 BRIDGER2      22.0  1  82.12
  11.550     36 BRIDGER2      22.0  1  82.51
  11.600     36 BRIDGER2      22.0  1  82.90
  11.650     36 BRIDGER2      22.0  1  83.29
  11.700     36 BRIDGER2      22.0  1  83.68
  11.750     36 BRIDGER2      22.0  1  84.07
  11.800     36 BRIDGER2      22.0  1  84.46
  11.850     36 BRIDGER2      22.0  1  84.85
  11.900     36 BRIDGER2      22.0  1  85.24
  11.950     36 BRIDGER2      22.0  1  85.63
  12.000     36 BRIDGER2      22.0  1  86.02
  12.050     36 BRIDGER2      22.0  1  86.41
  12.100     36 BRIDGER2      22.0  1  86.80
  12.150     36 BRIDGER2      22.0  1  87.19
  12.200     36 BRIDGER2      22.0  1  87.58
  12.250     36 BRIDGER2      22.0  1  87.97
  12.300     36 BRIDGER2      22.0  1  88.36
  12.350     36 BRIDGER2      22.0  1  88.75
  12.400     36 BRIDGER2      22.0  1  89.14
  12.450     36 BRIDGER2      22.0  1  89.53
  12.500     36 BRIDGER2      22.0  1  89.92
  12.550     36 BRIDGER2      22.0  1  90.31
  12.600     36 BRIDGER2      22.0  1  90.70
  12.650     36 BRIDGER2      22.0  1  91.09
  12.700     36 BRIDGER2      22.0  1  91.48
  12.750     36 BRIDGER2      22.0  1  91.87
  12.800     36 BRIDGER2      22.0  1  92.26
  12.850     36 BRIDGER2      22.0  1  92.65
  12.900     36 BRIDGER2      22.0  1  93.04
  12.950     36 BRIDGER2      22.0  1  93.43
  13.000     36 BRIDGER2      22.0  1  93.82
  13.050     36 BRIDGER2      22.0  1  94.21
  13.100     36 BRIDGER2      22.0  1  94.60
  13.150     36 BRIDGER2      22.0  1  94.99
  13.200     36 BRIDGER2      22.0  1  95.38
  13.250     36 BRIDGER2      22.0  1  95.77
  13.300     36 BRIDGER2      22.0  1  96.16
  13.350     36 BRIDGER2      22.0  1  96.55
  13.400     36 BRIDGER2      22.0  1  96.94
  13.450     36 BRIDGER2      22.0  1  97.33
  13.500     36 BRIDGER2      22.0  1  97.72
  13.550     36 BRIDGER2      22.0  1  98.11
  13.600     36 BRIDGER2      22.0  1  98.50
  13.650     36 BRIDGER2      22.0  1  98.89
  13.700     36 BRIDGER2      22.0  1  99.28
  13.750     36 BRIDGER2      22.0  1  99.67
  13.800     36 BRIDGER2      22.0  1  100.06
  13.850     36 BRIDGER2      22.0  1  100.45
  13.900     36 BRIDGER2      22.0  1  100.84
  13.950     36 BRIDGER2      22.0  1  101.23
  14.000     36 BRIDGER2      22.0  1  101.62
  14.050     36 BRIDGER2      22.0  1  102.01
  14.100     36 BRIDGER2      22.0  1  102.40
  14.150     36 BRIDGER2      22.0  1  102.79
  14.200     36 BRIDGER2      22.0  1  103.18
  14.250     36 BRIDGER2      22.0  1  103.57
  14.300     36 BRIDGER2      22.0  1  103.96
  14.350     36 BRIDGER2      22.0  1  104.35
  14.400     36 BRIDGER2      22.0  1  104.74
  14.450     36 BRIDGER2      22.0  1  105.13
  14.500     36 BRIDGER2      22.0  1  105.52
  14.550     36 BRIDGER2      22.0  1  105.91
  14.600     36 BRIDGER2      22.0  1  106.30
  14.650     36 BRIDGER2      22.0  1  106.69
  14.700     36 BRIDGER2      22.0  1  107.08
  14.750     36 BRIDGER2      22.0  1  107.47
  14.800     36 BRIDGER2      22.0  1  107.86
  14.850     36 BRIDGER2      22.0  1  108.25
  14.900     36 BRIDGER2      22.0  1  108.64
  14.950     36 BRIDGER2      22.0  1  109.03
  15.000     36 BRIDGER2      22.0  1  109.42
  15.050     36 BRIDGER2      22.0  1  109.81
  15.100     36 BRIDGER2      22.0  1  110.20
  15.150     36 BRIDGER2      22.0  1  110.59
  15.200     36 BRIDGER2      22.0  1  110.98
  15.250     36 BRIDGER2      22.0  1  111.37
  15.300     36 BRIDGER2      22.0  1  111.76
  15.350     36 BRIDGER2      22.0  1  112.15
  15.400     36 BRIDGER2      22.0  1  112.54
  15.450     36 BRIDGER2      22.0  1  112.93
  15.500     36 BRIDGER2      22.0  1  113.32
  15.550     36 BRIDGER2      22.0  1  113.71
  15.600     36 BRIDGER2      22.0  1  114.10
  15.650     36 BRIDGER2      22.0  1  114.49
  15.700     36 BRIDGER2      22.0  1  114.88
  15.750     36 BRIDGER2      22.0  1  115.27
  15.800     36 BRIDGER2      22.0  1  115.66
  15.850     36 BRIDGER2      22.0  1  116.05
  15.900     36 BRIDGER2      22.0  1  116.44
  15.950     36 BRIDGER2      22.0  1  116.83
  16.000     36 BRIDGER2      22.0  1  117.22
  16.050     36 BRIDGER2      22.0  1  117.61
  16.100     36 BRIDGER2      22.0  1  118.00
  16.150     36 BRIDGER2      22.0  1  118.39
  16.200     36 BRIDGER2      22.0  1  118.78
  16.250     36 BRIDGER2      22.0  1  119.17
  16.300     36 BRIDGER2      22.0  1  119.56
  16.350     36 BRIDGER2      22.0  1  119.95
  16.400     36 BRIDGER2      22.0  1  120.34
  16.450     36 BRIDGER2      22.0  1  120.73
  16.500     36 BRIDGER2      22.0  1  121.12
  16.550     36 BRIDGER2      22.0  1  121.51
  16.600     36 BRIDGER2      22.0  1  121.90
  16.650     36 BRIDGER2      22.0  1  122.29
  16.700     36 BRIDGER2      22.0  1  122.68
  16.750     36 BRIDGER2      22.0  1  123.07
  16.800     36 BRIDGER2      22.0  1  123.46
  16.850     36 BRIDGER2      22.0  1  123.85
  16.900     36 BRIDGER2      22.0  1  124.24
  16.950     36 BRIDGER2      22.0  1  124.63
  17.000     36 BRIDGER2      22.0  1  125.02
  17.050     36 BRIDGER2      22.0  1  125.41
  17.100     36 BRIDGER2      22.0  1  125.80
