PROTECTING THE POWER GRID: STRATEGIES AGAINST DISTRIBUTED CONTROLLER COMPROMISE

BY

SHAMINA S. HOSSAIN-MCKENZIE

DISSERTATION

Submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy in Electrical and Computer Engineering
in the Graduate College of the
University of Illinois at Urbana-Champaign, 2017

Urbana, Illinois

Doctoral Committee:

Professor Thomas Overbye, Chair
Assistant Professor Katherine Davis, Texas A&M University
Assistant Professor Saman Zonouz, Rutgers University
Assistant Professor Hao Zhu
Professor Peter Sauer

ABSTRACT

The electric power grid is a complex, interconnected cyber-physical system comprised of collaborating elements for monitoring and control. Distributed controllers play a prominent role in deploying this cohesive execution and are ubiquitous in the grid. As global information is shared and acted upon, faster response to system changes is achieved. However, failure or malfunction of a few or even one distributed controller in the entire system can cause cascading, detrimental effects. In the worst case, widespread blackouts can result, as exemplified by several historic cases.

Furthermore, if controllers are maliciously compromised by an adversary, they can be manipulated to drive the power system to an unsafe state. Due to the shift from proprietary control protocols to popular, accessible network protocols and other modernization factors, the power system is extremely vulnerable to cyber attacks. Cyber attacks against the grid have increased significantly in recent years and can cause severe, physical consequences. Attack vectors for distributed controllers range from execution of malicious commands that can cause sensitive equipment damage to forced system topology changes creating instability. These vulnerabilities and risks need to be fully understood, and greater technical capabilities are necessary to create resilient and dynamic defenses.

Proactive strategies must be developed to protect the power grid from distributed controller compromise or failure. This research investigates the role distributed controllers play in the grid and how their loss or compromise impacts the system. Specifically, an analytic method based on controllability analysis is derived using clustering and factorization techniques on controller sensitivities. In this manner, insight into the control support groups and sets of critical, essential, and redundant controllers for distributed controllers in the power system is achieved.

Subsequently, we introduce proactive strategies that utilize these roles and grouping results for responding to controller compromise using the remaining set. These actions can be taken immediately to reduce system stress and mitigate compromise consequences as the compromise itself is investigated and eliminated by appropriate security mechanisms. These strategies are demonstrated with several compromise scenarios, and an overall framework is presented. Additionally, the controller role and group insights are applied to aid in developing an analytic corrective control selection for fast and automated remedial action scheme (RAS) design.

Techniques to aid the verification of control commands and the detection of abnormal control action behavior are also presented. In particular, an augmented DC power flow algorithm using real-time measurements is developed that obtains both faster speed and higher accuracy than existing linear methods. For detecting abnormal behavior, a generator control action classification framework is presented that leverages known power system behaviors to enhance the use of data mining tools. Finally, the importance of incorporating power system knowledge into machine learning applications is emphasized with a study that improves power system neural network construction using modal analysis. This dissertation details these methodologies and their roles in realizing a more cohesive and resilient power system in the increasingly cyber-physical world.

To Baba and Ammu, for teaching me the values of perseverance and passion.

ACKNOWLEDGMENTS

I am beyond grateful for the instrumental and valuable advice, guidance, and knowledge dispensed by my mentors and advisor: Professor Katherine Davis, Professor Saman Zonouz, and Professor Thomas Overbye.

Thank you Kate, for your endless enthusiasm for our work and always inspiring me. From fielding ideas with me to debugging code together, you have truly helped me grow both as a researcher and person. I am very grateful for your mentorship and look forward to our future endeavors. Saman, you have taught me invaluable skills for approaching research from various perspectives. I am thankful for all your advice and kind encouragement over the last few years. Professor Overbye, thank you for all your guidance from Master's to Ph.D.; your passion and expertise in power systems research has inspired my interest even further. I have learned so much from you, and am grateful for your continuous support.

Many thanks to my doctoral committee, especially Professor Sauer and Professor Zhu. Your advice and profound knowledge aided my research greatly. I would also like to thank the National Science Foundation (NSF): Award Numbers CNS 1446229 and CNS 1446471, ARPA-E: Award No. DE-AR0000233 with Smart Wire Grid, Inc., and PowerWorld Corporation for their support and sponsorship of this research. I am also very grateful for the ECE Editorial Services, especially Jamie, Jan, and Matt, and their indispensable help in editing and preparing my dissertation.

To all my classmates at UIUC, you have become my closest friends and source of laughter, motivation, and creativity. From Everitt to ECEB, the late study nights and frequent coffee breaks have remained constant—and propelled me forward. I appreciate everyone's help and encouragement, and special thanks to Giang Chau and Siming for discussing research with me and always providing wise insight and ideas. And thank you Giang Chau for being an incredible friend (and roommate). Enver, Maryam, Uyen, Ceci, Andy,

Jaehee-Ian-Won, Lisa, Sriharsha, Josh, Beverly, Komal, Desiree, Kathleen, Trevor, Kai, Stanton, and all my wonderful friends, at UIUC and beyond, I am forever grateful for your amazing friendship.

I would not be where I am today without the support and love of my family. Ammu and Baba, I am so thankful for your ceaseless encouragement and belief that I could achieve anything with perseverance and passion. Thank you Wafiq and Boru Apu for all your love, occasional bickering (keeps us healthy), and being the best boogies. And so many thanks to Mom and Dad (Marv and Cinda), for welcoming me so completely into your family, your love, and continual support.

And the most thanks to my other half, Taylor. Thank you for always believing in me, being my partner on all adventures, and your endless love.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

The electric power grid is a complex, interconnected cyber-physical system in which a variety of mechanisms, algorithms, and individuals work together to power our modern society. In particular, power systems are critical infrastructures comprised of collaborating elements for monitoring and control. Distributed controllers play a prominent role in deploying this cohesive execution and are ubiquitous in their presence in the grid. As global information is shared and acted upon, if one distributed controller fails, the remaining set is quick to respond and ensure the overall control objective is maintained. However, multiple failures can cause detrimental, cascading effects (e.g., overloads leading to blackout) as the set struggles to automatically meet the control goal. Furthermore, if the controllers are maliciously compromised, they can be manipulated to drive the power system to an unsafe or unreliable operating state. Attack vectors for distributed controllers range from execution of malicious commands that can cause damage to sensitive equipment to forced system topology changes causing instability. *Therefore, this research seeks to provide analytic, proactive strategies for protecting the power grid from distributed controller compromise or failure.*

History of Automated Control

Automated control, including distributed controllers, has been in use for more than 2000 years. Among the earliest developments were water clocks around 270 B.C. by the Greek inventor Ktesibios. The device was a servomechanism, thus consisting of only one feedback loop. Time was measured by the regulated flow of liquid into or out of a vessel and the collected amount was subsequently measured to track time [1]. Onward from ancient times to 1900, automatic devices were devised for controlling temperature, pressures, liquid levels, and the speed of rotating machinery. However, the most significant innovation was the steam engine governor by James Watt and its improvements in the subsequent decades [1]. This period also encompassed the work of James Maxwell, involving the derivation of linear differential equations for various governor mechanisms [2]. During the mid-1900s, the World Wars motivated theoretical understanding of the control systems used and development of systems, such as those used to aim anti-aircraft guns. Many classical control techniques were established during this time, specifically for linear single-input and single-output (SISO) systems.

Modern control theory started addressing the difficult problem of how to choose the control structure that would give the best performance and how to define "best performance," thus optimal control theory [3]. More sophisticated design problems were studied with multi-input and multi-output (MIMO) systems. This period also gave rise to the state-space approach and the concepts of observability and controllability [4].

In this vast timeline, control systems moved from single-loop servomechanisms to large-scale, complex systems such as the power grid. When arc lamps were in use in the early 1900s, constant voltage or current supply was desired to sustain the gap in the electrodes, prompting the creation of a power network [5]. Power system monitoring and control began to be designed and implemented in the early 1900s, and central control rooms became a commonplace at power plants in the 1920s. By the 1930s, the electricity interchange, realized through interconnecting individual utilities and generators, was enhancing reliability and reducing operating costs. This motivated analog computers for monitoring and controlling generator output, tie-line power flows, and line frequency.

However, these computers were limited to small process control systems or large mainframe systems. Digital control was introduced in the 1960s, and with the great Northeast blackout in 1965, was catapulted to a primary role [6]. Operator control could be significantly enhanced with the use of advanced computer technologies to aid in emergency situations such as an imminent blackout. The energy management system (EMS), the collection of various computer-aided tools used by operators to monitor and control the grid, was born. As time progressed and our processing power grew, graphical user interfaces (GUIs) and visual displays were developed to further improve the EMS [7]. Today, the industrial control system of the power grid comprises complex feedback loops via the various interconnections of electric components, a multitude of control algorithms, and numerous controllers.

Power System Vulnerabilities

In power systems, the data pathways and vulnerability landscape can be partitioned into three major areas: sensors, algorithms, and control. The widespread sensors perform monitoring and provide real-time operational awareness via a supervisory control and data acquisition (SCADA) network. The measurements are used to execute various algorithms such as state estimation and real-time contingency analysis in an EMS at a control center.

Control action decisions are ultimately made, using the result of these analyses. In this work, the emphasis is on control, rather than sensors or algorithms. Attacks on situational awareness can instigate devastating consequences by misleading grid operators. Yet, attacks on controllers and the control channels are arguably worse as they can cause immediate and direct impact without invoking additional actions from operators. Thus, in considering adversarial cyber attacks on the grid, this dissertation focuses on distributed controllers.

Physical Consequences of Cyber Attacks

From February 28th, 2000, to April 23, 2000, one of the first widely known cases of an adversary maliciously compromising a control system occurred. A disgruntled, former employee of Hunter Watertech, an Australian firm that installed SCADA radio-controlled sewage equipment for the Maroochy Shire Water Services (Queensland, Australia), executed the attack(s) [8, 9]. The attacker packed his car with stolen radio equipment and a computer, and on 46 occasions during that period, issued radio commands to distributed sewage equipment.

These malicious commands caused 800,000 liters of raw sewage to overflow into public parks, rivers, and the grounds of a hotel, resulting in death of marine life, polluted water, and an unbearable stench for local residents. Further details and analysis of this attack are provided in [8, 9]. Such severe consequences were achieved by only one, knowledgeable attacker. This severity motivates much-needed protection strategies for industrial control systems (ICSs), including the power system.

Cyber-related risks and vulnerabilities have traditionally been thought to remain in the cyber-world. The power grid's ICS historically utilized propriety controls and were difficult to attack using cyber-based methods. This difficulty was due to the proprietary protocol, device age, and inability to find detailed technical information on the protocols/devices on the web or from the technical vendors themselves—achieving “security by obscurity” [5]. However, modern ICSs are being outfitted with publicly available operating systems and communicating via popular networking protocols TCP/IP [10].

Nevertheless, the perception of cyber attacks and their abilities began to change in 2007, when the Aurora project at Idaho National Labs demonstrated how a cyber hacker could inflict serious damage to a generator using only cyber commands [11]. In 2010, a real-world case with very real and severe physical consequences occurred: the Stuxnet worm traveled through cyberspace undetected, maliciously modifying programmable logic controllers (PLCs). This caused Iranian nuclear centrifuges to spin out of control, inflicting substantial physical damage—about about 20% of the centrifuges were destroyed [12]. These events demonstrated clearly that cyber attacks can cause severe detriment to infrastructure and public safety, and that they are a national security concern [13].

About 59% of power and utility companies have reported a recent significant cybersecurity incident in EY’s Global Information Security Survey for 2016-2017 [14]. Distributed controllers have increasingly cyber-physical capabilities that involve automated actions from received or collected data, and communication across many devices renders them vulnerable to cyber attacks. These cyber attacks can have severe physical consequences; the compromise of distributed controllers can cause damage to sensitive equipment or even cascading blackouts, as exemplified by the presented cases.

Such compromises can be masked to the operator by sending false reports of a safe, normal state (cyber aspect) while detrimental effects are occurring, such as overloaded lines (physical aspect). For example, as malicious modifications occurred, the Stuxnet computer worm caused the PLC to report back a loop of normal operation values to the user [12]. Therefore, both the cyber and physical impacts must be considered when addressing distributed controllers. Furthermore, the compromise of a select few controllers can cause serious consequences – an attacker does not need to gain access to all the distributed controllers. Background on distributed controllers is provided next.

Distributed Controllers

From new verification and validation techniques to algorithms to improve control and operation, as in this research, cyber-physical methods are key in realizing the most effective cyber-physical power grid. Distributed controllers are a prominent aspect of executing a cohesive cyber-physical implementation. Centralized control boasts one central controller with global information and, thus, causes much organizational and computational burden, especially in large, geographically expansive systems [15]. Furthermore, this centralized architecture increases vulnerabilities to security breaches as only one controller needs to be compromised to topple the rest. With advances in communication technologies, as well as increased needs in applications such as microgrids, distributed control schemes are being increasingly studied and implemented. In distributed control architecture, there exists no centralized controller (with the global information) but the controllers can communicate and share information with other controllers [15, 16].

The distributed control coordination of the cyber-physical power system controllers is being used for a variety of applications, from distributed flexible AC transmission system (D-FACTS) devices for power flow control to AGC schemes. The power system is benefiting greatly from its implementation, as more flexibility and robustness are achieved. However, to maintain the robust qualities of distributed control, insight into the control interactions in each system as well as thorough assessment of vulnerabilities—including both inadvertent failure and malicious compromise of distributed controller(s)—is necessary.

Distributed Control Failures

The malfunction or failure of distributed controllers has played a historical role in power system blackouts. For example, on July 13th, 1977, a collapse of the New York Con Edison system occurred (affecting 8 million people, for 5-25 hours) due to several factors: natural events, problematic design features, operating errors, and equipment malfunction [17]. In particular, the distributed protective equipment of each line operated incorrectly when lightning struck two lines, resulting in multiple tripped lines.

In Italy, on September 28th, 2003, a major country-wide blackout transpired where a tree flashover hit a tie-line (Italy-Switzerland), and connection was not re-established by the auto-recloser [17]. The auto-recloser was previously heavily loaded before tripping and could not function properly; thus, a cascading blackout occurred as tie-lines with other border countries also tripped. Essentially, the frequency decay was not controlled sufficiently to prevent the tripping of generation. These two major cases illustrate how the power system is dependent on the proper functioning of distributed controllers.

The failure of one can cause severe impacts and, in the above situations, blackouts. Failure can come from benign sources such as design glitches or weather, but also from malicious entities. These sources have become a more critical problem in recent decades, as cyber-adversarial presence has increased. For example, cyber attacks in the automatic generation control (AGC) are currently being studied by various researchers. AGC is used to allow many generator units to participate in regulation between generation and load, with generator setpoints changed by distributed controllers. It tracks the load variations while maintaining system frequency, net tie-interchanges, and optimal generation levels close to the scheduled values [18, 19].

AGC is integral to the operation of the grid, but is susceptible to failure due to certain cases of measurement noise, as studied by Zhang and Dominguez-Garcia [20]. They demonstrated that attackers are capable of malicious manipulation to the measurements, but even regular noise in the communication channels can contribute to the damaging distortions. Ultimately, the class of random noise with state-dependent intensity can destabilize the system model and cause divergence in the AGC scheme [20]. Vrakopoulou et al. discussed how the cyber-physical interaction of the power system (physical) and SCADA system (cyber) gives rise to security issues. The links between these physical and cyber components are vulnerable to attack. Specifically, the authors provide impact analysis of a cyber attack on the AGC signal and conduct feasibility analysis to determine the attack patterns that will harmfully disturb the power system [19, 21].

AGC is only one example of an integral power system function rendered vulnerable due to the unprotected links between the cyber and physical systems. These links are heavily comprised of distributed controllers and require protection and defense. The malicious compromise of distributed controller(s) can drive the power system into unsafe states and cause damage. In particular, the physical consequences of cyber attacks are of significant concern, as demonstrated by the Maroochy Shire sewage and Stuxnet attacks discussed earlier [8, 9, 12].

Distrusted Control

Attack vectors for distributed controllers range from execution of malicious commands that can cause damage to sensitive equipment to forced system topology changes that cause instability. Distrusted control describes the situation in which controller(s) have been compromised and are under the command of a sophisticated attacker. That is, the attacker can craft control tasks or commands in a legitimate format and successfully transmit them. If the adversary is able to intercept the network packets sent to the control center in *response* to the execution of the control tasks, the attacker may even be able to mask the alterations and, thus, hide their presence [22]. In a severe case, the attacker could command all the controllers or gain significant, inside access to the control center.

Defenses must be developed to both prevent a distributed controller from being compromised *and* to mitigate adverse effects when controller compromise has occurred. Factors that must be considered in these designs are:

- The attack vector: the capabilities of the attacker in what they can gain access to or control and what type of attacks they can execute (e.g., concurrent access to certain devices not possible)
- What can be trusted (e.g., intrusion detection systems (IDSs))
- The impact on controllability and stability of the system under various attacks; the resilience of the system, under how much stress and for what duration the grid can maintain service and safe operation
- The interaction of the cyber and physical components, which needs to be included in the attack vector and defense strategies

Specifically, the *cyber-physical* vulnerabilities must be studied and mitigated. Both the cyber and physical aspects of the system must be leveraged to develop effective protection and defense strategies. For example, a relay that is maliciously controlled by an attacker could be opened, but then closed with the cyber-side close command. However, it could remain under the attacker's control, necessitating a physical, power-side action of changing the system topology to isolate the controller. Yet, to permanently mitigate this compromised relay, cyber tolerance mechanisms are needed to "clean" the system from the malicious control resulting from cyber vulnerabilities [23].

The Need for Resilient, Dynamic Defenses

The issues listed above indicate the adverse vulnerabilities in distributed controller security. Conversely, even if the controllers are not maliciously compromised, they can be subject to failure or malfunction. For both of these cases, insight into their interactions with each other and impact on system controllability is significantly helpful; the cyber and physical attributes of the system must also be leveraged, as discussed in the following section. Nonetheless, this detailed information about the role of each controller allows for the powerful development of techniques to improve control as well as protect system controllability. In addition to these controllability analysis techniques, distributed controller vulnerabilities must be addressed from a detection and verification standpoint to comprehensively improve their defense.

The power grid is a critical infrastructure that is a prime target for malicious attackers. It is susceptible to cyber attacks, as vulnerabilities in the current ICSs exist due to generalized communication protocols and operating systems—deep, system-specific knowledge is no longer necessary. As demonstrated in various blackout cases, as well as research findings, the failure of distributed controllers can impact the power system severely—including physical impacts. These distributed controllers can be compromised with cyber attacks, causing them to fail or act maliciously. These vulnerabilities and risks need to be fully understood, and greater technical capabilities are necessary to create a resilient and dynamic defense [13]. The work in this dissertation seeks to contribute to that effort, providing the essential insight into how control should be maintained or regained in a cyber-adversarial environment.

Distributed controller focused control and defense strategies need to be developed, and the interactive characteristics—both between the cyber and physical layers as well as the individual controllers—must be taken into consideration. These attributes are key in analyzing distributed controllers, and their inclusion is a novel contribution of this dissertation work. This research provides the analytic methods to gain insight into the control support groups and sets of critical, essential, and redundant controllers for distributed controllers in the power system. Using these results, response strategies are formulated using the remaining, operational controllers to minimize system stress and prevent damage. Furthermore, the role and groups have versatile application and aid analytic corrective control selection for fast, automated remedial action schemes (RAS). Additionally, techniques to aid the verification of control commands and the detection of abnormal control action behavior are also presented.

CHAPTER 2

SOLUTION APPROACH

2.1 An Interdependent Future

Distributed controllers are vulnerable to cyber attacks, and effective defenses must be developed using detailed information on the possible attack vectors, controllability, and cyber-physical interactions. This work provides these insights, specifically on the role of each distributed controller within the device set as well as within the entire, interconnected system. These results are applicable broadly, not only to malicious compromise situations; controllers can malfunction or fail due to benign reasons—strategies to maintain or regain system control and mitigate adverse consequences are still necessitated and highly desired. Therefore, using the role and groups results, control response strategies are developed to respond to such events and minimize system stress.

Additionally, effective controller placement can be performed such that maximal, spanning control is achieved. With knowledge of the controller roles and their control spans, integral power system protection mechanisms such as remedial action schemes (RAS) can also benefit. Verification and detection techniques need to be improved and developed, specifically focused on distributed controllers. These methods are developed and augmented in this dissertation, providing a comprehensive view of the security of distributed controllers. With greater insight into the effect and span of each controller, the control and defense schemes can be significantly improved, in particular, by leveraging the cyber-physical attributes of the power system. For instance, the real-time measurements obtained from all across the power system can be analyzed in combination with specific control functions, resulting in powerful sensitivity information. Such information can be used to deconstruct controller critical, essential, and redundant sets, as detailed in later chapters. The plethora of system data can be investigated for classification of control actions (to flag abnormal behaviors) and other applications by applying machine learning algorithms. Enhancing traditional power system analyses with cyber-focused data mining methods and other techniques enables resilient protection, situational awareness, and improved control.

2.2 Contributions

Specifically, this research develops methods for improved control and defense of distributed controllers in cyber-physical power systems. Insight on control support groups and controller redundant, essential, and critical sets is achieved using clustering and factorization techniques. Ultimately, we can use these results to design defensive strategies to maintain or regain control in a cyber-adversarial environment and best mitigate adverse consequences. A control response framework is developed to respond to distributed controller compromise using the remaining, operational set. Additionally, versatile application of the controller role and group results is demonstrated with an analytic corrective control selection algorithm for fast, automated remedial action schemes (RAS).

Further insight is obtained using an augmented DC power flow method (augDC-PF) to backsolve for control input safety ranges in a control input verification case study. This is motivated and used in the overall Distributed Just-Ahead-of-Time Verification of Cyber-Physical Critical Infrastructure project, discussed in Section 2.3.2. Given an abnormal event (due to failure or compromise) does occur, a generator control action classification scheme was developed using support vector machine (SVM). The SVM model was enhanced using only localized voltage measurements, reducing the training while obtaining an effective classification model. This idea of leveraging power system knowledge and analyses to improve machine learning methods is exemplified with an additional study of improving neural network construction using modal analysis.

This comprehensive study of distributed controllers in power systems seeks to offer greater insight into the span and effect of control, how such information benefits response strategies to counter controller compromise, and how expansive real-time measurements can be leveraged with various data mining methods. The following chapters detail these methodologies and their roles in realizing a more cohesive and resilient power system in the increasingly cyber-physical world.

The main contributions of the work presented in this document are:

1. Analytic algorithm that processes controller sensitivities using clustering and factorization techniques to derive insight into the distributed controller set
   - Discovers control support groups via clustering, that is, which controllers are highly coupled with the control objective and each other
   - Introduces a novel algorithm for determining the number of control support groups (clusters) using a sensitivity-based threshold
   - Identifies the critical, essential, and redundant controller sets via factorization, and thus, the role each controller plays in overall system controllability
2. Application of discovered role and group results for responding to controller compromise in a cyber-adversarial environment
   - Decomposes transformed basis to determine content of equivalent line flows and ranking of redundant controllers from transformed sensitivities
     - Aiding placement to avoid critical roles and eliminating excessive redundancy
   - Studies dependence of role and control group results on system operating point
     - Observed pattern of recurrent controller roles over all operating points; certain controllers frequently assigned specific role
     - The recurrent essential or critical controllers repeatedly have expansive control span and can be leveraged in response to compromises
   - Develops a control response framework for the distributed controller compromise given compromise or failure of device(s) within the set

    - This response can be immediately deployed to reduce system stress and mitigate compromise consequences while the actual cause and removal of the compromise is investigated by security mechanisms

  - Incorporates stability assessment in the overall control response framework

    - Framework reacts whenever a setting change is observed with the compromised control and assesses impact on stability
    - Maintaining stability must be prioritized and its inclusion in the framework is necessary for a comprehensive response

3. Analytic corrective control selection for fast, automated remedial action schemes

   - Demonstrates versatility of distributed controller role and interaction discovery algorithm, specifically for remedial action schemes (RAS) and generation redispatch
   - Finds critical generators which enable significant reduction in violation index and computation time

4. Augmented DC power flow method with real-time measurements

   - Achieves both speed and accuracy compared to existing linear algorithms, which is especially useful for real-time operations such as control input verification

5. Generator control action classification based on localized voltage measurements

   - Leverages known power system behaviors (e.g., localized voltage sags) to enhance classification of control actions using support vector machine (SVM)

6. Improved neural network construction using modal analysis

   - Utilizes power system analyses and behavioral knowledge to enhance machine learning algorithms, specifically neural network design

- Seeks to eliminate trial-and-error methods for selecting number of neurons in architecture, reducing training time and contributing to overall goal of a systematic approach of constructing neural networks for power systems

2.3 Cyber-Physical Systems: The Role of Distributed Controllers

2.3.1 Cyber-Physical Systems

Cyber technologies, from the computers that perform state estimation calculations to phasor measurement units (PMUs), have been steadily integrated into the power system for decades. The seamless integration of the computational algorithms and physical components is what cyber-physical systems such as the power grid are built from and depend upon [24]. In the power system, the physical entities range from generators to protection devices and the computer-based algorithms that control or monitor them involve taking a control action such as changing generator setpoint or detecting when a fault occurs. These algorithms automate many processes in the power system and have significantly improved efficiency and situational awareness, allowing the grid to function more cohesively.

Cyber-physical systems (CPSs) integrate dynamics of the physical processes with those of software and networking, creating a more powerful and resilient system. Unlike embedded systems, where computation is paramount, CPSs seek to provide abstractions and modeling as well as design and analysis techniques for the integrated whole, combining the physical focus on dynamics (evolution of system states over time) and the cyber focus on processes of transforming data [25]. The challenges lie in dealing with these discrete and continuous dynamics, from increasing complexity to failures with cyber *and* physical actions [26].

CPSs have already begun to be and will be the foundation of our critical infrastructure. Examples include personalized healthcare and traffic flow management—CPS technologies impact many aspects of our core infrastructure. Capability, adaptability, and scalability as well as resiliency and security are improved and enabled by advances in CPSs. CPSs are advanced by innovations such as low-cost, increased capability sensors, more efficient computing devices, wireless communication, increased internet bandwidth, and power domain advances such as renewables, energy harvesting, and improvements in energy capacity [26]. The power grid plays an integral role in this CPS mission and, therefore, requires thorough investigation and development of novel CPS-focused methods and technologies.

2.3.2 Related, Motivating Project

Cyber-physical systems (CPSs) integrate the dynamics of the physical processes with those of software and networking. The interdependencies between the cyber and physical layers of the power system are exemplified when considering distributed controllers. Figure 2.1 shows an overview of the design of a cyber-physical response system (CPR) (detailed in [23]).

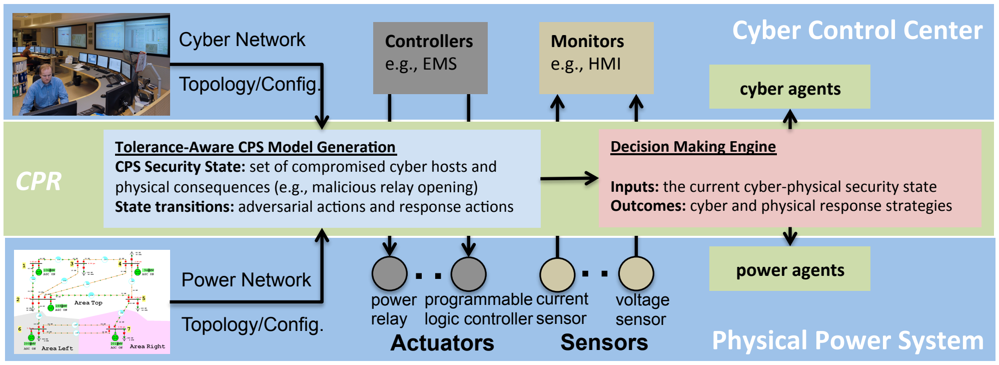

Cyber Network
Topology/Config.
Controllers
e.g., EMS
Monitors
e.g., HMI
Cyber Control Center
cyber agents
CPR
Tolerance-Aware CPS Model Generation
CPS Security State: set of compromised cyber hosts and physical consequences (e.g., malicious relay opening)
State transitions: adversarial actions and response actions
Decision Making Engine
Inputs: the current cyber-physical security state
Outcomes: cyber and physical response strategies
Power Network
Topology/Config.
power relay
programmable logic controller
current sensor
voltage sensor
Actuators
Sensors
power agents
Physical Power System

Figure 2.1: Overview of cyber-physical response system (CPR) and its interaction with the cyber and physical layers of the power system [23].

The CPR mechanism, the middle layer, must interact and glean information from both the cyber and physical sides of the power system to make the most effective response decision. The physical layer consists of the various actuators and sensors while the cyber layer possesses the controllers and human-machine-interfaces (HMI). This emphasis on considering both cyber and physical layers is important not only when developing response strategies, but for any methodology or design involving the power system. Thus, it must also be studied and integrated when analyzing distributed controllers in the power system. In particular, programmable logic controllers (PLCs) that are distributed throughout the power system play a significant role.

PLCs are industrial digital computers that are used to provide controls of any industrial system by replacing switchboards of relays to perform the operation [27]. They are able to automatically control the system by acquiring input signals from the operator or substation and then appropriately commanding the actuators of the controlled entities (e.g., generation output). In this manner, the reliability is improved and ease of programming is achieved across various actuators.

In the context of distributed controllers, a malicious attacker could upload detrimental control codes to the PLCs and cause severe consequences. For example, the attacker could command all the relays to be opened—as communicated by the code sent to the PLCs to all the relays—resulting in overloaded lines and damage to sensitive equipment. Within the cyber-side of the power system, the attacker can also mislead the control room operators by reporting that nothing has changed, that the relays are still closed.

This scenario is one of many that motivated the Distributed Just-Ahead-of-Time Verification of Cyber-Physical Critical Infrastructure project, funded by the National Science Foundation (NSF), Award Numbers 1446229 and 1446471 [28]. The work of this dissertation is a part of this overall project, though the results are versatile and broadly useful. Nonetheless, the project focuses on the cyber-physical verification (CPV) of control commands sent to PLCs in a power system.

The CPV project aims to ensure that no unsafe code will run on any PLC in the system, given a malicious adversary has already gained access to the system. A distributed Just-Ahead-of-Time (JAT) verification technique is being developed that is mathematically rigorous and practically deployable. JAT is able to check running PLC code for a rich set of security or safety properties and provide advanced warning of any code that would lead to unsafe states (violating the safety properties). The overall approach is illustrated in Figure 2.2.

Figure 2.2 includes a temporal execution graph (TEG) that shows all the possible execution paths of a PLC program from a given initial state. A fixed number of states into the future is shown (shallow TEG) and any branches not reachable (as deemed from the actual measurements) are pruned while each reachable branch is expanded. In other words, the JAT tool acts as a bump-in-the-wire between the human-machine interface (HMI) and the PLC and intercepts any control command code. This code is analyzed using the

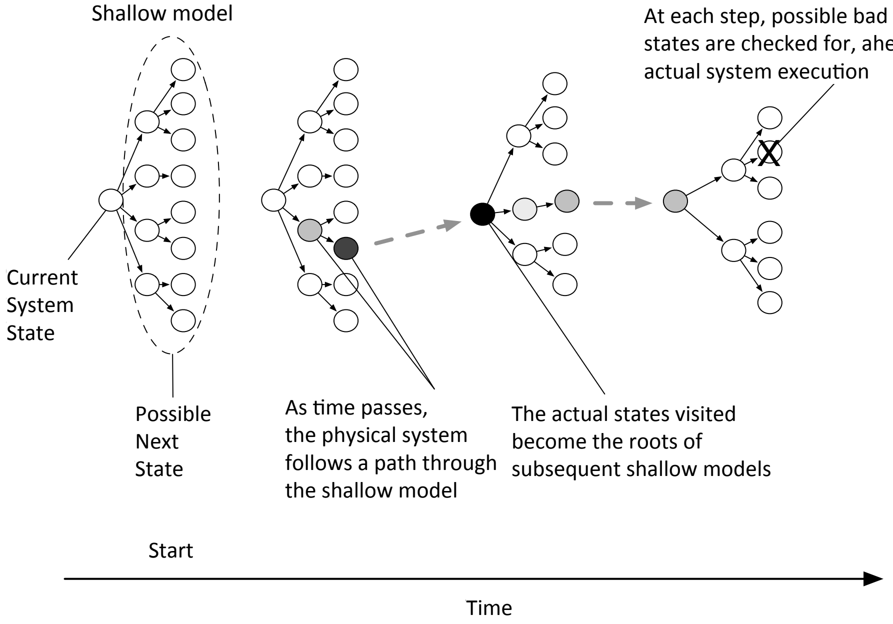

Shallow model
At each step, possible bad future states are checked for, ahead of actual system execution
X
Current System State
Possible Next State
As time passes, the physical system follows a path through the shallow model
The actual states visited become the roots of subsequent shallow models
Start
Time

Figure 2.2: Just-Ahead-of-Time (JAT) verification technique overview.

TEG, employing a variety of innovative concepts and methods from partially observable hybrid automata integration to real-time, data-driven power system model estimation. The full solution approach and details are found in [23, 28, 29].

The control logic code is analyzed to determine if any unsafe state will be encountered in its execution path in any future state if that code is run on the PLC. The states encountered by the paths are deemed safe or unsafe using power system analyses; e.g., constraints such as voltage or line flow limits must be satisfied. Thus, if a control input drives the system to an unsafe state (e.g., violates constraints), as gleaned from the power flow results, that control input is flagged as unsafe and is not executed. Symbolic executions of these analyses are utilized to explore all possible control logic execution paths. The symbolic execution, explained further in Chapter 7, uses symbols as control inputs and contains logical path conditions, such as satisfying the power system constraints.

This highly interdisciplinary project focuses on the verification of control inputs, via PLCs, in a power system. More importantly, it emphasizes the need to consider both cyber and physical layers of the power system together to create the most effective and robust solution when considering secure control. The algorithms and techniques developed in this thesis approach the problem of control in the cyber-physical grid, and specifically from the perspective of distributed controllers. The placement of controllers, the impact and defense from distrusted control, and the verification of control commands encompass the full, 360° view and analysis of power system distributed controllers.

By designing cyber-physical, data-driven methods to improve control of distributed controllers in power systems, this dissertation aids the protection and control efforts highlighted by the CPV project and previous work in controllability analysis, placement, and distrusted control. Within the CPV project, this work seeks to develop:

1. The power system analyses needed to assess each state of the TEG—fast and accurate methods to determine whether safety constraints have been violated

2. Data mining techniques to analyze control actions (e.g., flag abnormal behavior), augmenting the JAT approach

3. A detailed controllability analysis to deliver crucial insight into the flexibility and redundancy of control within the power system

Using these results, strategies to respond to compromises such as malicious control logic program execution can be derived such that system controllability is prioritized and adverse consequences are minimized (e.g., sustained system stress).

CHAPTER 3

LITERATURE REVIEW

3.1 Controllability Analysis in Power Systems

There are various components and behaviors we would like to control in the power system. We may seek to mitigate the impact of a disturbance (large or small) and prevent the loss of service or damage to equipment. Or, perhaps, we would like to alter supply at various buses due to load change. Control systems and controllers allow us to enact these changes in system properties such as topology or equipment settings (e.g., tap settings on transformers) and system behaviors (e.g., power flow control using FACTS devices).

However, the effectiveness of these controls, especially to influence behaviors, within the power system depends on the controllability of the system. This relies on the controllers (location distribution, extent of abilities) and the power system itself (topology, constraints). For example, if the power system is at the brink of voltage collapse, we would like to utilize the available controls to avoid realizing the collapse and other detrimental effects. Yet, can we be guaranteed that applying the appropriate controls will shift our power system from its dire, nearly unstable state to a safe, normal state? It depends on the controllability region of the system.

In power systems, the controllability region is the subset of the state space on which the available controls can be used to steer the power system from one state to any other state [30]. In general, the power system dynamical equation can be written as:

$$\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}) + \sum_{i=1}^{m} \mathbf{g_i}(\mathbf{x})u_i,\ \ \mathbf{x} \in \mathbf{\Xi} \tag{3.1}$$

where $\mathbf{x}$ is an n-vector of dynamic variables (e.g., generator rotor angles), $\mathbf{f}(\mathbf{x})$ is a vector consisting primarily of the power flow equations, and $\sum_{i=1}^{m} \mathbf{g_i}(\mathbf{x})u_i$

represents the effects of the controls on the system. The scalars $u_i, \ i = 1, ..., m$, are the system controls (e.g., generator mechanical power injections) and are usually piece-wise constant in time, due to device physical characteristics. System state space, $\boldsymbol{\Xi}$, is an open subset of the n-dimensional Euclidean space. If we have $X(x_0, u, t) \in \boldsymbol{\Xi}$ representing the system movement with the initial state x_0, control u, and $0 \leq t \leq \infty$, the controllability region satisfies:

$$X(s_1, u, t) = s_2, \ u \in \mathbf{U} \text{ and } 0 \leq t \leq \infty \tag{3.2}$$

where every pair of states s_1 and $s_2 \in \mathbf{Z}$ satisfies (3.2). $\mathbf{Z}$ is the controllability region, a subset of $\boldsymbol{\Xi}$. Therefore, the system presented in (3.1) can be steered from a state to any other state within the controllability region. Further proofs and other references can be found in [30]. This formulation is developed in more detail in later chapters.

Nonetheless, the calculation of the controllability region is more difficult for a nonlinear system than a linear system. The power system is nonlinear in nature, as most physical systems are, but is often approximated as a linear system to simplify and achieve more tractable analysis. As Satchidanandan et al. stated when developing an active defense strategy for networked cyber-physical systems, they assumed linear systems because it results in more tractable, useable calculations; the results are not specific to a nonlinear system (and its many intricacies) but can be generalized to a broad class of systems [31].

Thus, controllability analysis in power systems has primarily been derived for linear systems. Classic linear methods developed for controllability and observability are the Popov, Belevitch, and Hautus (PBH) eigenvector tests using rank conditions [32]. Yet, these tests only provide answers in a "yes or no" fashion—e.g., yes the system is observable or no, the system is not observable. Although useful, more detail and having a measure of controllability (or the dual, observability) are desired. Hamdan and Elabdalla [33] and Hamadan and Nayfeh [34] proposed using the cosine of the angle between appropriate subspaces to develop a quantified measure for controllability and observability of linear systems. Linear systems provide the means for more clear-cut formulation and provide results that are, for the most part, effective in application to the real, nonlinear systems.

3.1.1 Review of Controllability Analysis Techniques

Nonlinear Controllability Analysis

The importance of discovering controllability region(s) within the power system has motivated many analysis methods and frameworks. As the calculation is complex and can be burdensome (especially for the nonlinear power system), various techniques have been derived to improve it. Differential geometry concepts were applied by Hong et al. to characterize and construct the complete controllability region of a power system using a nonlinear model [35].

As the application of differential geometry had produced significant results in the area of nonlinear control, Hong et al. sought to apply it to power system controllability. Presented in 1999, such a systematic approach using a nonlinear control model was new and, to the best of their knowledge, one of the first applications of nonlinear controllability theory in power systems. They modeled the power system as a nonlinear controlled dynamical system with unbounded and bounded controls such as tap changers, capacitor banks, and mechanical power input to generators.

By characterizing the entire control state space as an open manifold, Ω, they used differential geometry concepts of foliations and leaves to discover the complete controllability region. A controlled dynamical system is completely controllable on Ω if any two states on Ω are reachable from each other. This is usually only achieved on a subset of the state space. A foliation of a manifold, Ω in this case, refers to a parallel decomposition of the manifold. Thus, if Ω is m-dimensional, the foliation of Ω is a family of disjoint submanifolds of Ω, necessarily of equal dimension, whose union is Ω. Further, the submanifold of the foliation is called a leaf of the foliation.

These leaves of the foliations contain the trajectories of the system, so the possible directions of motion from any state are tangential to the leaf. This is the basis for constructing the complete controllability region for unbounded controls. Next, they consider the equilibrium set of the system that also meets the rank condition and prove that any state on that set is locally controllable—any two states on a connected component of the set are reachable from each other. Further lemmas and proofs, as well as definitions of local controllability, reachability, etc., are provided in [35].

Since any two states on the rank condition-satisfied equilibrium set, E', are reachable from each other, a finite sequence of controls can be constructed to move the system to a neighborhood of intersection between the leaves of the foliation (the trajectories of the system) and E'. This is represented conceptually in Figure 3.1, where L_λ is a leaf of the foliation. Thus, the complete controllability region for a controlled dynamical system with unbounded controls is a union of the leaves of the foliation that intersect with the rank condition-satisfied equilibrium set. Within this region, the system can be steered from any other state if the controls (e.g., var compensation levels or OLTC reference voltage values) can be adjusted without limitation (unbounded control). The authors also derive the case for bounded controls where similar analysis was applied but cannot geometrically be described with foliations. Nonetheless, the complete controllability region is found to be the intersection of the reachability and incident regions [35].

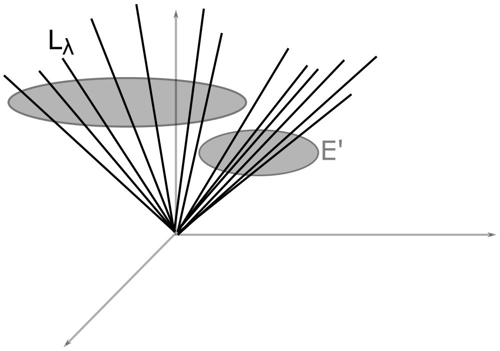


Figure 3.1: Representation of the complete controllability region with the intersection of the leaves of the foliation and the equilibrium set, based on an image from [35].

All in all, the developed theory gives sufficient conditions for complete controllability of a power system with a *nonlinear* control model with unbounded and bounded control. These results are significant in applying the differential geometry to achieve the controllability regions, especially for the unbounded control case. Nonetheless, it is not realistic to have unbounded control, although its theoretical results are very interesting and meaningful for other branches of research.

The bounded control complete controllability region was calculated, but the authors state more work is needed in making the computation of the incident and reachability regions more feasible and less burdensome. It is very difficult to compute these regions and systems with more complexity and increasing number of controls may not scale well. More tractable controllability analysis for a nonlinear, controlled power system is needed.

Linear Controllability Analysis: Quantified Measures of Controllability

Within linear controllability analysis, we can utilize techniques such as the aforementioned PBH eigenvector tests to determine whether a system is controllable. This is a "yes/no" answer but remains very useful when analyzing a system's capabilities. Nonetheless, it is even more helpful to have a quantified measure of controllability, that is, to be able to determine just how controllable a system is—a range of controllability. Specifically, modal controllability is studied where the impact of inputs on modes (associated with the system's eigenvalues) is analyzed.

Assume the following linear model of a power system:

$$\dot{x} = Ax + Bu \tag{3.3}$$

$$y = C^T x \tag{3.4}$$

where $x \in R^n$, $u \in R^m$, and $y \in R^l$. If q_i is a left eigenvector of A (p_i is a right eigenvector of A), the PBH eigenvector tests check whether q_i and b_j (the jth column of B) are orthogonal. If orthogonal, the ith mode is not controllable from the jth input. To achieve a measure of controllability, we cannot use the magnitude of $q_i^T b$ as a measure of the modal controllability. This is because the left and right eigenvectors, q_i and p_i, respectively, are scaled arbitrarily and we cannot depend upon or use rescaling.

Thus, Hamdan and Elabdalla [33] propose using the cosine of the angle between the A and B subspaces for a quantified measure of controllability (A and C for observability). However, to use this measure, the system must have distinct eigenvalues and a well-conditioned modal matrix. The authors show that condition numbers can be calculated for each eigenvalue and how to check that these conditions are satisfied (and that they usually are) [33]. Nonetheless, their proposition is that the controllability of the ith mode in the input is proportional to the cosine of the angle between q_i and b:

$$cos[\theta(q_i, b)] = \frac{|q_i^T b|}{||(q_i)||||b||} \tag{3.5}$$

If the result is zero, meaning the vectors are orthogonal, the mode is said to be decoupled from the input and completely uncontrollable. Otherwise, we have a measure of how controllable the system is with the resultant range $[0, 1]$—it is a continuous function of the distance between the two subspaces. We can consider the matrix B as an energy injection map where the controllability measure provides an indication of the energy level of the input signal.

A gross measure of modal controllability can also be derived, considering all inputs impacting the mode. After calculating (3.5) for every mode and every input, we have a matrix of controllability measures with the number of rows equal to the number of modes and the number of columns equal to the number of inputs. Thus, the norm of the ith row of the matrix is a measure of the gross controllability of the ith mode from all inputs.

Hamdan and Nayfeh [34] use this information to compute the recovery region of a system after a disturbance occurs. The recovery region is a set of initial conditions that can be steered to the origin in a finite time using admissible control—called controllability to the origin. This is related to the complete controllability region presented by Hong et al., presented in the previous section. For a single-input-single-output (SISO) system, the recovery region can be characterized as a parallelpiped in which each semiaxis has a length proportional to the controllability measure of the corresponding mode. This is easily extended to the multiple-input-multiple-output (MIMO) case (and with many state variables). Thus, the measures of gross controllability indicate the shape of the recovery region.

Hamdan and Nayfeh [34] also determined that the product of the controllability and observability measures provides a joint measure of controllability and observability of the mode and input (which can be an input from a machine/generator such as mechanical power). They also relate this concept to generator coherency (group of machines that are strongly coupled to some modes and weakly coupled to the rest) and residue matrix derived from the transfer function of a MIMO system where the magnitude of the residue can also be considered an indication of the joint modal controllability and observability. These observations are detailed further in their 1989 paper.

3.2 Distributed Controllers in Power Systems

3.2.1 Effective Placement of Distributed Controllers

When placing distributed controllers in a given power system, understanding controllability and observability is essential to study to achieve effective control. For this application, Messina and Nayebzadeh [36] formulated a design procedure using modal analysis to derive controllability and observability measures to place multiple controllers. Specifically, they aimed to place static var compensators (SVCs, a type of FACTs device) for power oscillation damping. The SVCs affect damping directly by modulating terminal voltages as well as indirectly with the response to the voltage, affecting the load and tie-line power. Expense of SVCs and the need to prevent adverse controller action require systematic placement; damping improvement using SVCs is also very location dependent.