  17.150     36 BRIDGER2      22.0  1  126.19
  17.200     36 BRIDGER2      22.0  1  126.58
  17.250     36 BRIDGER2      22.0  1  126.97
  17.300     36 BRIDGER2      22.0  1  127.36
  17.350     36 BRIDGER2      22.0  1  127.75
  17.400     36 BRIDGER2      22.0  1  128.14
  17.450     36 BRIDGER2      22.0  1  128.53
  17.500     36 BRIDGER2      22.0  1  128.92
  17.550     36 BRIDGER2      22.0  1  129.31
  17.600     36 BRIDGER2      22.0  1  129.70
  17.650     36 BRIDGER2      22.0  1  130.09
  17.700     36 BRIDGER2      22.0  1  130.48
  17.750     36 BRIDGER2      22.0  1  130.87
  17.800     36 BRIDGER2      22.0  1  131.26
  17.850     36 BRIDGER2      22.0  1  131.65
  17.900     36 BRIDGER2      22.0  1  132.04
  17.950     36 BRIDGER2      22.0  1  132.43
  18.000     36 BRIDGER2      22.0  1  132.82
  18.050     36 BRIDGER2      22.0  1  133.21
  18.100     36 BRIDGER2      22.0  1  133.60
  18.150     36 BRIDGER2      22.0  1  133.99
  18.200     36 BRIDGER2      22.0  1  134.38
  18.250     36 BRIDGER2      22.0  1  134.77
  18.300     36 BRIDGER2      22.0  1  135.16
  18.350     36 BRIDGER2      22.0  1  135.55
  18.400     36 BRIDGER2      22.0  1  135.94
  18.450     36 BRIDGER2      22.0  1  136.33
  18.500     36 BRIDGER2      22.0  1  136.72
  18.550     36 BRIDGER2      22.0  1  137.11
  18.600     36 BRIDGER2      22.0  1  137.50
  18.650     36 BRIDGER2      22.0  1  137.89
  18.700     36 BRIDGER2      22.0  1  138.28
  18.750     36 BRIDGER2      22.0  1  138.67
  18.800     36 BRIDGER2      22.0  1  139.06
  18.850     36 BRIDGER2      22.0  1  139.45
  18.900     36 BRIDGER2      22.0  1  139.84
  18.950     36 BRIDGER2
```

Chapter 5: Conclusions and Future Work

This chapter concludes this thesis describing the major contributions of this study and the future research areas in the development and deployment of hybrid remedial action schemes to improve the reliability and resilience of the power grid.

5.1 Conclusions

In this thesis, the design of two RAS schemes were studied; one utilized an event-based RAS model to increase the transient stability index of a power system island, while the other deployed a hybrid RAS (event-based and parameter-based) to detect false data injection in a power system measurement used for RAS and take appropriate remedial action despite the presence of compromised data.

An overview of RAS schemes, their classification and features were described. A methodology for improving the transient stability index of an islanded power system by the deployment of RAS scheme was proposed. The proposed approach utilized an event-based RAS scheme to ensure generation-load balance in the island, thereby improving its transient stability index. The design, implementation, deployment and validation of the proposed scheme were presented.

Hybrid RAS logic that is resilient to data-based attack was proposed and applied on the power system island formulated. The case of a cyber-attack creating a false negative condition in which the RAS scheme would not be triggered when it should was considered. The proposed RAS scheme was able to detect false status updates communicated to the controller and was able to take the correct action despite the presence of the false status update. The deployment and validation of the scheme were presented in two cases.

5.2 Contributions

The main goal of this research was to explore ways of improving the resilience, stability and reliability of the power system through the deployment of remedial action schemes. The first contribution of this thesis is the deployment of an event-based RAS scheme to improve the transient stability index of an islanded power system. The RAS scheme ensures generation-load balance of the island ensuring stability when disturbing events occur.

The second contribution of this thesis is the introduction of a hybrid RAS scheme which is false data-resilient. The scheme is able to detect false negative conditions induced by false status updates introduced by an adversary. In contrast to the typical event-based RAS scheme, the proposed RAS scheme utilizes both event-based and parameter-based schemes to achieve its false data resilience. Extensive contingency analyses were conducted to obtain the required verification parameters needed to design and deploy the robust RAS scheme. The performance of the scheme was demonstrated through simulation.

5.3 Recommendations for Future Work

In the proposed RAS schemes, the remedial actions required to maintain the stability of a power system in the face of severe disturbance were obtained through contingency analysis, which are based on power flow studies and are thus static in nature. Design and deployment of dynamic RAS scheme would be a lot more efficient and effective. A dynamic RAS scheme will be flexible and intelligent enough to determine the required RAS action in a per event basis in real-time. This ensures the RAS scheme reacts to events that were not considered during pre-fault contingency analysis. Also, dynamic state estimation could be developed to provide fast and accurate measurement data for the RAS scheme.