The authors motivate the use of a linear system with their solution approach: damping is a linear phenomenon, warranting the analysis of a linear system. Modal analysis of the linear system is utilized where the modal bus voltage deviations and modal power oscillation flow are derived. The most effective bus for damping a particular oscillation mode and the patterns of oscillation energy exchanged are gleaned from these quantities, respectively.

To assess the effectiveness of SVCs to enhance damping of a specific mode, controllability and observability concepts are applied. A system is controllable or observable if the appropriate matrices (from the state space representation, as detailed in the previous section) are full rank. Another way to check the matrix rank is based on the insight that it equals the number of nonzero singular values; from this, the authors use the magnitude of the nonzero minimum singular value (MSV) to measure how far the matrix is from a matrix of lower rank—it is a quantitative measure of controllability and observability.

An augmented matrix, for both observability and controllability, is formed and its MSV is interpreted as a location index to indicate the effectiveness of SVCs to enhance damping of a particular mode. In this manner, the controllers (e.g., SVCs) can be sited across the power system such that effective control is achieved (e.g., oscillation damping) and adverse controller interactions avoided (no competing devices due to effective placement).

This work is similar to that of Hamdan and Elabdalla [33] in developing a quantitative measure but for the specific application of placing distributed controllers. However, it is worth investigating if scaling affects the MSV measure and if that can cause incorrect controllability or observability measures. Nonetheless, effective placement constitutes a significant portion of distributed controller research.

The placement of FACTS devices was also studied by Sharma et al. [37] for which they proposed using an extended voltage phasors approach (EVPA). Their method identified the most critical segments or buses in the power system from a voltage stability perspective. The EVPA method modifies the traditional voltage phasors approach (VPA) [38] by identifying not only the critical transmission paths but also the critical segments or buses. They hypothesize that the segment with the maximum corrected voltage drop in the critical path is the best location for placing a FACTS controller. In particular, they studied SVCs, static synchronous compensators (STATCOM), and thyristor-controlled series compensators (TCSCs). The EVPA method was successful in its correct identification of critical transmission paths *and* critical segments, as tested with various systems and validated with a known algorithm. However, the placement of the FACTS device, although effective from a voltage stability viewpoint, may not be for transient stability.

Leung and Chung [39] developed an optimal placement method for FACTS controllers using genetic algorithms. Genetic algorithms are search techniques that inherit their name from studying the concept of species evolution through generations. Essentially, the search is conducted starting from a population of points rather than a single point. Only the objective function's value and information are utilized, and the calculation concentrates on obtaining a coding of the parameter sets, not the parameters themselves. All in all, the authors seek to find the minimum generation cost by placing the FACTS device while satisfying various power system constraints (e.g., power flow, line flow). Essentially, they studied the placement of FACTS controllers from an economics standpoint and formulated a multi-objective optimization problem using genetic algorithms (allowing multiple objectives to be solved). The main drawback was the time consumption when considering a large system—the method did not scale well.

Besides FACTS controllers, research has also been conducted for the placement and control of Mvar (Q) controllable buses, or Q-C buses, by Rogers et al. [40]. Their overall framework sought to develop a comprehensive form of reactive power control that extends from the transmission level to the customer level. Leveraging the coupling of reactive power and voltage, the developed methodology identified the low-voltage buses and, subsequently, the Q-C buses identified as most effective are instructed to provide reactive power support. Thus, system voltages can be restored [40]. The Q-C bus locations must be selected so that the most effective reactive power support can be provided. Sensitivity analysis (voltage magnitude to reactive power injection) and classification of the loads are used to determine the best, most effective control placement of the Q-C buses.

As exemplified by this review of distributed controller placement algorithms, it is a topic of prime importance when deploying effective control. There are various techniques (e.g., modal analysis, optimization) that can be applied, but accurate controllability analysis, consideration of stability from many perspectives, ability to encompass various control objectives, and scalability are key challenges that need to be addressed to develop the most effective placement strategy for distributed controllers. This dissertation aids those endeavors, especially by leveraging sensitivity analysis to capture the intricate relationships between the controllers and system behaviors.

Nonetheless, these endeavors are in parallel with the efforts for preventing distrusted control and maintaining full system control. These works are reviewed in the following section.

3.2.2 Distrusted Control

Cascading Failures in Interdependent Networks

To address why distrusted control or failure of a small fraction of power system nodes can have such significant, devastating effects, it is important to study the nature of interconnected systems. Buldyrev et al. [41] discussed the catastrophic cascade of failures that can occur in interdependent networks in their 2010 *Nature* paper. They motivated the need for cyber-physical system analysis, rather than focusing on single, non-interacting networks. A framework to understand the robustness of the interacting networks (e.g., communication and control in power systems) subject to cascading failures is presented. They demonstrated how the failure of a small fraction of nodes of one network can lead to the complete fragmentation of the system of several interdependent networks.

An analytic approach to determine the critical fraction of nodes is developed. The removal of these nodes will lead to a failure cascade and complete fragmentation of the interdependent networks. Buldyrev et al. demonstrate that the broad degree of distribution increases vulnerability to random failures, unlike single networks. Graph theory, specifically Erdos networks and power law, and percolation concepts are applied to determine the critical threshold of the interconnected system in regards to splitting or remaining intact. These ideas and formulations are elaborated further in [41].

A motivating example of the September 18th, 2003, Italy blackout is provided and analyzed [42]. Figure 3.2 displays the iterative process of the cascade of failures in the interconnected power network (overlaid on the Italy map) and Internet network (shifted from the Italy map). Buldyrev et al. drew the networks using real geographical locations and the nearest Internet servers are connected to each power plant.

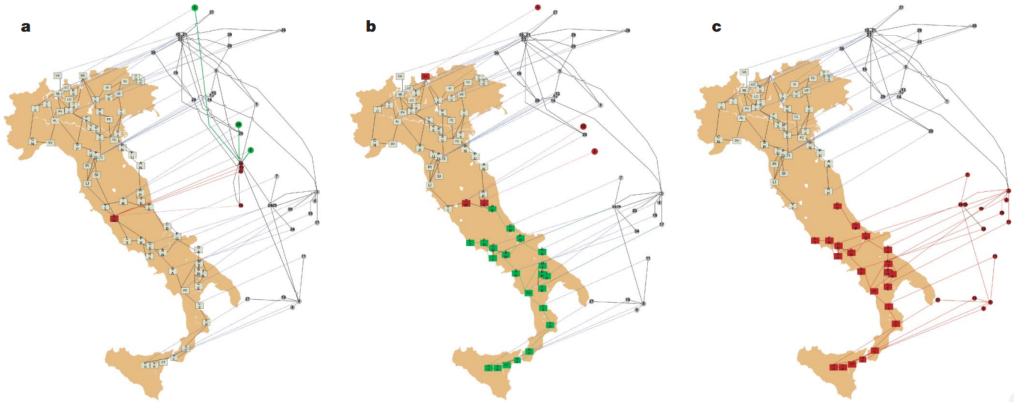


Figure 3.2: From **a-c**, a power node is removed resulting in connected Internet nodes being removed (highlighted in red). The nodes that will be subsequently fragmented are highlighted in green within each network. Ultimately, a cascade of node removal occurs due to disconnection of a power or Internet node, increasing system fragmentation [41].

Within this dissertation, we focus on the removal of nodes within the distributed controller network, either from failure or compromise. It must be recognized that a fraction of the set can cause cascading failures or significant, detrimental impact, as demonstrated by Buldyrev et al. Node loss affects not only controllability but also phenomena such as stability, as will be discussed in Section 3.3, and has severe consequences in the form of distrusted control and other cyber attacks, as examined next.

Cyber Attacks on Distributed Controllers

The impact of cyber attacks on distributed FACTS controllers has been studied by Chen et al. [43]. The paper discusses several attack scenarios and stability indices to quantify the impacts. Using a 39-bus system and simulations, they found that modification attacks, when measurement values are changed (e.g., added bias), can cause severe consequences especially when followed by a contingency; the system voltage or angle can become unstable. Further consequences related to the type of FACTS device (STATCOM vs. SVC) and type of bias (positive vs. negative) are also presented.

Similarly, Xiang et al. [44] examined the impact on power system reliability of unified power flow controllers (UPFCs). These devices control active and reactive power flows and their operation depends on both the physical and cyber systems. With this insight, the authors develop an integrated analysis and reliability model that encompasses both cyber and physical parts as well as the four operation states of the UPFC. The expected energy not supplied (EENS), an index for quantifying the reliability of the power system, was the focus of their study. The comprehensive model was then analyzed and it is shown that cyber attacks against UPFC may have an adverse influence. The system reliability can be decreased with increased frequency of successful attacks.

Both of these works involve the compromise of distributed controllers in the power system. Yet only the consequences of these cyber attacks are discussed, specifically in the context of power system transient stability and reliability. Studies such as these are foundational in establishing the need for protection of controllers in power systems, as severe consequences can occur. The need must now be addressed in the form of schemes and analyses for the protection of distributed control devices. By examining the impact of compromised controllers on the system controllability, we will gain greater insight into how to protect the controllers to maintain system control and avoid serious damage to reliability and transient stability. Furthermore, proactive defenses such as verification of the control commands before execution are motivated, as discussed in Section 2.3.2.

Compromises and Malfunctions within Control Systems

The impact of misbehaving controllers is explored from both a malicious standpoint (e.g., infections with malware) and a benign standpoint (e.g., malfunctions due to failures). Gawand et al. [45] developed control-aware techniques using data stream analysis concepts for the protection of industrial control systems (ICSs) from malware. The authors claim that complete protection against malicious software in power control systems is exceedingly difficult in practice. These systems are often uniquely configured based on deep knowledge of the particular controllers, the power system under control, and without much consideration of potential malicious adversaries. Yet the use of data stream analysis in their detection techniques can become time-consuming in large systems.

De Lima and Yen [46] proposed a supervisory system capable of detecting controller malfunctions before the stability of the plant is compromised. It is also able to differentiate between controller malfunctions and faults within the plant. However, the occurrence of multiple faults cannot yet be handled. They concentrate on the identification of plant disturbances to best decide remedial actions. This dissertation work seeks to leverage the relationships between the controllers and the power system—the cyber-physical system—to protect and mitigate any plant disturbance identified for any size system. Nonetheless, it is evident that controller malfunction and/or compromise is a significant issue that can severely impact the power system.

Active Defenses

Given the attacker has already gained access to the power system and is able to execute certain actions within it, active defense mechanisms become integral for protection and mitigation. Davis et al. [47], from the perspective of false data injection attacks, introduce a proactive defense method to detect such attacks. The false data injected by an attacker can mislead the power system operator or any automated, data-dependent devices to make decisions and perform control actions based on a false state of the system [48–50]. Therefore, using a probing approach, their work proposes a perturbation-based detection strategy that is able to identify false data injection attacks. By using the value of the data over time via a sequence of probes, they are able to detect that an attack is occurring, at which meters and what the changes in the values are [47]. Although this work focuses on unobservable attacks (as the false data injections still satisfy system model equations), the concept of probing signals can also be extended to controller commands specifically.

Satchidanandan and Kumar [31] addressed the issue of secure control in a networked cyber-physical system. They developed a protocol where honest or uncompromised controller nodes superimpose stochastically independent probing signals on top of the control law they intend to apply. Malicious nodes can forward packets not actually received, introduce intentional delays, alter packets before forwarding, and/or impersonate a different node in the system.

Essentially, the key idea was to inject into the actuation signal a component that is not known in advance. This idea is captured through the use of physical watermarking where the controller commands actuators to inject into the system a component that is random (and not known in advance). The random variables are the actuator node's privately imposed excitation (distribution public but value is not disclosed) and, thus, force the sensor (communicating with the actuator node) to report measurements that are correlated with the random variable. In this manner, any attempt from the sensor to distort the process noise (e.g., alter the data packets) will also distort the watermark. This allows the honest nodes to discover the malicious activity. To avoid this detection, the malicious sensors are restricted to only minimal distortion and cannot cause any viable damage. The full protocol framework is detailed in [31].

Satchidanandan and Kumar, and Davis et al., utilize the intuition that they expect the system to react or behave in a unique way after a certain action (e.g., probing or watermarking). They use this intuition to their advantage and observe the responses to their probing actions to detect malicious or abnormal activity. In a cross-checking approach, Lin et al. [22] developed a framework that relies on distributed IDSs to perform semantic analysis on SCADA network packets. The execution consequences of control commands are analyzed and the distributed IDS instances create trusted communication to detect any compromise of sensor measurements or control commands.

This involves combining system knowledge of both cyber and physical infrastructure to best estimate the execution consequences, which is a crucial need in the modern power grid, as will be motivated and discussed in Section 2.3.2.

Lastly, Srikantha and Kundur [51] studied denial of service (DoS) attacks in a cyber-enabled power grid and demonstrated that adversaries can disrupt the grid by only targeting a subset of the cyber communication nodes. As an active defense, they proposed a collaborative reputation-based topology configuration scheme. Using game theoretic principles, it is proved that the a low-latency Nash equilibrium routing topology always exists for the system [51]. Therefore, during a DoS attack, where the delays introduced by the attacks can cause the system to be unstable, their proposed algorithm is able to maintain dynamic stability. The algorithm enables the remaining, uncompromised cyber nodes to rapidly converge to an equilibrium topology and maintain dynamic stability.

3.3 Impact on Stability

3.3.1 Classification of Power System Stability

When developing control defense strategies, the impact on both the system controllability *and* stability must be considered. Within distrusted control, the cyber attacks launched by the adversary can cause various control changes in the power system. These malicious changes can destabilize the system, even if we maintain full system control, unless we monitor the system stability and react quickly with our uncompromised distributed controllers. Therefore, it is necessary to perform stability assessments during detrimental events such as failure or compromise of distributed controllers. If stability is lost, a very serious situation is encountered and sophisticated, additional strategies are needed to attempt to regain it or minimize damage.

Power system stability is integral to secure system operation, and as such, has been studied and addressed for several decades. It is defined by Kundur et al. [52] as follows:

> Power system stability is the ability of an electric power system, for a given initial operating condition, to regain a state of oper-

> ating equilibrium after being subjected to a physical disturbance, with most system variables bounded so that practically the entire system remains intact.

It is further elaborated as a property of the system motion around an equilibrium set—the initial operating conditions. Disturbances can be characterized as small (e.g., load changes) or large (e.g., loss of generator, significant faults). The larger finite region of attraction for a stable equilibrium set results in a more robust system, especially against large disturbances. It is unrealistic to design a system that is stable for every possible disturbance, so the most probable disturbances are considered [52]. Resiliency and reliability must always be maximized.

The grid is complex and interconnected; various stressed conditions may occur and give rise to different types of instability. If not mitigated, instability can disrupt system operation, damage components, and, in the worst case, instigate blackout. There are three main categories of power system stability, considering its physical nature, size of disturbance, and devices, processes, and time span, listed below:

1. Rotor Angle Stability
    - The ability of synchronous machines in power system to remain in synchronism after a disturbance
2. Frequency Stability
    - The ability of a power system to maintain steady frequency given significant imbalance between generation and load after a severe disturbance (e.g., system upset)
3. Voltage Stability
    - The ability of the power system to maintain steady voltages at all buses in the system after a disturbance from a given initial operating condition

Further explanation and details are provided in [52]. Within these categories, we study *types* of stability that are most suitable considering application, disturbances, and time spans. These types can be summarized in the list below:

1. Lyapunov Stability
2. Input-Output Stability
3. Stability of Linear Systems
4. Partial Stability

Definitions and formulations of these types of stability are provided in [52] and various power system stability literature. The first two, Lyapunov and input-output stability, are most applicable for studying power system nonlinear behavior after large disturbances. The last, partial stability, is effective in classifying power system stability into the different aforementioned categories. In this work, we concentrate on stability of linear systems, which is often utilized for small-signal stability analysis in power systems. The classification of power system stability with the described categories and types is visually represented in Figure 3.3.

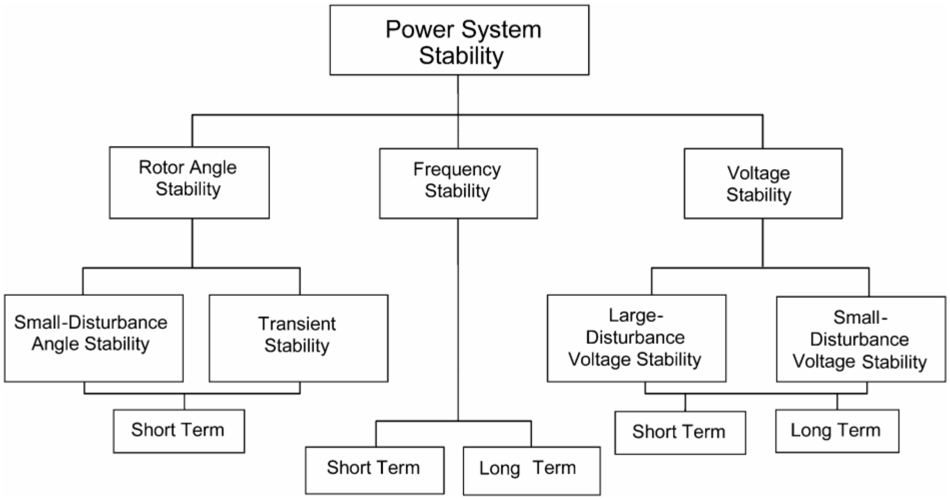


Figure 3.3: Types and categories of power system stability considering time spans [52].

To develop effective control defense strategies, as will be detailed in this dissertation, we must consider stability in our formulation. Power system stability is complex; strategies to mitigate or eliminate instability are complicated and require intensive formulation and study beyond the scope of this work. However, it is recognized that the stability of the system, under distributed controller compromise of failure, must be considered and monitored within the developed strategies that seek to maintain system controllability. In this manner, we apply linear system stability concepts to evaluate the state of the system in regards to stability and, if instability arises, alert operators to take appropriate action and/or apply suitable stability mitigation strategies.

3.3.2 Cyber Attacks and the Evaluation of Stability

Amini et al. utilized linear system stability to evaluate dynamic load altering attacks (D-LAA) against power system stability in [53]. Power system cyber attacks target the generation sector, distribution and control sector, and the consumption or load sector. Their work focused on the latter, in which demand response (DR) programs that are used by utilities to control the load at the user side of the meter in response to grid condition changes are a prominent target. A D-LAA consists of an adversary attempting to control and change a group of remotely accessible and unsecured controllable loads in order to damage the system through circuit overflow or other mechanisms [53]. The changes enacted by the D-LAA are not only in the amount of load, but also in the dynamic trajectory of the load over time. The attack is based on feedback from power system frequency.

The authors formulate and analyze a closed-loop D-LAA against power system stability using feedback frequency. Subsequently, a protection scheme is designed against various types of D-LAA by formulating and solving a non-convex pole placement optimization problem. The objective is to minimize the total vulnerable load that must be protected to assure power system stability under D-LAAs against the remaining unprotected vulnerable loads. Details on this optimization problem and D-LAA characterization are provided in the full paper [53].

Essentially, the protection scheme identifies which loads must be protected—the critical loads. In this manner, with those critical loads (the minimum amount) protected, power system stability is assured under D-LAAs against the remaining unprotected vulnerable loads. The stability is assessed by checking that the poles of the system remain in the left half plane (LHP) during D-LAA attacks on unprotected vulnerable loads [54]. The system is closed-loop system stable if there exists a symmetric positive semi-definite matrix satisfying the inequality conditions. Using coordinate descent method, the results identify the fraction of loads that need to be protected to maintain stability. An example result for the IEEE 39-bus system is shown in Figure 3.4.

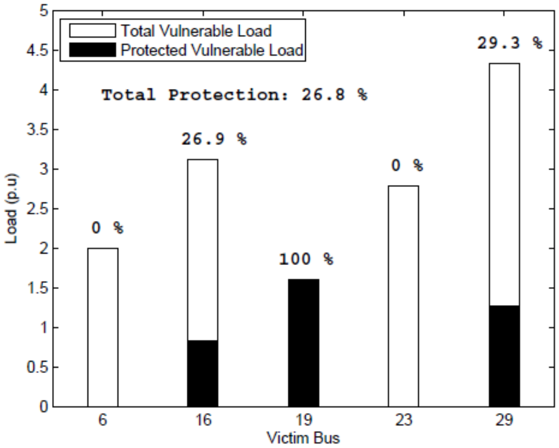


Figure 3.4: Optimal load protection scheme for IEEE 39-bus system [53].

Therefore, identifying the critical loads and the fraction that needs to be protected to maintain the loads is achieved by examining the linear system model. In particular, the poles of the system are studied and the solution approach is to “backsolve” for the vulnerable load amount settings.

3.4 Key Points

Moving forward, the key takeaways and points to address are:

1. The effective placement of distributed controllers to achieve flexible control within the power system is significant and warrants the development of accurate and scalable techniques.

2. Given the sited distributed controllers, the impact of distrusted, compromised controllers and subsequent defense mechanisms are necessary to study.

    - Insights into the roles of the distributed controllers and their contributions to system controllability and interactions with one another are needed.

  - Such information can benefit control response strategies to mitigate and minimize compromise consequences.

- Nonlinear controllability analysis provides the most robust analysis but is intractable for realistic cases of bounded control.
- Linear controllability analysis offers more computationally efficient and widely applicable results for a broad class of systems.

3. When developing control defense strategies, the impact on both system controllability and stability must be considered.

   - There are various categories and types of stability that must be appropriately chosen for study depending on the application.
   - Strategies to mitigate or eliminate instability, which are beyond the scope of this work, are complicated and require intensive formulation; stability assessment needs to be included.
   - Protection schemes are being developed to protect power system stability from cyber attacks but mostly concentrate on the planning stage to reduce vulnerability.

4. Proactive defense requires real-time analysis, but to eliminate any malicious control actions (no allowance of "minimal"), verification of the control commands before execution is required.

   - As the power grid is a cyber-physical system, the control commands must be examined from the points of view of both the cyber and physical layers.

CHAPTER 4

DISTRIBUTED CONTROLLER ROLE AND INTERACTION DISCOVERY

4.1 Problem Statement

The smart grid initiative has driven the industry toward increasingly sophisticated systems of sensors, algorithms, and controllers that are involved in widespread communications and online decisions in power systems. Distributed controllers play a prominent role in deploying this cohesive execution and are ubiquitous in their presence in the grid. As discussed previously, global information is shared and acted upon; if one distributed controller fails, the remaining set is quick to respond and ensure the overall control objective is maintained. However, multiple failures can cause detrimental, cascading effects (e.g., overloads leading to blackout) as the set struggles to automatically meet the control goal. Furthermore, if the controllers are maliciously compromised, they can be manipulated to drive the power system to an unsafe or unreliable operating state. Attack vectors for distributed controllers range from execution of malicious commands that can cause damage, to sensitive equipment, to forced system topology changes causing instability.

In this regard, distrusted control can be defined as when controller(s) from the complete set are compromised and under the command of a sophisticated attacker. This adversary can craft these commands in a legitimate format and thus have them successfully executed in the system. Furthermore, these alterations could be masked to the operator or any security systems. Cyber attacks on the power grid are a serious issue, with about 40% of total critical infrastructure cyber incidents reported to the Department of Homeland Security from 2009 to 2014 occurring in the energy sector [55]. In fact, one of the first large-scale attacks on a power grid occurred in December 2015 in Ukraine, where cyber attacks led to the disconnection of 7 substations and power outage to 225,000 customers for several hours [56]. If not dealt with swiftly, these attacks can have a high cost to society and can cause serious damage [57]. Additionally, the threat of physical consequences resulting from these cyber attacks has become a serious concern, as demonstrated by [11,12]. Hence, security of the corresponding control systems is critical to trustworthy grid operation as well as national security and public safety.

In preventing and mitigating these attacks, specifically on distributed controllers, we must consider: the attack vectors, adversary capabilities, trusted entities, and impact on system controllability and stability. With the modern power grid increasingly being outfitted with publicly available operating systems, network or Internet communication, and third-party software, there are many more access points for an attacker to gain entry. We no longer have the benefit of "security by obscurity" as historically achieved by proprietary control protocols that varied utility to utility – the adversary no longer needs to be deeply knowledgeable of the specific utility system to launch a successful attack [5].

In this chapter, we focus on attacks which disrupt system control resulting from compromised or failed distributed controller(s). As mentioned, controller-based threats include execution of malicious control commands as well as changes to controller-level code and binaries which may drive the system to an unsafe or unreliable operating state. In particular, this work provides an analytic solution to help restore the control capability of a system given a controller attack. By identifying the role of each controller, whether they are critical, essential, or redundant to system controllability, we can develop powerful techniques to improve control as well as protect the system. Furthermore, discovering the control support groups that indicate the interaction of the controllers with one another provides useful information. This insight can allow development of systematic method(s) to ensure or regain control of the system given compromise or failure. A control response algorithm using the remaining, uncompromised controllers is provided in Chapter 5.

4.2 Power System Controllability

As discussed in Section 3.1, the controllable region is the subset of the state space on which the available controls can be used to steer the power system from one state to any other state [30]. In general, the power system dynamical equation can be written as:

$$\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}) + \sum_{i=1}^{m} \mathbf{g_i}(\mathbf{x})u_i, \ \mathbf{x} \in \mathbf{\Xi} \tag{4.1}$$

where $\mathbf{x}$ is an n-vector of dynamic variables (e.g., generator rotor angles), $\mathbf{f}(\mathbf{x})$ is a vector consisting primarily of the power flow equations, and $\sum_{i=1}^{m} \mathbf{g_i}(\mathbf{x})u_i$ represents the effects of the controls on the system. The scalars $u_i, \ i = 1, ..., m$, are the system controls (e.g., generator mechanical power injections) and are usually piece-wise constant in time, due to device physical characteristics. System state space, $\mathbf{\Xi}$, is an open subset of the n-dimensional Euclidean space. If we have $X(s_1, u, t) \in \mathbf{\Xi}$ representing the system movement with the initial state s_1, control u, and $0 \leq t \leq \infty$, the controllable region satisfies:

$$X(s_1, u, t) = s_2, \ u \in \mathbf{U} \text{ and } 0 \leq t \leq \infty \tag{4.2}$$

where every pair of states s_1 and $s_2 \in \mathbf{Z}$ satisfies (4.2). $\mathbf{Z}$ is the controllable region, a subset of $\mathbf{\Xi}$. Therefore, the system presented in (4.1) can be steered from a state to any other state within the controllable region. Further proofs and other references can be found in [30]. For this work, we will focus on decomposing the set of controls $\sum_{i=1}^{m} \mathbf{g_i}(\mathbf{x})u_i$ into the controller role and control support group sets.

4.2.1 Controllability Analysis Techniques

Classic linear methods developed for controllability and observability are the Popov, Belevitch, and Hautus (PBH) eigenvector tests using rank conditions [32]. Yet, these tests only provide answers in a "yes or no" fashion—e.g., yes the system is observable or no, the system is not observable. Although useful, more detailed measures of controllability (or the dual, observability, as discussed in Section 4.2.2) are desired.

Hamdan and Elabdalla [33] and Hamadan and Nayfeh [34] proposed using the cosine of the angle between appropriate subspaces to develop a quantified measure for controllability and observability of linear systems. Given the linear system

$$\dot{\mathbf{x}} = \mathbf{Ax} + \mathbf{Bu}; \quad \mathbf{y} = \mathbf{C^T x} \tag{4.3}$$

where the left eigenvectors of $\mathbf{A}$, $\mathbf{q_i}$, and columns of $\mathbf{B}$, $\mathbf{b}$, are used to calculate the controllability measure,

$$cos[\theta(\mathbf{q_i}, \mathbf{b})] = \frac{|\mathbf{q_i}^{\mathbf{T}}\mathbf{b}|}{\|(\mathbf{q_i})\|\|\mathbf{b}\|} \tag{4.4}$$

In this manner, the measure is a continuous function of the distance between the two subspaces. Thus, instead of the pass/fail controllability result per mode as provided by the classic PBH eigenvector tests, a measure for the range of controllability is achieved. Further work by Hamadan and Nayfeh [34] demonstrated joint measures of controllability and observability and generator coherency relations.

Messina and Nayebzadeh [36] formulated a design procedure using modal analysis to derive quantitative controllability and observability measures to place multiple controllers. To check if the controllability or observability matrices, $\mathbf{A}$ or $\mathbf{B}$ in (4.3), are full rank, they examined the number of nonzero singular values. Thus, the magnitude of the nonzero minimum singular value (MSV) is used to measure how far the matrix is from a matrix of lower rank. Further details on these methods as well as nonlinear controllability analysis are provided in Section 3.1. Nonetheless, our proposed methodology delves into the relationships *between* the controllers to determine control support groups and, with the subsequent placement, extends to identifying critical and essential controllers that ensure system controllability.

4.2.2 Observability Analysis Techniques of Interest

Unlike controllability, system observability analysis has been investigated in the cyber security context, particularly data attacks. A system is observable if at time t_0 there exists a finite time $t_1 > t_0$ such that for any initial state s_0 at t_0, knowledge of the input $u(t)$ and the output $y(t)$ for $t_0 \leq t \leq t_1$ suffices to determine s_0. Observability and controllability are dual concepts; if the dual of system is observable, the original system is controllable. Conversely, the original system is observable if and only if the dual is controllable [58].

Bobba et al. [59] explored the detection of false data injection attacks. They identified a set of basic measurements to protect what is necessary and sufficient for detecting such attacks and ensuring system observability. The system measurements were mapped to a new equivalent state space where lower-upper (LU) matrix decomposition was applied to determine the sets of basic and redundant measurements, as in [60]. Kosut et al. [61] studied malicious data attacks and developed a graph-theoretic security index to find the smallest set of attacked meters capable of causing network unobservability. Both papers focus on observability, essential in protecting against data attacks on sensors. However, these analyses do not extend to and are inadequate when dealing with system actuation and compromised controllers. Controllability analysis must be applied to gain the necessary insights into protecting against loss of system control.

4.3 Solution Overview

In this chapter, we focus on distributed control devices and the impact of compromised controllers on system controllability within a cyber-adversarial environment. We study how to determine the amount of flexibility and redundancy of control available for any given power system topology and controller configuration. Similar to the work of Bobba et al. [59] that determined the sets of basic and redundant measurements, we seek to motivate and invoke the use of these and other observability-based methods to also study control. Using clustering and factorization techniques, the proposed work identifies the essential and critical controllers for maintaining controllability of the system as well as the redundant ones. With this classification, the compromise of controllers can be analyzed to determine how the remaining controllers should react to restore the system to its normative state.

- *Critical controllers* ($\mathbf{g}_{\mathbf{C}_\mathbf{i}}(\mathbf{x})\mathbf{u}_{\mathbf{C}_\mathbf{i}}$): devices that are irreplaceable and mandatory for system controllability

- *Essential controllers* ($\mathbf{g}_{\mathbf{E}_\mathbf{i}}(\mathbf{x})\mathbf{u}_{\mathbf{E}_\mathbf{i}}$): minimal set of devices required to maintain system controllability

- *Redundant controllers* ($\mathbf{g}_{\mathbf{R}_\mathbf{i}}(\mathbf{x})\mathbf{u}_{\mathbf{R}_\mathbf{i}}$): devices that can be removed without affecting system controllability

Our method performs power system controllability analysis to provide an analytical solution to restore or maintain system control given a controller attack. Specifically, the controlled dynamical power system (4.1) can be described with each controller identified as critical, essential, or redundant:

$$\begin{aligned}\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}) &+ \{\mathbf{g}_{\mathbf{C_1}}(\mathbf{x})u_{C_1} + \mathbf{g}_{\mathbf{C_2}}(\mathbf{x})u_{C_2} + ... + \mathbf{g}_{\mathbf{C_{TC}}}(\mathbf{x})u_{C_{TC}}\} \\ &+ \{\mathbf{g}_{\mathbf{E_1}}(\mathbf{x})u_{E_1} + \mathbf{g}_{\mathbf{E_2}}(\mathbf{x})u_{E_2} + ... + \mathbf{g}_{\mathbf{E_{TE}}}(\mathbf{x})u_{E_{TE}}\} \\ &+ \{\mathbf{g}_{\mathbf{R_1}}(\mathbf{x})u_{R_1} + \mathbf{g}_{\mathbf{R_2}}(\mathbf{x})u_{R_2} + ... + \mathbf{g}_{\mathbf{R_{TR}}}(\mathbf{x})u_{R_{TR}}\}\end{aligned} \tag{4.5}$$

where $\mathbf{x} \in \Xi$ and C_1 to C_{TC} represents the critical controllers where TC is the total number. Similarly, E_1 to E_{TE} represents the essential controllers where TE is the total number and R_1 to R_{TR} represents the redundant controllers where TR is the total number.

Figure 4.1 shows the high-level architecture of the proposed method. The algorithm uses clustering and factorization along with sensitivity analysis and provides a general power grid controllability analysis that can be applied to any control parameters and any deployed controller devices (only the appropriate sensitivities are required).

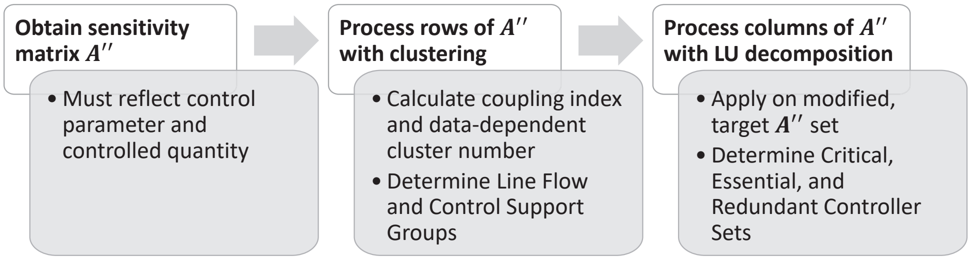

Obtain sensitivity matrix A''
• Must reflect control parameter and controlled quantity
Process rows of A'' with clustering
• Calculate coupling index and data-dependent cluster number
• Determine Line Flow and Control Support Groups
Process columns of A'' with LU decomposition
• Apply on modified, target A'' set
• Determine Critical, Essential, and Redundant Controller Sets

Figure 4.1: Proposed methodology that applies clustering and factorization methods to process controller sensitivities.

In the following sections, we provide the details on the methodology using clustering and factorization techniques. The algorithms calculate and process the sensitivities to determine the control support groups.

- *Control support groups*: the controllers that are highly coupled for impact on both the control objective and each other

Controller coupling is discussed further in Section 4.5. For example, given 8 controllers (one on each transmission line in an 8-line system), we can describe the system using the control support groups:

$$\begin{aligned}\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}) + \overbrace{\mathbf{g_1}(\mathbf{x})u_1 + \mathbf{g_4}(\mathbf{x})u_4}^{\text{GROUP 1}} + \overbrace{\mathbf{g_3}(\mathbf{x})u_3 + \mathbf{g_6}(\mathbf{x})u_6 + \mathbf{g_8}(\mathbf{x})u_8}^{\text{GROUP 2}} \\ + \overbrace{\mathbf{g_2}(\mathbf{x})u_2 + \mathbf{g_5}(\mathbf{x})u_5 + \mathbf{g_7}(\mathbf{x})u_7}^{\text{GROUP 3}}\end{aligned} \tag{4.6}$$

Each of the square bracket pairs, $GR1 - GR3$, embodies a control support group—there are 3 in total. In this case, we achieve information on which controllers work most effectively together on controlling a specific group of transmission lines. Using these grouping results, a target set of lines/devices can be determined that encompass the necessary control, one from each independent group. This target set's sensitivity matrix is then analyzed to determine the critical, essential, and redundant sets of controllers. Further insight into the use of these results will be detailed throughout the chapter, specifically Section 4.8. The novel contributions of this work are as follows:

1. Determining controllability-equivalence sets, the control support groups, via clustering
2. Computing the number of equivalence sets (clusters) using a novel sensitivity-based method
3. Identifying the critical, essential, and redundant controller sets via factorization

4.4 Leveraging Sensitivities

A system's sensitivity matrix ($\mathbf{A}''$ in Figure 4.1) is often used for robust control to ensure controller parameters are chosen in such a way that the closed loop system is not sensitive to variations in process dynamics [62]. With such sensitivity information, placement of the control devices to achieve various objectives is facilitated as well as details on the impact of compromised controllers on overall system controllability.

For our application, we require knowledge of the independently controllable lines as well as the controller role sets. The sets of those lines can be defined as:

- *Line flow groups*: the sets of transmission lines that can be controlled independently

The control support groups, as defined in Section 4.3, provide the corresponding control. To obtain these groups, we cluster the rows of the sensitivity matrix and then investigate which lines are most affected by each other as well as those that are not and have no relation. Additionally, we decompose the transposed sensitivity matrix to determine the critical, essential, and redundant sets of controllers.

The appropriate sensitivities to be utilized depend on the control device and objective. To exemplify the framework, we use distributed flexible AC transmission system (D-FACTS) devices. The versatile array of D-FACTS devices for power flow control includes distributed series reactors (DSRs) and distributed static series compensators (DSSCs), and is currently deployed by SmartWires Inc. [63,64]. We focus on DSSCs in this work, but are motivated by the flexibility of D-FACTS and the various sensitivities that can be derived. The results presented in this chapter will be broadly useful and clearly indicate how any controller and control objective may be interchanged. This controller acts as a synchronous voltage source in series with the line, changing the line's effective impedance and thus its power flow [64–66]. Therefore, we concentrate on sensitivities considering power flows. Specifically, we use the total power flow to impedance sensitivity matrix. It reflects both direct (i.e., change in impedance of a line and its direct impact on that line's power flow) and indirect (i.e., change in impedance of a line and its indirect impact on all other lines' power flows) sensitivities. This sensitivity matrix is represented as $\mathbf{\Omega}$.

$$\Delta \mathbf{P}_{\mathbf{flow.total}} = [\mathbf{\Omega}] \cdot \Delta \mathbf{x} \tag{4.7}$$

where $\Delta \mathbf{P}_{\mathbf{flow.total}}$ are the changes in the line power flows and $\Delta \mathbf{x}$ are the impedances. Including the indirect power flow sensitivities in the calculation of $\mathbf{\Omega}$ allows the representation of the impact of lines on all other lines, which is very useful for our analysis in determining line flow groups. Nonetheless, other sensitivity matrices can be used depending on the desired application; further sensitivity formulations for D-FACTS devices are developed in [67].

With the calculated sensitivity matrix, we can apply clustering to determine the control support and line flow groups. The matrix is represented as $\mathbf{A}''$ in Figure 4.1. It is important to note that the algorithms presented

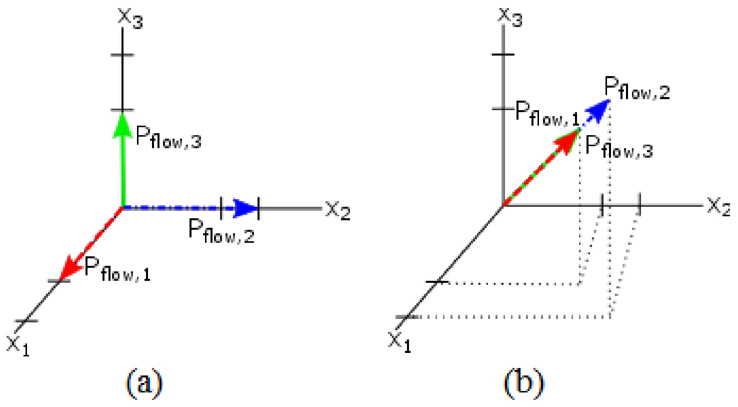


Figure 4.2: Completely decoupled line flows (a) and completely coupled line flows (b) [67].

in this work are applicable to any controller and control objective; only the appropriate sensitivity matrix needs to be selected, or more precisely, one that reflects the controlled quantities and the control objective.

4.5 Controllability-Equivalence Sets

By obtaining sets of line flows that can be independently controlled with respect to other sets in a system, we can gain valuable insight on the influence of various controllers and the control support groups. Identifying these line flow groups is a key step in achieving comprehensive power flow control. Within each set, it only makes sense to control one line flow, as they are all highly coupled given the power system topology; controlling one line flow will always strongly impact the others in a predictable way. The example application is the placement of D-FACTS devices, where the goal is to achieve the most comprehensive control over the greatest number of lines.

4.5.1 Control Support Groups

To provide the most complete and effective control for the entire system, it is necessary to identify how the controlling of different line flows are related to each other by determining the control support groups [67]. We can study a trivial example shown in Figure 4.2 where line flow vectors are illustrated as completely coupled or decoupled. When the vectors are orthogonal, the line flows are completely decoupled as shown in Figure 4.2(a.), and can be controlled independently. Conversely, in the completely coupled case in Figure 4.2(b.), the row vectors are aligned and the angle between them is 0°. When line flows are highly coupled, only one needs to be controlled, as the others will respond as well. Independent control of those lines cannot be achieved. When the row vectors are exactly aligned but point in opposite directions (angle of 180°), the lines are still completely coupled [67].

The ability of certain lines to exhibit this independently controllable property is discernible from the relationships in the sensitivities. We can compare the cosine of the angles between vectors and determine the coupling sets. Subsequently, grouping of line flows can be determined using any appropriate clustering algorithm.

4.5.2 Coupling Index

We leverage the line flow vector angle relationships, to determine the controllability-equivalence sets by comparing the angles between row vectors of the sensitivity matrix to find the coupled and decoupled sets of lines flows. To calculate and compare these angles, we utilize the coupling index (CI) and measure the cosine similarity [68]. The CI is equal to the cosine of the angle between two row vectors, $\mathbf{v_1}$ and $\mathbf{v_2}$, of the sensitivity matrix $\mathbf{A}''$ as in (4.8).

$$cos\theta_{\mathbf{v_1}\mathbf{v_2}} = \frac{\mathbf{v_1} \cdot \mathbf{v_2}}{\|\mathbf{v_1}\|\|\mathbf{v_2}\|} \tag{4.8}$$

The clusters identified using the CI are approximately orthogonal to each other. The CI has values between -1 and 1. By clustering on the rows of the sensitivity matrix using CI, the coupled and decoupled sets of line flows can be determined. Thus, each cluster will be independent and decoupled from the other sets. Within the cluster, the line flows are coupled and dependent on one another.

4.6 Number of Clusters

Our solution will determine the controllability-equivalence sets through clustering using the coupling indices, CI, calculated from the sensitivity matrix.

A well-known challenge for clustering algorithms (i.e., k-means or k-mediods) is the selection of the number of clusters k [69, 70]. For our application, it is difficult to arbitrarily select k as it will change on a system by system basis. We want to find the clusters that most accurately reflect how we can effectively control lines that are either highly dependent on or independent of each other. Thus, we require highly cohesive clustering.

We chose to use hierarchical agglomerative clustering as it groups data by creating a cluster tree or dendogram. The goal was to avoid strict manual selection of k. When cutting the hierarchical tree into clusters, the algorithm requires either a cutoff value c (where to cut the tree) or maximum threshold value k_m for the number of clusters to form [71]. Thus, even if we assign k_m, it provides a maximum number of clusters rather than a strict rule to form exactly (possibly non-optimal number of) k clusters as in k-means. The proposed framework implements a solution based on the sensitivity matrix to determine the number of most significant clusters that represent controllability-equivalence sets.

4.6.1 Sensitivity-based Threshold

The controllability-equivalence set methodology computes the coupling indices that indicate the cosine similarities between lines. In this section, we describe our method of deriving k_m from the system sensitivities so that we can achieve the most suitable clustering for the line flow groups.

To leverage the sensitivity matrix and its inherent groupings, singular values are studied and are computed using singular value decomposition (SVD). The SVD of a $m \times n$ matrix $\boldsymbol{A}$ is

$$\mathbf{A} = \mathbf{U\Sigma V^T} \tag{4.9}$$

where $\mathbf{U}$ is a $m \times m$ orthogonal matrix, $\mathbf{V}$ is a $n \times n$ orthogonal matrix, and $\mathbf{\Sigma}$ is a $m \times n$ diagonal matrix with the singular values listed in decreasing order [72, 73]. The method applies SVD to obtain a rank reduced approximation of a data set to generalize some properties or structure. One interpretation of the singular values is information on the largest contributions to the matrix and its general structure. Therefore, the most significant or largest singular values represent the most significant groups present in the data, which in our case is the sensitivity matrix.

Using the number of most significant singular values from the sensitivity matrix, we can achieve an initial guess for the number of clusters and for our choice of hierarchical clustering threshold, i.e., k_m. To determine which singular values are most significant, our methodology calculates an *optimal hard threshold* using the techniques detailed by Gavish and Donoho [74]. Henceforth, we will call their algorithm the *hard threshold singular value* (HTSV) method. HTSV considers the recovery of low-rank matrices from noisy data by hard thresholding singular values. The HTSV thresholding rules adapt to unknown rank and noise level in an optimal manner and provide better results than truncated SVD (TSVD) [75].

For a nonsquare $m \times n$ matrix with an unknown noise level, the optimal threshold value $\hat{\tau}^*$ is:

$$\hat{\tau}^* = \omega(\beta) \cdot y_{med} \tag{4.10}$$

where y_{med} is the median singular value of the data matrix $\mathbf{Y}$ and the optimal hard threshold coefficient is dimension-dependent ($\beta = \frac{m}{n}$) and calculated using a numerical formula, $\omega(\beta)$. If the matrix is square, $\omega(\beta)$ is simply replaced by $\frac{4}{\sqrt{3}}$ [74]. The final result is not a fixed threshold chosen *a-priori* but a data dependent threshold, which is preferred in our case.

4.6.2 Silhouette-Based Refinement

With the number of singular values from the sensitivity matrix that satisfy the hard threshold, an initial minimum number of clusters k_{in} is found. Since we seek high cohesiveness within our clusters for effective control, we then iterate on k_{in} by evaluating (1) sil_{CV}, the coefficient of variance (the ratio of standard deviation to the mean) and (2) sil_{avg}, the average of the resultant cluster's silhouette values for k_{in}. Satisfying these conditions, low sil_{CV} and high sil_{avg}, ensures the objects within the clusters are well-matched and cohesive.

The silhouette technique is used to evaluate how well each object lies within its cluster. That is, silhouettes compare how similar an object is to the other objects in its cluster when compared to the objects in other clusters. The silhouette value, sil_i for the i-th object, ranges from -1 to 1; thus, the closer sil_i is to 1, the more well matched it is to its own cluster and poorly-matched to neighboring clusters [76].

By iterating on k_{in} and satisfying the above mentioned conditions to achieve highly cohesive clusters, we obtain k_f to input as the final maximum number of clusters k_m for the hierarchical clustering or as k for other methods. This process is illustrated in Figure 4.3.

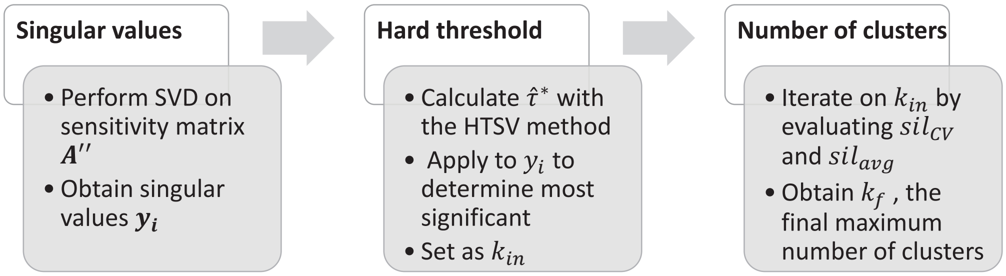

Singular values
• Perform SVD on sensitivity matrix $\boldsymbol{A}''$
• Obtain singular values $\boldsymbol{y_i}$
Hard threshold
• Calculate $\hat{\tau}^*$ with the HTSV method
• Apply to y_i to determine most significant
• Set as k_{in}
Number of clusters
• Iterate on k_{in} by evaluating sil_{CV} and sil_{avg}
• Obtain k_f , the final maximum number of clusters

Figure 4.3: Cluster number selection calculated using the sensitivity matrix singular values and sil_{avg}, sil_{CV} results.

4.7 Critical, Essential, and Redundant Controller Sets

With the resultant control support and line flow groups, the power grid operators and security administrators can specify the number of controllers to consider as well as an objective for each group of interest. The devices can be placed for maximum controllability such that the most independent controllability of groups is achieved. A target set of lines can be derived, as only one line from each independent group needs to be controlled. Hence, the target set is analyzed to discover the critical, essential, and redundant sets of controllers.

Consequently, the protection of critical controllers would be necessary in maintaining system controllability. If a controller from any set is compromised, we can determine how to recover the system controllability using controllers from its support group. This requires examining the coupling of the columns of the sensitivity matrix (of the target set), henceforth generally labeled as $\mathbf{A}''$, or the rows of $[\mathbf{A}'']^{\mathbf{T}}$, to identify candidate lines with the best spread (linearly independent) to meet the objective.

As mentioned previously, such as the work by Bobba et al. [59], detailed observability analysis has been investigated by many research groups. Particularly, Chen and Abur [77] defined a *critical* measurement as one whose elimination from the measurement set results in an unobservable system.

A similar methodology can be applied to identify critical controllers as well. We apply the analysis on our sensitivity matrix to study controllability, the dual of observability. The idea is to perform a change of basis to obtain a mapping from measurements to equivalent states. Instead of using this decomposition to examine the redundancy of measurements for estimating states, we use it to examine the set of control devices needed to control equivalent line flows. Define $[\mathbf{A}^{''}]^{\mathbf{T}}$, where the rows correspond to control devices and columns correspond to the variable being controlled. For simplicity, we continue to use the example of D-FACTS devices with columns corresponding to the real power flows to be controlled. Again, we only consider the real power flows of the target set of lines, as determined from the clustering results.

LU factorization is applied to obtain the change of basis, decomposing the transposed sensitivity matrix to lower and upper triangular factors; [78] describes the LU factorization method. The following decomposition of $[\mathbf{A}^{''}]^{\mathbf{T}}$ is obtained as:

$$[\mathbf{A}^{''}]^{\mathbf{T}} = \mathbf{P^{-1}L_F U_F} \tag{4.11}$$

$$\mathbf{L_F} = \begin{bmatrix} \mathbf{L_b} \\ \mathbf{M} \end{bmatrix} \tag{4.12}$$

Using the Peters-Wilkinson [78] method, we are able to decompose $[\mathbf{A}^{''}]^{\mathbf{T}}$ into its factors, where $\mathbf{P}$ is the permutation matrix and $\mathbf{L_F}$ and $\mathbf{U_F}$ are the lower and upper triangular factors of dimension n, respectively. M is a sparse, rectangular matrix with rows corresponding to redundant controllers. The new basis has the structure:

$$\mathbf{L_{CER}} = \mathbf{L_F L_b^{-1}} = \begin{bmatrix} \mathbf{I_n} \\ \mathbf{R} \end{bmatrix} \tag{4.13}$$

The new basis, shown in (4.13), must be full rank for a controllable system and this requires the $m \times (n-1)$ matrix to have a column rank of $(n-1)$ to be a controllable n-bus system with m-measurements. Since $\mathbf{L_F}$ and $\mathbf{U_F}$ will be nonsingular for a controllable system, the rank of $[\mathbf{A}^{''}]^{\mathbf{T}}$ can be confirmed by checking the rank of the transformed factor $\mathbf{L_{CER}}$. Also, $\mathbf{L_F}$ has full rank and with (4.13) multiplied by $\mathbf{L_b^{-1}}$ from the right, the row identities will be preserved in the transformed matrix $\mathbf{L_{CER}}$. Each row of the matrix will, therefore, correspond to the respective controllers [77].

Rows of $\mathbf{I_n}$ correspond to essential controls that are sufficient to assure independent controllability of the equivalent line flows. If the essential controller is the only non-zero entry of an equivalent line flow column, it is the *only* controller that can control it and is irreplaceable. There is only one entry for that line flow and it is in $\mathbf{I_n}$. Thus, the control corresponding to that row in $\mathbf{I_n}$ is critical, since that equivalent line flow cannot be independently controlled by any of the other devices. Rows of $\mathbf{R}$ correspond to redundant controls. These roles were defined in Section 4.3. Columns correspond to the equivalent flows which can easily be mapped back to the original flows using the permutation matrix $\mathbf{P}$ obtained from the LU decomposition step.

4.8 Evaluations

The proposed methodology to discover the distributed controller role and interaction (controllability-equivalence sets) was tested on several systems, as presented in this section. Detailed results are provided with the small, 7-bus system to exemplify the algorithms, and overall results are provided for two large systems to demonstrate scalability and utility.

4.8.1 PowerWorld 7-bus System

We first evaluate a 7-bus system with 5 generators and 11 lines that is modeled in PowerWorld as the *B7 DFACTS DEMO* case [79]. For this study, we assume the controllers are D-FACTS devices whose control objective is to change line flows by changing the effective impedance of lines. We first perform an *a-priori* grouping of parallel lines. In this case, there are two parallel lines, lines 10 and 11. Whichever line flow group and critical or redundant set line 10 is placed in, line 11 is also in. We also exclude the transformers as D-FACTS controller placement options. Lastly, we posit there is a controller on every allowable line for simplicity, but this can be easily altered as well.

Using the total power flow to impedance sensitivity matrix $\mathbf{\Omega}$, discussed in Section 4.4, we compute the CI matrix to measure the cosine similarity between row elements of $\mathbf{\Omega}$. Next, we perform SVD on $\mathbf{\Omega}$ and obtain the

Table 4.1: Singular Values y_i of $\mathbf{\Omega}$

y_1	y_2	y_3	y_4	y_5	y_6	y_7	...
4.13	3.24	1.14	1.06	0.41	0.02	0.01	...

Table 4.2: Line Flow Grouping Clusters

Clus1	Clus2	Clus3	Clus4	Clus5	Clus6
L1, L2, L6, L8	L3, L4	L5	L7	L9	L10, L11

singular values, y_i, shown in Table 4.1 where y_8, y_9, and y_{10} are near zero.

With the calculated hard threshold $\hat{\tau^*} = 0.503$ for the $n \times n$ sensitivity matrix $\mathbf{\Omega}$, we find that 4 singular values satisfy this threshold. Therefore, we set $k_{in} = 4$ and then iterate on it to achieve the most accurate clustering with the coefficient of variance below 0.1 and the average silhouette value above 0.9. These are strict constraints that allow for cohesive clusters, as required for our application. In this manner, the number of clusters is increased to 6 so we set $k_m = 6$ and achieve our line flow groups. The resultant line flow groups, labeled Clus1-Clus6, are provided in Table 4.2.

Figure 4.4 displays the silhouette plots for varying maximum cluster number values (k_{in} to k_f) and Table 4.3 summarizes average silhouette values for the varying k_m. For comparison, we show the k-means clustering results as well.

These results indicate that hierarchical clustering performs the best for our application. Its accuracy increases consistently (unlike k-means) and also achieves the required threshold rapidly. As mentioned in Section 4.6.2, the closer sil_{avg} is to 1, the more accurate or well-matched the clustering is. Note that line 11 (parallel with line 10) is also included in the final results. The clusters are visually represented in Figure 4.5. The lines are colored according to cluster membership, a black line indicates only that line was in

Table 4.3: Average Silhouette Values

	$k_m/k = 4$	$k_m/k = 5$	$k_m/k = 6$
sil_{avg,k_m}	0.784	0.801	**0.969**
$sil_{avg,k}$	0.808	0.665	0.815

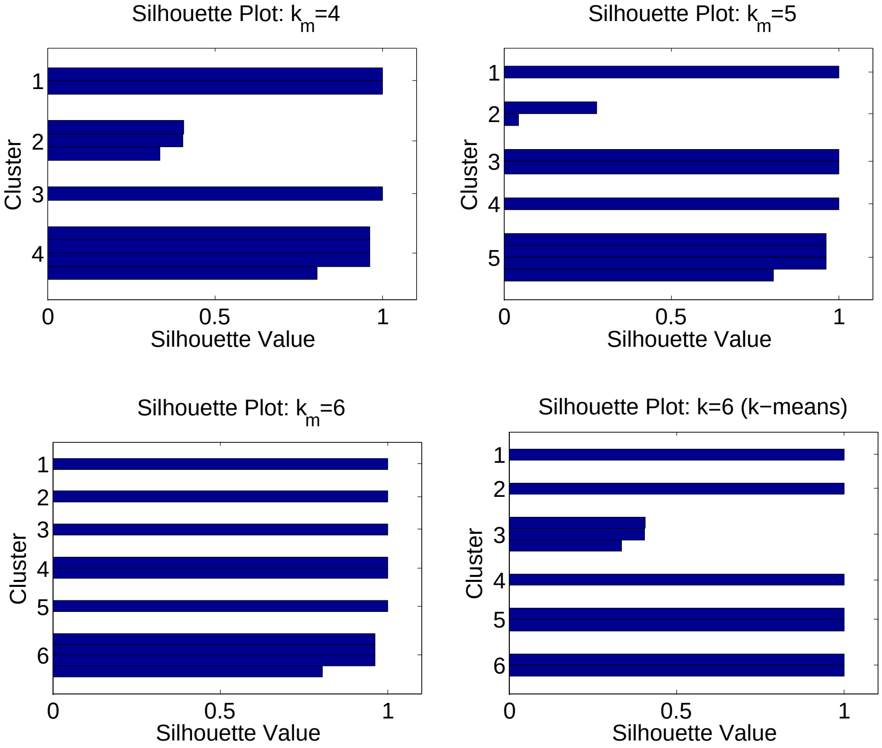


Figure 4.4: Silhouette plots for varying max cluster k_m and k-means k.

the cluster – not grouped with any other line.

Now that we have the line flow groups, we can determine the the critical, essential, and redundant sets of controllers. In fact, the cluster results can be used to determine the target set of lines. Only one line in each line flow group needs to be controlled, so one line from each cluster can be selected to be analyzed with the controller sets. For example, a target set of lines that encompasses control of the entire system can be $L1$, $L3$, $L5$, $L7$, $L9$, and $L10$ (L: line). By applying the decomposition method on the transposed sensitivity matrix, $[\mathbf{A}'']^{\mathbf{T}}$, comprised of the targeted lines and all possible controllers, we achieve the new basis $\mathbf{L_{CER}}$ shown in Table 4.4 and results provided in Table 4.5.

By examining Table 4.4, we can determine the critical, essential, and redundant controllers. An equivalent line flow column with only one non-zero entry, as highlighted for **EQ.L3**, has only one device that can control it and thus is a critical controller corresponding to row 3. The essential controllers are discovered by examining the first 6 rows ($\mathbf{I_n}$) and the remaining 4 rows ($\mathbf{R}$) correspond to redundant controls. We can, therefore, deduce that if

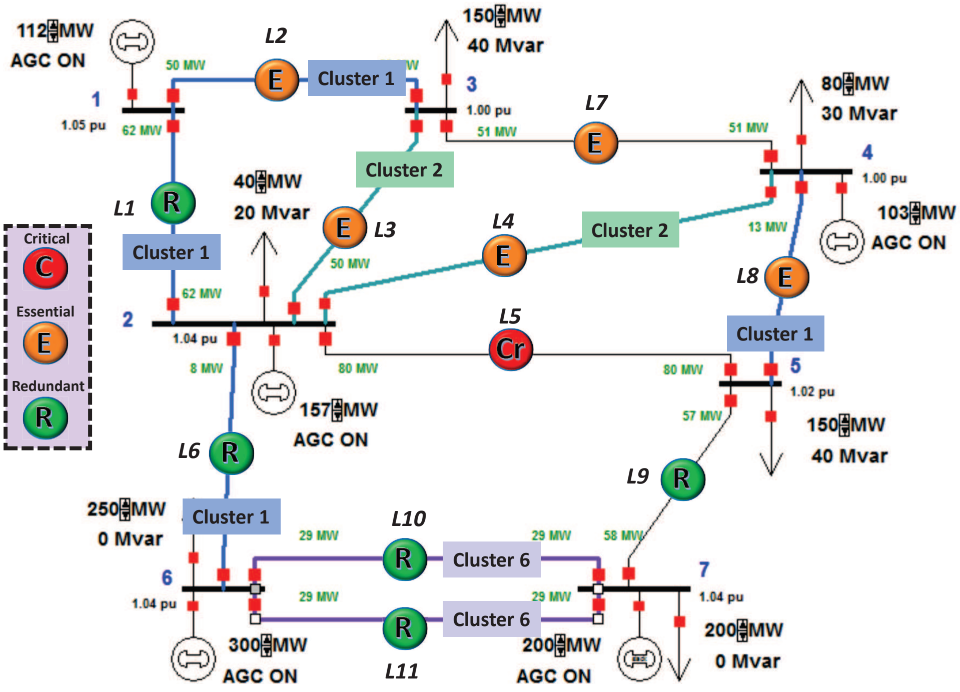


Figure 4.5: 7-bus case with lines colored according to cluster group and labeled with critical, essential, and redundant controllers.

Table 4.4: Transformed Basis

EQ.L1	EQ.L2	EQ.L3	EQ.L4	EQ.L5	EQ.L6
1.0000	0	0	0	0	0
0	1.0000	0	0	0	0
0	0	1.0000	0	0	0
0	0	0	1.0000	0	0
0	0	0	0	1.0000	0
0	0	0	0	0	1.0000
-0.0014	-0.0000	-0.0000	0.0899	-0.0000	-0.0000
-0.0144	0.0000	-0.0000	0.9227	-0.0000	-0.0000
0.0000	1.5107	0.0000	-0.0018	-1.0644	0.7466
-0.1250	-0.0000	0.0000	-0.1865	0.0000	-0.0000

Table 4.5: Critical, Essential, and Redundant Controller Sets

	Lines with Controllers
Critical Set	L5
Essential Set	L2, L3, L4, L7, L8
Redundant Set	L1, L6, L9, L10, L11

there are controllers on every line, the critical and essential controllers on lines 2, 3, 4, 5, 7, and 8 would provide full system controllability. The locations of the critical, essential, and redundant controllers for the 7-bus system are also illustrated in Figure 4.5.

Insights for Regaining Control

With these valuable results about the flexibility and redundancy of the control, we can effectively strategize regaining control of a given system after a controller attack. The resultant line flow grouping clusters and critical and redundant controller sets are shown in combination in (4.14).

$$\begin{aligned}\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}) + &\overbrace{\mathbf{g}_{\mathbf{R_1}}(\mathbf{x})u_{R_1} + \mathbf{g}_{\mathbf{E_2}}(\mathbf{x})u_{E_2} + \mathbf{g}_{\mathbf{R_6}}(\mathbf{x})u_{R_6} + \mathbf{g}_{\mathbf{E_8}}(\mathbf{x})u_{E_8}}^{\text{GROUP 1}} \\ &+ \overbrace{\mathbf{g}_{\mathbf{E_3}}(\mathbf{x})u_{E_3} + \mathbf{g}_{\mathbf{E_4}}(\mathbf{x})u_{E_4}}^{\text{GROUP 2}} + \overbrace{\mathbf{g}_{\mathbf{C_5}}(\mathbf{x})u_{C_5}}^{\text{GROUP 3}} + \overbrace{\mathbf{g}_{\mathbf{E_7}}(\mathbf{x})u_{E_7}}^{\text{GROUP 4}} \\ &+ \overbrace{\mathbf{g}_{\mathbf{R_9}}(\mathbf{x})u_{R_9}}^{\text{GROUP 5}} + \overbrace{\mathbf{g}_{\mathbf{R_{10}}}(\mathbf{x})u_{R_{10}} + \mathbf{g}_{\mathbf{R_{11}}}(\mathbf{x})u_{R_{11}}}^{\text{GROUP 6}}\end{aligned} \tag{4.14}$$

The following situations could arise and, with our insights from this analysis, we can respond in the corresponding manners:

#1 **Redundant Controller(s) Compromised**

If the controllers on $L1$ and $L9$ are compromised, we know from the clustered line flow groupings that for $L1$ controller, we can most effectively use the essential controllers in $GR1$ to best mitigate any adverse actions from $L1$ controller. The redundant controller on $L6$ can be used, additionally. Since no critical or essential controllers have been compromised, we still maintain full system control. We see that $L9$ controller is independently controlled (no other members in cluster), so perhaps we need the efforts of multiple, uncompromised controls to counter any malicious actions.

#2 **Critical or Essential Controller(s) Compromised**

If $L2$, $L5$, and $L8$ controllers are compromised, we know that $L1$ and $L6$ redundant controllers will be most effective in mitigating any actions of $L2$ or $L6$ essential controllers. However, since the critical controller on $L5$ is compromised, we do not have full system control. All other "safe" controller actions are necessary in trying to regain control of the system. This is true for $L5$ controller as well, especially since it has no other controls in its support group. If combination of critical, essential, and redundant controllers compromised, a similar response of utilizing all uncompromised system controls to regain system control is needed.

4.8.2 IEEE 118-bus and Synthetic Texas 2000-bus Systems

To further demonstrate utility and efficiency, two larger systems were tested: the IEEE 118-bus system (54 generators and 179 lines, excluding parallel lines and lines with transformers), shown partially with results in Figure 4.6 (full system cluster results shown in Figure A.1), and the Texas 2000-bus system case, shown in Figure 4.7, that is entirely synthetic, built from public information and a statistical analysis of real power systems (282 generators and 3043 lines) [80–82]. The system is color-coded according to areas (8 total) in Figure 4.7. The proposed methodology was evaluated with both cases and effectively provided the controller role and control support group (and line flow groups, continuing the D-FACTS devices example) results. The computation time of calculating the controller roles remained low, 0.009 s to 5.22 s, for all cases including the 7-bus system. The computation time for the clustering algorithm, to determine the control support groups, also was within a few seconds for the 7-bus and 118-bus cases but became excessive (16.16 min) for the 2000-bus case. This indicates the clustering algorithm must be improved with computation time in mind, which is within our future work. Currently, the iterative evaluation of the silhouette values during clustering is computationally burdensome. This aspect will be studied further to either improve upon (only evaluate periodically) or remove from the clustering process.

4.9 Conclusion

The presented methodology provides significant insight on how to best regain or maintain control given controller compromise or failure. We gain information on 1) the control support groups, the controllers that are highly coupled for both impact on the control objective and each other, 2) which controllers are critical and essential in maintaining system controllability, and 3) which controllers are redundant and can be managed more readily

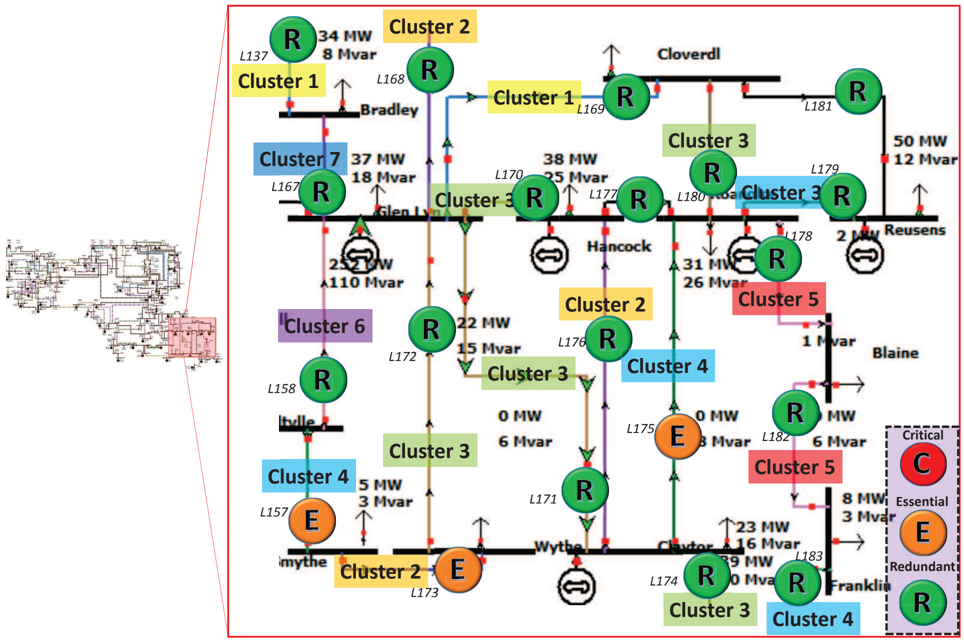


Figure 4.6: Partial 118-bus system where each line is colored according to cluster membership and labeled with critical (red), essential (orange), and redundant (green) controllers.

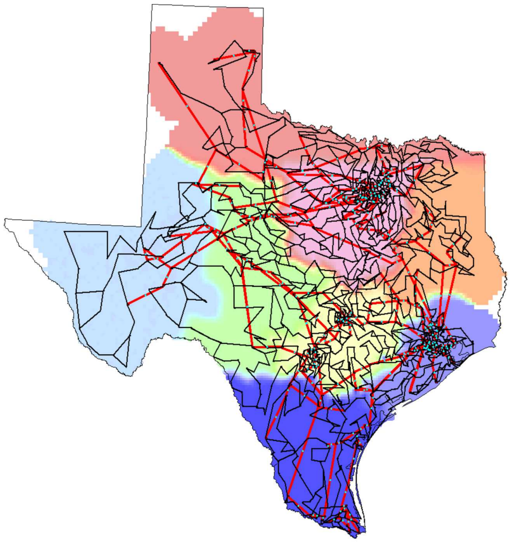


Figure 4.7: Synthetic Texas 2000-bus system [82].

if compromised. Thus, if a given controller in a redundant set is compromised, a set of essential and critical controllers can be used to restore the system and mitigate any adverse consequences. Conversely, if an essential or critical controller is compromised, immediate remedial actions are necessary as full system controllability is no longer maintained, especially for critical controller compromise.

These insights can allow for strategic protection schemes, as well as a prioritization of cyber (and physical) defense mechanisms surrounding critical and essential sets of controllers. System restoration strategies and further security measures on critical control points are aided significantly with the results of this analysis. In this dissertation, the controller role and group results are leveraged to develop a control response framework for the remaining set of distributed controllers after a compromise occurs. This is subsequently detailed in Chapter 5. Furthermore, the presented method can be applied to develop an analytic corrective control selection algorithm that can be used with remedial action schemes (RAS) to effectively respond to contingencies and significantly reduce computation time. The formulation and demonstration of the RAS application are provided in Chapter 6.

CHAPTER 5

PROACTIVE STRATEGIES FOR DISTRIBUTED CONTROLLER COMPROMISE

5.1 Application of Discovered Role and Group Results

The controllability analysis-based clustering and factorization methodology for distributed controller interaction and role discovery, presented in Chapter 4, provides two main results:

1. *Control support groups*: the controllers that are highly coupled for impact on both the control objective and each other; obtained by clustering the sensitivity matrix

2. The roles of each distributed controller in a given set; identified through factorization of the sensitivity matrix

    - *Critical controllers*: devices that are irreplaceable and mandatory for system controllability
    - *Essential controllers*: a minimal set of devices required to maintain system controllability
    - *Redundant controllers*: devices that can be removed without affecting system controllability

With these groups and roles identified, they can be utilized for distributed controller placement methods and control response strategies for compromise or failure. In this chapter, the transformed matrix presented in Equation (4.13) is deconstructed and studied to determine the composition of the equivalent line flows and ranking of the redundant controllers. With the decomposed composition of the equivalent line flows, placement strategies for distributed controllers can be improved. For example, if an essential controller becomes compromised, we know which original lines will be affected the most and can focus on recovering their control and minimizing overloads.

Subsequently, with the ranking of the redundant controllers and the main control support group and controller role results, strategies for responding to controller compromise or failure are developed. The D-FACTS controller example is continued from the previous chapters. Response strategies using D-FACTS are formulated for cases of compromise or failure of devices within the set. However, the D-FACTS compromise scenarios considered in this work do not have significantly detrimental impact on the power system, due to device limits. Although more severe scenarios can be developed by considering sophisticated, coordinated attacks, we demonstrate more detrimental scenarios with compromised generator outages.

In particular, generation redispatch calculated for power system remedial action schemes (RAS) after generator outage, from compromise or benign causes, is explored. After contingencies that result in stressed conditions in the power grid, corrective actions are deployed to prevent or mitigate system instability as well as maintain system reliability—these actions may be calculated and implemented with RAS. Cyber contingencies warrant fast, online RAS schemes, as they are difficult to predict and cannot be resolved using look-up tables.

The distributed controller role and interaction discovery methodology is employed to analytically determine the critical controls that would be most effective to use when designing automatic RAS. In this manner, the critical controls selected would reduce the contingency violations efficiently and ignore controls with minimal impact. Specifically, generation redispatch for RAS is studied, where the generators are the distributed controllers and the line real power flows are the controlled quantities. The aim is to reduce line overloads after a contingency has occurred using generator redispatch; this redispatch is calculated with the analytic corrective control selection. Chapter 6 presents the formulation and results for this work.

By exploring the application of the control support group and controller role results, for placement as well as control response, an overall framework for monitoring and governing power system distributed controllers is derived. This framework dictates the calculation of the roles and groups, uses the roles to formulate responses to compromise or failure in terms of maintaining system controllability, and, ultimately, is extensible for incorporating intrusion detection/recovery and stability control strategy mechanisms. The stability of the power system must be assessed both after compromise or failure and during control response by the distributed controllers. If the system approaches instability, appropriate stability control strategies must be deployed. Such strategies are beyond the scope of this work but can be used in conjunction with the overall framework, as will be discussed later in this chapter. Thus, this chapter details the application of the distributed controller role and control support group results and presents the overall framework formulation for governing distributed controllers, providing a comprehensive view of the utility of this research.

5.2 Basis Decomposition

In Section 4.7, LU factorization is performed on the sensitivity matrix to obtain the transformed basis shown in Equation 5.1. The basis has the structure:

$$\mathbf{L_{CER}} = \mathbf{L_F}\mathbf{L_b^{-1}} = \begin{bmatrix} \mathbf{I_n} \\ \mathbf{R} \end{bmatrix} \tag{5.1}$$

This transformed basis provides the critical, essential, and redundant controller roles. We achieve the equivalent lines flows of the studied system and the controllers that provide the corresponding control. Further information can be gleaned from the matrix by deconstructing the equivalent line flows (i.e., which lines they are composed of) and understanding the basis values for the redundant controllers (e.g., are they the original sensitivities?). This will be elucidated with an example, but first, a review of LU factorization is pertinent.

5.2.1 LU Factorization Review

LU factorization is the matrix form of Gaussian elimination, where a matrix is factored as the product of a lower triangular matrix (L) and an upper triangular matrix (U). Gaussian elimination solves systems of linear equations by using elementary elimination matrices to reduce a system into upper triangular form and using back-substitution to solve the original, linear system [72]. If we have the following linear system:

$$\mathbf{Ax} = \mathbf{b} \tag{5.2}$$

then choose an elementary elimination matrix, $\mathbf{M_1}$, to eliminate (zero) all the entries in the first column, below the first row, such that only a_{11} remains and is our pivot. Therefore, we have performed the operation shown in Equation (5.3).

$$\mathbf{M_1 A x} = \mathbf{M_1 b} \tag{5.3}$$

The solution remains unchanged and we continue the process with a_{22} and successively zero all the subdiagonal entries. The resulting system is upper triangular and can be solved with back-substitution.

$$\mathbf{M_{n-1} ... M_1 A x} = \mathbf{M_{n-1} ... M_1 b} \tag{5.4}$$

$$\mathbf{M A x} = \mathbf{M b} \tag{5.5}$$

Gaussian elimination is achieved using the elementary elimination matrices $\mathbf{M}$; LU factorization is based on $\mathbf{M}$ as well, where $\mathbf{L}$ is composed of:

$$\mathbf{L} = \mathbf{M^{-1}} = \mathbf{M_1^{-1} ... M_{n-1}^{-1}} = \mathbf{L_n ... L_{n-1}} \tag{5.6}$$

Furthermore, $\mathbf{U}$ is achieved with:

$$\mathbf{U} = \mathbf{M A} \tag{5.7}$$

Thus, we obtain the LU factorization of Equation (5.2).

$$\mathbf{A x} = \mathbf{b} \tag{5.8}$$

$$\mathbf{M A x} = \mathbf{M b} \tag{5.9}$$

$$\mathbf{M^{-1} M A x} = \mathbf{M^{-1} M b} \tag{5.10}$$

$$\mathbf{L U x} = \mathbf{b} \tag{5.11}$$

$$\therefore \mathbf{A} = \mathbf{L U} \tag{5.12}$$

5.2.2 Deconstructing the Transformed Basis

With this understanding of LU factorization, we can return the transformed basis equation that was obtained in the following manner (and detailed fur-

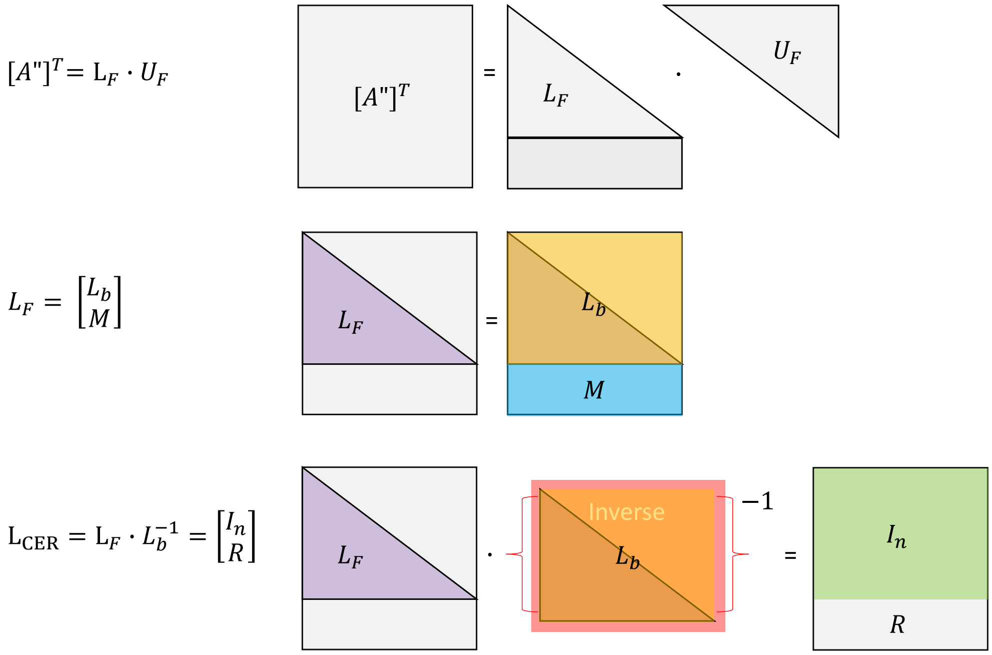

$[A"]^T = L_F \cdot U_F$
$[A"]^T$
=
L_F
·
U_F
$L_F = \begin{bmatrix} L_b \\ M \end{bmatrix}$
L_F
=
L_b
M
$L_{CER} = L_F \cdot L_b^{-1} = \begin{bmatrix} I_n \\ R \end{bmatrix}$
L_F
·
Inverse
L_b
-1
=
I_n
R

Figure 5.1: The LU factorization of the transposed sensitivity matrix is illustrated, ultimately resulting in the transformed basis.

ther in Chapter 4).

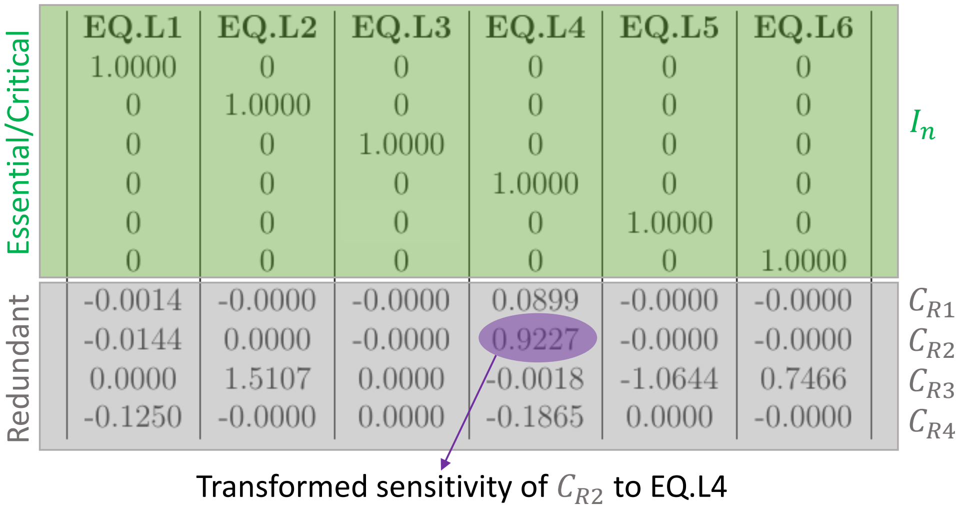
$$[\mathbf{A}'']^{\mathbf{T}} = \mathbf{P}^{-1}\mathbf{L_F}\mathbf{U_F} \tag{5.13}$$

$$\mathbf{L_F} = \begin{bmatrix} \mathbf{L_b} \\ \mathbf{M} \end{bmatrix} \tag{5.14}$$

As mentioned previously, $[\mathbf{A}'']^{\mathbf{T}}$ is the transposed sensitivity matrix, and with LU factorization we obtain $\mathbf{P}$, the permutation matrix, and $\mathbf{L_F}$ and $\mathbf{U_F}$ as the lower and upper triangular factors of dimension n, respectively. $\mathbf{M}$ is a sparse, rectangular matrix with rows corresponding to redundant controllers. The transformed basis has the subsequent structure that is further decomposed into $\mathbf{I_n}$ and $\mathbf{R}$:

$$\mathbf{L_{CER}} = \mathbf{L_F}\mathbf{L_b^{-1}} = \begin{bmatrix} \mathbf{I_n} \\ \mathbf{R} \end{bmatrix} \tag{5.15}$$

The formulation of the transformed matrix using LU factorization is visualized in Figure 5.1. Next, we address the question of the composition of the equivalent line flows. For example, the resultant basis for the PowerWorld 7-bus system was presented in Chapter 4, shown in Figure 5.2 [79]. We seek to know the mapping between the line flows and the equivalent line



		EQ.L1	EQ.L2	EQ.L3	EQ.L4	EQ.L5	EQ.L6	
Essential/Critical		1.0000	0	0	0	0	0	I_n
		0	1.0000	0	0	0	0	
		0	0	1.0000	0	0	0	
		0	0	0	1.0000	0	0	
		0	0	0	0	1.0000	0	
		0	0	0	0	0	1.0000	
Redundant		-0.0014	-0.0000	-0.0000	0.0899	-0.0000	-0.0000	C_{R1}
		-0.0144	0.0000	-0.0000	0.9227	-0.0000	-0.0000	C_{R2}
		0.0000	1.5107	0.0000	-0.0018	-1.0644	0.7466	C_{R3}
		-0.1250	-0.0000	0.0000	-0.1865	0.0000	-0.0000	C_{R4}

Transformed sensitivity of C_{R2} to EQ.L4

Figure 5.2: Transformed basis L_{CER} with labeled controller roles for PowerWorld 7-bus system [79].

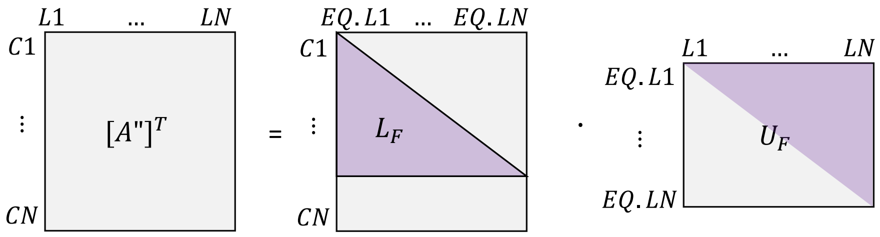


Figure 5.3: Visual representation of LU factorization of transposed sensitivity matrix where $\mathbf{U_F}$ maps the original line flows to equivalent line flows in the transformed basis.

flows, which are linear combinations of the original quantities. For example, in Figure 5.2: For the highlighted (in purple) transformed sensitivity of the redundant controller C_{R2} to the equivalent line flow 4, what is the original line flow composition of **EQ**.**L4**?

From Equation (5.7), it is apparent that the upper triangular factor $\mathbf{U}$ maps the original matrix, using the product of elementary elimination matrices $\mathbf{M}$, to its new basis. The lower triangular matrix, $\mathbf{L}$, is only the product of the inverse $\mathbf{M}$ and does not involve the original $\mathbf{A}$, in the general linear system example. In terms of the equivalent line flows and controllers (e.g., D-FACTS), this relationship can be visualized as presented in Figure 5.3.

Therefore, $\mathbf{U_F}$ maps the original transposed sensitivity matrix $[\mathbf{A}'']^{\mathbf{T}}$ and line flows to the transformed basis with equivalent line flows. Again, $[\mathbf{A}'']^{\mathbf{T}}$

Table 5.1: Upper Triangular Factor $\mathbf{U_F}$

	L1	**L2**	**L3**	**L4**	**L5**	**L6**
EQ.L1	1.9165	-0.3014	0.6138	0.4783	-0.7696	1.3766
EQ.L2	0	-1.6761	-0.5473	-0.7116	-0.9459	0.4046
EQ.L3	0	0	-1.4221	0.7592	-0.7507	-0.6497
EQ.L4	0	0	0	1.2547	-1.2407	1.2444
EQ.L5	0	0	0	0	-0.0041	0.0113
EQ.L6	0	0	0	0	0	-0.0063

represents the sensitivities of controllers to the real power line flows in the system. The sensitivity matrix formulation is detailed in Section 4.4. The equivalent line flow composition is captured in $\mathbf{U_F}$, as shown in Figure 5.3. The entries in $\mathbf{U_F}$ signify the presence of each original line flow in the equivalent line flows. The $\mathbf{U_F}$ for the example 7-bus system is shown in Table 5.1.

Using the $\mathbf{U_F}$ entries, we can determine the composition of the equivalent line flows, which are linear combinations of the original line flows. The coefficients of each equivalent line flow linear combination are provided by $\mathbf{U_F}$ and are shown in Equations (5.16)-(5.21).

$$\begin{aligned}\mathbf{EQ.L1} =& 1.9165 \cdot L_1 - 0.3014 \cdot L_2 + 0.6138 \cdot L_3 + \\ & 0.4783 \cdot L_4 - 0.7696 \cdot L_5 + 1.3766 \cdot L_6\end{aligned} \tag{5.16}$$

$$\begin{aligned}\mathbf{EQ.L2} =& -1.6761 \cdot L_2 - 0.5473 \cdot L_3 - 0.7116 \cdot L_4 \\ & - 0.9459 \cdot L_5 + 0.4046 \cdot L_6\end{aligned} \tag{5.17}$$

$$\mathbf{EQ.L3} = -1.4221 \cdot L_3 + 0.7592 \cdot L_4 - 0.7507 \cdot L_5 - 0.6497 \cdot L_6 \tag{5.18}$$

$$\mathbf{EQ.L4} = 1.2547 \cdot L_4 - 1.2407 \cdot L_5 + 1.2444 \cdot L_6 \tag{5.19}$$

$$\mathbf{EQ.L5} = -0.0041 \cdot L_5 + 0.0113 \cdot L_6 \tag{5.20}$$

$$\mathbf{EQ.L6} = -0.0063 \cdot L_6 \tag{5.21}$$

5.2.3 Ranking Redundant Controllers

Thus, the composition of each equivalent line flow is obtained and can aid controller placement and response efforts. Another crucial insight we obtain from the transformed basis in Figure 5.2 is how the redundant controllers $C_{R1} - C_{R4}$ (corresponding to Controllers # $6, 1, 9, 10$, respectively) should be ranked for each equivalent controller. With this information, when compromise or failure occurs for one of the essential controllers (in $\mathbf{I_n}$), we know which redundant controllers to respond with effectively. The entries of $\mathbf{R}$ represent the transformed sensitivities: sensitivity of each redundant controller to each equivalent line flow.

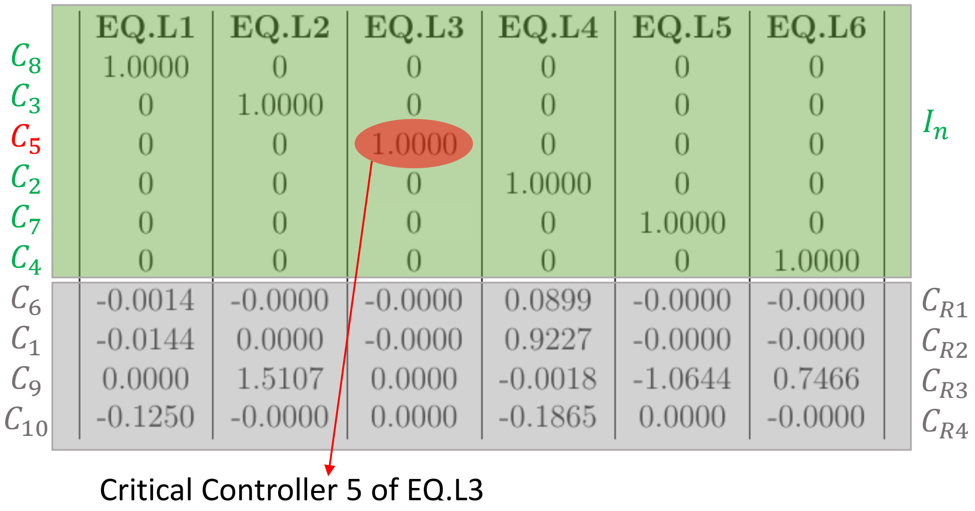
If the essential controller corresponding to $\mathbf{EQ}.\mathbf{L4}$ is compromised, we learn from the transformed basis that C_{R2} has the highest sensitivity to $\mathbf{EQ}.\mathbf{L4}$ and is the top redundant controller candidate for responding to the compromise. C_{R4} has the next highest sensitivity (magnitude) and can be used in conjunction or following C_{R2}. Yet, C_{R1} and C_{R3} have low sensitivities and will not be very effective in solo response. Depending on the compromise or failure situation, we can utilize this information to either use the most sensitive redundant controllers (cannot spare all due to multiple situations) or utilize all redundant controllers in response, but prioritize changing settings of the highly ranked controllers. Essential controllers with no redundant controllers (entries of 0 in corresponding column of R) are critical controllers.

5.2.4 Improving Controller Placement

An equivalent line flow's decomposition is known from the $\mathbf{U_F}$ entries, an example of which was shown in Equations (5.16)-(5.21). This is particularly useful when a critical controller is discovered (no other controller can provide needed control to the corresponding equivalent line flow) and we want to convert it to essential. In this section, an intuitive example is detailed of how this conversion would occur in a brute-force manner. Ultimately, the equivalent line flow decomposition results could be paired with optimization algorithms to determine effective controller placement and avoid critical roles. Such techniques have been developed for PMU placement and observability, but can be extended to controllers utilizing the insights presented [77].