The proposed schemes introduced in this research will only be effective in a relatively small power system. It is not scalable enough to be deployed in a much larger system due to the extensive contingency analysis studies that would be required to determine the remedial

action to take for each event. Such a scheme that would lend itself to deployment in larger power system can be more efficiently implemented, deployed and verified through extensive study.

Bibliography

- [1] C.F. Henville and E. Struyk. “RAS and Stretched Power Systems”. In: *Western Protective Relay Conference Spokane Washington*. 2006.
- [2] Arun Shrestha, Valentina Cecchi, and Robert W. Cox. “Dynamic Remedial Action Scheme using Online Transient Stability Analysis”. In: *2014 North American Power Symposium (NAPS) Pullman, WA, USA*. IEEE. 2014, pp. 1–6.
- [3] M. Vaughan et al. “Idaho Power RAS: A dynamic Remedial Action Case Study”. In: *proceedings of the 64th Annual Georgia Tech Protective Relaying Conference, Atlanta, GA*. 2010.
- [4] Yichen Zhang, Mohammad Ehsan Raoufat, and Kevin Tomsovic. “Remedial Action Schemes and Defense Systems”. In: *Smart Grid Handbook (2016)*, pp. 1–10.
- [5] Siemens and Ponemon Institute. “Siemens and Ponemon Institute study finds utility industry vulnerable to cyberattacks”. In: 2019.
- [6] DSATools User Manual. “Powertech Labs Inc”. In: *Surrey British Columbia, Canada (2007)*.
- [7] Prabha Kundur et al. “Definition and Classification of Power System Stability IEEE/CIGRE Joint Task Force on Stability Terms and Definitions”. In: *IEEE transactions on Power Systems* 19.3 (2004), pp. 1387–1401.
- [8] Robert Schmaranz, Herwig Renner, and Ignaz Hübl. “Rotor Angle Stability and the Effects on Protection Devices in Distribution Networks”. In: *KELAG, Klagenfurt, Austria and University of Technology, Graz, Austria. 19th International Conference on Electricity Distribution, Vienna, 05–21–07*. 2006.
- [9] Prabha Kundur, Neal J. Balu, and Mark G. Lauby. *Power System Stability and Control*. Vol. 7. McGraw-hill New York, 1994.
- [10] Thierry Van Cutsem and Costas Vournas. *Voltage Stability of Electric Power Systems*. Springer Science & Business Media, 2007.

- [11] N. Hatziargyriou, E. Karapidakis, and D. Hatzifotis. “Frequency Stability of Power Systems in Large Islands with High Wind Power Penetration”. In: *Bulk Power Syst. Dynamics Control Symp.âIV Restructuring*. Vol. 102. 1998, p. 4.
- [12] Mathaios Panteli et al. “Assessing the Impact of Insufficient Situation Awareness on Power System Operation”. In: *IEEE Transactions on power systems* 28.3 (2013), pp. 2967–2977.
- [13] Lamine Mili. “Taxonomy of the Characteristics of Power System Operating States”. In: *2nd NSF-VT Resilient and Sustainable Critical Infrastructures (RESIN) Workshop*. 2011, pp. 13–15.
- [14] Lester H Fink and Kjell Carlsen. “Operating Under Stress and Strain [Electrical Power Systems Control Under Emergency Conditions]”. In: *IEEE spectrum* 15.3 (1978), pp. 48–53.
- [15] P.M. Anderson and B.K. LeReverend. “Industry Experience with Special Protection Schemes”. In: *IEEE Transactions on Power Systems* 11.3 (1996), pp. 1166–1179.
- [16] NERC. “NERC Report âSpecial Protection Scheme (SPS)/Remedial Action Schemes (RAS): Assessment of Definition, Regional Practices, and Application of Related Standardsâ”. In: (1964).
- [17] WECC. *Remedial Action Scheme Design Guide*. https://www.wecc.org/Reliability/RWGRASDesignGuide_Final.pdf. [Online; accessed 19-October-2019]. 2016.
- [18] R. Ramanathan, Anand Papat, and Brian Tuck. “Technique to Implement Remedial Action Schemes in Variable Transfer Limits Computation”. In: *2014 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC)*. IEEE. 2014, pp. 1–5.
- [19] R Ramanathan, Brian Tuck, and James O’Brien. “BPA’s Experience of Implementing Remedial Action Schemes in Power Flow for Operation Studies”. In: *2013 IEEE Power & Energy Society General Meeting*. IEEE. 2013, pp. 1–5.

- [20] Parviz Khaledian, Brian K. Johnson, and Saied Hemati. “Power Grid Security Improvement by Remedial Action Schemes Using Vulnerability Assessment Based on Fault Chains and Power Flow”. In: *2018 IEEE International Conference on Probabilistic Methods Applied to Power Systems (PMAPS)*. IEEE. 2018, pp. 1–6.
- [21] Matthew Varghese et al. “The CAISO Experience of Implementing Automated Remedial Action Schemes in Energy Management Systems”. In: *2009 IEEE Power & Energy Society General Meeting*. IEEE. 2009, pp. 1–5.
- [22] Meimanat May Mahmoudi et al. “Implementation and Testing of Remedial Action Schemes for Real-Time Transient Stability Studies”. In: *2017 IEEE Power & Energy Society General Meeting*. IEEE. 2017, pp. 1–5.
- [23] Robin Jenkins and David Dolezilek. “Case study: Application of Wide-Area, Communications-Assisted Remedial Action Schemes Improves Transmission Reliability”. In: (2011).
- [24] Yao Liu, Peng Ning, and Michael K. Reiter. “False Data Injection Attacks against State Estimation in Electric Power Grids”. In: *ACM Transactions on Information and System Security (TISSEC)* 14.1 (2011), pp. 1–33.
- [25] Qingyu Yang et al. “On False Data-Injection Attacks against Power System State Estimation: Modeling and Countermeasures”. In: *IEEE Transactions on Parallel and Distributed Systems* 25.3 (2013), pp. 717–729.
- [26] Babatunde Ajao et al. “Implementation of Remedial Action Scheme for Transient Stability Index Improvement of Power System Island”. In: *2020 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*. IEEE. 2020, pp. 1–5.
- [27] J. Duncan Glover, Mulukutla S. Sarma, and Thomas Overbye. *Power System Analysis & Design, SI version*. Cengage Learning, 2012.
- [28] Daniel Ruiz-Vega and Mania Pavella. “A Comprehensive Approach to Transient Stability Control. II. Open Loop Emergency Control”. In: *IEEE Transactions on Power Systems* 18.4 (2003), pp. 1454–1460.

- [29] DSA Tools. “TSAT Model Manual”. In: *Powertech Labs Inc., British Columbia, Canada* (2011), p. 106.
- [30] J. Wirfs-Brock. “The Realities of Cybersecurity at a Rural Utility”. In: *Inside Energy* (2015).
- [31] Michael J. Assante. “Confirmation of a Coordinated Attack on the Ukrainian Power Grid”. In: *SANS Industrial Control Systems Security Blog* 207 (2016).
- [32] Shamina Hossain-McKenzie et al. “Analytic Corrective Control Selection for Online Remedial Action Scheme Design in a Cyber Adversarial Environment”. In: *IET Cyber-Physical Systems: Theory & Applications* 2.4 (2017), pp. 188–197.
- [33] Chen-Ching Liu et al. “Intruders in the Grid”. In: *IEEE Power and Energy magazine* 10.1 (2011), pp. 58–66.
- [34] Mohsen Khalaf, Ali Hooshyar, and Ehab El-Saadany. “On False Data Injection in Wide Area Protection Schemes”. In: *2018 IEEE Power & Energy Society General Meeting (PESGM)*. IEEE. 2018, pp. 1–5.
- [35] Jaime De La Ree et al. “Synchronized Phasor Measurement Applications in Power Systems”. In: *IEEE Transactions on smart grid* 1.1 (2010), pp. 20–27.
- [36] Aditya Ashok, Manimaran Govindarasu, and Jianhui Wang. “Cyber-Physical Attack-Resilient Wide-Area Monitoring, Protection, and Control for the Power Grid”. In: *Proceedings of the IEEE* 105.7 (2017), pp. 1389–1407.
- [37] Siddharth Sridhar, Adam Hahn, and Manimaran Govindarasu. “Cyber-Physical System Security for the Electric Power Grid”. In: *Proceedings of the IEEE* 100.1 (2011), pp. 210–224.
- [38] Y. Yang et al. “Impact of Cyber-Security Issues on Smart Grid”. In: *2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies*. IEEE. 2011, pp. 1–7.

- [39] *Electric Grid Cybersecurity*. <https://fas.org/sgp/crs/homesec/R45312.pdf>. [Online; accessed 10-October-2019]. 2018.
- [40] FERC. *Revised Critical Infrastructure Protection Reliability Standards*. https://www.ferc.gov/sites/default/files/2020-04/E-9_6.pdf. [Online; accessed 9-October-2019]. 2015.
- [41] NERC. *Cyber Security Supply Chain Risks*. [https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERCSupplyChainFinalReport\(20190517\).pdf](https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERCSupplyChainFinalReport(20190517).pdf). [Online; accessed 20-April-2020]. 2019.
- [42] Solveig Ward et al. “Cyber Security Issues for Protective Relays; C1 Working Group Members of Power System Relaying Committee”. In: *2007 IEEE Power Engineering Society General Meeting. Tampa, FL, USA*. 2007.

Appendix A: The full results from TSAT package of DSATools for IEEE 179 bus system

These results are specific to the power system island under the focus in Chapter 4. The units are in MW.

ACTIVE POWER FLOW ON TRANSMISSION LINES IN THE ISLAND									
Time (s)	L31 - L32	L31 - L80	L33 - L34	L68 - L71	L68 - L71	L69 - L72	L69 - L72	L69 - L76	L75 - L78
0	-748.536	698.5353	-767.689	880.1519	777.7189	740.0445	740.0445	-986.456	-1026.2
0.07	-748.536	698.5349	-767.688	880.1517	777.7188	740.0445	740.0445	-986.455	-1026.2
0.14	-748.536	698.5333	-767.688	880.1541	777.7209	740.0341	740.0341	-986.452	-1026.2
0.21	-748.535	698.53	-767.688	880.1577	777.7239	740.0447	740.0446	-986.448	-1026.2
0.28	-748.534	698.5258	-767.687	880.1629	777.7286	740.0447	740.0446	-986.445	-1026.2
0.35	-748.533	698.5203	-767.685	880.1607	777.7266	740.0227	740.0227	-986.444	-1026.19
0.42	-748.531	698.5138	-767.684	880.1582	777.7245	740.0226	740.0226	-986.445	-1026.19
0.49	-748.53	698.5074	-767.682	880.1602	777.7263	740.0337	740.0337	-986.446	-1026.19