In the 7-bus system example, the controller corresponding to Row 3 and $\mathbf{EQ}.\mathbf{L3}$ of the transformed basis is critical, as shown in Figure 5.4. The critical controller is controller 5 (alternatively labeled, the controller on $L5$), which we derive from the LU factorization permutation matrix. The composition of $EQ.L3$ is shown in Equation (5.22).

$$\mathbf{EQ}.\mathbf{L3} = -1.4221 \cdot L_3 + 0.7592 \cdot L_4 - 0.7507 \cdot L_5 - 0.6497 \cdot L_6 \qquad (5.22)$$



	EQ.L1	EQ.L2	EQ.L3	EQ.L4	EQ.L5	EQ.L6	
C_8	1.0000	0	0	0	0	0	
C_3	0	1.0000	0	0	0	0	
C_5	0	0	1.0000	0	0	0	I_n
C_2	0	0	0	1.0000	0	0	
C_7	0	0	0	0	1.0000	0	
C_4	0	0	0	0	0	1.0000	
C_6	-0.0014	-0.0000	-0.0000	0.0899	-0.0000	-0.0000	C_{R1}
C_1	-0.0144	0.0000	-0.0000	0.9227	-0.0000	-0.0000	C_{R2}
C_9	0.0000	1.5107	0.0000	-0.0018	-1.0644	0.7466	C_{R3}
C_{10}	-0.1250	-0.0000	0.0000	-0.1865	0.0000	-0.0000	C_{R4}

Critical Controller 5 of EQ.L3

Figure 5.4: Transformed basis L_{CER} with labeled critical controller for PowerWorld 7-bus system [79].

Table 5.2: Transformed Basis with Added Redundant Controller to Line 5

EQ.L1	EQ.L2	EQ.L3	EQ.L4	EQ.L5	EQ.L6
1.0000	0	0	0	0	0
0	1.0000	0	0	0	0
0	0	1.0000	0	0	0
0	0	0	1.0000	0	0
0	0	0	0	1.0000	0
0	0	0	0	0	1.0000
-0.0014	-0.0000	-0.0000	0.0899	-0.0000	-0.0000
-0.0000	0.0000	1.0000	-0.0000	-0.0000	0.0000
-0.0144	0.0000	-0.0000	0.9227	-0.0000	-0.0000
0.0000	1.5107	0.0000	-0.0018	-1.0644	0.7466
-0.1250	-0.0000	0.0000	-0.1865	0.0000	-0.0000

The equation indicates that L_3 has the most significant presence in **EQ.L3**. L_3 corresponds to L_5 in the original 7-bus system, due to the selection of target line flows for factorization, as illustrated in Figure 5.5. The use of target line flows is explained in Section 4.7. Therefore, line flow 5 would be most severely impacted if critical controller 5 was compromised. To remedy this and convert the controller to essential, we need to add another controller (in this example, D-FACTS) to be redundant to line 5. Therefore, by adding a second controller to line 5, the transformed basis (after re-factorizing the sensitivity matrix) shown in Table 5.2 is obtained.

There are 12 total controllers now, one on each line (including parallel

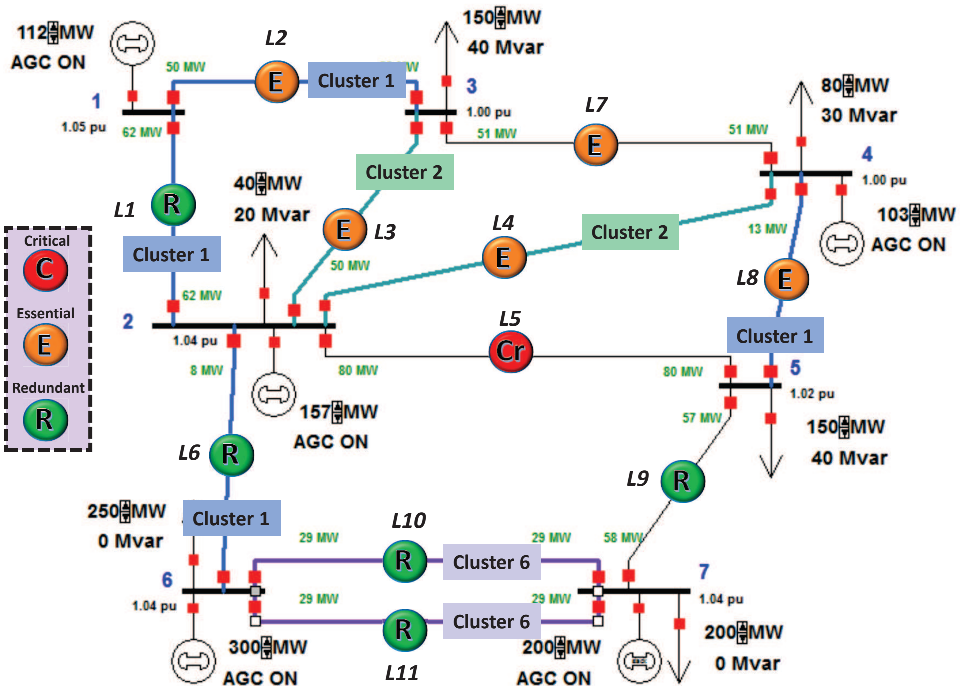


Figure 5.5: PowerWorld 7-bus system with lines colored according to cluster group and labeled with critical, essential, and redundant controllers.

line) and an additional controller on $L5$. This is illustrated in Figure 5.6. Controller 6 is redundant to **EQ.L3** and converts controller 5 from critical to essential—with magnitude 1 in the transformed basis, controllers 5 and 6 are now interchangeable for controlling **EQ.L3**. As a result, there are no critical controllers and the loss of system controllability risk is reduced.

This is just an intuitive example that demonstrates the utility of the transformed basis. In this small system, we have already assumed a controller is on every line and the existence of multiple controllers on one line is not realistic, for most controller types. Nonetheless, in a larger and realistic system, we would not have controllers on every line and the addition of controllers to certain lines (not multiple) would actually eliminate critical roles. An optimization algorithm could be developed that aids a system to have a desired level of redundancy and eliminate all critical roles in the system. Chen and Abur formulated a method to perform the optimization for the placement of PMUs considering system observability that could be extended to this application [77].

Lastly, if there was a redundant controller set for which the transformed sensitivities were very high for each controller to only one equivalent line flow,

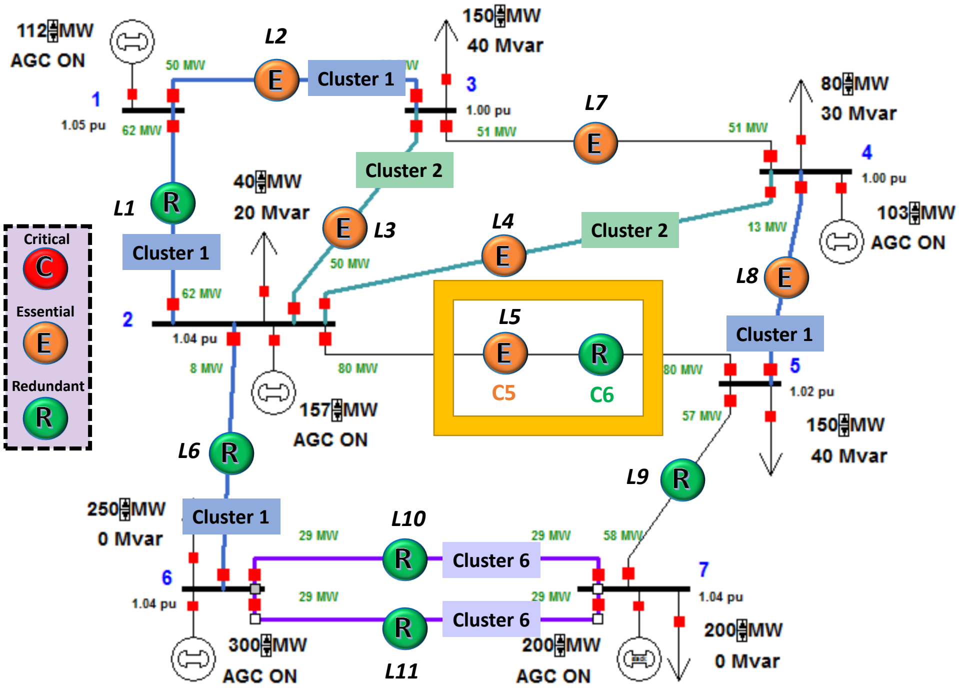


Figure 5.6: PowerWorld 7-bus system with lines colored according to cluster group and labeled with essential and redundant controllers; highlighted in the yellow box is added controller, $C6$, that converted $C5$ from critical to essential.

excessive redundancy is indicated. If a redundant controller does not have much impact on any other equivalent line flow (especially if the actual line composition overlaps with other equivalent line flows) and other significant redundant controllers are present for that equivalent line flow, it can be removed. Thus, this type of study can be performed as a planning tool for placing distributed controllers in the power system. In this manner, the minimum set of controllers can be placed and selected such that there exist no critical controllers and unnecessary controllers are not used (reducing cost).

All in all, two main insights are achieved from the study of the transformed basis:

1. The composition of the equivalent line flows in terms of the original line flows
   - Aid controller placement to avoid critical roles and eliminate excessive redundancy
2. Ranking of redundant controllers from the transformed sensitivities

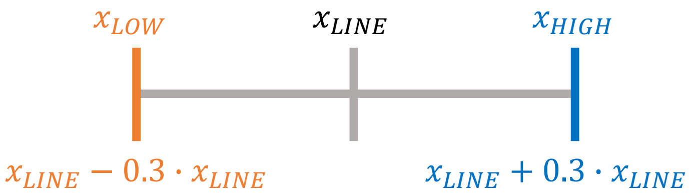

x_{LOW}
x_{LINE}
x_{HIGH}
$x_{LINE} - 0.3 \cdot x_{LINE}$
$x_{LINE} + 0.3 \cdot x_{LINE}$

Figure 5.7: Range of settings for D-FACTS devices and its change to line impedance to test state-dependence of controller roles and control support groups.

- During essential controller compromise or failure, respond with most effective redundant controllers and avoid using controllers that have no or very minimal impact

5.3 State-Dependence of Roles and Groups

The previous section demonstrates the insight gained from the transformed sensitivity matrix basis and how that information can be leveraged. Next, we examine how the controller roles and control support groups change with varying operating points. Originally, we calculated the roles and groups for a specific operating point, usually normal operation, and sought to apply those results generally. Nonetheless, that approach may not be correct if the results do, in fact, change significantly for different states of the power system.

To test the state-dependence of the results, the 7-bus system was studied with different settings of D-FACTS controllers, which in turn were changing the line power flows. The settings, the effective impedance of each device, were varied from ±30% of the line impedance. This is illustrated in Figure 5.7 and the ±30% variation is derived from the D-FACTS controller limits defined in PowerWorld [83]. The subsequent settings for the D-FACTS, x_{DF}, can be derived from:

$$x_{line,new} = \pm 0.3 \cdot x_{line} + x_{line} \tag{5.23}$$

$$x_{DF} = x_{line,new} - x_{line} \tag{5.24}$$

Essentially, for this specific range example, the setting for the D-FACTS devices will vary within the range:

$$x_{DF} = [-0.3 \cdot x_{line} \quad 0 \quad 0.3 \cdot x_{line}] \tag{5.25}$$

where 0 indicates that the controller is not in use and the line is at its original impedance. For testing the different operating points, we consider two situations: when two D-FACTS are in use and when four D-FACTS are in use. Therefore, for two D-FACTS, we determine combinations of the entire set, two at a time, for the various settings. For example, in the 7-bus system, we consider 10 lines with a D-FACTS device on each. For different pair combinations of the devices, we have 100 combinations. For each of these pairs, there can be 3 different settings ($[x_{DF,LOW} \quad x_{DF,0} \quad x_{DF,HIGH}]$), for a total of $3x3$ or 9 setting combinations. Thus, there are 900 different D-FACTS pair and setting states; this is graphically represented in a cell format in Figure 5.8. Additionally, we test combinations of 4 controllers in the same manner, and the visualization is shown in Figure 5.9. There are $81,000$ device and setting combinations in this case. We consider 4 device combinations as the maximum for this study due to the severe computational burden that results for a higher number. A possible method for reducing this computation time while testing a broad range of operating points is to only consider one controller from each control support group.

With these various operating points, for both 2 and 4 D-FACTS device combinations, the controller role and control support groups can be calculated and compared across different states. These results are illustrated in Figures 5.10-5.13. Figures 5.10 and 5.11 show the number of occurrences of each controller as essential or critical over all the operating points. As indicated for both combination sets, a pattern of recurrent essential or critical controllers emerges. Controllers # $1, 2, 3, 8, 9$ have a significant presence as essential or critical over all the operating points (varied with ±30% of the D-FACTS settings). Similarly, in Figures 5.12 and 5.13, the number of occurrences for each controller as critical over all operating points, for both 2 and 4 device combinations, is provided. It is apparent that Controller #5 has a critical role frequently, especially compared with the rest of the set.

These results highlight two main points:

1. The controller role results do change as the operating point varies.

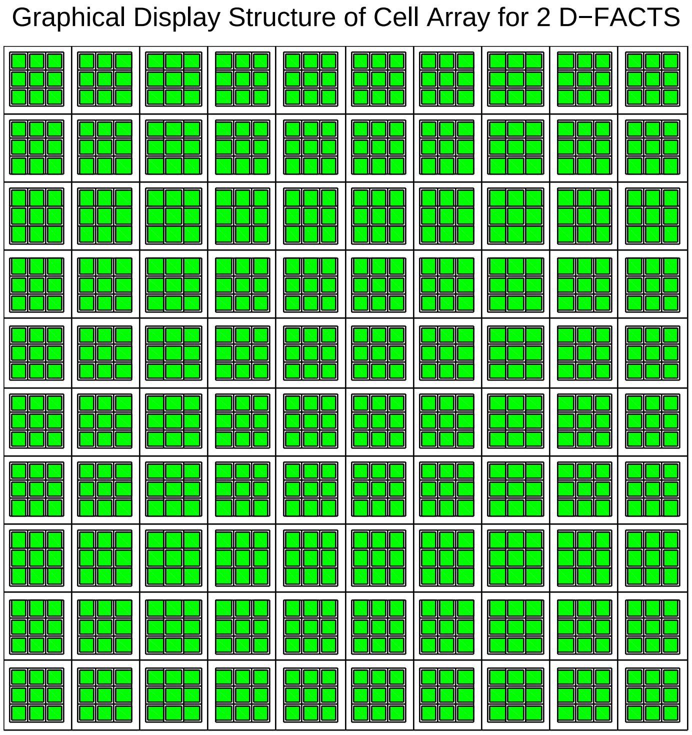


Figure 5.8: Cell structure visual representation of D-FACTS pair and setting combinations.

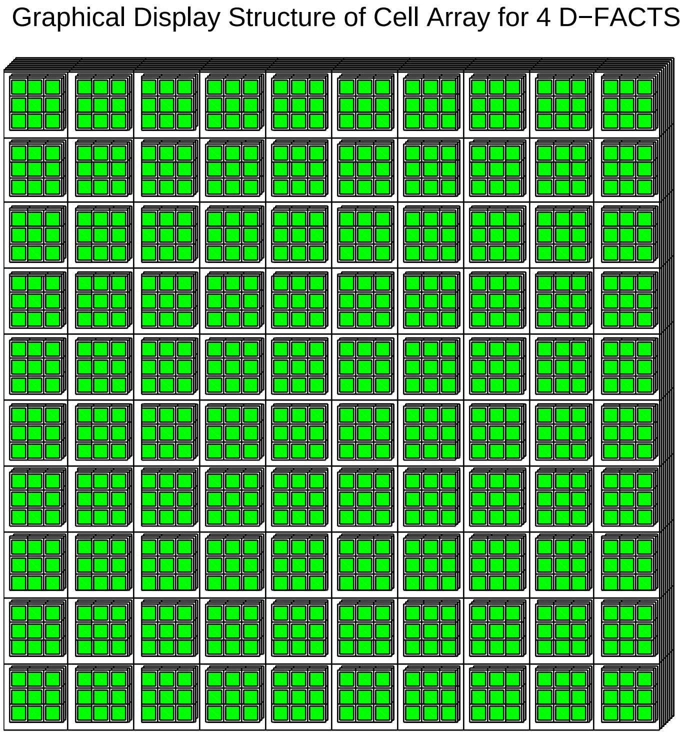


Figure 5.9: Cell structure visual representation of 4 D-FACTS device and setting combinations.

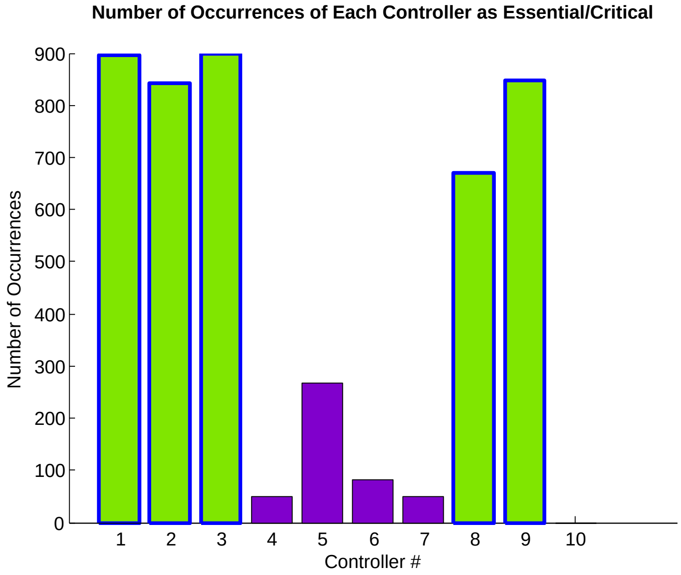


Figure 5.10: 2 D-FACTS combinations: occurrences of each controller as essential or critical over all operating points.

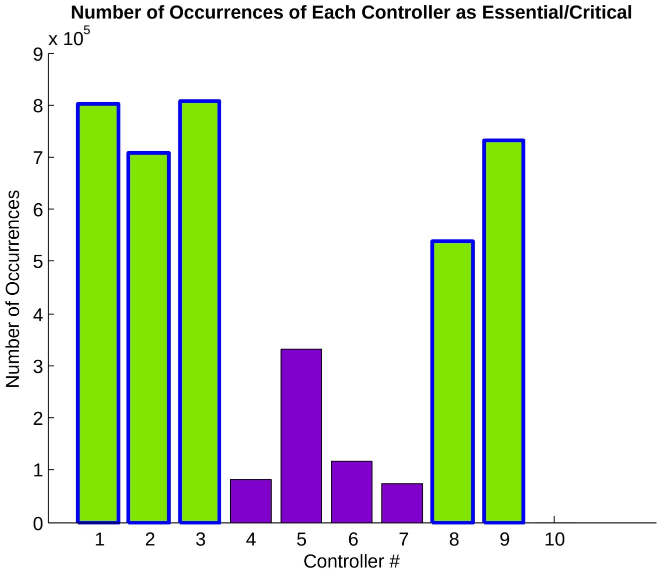


Figure 5.11: 4 D-FACTS combinations: occurrences of each controller as essential or critical over all operating points.

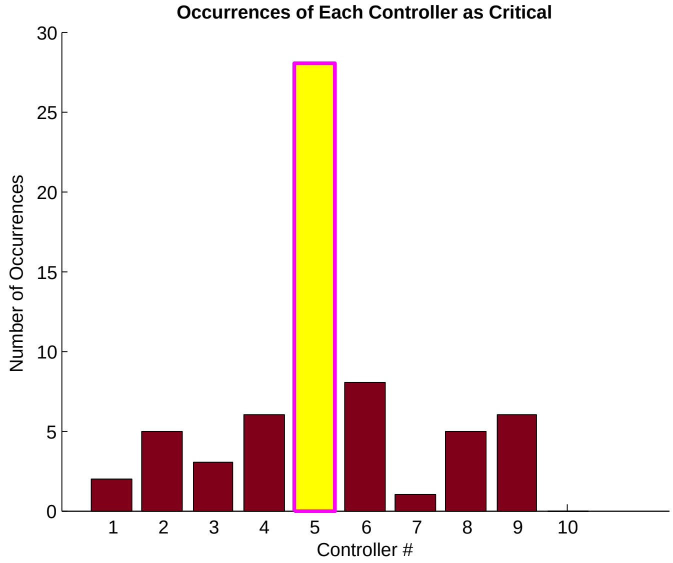


Figure 5.12: 2 D-FACTS combinations: occurrences of each controller as **critical** over all operating points.

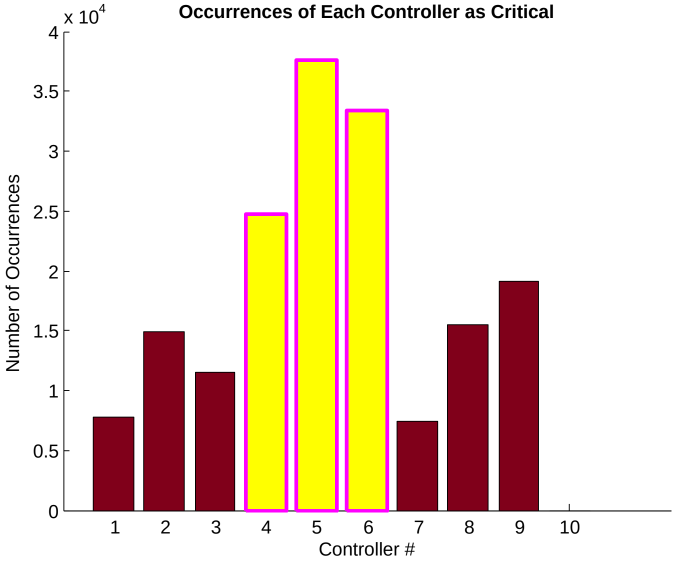


Figure 5.13: 4 D-FACTS combinations: occurrences of each controller as **critical** over all operating points.

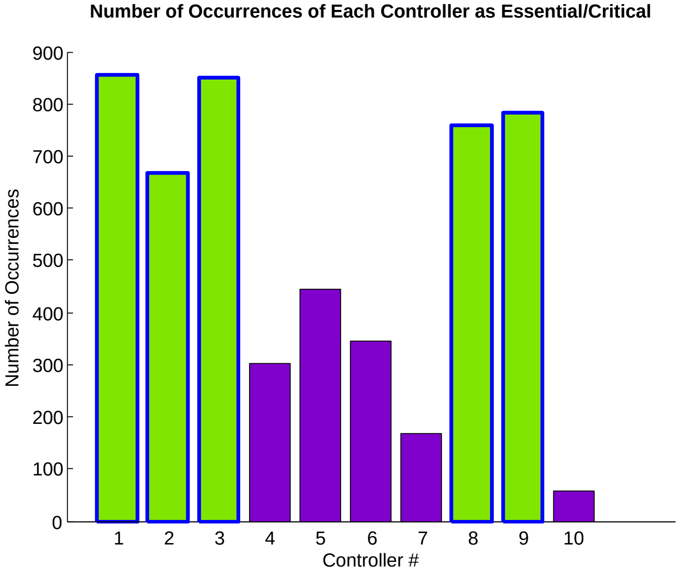


Figure 5.14: 2 D-FACTS combinations: occurrences of each controller as essential or critical over all operating points, with ±90% change in x_{LINE}.

2. Some controllers are frequently a certain role; a pattern exists over all the operating points

To further explore these observations, the effective impedance of each device was varied ±90% of the line impedance. This is not physically possible for the D-FACTS devices due to limits, but in the coded device model, it was used to obtain dramatically different operating points to test. The controller role results are shown in Figures 5.14 and 5.15, as tested with 2 D-FACTS device combinations.

For this broader range of operating points, the same pattern emerges with Controllers # $1, 2, 3, 8, 9$ as essential or critical, frequently, and Controller #5 as critical. However, it is useful to note that Controllers # $8, 9$ increase in frequency as critical, although they are not the highest. These additional results reinforce the observation points aforementioned and are particularly useful when designing a control response framework for distributed controllers when compromise or failure occurs.

For the 4 D-FACTS combinations, the results vary more dramatically, as shown in Figure 5.16 and Figure 5.17. Controllers # $1, 2, 3, 8, 9$ still have high frequency as essential or critical and Controller #5 has the highest number of occurrences as critical. Yet, these controllers do not exhibit the

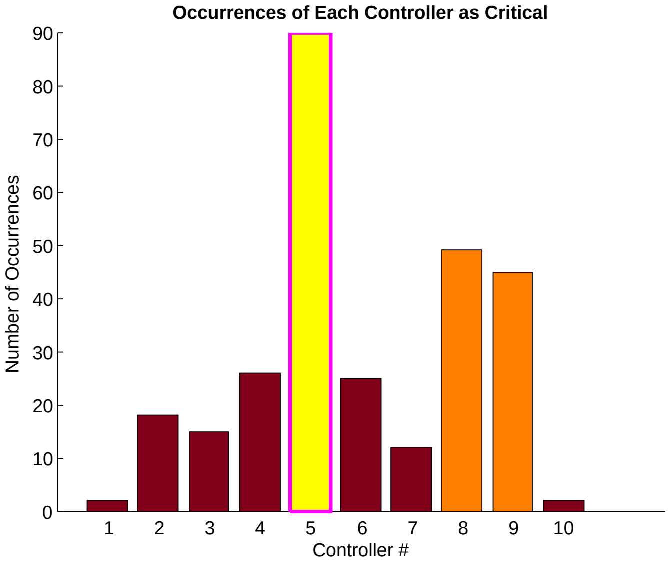


Figure 5.15: 2 D-FACTS combinations: occurrences of each controller as **critical** over all operating points, with ±90% change in x_{LINE}.

distinct pattern as previously observed with the ±30% testing. The essential or critical controller pattern remains similar, with the addition of Controller #5. This is expected, as we already observed Controller #5 to be frequently critical. However, Controllers # $4, 6, 8, 9$ exhibit high numbers of occurrences as critical, as shown in Figure 5.17. This behavior indicates that there are certain operating points for which the recurrent pattern is not dominant and recalculation of the roles is necessary for formulating the most effective control response. This point will be elaborated upon in the next section.

Results were also obtained for the clustering of the different controllers. Again, the clusters or control support groups varied for different operating points but general patterns still emerged (e.g., this controller is often assigned to this cluster or this cluster is usually composed of these controllers).

Figure 5.18a compares results for the membership of Cluster 2, for the 2 D-FACTS ±30% scenario, in which controllers 3 and 4 are frequent members. This observation is further reinforced when examining the occurrence of controller 3 being assigned to Cluster 2 in Figures 5.18b (similar results were obtained for controller 4). The D-FACTS controllers are placed on each line; clustering the controllers also provides results for the clustering of the lines, as indicated by the plots. For simplicity, we will only refer to controllers.

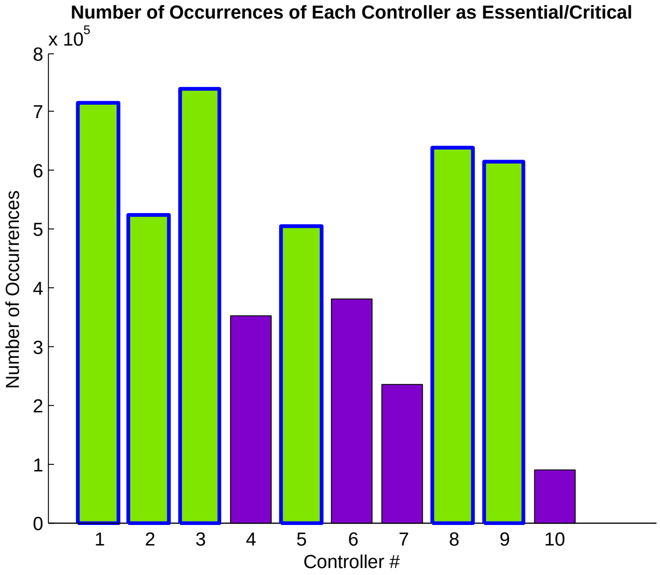


Figure 5.16: 4 D-FACTS combinations: occurrences of each controller as essential or critical over all operating points, with ±90% change in x_{LINE}.

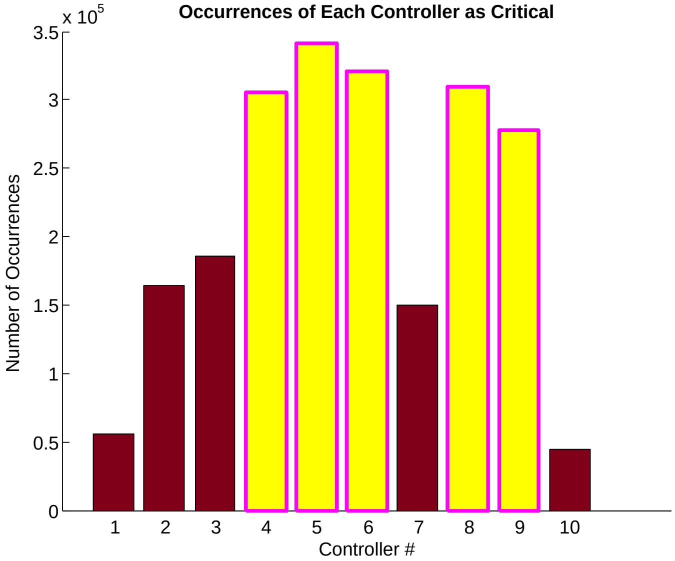
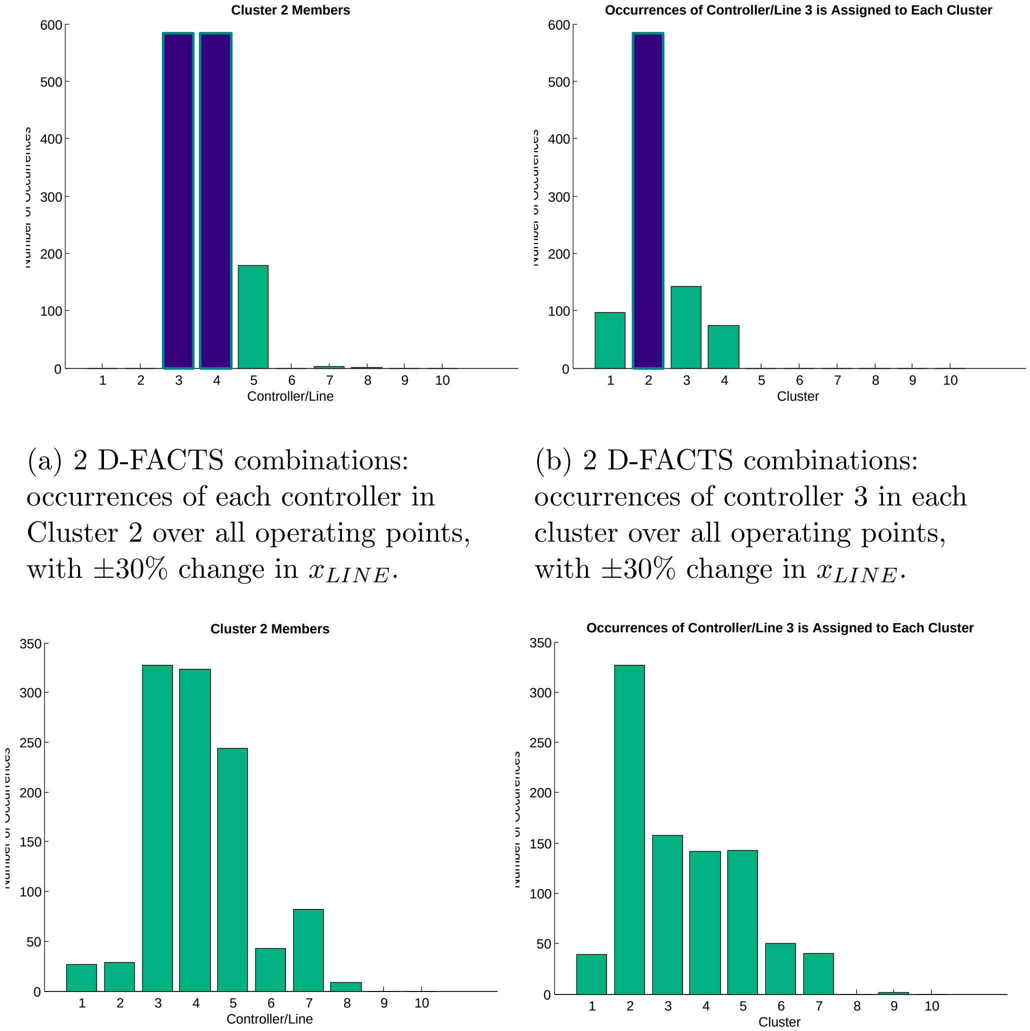


Figure 5.17: 4 D-FACTS combinations: occurrences of each controller as **critical** over all operating points, with ±90% change in x_{LINE}.



(a) 2 D-FACTS combinations: occurrences of each controller in Cluster 2 over all operating points, with ±30% change in x_{LINE}.

(b) 2 D-FACTS combinations: occurrences of controller 3 in each cluster over all operating points, with ±30% change in x_{LINE}.

(c) 2 D-FACTS combinations: occurrences of controller 4 in each cluster over all operating points, with ±30% change in x_{LINE}.

(d) 2 D-FACTS combinations: occurrences of each controller in Cluster 2 over all operating points, with ±90% change in x_{LINE}.

Figure 5.18: Frequency of cluster membership for various operating points.

When the system state is varied dramatically, as in the 2 D-FACTS ±90% case, controllers 3 and 4 remain highest in frequency but other controllers also increase in occurrence, as shown in Figure 5.18c. This behavior is also illustrated with Figure 5.18d, where controller 3 is assigned to Cluster 2 most frequently. Nonetheless, its assignment to other clusters has also increased in frequency.

The IEEE 118-bus system was also tested with varying operating points, for both ±30% and ±90% changes in x_{LINE}. D-FACTS were presumed to be on every line (186 lines) and a change in a single device was considered, rather than 2 or 4 D-FACTS combination. The computation time was excessive for more than 1 device change. This can be avoided by not assuming there is a device on each line or only analyzing a controller from each control support group. Nonetheless, it was found that as the operating point changed, the resultant controller roles remained the same, for both ±30% and ±90% changes in x_{LINE}. This is exemplified by Figure 5.19.

This is expected, as the change in a single D-FACTS device will not impact the large 118-system substantially. However, more significant system changes such as line outages or faults will impact the controller role and control support group results. A recurrent set of controller roles could emerge depending on the extent of system change. If so, they can be used in response, as detailed in the next section, but otherwise should be recalculated for every operating point.

Also, there are no critical controllers, which is good for the system but may also indicate that we have excessive redundancy. A device on every line is unnecessary, but this analysis aids in determining what the control support groups are and that only one controller from each is needed to control the equivalent line flows. Therefore, we can nearly halve the number of controllers from 186 to 91, where there were 91 control support groups for the 118-bus system.

Therefore, the main observations from studying the frequency of cluster membership over the different operating points are:

- For both the 2 D-FACTS and 4 D-FACTS combination cases, with ±30% change in x_{LINE}, the results are similar with distinct cluster membership.

- When the variation is increased to ±90% change in x_{LINE} (not possible

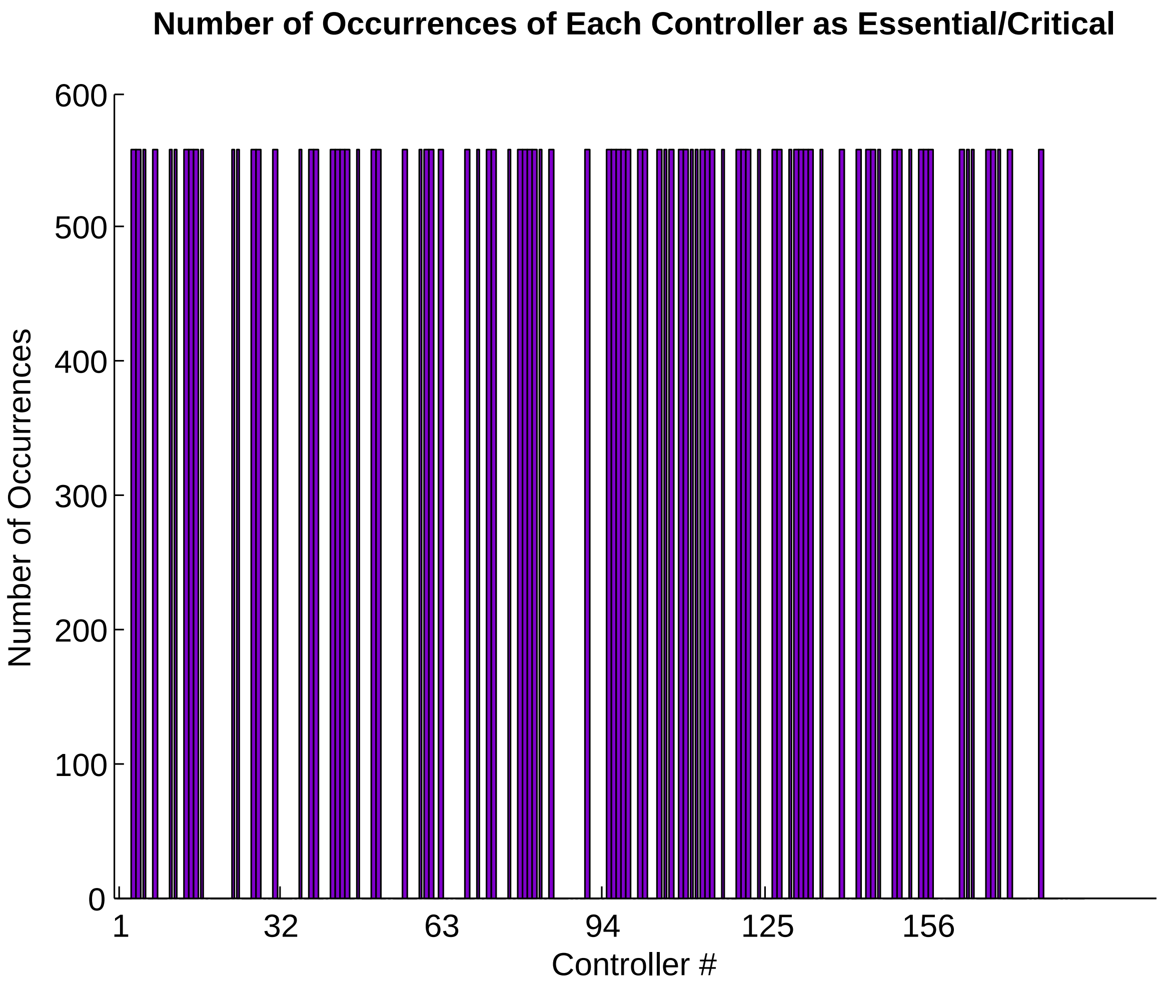


Figure 5.19: 1 D-FACT: occurrences of each controller as essential or critical over all operating points for both ±30% and ±90% changes in x_{LINE}.

setting for the device, but used to test dramatic change in operating point), the cluster membership patterns are less discernible.

  - The same controllers still appear dominant, but other cluster member's occurrences increase in frequency.

- Large systems are not substantially impacted by the D-FACTS changes, so the controller roles are always the same.

All in all, intriguing results were obtained from testing different operating points and comparing the controller role and cluster results. The patterns that emerged, having certain controllers be recurrent in specific roles or assigned to specific clusters, can be leveraged for control response. A framework can be designed in which these recurring essential or critical controls, the ones that have the largest span of control over the equivalent line flows, can be utilized when responding to controller compromise or failure. This framework is demonstrated in the next section.

5.4 Responding to Compromise or Failure of Distributed Controllers

Controller compromise or failure within the distributed controller set can have serious consequences due to cascading, detrimental effects. Mitigation requires rapid response such that sustained line overloads, sensitive equipment damage, and, in the worst case, blackout are prevented. This dissertation seeks to address this problem, particularly with the presented analytic controller role and control support group methodology. Proactive strategies must be developed using these results.

In Chapter 4, the controllability analysis based method that processed the controller sensitivities using clustering and factorization techniques was presented. The resultant controller roles and control support groups were demonstrated in their use with several compromise scenarios. In particular, comparison between critical, essential, and redundant controller compromises is presented as well as how the response should differ. In this section, different scenarios are tested with the proposed responses in simulation, using PowerWorld [84], and a general response strategy is developed.

To address the difference in response, from the remaining, uncompromised set of distributed controllers, critical controllers are a crucial aspect. As defined previously, critical controllers are devices that are irreplaceable and mandatory for system controllability. Thus, when a critical controller is compromised, we have lost full system control and have no redundant controllers to salvage some control of the now uncontrolled equivalent line flow. As such, this situation is severe and requires immediate response from other system controllers and defense mechanisms.

However, it is important to note that the priority of responding immediately to the compromise or failure of a critical controller is dependent on the type of device. For example, if a D-FACTS device on a line was compromised but the most malicious change incurred only increased the line flow slightly (not overloading), perhaps immediate response is not necessary. A more serious situation could arise if multiple D-FACTS devices were compromised at once, or if a different type of controller was compromised, such as a static var compensator (SVC) that can destabilize system voltage or angle with modification attacks [43].

Nonetheless, assuming that the critical controllers do require immediate response and detrimentally impact system controllability, we must be proactive and seek to eliminate their critical role in the planning stage. This was demonstrated in Section 5.2, where redundancy was added to the corresponding equivalent line flow and transformed the critical controller to essential. Yet, critical roles can result due to changes in system state after failure and compromise, and in those cases, the compromised critical controller(s) must be prioritized and additional defense mechanisms are needed.

5.4.1 Distributed Control Response Framework

When the compromise of any distributed controller (critical, essential, or redundant) occurs, an appropriate response must be formulated from the remaining set. Yet, the true response to the cyber-physical compromise of the targeted controller, the “cleaning” of the system from the intrusion, and overall diagnosis must be performed by actual cyber-physical defense mechanisms. The response of the remaining, uncompromised set of distributed controllers seeks to minimize stressed conditions and prevent damage to sensitive equipment. The distributed controller response is immediate, as soon as a compromise or abnormal behavior is detected, and occurs while the event is investigated through security protocols. Examples of these protocols were provided in Section 3.2.2 as well as in Section 2.3.2 where a cyber-physical response system (CPR) design was presented as a related, motivating project.

The compromise of a distributed controller is realized through the intrusion detection system (IDS) or just general monitoring. The rapid changes in settings of a specific controller and lack of need or logic, as observed from the current system state, should flag the operator, the remaining distributed controller set, and security systems that something is amiss. Thus, with the flag or alarm that a controller has been compromised, the main pieces of information at hand are:

- A controller has been compromised and its identity is known
- The settings of the controller are changing for some unknown objective.
    - The setting change is not warranted by the state of the system because there is no apparent need.
    - This behavior is abnormal.
- The identity of the compromised device may or may not be known.
    - If the controller identity is known, the role of the controller as critical, essential, or redundant is known, and its control support group is known.

However, in some cases, there may be no IDS or security system in place that can identify the compromised controller. In that case, the changing of controller settings that worsen the system state and were not warranted can flag abnormal behavior. The distributed controller set can respond in the meantime, to minimize overload and system stress, while the abnormal changes are investigated. In fact, the recurrent essential or critical controller results discovered by the state-dependence testing in the last section could prove useful when the identity is unknown. The failure of a controller can benefit from the same control response, where the failed controller is known, and if the quantity it was controlling is severely impacted, the remaining distributed controller set can respond effectively.

To formulate a general control response for the set of “safe”, uncompromised distributed controllers, the results from testing the role and group methodology over many operating points can be leveraged. As presented in Section 5.3, it was observed that although the role and group assignments do change over different operating points, a pattern of recurrent results does emerge. This pattern indicates that certain controllers frequently take on specific roles over all the system states tested. This implies that those results can be generally applied to be most effective for any operating point, especially when it is not feasible to recalculate the roles and groups in real-time.

The application of these general results compared to current system state roles and groups can be demonstrated with the PowerWorld 7-bus system [79]. Using the D-FACTS controller example, we have a set of 10 controllers (excluding parallel line 11) of which Controller #2 is compromised. This controller, on Line 2, is set to +30% of its line impedance, the maximum, to increase Line 2 from 44% MVA to 55% MVA. As this abnormal behavior is investigated by security mechanisms, the remaining set of D-FACTS devices can be used to respond and reduce the line flow increase. Table 5.3 lists several selection methods for the subset of the remaining D-FACTS controllers that should be used to respond to the Controller #2 compromise. The minimum, effective number should be used such that system disruption is low.

For each selection of response controllers, the corresponding settings must be calculated to most effectively reduce the line loading increase. For the D-FACTS devices, the setting of the injected effective impedance, x_{DF}, must be calculated for each of the selected devices. For the D-FACTS line power flow control application, a control algorithm developed by Rogers and Overbye in [67] was applied. The method utilizes an optimization framework where the objective was to determine line impedance settings of the selected devices and minimize the differences between the actual and desired power flows. The objective function, f_0, in Equation (5.26) represents this goal where L represents the number of lines to be targeted for control.

$$f_0 = \sum_{i=1}^{L} [P_{flow,desired}(x) - P_{flow,actual}(x)]_i^2 \tag{5.26}$$

Rogers and Overbye stated the line flow control optimization problem as shown in Equations (5.27)-(5.30).

$$
\begin{aligned}
min\ f_0 && (5.27)\\
s.t.\ \mathbf{f}_{(p,q)}(\mathbf{s}_{(\theta,V)}) = 0 && (5.28)\\
\mathbf{x} \leq \mathbf{x}_{max} && (5.29)\\
\mathbf{x} \geq \mathbf{x}_{min} && (5.30)
\end{aligned}
$$

Equation (5.28) represents the first constraint of the AC power balance equations and Equations (5.29) and (5.30) provide the device limits for change in line impedance. This line impedance is the altered impedance after the D-FACTS device x_{DF} has been injected, as shown previously in Equation (5.24). This minimization problem is solved using steepest descent, and the D-FACTS settings for each selected controller are found such that the best attempt at achieving the desired power flows is achieved [85]. The convergence of the power flow solution, with the implemented D-FACTS settings found by the algorithm, is checked for every set. Full details on this control algorithm for D-FACTS devices are provided in [67].

Returning to selection of controllers for responding to compromise or failure, Table 5.3 presents the selected response controllers using various methods and the calculated settings for each. These x_{DF} settings are computed using the control framework presented by Rogers and Overbye [67]. For this response application, the line flow targeted for control was set as the compromised line and the control framework calculated the settings, with the specified response set, to best mitigate the compromised line flow. The Recurrent CE and Recurrent R selection algorithms are derived from the state-dependence tests in the previous section, where the controller role and group results were calculated across various operating points. For the 7-bus system, the recurrent controllers were Controllers $\#1, 2, 3, 8, 9$. For the compromise of Controller $\#2$, we exclude it from the list of response controllers. Table 5.3 displays the resultant % MVA of $L2$ after each of the response controller sets and their corresponding settings are applied to the system to reduce the line flow.