0.56	-748.528	698.5002	-767.679	880.1567	777.7231	740.0331	740.033	-986.448	-1026.19
0.63	-748.525	698.4936	-767.678	880.1584	777.7247	740.054	740.054	-986.45	-1026.19
0.7	-748.523	698.4872	-767.674	880.1616	777.7275	740.0313	740.0312	-986.449	-1026.19
0.77	-748.52	698.4814	-767.671	880.1588	777.725	740.03	740.03	-986.448	-1026.19
0.84	-748.517	698.4769	-767.668	880.1599	777.726	740.0287	740.0287	-986.448	-1026.19
0.91	-748.513	698.4742	-767.665	880.1578	777.7241	740.0388	740.0388	-986.449	-1026.19
0.98	-748.51	698.4723	-767.661	880.1617	777.7276	740.0373	740.0373	-986.45	-1026.19
1	-748.509	698.4718	-767.66	880.1602	777.7263	740.0256	740.0256	-986.449	-1026.19
1	-687.818	40.06561	-705.495	621.5902	547.7285	490.2306	490.2306	-650.762	-1.8014
1	238.1173	141.9918	213.6878	621.4061	547.5653	490.3484	490.3484	-650.966	-1.81567
1.07	238.1785	96.8372	213.7422	617.2968	543.9207	493.9083	493.9083	-656.883	-1.85628

ACTIVE POWER FLOW ON TRANSMISSION LINES IN THE ISLAND									
Time (s)	L75 - L73	L75 - L76	L78 - L66	L78 - L76	L78 - L76	L78 - L66	L78 - L74	L81 - L180	L82 - L76
0	-1488.14	-69.672	-1100.7	960.1025	1116.888	-1100.7	0.111329	865.3408	-504.642
0.07	-1488.14	-69.6726	-1100.7	960.1014	1116.886	-1100.7	0.1113	865.3403	-504.643
0.14	-1488.14	-69.6743	-1100.7	960.0971	1116.881	-1100.7	0.1113	865.3393	-504.643
0.21	-1488.14	-69.6768	-1100.7	960.0914	1116.875	-1100.7	0.111338	865.3381	-504.645
0.28	-1488.14	-69.6797	-1100.7	960.0845	1116.867	-1100.7	0.111333	865.337	-504.646
0.35	-1488.14	-69.6825	-1100.7	960.077	1116.858	-1100.7	0.111299	865.3371	-504.647
0.42	-1488.14	-69.6851	-1100.7	960.0708	1116.851	-1100.7	0.111305	865.3381	-504.647
0.49	-1488.14	-69.6873	-1100.7	960.0657	1116.845	-1100.7	0.111289	865.3401	-504.645
0.56	-1488.14	-69.689	-1100.7	960.0618	1116.84	-1100.7	0.111302	865.3433	-504.643
0.63	-1488.14	-69.69	-1100.7	960.0596	1116.838	-1100.7	0.111322	865.3466	-504.64
0.7	-1488.14	-69.6905	-1100.7	960.059	1116.837	-1100.7	0.111324	865.3495	-504.636
0.77	-1488.14	-69.6902	-1100.7	960.0598	1116.838	-1100.7	0.111323	865.3521	-504.633
0.84	-1488.14	-69.6901	-1100.7	960.0603	1116.839	-1100.7	0.111359	865.3539	-504.629
0.91	-1488.14	-69.6898	-1100.7	960.0618	1116.84	-1100.7	0.111333	865.3554	-504.627
0.98	-1488.14	-69.6896	-1100.7	960.0623	1116.841	-1100.7	0.111289	865.3563	-504.625
1	-1488.14	-69.6893	-1100.7	960.0626	1116.841	-1100.7	0.111328	865.3568	-504.624
1	3.74E-09	1.305101	-76.7139	105.5929	131.5383	-76.7139	-1.6E-06	2.88E-06	73.60465
1	-5.8E-08	1.319761	-76.2604	106.5924	132.6729	-76.2604	1.46E-05	-6E-06	73.59945
1.07	3.71E-08	1.361867	-75.0636	109.4585	135.9153	-75.0636	-5.3E-06	-1E-05	73.56541

ACTIVE POWER FLOW OF THE TRANSMISSION LINES IN THE ISLAND									
Time (s)	L82 - L76	L82 - L76	L82 - L87	L82 - L91	L82 - L95	L83 - L89	L87 - L88	L88 - L86	L89 - L90
0	-860.612	-504.434	431.4089	731.8939	773.0029	-1272.21	430.7387	430.7387	-1282.95
0.07	-860.613	-504.435	431.4087	731.893	773.002	-1272.21	430.7386	430.7389	-1282.95
0.14	-860.614	-504.435	431.4099	731.8928	772.9877	-1272.21	430.7401	430.7404	-1282.95
0.21	-860.617	-504.437	431.4158	731.9044	773.0139	-1272.21	430.7454	430.7455	-1282.95
0.28	-860.619	-504.438	431.417	731.914	772.9932	-1272.21	430.7468	430.7469	-1282.95
0.35	-860.619	-504.439	431.4182	731.9052	772.9993	-1272.21	430.7484	430.7484	-1282.95
0.42	-860.62	-504.439	431.4175	731.9053	772.9987	-1272.21	430.7472	430.747	-1282.95
0.49	-860.617	-504.437	431.4158	731.9129	773.0049	-1272.21	430.7451	430.7444	-1282.95
0.56	-860.613	-504.435	431.4086	731.9131	772.991	-1272.21	430.7389	430.7391	-1282.95
0.63	-860.608	-504.432	431.4052	731.8741	772.9979	-1272.21	430.7344	430.734	-1282.95
0.7	-860.602	-504.428	431.3991	731.9199	772.9968	-1272.21	430.7294	430.7289	-1282.94
0.77	-860.595	-504.425	431.3921	731.8948	772.9724	-1272.2	430.7224	430.7223	-1282.94
0.84	-860.59	-504.421	431.386	731.8943	772.9869	-1272.2	430.7159	430.7162	-1282.94
0.91	-860.585	-504.419	431.3854	731.8718	772.98	-1272.2	430.7152	430.7141	-1282.93
0.98	-860.582	-504.417	431.38	731.8583	772.9666	-1272.19	430.7097	430.7097	-1282.93
1	-860.581	-504.416	431.3775	731.8664	772.9613	-1272.19	430.7078	430.7085	-1282.93
1	125.4738	73.55439	-89.9612	-67.5571	-71.1485	91.12344	-90.098	-90.098	90.89948