The Recurrent CE selection algorithm performs best, where the loading of Line 2 is reduced from 55% MVA to 48.9% MVA, where the original loading was 44% MVA. Recurrent CE and R represent the general (highest frequency of occurrence over the operating points) controller roles, for critical/essential roles or redundant roles, respectively. The Current CE, R, and Ranked R methods are calculated with the current operating point of the system, including the compromise. The Current Ranked R algorithm considers only the redundant controllers with high sensitivity to the equivalent line flow that corresponded to Controller #2.

Nevertheless, the Recurrent CE method is most successful in reducing the line flow increase and can be used as a general response to controller compromises. However, the recurrent critical or redundant controllers became less distinct and significant when the system state changed dramatically when the line impedance was varied by 90% in Figure 5.14 versus the 30% case. Therefore, a threshold of change in system state from normal operation to a compromised state, for the quantity of interest (e.g., line flow), can be used to determine when to use the Recurrent CE or the Current CE set. The Recurrent CE is effective and applicable for a smaller range of operating points; beyond that, the current system state should be used to calculate the roles and groups. Additionally, it is useful when the compromised controller identity is unknown, as the response is broadly useful for most operating points. This control response method is illustrated in Figure 5.20. This control response algorithm for the distributed controllers is tested for different controller compromises in the PowerWorld 7-bus system, including Controller 2. Again, the D-FACTS example is continued and an adversary changes the injected effective impedance x_{DF} by the maximum increase of 30%, according to device limits, such that the line flow of the targeted controller is increased as much as possible [83]. Due to the 30% change in impedance, the change in the system state, especially the compromised line, was low and under 15% for this system. Therefore, a threshold value related to the device limits for the change in impedance, such as 20%, can be set and the recurrent results for the controller roles can be used for response for each compromise below the threshold. This threshold selection can be explored and validated further in future work.

Table 5.4 presents the results for each compromise, comparing the original, compromised, and response % MVA of the line of interest. The corresponding settings for the response set (excluding compromised controllers) are discovered with the D-FACTS control algorithm formulated by Rogers and Overbye [67]. In most of the compromise cases, the response set is able to

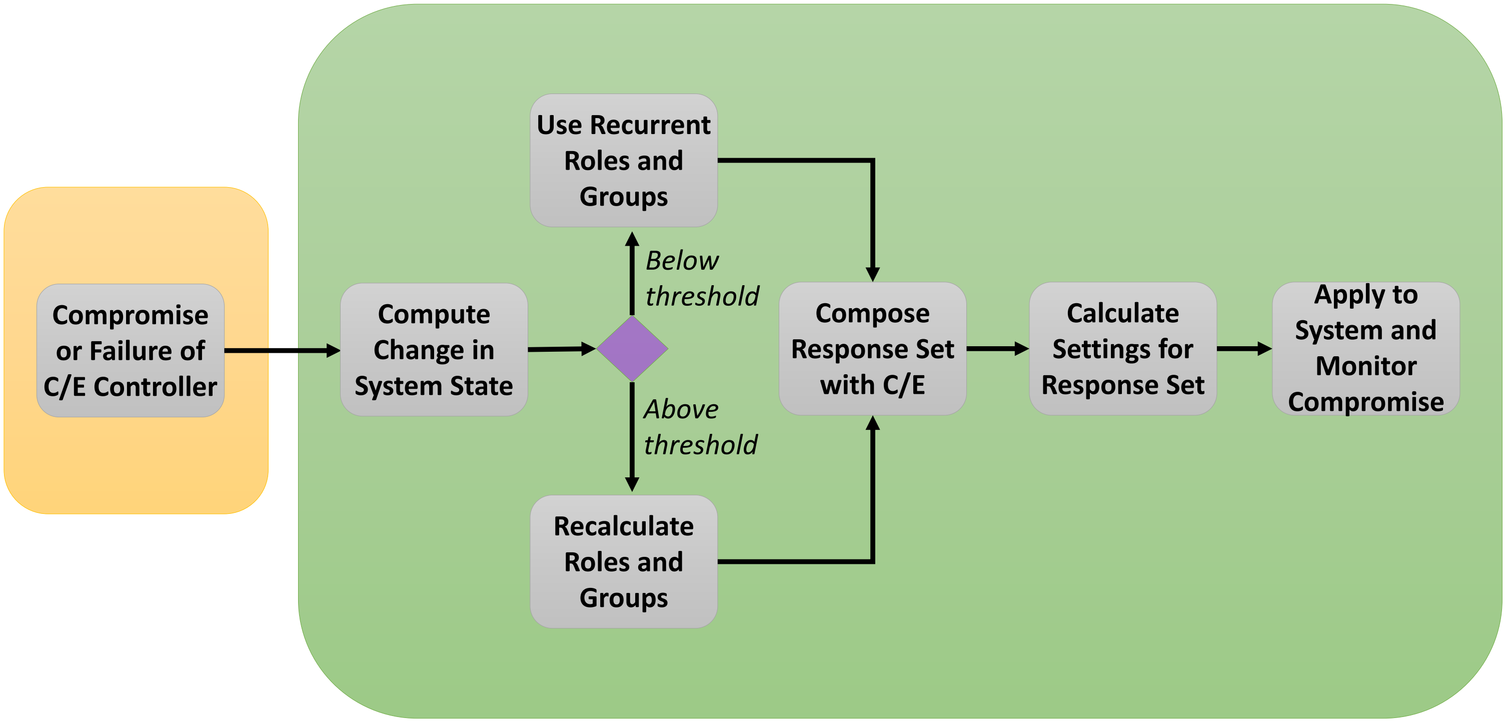

Compromise or Failure of C/E Controller
Compute Change in System State
Use Recurrent Roles and Groups
Below threshold
Above threshold
Recalculate Roles and Groups
Compose Response Set with C/E
Calculate Settings for Response Set
Apply to System and Monitor Compromise

Figure 5.20: Control response strategy for remaining set of distributed controllers when a compromise or failure has occurred.

reduce the line flow % MVA closer to the original flow. For example, for the compromises of Controllers $\#2, 4, 5$, the response set reduced the deviation from the original loading of $11-12\%$ to $2-5\%$. Compromises at Controllers $7, 9, 10$ induced smaller deviations, but Controllers 7 and 9 were successful in reducing it from $0.8-4\%$ to $0.6-2\%$. The only case for which the response set was not effective was the compromise of Controller 9 when the line flow was increased by 2.7% MVA and response set further increased it to 3.1% MVA. This result could be due to the system topology and/or the settings chosen for the response set. The optimization method for selecting these control settings for D-FACTS can be improved on and designed to be more fine-grained for small changes in line flows. Finally, the compromise of multiple controllers was also tested with Controllers $2, 10$ and Controllers $4, 5, 9$. For both cases, the increases in line flow were reduced satisfactorily.

Nevertheless, as observed from the compromised line flow results, the D-FACTS can disrupt the line flows in the power system but do not severely impact the operation of the grid. Their compromise must be mitigated, and perhaps using an automatic response strategy, as presented, is sufficient to address the compromises as the intrusion or failure is investigated. However, there are classes of distributed controllers for which compromises can cause significant and immediate consequences for the power system. An example is if we consider generators as distributed controllers and evaluate the impact of generator outages. In particular, we can study Remedial Action Schemes (RAS) that employ generator redispatch to mitigate power system contingencies. In Chapter 6, an analytic corrective control selection for fast, automated remedial action schemes is formulated using the controller role and group techniques. It identifies the critical or most effective generators to use for redispatch, significantly reducing the search space and computation time.

5.5 Overall Framework

5.5.1 Stability

When developing control defense strategies, the impact on both the system controllability *and* stability must be considered. Within distrusted control, the cyber attacks launched by the adversary can cause various control changes in the power system. Despite full system control, these malicious changes can destabilize the system, unless we monitor the system stability and react quickly with our uncompromised distributed controllers. Therefore, it is necessary to perform stability assessments during detrimental events such as failure or compromise of distributed controllers. If stability is lost, a very serious situation is encountered and sophisticated, additional strategies are needed to attempt to regain it or minimize damage.

Developing these stability control strategies is beyond the scope of this work, but those methods can be used in conjunction with the presented framework. The overall framework, including stability control strategies, will be provided later in this section. Nonetheless, it is pertinent that the stability is monitored after the compromise and also after the response of the remaining distributed controllers. If system instability or near instability is detected, a stability control method must be employed immediately.

As discussed in Section 3.3, there are various categories and types of stability. For this application, we apply linear system stability concepts—often used for small-signal stability analysis in power systems. Depending on the distributed controller being studied, the stability type and monitoring method will vary (i.e., generators and transient stability or D-FACTS and angle stability). Nonetheless, for the example D-FACTS device, linear system stability is performed as a simple approach and is applied by monitoring the eigenvalues of the system.

Small-signal stability analyzes the ability of the power system to maintain synchronism after a small disturbance. It is utilized to determine how close the system is to instability and understand the system response to these disturbances. The system is linearized about an equilibrium point and eigenvalues are calculated from the linear system matrix [86]. This model-based calculation of small-signal stability can be calculated in the following manner. The power system is described by:

$$\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}, \mathbf{y}) \qquad \mathbf{0} = \mathbf{g}(\mathbf{x}, \mathbf{y}) \tag{5.31}$$

where $\mathbf{x}$ is the vector of state variables and $\mathbf{y}$ is the vector of the algebraic variables. Subsequently, the system is linearized about the equilibrium point as:

$$\mathbf{\Delta \dot{x}} = \mathbf{A\Delta x} + \mathbf{B\Delta y} \tag{5.32}$$

$$\mathbf{0} = \mathbf{C\Delta x} + \mathbf{D\Delta y} \tag{5.33}$$

Next, variable $\boldsymbol{\Delta y}$ in (5.32) is substituted using (5.33) to derive a differential equation consisting solely of variable $\boldsymbol{\Delta x}$:

$$\mathbf{\Delta \dot{x}} = (\mathbf{A} - \mathbf{BD^{-1}C})\mathbf{\Delta x} \tag{5.34}$$

$$\mathbf{A_{sys}} := \mathbf{A} - \mathbf{BD^{-1}C} \tag{5.35}$$

$$\mathbf{\Delta \dot{x}} = \mathbf{A_{sys}\Delta x} \tag{5.36}$$

Equation (5.36) represents the deviation of the system's state away from the equilibrium point. Thus, small-signal analysis is performed by studying the eigenvalues and other properties of $\mathbf{A_{sys}}$. For simplicity, matrix $\mathbf{A_{sys}}$ will be referred to as $\mathbf{A}$ from hereon. The eigenvalues λ_i, $i = 1..n$, correspond to the modes of the system and are the solutions of the following equation:

$$\det(\mathbf{A} - \lambda\mathbf{I}) = \mathbf{0} \tag{5.37}$$

Assuming all the eigenvalues are distinct, for each λ_i there exists a right eigenvector $\mathbf{v_i}$ such that:

$$\mathbf{Av_i} = \lambda_\mathbf{i}\mathbf{v_i} \tag{5.38}$$

Similarly, for each eigenvalue there exists a left eigenvector $\mathbf{w_i}$ and the right and left eigenvectors are orthogonal.

$$\mathbf{w_i}^\mathbf{T}\mathbf{A} = \mathbf{w_i}^\mathbf{T}\lambda_\mathbf{i} \qquad \mathbf{A^T w_i} = \lambda_\mathbf{i}\mathbf{w_i} \tag{5.39}$$

Equation (5.36) needs to be decoupled to clarify the effect of the matrix $\mathbf{A}$'s parameters to the state vector $\mathbf{x}$. The decoupling can be conducted using the matrix of right and left eigenvectors. Define the modal matrices $\mathbf{V}$ and $\mathbf{W}$ as:

$$\mathbf{V} = \begin{bmatrix} \mathbf{v_1} & \dots & \mathbf{v_n} \end{bmatrix} \qquad \mathbf{W} = \begin{bmatrix} \mathbf{w_1^T} \\ \dots \\ \mathbf{w_n^T} \end{bmatrix} \tag{5.40}$$

Equation (5.38) is rewritten as:

$$\mathbf{A}V = V\mathbf{\Lambda} \tag{5.41}$$

where

$$\mathbf{\Lambda} = Diag(\lambda_i) \tag{5.42}$$

It follows that

$$\mathbf{V^{-1}AV} =\mathbf{\Lambda} \tag{5.43}$$

To decouple the variables, define vector $\mathbf{z}$ as

$$\mathbf{\Delta x} = \mathbf{Vz} \tag{5.44}$$

$$\mathbf{\Delta \dot{x}} = \mathbf{V\dot{z}} = \mathbf{A\Delta x} = \mathbf{AVz} \tag{5.45}$$

$$\mathbf{\dot{z}} = \mathbf{V^{-1}AVz} =\mathbf{\Lambda z} \tag{5.46}$$

Since $\mathbf{\Lambda}$ is a diagonal matrix, Equation (5.46) can be uncoupled as:

$$\dot{z_i} = \lambda_i z_i \tag{5.47}$$

After applying (5.47) to (5.44), the response $\mathbf{\Delta x}(t)$ can be rewritten as an equation of individual eigenvalues and right eigenvectors [86].

$$\mathbf{\Delta x}(t) = \sum_{i=1}^{n} \mathbf{v_i} z_i(0) e^{\lambda_i t} \tag{5.48}$$

The resultant complex eigenvalues are then analyzed to determine the state of the system, in terms of stability, after a small disturbance. The following characteristics are utilized in judging the eigenvalues [87]:

- Positive real part of an eigenvalue indicates potentially unstable states.
- Negative eigenvalue with significantly large magnitude can indicate extremely fast system states that may cause numerical instability.
  - Often caused by specific exciter models that contain extremely fast feedback loops; special consideration in the numeric integration algorithm is warranted

Therefore, the eigenvalues of the power system can be calculated and used to determine the stability. To incorporate into the control response strategy presented earlier, specifically for D-FACTS devices, PowerWorld [84] was used to automatically compute the eigenvalues. In particular, the single machine infinite bus (SMIB) eigenvalue tool was applied. Essentially, small-signal stability analysis is performed with a system associated with a single generator connected to the rest of the system through an equivalent transmission line. The equivalent line's impedance is computed using the driving point impedance looking into the system and the rest of the system is assumed to be an infinite bus. The infinite bus voltage is set to match the generator's real and reactive power injection and voltage [86, 87].

PowerWorld builds this dynamic model of the SMIB and it includes all the generator's dynamic models: machine model, exciter, governor, and stabilizer. The linear matrix of the SMIB and all its dynamic states is composed and eigenvalue analysis is performed on the derived $\mathbf{A_{sys}}$, as formulated earlier. Table 5.4 compromise scenarios are augmented with the stability assessment of monitoring the eigenvalues after compromise and response. Examples of these assessments are presented in Tables 5.5-5.7 for the compromise of Controller #4 and in Tables 5.8-5.10 for the compromise of Controller #10. The details of the compromise and response were provided previously in Table 5.4.

For this D-FACTS compromise example, the eigenvalues are not significantly impacted, though slight variations can be observed from the SMIB eigenvalues. The controllers do not considerably change the system state, thus, their impact is minimal on the overall stability. However, this impact depends on the type of controller, so stability assessment must always be performed generally for the control response framework. We also observe that Gen.6 has a positive real part for Eigenvalue 1, which could indicate potential instability, but the value is quite small and remains between 0.03 and 0.04 for all of the tested compromise cases. It exists during normal operation and does not change dramatically as the compromise and response situations are applied. Nonetheless, SMIB eigenvalue analysis is a simplistic approach that was chosen to illustrate the type of assessment needed; more sophisticated methods are needed to gain more accurate eigenvalue results such that positive eigenvalues, small or large, can be assessed more rigorously.

All in all, the overall framework for addressing the compromise or failure of a distributed controller can be summarized as shown in Figure 5.21.

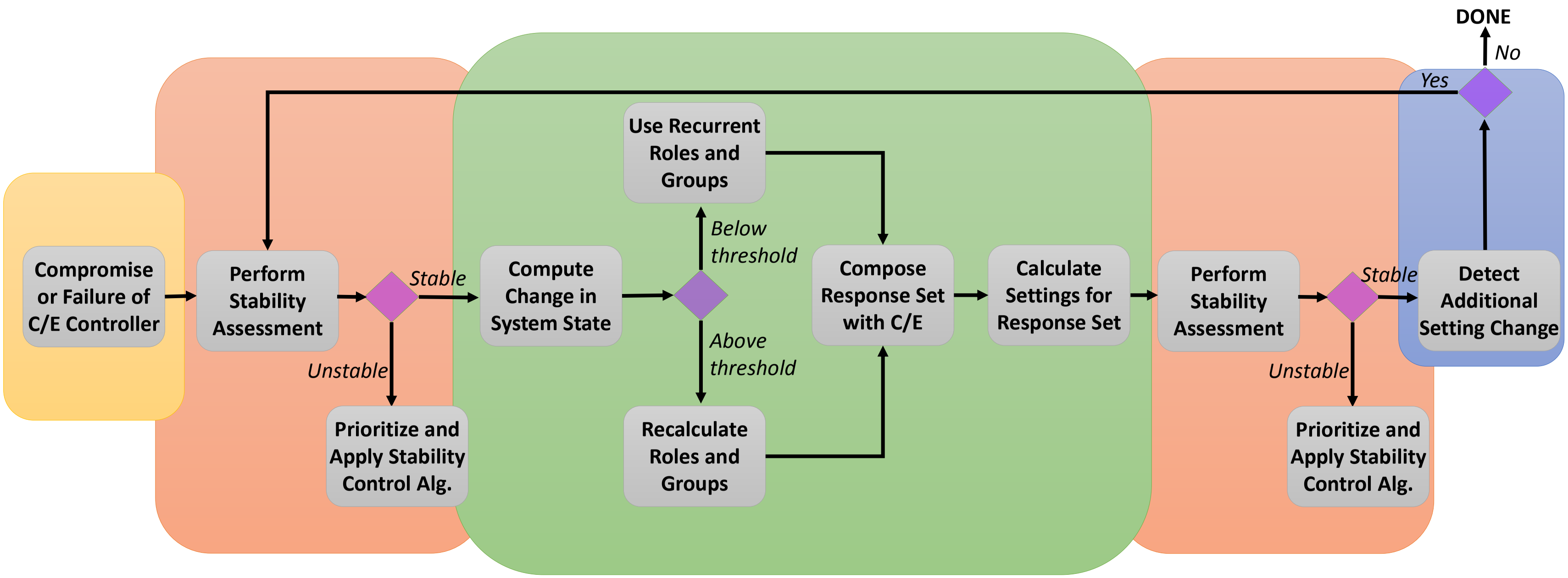

DONE
No
Yes
Compromise or Failure of C/E Controller
Perform Stability Assessment
Stable
Unstable
Prioritize and Apply Stability Control Alg.
Compute Change in System State
Below threshold
Above threshold
Use Recurrent Roles and Groups
Recalculate Roles and Groups
Compose Response Set with C/E
Calculate Settings for Response Set
Perform Stability Assessment
Stable
Unstable
Prioritize and Apply Stability Control Alg.
Detect Additional Setting Change

Figure 5.21: Overall control response framework given compromise or failure of distributed controllers.

The distributed control response framework, given the stability assessment does not detect instability, responds to the compromise of a critical or essential controller and uses either recurrent or current CE controllers to respond. The settings for the controllers are selected using a controller-specific control algorithm and applied to the system to best reduce system stress and maintain operation during the compromise. If an additional setting change is detected in the compromised controller, the response framework continues. If a redundant controller is compromised, this framework can be applied, but since the redundant device can be removed without affecting system controllability, resources can be conserved and we can avoid changing other controller settings unnecessarily. In fact, the redundant controller should be taken offline as the compromise is investigated.

Therefore, the control response framework can be utilized when a device, within a distributed controller set, is compromised or fails. It employs the essential or critical controllers to provide effective response, as these controllers have the largest control span over the system—they encompass all the equivalent line flows, excluding that of a compromised device. Initially, in Chapter 4, it was suggested the control support group members could be utilized in response. This remains true, but is less effective in a smaller system. The response controllers need to have wide control span, which is not observed in a small system in which only a couple or a few controllers compose a control support groups. Nonetheless, as the essential or critical controllers encompass all the line flows (via equivalent line flows), they will *always* provide the control necessary to best mitigate the compromise. Redundant controllers to the corresponding compromised controller can additionally be used, if not already within the response set, only if the transformed sensitivities are high. Therefore, the main contributions of this chapter are summarized as:

1. The transformed basis resulting from the factorization of the sensitivities can be decomposed to discover the composition of the equivalent line flows and to rank redundant controllers.

    - Can aid controller placement to avoid critical roles, avoid excessive redundancy, and also rank the redundant controllers.

2. The system state or operating point dependence of role and group assignments is explored and the results exhibit recurrent behavior.

  - The recurrent essential or critical controllers repeatedly have expansive control span and can be leveraged in response to compromises or failures.

3. A control response framework can be developed for the distributed controller compromise given compromise or failure of device(s) within the set.

   - This response can be immediately deployed to reduce system stress and mitigate compromise consequences, while the actual cause and removal of the compromise are investigated by IDS, intrusion recovery methods, or other security mechanisms.

4. The overall control response framework reacts whenever a setting change is observed with the compromised control and should include stability assessment.

   - Maintaining stability must be prioritized and its inclusion in the framework is necessary for a comprehensive response.

Table 5.3: Responding to Controller 2 Compromise with Various Response Controllers (C#) and Settings; Original MVA$_{L2}$ = 44 %

Controller #2 Compromise ($x_{DF} = -0.072pu, 55\%$ MVA$_{L2}$)			
Selection Method	**Response C#**	**Settings(pu)**	**MVA$_{L2}$**
Recurrent CE	1,3,8,9	-0.015,-0.054,0.072,-0.018	48.9%
Recurrent R	4,5,6,7,10	-0.054,-0.036,0.018,-0.009,-0.072	51.4%
Current CE	4,5,7,8,9	-0.054,-0.036,-0.009,0.072,-0.018	51.1%
Current R	1,3,6,10	-0.015,-0.054,0.0171,-0.072	49.3%
Current Ranked R	1,10	-0.015,0.072	53.4%

Table 5.4: Responding to Various Controller Compromises with Recurrent CE Response Set and Calculated Settings

C#$_{Compr.}$	x_{DF} (pu)	**MVA** $_{L\#,Orig.}$	**MVA** $_{L\#,Compr.}$	**C#**$_{Resp.}$	**Settings** (pu)	**MVA** $_{L\#,Resp.}$
2	-0.072	44.2%	55.7%	1,3,8,9	-0.015,-0.054, 0.072,-0.018	48.9%
4	-0.054	44.5%	56.8%	1,2,3,8,9	0.015,-0.072, -0.054,0.072,-0.018	46.8%
5	-0.036	67.6%	78.6%	1,2,3,8,9	0.015,-0.072, -0.054,-0.072,-0.018	71.9%
7	-0.009	23.5%	24.3%	1,2,3,8,9	0.0088,-0.0077, -0.0127,0.002,0.0017	22.9%
9	-0.018	32.8%	35.5%	1,2,3,8	-0.015,0.072, 0.0702,0.072	35.9%
10	-0.072	14%	17.6%	1,2,3,8,9	0.015,-0.072, -0.054,-0.072,0.018	15.7%
2,10	-0.072,-0.072	44.2%, 14%	55.5%, 17.3%	1,3,8,9	-0.015,-0.054, 0.072,0.018	49%, 16.3%
4,5,9	-0.054,-0.036, -0.018	44.5%, 67.6%, 32.8%	53.8%, 74.4%, 31.5%	1,2,3,8	0.015,-0.072, -0.054,-0.072	46.8%, 70.4%, 31.6%

Table 5.5: SMIB Eigenvalues for Normal Operation

	Eigenvalue 1	**Eigenvalue 2**	**Eigenvalue 3**	**Eigenvalue 4**	**Eigenvalue 5**
Gen.1	-0.6069 + j0.0000	-1.4846 + j12.4373	-1.4846 - j12.4373	-28.3854 + j0.0000	-40.9613 + j0.0000
Gen.2	-0.5872 + j0.0000	-1.5519 + j13.7166	-1.5519 - j13.7166	-28.5133 + j0.0000	-44.3302 + j0.0000
Gen.4	-0.5744 + j0.0000	-1.3451 + j11.7360	-1.3451 - j11.7360	-28.3722 + j0.0000	-40.7493 + j0.0000
Gen.6	0.0418 + j0.0000	-1.1822 + j13.8982	-1.1822 - j13.8982	-28.2034 + j0.0000	-43.3662 + j0.0000
Gen.7	-0.3296 + j0.0000	-1.1701 + j13.2015	-1.1701 - j13.2015	-28.2530 + j0.0000	-40.9798 + j0.0000

Table 5.6: SMIB Eigenvalues after Controller #4 Compromise ($x_{DF} = -0.054$)

	Eigenvalue 1	**Eigenvalue 2**	**Eigenvalue 3**	**Eigenvalue 4**	**Eigenvalue 5**
Gen.1	-0.6067 + j0.0000	-1.4871 + j12.4394	-1.4871 - j12.4394	-28.3866 + j0.0000	-40.9847 + j0.0000
Gen.2	-0.6171 + j0.0000	-1.5547 + j13.7892	-1.5547 - j13.7892	-28.5277 + j0.0000	-44.4127 + j0.0000
Gen.4	-0.5576 + j0.0000	-1.3927 + j11.7630	-1.3927 - j11.7630	-28.3917 + j0.0000	-41.2139 + j0.0000
Gen.6	0.0403 + j0.0000	-1.1842 + j13.9126	-1.1842 - j13.9126	-28.2054 + j0.0000	-43.4071 + j0.0000
Gen.7	-0.3290 + j0.0000	-1.1706 + j13.2035	-1.1706 - j13.2035	-28.2531 + j0.0000	-40.9866 + j0.0000

Table 5.7: SMIB Eigenvalues after Controller $\#1, 2, 3, 8, 9$ Response ($x_{DF} = 0.015, -0.072, -0.054, 0.072, -0.018$)

	Eigenvalue 1	**Eigenvalue 2**	**Eigenvalue 3**	**Eigenvalue 4**	**Eigenvalue 5**
Gen.1	-0.6012 + j0.0000	-1.4534 + j12.3834	-1.4534 - j12.3834	-28.3659 + j0.0000	-40.6191 + j0.0000
Gen.2	-0.6310 + j0.0000	-1.5517 + j13.8179	-1.5517 - j13.8179	-28.5322 + j0.0000	-44.4035 + j0.0000
Gen.4	-0.5091 + j0.0000	-1.4280 + j11.7232	-1.4280 - j11.7232	-28.3895 + j0.0000	-41.4532 + j0.0000
Gen.6	0.0408 + j0.0000	-1.1831 + j13.9026	-1.1831 - j13.9026	-28.2043 + j0.0000	-43.3768 + j0.0000
Gen.7	-0.3467 + j0.0000	-1.1832 + j13.2702	-1.1832 - j13.2702	-28.2685 + j0.0000	-41.1719 + j0.0000

Table 5.8: SMIB Eigenvalues for Normal Operation

	Eigenvalue 1	**Eigenvalue 2**	**Eigenvalue 3**	**Eigenvalue 4**	**Eigenvalue 5**
Gen.1	-0.6069 + j0.0000	-1.4846 + j12.4373	-1.4846 - j12.4373	-28.3854 + j0.0000	-40.9613 + j0.0000
Gen.2	-0.5872 + j0.0000	-1.5519 + j13.7166	-1.5519 - j13.7166	-28.5133 + j0.0000	-44.3302 + j0.0000
Gen.4	-0.5744 + j0.0000	-1.3451 + j11.7360	-1.3451 - j11.7360	-28.3722 + j0.0000	-40.7493 + j0.0000
Gen.6	0.0418 + j0.0000	-1.1822 + j13.8982	-1.1822 - j13.8982	-28.2034 + j0.0000	-43.3662 + j0.0000
Gen.7	-0.3296 + j0.0000	-1.1701 + j13.2015	-1.1701 - j13.2015	-28.2530 + j0.0000	-40.9798 + j0.0000

Table 5.9: SMIB Eigenvalues after Controller #10 Compromise ($x_{DF} = -0.072$)

	Eigenvalue 1	**Eigenvalue 2**	**Eigenvalue 3**	**Eigenvalue 4**	**Eigenvalue 5**
Gen.1	-0.6070 + j0.0000	-1.4852 + j12.4382	-1.4852 - j12.4382	-28.3857 + j0.0000	-40.9670 + j0.0000
Gen.2	-0.5864 + j0.0000	-1.5531 + j13.7169	-1.5531 - j13.7169	-28.5137 + j0.0000	-44.3428 + j0.0000
Gen.4	-0.5740 + j0.0000	-1.3453 + j11.7352	-1.3453 - j11.7352	-28.3721 + j0.0000	-40.7492 + j0.0000
Gen.6	0.0375 + j0.0000	-1.1930 + j13.9691	-1.1930 - j13.9691	-28.2128 + j0.0000	-43.5824 + j0.0000
Gen.7	-0.3468 + j0.0000	-1.1959 + j13.3143	-1.1959 - j13.3143	-28.2746 + j0.0000	-41.3348 + j0.0000

Table 5.10: SMIB Eigenvalues after Controller #1, 2, 3, 8, 9 Response ($x_{DF} = 0.015, -0.072, -0.054, -0.072, 0.018$)

	Eigenvalue 1	**Eigenvalue 2**	**Eigenvalue 3**	**Eigenvalue 4**	**Eigenvalue 5**
Gen.1	-0.6008 + j0.0000	-1.4503 + j12.3781	-1.4503 - j12.3781	-28.3643 + j0.0000	-40.5852 + j0.0000
Gen.2	-0.6250 + j0.0000	-1.5405 + j13.7842	-1.5405 - j13.7842	-28.5235 + j0.0000	-44.2639 + j0.0000
Gen.4	-0.5425 + j0.0000	-1.4163 + j11.7660	-1.4163 - j11.7660	-28.3987 + j0.0000	-41.4346 + j0.0000
Gen.6	0.0386 + j0.0000	-1.1929 + j13.9661	-1.1929 - j13.9661	-28.2123 + j0.0000	-43.5767 + j0.0000
Gen.7	-0.3314 + j0.0000	-1.1867 + j13.2654	-1.1867 - j13.2654	-28.2627 + j0.0000	-41.2006 + j0.0000

CHAPTER 6

ANALYTIC CORRECTIVE CONTROL SELECTION FOR FAST, AUTOMATED REMEDIAL ACTION SCHEMES

6.1 Problem Statement

When abnormal, stressed conditions occur in the power grid, corrective actions are necessitated to prevent or mitigate system instability. The North American Electric Reliability Corporation (NERC) defines a remedial action scheme (RAS) as an automatic protection system that detects those conditions and takes corrective actions to maintain system reliability, not limited to only component isolation [88]. These actions may include changes to demand, generation, or system topology to maintain stability, acceptable voltage levels, and allowable power flows. Corrective actions are used to restore the power system's safe operational mode; further details on these actions are described in [88–91].

These violations can occur for a variety of reasons, including increasing penetration of renewables to the micro-grids that connect or disconnect smaller entities to or from the bulk power grid infrastructure. Furthermore, cyber attacks have become a serious concern in the recent years. In fact, the Department of Homeland Security reported that from 2009 to 2014, about 40% of total critical infrastructure cyber incidents occurred in the energy sector [55]. In December 2015, one of the first large-scale attacks on a power grid occurred in Ukraine, where cyber attacks led to the disconnection of seven substations and power outage to 225,000 customers for several hours [56]. Power system cyber vulnerabilities have increased due to the shift from proprietary control protocols to popular, accessible network protocols, and other modernization factors. An adversary can exploit these unsecured access points and can potentially drive the power system to an unsafe state. Even more disconcerting is the ability of cyber attacks to cause physical damage to the grid, as demonstrated by [11].

The electric power grid is a complex, interconnected cyber-physical system, and as such, RAS procedures must be capable to protect against accidental failures and malicious endeavors such as cyber attacks; especially, when severe physical consequences can result. Therefore, techniques that provide the most effective response, are computationally efficient, and are suitable for online RAS applications (e.g., cyber attacks) in large-scale power systems are desired. Conventional RAS designs use offline calculations to determine the best control action for the most credible contingencies with different topology, generation, and load scenarios. These actions are subsequently stored and executed in real-time when the contingency occurs [92,93]. Cyber attack contingencies cannot be accounted for in a look-up table—these incidents are often unpredictable, and their characteristics are constantly changing. Predefined tables may not encompass all possibilities and require extensive data management. Thus, online RAS is necessitated as the most current system state and real-time calculation of corrective controls are required to provide the most suitable and effective response.

For online RAS applications, computation time is paramount. In the conventional implementation, various control actions and settings calculated with the post-contingency state must be iterated through to determine the most suitable action without significant concern for running time. However, online RAS designs require the computation time to be as fast as possible, as the corrective control must be executed immediately. It quickly becomes computationally burdensome to iterate through control actions and settings in real-time.

There have not been many efforts to design online RAS, though there are some strategies that consider system dynamics when selecting corrective control actions [94–96]. Transient stability, although allowing more thorough analysis, considerably increases the computation time. A Smart RAS scheme [97] was developed by Wang and Rodriguez that utilizes synchrophasor-measurements of real power on tie-lines between two grid areas to trigger RAS. They are motivated by intermittent renewable generation and load mutability and design a no-parameter model and no-setting criteria to best predict and mitigate instability (by effectively triggering RAS). Atighechi et al. [98] designed a fast load-shedding RAS method for the British Columbia (BC) Hydro system that applies dynamic and steady-state responses for different contingencies to best mitigate transient stability and voltage collapse.

Lastly, Hitachi is working with Bonneville Power Administration (BPA) to build [99] a new RAS prototype that uses synchrophasor input and online contingency to account for new sources of power system disturbances from renewable energies and electric vehicles. Their design, summarized in [99], computes every 30 seconds and automatically calculates response actions against contingencies by using historical snapshots. The Hitachi-BPA project is the most prominent online RAS project, to our knowledge, and motivates the need and application of such designs. An automated RAS method was recently developed by Kazerooni [100], within our research team, that contributes to that effort and seeks to use steady-state analysis techniques to increase speed.

As the online RAS design by Kazerooni is one of the few works that considers online RAS design and full details of the algorithm are available, it is utilized to develop the analytic corrective control selection (ACCS) algorithm. ACCS seeks to further improve speed and efficiency by identifying the most effective corrective controls to use and avoiding calculation with all available controls. This chapter presents an algorithmic solution that processes sensitivities and applies clustering and factorization techniques to determine the critical controls that should be used for fast, automated RAS. In the literature reviewed, RAS designs do not employ ACCS or similar algorithms. This is due to the dearth of online RAS methods and thus, lack of need to narrow the corrective control search space as the calculations are performed offline. In particular, for generation redispatch, which is the focus of this work, usually economics are the primary concern and the cheapest generators are selected [101].

The fast load-shedding RAS design by Atighechi et al. [98], mentioned previously, selects load shedding candidates using sensitivity analysis, similar to ACCS. Their method utilizes dynamic performance and steady-state voltage sensitivity analysis at each bus and the final load shedding sequence is determined by the combination of those analyses, load level, type, and system topology. Another algorithm for control strategies against voltage collapse using relays is presented by Song et al. in [102] where critical relays are identified using sensitivity analysis. These relays are critical in a negative sense, meaning their operation may significantly deteriorate the system in terms of voltage stability. In both of these works, although sensitivity analysis is leveraged, controllability analysis concepts are not applied to determine the most effective controls. Specifically, the corrective controls with largest control span and, thus, most significant impact on the system are not found.

In this work, the analytic corrective control algorithm (ACCS) determines critical controls to be utilized with fast, automated RAS given a power system contingency. The critical controls identified comprise the minimum set that is most effective in reducing the violations at various, stressed areas of the system and significantly improves computation time, indicating suitability for online RAS applications. The controllability-analysis based formulation utilizes clustering and factorization techniques that process sensitivities, as was introduced in Chapter 4. Thus, this application further demonstrates the versatility and utility of the distributed controller role and interaction discovery algorithm, as will be detailed in the following sections.

6.2 Solution Overview

Kazerooni [100] developed an automated RAS procedure to protect large-scale power systems against accidental failures or malicious endeavors such as cyber attacks using steady-state analysis techniques. Specifically, the procedure focused on generation redispatch techniques [94, 103, 104]. This work was developed within our research team and as one of few online RAS designs with fully available details; we thus utilize its framework to develop the analytic corrective control selection algorithm. Nonetheless, this novel online RAS algorithm offers fast computation and proposes a fast, greedy algorithm through control subspace synthesis that utilizes heuristics to narrow the search space, which will be discussed further.

The RAS algorithm is capable of online execution for rapid analysis while providing resilient solutions. Since RAS designs that utilize transient stability analysis are computationally expensive and not yet appropriate for online applications, this steady-state analysis based RAS algorithm is favorable for situations in which control actions need to be calculated as quickly as possible (e.g., during a cyber attack). Additionally, this automated RAS procedure develops a security assessment measure, the violation index, that evaluates the security of each candidate action. The violation index depends on the aggregate of violations in the physical and operating constraints of the system and is used by the online RAS to select the most appropriate controls.

Further details on this algorithm are provided in Section 6.3.

The critical generators are identified to reduce the search space, thus reducing the exhaustive search for generation redispatch calculation. The RAS algorithm employs a proximity-based critical generator identification (PCGI) method. Kazerooni leveraged insight that some generators may be significantly more effective than others for system security. Empirical studies were performed that indicated geographically clustered violations (e.g., lines and buses) and, as a result, generators nearest to these stressed areas were identified as critical. Graph theory and proximity measures are applied to discover these critical generators, as described in Section 6.3.2. In this manner, insignificant generators are eliminated from the search. Although this method is effective in reducing the search space, it possesses several disadvantages:

- A user-specified default number of critical generators is utilized; a smaller set of critical generators may exist and reduce search space further.
- The PCGI method is based on empirical analyses and may not apply to all systems and/or contingencies.
- The method does not consider effective generators that are located away from the violated area(s).

The work presented in this chapter provides an analytic critical control identification method. Rather than relying on proximity-measures derived empirically, a controllability analysis-based formulation is developed. The critical controls identified are the most effective in reducing the violations at the various stressed areas of the system. In fact, they are essential for the controllability of those violated areas. This is achieved by leveraging sensitivities, considering the relationship between the corrective controls (e.g., generators) and the violations (e.g., overloaded lines). Clustering and factorization methods are applied to analytically discover the critical controls. While this chapter focuses on generators as the critical control for generation redispatch, this methodology is broadly applicable to any corrective control for which a sensitivity matrix in relation to the violated components can be derived.

As presented in the evaluations (Section 6.7), the analytic corrective control selection (ACCS) algorithm not only utilizes a lower number of critical generators than the proximity-based method but also achieves significant reduction of the violation index. When PCGI is set to the same number of resultant critical generators, a different set is found and is less effective in reducing the violation index. Therefore, ACCS is able to significantly reduce the computation time while also identifying the most broadly effective critical controls for all violations.

With the inclusion of the ACCS algorithm within the online RAS design, fast and effective response is achieved for generation redispatch applications. In particular, with its automated and online response ability, the overall design can be used as a defense mechanism to maintain system reliability when cyber attacks occur. Characterized as a large disturbance, generator outage(s) can have significant impact on the system that range from overloaded lines, to loss of service to load(s), to sensitive equipment damage. In the worst case, cascading effects from the stressed system can lead to blackout. Generator outages can be caused by certain system conditions and other contingencies (e.g., faults or equipment malfunction), but also as a result of cyber attacks.

Two real-world examples of generator outages caused by cyber adversaries include the Ukraine event and the Aurora generator test. As mentioned in the previous section, the December 2015 large-scale cyber attack on the Ukraine power grid caused a blackout for thousands of customers by disconnecting seven substations. Specifically, the attackers, after gaining remote control of the SCADA distribution management system, caused unnecessary "scheduled" maintenance outages of various generators (associated with the targeted connected loads) [56, 105]. In the 2007 Aurora generator test, researchers at Idaho National Laboratories (INL) demonstrated that using only cyber commands, they could cause a generator to explode. The command consisted of rapidly switching the generator's circuit breakers out of phase with the rest of the grid [11]. This case particularly demonstrates the serious physical consequences that can result from cyber attacks.

Effective response to cyber attacks requires actions from both the cyber and physical layers of the power grid. For example, a compromised, outaged generator must be "cleaned" of the intrusion using cyber mechanisms such as intrusion detection and/or recovery systems. Meanwhile, the physical power system must react to maintain system reliability by maintaining continuous service, relieving stressed components, and preventing damage. In the case

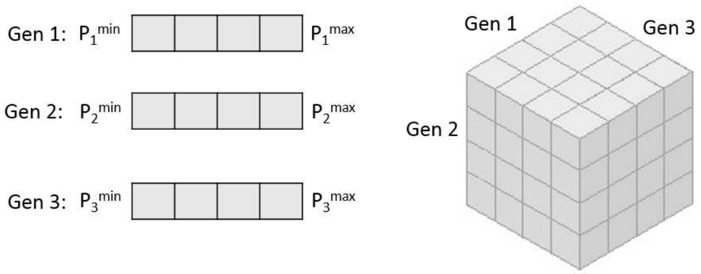


Figure 6.1: Security-compliant generator dispatch subspace synthesis.

of generator outage, one approach is utilizing generation redispatch to ensure system operation. A cyber-physical response (CPR) mechanism that employs both layers to respond to various contingencies is being developed within our research team as well, as detailed in [23].

The online RAS formulation with ACCS enables quick and effective response to generator outage that utilizes the minimum set of generators with the most impact in the system, for the specific outage(s). As the generation redispatch is automatic and calculated online, it can follow the trajectory of the cyber attack and update the redispatch to best maintain system reliability. In this manner, this design can aid in defending the attacked system, responding with the most suitable remedial actions even as the attack is changing. This compromised, outaged generator scenario is further formulated in Section 6.7.

Details on the automated RAS scheme and PCGI are given in Section 6.3, and ACCS is presented in Section 6.4-6.6. Finally, evaluations are presented in Section 6.7 with the IEEE 24-bus case and the IEEE 118-bus case, and conclusions are provided in Section 6.8.

6.3 Automated Remedial Action Scheme Algorithm

The automated RAS procedure developed by Kazerooni, particularly the selection of critical generators, is briefly described in this section, with the full details provided in [100]. For generation redispatch applications, the feasible control subspace of the power system with n generators is discretized into equally distant n-dimensional cubes, as shown in Figure 6.1. Each point in the grid corresponds to one control action vector dependent on each generator's allowed dispatch MW range. The power flow is solved for each action and the resultant security constraints are evaluated. The actions that do not violate any constraints are identified as possible RAS solutions.

6.3.1 Proposed Violation Index

It is possible that no control actions can be taken that will satisfy all of the security constraints. In this case, the actions that violate fewer constraints and provide a more secure state are selected. A violation index may be defined to evaluate the resultant security of the system after an action. Aggregate MVA overload (AMWCO) is introduced in [106], which evaluates the system security based on the total number of power flow violations:

$$AMWCO = \sum_{(i,j)\in\mathcal{I}} \max\{0, P_{ij}^{(k)} - P_{ij}^{max}\} \tag{6.1}$$

where $P_{i,j}$ is the active power on the line between buses i and j, $P_{i,j}^{max}$ is the flow limit of this line, and $\mathcal{I}$ is the set of all (i, j) for which there is a line connecting bus i to bus j. This security index considers only the line flow violations, and excludes the bus voltage or the generator power limits. To account for additional types of limits, a general violation index is defined,

$$Violation^{(k)} = w_I S_I^{(k)} + w_V S_V^{(k)} + w_P S_P^{(k)} + w_Q S_Q^{(k)} \tag{6.2}$$

where $S_I^{(k)}$, $S_V^{(k)}$, $S_P^{(k)}$, and $S_Q^{(k)}$ are respectively the security indices of the line flows, bus voltages, generator active power and reactive power for action k. The corresponding weights w_I, w_V, w_P and w_Q capture varying importance of different violation types. These weights are currently assigned heuristically with generator limits weighed more heavily and current limits with the lowest weight. A systematic approach for assigning weights will be developed in future work. The security index for the line flows is given by:

$$S_I^{(k)} = \sum_{(i,j)\in\mathcal{I}} \frac{\max\{0, P_{ij}^{(k)} - P_{ij}^{max}\}}{P_{ij}^{max}} \tag{6.3}$$

In this case, the MVA overloads are normalized by the line flow limits. The violation index for bus voltage and generator limits are defined similarly and the aggregate violations are normalized by their upper bound limits. In this manner, the terms corresponding to each constraint that appear in the violation index reflect their actual importance to the system security.

Furthermore, the violation index in this design is static, though dynamic versions can be incorporated. As the current focus is to reduce computation time to develop fast, effective RAS for online use, the static index was applied. Indices based on transient stability analysis and dynamic response may significantly increase calculation time, and future work will study how this can be improved.

6.3.2 Proximity-based Critical Generation Identification

The computation complexity of the control subspace synthesis algorithm is $\mathcal{O}(R^n)$, where R is the discretization granularity for the individual generators, n is the number of generators that can participate in the dispatch, and $\mathcal{O}()$ is the big O time complexity notation. The complexity is exponential in the number of participating generators, which results in significant computational burden for large systems. To tackle this issue, one approach is to reduce the number of participating generators. Individual generators may have varying impact on the overall system security with some generators crucial and others less significant. Excluding less significant generators from the search reduces the number of candidates, while still providing enough candidates to keep the performance near optimal.

A greedy algorithm is employed to identify the insignificant generators based on graph theory and proximity measures. For every contingency, the lines and buses at which the constraints are violated are identified. Based on empirical analyses, it is observed the identified lines and buses are often clustered at one or multiple locations in the network. The generators close to the areas under stress are classified as crucial and the ones which are further away are labeled as insignificant. The most critical generators are determined in the first level of the algorithm and less critical ones are determined in subsequent levels. The levels are executed consecutively until the number of critical generators reaches a user-specified value. Algorithm 1 describes the procedure.

Algorithm 1 Proximity-based Critical Generator Identification (PCGI)

```
procedure PCGI(Network State and Limits)
    $\mathcal{U}^1_{Critbus}$ = Set of busses with Violations
    $\mathcal{U}^1_{Critgen} = \mathcal{U}_{PV} \cap \mathcal{U}^1_{Critbus}$
    $k = 1$
    while $Size(\mathcal{U}^k_{Critgen}) < CritgenMax$ do
        $\mathcal{U}^k_{Critbus} = \mathcal{U}^{k-1}_{Critbus} \cup N(\mathcal{U}^{k-1}_{Critbus})$
        $\mathcal{U}^k_{CritGen} = \mathcal{U}^{k-1}_{CritGen} \cup (\mathcal{U}_{PV} \cap \mathcal{U}^k_{Critbus})$
        $k = k + 1$
    end while
end procedure
```

In Algorithm 1, $\mathcal{U}^k_{Critbus}$ and $\mathcal{U}^k_{Critbus}$ are respectively the set of critical buses and critical generators at level k, $CritGenMax$ is the maximum number of critical generators defined by the user and $Size(x)$ returns the size of the set x. This heuristic technique provided decent results for the cases tested by Kazerooni but does not provide the best selection of critical generators, as discussed in Section 6.2. Therefore, a systematic approach with theoretical guarantees to identify the truly optimal set of critical generators is desired. ACCS seeks to provide this analytic solution based on controllability analysis, subsequently identifying the most effective generators in *controlling* and thus reducing the stress of the post-contingency overloads or other violations.

Finally, computation time can be further reduced through using DC power flow (DCPF) instead of AC power flow to get the system states for each possible action. Since the DCPF solution is not accurate, it could be used as a fast screening tool before detailed ACPF analysis is performed on the top candidates. The violation index of all the candidate actions is calculated based on their DCPF solutions and the top candidates are selected. AC power flow is solved for only the top candidates; exact violation indices are calculated and the best action is obtained accordingly.

6.4 Analytic Corrective Control Selection

The proposed method leverages the sensitivities between the available corrective controls and the violated components. Clustering is performed to discover violation groups, discussed in Section 6.5, and factorization techniques are applied to identify the critical corrective controls, presented in Section 6.6. The algorithm is controllability analysis-based as rank conditions are applied in the factorization process. The critical corrective control selection can be alternatively described as discovering the most effective controls in *controlling* the violated components and reducing the overall system stress. This interpretation and derivation of techniques was introduced for the distributed controller role and interaction discovery algorithm presented in Chapter 4.

The ACCS algorithm is general and can be applied to any type of corrective control and violations, as long as the appropriate sensitivity matrix is computed. To aid in the explanation of the method, this work utilizes a generator outage example, where the violations are line overloads and the corrective controls are generators.

6.4.1 Sensitivities of Critical Controls and Violations

A system's sensitivity matrix provides powerful information about the relationships between components in a system [107]. For generation redispatch, sensitivities provide insight into the interaction between available generators and violations. Considering generator outage(s) and line overload(s), the sensitivity of each line's real power flow to each available generator's real power changes is represented in the matrix $\boldsymbol{\Psi}$.

$$\Delta \mathbf{P_{flow.line,overloaded}} = [\boldsymbol{\Psi}] \cdot \Delta \mathbf{G_{MW}} \tag{6.4}$$

With $\boldsymbol{\Psi}$, the sensitivities pertaining to the available generators and overloaded lines can be processed to discover which generators cause the greatest impact on the line flows. A subset of the sensitivity matrix is used in the current approach, where rows are associated with overloaded lines and columns with the available generators (excluding the slack bus and outaged generator(s)). The identified effective controls should be utilized by the automated RAS procedure.

6.5 Clustering Violations

ACCS clusters the rows of $\mathbf{\Psi}$, the overloaded lines, and determines which overloaded lines impact each other and which do not. The results of this step provide:

- *Violation groups*: for generation redispatch, the sets of overloaded transmission lines that can be controlled independently

Each violation group discovered is comprised of overloaded lines that impact each other significantly; they are highly coupled. Within each set, it only makes sense to target one overloaded line to control, as controlling one line flow will always strongly impact the others in a predictable way. The generator(s) selected to reduce the overload of that one line will also be effective for the rest of the overloaded lines within the violation group, whereas a different violation group will have different sensitivities and require calculation for generator(s) most effective for those overloaded lines. In this manner, a target set of overloaded lines, the most sensitive from each violation group, can be selected to further process and determine the critical generators that can provide the best corresponding control.

To determine these violation groups, we perform k-means clustering upon the cosine similarities between the different overloaded line sensitivities [68]. By comparing the angles between row vectors of $\mathbf{\Psi}$, the overloaded lines, the coupled and decoupled sets of overloaded lines and their real power flows are found. To calculate and compare these angles, we utilize the coupling index (CI) and measure the cosine similarity [68]. The CI is equal to the cosine of the angle between two row vectors, $\mathbf{v_1}$ and $\mathbf{v_2}$ of the sensitivity matrix $\mathbf{\Psi}$, as shown below.

$$cos\theta_{\mathbf{v_1}\mathbf{v_2}} = \frac{\mathbf{v_1} \cdot \mathbf{v_2}}{\|\mathbf{v_1}\|\|\mathbf{v_2}\|} \tag{6.5}$$

The clusters, or violation groups, identified using the CI are approximately orthogonal to each other. The CI has values between -1 and 1. By clustering on the rows of the sensitivity matrix using CI, the coupled and decoupled sets of overloaded line flows can be determined. Thus, each cluster will be independent and decoupled from the other sets. Within the cluster, the line flows are coupled and dependent on one another.

For k-means clustering, we must provide k, the number violation groups we seek. However, we do not want to arbitrarily select k, as it will not be unlike the PCGI default number of critical generator specification. We would like an analytic solution that can determine the most suitable number of violation groups that is dependent on the system topology and current state, involving the generator outage and line overloads. The resultant clusters should be highly cohesive, the overloaded lines within each violation group should be very dependent on each other.

To leverage the sensitivity matrix and its inherent groupings, the proposed ACCS method uses the singular values that are computed using singular value decomposition (SVD). The SVD of a $m \times n$ matrix $\mathbf{\Psi}$ is:

$$\mathbf{\Psi} = \mathbf{U \Sigma V^T} \tag{6.6}$$

where $\mathbf{U}$ is an $m \times m$ orthogonal matrix, $\mathbf{V}$ is an $n \times n$ orthogonal matrix, and $\mathbf{\Sigma}$ is an $m \times n$ diagonal matrix with the singular values listed in decreasing order [72, 73]. The algorithm uses SVD to obtain a rank reduced approximation of a data set to generalize some properties or structure. One interpretation of the singular values is information on the largest contributions to the matrix and its general structure. Therefore, the most significant or largest singular values represent the most significant groups present in the data, which in our case is the sensitivity matrix.

Using the number of most significant singular values from the sensitivity matrix, ACCS achieves an initial guess for the number of clusters, k, for k-means clustering. To determine which singular values are most significant, ACCS calculates an *optimal hard threshold* using the techniques detailed by Gavish and Donoho, rigorously derived in [74], and henceforth referred to as the *hard threshold singular value* (HTSV) method. HTSV considers the recovery of low-rank matrices from noisy data by hard thresholding singular values. The HTSV thresholding rules adapt to the unknown rank and unknown noise level in an optimal manner and provide better results than truncated SVD (TSVD) [75]. The final result is not a fixed threshold chosen *a-priori* but a data-dependent threshold, which is preferred for ACCS.

For a nonsquare $m \times n$ matrix with an unknown noise level, the optimal threshold value $\hat{\tau}^*$ is:

$$\hat{\tau}^* = \omega(\beta) \cdot y_{med} \tag{6.7}$$

where y_{med} is the median singular value of the data matrix $\mathbf{Y}$ and the optimal hard threshold coefficient is dimension-dependent ($\beta = \frac{m}{n}$) and calculated using a numerical formula, $\omega(\beta)$. If the matrix is square, $\omega(\beta)$ is simply replaced by $\frac{4}{\sqrt{3}}$ [74].

6.6 Identifying Critical Corrective Controls

With the clustered violation groups, ACCS selects one line from each group to form a target set of overloaded lines to process. Within each violation group, ACCS examines each overloaded line's average sensitivity to all available generators. The most sensitive overloaded line is selected for inclusion in the target set. Subsequently, the critical generators that are selected for this target set will be effective in reducing the violation index for all the overloaded lines. Furthermore, the sensitivities to be processed via factorization are further reduced and computation time is lowered.

With the target set's sensitivity matrix, $\boldsymbol{\Psi_{TAR}}$, with target overloaded lines on the rows (one from each violation group) and available generators on the columns, the factorization method is applied to determine which of the generators are critical. These critical generators, defined below, are to be used with the automated RAS scheme, particularly with the continued example of generation redispatch after generator outage(s).

- *Critical generators*: for generation redispatch, the minimum set of available generators needed to effectively respond to control the target overloaded lines and reduce violations

This determination requires examining the coupling of the columns of $\boldsymbol{\Psi_{TAR}}$, or the rows of $\boldsymbol{\Psi^{T}_{TAR}}$, to identify which generators will be most effective in reducing the violation index of the overloaded lines. This analysis is motivated by observability analysis-based algorithms that sought to identify critical measurements to protect against data injection attacks [59,77]. This can be similarly applied to identify the critical generators, where controllability analysis is used to determine which of the generators are essential in controlling the overloaded target lines, reducing the violation index. Background on power system controllability is provided next, in Section 6.6.1.

6.6.1 Power System Controllability

In power systems, the controllable region is the subset of the state space on which the available controls can be used to steer the power system from one state to any other state [30]. In general, the power system dynamical equation can be written as:

$$\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}) + \sum_{i=1}^{m} \mathbf{g_i}(\mathbf{x}) u_i, \ \mathbf{x} \in \boldsymbol{\Xi} \tag{6.8}$$

where $\mathbf{x}$ is an n-vector of dynamic variables (e.g., line power flows), $\mathbf{f}(\mathbf{x})$ is a vector consisting primarily of the power flow equations, and $\sum_{i=1}^{m} \mathbf{g_i}(\mathbf{x}) u_i$ represents the effects of the controls on the system. The scalars $u_i, \ i = 1, ..., m$, are the system controls (e.g., generator real power injections) and are usually piece-wise constant in time, due to device physical characteristics. System state space, $\boldsymbol{\Xi}$, is an open subset of the n-dimensional Euclidean space. If $X(s_1, u, t) \in \boldsymbol{\Xi}$ represents the system movement with the initial state s_1, control u, and $0 \leq t \leq \infty$, the controllable region satisfies:

$$X(s_1, u, t) = s_2, \ u \in \mathbf{U} \text{ and } 0 \leq t \leq \infty \tag{6.9}$$

where every pair of states s_1 and $s_2 \in \mathbf{Z}$ satisfies (6.9). $\mathbf{Z}$ is the controllable region, a subset of $\boldsymbol{\Xi}$. Therefore, the system presented in (6.8) can be steered from a state to any other state within the controllable region. Further proofs and other references can be found in [30]. The set of controls is defined as the available generators in this work, and ACCS decomposes this set to identify the critical generators for use in online RAS.

6.6.2 Critical Generators

To identify the critical generators, ACCS processes $\boldsymbol{\Psi_{TAR}^{T}}$ using factorization techniques. The method performs a change of basis that maps available generators to equivalent controllable states. The equivalent states are the real power flows of the overloaded lines. Thus, ACCS identifies the set of available generators needed to control those equivalent overloaded line flows and most effectively reduce the violation index through generation redispatch. The generation redispatch output quantities to be assigned to these critical generators are found using the automated RAS procedure presented in Section 6.3.

Rows in $\boldsymbol{\Psi_{TAR}^{T}}$ correspond to available generators and columns correspond to the target overloaded line flows. LU factorization is applied to obtain the change of basis, decomposing the transposed sensitivity matrix to lower and upper triangular factors; [78] describes the LU factorization method. The following decomposition of $\boldsymbol{\Psi_{TAR}^{T}}$ is obtained as:

$$\boldsymbol{\Psi_{TAR}^{T}} = \mathbf{P^{-1}L_F U_F} \tag{6.10}$$

$$\mathbf{L_F} = \begin{bmatrix} \mathbf{L_b} \\ \mathbf{M} \end{bmatrix} \tag{6.11}$$

Using the Peters-Wilkinson [78] method, ACCS decomposes $\boldsymbol{\Psi_{TAR}^{T}}$ into its factors, where $\mathbf{P}$ is the permutation matrix and $\mathbf{L_F}$ and $\mathbf{U_F}$ are the lower and upper triangular factors of dimension n, respectively. $\mathbf{M}$ is a sparse, rectangular matrix with rows corresponding to the less effective available generators. The new basis has the structure:

$$\mathbf{L_{CER}} = \mathbf{L_F L_b^{-1}} = \begin{bmatrix} \mathbf{G_{CRIT}} \\ \mathbf{G_{REM}} \end{bmatrix} \tag{6.12}$$

The transformed basis, shown in (6.12), must be full rank for a controllable system and this requires the $m \times (n-1)$ matrix to have a column rank of $(n-1)$ to be a controllable n-bus system with m-measurements [77]. Since $\mathbf{L_F}$ and $\mathbf{U_F}$ will be nonsingular for a controllable system, the rank of $\boldsymbol{\Psi_{TAR}^{T}}$ can be confirmed by checking the rank of the transformed factor $\mathbf{L_{CER}}$. Also, $\mathbf{L_b}$ has full rank and with (6.12) multiplied by $\mathbf{L_b^{-1}}$ from the right, the row identities will be preserved in the transformed matrix $\mathbf{L_{CER}}$. Each row of the matrix will therefore correspond to the respective available generators [77].

Rows of $\mathbf{G_{CRIT}}$ correspond to essential corrective controls, in this case available generators, that are sufficient to assure independent controllability of the equivalent overloaded line flows. The rows of $\mathbf{G_{REM}}$ correspond to the corrective controls that can be removed from the generation redispatch procedure. Columns correspond to the equivalent overloaded line flows which can easily be mapped back to the original flows using the permutation matrix $\mathbf{P}$ obtained from the LU decomposition step. Again, these equivalent overloaded lines are composed of the target set of overloaded lines obtained from the clustered violation groups.

The resultant critical generators are the most effective minimum set responding to all the line overloads. Thus, the least number of generators can be used with the automated RAS scheme—reducing computation time significantly while effectively responding to geographically diverse line overloads.

6.7 Evaluations

The analytic corrective control selection (ACCS) method is summarized in the flowchart shown in Figure 6.2. For this chapter, the example contingency of generator outage(s) and resultant overloaded lines is used and reflected in the flowchart. Nonetheless, this ACCS algorithm is applicable to any contingency and violation; an appropriate sensitivity matrix must be calculated that reflects the available corrective controls and violated components.

As described in Section 6.2, generator outages are large disturbances that can have significant impact on the power system. Thus, this work focuses on such contingencies and the subsequent generation redispatch calculations to be computed by the presented online RAS design in conjunction with the ACCS algorithm. Real-world cases such as the large-scale cyber attack on the Ukraine power grid and the Aurora generator test exemplify the severity of the consequences that could occur as well as how generators can be prominent targets by adversaries [11,56,105]. Therefore, when generator outages occur, from either benign (accidental or malfunction) or malicious (cyber attack) sources, a quick and effective response is necessitated to maintain the system reliability via remedial actions such as generation redispatch. As discussed previously, both cyber and physical responses are required to best respond to the attack. The compromise and intrusion by adversaries must be removed using cyber defense mechanisms such as intrusion recovery systems and the physical, system-side actions are necessary to maintain grid operation and safety [23].

To protect system reliability during a cyber attack, specifically considering malicious generator outage(s), the online RAS algorithm with ACCS enables automatic and immediate response that can be recalculated as the attack trajectory changes. Thus, as compromise is being investigated by cyber-

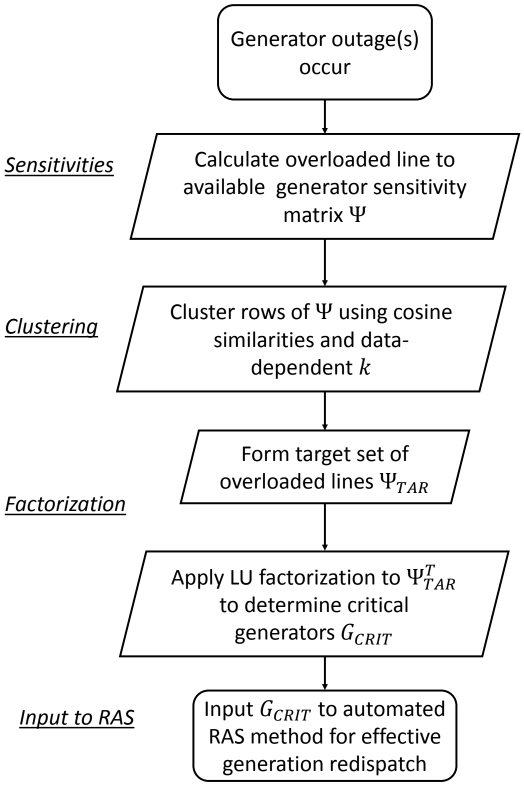

Generator outage(s) occur
Sensitivities
Calculate overloaded line to available generator sensitivity matrix Ψ
Clustering
Cluster rows of Ψ using cosine similarities and data-dependent k
Form target set of overloaded lines Ψ_{TAR}
Factorization
Apply LU factorization to Ψ_{TAR}^T to determine critical generators G_{CRIT}
Input to RAS
Input G_{CRIT} to automated RAS method for effective generation redispatch

Figure 6.2: Flowchart of proposed analytic corrective control selection (ACCS) method that uses clustering and factorization methods to obtain critical generators to input to automated RAS designs for generator outage(s) contingencies.

physical security mechanisms, the effective generation redispatch response seeks to minimize stressed conditions and prevent damage to sensitive equipment. This response is demonstrated with the IEEE 24-bus and IEEE 118-bus systems where the cyber attack scenario has the following assumptions:

- Generator outage(s) have occurred due to malicious compromise or accident/malfunction.
    - Cyber adversary may have gained access to generator controls (e.g., through SCADA distribution management system) and caused the generator to shut down, damage itself, or vary its output.
- Cyber-physical security mechanisms investigate and seek to mitigate the compromise.
- During the attack, the online RAS design with ACCS aims to maintain

Table 6.1: IEEE 24-bus Generator (Gen.) Outage Scenarios: Resultant Overloaded Lines and Violation Index (Viol.)

Outage Scenarios		
Outaged Gen.(s)	Overloaded Lines	Viol.
Gen.7	L1,L3,L12,L13	0.1421
Gen.23	L1,L3,L4,L5,L7,L8,L32	0.2183
Gen.7,13	L1,L2,L3,L5,L6,L26,L28,L33	0.6380

system reliability by formulating the most effective generation redispatch.

- As the attack trajectory changes, the enhanced RAS mechanism is able to respond accordingly with its online computation.

6.7.1 IEEE 24-Bus System

The ACCS algorithm is evaluated using an IEEE 24-bus system which has 11 generators and 38 lines, modeled in PowerWorld, a power system simulation software [108]. For this study, ACCS is used to identify the critical generators to be used in reducing/eliminating line overloads after a generator outage, from compromise or accident/malfunction, has occurred. The resultant critical generators will be input for the automated RAS procedure by Kazerooni [100] to perform generator redispatch. For this system, all sets of available generators are analyzed, excluding the slack and outaged generator(s), and three different outage scenarios are considered, as presented in Table 6.1. These generator outages were simulated in PowerWorld and the resultant overloaded lines and violation indices are listed. Additionally, "almost" overloaded lines operating at over 80% of the MVA line limits are also considered. In this manner, the generators selected as a result of ACCS secure the system and reduce stress.

The first case considers an outage of generator 7 (Gen.7) and the subsequent line flow violations in Table 6.1. The post-contingency sensitivity matrix, $\mathbf{\Psi}$, is calculated for the four overloaded lines and nine available generators. These sensitivities reflect how each overloaded line's real power flow responds to each available generator's real power changes, as discussed in Section 6.4.

Next, ACCS clusters the rows of $\mathbf{\Psi}$ to obtain the violation groups. The

Table 6.2: Singular Values y_i of $\mathbf{\Psi}$

y_1	y_2	y_3	y_4
1.7400	0.4590	0.0077	0.0180

Table 6.3: Violation Groups (V.G.) for Gen.7 Outage

V.G. 1	L1,L3,L12
V.G. 2	L13

coupling index (CI) calculation is applied to $\mathbf{\Psi}$ and the cosine similarities are subsequently clustered. To determine a data-dependent k for k-means clustering, singular value decomposition (SVD) is applied to obtain the singular values, y_i, of $\mathbf{\Psi}$. These are listed in Table 6.2. The *hard threshold singular value* (HTSV) method by Gavish and Donoho [74] is utilized to determine the most significant singular values. The algorithm, discussed in Section 6.5, outputs:

$$\hat{\tau}^* = \omega(\beta) \cdot y_{med} = 0.489 \tag{6.13}$$

which we relax slightly to include any y_i that are within 10% of the threshold. Therefore, y_1 and y_2 satisfy the hard threshold and we set $k = 2$. Next, $\mathbf{\Psi}$ is clustered using the k-means method with $k = 2$ and the cosine similarities. Two violation groups are obtained, as shown in Table 6.3.

Figure 6.3 displays the resultant silhouette values from the clustering results. The silhouette technique is used to evaluate how well each object lies within its cluster. That is, silhouettes compare how similar an object is to the other objects in its cluster when compared to the objects in other clusters. The silhouette value, sil_i for the i-th object, ranges from -1 to 1, thus the closer sil_i is to 1, the more well matched it is to its own cluster and poorly matched to neighboring clusters [76]. The silhouette values for all four of our objects, the overloaded lines, are close to 1, and therefore indicate suitable clustering.

With the violation group results, the target set of overloaded lines, $\mathbf{\Psi_{TAR}}$, is formulated. From V.G. 1, L1 is the most sensitive overloaded line and V.G. 2 has only one line, L13. Thus, $\mathbf{\Psi_{TAR}}$, is comprised of sensitivities between the target L1 and L13 and the nine available generators.

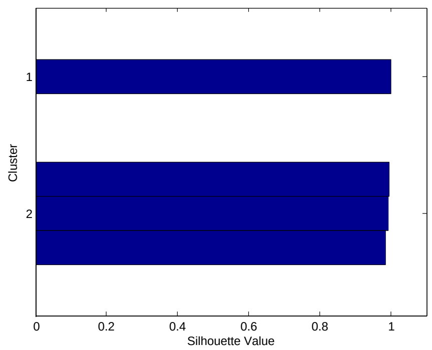


Figure 6.3: Silhouette values for overloaded lines in each violation group/cluster after Gen.7 outage.

$\boldsymbol{\Psi_{TAR}^{T}}$ is processed using LU factorization to identify the critical generators, $\mathbf{G_{CRIT}}$, the minimum set of available generators needed to effectively respond or control the overloaded lines. For the Gen.7 outage, ACCS obtains the result:

$$\mathbf{G_{CRIT}} = [\mathbf{2\ 15}] \tag{6.14}$$

Gen.2 and Gen.15 are critical and should be input into the automated RAS algorithm to determine the generation redispatch settings. Table 6.4 summarizes the results where ACCS is compared with the proximity-based critical generator (PCGI) method developed by Kazerooni where a user-defined default of five generators is always used. The ACCS results are also compared with a modified PCGI (MPCGI) method in which the default was set to the data-dependent number of critical generators found by ACCS, essentially using the same number of critical generators found by ACCS in the PCGI method. In this manner, the ACCS algorithm's ability to find the most effective generators to reduce the violation index is apparent.

The results indicate that the ACCS method was able to reduce the violation index (Viol.) most significantly (the original, post-contingency viol. is shown in Table 6.1). The PCGI method reduces the violation index acceptably as well, but has a considerably larger computation time (Comp. Time, 0.5318 s vs. 11.071 s). When the proximity-based method, MPCGI, is set to the same number of critical generators in ACCS's $\mathbf{G_{CRIT}}$, the violation index has not been reduced as effectively. The proximity-based method only considers the nearby generators and does not find the most effective generators needed to respond to the line overloads. The ACCS algorithm, on the other hand, considers the whole set of available generators to obtain the overall critical set. The computation time (Comp. Time) reflects the time for the automated RAS method to determine generation redispatch quantities. Note that ACCS, PCGI, and MPCGI calculate the critical generators in less than 1 s, and therefore add minimal computational overhead to the RAS algorithm.

Since both ACCS and MPCGI consider only two generators, the RAS computation time is similar. The PCGI with the default of five critical generators takes much longer, as the iterative generation dispatch must search for the best result between five generators. The critical generators found by each method are represented in Figure 6.4.

Table 6.4: IEEE 24-bus: Gen.7 Outage Results

	Viol.	**Comp. Time**	**$\mathbf{G_{CRIT}}$**
ACCS	0.0371	0.5318 s	[2 15]
PCGI	0.0431	11.0171 s	[2 13 14 15 23]
MPCGI	0.0819	0.5828 s	[2 13]

The Gen.23 outage scenario results are also presented in Table 6.5. It can be observed that ACCS finds a much smaller critical generator set (Gen.2 and Gen.15) while achieving a low violation index and fast computation time. PCGI achieves a similar (slightly better) reduction of the violation index, but does so with five critical generators and, thus, a much longer generation redispatch calculation. MPCGI has the fastest computation with two critical generators, as found by the ACCS method, but has the worst performance and does not reduce the violation index significantly.

Table 6.5: IEEE 24-bus: Gen.23 Outage Results

	Viol.	**Comp. Time**	**$\mathbf{G_{CRIT}}$**
ACCS	0.0562	1.0765 s	[2 15]
PCGI	0.0517	11.0692 s	[2 13 14 15 23]
MPCGI	0.1472	0.6146 s	[2 7]

The results for the double outage of Gen.7 and Gen.13 are shown in Table 6.6. Additionally, these results in comparison to the PCGI and MPCGI methods are displayed in Figure 6.5. In this case, the ACCS method has the best performance in selecting the most effective critical generators. The

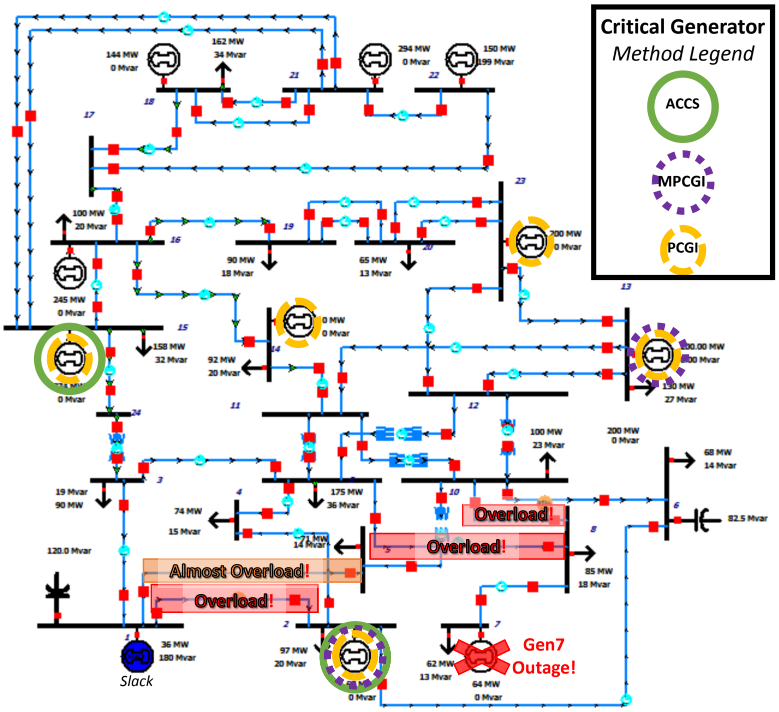


Figure 6.4: Gen.7 outage in the IEEE 24-bus system with overloaded and almost overloaded lines highlighted in red and the critical generators found by the ACCS, PCGI, and MPCGI methods labeled.

PCGI algorithm performs fairly well, but at the expense of excessive computation time. The MPCGI method does not select the most effective critical generators and therefore has the least reduction in violation index.

Table 6.6: IEEE 24-bus: Gen.7 and Gen.13 Outage Results

	Viol.	**Comp. Time**	**G_{CRIT}**
ACCS	0.0371	0.6734 s	[2 15]
PCGI	0.0489	14.3243 s	[2 14 15 16 23]
MPCGI	0.0819	0.5818 s	[2 14]

6.7.2 IEEE 118-Bus System

The IEEE 118-bus system in Figure 6.6 was also tested with the compromised generator scenario shown in Table 6.7. The system has 54 generators and 186 lines, modeled in PowerWorld [80]. Evaluations for this system consider

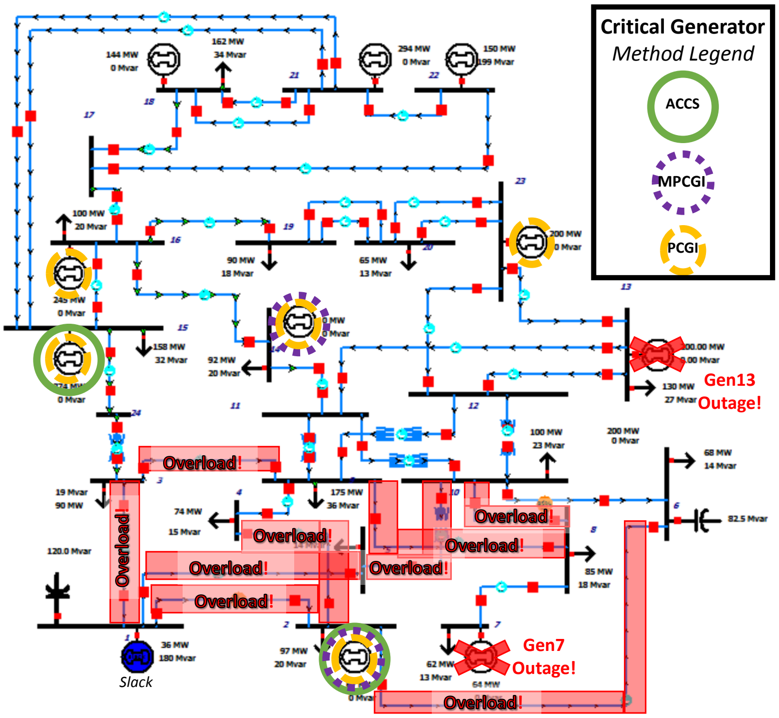


Figure 6.5: Gen.7 and Gen.13 outage in the IEEE 24-bus system with overloaded lines highlighted in red and the critical generators found by the ACCS, PCGI, and MPCGI methods labeled.

generator outage and line overloads (violating MVA limits), specifically the outage of Gen.10, which results in the largest violation index.

The results, shown in Table 6.8, indicate that the ACCS algorithm selected the most effective critical generators for reducing the violations. Using only four critical generators, the violation index was reduced from the original 1.257 to 0.0751. The default number of critical generators for large cases, such as the IEEE 118-bus, was set to eight generators in the PCGI method. The PCGI algorithm was able to achieve acceptable reduction of the violation index but with significantly larger computation time with eight generators to

Table 6.7: IEEE 118-bus Generator (Gen.) Outage Scenarios: Resultant Overloaded Lines and Violation Index (Viol.)

Outage Scenarios		
Outaged Gen.(s)	Overloaded Lines	Viol.
Gen.10	L21, L33, L37, L40, L57, L63, L66, L70, L85, L123	1.257

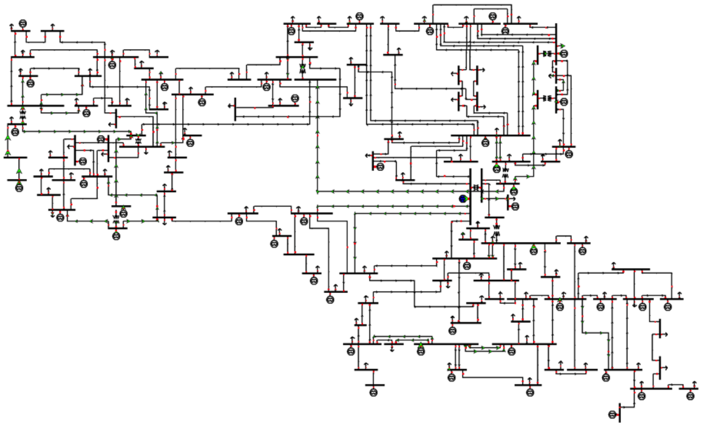


Figure 6.6: IEEE 118-bus case with 54 generators and 186 lines.

Table 6.8: IEEE 118-bus: Gen.10 Outage Results

	Viol.	**Comp. Time**	$\mathbf{G_{CRIT}}$
ACCS	0.0751	1.8110 s	[4 36 49 73]
PCGI	0.0928	5.3096 s	[8 15 18 19 24 25 32 34]
MPCGI	0.1149	1.7704 s	[8 15 18 19]

input for generation redispatch. Lastly, the MPCGI method, set to the same number as ACCS as discovered through clustering, obtains similar computation time (as expected) but suffers in performance with the least reduction in the violation index.

6.8 Conclusion

Offline RAS calculations and resultant look-up tables do not suffice for unpredictable events such as cyber attacks on the power grid. In moving forward to address this shortcoming, this chapter presents solutions to support online RAS through real-time computation of corrective controls, where the resultant controls are determined based on the current system state and designed to provide the most suitable and effective response. An algorithm is presented to select the most effective corrective controls to use with online RAS, significantly reducing computation time. The resulting online RAS could respond automatically and effectively even as the attack trajectory changes in the system.

The analytic corrective control selection (ACCS) method developed in this work derives a controllability analysis-based formulation that leverages sensitivities and applies clustering and factorization techniques. It demonstrates the utility and versatility of the distributed controller role and interaction discovery algorithm presented in Chapter 4 and aids the focus of this dissertation of fast and effective response to distributed controller compromise. In this manner, the critical corrective controls identified are the most effective in reducing violations in various, stressed areas of the system and are the minimum set. For generation redispatch examples, demonstrated with compromised generator outage(s) in the IEEE 24-bus and IEEE 118-bus systems, the critical generators selected by ACCS provide significant reduction in the violation index. Furthermore, only a fraction of the set of available generators are needed. The computation of RAS for generation redispatch was much faster, as a small set of generators could be used. These results indicate that ACCS finds the most comprehensive and effective minimal set of critical generators or corrective controls to utilize with RAS and plays an important role in successfully restoring the system to a normative state while undergoing a cyber attack. The negligible computation overhead by ACCS and subsequent speedy RAS calculations, with the minimum set, is promising for use in online RAS designs.

This work can be extended to utilize DCOPF or ACOPF given improvements to their formulations to reduce computation time, as maximizing reliability slows down the implementation [109]. This further work could contribute both to improving the violation index calculation to appropriately reflect all constraints for different contingencies beyond generator outage and to developing a systematic approach to selecting weights. Furthermore, when considering multiple types of violations (e.g., line flow limits *and* voltage limits), violation groups derived from clustering the sensitivity matrix must reflect all limits. An interesting future direction would be to study how appropriate sensitivity matrices could be derived reflecting multiple violation types or if the overlap of violation groups (calculated separately for each violation type) provides minimal computational overhead.

CHAPTER 7

POWER FLOW ANALYSIS FOR CONTROL INPUT VERIFICATION

7.1 Problem Statement

In the study of power systems, power flow analysis has been both a fundamental and critical tool. It has traditionally been applied to estimate power flows, real and reactive, on all lines of a given system and determine the bus voltage and phase angle values in steady-state operation. Both AC and DC methods have been developed, but one of the most notable algorithms is the Newton-Raphson power flow (NR-PF) [110]. The root-solving technique is a nonlinear AC method and is utilized to obtain power flow results with quadratic convergence.

However, for many applications besides planning, adequate speed is not achieved with NR-PF. For example, congestion-constrained market applications and contingency analysis both need fast power flow results [111, 112]. Speed is especially important for online protection schemes; the verification of input control logic programs *before* execution requires very fast and accurate power flow results. Programmable logic controllers (PLCs) are prominently utilized distributed controllers in the power system, used for executing a variety of system controls. The verification tool developed for the overall project uses symbolic execution to explore the future state space to determine if the execution of the control input will lead to a safe or unsafe state. The decision of safety is determined using power flow results and system constraints. This tool is described further in [23, 28], as well as in Section 2.3.2, and the case study later in this chapter; it is the motivation for this work. Nonetheless, such safety-dependent analysis requires highly accurate results as achieved with NR-PF but at a higher speed.

The NR-PF requires calculations of both partial derivatives and Jacobian matrices, slowing down the method. The non-linearity causes the solution of very large AC power flow models to be excessively slow, and thus infeasible; the computational burden and number of iterations increase with the size of the system. To combat this, alternate methods such as DC power flow (DC-PF), fast decoupled power flow (FD-PF), and dishonest Newton-Raphson power flow (DNR-PF) can be used to expedite the process [112–114]. These algorithms make simplifying assumptions and, as a result, have lower accuracy than the NR-PF result. DC-PF exhibits the least burden but also implements the most severe approximations. The speed, nevertheless, remains an attractive feature.

Applications such as fault analysis or the control input verification require fast, reliable calculations for power flow. Speed is of utmost importance but the trade-off with accuracy in the previously mentioned algorithms is a significant drawback. A power flow method that preserves the accuracy of the traditional NR-PF, or comes close, with the speed of the alternative methods is necessitated. Lu et al. [115] developed a method, improved DC power flow (impDC-PF), that applies correction terms derived from the NR-PF formulation and calculates them using historical data. These correction terms are applied to the DC-PF method, maintaining the linear formulation, and they improve the accuracy significantly while maintaining the speed.

Yet, there exist some negatives that the proposed algorithm, augmented DC power flow (augDC-PF), intends to mitigate and improve. The fact that the correction terms are calculated with historical terms requires this data to be processed and adapted to the current operation point (hours, days, seasons). There is some overhead in calculating the correction terms to correctly reflect the current situation, even if it is only a prior calculation. Calculation based on historical data also draws attention to the case when the system topology changes. In this case, the historical data is not accurate and perhaps not even applicable depending on the extent of the topology changes.

For both speed and accuracy requirements, the improved DC power flow method is not the best and viable option. Therefore, this chapter proposes an augmented DC power flow method that fixes the problems listed above and offers further improvements. This augmented method uses the addition of real-time measurements to mitigate the historical data drawbacks and also achieve greater accuracy. The method's performance when topology changes and when full system observability is not achieved is presented. The case study involving control input verification is also presented to showcase the method's versatility and motivation. In particular, the ability to use the symbolic power flow results to backsolve for control input safety ranges is presented. This is demonstrated within the full context of the verification tool in [28].

7.2 Background

The traditional power flow analysis methods NR-PF, FD-PF, DC-PF, and DNR-PF are summarized in this section. Background on the impDC-PF algorithm and the use of real-time measurements is presented as well.

7.2.1 Newton-Raphson Power Flow

The Newton-Raphson method solves a nonlinear equation in the form of $y = f(x)$, defined in the power flow problem as:

$$x = \begin{bmatrix} \delta \\ V \end{bmatrix} = \begin{bmatrix} \delta_2 \\ \vdots \\ \delta_N \\ V_2 \\ \vdots \\ V_N \end{bmatrix} \quad y = \begin{bmatrix} P \\ Q \end{bmatrix} = \begin{bmatrix} P_2 \\ \vdots \\ P_N \\ Q_2 \\ \vdots \\ Q_N \end{bmatrix} \tag{7.1}$$

$$f(x) = \begin{bmatrix} P(x) \\ Q(x) \end{bmatrix} = \begin{bmatrix} P_2(x) \\ \vdots \\ P_N(x) \\ Q_2(x) \\ \vdots \\ Q_N(x) \end{bmatrix} \tag{7.2}$$

The x vector includes the voltage magnitude, V, and voltage phase angle, δ, quantities that are to be solved for. The y vector is composed of the real and reactive power flow equations shown below:

$$y_k = P_k = P_k(x) \tag{7.3}$$

$$= V_k \sum_{n=1}^{N} Y_{kn} V_n cos(\delta_k - \delta_n - \theta_{kn}) \tag{7.4}$$

$$y_{k+N} = Q_k = Q_k(x) \tag{7.5}$$

$$= V_k \sum_{n=1}^{N} Y_{kn} V_n sin(\delta_k - \delta_n - \theta_{kn}) \tag{7.6}$$

$$k = 2, 3, ..., N \tag{7.7}$$

The slack bus is assumed to be bus 1, when $k = 1$, and the δ_1 and V_1 quantities are known to be 0 and 1 $p.u.$, respectively. The power flow equations are not written for the slack bus. With this model, the Newton-Raphson root solving technique is applied: the Jacobian matrix is calculated and iterative Gauss elimination is used to iteratively solve the system, provided an initial guess. Convergence criteria are based on the power mismatch and boast quadratic convergence due to the use of Newton-Raphson. Further details about the treatment of different kinds of buses as well as the procedure can be found in [116].

7.2.2 Approximate Power Flow Algorithms

As mentioned previously, many applications that involve large systems and/or need speed require the use of alternative power flow methods such as the DC-PF and DNR-PF algorithms. Although they are much faster than the traditional NR-PF solution, there still exists a trade-off with accuracy. These techniques are detailed in the following sections.

Dishonest Newton-Raphson Power Flow

The DNR-PF is a variation of the NR-PF algorithm in which the Jacobian matrix is not calculated at every iteration but is kept constant after being computed with the initial guess input. This reduces the computational burden as most of the time in the NR-PF iteration is spent dealing with the Jacobian matrix, both for calculation and factorization [117]. The extreme case is when it is only calculated once with the initial guess, but typically it is occasionally recomputed and refactorized. Nonetheless, significant time savings occur with skipping the Jacobian computations in every iteration. The solution is subsequently computed in the same procedure as the traditional NR-PF. This simplification, however, is severe and results in an increased number of iterations to reach convergence as well as less accuracy. Thus, this method is not usually used for power flow analysis in practice as it does not yield substantially beneficial results.

Fast Decoupled Power Flow

In decoupled power flow, the relationships between the state variables and power injections are leveraged. The changes in voltage magnitude V affect imaginary power Q more significantly than real power P, and changes in voltage phase angle δ affect P more significantly than Q. Using this knowledge, a decoupling approximation can be made in which the partial derivatives in the Jacobian matrix, $\frac{\partial P}{\partial V}$ and $\frac{\partial Q}{\partial \delta}$, are assumed to be zero since they are already small. In each iteration, the solution guess for δ and V can be computed separately and, therefore, are decoupled. Two justifications for these Jacobian approximations are:

1. Usually $r << x$, and thus, $|G_{ij}| << |B_{ij}|$, where the impedance is $r + jx$; $|G_{ij}| \approx 0$.
2. Typically δ_{ij} is small, so $sin(\delta_{ij}) \approx 0$, $cos(\delta_{ij}) \approx 1$.

For fast decoupled power flow, further simplification is made by building and factorizing the Jacobian once, as with the DNR-PF method. Voltage magnitudes can also be assumed to be 1 $p.u.$ to reduce the burden even more. This increases the speed of computation (especially when only an approximate solution is required and the number of iterations can be fixed), but again, only an approximate solution results. Specifics about the method can be found in [113, 116, 117].

DC Power Flow

The DC-PF involves severe approximations in which reactive power is ignored, voltages are assumed to be 1 $p.u.$, and conductances (G) are ignored where $Y = G + jB$ [112]. This renders the power flow equations as a linear set of equations, as follows:

$$\delta = -B^{-1}P \tag{7.8}$$

where δ is the voltage phase angle vector, B is the vector of susceptances (the imaginary portion of the admittance), and P is the real power injection vector. Thus, an approximate solution for the power flow is obtained for the phase angles while the voltage magnitudes are assumed to be 1 $p.u.$ Yet this speedy algorithm yields an inexact solution, which is not suitable in all applications as examined next.

7.2.3 Improved DC Power Flow

The DC-PF is widely used when computational speed is prioritized and approximate results are suitable to use. In one case study [118], it was found that the DC power flow was about 60 times faster than AC methods. However, typical error for DC power flow solutions is about 4.6%, due to the severe approximations made. Therefore, there are accuracy and speed trade-offs when dealing with AC and DC power flow methods. Lu et al. [115] developed an improved DC power flow method using empirical knowledge of the system from historical data. They found an 80% reduction in error with their method while maintaining the linear formulation and computational speed. By deriving correction terms from the AC formulation of power flow equations, correction terms were created to add to the DC formulation and still maintain the linear formulation.

The correction terms include bus voltages and phase angles and are based on the historical data. Historical data is studied to identify patterns and determine distributions as a function of hours, days, seasons, etc. Essentially, the historical data must be processed to obtain reasonable estimation of the current operating point of the system. However, this use of historical data is not always suitable as the estimate may not be close enough to the current operating point or satisfactorily adapted to it. The authors state that the calculation of the correction terms can be done offline or as a pre-processing step. This derivation and the details of the impDC-PF algorithm are further discussed in the development of the augDC-PF method.

7.2.4 Augmented DC Power Flow with Real-Time Measurements

Phasor measurement units (PMUs) have been broadly deployed in recent decades for synchronized real-time measurements of power system quantities such as voltage, current, and frequency [119]. Thus, with PMUs or similar distributed measurement devices, access to expansive, fast-sampled power system data can be obtained. These real-time measurements are used in the formulation of the augDC-PF method and allow for more flexibility and accuracy in the algorithm, as discussed in the following section.