1	125.465	73.54919	-89.9558	-67.5487	-71.1404	91.11713	-90.0926	-90.0924	90.89319
1.07	125.407	73.5152	-89.9127	-67.5238	-71.1001	91.07378	-90.0493	-90.0493	90.84991

ACTIVE POWER FLOW OF THE TRANSMISSION LINES IN THE ISLAND										
Time (s)	L90 - L86	L91 - 92	L92 - L93	L93 - L94	L94 - L83	L95 - L96	L96 - L97	L97 - L98	L98 - L83	L180 - L86
0	-1282.95	728.7153	728.7216	725.2859	725.2829	769.475	769.4691	765.6358	765.6359	865.3409
0.07	-1282.95	728.7142	728.7181	725.2825	725.2833	769.4741	769.4731	765.6401	765.6359	865.3405
0.14	-1282.95	728.7141	728.7201	725.2841	725.2838	769.4599	769.4738	765.6403	765.6369	865.3393
0.21	-1282.95	728.7258	728.7201	725.2845	725.2863	769.4861	769.4768	765.6437	765.6387	865.3383
0.28	-1282.95	728.7353	728.7216	725.2861	725.2867	769.4656	769.4752	765.6417	765.64	865.3372
0.35	-1282.95	728.7266	728.7255	725.2896	725.2875	769.4718	769.4771	765.6434	765.6407	865.3371
0.42	-1282.95	728.7266	728.7202	725.2841	725.2871	769.4711	769.4719	765.6382	765.6404	865.3384
0.49	-1282.95	728.7341	728.7228	725.2874	725.2863	769.4773	769.4736	765.6413	765.6397	865.3402
0.56	-1282.95	728.7343	728.7203	725.2845	725.2839	769.4634	769.47	765.6366	765.6373	865.3433
0.63	-1282.95	728.6952	728.7173	725.2819	725.2819	769.47	769.4712	765.6388	765.6346	865.3464
0.7	-1282.94	728.7413	728.716	725.2805	725.2781	769.4694	769.464	765.6309	765.6307	865.3497
0.77	-1282.94	728.7162	728.7101	725.2746	725.2745	769.4451	769.457	765.6235	765.6273	865.352
0.84	-1282.93	728.7159	728.71	725.2743	725.2712	769.4595	769.4571	765.624	765.6236	865.3539
0.91	-1282.93	728.6936	728.7098	725.2737	725.2685	769.4525	769.4556	765.6226	765.6208	865.3552
0.98	-1282.93	728.6798	728.6985	725.2623	725.2667	769.4394	769.4492	765.616	765.6188	865.3566
1	-1282.93	728.6881	728.7021	725.2662	725.2665	769.4339	769.4485	765.6149	765.6189	865.357
1	90.89982	-67.7689	-67.7684	-67.8809	-67.8827	-71.3613	-71.3592	-71.476	-71.4759	8.71E-06
1	90.89333	-67.7605	-67.7649	-67.8773	-67.8781	-71.3532	-71.3545	-71.4712	-71.4711	-3.6E-06
1.07	90.85004	-67.7355	-67.7354	-67.8478	-67.8466	-71.3128	-71.3219	-71.4386	-71.4384	-1.4E-06

ACTIVE POWER FLOW ON TRANSMISSION LINES IN THE ISLAND									
Time (s)	L31 - L32	L31 - L80	L33 - L34	L68 - L71	L68 - L71	L69 - L72	L69 - L72	L69 - L76	L75 - L78
0	-748.536	698.5353	-767.689	880.1553	777.7219	740.0447	740.0446	-986.456	-1026.2
0.07	-748.536	698.5351	-767.688	880.1552	777.7217	740.0447	740.0446	-986.455	-1026.2
0.14	-748.536	698.5331	-767.688	880.1551	777.7216	740.0448	740.0447	-986.452	-1026.2
0.21	-748.535	698.5299	-767.687	880.1569	777.7234	740.0345	740.0345	-986.448	-1026.2
0.28	-748.534	698.525	-767.687	880.1569	777.7234	740.0345	740.0345	-986.446	-1026.2
0.35	-748.533	698.5196	-767.685	880.1632	777.7289	740.0344	740.0344	-986.445	-1026.19
0.42	-748.531	698.5132	-767.684	880.1614	777.7273	740.0342	740.0341	-986.445	-1026.19
0.49	-748.53	698.5064	-767.682	880.1593	777.7255	740.0225	740.0225	-986.447	-1026.19
0.56	-748.527	698.4997	-767.68	880.159	777.7252	740.0333	740.0333	-986.449	-1026.19
0.63	-748.525	698.4926	-767.677	880.1582	777.7245	740.0325	740.0325	-986.449	-1026.19
0.7	-748.522	698.4857	-767.674	880.158	777.7243	740.0421	740.0421	-986.45	-1026.19
0.77	-748.519	698.48	-767.671	880.1588	777.725	740.0306	740.0306	-986.448	-1026.19
0.84	-748.516	698.476	-767.667	880.1649	777.7304	740.0294	740.0294	-986.448	-1026.19
0.91	-748.513	698.4725	-767.664	880.1602	777.7263	740.028	740.028	-986.448	-1026.19
0.98	-748.509	698.4713	-767.66	880.1641	777.7297	740.0378	740.0378	-986.45	-1026.19
1	-748.509	698.4708	-767.66	880.1599	777.726	740.0372	740.0373	-986.451	-1026.19
1	49.68333	473.5733	-2.3E-07	731.0449	645.246	781.6735	781.6735	-1070.19	-910.593
1	52.59856	802.4468	-9.8E-08	727.0788	641.7335	786.9304	786.9304	-1078.61	-922.915
1.07	52.59503	831.6399	-2.7E-07	736.2159	649.8369	779.5085	779.5085	-1066.2	-915.967

ACTIVE POWER FLOW ON TRANSMISSION LINES IN THE ISLAND									
Time (s)	L75 - L73	L75 - L76	L78 - L66	L78 - L76	L78 - L76	L78 - L66	L78 - L74	L81 - L180	L82 - L76
0	-1488.14	-69.6724	-1100.7	960.1025	1116.888	-1100.7	0.111318	865.3403	-504.641
0.07	-1488.14	-69.673	-1100.7	960.101	1116.886	-1100.7	0.111327	865.34	-504.641