7.3 Proposed Augmented DC Power Flow Method

The proposed augDC-PF method seeks to achieve both accuracy and speed. Discussed in the background section, most of the speed-focused power flow algorithms incur a trade-off with accuracy. The impDC-PF is a first step towards this goal, but augDC-PF remedies its existing issues and seeks to improve on it. This section details the augDC-PF method.

7.3.1 Augmented DC Power Flow Method

As discussed previously, impDC-PF requires pre-processing of historical data to adapt to the current operating point and does not reflect topology changes. These issues must be addressed for applications in which both speed and accuracy are vital. Therefore, the proposed algorithm incorporates an augmented DC power flow (augDC-PF) method that solves the problems listed above and also offers further improvements. The augDC-PF uses the addition of real-time measurements to mitigate the historical data drawbacks and achieve greater accuracy. The linear formulation of the DC-PF is key to preserving this speed.

In this work, we propose an augmented DC power flow method (augDC-PF) in which the correction terms are derived in the same manner as Lu et al. [115], but instead of using historical data, we utilize online, real-time data obtained from distributed monitoring devices such as PMUs. This eliminates processing steps in estimating current operating points based on the historical data and adapting it to the season, day, and hour. The PMU data will already reflect the present operating points as well as topology changes (the historical data would not be applicable, in this case). Thus, the correction terms are more accurately calculated and better results can be obtained. The augDC-PF algorithm is formulated as follows:

The power flow equation for real power flow (between buses k and m, for n total buses) is:

$$P_k = \sum_{m=1}^{n} V_k V_m (G_{km} cos\theta_{km} + B_{km} sin\theta_{km}) \tag{7.9}$$

The DC-PF equation is:

$$P_k = \sum_{m=1}^{n} B_{km}\theta_{km} \tag{7.10}$$

If we rearrange (7.9) to the same form as (7.10), we obtain:

$$P_k - \sum_{m=1}^{n} V_k V_m G_{km} cos\theta_{km} = \sum_{m=1}^{n} V_k V_m B_{km} sin\theta_{km} \tag{7.11}$$

By studying (7.11), correction terms are derived:

$$P_{k_{corr}} = -\sum_{m=1}^{n} V_k V_m G_{km} cos\theta_{km} \tag{7.12}$$

$$B_{km_{corr}} = \frac{V_k V_m sin\theta_{km}}{\theta_{km}} \tag{7.13}$$

Then we have:

$$P_k^* = P_k + P_{k_{corr}} \tag{7.14}$$

$$B_{km}^* = B_{km} \cdot B_{km_{corr}} \tag{7.15}$$

Substituting these values, we obtain the original DC-PF linear formulation:

$$P_k^* = \sum_{m=1}^{n} B_{km}^*\theta_{km} \tag{7.16}$$

The terms are now more accurately calculated; the correction terms include

V_k, V_m, and phase angles θ_{km} and are based on the real-time PMU data, as exemplified in the next section.

7.4 Evaluation Results

The augDC-PF method improves the impDC-PF method with the inclusion of real-time measurements, leading to online calculation of the correction terms based on the current operating point. Thus, it maintains both speed and accuracy, which is explored in this section. The effect of reducing the set of PMU measurements is also investigated. The proposed method has extended capabilities of dealing with topology changes, which are illustrated with a small example. Lastly, a control input verification case study is presented to emphasize the need and usefulness of augDC-PF.

7.4.1 Speed and Accuracy of Method

The augDC-PF method was tested with PowerWorld 37-bus and 5-bus system cases [84] and studied in terms of speed and accuracy. The algorithm was implemented in Matlab and compared against traditional methods such as NR-PF and DC-PF. To emulate the real-time (e.g. PMU) measurements, PowerWorld Simulator was utilized. The system is shown in Figure 7.1, with bus 1 as the slack bus.

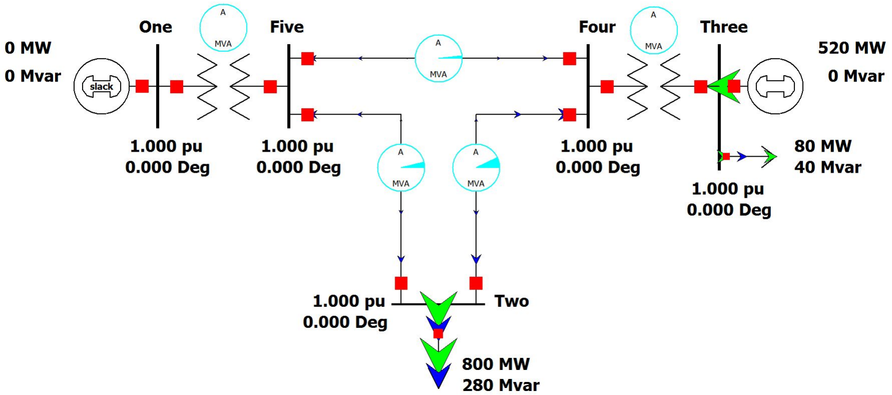


Figure 7.1: PowerWorld 5-bus system.

By using the real-time measurements and correction terms, the augDC-PF method improved accuracy and preserved speed. The augDC-PF achieves greater accuracy than DC-PF (as well as impDC-PF, which is based on historical data) while maintaining the linear formulation. An example of this improvement is shown in Figure 7.2 where the NR-PF results are compared with both the DC-PF and augDC-PF methods for the IEEE 37-bus case system. It was found that the performance of the augDC-PF method was superior. The average error for augDC-PF is significantly lower than that of DC-PF, as illustrated in the error plot.

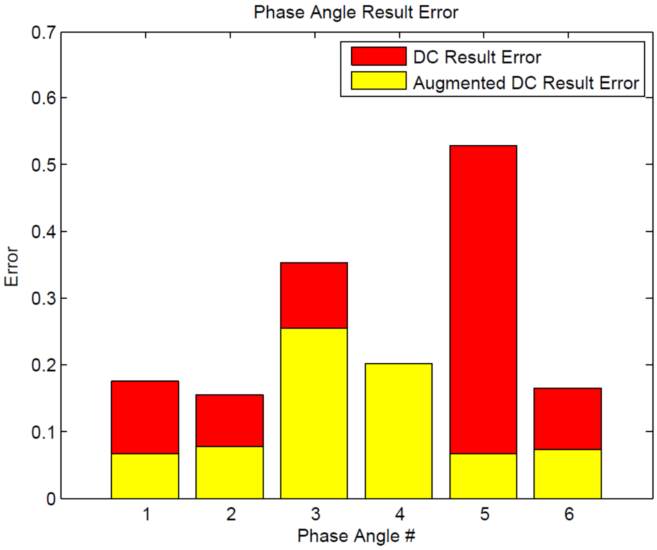


Figure 7.2: The differences between the benchmark NR-PF results (for phase angles) and both DC-PF and augDC-PF algorithms are compared for an IEEE 37-bus system; the augDC-PF method exhibits less error, thus superior performance.

Compared with the NR-PF computation time, the augDC-PF algorithm is much faster and requires only one iteration. This is shown in Figure 7.3 where the computation time for the NR-PF method, cumulative as the iterations increase, is compared with the computation time of the single iteration augDC-PF method.

These results indicate that the augDC-PF method is a promising solution for applications where both accuracy and speed are necessary. The impDC-PF method and augDC-PF method are directly compared when considering topology changes, again demonstrating the benefits of augDC-PF.

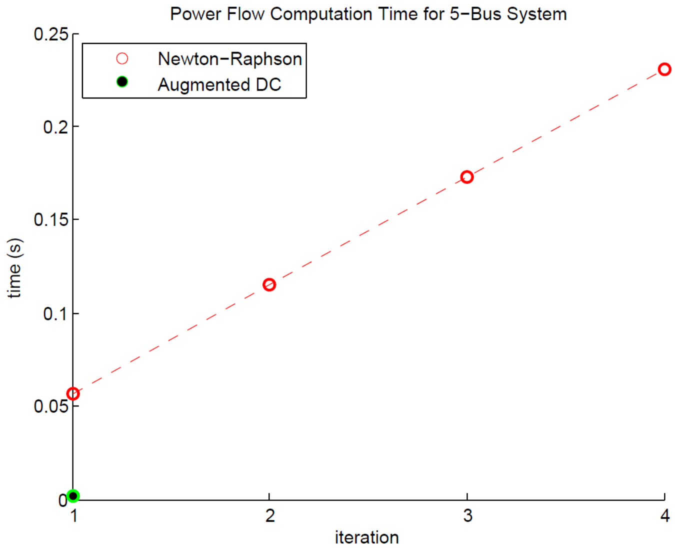


Figure 7.3: For the PowerWorld 5-bus system, the computation time for the NR-PF method involves several iterations, increasing the total time, whereas the augDC-PF algorithm requires only one iteration.

7.4.2 Addressing Dynamic Changes in Topology

One of the main drawbacks of the impDC-PF algorithm is the inability to reflect topology changes when calculating correction terms from historical data. This can be remedied with the use of PMU measurements in the correction term calculation, as in augDC-PF. In this case, the PMU data reflects the current operating point automatically, incorporating any changes in the system. These changes include anything from weather to topology changes (e.g., line(s) being opened or closed). The impDC-PF method has to adapt historical data in the pre-processing step to best match the current operating point (not including topology changes), resulting in varying overhead in computation.

An example topology change is the line between bus 4 and bus 5 being opened in the 5-bus system presented in Figure 7.1. For the impDC-PF method, the historical data used to calculate the correction terms is still based on the original topology of the system (with the line between bus 4 and bus 5 closed). The subsequent results are less accurate than the results from augDC-PF where the topology change has been taken into account. This is exemplified in Table 7.1. Using the NR-PF results as the benchmark, the error is computed for the impDC-PF and augDC-PF methods with the

Table 7.1: Comparison of Results with Topology Change; Error Calculated Using NR-PF Results as Benchmark

	NR-PF	impDC-PF	augDC-PF
θ_2	-0.3428	-0.4850	-0.2516
θ_3	0.2382	0.0938	0.2489
θ_4	0.1991	0.0529	0.2155
θ_5	-0.0817	-0.1139	-0.0705
$error_{NR}$	**0**	**0.2520**	**0.0940**

Euclidean error norm. The augDC-PF method performs much better than the impDC-PF method with an error of 0.0940 vs. 0.2520. This is due to the inclusion of the current operating point PMU measurements that reflect the topology changes in the augDC-PF formulation. Therefore, the historical data drawbacks present in impDC-PF are remedied within augDC-PF and better performance is achieved.

7.4.3 Reduced Set of PMU Measurements

In the preliminary results presented, it was assumed that PMU measurements from every bus are available, resulting in very accurate correction terms. However, this is not a realistic assumption as it is not usually available at every bus in a system. There is ongoing research with the optimal placement of PMUs to ensure full system observability, in which case augDC-PF would perform as before. Xu and Abur [120] presented a numerical method that uses integer programming to determine optimal PMU placement considering mixed and conventional measurement sets whose objective is to minimize cost while maintaining system observability.

When this strategy is implemented with the 5-bus system in Figure 7.1 with a simple cost set (assuming the same, average price for every PMU device and installation), it is found that PMUs at bus 4 and 5 ensure system observability and incur the least cost. Full system observability is achieved because given a PMU at a bus, the bus voltage phasor and all current phasors along lines connected to that bus will also be available. This also implies that this bus voltage, along with all adjacent bus voltages, will also be available (solvable). Therefore, quantities reflecting the current operating point of the system are available/solvable, allowing for the accurate calculation of the correction terms and very similar results to before, when assuming PMUs at each bus. Complete details on the optimal PMU placement strategy are explained in [120].

However, if full system observability is not achieved and such optimal PMU placement is not employed, augDC-PF's correction term computation is not as accurate. Note that we assume no measurement is corrupted (accidentally or maliciously) [120]. Yet sample results, shown in Table 7.2, indicate that the results do not vary too drastically.

Table 7.2: Effect of Reducing PMU Measurement Locations on Results, Compared with the NR-PF Results as the Benchmark

	NR-PF	augDC-PF	augDC-PF	augDC-PF
PMUs at	-	*all buses*	*bus 2, 5*	*bus 3*
θ_2	-0.3263	0.3500	-0.2567	-0.3536
θ_3	0.0091	-0.0030	0.3872	0.1152
θ_4	-0.0349	-0.04881	0.2602	-0.0455
θ_5	-0.0720	-0.0805	-0.01290	-0.0812
$error_{NR}$	**0**	**0.0294**	**0.4495**	**0.1104**

As presented in Table 7.2, augDC-PF has the best performance when full system observability is achieved. In this case, there are PMUs available at each bus but the same results would be obtainable if optimal PMU placement was conducted (full system observability obtained). Then, the available PMU measurements would ensure all other bus quantities (e.g., voltages) are solvable.

Nonetheless, when full system observability is not acquired, as in the case when there are PMUs only at bus 2 and 3 or just at bus 3, the method suffers. As expected, the error of the result, expressed as its difference from that of the benchmark NR-PF results, increases. This is due to the fact that the correction terms are based on these measurements, and with reduced observability, many quantities are no longer available. The error when there is a PMU only at bus 3 is somewhat reasonable, indicating that there may be certain situations in which the method performs adequately. This will be investigated further in future work.

7.4.4 Case Study: Control Input Verification

For various power system applications, such as real-time control, both speed and accuracy of the power flow algorithm are needed—rough approximations do not suffice. This is especially the case with the aforementioned control input verification tool for power systems. In this case, control logic programs upload to programmable logic controllers (PLCs) by the engineering work stations. These programs are verified by exploring all feasible execution paths stemming from them [29]. The states encountered by the paths are deemed safe or unsafe using power system analyses (such as NR-PF); e.g., constraints such as voltage or line flow limits must be satisfied. Thus, if a control input drives the system to an unsafe state (e.g., violates constraints), as gleaned from the power flow results, that control input is flagged as "bad" and not executed.

Symbolic executions of these analyses are utilized to explore all possible control logic execution paths. The symbolic execution uses symbols as control inputs and contains logical path conditions, such as satisfying the power system constraints. All feasible paths are explored using special solvers [121]. Ultimately, using the symbolic power flow results for a symbolic control input, a "safe" range for the control input can be derived by backsolving using system constraints. This aspect of the control verification tool will be studied in this case study regarding how augDC-PF handles symbolic variables quickly and renders accurate results when backsolving for concrete "safe" values. Crucial aspects of this tool are speed (the commands must be verified before execution) and accuracy (safety is dependent on it). Details on symbolic execution and the verification tool are presented in [29].

The inclusion of symbolic variables significantly impacts traditional methods such as NR-PF. Both partial derivatives and the Jacobian matrix must be computed with the symbolic variables, slowing the algorithm significantly as each iteration's parametric result becomes increasingly complex. When testing the small 5-bus system in Figure 7.1, without symbolic execution, each iteration takes only a few milliseconds. However, with symbolic real power injection, solving the NR-PF is intractable and is excessively slow even for two or three iterations. The scalability of the symbolic NR-PF is shown for a 2-bus system and the 5-bus system in Figure 7.4 and Figure 7.5. Therefore, alternate methods must be considered, such as augDC-PF.

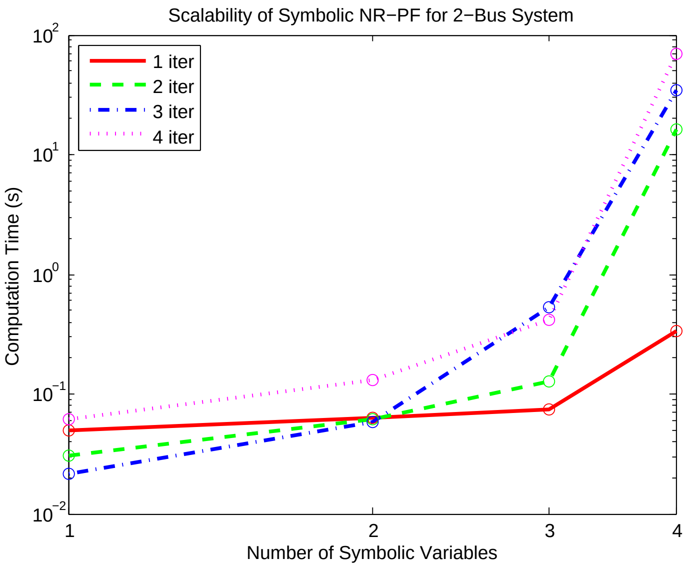


Figure 7.4: As the number of iterations and the number of symbolic variables increase, the computation time steeply increases for the 2-bus power system after the inclusion of 3 symbolic variables.

Next, the augDC-PF method was implemented with the inclusion of a symbolic control input, in this case a real power injection. If the symbolic control input is b, we can backtrack from the power flow solution and the safety and reliability constraints and try to find the range of b that satisfies constraints and is "safe" (for power system operation). Voltage angle constraints are derived from FERC standards [122], and for the 5-bus system in Figure 7.1 the angle constraints are:

$$|\theta_1(b) - \theta_5(b)| < 90^\circ \tag{7.17}$$

$$|\theta_5(b) - \theta_2(b)| < 90^\circ \tag{7.18}$$

$$|\theta_4(b) - \theta_2(b)| < 90^\circ \tag{7.19}$$

$$|\theta_4(b) - \theta_3(b)| < 90^\circ \tag{7.20}$$

The phase angle results from the augDC-PF method are used to compute the angle difference constraints and the safe range of the symbolic control input, b. Each phase angle result is in terms of b. Subsequently, the intersection of the resulting inequality constraints is used as the final angle constraint which satisfies all angle difference requirements, as shown below (ang as shorthand

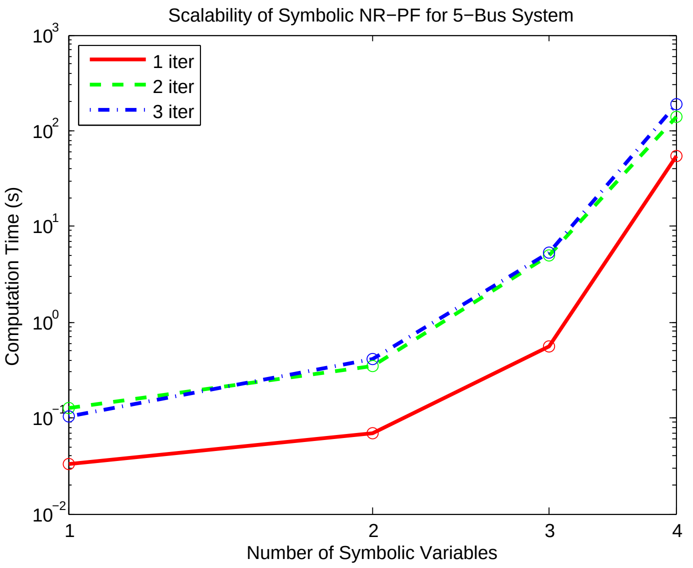


Figure 7.5: Similar to the behavior of the 2-bus system, the computation time increases as the number of iterations and symbolic variables increases with relatively longer computation time requirements.

for angle):

$$b_{min_{ang}} < b < b_{max_{ang}} \tag{7.21}$$

With this final angle constraint, the range can be narrowed to satisfy other, more critical constraints. Since the voltage angle constraints are not easily violated, a large safe range of control input b results. Therefore, further constraints, more critical to safe system operation, are applied using this narrowed range.

A more commonly applied constraint is that of the line flows in the system. By enforcing the MVA ratings of each line in the system, the range of safe control input is further reduced. Applying line flow constraints, according to each line's MVA rating alongside the angle constraints, results in a much narrower safe control input range. With S_{km} representing the line flow between bus k and bus m, line flow constraints for the 5-bus system are:

$$|S_{15}(b)| < 6\ p.u. \tag{7.22}$$

$$|S_{54}(b)| < 12\ p.u. \tag{7.23}$$

$$|S_{43}(b)| < 10\ p.u. \tag{7.24}$$

$$|S_{52}(b)| < 12\ p.u. \tag{7.25}$$

$$|S_{42}(b)| < 12\ p.u. \tag{7.26}$$

By again deriving the intersection of these constraints and combining with the final angle constraint in (7.21), we achieve the following safe range for the control input (lf stands for line flow):

$$b_{min_{ang,lf}} < b < b_{max_{ang,lf}} \tag{7.27}$$

In this case, this new range for the acceptable per-unit real power injection satisfies both the line flow and angle constraints for continued, secure system operation. Figure 7.6 exemplifies the concrete case in which both constraints are applied, resulting in a safe range for b between 4.529 and 14.029 $p.u.$, as shown by the shaded region. The accuracy of the phase angle, θ, is compared against the benchmark NR-PF result ($b = 0$) for varying values of b, the control input for real power injection. Figure 7.7 illustrates further the accuracy of the augDC-PF method in comparison with the benchmark NR-PF results ($b = 0$) for varying b values. It can be noted that each phase angle is impacted differently with the changing control input values; the θ_3 error significantly increases as b is varied whereas θ_2 error remains relatively low. Therefore, the augDC-PF method effectively allows for the analysis of symbolic control inputs with the application of constraints, as derived from the system. Voltage limits can also be implemented, resulting in an overall constraint for the control input that satisfies all the safety requirements in the given system. In this manner, the verification process can proceed to the next step with the resultant safe control input range. Further details of the full verification tool are provided in Section 2.3.2 and in [23, 28, 123].

The use of augDC-PF in this case study was necessary, as both accuracy and speed were required. Traditional, high-accuracy methods such as NR-PF were too slow and could not handle the inclusion of symbolic variables. Yet high-speed methods such as DC-PF or DNR-PF lacked the accuracy needed to achieve results the control input verification required for thorough safety analysis. Thus, the augDC-PF method satisfies both needs and performs efficiently. This application is one of many that could benefit from augDC-PF; its increased accuracy but maintained speed makes it more valuable than the existing speed-focused algorithms.

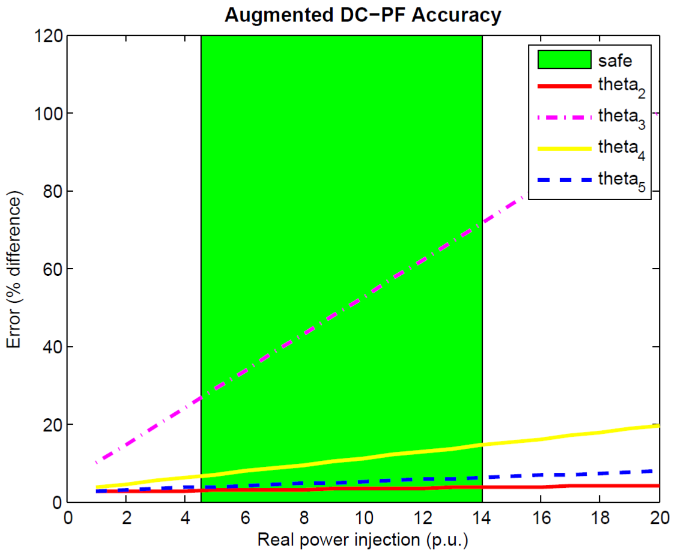


Figure 7.6: The difference between the benchmark NR-PF result ($b = 0$) for each phase angle, θ, and augDC-PF results for varying values of b. The shaded green region represents the safe range for b with both line flow and angle constraints applied.

7.5 Conclusions

By using real-time measurements to derive correction terms and deal with topology changes, the augDC-PF method is a versatile, fast, and accurate power flow method. The drawbacks in using historical data, in impDC-PF, such as inability to deal with topology changes and computation overhead in adapting the data to the current operating point, are remedied in the proposed method. Greater accuracy is achieved since the correction terms can be calculated online, using the real-time measurements. Its linear formulation maintains the speed coveted in DC-PF. Reduced PMU measurement locations can also be handled, with or without full system observability.

The augDC-PF method is flexible and will be useful in a variety of applications, as exemplified by the control input verification case study. It maintained both high accuracy and speed, as needed to determine if a control logic program would lead to a “safe” or “unsafe” state. In this manner, violation of safety constraints is determined in a timely manner, to best execute the Just-Ahead-of-Time verification described in Section 2.3.2. Nonetheless, the augDC-PF algorithm is broadly useful to many applications and helps reduce the speed and accuracy trade-off in traditionally speed-focused power

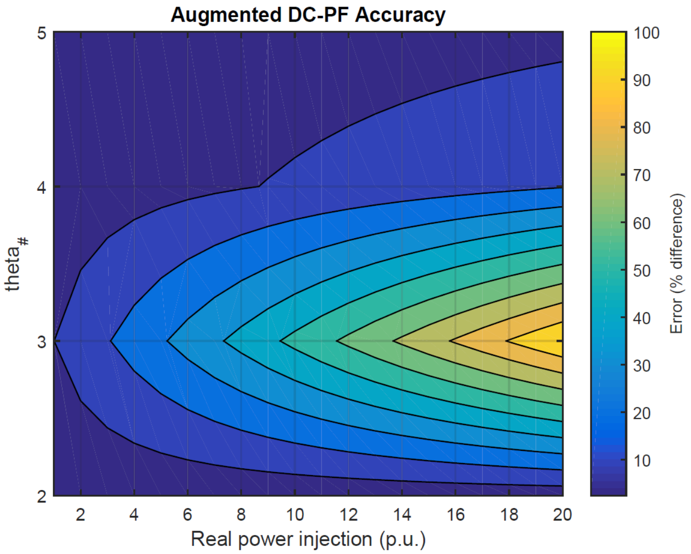


Figure 7.7: Contour plot of error for each phase angle with varying b values; the color bar represents the level of error.

flow methods.

CHAPTER 8

GENERATOR CONTROL ACTION CLASSIFICATION BASED ON LOCALIZED VOLTAGE MEASUREMENTS

8.1 Problem Statement

Distributed controls play an integral role in the power system, as this work has exemplified in the previous chapters. Their functions range from roles in power flow control, such as the D-FACTS devices, to protective relays to automatic generator control actions (e.g., automatic voltage regulators (AVRs)). When these control actions occur, they impact the power system quantities of the local area in a predictable manner. For example, when the governor setpoint of a generator is changed via a control action, the system voltage data exhibits discernible effects, dependent on the type of control action and location. These effects are most significant in the local area of the generator at which the control action was enacted.

Leveraging this insight into the power system's behavior, especially its impact on the voltage profiles, we can enhance classification algorithms. We can focus only on the localized measurements, reducing the training data sets—instead of using widespread data from the entire system, as most data mining algorithms do. Thus, we can improve the usability of data mining algorithms in power systems, as we can enhance the methods with domain-specific knowledge to achieve faster and more accurate results.

For this particular problem, the question is: Can we just use a few data sets (e.g., from generator buses) to classify the generator control actions? In this manner, we develop a generator control action classification algorithm that uses a reduced, insightful set of data. In this manner, detection of malicious, or at least abnormal, control actions can be aided. Any set of voltage data that cannot be classified as a control action at a certain generator (or as the normative state with no control actions occurring) is flagged as abnormal and the operator can be notified.

This method aids the efforts of the cyber-physical verification (CPV) project discussed in Section 2.3.2. It acts as a secondary check that the verified control commands that are enacted impact the system as expected, as gleaned from the successful identification of the generator control actions from the resultant change in the system voltage data. Yet, if abnormal system behavior is observed (the classification fails), the event is flagged and the cyber-physical response (CPR) system can be called, also presented in Section 2.3.2.

8.1.1 Data Mining in Power Systems

Increasing use of distributed monitoring devices, smart meters and appliances, and other measurement sources has defined an essential and significant role of data analytics in the realm of power systems. Access to these measurements can be very useful in power systems and improve decision making, situational awareness, and speed of response; this data has large volume, high velocity (fast-paced processing and analysis), and is of increasing variety [124].

Specifically, the study of voltage disturbances has become a principle research topic with the influx of fast-sampled, wide-area voltage data from the distributed monitoring devices. Voltage disturbances are common occurrences in power systems and can be caused by various faults or control actions. In power systems research, work has been done in identifying the events that cause voltage dips or swells using signal processing and statistical methods [125].

Recently, data mining techniques have been applied to power systems, usually on a larger, macro-scale using whole system data [126]. Such data include measurements from transmission buses, substations, or other major components in the network. The increase of near real-time voltage measurements from multiple locations all across the power grid has rendered such voltage analyses as "big data" problems. To process these large volumes of data, methods such as neural networks, support vector machines, clustering, etc., are being applied and integrated into studies [127]. Therefore, data mining techniques have become integral in power system analyses, especially in the area of voltage disturbances.

However, although this big data analysis is useful and enables powerful insight, further studies on small-scale systems need to be conducted. By focusing on single components such as generators in the power grid, we can provide concrete and detailed insights into individual operators to better understand situational awareness. Furthermore, we would like to leverage our knowledge of power system behavior, based on its dynamics and topology. With this insight, we know which parts of the system are most impacted by different events. Therefore, the training data set can be reduced to include only the single components or areas that will be impacted by the actions we seek to classify, enabling faster and more accurate response to unexpected events in the power system.

This low-level data is also more difficult to mimic than broad system behavior data, helping prevent, or more quickly detect, malicious activity. Those disturbances not classified can be flagged as outliers or abnormal behaviors to be investigated for malicious activities or equipment failures. The deployment of distributed voltage monitoring devices allows access to localized voltage measurements. We can obtain localized data around a single component, such as a generator, and perform small scale analysis.

An application for such small-scale analysis is classifying control actions of generators in a system based on the localized voltage dip measurements. When a control action such as changing exciter voltage setpoint is enacted, the bus terminal voltage changes—the magnitude can dip or swell for a specific duration. Thus, a voltage disturbance occurs. Since the different control actions cause discernible voltage dip behaviors, one can study the localized voltage data to determine what control action caused the disturbance.

In this chapter, we develop a generator control action classification method using wavelet decomposition and support vector machine (SVM) applied to localized voltage measurements. With this method, a voltage disturbance is classified as a control action, such as change in governor setpoint or exciter voltage setpoint, that has occurred at a particular generator in the system. This work essentially explores root causes of voltage disturbances, focusing on generator control action events. Furthermore, we investigate the method's performance when the availability of training data, the generator bus voltage measurements, is reduced and we lack data from each generator bus.

8.2 Background

The behavior of voltage disturbances, either dips or swells, is integral to the development of this classification method. Background on voltage disturbances and a review of the data mining techniques that have been previously applied to the area are presented in this section.

8.2.1 Voltage Disturbances

Voltage dips can occur due to events such as a motor starting, various faults, switching of generators, and energizing of transformers. A voltage dip is defined as a reduction of the voltage magnitude from threshold value with a duration of a few cycles to several seconds [128]. This reduction can be anywhere from 10% to 90% of the supply voltage and last 10 ms to 1 min. Voltage dips can also be generalized to voltage disturbances, which can be characterized as a dips, swells (increase in voltage), or interruptions. The characterization of voltage disturbances according to voltage magnitude change and duration is illustrated in Figure 8.1. It is important to determine the cause of voltage dips swiftly and accurately to employ mitigation techniques. Voltage dips can have detrimental effects on the power system; they have

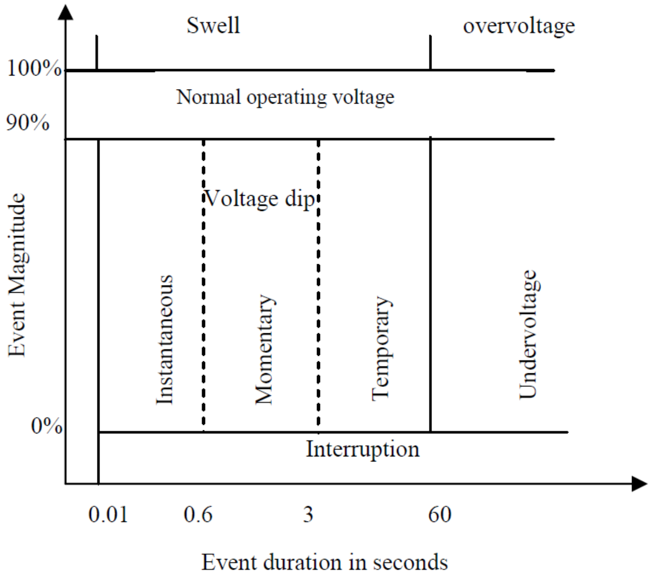


Figure 8.1: Voltage disturbance definition from IEEE Std. 1159-1995 [128].

been identified as one of the main power quality problems due to their high costs and potential to damage sensitive equipment.

Nonetheless, voltage dips can be characterized by their magnitude and duration. They can be classified by their signature, or dip type, by defining complex voltages and phasor diagrams based on the relations between minimum line-to-ground voltage and minimum line-to-line voltage. Using such classifications, the dips can be classified as being caused by faults, motors, transformer energizing, etc. By defining different classes of voltage dips and access to power system voltage data, techniques can be applied to identify voltage dip types using only measurements.

With access to these expansive measurements, characteristic voltage profiles can be constructed for particular events. For example, in the case of a generator control action, a specific control action such as a change in exciter voltage setpoint (EVS) will have a different effect on the voltage profiles of the generator buses than a change in governor setpoint (GS). Furthermore, the behavior of the voltage profiles will be different depending on the generator at which the action was incurred and the type of control action. In Figure 8.2, a change in EVS (to 1 *p.u.*) was enacted on Generator 2 and the voltage profiles for all the generator buses in the 9-bus system are shown, where Generator 1 is the slack bus. It can be observed that each of the voltage profiles, constructed with the localized generator bus voltage measurements (simulated, without noise), is discernible for each generator. As expected, Generator 2, where the control action occurred, has the most significant change in its voltage profile.

Therefore, voltage disturbances caused by events such as control actions or faults will have discernible effects on the system voltage data, or voltage profiles. Access to the voltage data from the distributed measurement devices allows access to broad, fast-sampled voltage data that can be analyzed with various methods. With the increasing number of measurements, data mining techniques have become more pertinent and useful, as is explored in the following section.

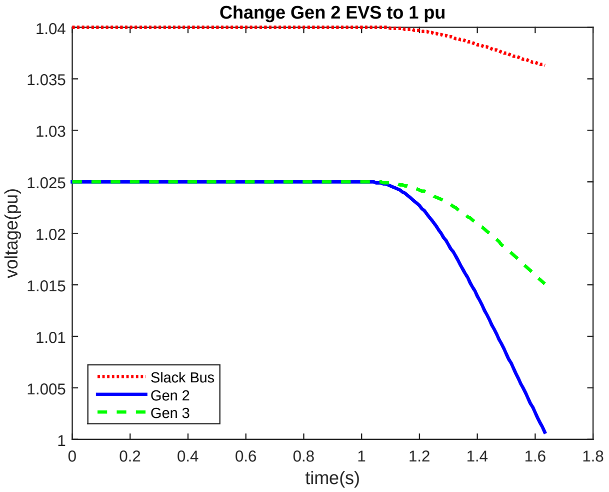


Figure 8.2: Voltage profiles of all the generator buses after a change in EVS at Generator 2.

8.2.2 Review of Data Mining Methods for Voltage Dip Problems

In the power systems domain, data mining (DM) techniques are implemented for multiple analytical purposes. More relevant studies to this research include Ipinnimo el al. [128], Li et al. [129], Alluri et al. [126], Seethalekshmi et al. [130, 131], and Parikh et al. [132]. In reviewing these papers, the general steps were:

1. Gather voltage data (e.g., from devices or simulated)
2. Convert voltage data (i.e., wavelet) into a format for DM techniques
3. Train a classifying model
4. Choose most suitable parameters
5. Validate accuracy of training model
6. Test/validate

One of the most pertinent steps is the conversion of the data. Voltage data (i.e., wavelet) needs to be converted into a format (i.e., symbolic string) that can be used with data mining techniques. A symbolic string such as Symbolic Aggregate ApproXimation (SAX) used by [126] is one method.

SAX is a well-known symbolic representation for time-series, similar to discrete Fourier translation (DFT), discrete wavelet translation (DWT), singular value decomposition (SVD), and piecewise aggregate approximation (PAA), which are the discretized data representations of time-series.

Although data mining based power system methods require more detailed measurements, the advent of distributed monitoring devices such as PMUs enables such data collection. The main benefits of applying DM techniques in power system analyses include the ability to generalize at high speed, learn from experience, synthesize complex mappings, and handle noisy or incomplete data. Moving forward, the use of DWT for data conversion and SVM based methods are promising techniques for the classification of voltage disturbance events in power systems. Motivation for using SVM for our work is explained further in Section 8.3.3.

8.3 Method

To classify the generator control actions based on localized voltage measurements, a method was developed using SVM and wavelet decomposition. The proposed method is summarized as follows: 1) Events that cause voltage dip and disturbances were simulated and samples were generated using PowerWorld. 2) By iterating through different types of mother wavelets, we found the optimal mother wavelet used during discrete wavelet transformation (DWT) that transforms voltage data into a form that can be used with SVM. 3) For SVM training, different kernel functions and parameters were tested to find the optimal set that yields the highest accuracy. 4) We performed k-fold cross-validation to validate our accuracy results (see Figure 8.3).

8.3.1 Event Simulation and Data Sampling

For method testing, simulation of voltage disturbance events to obtain the time-series voltage data was necessitated. These simulations were performed in PowerWorld Simulator, an interactive power system simulation software, using the transient stability tool. In this manner, time-series voltage data can be obtained during a specified simulation period, with the event incurred

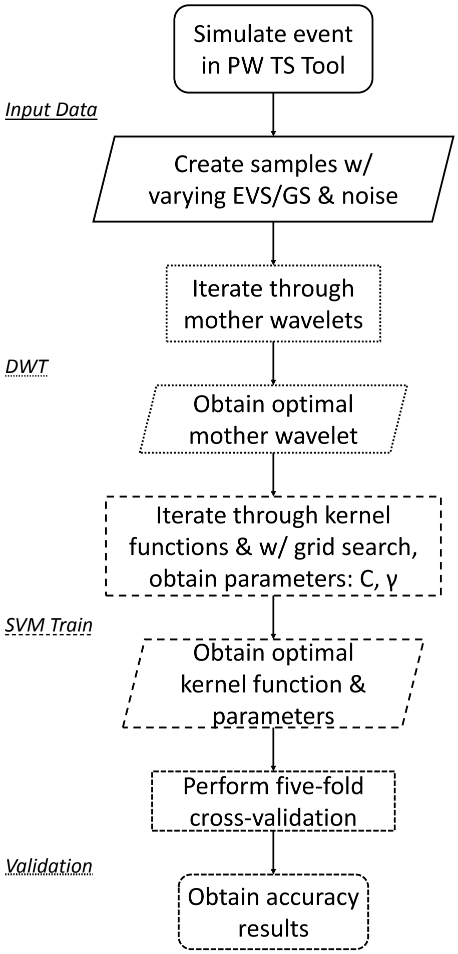

Simulate event in PW TS Tool
Input Data
Create samples w/ varying EVS/GS & noise
Iterate through mother wavelets
DWT
Obtain optimal mother wavelet
Iterate through kernel functions & w/ grid search, obtain parameters: C, γ
SVM Train
Obtain optimal kernel function & parameters
Perform five-fold cross-validation
Validation
Obtain accuracy results

Figure 8.3: Process model for the proposed method.

at a certain time point.

By applying the different generator control actions at each of the generators in the system, the time-series voltage disturbance data was captured for each event. Noise was added to these data sets in Matlab, a computational platform, to create further samples and reflect real-world conditions.

8.3.2 Data Conversion

To use signal behaviors as features, wavelet data needs to be decomposed into localized time and frequency components. Choosing a right mother wavelet is crucial in characterizing signals. A wavelet is a basis function that is isolated with respect to time or spatial location and frequency or wave number. It is defined by the parent wavelets: the mother wavelet characterizes the basic wavelet shape (the wavelet function) and the father wavelet characterizes the basic wavelet scale (scaling function) in the time domain. In power systems, Daubechies (db) has been known as the best wavelet family for characterizing voltage signals [132, 133]. Discrete wavelet transformation (DWT) is used to decompose the original signals to two halves of frequency components using high-pass and low-pass filters. To find the most suitable wavelet type, within the family of db, all wavelet types, db1 to db45, were tested for our case.

8.3.3 Data Mining Technique for Classification

Among the literature we have surveyed, ANN and SVM are two classifiers that can be compared against each other and perhaps are the most suitable techniques for our purpose. Seethalekshmi et al. [131] claim that SVM (structural risk minimization) is better than ANN (empirical risk minimization). Empirical risk minimization involves many uncertainties associated with empirical data and is centered around approximation.

Though Tsallis wavelet energy entropy (TWEE) and clustering were used to classify transient voltage disturbances by Li et al. [129], extensive training information is required to apply TWEE for feature extraction. Various faults with different parameters need to be applied to construct the TWEE curves, which can be system dependent and become computationally burdensome as the system size increases. The use of particle swarm optimization, genetic algorithms, and neural networks was also discussed in the context of power systems with distributed generation. Yet, the need for approximations with neural networks and increased complexity motivates the use of the SVM method for our work.

Support Vector Machine

SVM has gained its popularity in power systems due to its effectiveness in classifying different wavelet behaviors. Classification tasks involve the separation of data into training and testing sets where each instance in the training set contains one target value or class label and several features/attributes [134]. Ultimately, the SVM method aims to produce a model using the training data to predict the target values of the test data given only the data attributes.

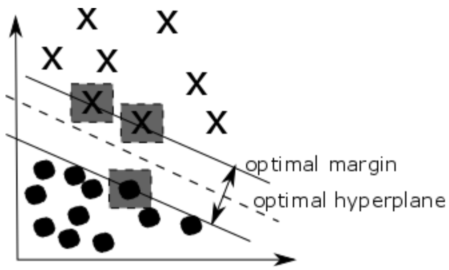


Figure 8.4: Linear SVM classification concept representation.

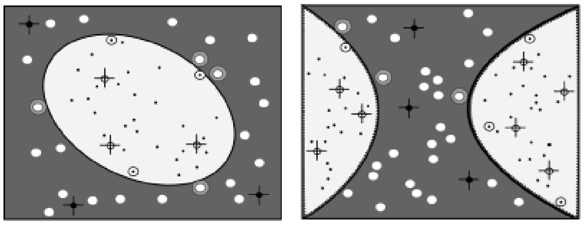


Figure 8.5: Nonlinear SVM classification concept representation.

SVM solves an optimization problem by fitting hyper-planes or decision boundaries that divide different sets of points. The linear SVM finds a hyperplane by computing a dot-product between the points and a normal vector to the hyperplane and is expressed as follows:

$$w \cdot x + b = 0 \tag{8.1}$$

where w is a normal vector, x is data points and b is a bias term. The optimal hyperplane best separates data points with maximized margin between the vectors (w) of the two classes (see Figure 8.4).

A nonlinear system including higher dimensional spaces requires use of a kernel function instead of the dot-product for separating spaces nonlinearly:

$$K(u, v) = \sum_{i=1}^{\infty} \gamma_i \phi_i(u) \cdot \phi_i(v) \tag{8.2}$$

where $\gamma_i \in \Re$ and ϕ_i are eigenvalues and eigenfunctions [135]. This kernel trick allows one to nonlinearly partition complicated data in a higher dimensional space. Figure 8.5 illustrates nonlinear separation of data points. There are multiple kernel functions that can be used to separate data points. For SVM, selection of a kernel function requires an iterative process to find one that yields the best accuracy. This process is detailed in Section 8.4.

8.3.4 Validation

K-fold cross-validation, which is commonly used in predictive models for adjusting parameters, is used. Input data is divided into training and testing data randomly with a fixed proportion (i.e., 80% training and 20% testing). Data is randomly partitioned into k subsets. One subset is used for testing and the remaining are used for training. This process is repeated k times and the results are averaged. The cross-validation procedure can prevent overfitting issues, improving the result accuracy [134].

8.4 Evaluations

8.4.1 Case Study: 9-Bus System

To develop our method, we simulated voltage dip data with different control actions incurred at different generators. A 9-bus power system case in PowerWorld was used for this study. The system has 3 generators: one at the slack bus (bus 1), one at bus 2, and one at bus 3. These are shown in the one-line diagram in Figure 8.6. Two control actions are used: change in exciter voltage setpoint (EVS) and change in governor setpoint (GS).

Ignoring the slack bus, the control action and generator combinations we have are:

1. Change in EVS at Generator 2
2. Change in EVS at Generator 3
3. Change in GS at Generator 3

Input Data Simulation The generator setpoints, for both exciter and governor, are varied in 0.01 $p.u.$ intervals for a range of $0.9 - 1.1$ $p.u.$ in PowerWorld. We do not consider the change in GS at Generator 2 as it does not affect the system voltage noticeably. The transient stability tool in PowerWorld is utilized to capture the effect of the setpoint change in a 10 s simulation, where the change is incurred at 1 s. The time-series voltage data for the generator bus voltages (bus 1, bus 2, bus 3) are obtained from PowerWorld and transferred to Matlab. To mimic real world data, normally

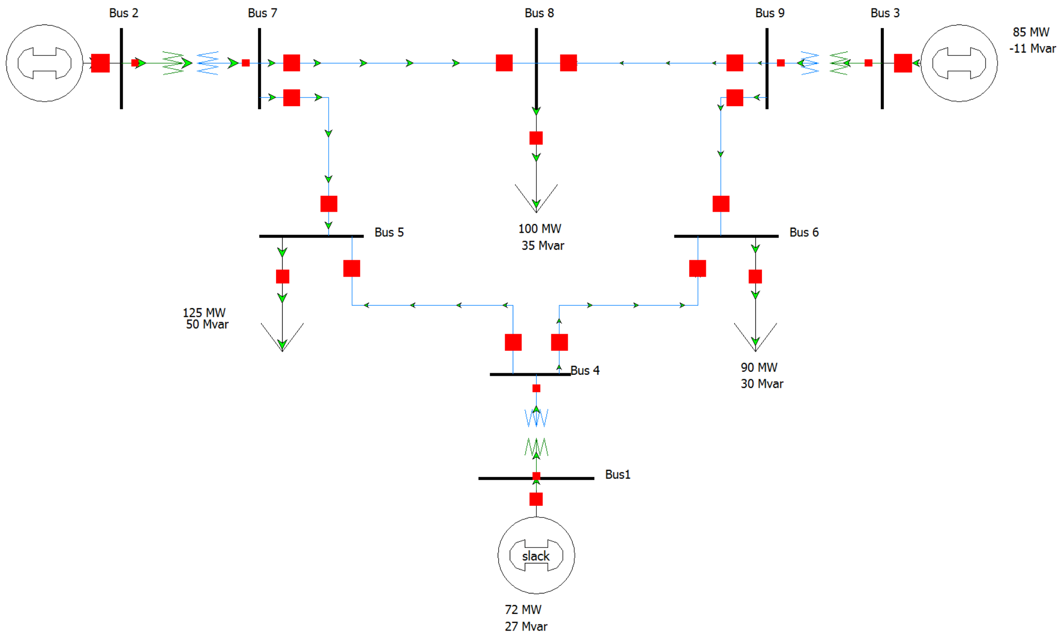


Figure 8.6: PowerWorld 9-bus system case with three generators at bus 1, bus 2, and bus 3.

distributed random noise is added to the voltage data. For every control action and generator event, as well as the specific setpoint change, 100 noisy samples were generated. In total, there are $6,000$ voltage profile sets that are input into our method.