0.14	-1488.14	-69.6747	-1100.7	960.0966	1116.881	-1100.7	0.111312	865.3388	-504.642
0.21	-1488.14	-69.6773	-1100.7	960.0903	1116.873	-1100.7	0.111322	865.3375	-504.644
0.28	-1488.14	-69.6799	-1100.7	960.0837	1116.866	-1100.7	0.111342	865.3366	-504.645
0.35	-1488.14	-69.6833	-1100.7	960.0757	1116.856	-1100.7	0.111292	865.3364	-504.645
0.42	-1488.14	-69.6859	-1100.7	960.0693	1116.849	-1100.7	0.111322	865.3376	-504.645
0.49	-1488.14	-69.6883	-1100.7	960.0635	1116.842	-1100.7	0.111297	865.34	-504.644
0.56	-1488.14	-69.6898	-1100.7	960.0598	1116.838	-1100.7	0.111345	865.3427	-504.641
0.63	-1488.14	-69.6908	-1100.7	960.0576	1116.835	-1100.7	0.111324	865.3459	-504.638
0.7	-1488.14	-69.6913	-1100.7	960.0573	1116.835	-1100.7	0.111329	865.3486	-504.635
0.77	-1488.14	-69.691	-1100.7	960.0576	1116.835	-1100.7	0.111304	865.3512	-504.631
0.84	-1488.14	-69.6908	-1100.7	960.0589	1116.837	-1100.7	0.111314	865.3532	-504.628
0.91	-1488.14	-69.6903	-1100.7	960.0602	1116.839	-1100.7	0.111313	865.3548	-504.625
0.98	-1488.14	-69.6903	-1100.7	960.061	1116.839	-1100.7	0.111307	865.3561	-504.623
1	-1488.14	-69.6898	-1100.7	960.0616	1116.84	-1100.7	0.111304	865.3563	-504.623
1	-1413.28	-134.763	-1045.08	714.1315	822.6403	-1045.08	0.105835	0	37.70742
1	-1416.64	-124.699	-1041.27	740.3097	852.4984	-1041.27	0.106483	0	37.69458
1.07	-1419.95	-133.874	-1036.16	718.4001	826.9634	-1036.16	0.106903	0	37.68704

ACTIVE POWER FLOW OF THE TRANSMISSION LINES IN THE ISLAND									
Time (s)	L82 - L76	L82 - L76	L82 - L87	L82 - L91	L82 - L95	L83 - L89	L87 - L88	L88 - L86	L89 - L90
0	-860.61	-504.433	431.4139	731.8827	772.9919	-1272.21	430.7439	430.7435	-1282.95
0.07	-860.61	-504.433	431.4124	731.8994	772.9908	-1272.21	430.7425	430.743	-1282.95
0.14	-860.612	-504.434	431.4153	731.9158	773.0073	-1272.21	430.7451	430.745	-1282.95
0.21	-860.614	-504.436	431.4186	731.9144	773.0057	-1272.21	430.7487	430.7486	-1282.95
0.28	-860.617	-504.437	431.4184	731.9083	773.0168	-1272.21	430.7487	430.7493	-1282.95
0.35	-860.617	-504.437	431.4207	731.8989	772.9903	-1272.21	430.7502	430.7498	-1282.95
0.42	-860.617	-504.437	431.4185	731.8847	773.0078	-1272.22	430.7478	430.7476	-1282.95
0.49	-860.614	-504.436	431.4172	731.8798	772.9725	-1272.21	430.7469	430.7467	-1282.95
0.56	-860.61	-504.434	431.4124	731.8952	773.0034	-1272.21	430.7421	430.7419	-1282.95
0.63	-860.605	-504.43	431.4049	731.903	772.9965	-1272.21	430.7351	430.736	-1282.95
0.7	-860.599	-504.427	431.4001	731.8733	772.9821	-1272.21	430.7295	430.7294	-1282.94
0.77	-860.593	-504.423	431.3954	731.88	772.9898	-1272.2	430.7249	430.7251	-1282.94
0.84	-860.587	-504.42	431.3874	731.8943	772.9872	-1272.2	430.7181	430.7193	-1282.94
0.91	-860.583	-504.417	431.3849	731.8887	772.9819	-1272.2	430.7147	430.7149	-1282.93
0.98	-860.579	-504.415	431.3832	731.8611	772.9846	-1272.2	430.7126	430.7117	-1282.93
1	-860.579	-504.415	431.3792	731.8827	772.9774	-1272.2	430.7093	430.7102	-1282.93
1	64.94245	37.94164	64.06546	-74.9653	-77.4313	99.08266	47.94558	47.94525	93.88481
1	64.92204	37.92939	64.32385	-75.0239	-77.5083	99.20792	48.16606	48.16614	93.99802
1.07	64.91047	37.92236	64.54717	-75.1082	-77.5857	99.31541	48.35672	48.35665	94.09516


ACTIVE POWER FLOW OF THE TRANSMISSION LINES IN THE ISLAND										
Time (s)	L90 - L86	L91 - 92	L92 - L93	L93 - L94	L94 - L83	L95 - L96	L96 - L97	L97 - L98	L98 - L83	L180 - L86
0	-1282.95	728.7041	728.7153	725.2795	725.2849	769.4644	769.4705	765.6371	765.6375	865.3403
0.07	-1282.95	728.7209	728.7212	725.2853	725.2853	769.4633	769.4685	765.6354	765.6385	865.3398
0.14	-1282.95	728.737	728.725	725.2894	725.2863	769.4796	769.479	765.646	765.6385	865.339
0.21	-1282.95	728.7355	728.7281	725.2924	725.2872	769.478	769.4783	765.6452	765.6401	865.3376
0.28	-1282.95	728.7297	728.7234	725.2871	725.288	769.4892	769.4747	765.6412	765.6413	865.3366
0.35	-1282.95	728.7203	728.7244	725.2883	725.2891	769.463	769.4765	765.6434	765.6423	865.3365
0.42	-1282.95	728.7059	728.73	725.2943	725.2885	769.48	769.4767	765.6436	765.6418	865.3376
0.49	-1282.95	728.7008	728.7278	725.2922	725.288	769.4446	769.4749	765.6415	765.6413	865.3398
0.56	-1282.95	728.7166	728.7214	725.2851	725.2855	769.4757	769.4745	765.6415	765.6386	865.3427
0.63	-1282.95	728.7245	728.7169	725.2808	725.2826	769.469	769.4677	765.6343	765.6359	865.3456
0.7	-1282.94	728.6945	728.7165	725.2809	725.2798	769.4545	769.472	765.6389	765.6321	865.3488
0.77	-1282.94	728.7012	728.7112	725.2756	725.2763	769.4622	769.4647	765.6314	765.6288	865.3514
0.84	-1282.94	728.7158	728.7036	725.2679	725.2733	769.4598	769.4591	765.626	765.6252	865.3534
0.91	-1282.94	728.7101	728.7086	725.273	725.2709	769.4543	769.4567	765.6237	765.6229	865.3547
0.98	-1282.93	728.6826	728.7013	725.2652	725.2689	769.4571	769.4561	765.623	765.6205	865.356
1	-1282.93	728.7042	728.7036	725.2685	725.2686	769.4499	769.4539	765.6209	765.6204	865.3564
1	93.88488	-75.2062	-75.1929	-75.7267	-75.7278	-77.7289	-77.73	-78.3548	-78.3599	0
1	93.99827	-75.2652	-75.2776	-75.8127	-75.8129	-77.8063	-77.8167	-78.443	-78.4459	0
1.07	94.09514	-75.3498	-75.3511	-75.8868	-75.8857	-77.8843	-77.8889	-78.5161	-78.5198	0

These are the buses in the power system island under the focus in this thesis.

BUSES MONITORED IN THE ISLAND			
S/N	BUS NO.	S/N	BUS NO.
1	BUS 30	21	BUS 79
2	BUS 31	22	BUS 80
3	BUS 32	23	BUS 81
4	BUS 33	24	BUS 82
5	BUS 34	25	BUS 83
6	BUS 35	26	BUS 86
7	BUS 65	27	BUS 87
8	BUS 66	28	BUS 88
9	BUS 67	29	BUS 89
10	BUS 68	30	BUS 90
11	BUS 69	31	BUS 91
12	BUS 70	32	BUS 92
13	BUS 71	33	BUS 93
14	BUS 72	34	BUS 94
15	BUS 73	35	BUS 95
16	BUS 74	36	BUS 96
17	BUS 75	37	BUS 97
18	BUS 76	38	BUS 98
19	BUS 77	39	BUS 180
20	BUS 78		

Appendix B: Copyright Permission

Part of this thesis is copyrighted by the Institution of Electrical and Electronics Engineers Inc. (IEEE). Permission for copying papers in this thesis has been issued by the IEEE. The format of this paper has been changed to match the format of this thesis. The changes include numbering of the tables, figures and their captions. Figure B.1 show the proof of copyright permissions for Chapter 3.



Implementation of Remedial Action Scheme for Transient Stability Index Improvement of Power System Island

Conference Proceedings: 2020 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)

Author: [::Babatunde:] [::Ajaoc:]; Parviz Khaledian; Brian K. Johnson; Yacine Chakhchoukh

Publisher: IEEE

Date: 17-20 Feb. 2020

Copyright © 2020, IEEE

Thesis / Dissertation Reuse

The IEEE does not require individuals working on a thesis to obtain a formal reuse license, however, you may print out this statement to be used as a permission grant:

Requirements to be followed when using any portion (e.g., figure, graph, table, or textual material) of an IEEE copyrighted paper in a thesis:

- 1) In the case of textual material (e.g., using short quotes or referring to the work within these papers) users must give full credit to the original source (author, paper, publication) followed by the IEEE copyright line © 2011 IEEE.
- 2) In the case of illustrations or tabular material, we require that the copyright line © [Year of original publication] IEEE appear prominently with each reprinted figure and/or table.
- 3) If a substantial portion of the original paper is to be used, and if you are not the senior author, also obtain the senior author's approval.

Requirements to be followed when using an entire IEEE copyrighted paper in a thesis:

- 1) The following IEEE copyright/ credit notice should be placed prominently in the references: © [year of original publication] IEEE. Reprinted, with permission, from [author names, paper title, IEEE publication title, and month/year of publication]
- 2) Only the accepted version of an IEEE copyrighted paper can be used when posting the paper or your thesis on-line.
- 3) In placing the thesis on the author's university website, please display the following message in a prominent place on the website: In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of [university/educational entity's name goes here]'s products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink.

If applicable, University Microfilms and/or ProQuest Library, or the Archives of Canada may supply single copies of the dissertation.

BACK
CLOSE WINDOW

© 2020 Copyright - All Rights Reserved | Copyright Clearance Center, Inc. | [Privacy statement](#) | [Terms and Conditions](#)
 Comments? We would like to hear from you. E-mail us at customer-care@copyright.com

Figure B.1: IEEE Permission for Copying a Paper as Chapter 3 in the Thesis