To use the obtained voltage data with SVM, the voltage signals were decomposed using DWT. For choosing a mother wavelet, Daubechies (db) has been used, as discussed further in the next section.

Discrete Wavelet Transformation Within wavelet family db, db1 to db45 were tested using a grid search to find a mother wavelet that yields the best result. Decomposition level is chosen as 6, which has a frequency band range of 31.25 to 62.5 Hz [132]. We found that db25 yields the highest accuracy for our case.

Support Vector Machine To find the optimal kernel function and parameters with the best accuracy, a grid search is performed. The grid search is recommended for finding the optimal set of SVM parameters because it avoids any approximations or heuristics via the exhaustive search. It can be easily parallelized because each (C,γ) is independent [134]. It is important that the optimal set is found, for instance, cost parameter C that optimizes the margin of a hyperplane and therefore dictates the number of misclassification and kernel parameters. In other words, SVM draws a decision boundary (a nonlinear hyperplane) in n-dimensional space that divides each class from the others. These parameters determine how these divisions are made; therefore, we have to search for an optimal set of these parameters that best maximizes the margin of the hyperplane.

The kernel functions tested are as follows [136]:

1. Polynomial: $K(u, v) = (\gamma u^T v + c)^d$

2. Radial Basis Function: $K(u, v) = exp(-\gamma * |u - v|^2)$

3. Sigmoid: $K(u, v) = tanh(\gamma * u' * v + c)$

4. Intersection: $K(u, v) = min(u, v)$

5. Jensen-Shannon's: $K(u, v) = \frac{u}{2} log(\frac{u+v}{u}) + \frac{v}{2} log(\frac{u+v}{u})$

where c, d and γ are kernel parameters. The cost parameter C and γ were iterated through ranges of $(10 : 10^7)$ and $(10^{-6} : 10])$, respectively. The trained models are five-fold cross-validated (i.e., data is randomly partitioned by a ratio of 80% to 20% for training and testing data, respectively and repeated five times).

Table 8.1: Summary of the Experiment, Showing Optimal Kernel Function and Its Parameters

Kernel	C	γ	Accuracy %
Polynomial	10^6	10^{-2}	86.76
RBF	10^7	10^{-5}	67.01
Sigmoid	10^7	10^{-3}	80.81
Intersection	10^7	10^{-6}	**98.14**
Jenson-Shannon's	10^3	10^{-4}	94.93

Validation The 6,000 noisy data samples were discretized using DWT with db25 mother wavelet at decomposition level 6, as discussed previously. The discretized and transformed wavelet data were trained using multiple kernel functions, varying values of parameters C and γ for comparison. The trained model was five-fold cross-validated. The model was trained and tested five times on 80/20 random split of the data (80% for training and 20% for testing).

The intersection kernel function with parameters $C = 10^7$ and $\gamma = 10^{-6}$ yielded the best average accuracy of 98.14%. The SVM parameters (C, γ) were the optimal set found via grid search, and indeed provided the best results. The results of different combinations of kernel functions and parameters are summarized in Table 8.1, which shows the parameter combination that yielded the best average accuracy for each kernel function. As exemplified, the grid search choice of the intersection kernel and associated parameters provided the highest accuracy.

8.4.2 Availability of Training Data

The aforementioned results assume that local voltage measurements are available from every generator in the 9-bus system. That is, we have voltage data from all 3 generators: one at the slack bus (bus 1), one at bus 2, and one at bus 3. However, measurements from each generator bus will not always be available or accessible. Our classification algorithm must be tested for the more realistic case in which voltage data from particular generator buses is not available for training the SVM model. We must examine the model's performance, with the reduced set of training data, in classifying all the generator control actions (change in EVS at Generator 2, change in EVS at Generator 3, change in GS at Generator 3).

The full set of data would include time-series bus voltage measurements for each of the generators: Generator 1, Generator 2, and Generator 3. The control actions to be classified occur at Generator 2 and Generator 3. Therefore, to exemplify when not all measurements are available, the cases presented in Table 8.2 are evaluated.

Table 8.2: Availability of Voltage Measurements from Each Generator Bus for Each Evaluation Case

	Available Data	**Unavailable Data**
Case 1	Generator 1, Generator 2	Generator 3
Case 2	Generator 1, Generator 3	Generator 2
Case 3	Generator 1	Generator 2, Generator 3

These cases were input into the method and the results are summarized (with SVM parameters) in Table 8.3. In addition, the wavelet type and decomposition level pairs (db,lev) for each case were found via grid search as (db34, 2), (db27, 3), and (db1, 6), respectively. As observed, Case 1 and Case 2 maintain high accuracy with average accuracy values of 98.97% and 97.94%, respectively. Therefore, even when Generator 2 or Generator 3 voltage data is not available, control actions occurring at Generator 2 and Generator 3 are still classified with high accuracy.

However, when data for both Generator 2 and Generator 3 is unavailable, as in Case 3, a lower average accuracy of 86.62% is obtained. From these tests, we can glean that the classification method performs fairly well when not all voltage data is available, but not when the majority is missing. Further study must be conducted on larger systems to investigate if the location of the generator, number of generators, and/or slack vs. non-slack bus generators contribute to these observations.

Table 8.3: Summary Results for Different Data Availability Cases with SVM Parameters and Average Accuracy Achieved

	Kernel	C	γ	Accuracy %
Case 1	Intersection	10^5	10^{-5}	98.97
Case 2	Intersection	10	10	97.94
Case 3	Intersection	10	10^{-6}	86.62

8.5 Conclusions

A method for classifying generator control actions using localized measurements was developed using SVM and wavelet decomposition. By iterating through different DWT parameters, kernel functions, and SVM parameters, the optimal set yielded the highest average accuracy of 98.14%. It was successful in identifying the different control actions, as well as the particular buses in which they were incurred. When the availability of training data, the generator bus voltage measurements, is reduced, the algorithm still performs with fairly high accuracy. These cases will be investigated further to gain insight into the range of availability that is necessary.

To extend this work, future plans include using larger systems and also testing real data. Furthermore, we would like to include other voltage disturbances in our study such as fault, motor starting, and transformer energizing events. In this manner, a more comprehensive classification of the voltage disturbance events can be obtained.

All in all, the developed classification method is able to successfully identify generator control actions (and on which bus they were incurred) based on localized voltage measurements, even with reduced availability of training data. This initial study provides the groundwork for applying our classification techniques to a broader spectrum of voltage disturbance events. Moreover, by leveraging knowledge of prior power system behavior, we are able to significantly reduce the training data set. This helps the usability of data mining algorithms in power systems, as we can enhance the methods with domain-specific knowledge to achieve faster and more accurate results.

CHAPTER 9

IMPROVING POWER SYSTEM NEURAL NETWORK CONSTRUCTION USING MODAL ANALYSIS

9.1 Problem Statement

From load forecasting to dynamic security assessment, artificial neural networks (ANN) have prominent and widespread applications in the power system domain [137–139]. Machine learning techniques such as ANN, support vector machine (SVM), clustering, and others have seen an increase in use over recent years, driven by the growing availability of data [127, 139]. Measurement sources include distributed monitoring devices such as phasor measurement units (PMUs) as well as smart meters and home appliances. By leveraging this access with powerful machine learning tools, power system decision making, situational awareness, and response are greatly improved.

In particular, ANN is extensively used in formulating power system solutions. This is due to attractive features such as the ability to learn complex nonlinear relationships and modular structures that can allow parallel processing [140]. An ANN is a biologically inspired programming paradigm that is able to learn from observational data [141]. ANNs are also computing systems; each is composed of a number of simple, highly interconnected processing elements, which process information by their dynamic state response to external inputs [142]. The large scale and nonlinearity of power systems are factors that contribute to their complexity, and ANNs hold promise for tackling these challenges.

Short-term load forecasting, defined as predicting future load series minutes, hours, or days ahead, has been achieved with ANN in experiments and practical tests. However, Hippert et al. [137] conducted a review and evaluation of these ANN-based forecasting systems to address skepticism that the ANN use has been systematically proven. Specifically, the study found that the neural network architectures chosen for the data samples were not suitable and perhaps too large with many parameters to be estimated, often resulting in overfitting and poor out-of-sample testing results [137]. The authors also noticed that the models were not systematically tested and that more rigorous results are needed to fully validate.

Besides load forecasting, ANNs have also been utilized to replace complex power system models to aid computation of different power system analyses. Xu et al. [143] considered the challenge of modeling nonlinear three-phase photovoltaic generators (PVGs) for power flow analysis. Transient stability assessment has been paired with ANN by Bahbah et al. [138] with generator angle and angular velocity prediction for multi-machine power systems. Additionally, Qian et al. [144] performed transient stability studies using ANN models for generators, excitation systems, and governors individually and subsequently linked them.

These ANN power system applications, both for load forecasting and replacing complex machine models, indicate experimental success. Yet, as noted by Hippert et al., no systematic approach is apparent, specifically with regard to selecting the number of ANN parameters (e.g., number of layers, number of neurons, activation function) and testing approaches. This work focuses on developing a data-dependent and *power system-dependent* procedure for the selection of ANN parameters. The approaches used presently rely on trial-and-error by assessing resultant accuracy iteratively, existing model setups that may not translate for a different application, and/or outsized ANNs that may suffer from overfitting.

Nonetheless, we seek to improve the selection of ANN parameters by leveraging power system behavioral knowledge. The power system exhibits patterns rooted in the physics of the various components and interconnections as well as specific topologies. For example, when a disturbance occurs, we know the oscillatory response of the system will be dictated by the modes of the system [145] and that the topology of the system will impact the stability of the system given such a disturbance. We also know that voltage disturbances, caused by faults or control actions, are localized and studying only local bus voltage measurements is sufficient for classification methods, significantly reducing training set size and computation time, as presented in Chapter 8. We develop analytical methods to reconstruct such insight into power system behavior and (in this work) to leverage it for ANN modeling applications, particularly to reduce trial-and-error.

To explore the connection between power system analyses and ANN parameter selection, this chapter develops a systematic method for selecting the number of neurons for a model. Instead of relying on trial-and-error or inconsistent heuristics, we present an algorithm that is dependent on the power system being studied and the data set. For this investigation, we replace generator models with ANN in a post-fault system. The input data consists of the generator real power and exciter field voltages, and the generator rotor angles are obtained as output, assessing the system stability. Modal analysis is applied to determine dominant modes of the system and we hypothesize that the number of dominant modes can be equated to the number of neurons to be used. This idea is developed further in the remainder of this chapter.

9.2 Literature Review

9.2.1 Artificial Neural Networks

An artificial neural network (ANN) processes a set of input data, usually referred to as training data, through its structure of weights, connections, and activation functions that are then adjusted using a specific training algorithm. Through these iterative adjustments, the ANN will increase its ability to correctly recognize patterns and classify or quantify an output. In this section, we will provide a brief description of ANNs, but comprehensive and detailed reviews can be found in [137, 140–142].

The basic unit of a neural network is an artificial neuron that receives input data information and processes it. The input values are linearly combined, using input weights and constant bias terms, and then an activation function is applied. An example is shown in Figure 9.1 (biases not shown). This nonlinear activation function is required to be non-decreasing and differentiable (e.g., sigmoid function).

For most power system applications, we utilize multilayer perceptron (MLP) networks that arrange the neurons, or more generally units, in layers [137]. In the feed-forward network, the outputs of one layer are inputs to the following layer; layers between are called hidden layers. The different weights on the connections and the bias terms are the parameters of the network, and estimating them is the focus of training the network using optimization

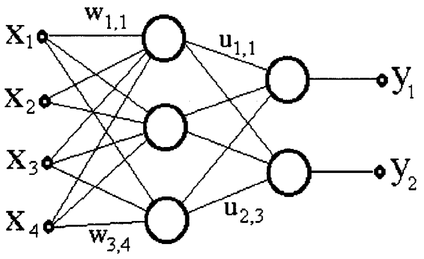


Figure 9.1: Example two-layer neural network with four input nodes, various weights, and two output nodes [137].

functions such as gradient descent.

9.2.2 Power Systems ANN Applications

Since the early 1990s, the electric power system industry has seen a new movement toward artificial intelligence and machine learning to either model or predict certain phenomena within the systems. Due to prior successes, the most researched areas include load forecasting, fault diagnosis, economic dispatch, security assessment, and transient stability [140].

One notable application is in load forecasting and its effects on economic development and planning. Current models have had difficulty in many areas such as finding a relationship between variable and instantaneous load demand and ability to reevaluate the set of laws that govern the complex system and adjust themselves with rapid nonlinear system-load changes [146]. Another prominent application is the ability to diagnose faults, their locations, and how to most effectively clear them. This is an important application because during the event of an outage an operator may become overwhelmed by the excessive amount of alarms and signals. An ANN in this setting has performed well in identifying problems and successfully diagnosing errors due to its flexibility in classification and its ability to handle noisy data which is generally produced during these events [146].

However, in this scenario, it is critical to have best case computational efficiency in order to avoid serious damage to the power system and the consumers it supports. This is an extremely difficult problem in modern ANN applications. During the 1990s, expert systems were the main tool used; however, they had a major drawback of not being able to handle the complexity of growing power systems. Recently, ANNs have been used to handle this complex problem; however, they too have a setback. With many neural units, or neurons, to model such a complex system, the cost, both in time and computational power, to train the model, whether it be feedforward, backpropagation, etc., is so large that at times it makes this model obsolete. Advancements in processing power and development of new training algorithms in the past decade have greatly benefited the feasibility of these models SP8.

Although the application of ANNs in these areas of power systems has proven useful, improved structure is needed. Of the many necessities of creating a reliable and accurate neural network, there are two main focuses for power system ANNs. They are efficiency and the handling of noisy data, both being mainly driven by the size of the ANN itself; efficiency calls for fewer neurons (units) and handling noisy data calls for more. For efficiency, it is important for a model to accurately and, in a timely manner, predict its output before any damage is incurred to a power system. Any additional units within an ANN will slow both training and prediction. Conversely, handling noisy data is a task that generally improves as the number of units increases. If many units are present in the network, a meaningless input can be pinpointed during training and have devalued weights so that the values have minimal effect on the generated output. However, with fewer units in the network, it is more difficult as each unit is influenced by many input variables. If one unit is influenced by both an important variable and an insignificant one, the average will be middle-tier influence on the generated output that devalues important information and overvalues meaningless information, which will clearly lead to increased error and inhibit successful modeling.

9.2.3 Selection of Number of Neurons

The goal of this chapter is to use a deep knowledge of power system behavior in order to find a balance of the two main focuses provided earlier, to create a potential best case number of units in a hidden neuron layer within an ANN model that can generate timely and accurate predictions, even with a set of noisy data.

Selection of a neural network structure, in many scenarios, is done through computation. The number of neurons can be set as an arbitrary value, and during training, a better number will be found through some algorithm [147]. In almost all cases, this selection increases the computational cost and time incurred by additional cross-validation. For power systems, this additional cost may not actually outweigh the small benefit from error minimization if there is a known value that can perform better under tighter time constraints.

In recent years, there have been many attempts to provide a standard for the number of neurons in the hidden layer of an ANN. Generally, these all relate the number of input neurons, output neurons, input variables, and a few other metrics to generate the appropriate number of units. However, they are unfortunately too general to be very accurate for all sets of data, as there are potentially many more unknown variables that go into this calculation [148].

As mentioned, the goal of this chapter is utilize a deep understanding of power system behavior in order to set a value for the number of hidden neurons in a neural network model. Through many experiments and generated results, we seek to link modal analysis of power systems with the number of neurons in the hidden layer of a neural network as we feel there can be a qualitative reason to model an ANN using the number of most dominant power system modes [149].

9.3 Method

9.3.1 Modal Analysis

Small signal stability is the ability of a power system to maintain its synchronism after a small disturbance. Modal analysis is the analysis of small signal stability through the eigenvalues; it also looks at the eigenvectors, the participation factors, and the mode shapes [86, 150, 151]. To obtain those parameters, first the power system is described by a set of equations:

$$\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}, \mathbf{y}) \qquad \mathbf{0} = \mathbf{g}(\mathbf{x}, \mathbf{y}) \tag{9.1}$$

where $\mathbf{x}$ is the vector of state variables (such as the generator rotor angles δ_i and rotor speed ω_i) and $\mathbf{y}$ is the vector of the algebraic variables (primarily the bus complex voltages). Next, the system can be linearized about the equilibrium point as:

$$\mathbf{\Delta\dot{x}} = \mathbf{A\Delta x} + \mathbf{B\Delta y} \tag{9.2}$$

$$\mathbf{0} = \mathbf{C\Delta x} + \mathbf{D\Delta y} \tag{9.3}$$

The variable $\boldsymbol{\Delta y}$ in (9.2) and can be substituted using (9.3) to derive a differential equation of only variable $\boldsymbol{\Delta x}$ as follows:

$$\mathbf{\Delta\dot{x}} = (\mathbf{A} - \mathbf{BD^{-1}C})\mathbf{\Delta x} \tag{9.4}$$

$$\mathbf{A_{sys}} := \mathbf{A} - \mathbf{BD^{-1}C} \tag{9.5}$$

$$\mathbf{\Delta\dot{x}} = \mathbf{A_{sys}\Delta x} \tag{9.6}$$

Equation (9.6) represents the deviation of the system's state away from the equilibrium point. As the result, small signal analysis is done by looking at the eigenvalues and other properties of $\mathbf{A_{sys}}$. The full derivation of the eigenvalues and eigenvectors from $\mathbf{A_{sys}}$ is provided in Section 5.5.1, but ultimately the response $\mathbf{\Delta x}(t)$ can be rewritten as an equation of individual eigenvalues and right eigenvectors [86].

$$\mathbf{\Delta x}(t) = \sum_{i=1}^{n} \mathbf{v_i} z_i(0) e^{\lambda_i t} \tag{9.7}$$

9.3.2 Mode-Dependent Neuron Number Algorithm

As described in the previous section, modal analysis provides powerful insight into a specific power system and its response to various disturbances. We obtain information on the prominent modes of the system and how they dominate the response of certain system changes or events. These modes are unique to the component, system topology, and disturbance that are being studied. Thus, discovering the dominant modes for a particular situation provides information on the dominant behaviors and patterns present.

Within our neural network model, the neurons, or units, are “activated” depending on the input data presented. This activation is dependent on the type of function used as well as the input/output weights and biases, the latter two of which are the results of the neural network training and optimization. Ultimately, the activated units determine the output result. A specific set of units is activated for a particular set of input data. Depending on the activation function, the activation can have discrete or continuous values. For example, for a simplistic step function, as shown in Figure 9.2, the unit is either “on” or “off”. However, for the popular sigmoid function shown in Figure 9.3, the activation will take on a value between 0 and 1. Different patterns or behaviors inherent within the input data are what differentiate the unit activation sets. The dominant modes of a dynamic system determine how the system will respond to a disturbance. The combination of these modes dictates the majority of the system response. In that case, what if the number of dominant modes could be equated to the number of units in the neural network?

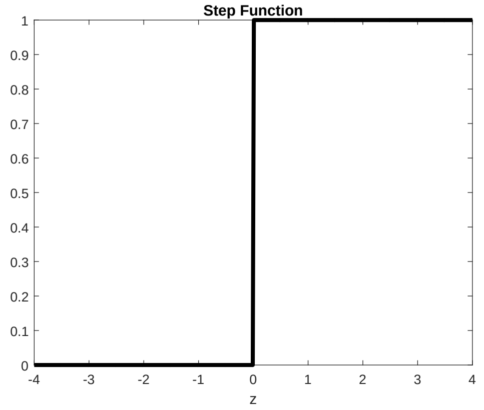


Figure 9.2: Step function.

The units and their combination provide the output result in the neural network. Our intuition from the power system and modal analysis motivates the hypothesis that the number of dominant modes represents the most significant patterns in the system and thus could capture the different behaviors successfully, similar to the function of neural network units. At the very least, the number of dominant modes provides an estimate of the number of units. To achieve this estimate, we follow the process illustrated in Figure 9.4. First, we obtain the model of the power system to analyze either mathematically or with power system simulation software. Depending on the application and what event is being studied, one may be more beneficial than the other. In

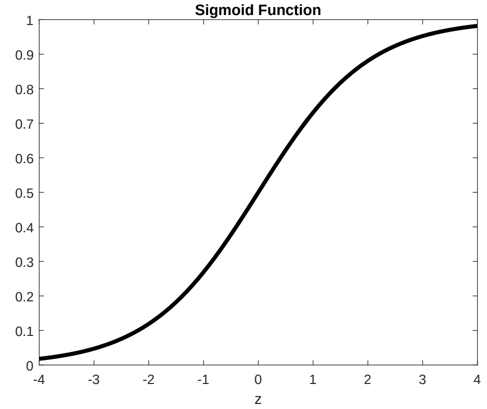


Figure 9.3: Sigmoid function.

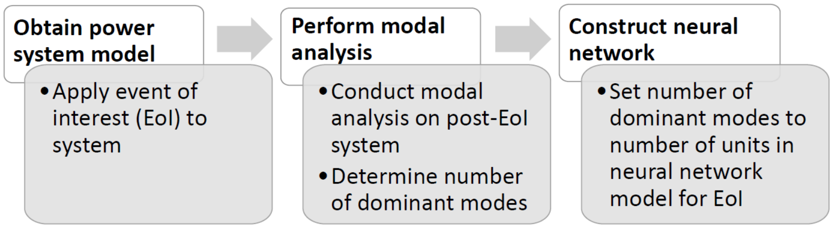

Obtain power system model
• Apply event of interest (EoI) to system
Perform modal analysis
• Conduct modal analysis on post-EoI system
• Determine number of dominant modes
Construct neural network
• Set number of dominant modes to number of units in neural network model for EoI

Figure 9.4: Mode-dependent neuron number algorithm.

our case, we model our system in PowerWorld [84], a simulation software, as we will study generator bus faults and the subsequent impact on rotor angle response.

The event of interest (EoI) that is being studied using the neural network, whether it be a change in load or a system fault, is applied to the system and modal analysis is conducted on the post-EoI system. Depending on the type of study being conducted, different components will vary the EoI parameters and modal analysis must be performed for each to obtain the most comprehensive result. In our example scenario, we only perform modal analysis once as we construct the neural network only for generators in various post-fault systems.

To determine the significant modes, methods using Prony analysis such as [152–154] can be used. We utilize the largest weighted percentage (LWP) values of each mode to determine the most dominant in the post-fault response, as calculated in PowerWorld. The LWP is the largest signal component in the mode weighted by time and is expressed as a percentage of total signal components. Subsequently, we analyze the LWP values by calculating the percent difference ($pDiff$) of the max LWP against the rest of the values, shown in (9.8); if $pDiff$ is less than the threshold difference of 50%, we count that mode as dominant.

$$pDiff = \frac{LWP - max(LWP)}{max(LWP)} \tag{9.8}$$

Finally, we set the number of dominant modes as the number units in the hidden layer of our neural network.

9.4 Evaluations

To demonstrate the mode-dependent neuron selection algorithm, we studied a neural network model developed for power system generators. The ANN takes input of the generator real power and electric field voltage and provides the rotor angle response after a balanced three-phase fault on a generator bus (all time-series data). Thus, we achieve the response without requiring the complex generator and system model. The input data selection is based on the experiment performed in [138]. The location of this fault varies, excluding the slack bus, and the clearing time also varies. For the training data set, a three-phase fault was applied at each generator bus and data was collected for 20 different clearing times (up to the critical clearing time). These faults were simulated in PowerWorld and the data was obtained with the transient stability toolbox [84].

A nonlinear autoregressive network with exogenous inputs (NARX) with one hidden layer is constructed with the training data set and the mode-dependent estimate of units is used and compared against other random or heuristic-based values. The NARX feedback neural network is often utilized for time-series prediction, as is our goal, and is described further in [155]. The post-fault generator rotor angle scenario is applied to the EPRI 20-bus system shown in Figure 9.5.

The system has 7 generators of which Generator #1 (at bus 1) is the slack bus and is excluded. Therefore, faults are simulated and data is obtained from 6 generators at 20 different clearing times for each. The mode-dependent neuron number algorithm, summarized in Figure 9.4, is applied and Table 9.1 displays an example set of resultant modes for a fault at Gen-

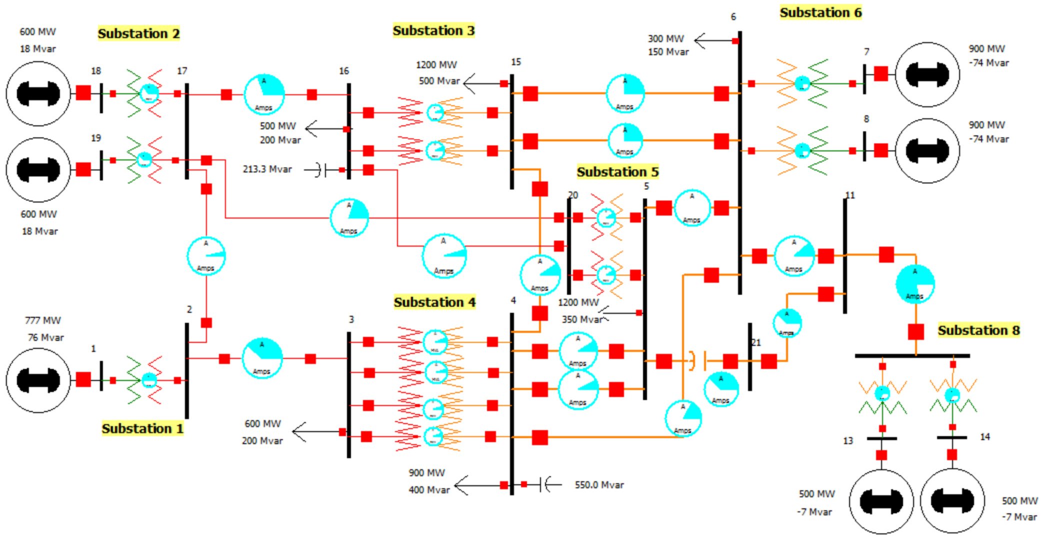


Figure 9.5: EPRI 20-bus system [84].

erator #2 (at bus 7) (number of dominant modes similar across generator buses).

Table 9.1: Resultant Modes and Largest Weighted Percentage

LWP (%)	pDiff (%)	Mode
69.945	0	0.0852
67.8717	0.029	-0.3936
61.021	0.128	-0.2199
52.0739	0.256	-2.0416
35.2362	0.496	-2.6339
29.078	0.584	-0.5904
8.9668	0.872	-1.5463

The dominant modes are highlighted, as calculated with (9.8). With 4 dominant modes, we equate to the number of units in the NARX neural network, as illustrated in Figure 9.6.

We calculate estimates for number of units from known heuristics summarized and discussed in [148]; Table 9.2 lists these estimates for our generator bus fault scenario. Figure 9.7 illustrates the average mean squared error (MSE) that represents the difference between the actual rotor angle response

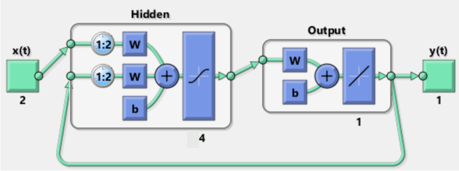


Figure 9.6: NARX neural network with 4 units [156].

Table 9.2: Heuristic Unit Number Methods [148]

Heuristic Method	Unit Estimate
Li et al. method	2
Tamura and Tateishi method	1
Zhang method	3
Jinchuan and Xinzhe method	2
Shibata and Ikeda method	1
Hunter et al. method	3
Sheela and Deepa method	5

(from simulation) and predicted rotor angle response (from the NARX network) for up to 1000 training iterations, in 100 iteration intervals, for various numbers of units (comparing our modal estimate against heuristics), and testing 20 different clearing times at Generator #2 (at bus 7). The mean MSE for each given number of units indicates lower values for 1 and 2 units, similar values for 4 and 5 units, and high error for 3 and 12 units. The mean MSEs for 1 and 2 units are misleading as the model prediction for the rotor angle response is inaccurate, and the low MSE results from consistently producing a relatively flat line through the true rotor angle response as illustrated in Figure 9.8a; it is unsuccessful in capturing all variance in the data.

However, our estimate of 4 units provides a decent estimate, an example of which is shown in Figure 9.8c, with comparatively low MSE error while capturing the variations in the actual response. Figures 9.8a-9.8d show examples of the NARX model's prediction of the rotor angle response for faults at Generator 2 (at bus 7) for different clearing times, number of units, and training iterations. The average MSE of all clearing time and training iterations is represented in the comprehensive Figure 9.7. Figure 9.8d illustrates

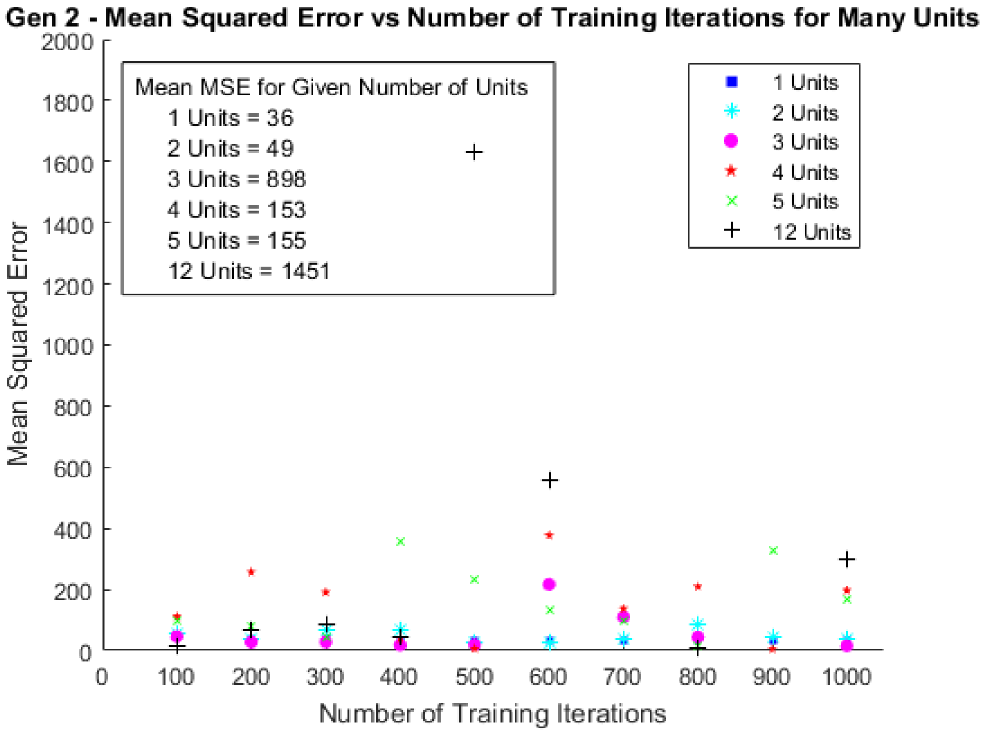
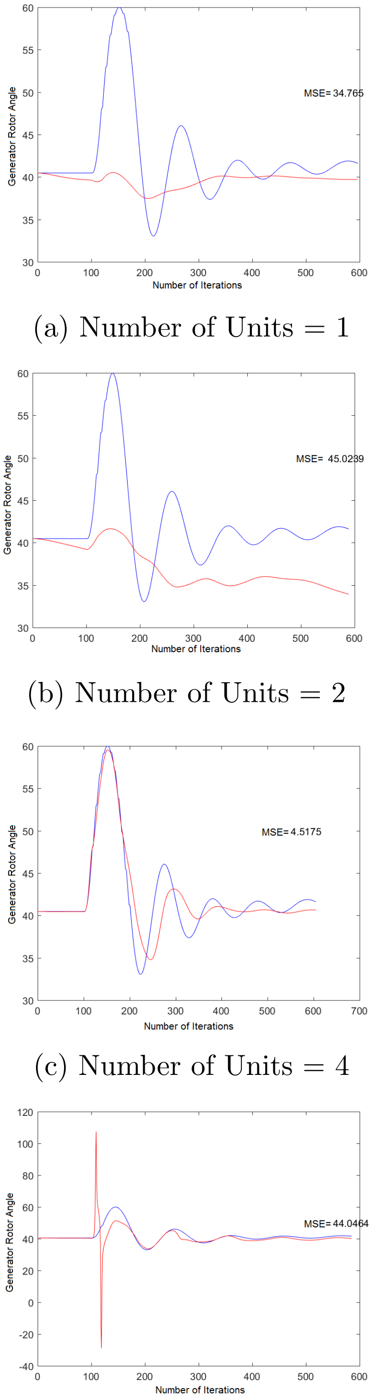


Figure 9.7: NARX: Average MSE for different unit number estimates over many training iterations and clearing times for faults at Generator #2 (at bus 7); the mode-dependent algorithm estimate is 4 units.

an overfitting situation with too many units, resulting in the spikes.

Yet, the NARX feedback neural network with 4 units does not provide good performance in predicting the rotor angle response and results in generally high MSE. The NARX network was a first-step selection to explore the mode-dependent neuron number algorithm and provided a good base in that respect. To improve our actual model prediction, to explore further in future work with the algorithm, we began testing with a layer recurrent neural network (LRNN) architecture in which each layer has a recurrent connection with a tap delay associated with it; essentially, the network is enabled to have infinite dynamic response to time-series input data [156]. The rotor angle response is greatly improved with this network, with our estimate of 4 units, and is represented in Figure 9.9.

The overall performance of this network is shown Figure 9.10 where training is performed with 70% of the data, testing and validation with 15% each. This cross-validation allows for the elimination of overfitting or underfitting issues [136]. An example testing result (fault at Generator #2 (at bus 7)) is



(a) Number of Units = 1

(b) Number of Units = 2

(c) Number of Units = 4

(d) Number of Units = 12

Figure 9.8: Comparison of true rotor angle response (blue line) with NARX network prediction (red line) for various numbers of units.

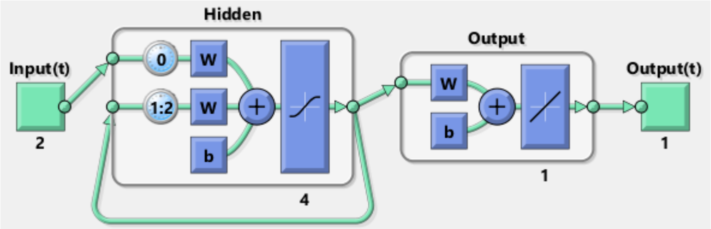


Figure 9.9: Layer recurrent neural network with 4 units [156].

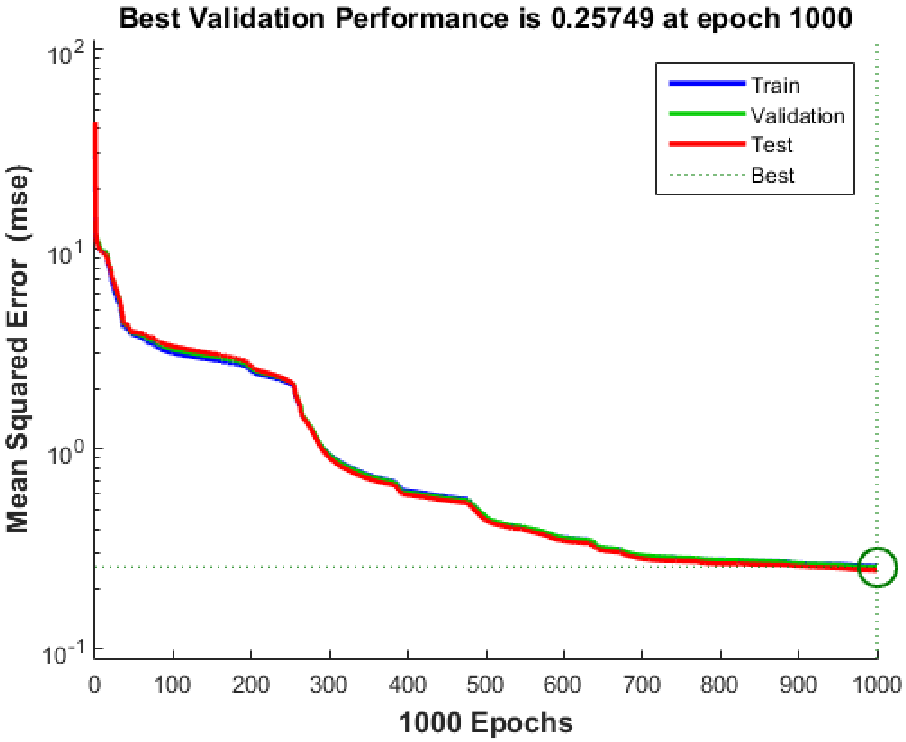


Figure 9.10: Overall performance of LRNN with 4 units.

shown in Figure 9.11 where a close prediction of the rotor angle response is achieved as well as an acceptably low MSE. Finally, preliminary results comparing the average MSE between unit estimates are shown in Figure 9.12 where the LRNN achieves significantly lower MSE and the mode-dependent estimate of 4 units performs best.

9.5 Conclusions and Future Work

Through experimental testing, this work tested a hypothesis that the number of dominant power system modes for a particular event can be equated to

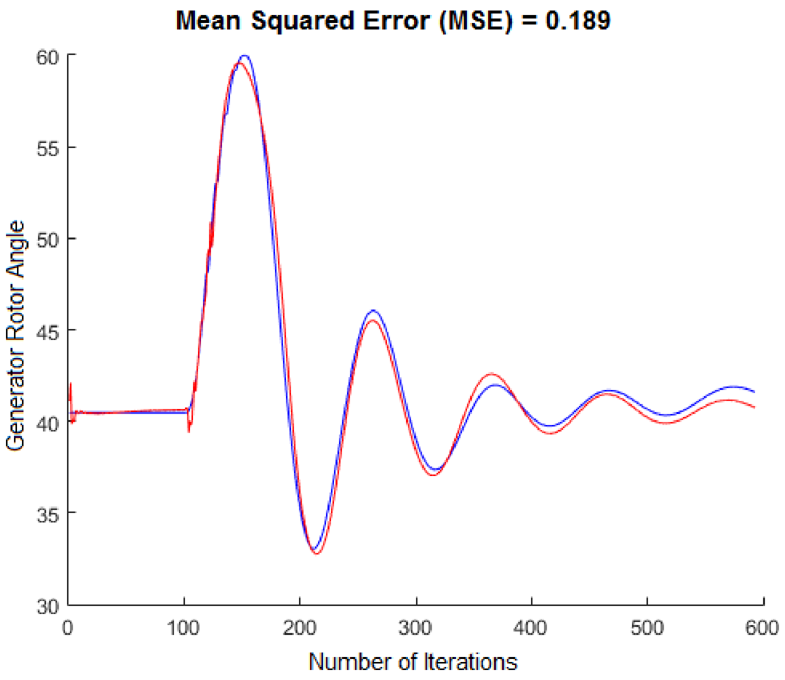


Figure 9.11: Comparison of true rotor angle response and LRNN prediction for 4 units.

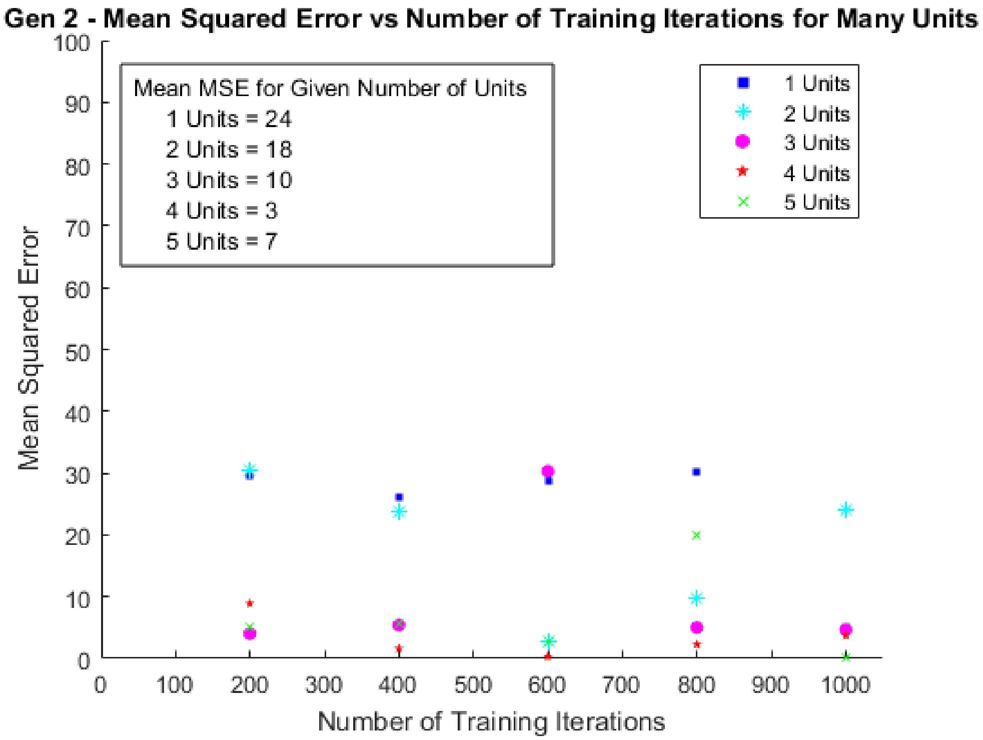


Figure 9.12: LRNN: Average MSE for different unit number estimates for faults at Generator #2 (at bus 7); the modal estimate is 4 units.

the number of units, or neurons, for construction of a neural network modeling the event and its characteristics. Our results indicate that the mode-dependent estimate of number of units provides promising performance, especially compared to known, generalized heuristics. We seek to develop systematic methods for power system neural network construction that leverages power system analyses and known behaviors. The generator control action classification based on localized voltage measurements, as presented previously in Chapter 8, demonstrated the benefit of incorporating power system knowledge. It also exemplifies the various machine learning algorithms that can be improved in this manner, not limited to support vector machine and neural networks.

This initial work can be extended to mathematically formulate the relationship between the neural network model and power system modes; future work can also explore different neural network architectures, increased data set size and input sources, and larger systems. In this manner, trial-and-error methods can be eliminated (which could lead to overfitting issues, excessive training time) and enable systematic, domain-dependent construction of effective artificial neural network models in power systems.

CHAPTER 10

CONCLUSION

This dissertation studies distributed controllers in the power system and their prominent function in the cohesive operation of the grid. These controller sets are used to achieve a variety of objectives, either individually or in a coordinated fashion, where a portion of or the entire set works together to achieve some goal. As such, the failure of one or a fraction of the device set can have widespread, detrimental impact on the remaining controllers and system. The rest of the set will struggle to maintain the overall goal, depending on the objective, and cascading effects can result. Furthermore, distributed controllers are vulnerable to cyber-physical compromise. Again, compromise within the set, single or multiple, will have broad impact. These compromised devices, under the control of an attacker, can be manipulated to drive the system to an unsafe state. From surpassing system limits to targeting sensitive equipment, the compromise of distributed controllers has serious consequences.

Distributed controllers are ubiquitous in the grid, yet they are susceptible to and prime targets for malicious compromise, as well as accidental failures. Proactive strategies must be developed to protect against these adverse incidents. Additionally, the existent vulnerabilities and risks need to be fully understood to best design these strategies. Several pertinent discussions, analyses, and methods are presented and developed in this dissertation to contribute to that effort.

10.1 Contributions

To protect against distributed controller compromise or failure, an analytic algorithm was developed that derives insight into the distributed controller set. With the controller role and grouping results, a control response framework was formulated to react immediately to compromise/failure using the remaining, “safe” controllers. The automatic response seeks to reduce system stress and mitigate compromise consequences, monitoring both system controllability and stability. The versatility of the analytic algorithm, which processes sensitivities using clustering and factorization techniques, is demonstrated with application to remedial action scheme (RAS) designs. In particular, an analytic corrective control selection algorithm was derived to identify the most effective controls, significantly reduce computation time, and therefore enable real-time RAS execution.

To further explore real-time applications, especially for control input verification in a cyber-adversarial environment, an augmented DC power flow algorithm was developed that used real-time measurements. The method achieved improvements in both speed and accuracy compared to existing linear algorithms. To aid detection of abnormal behavior and also leverage known power system behaviors, a generator control action classification method was designed using localized voltage measurements. Finally, to further explore enhancing machine learning algorithms with power system analyses and behavioral knowledge, neural networks were studied. Specifically, improved neural network construction was obtained using modal analysis to systematically select the number of neurons.

10.2 Extensions

The algorithms and techniques presented seek to aid in developing proactive strategies for distributed controllers, verification and classification of control actions, and enhance the use of data mining tools. Addressing and mitigating distributed controller compromise was the main focus of this dissertation. Specifically, system control, control actions, and control response were studied and incorporated into the methods.

A natural extension to this work, especially the overall control response framework presented in Chapter 5, is to integrate stability analysis. As mentioned previously, stability of the system must be prioritized and appropriate stability control strategies must be deployed to mitigate any detected stability. A simplistic stability assessment was presented using linear system stability concepts, but more rigorous analyses are warranted. Different categories and types of stability must be studied, as presented in Chapter 3. For example, the use of real-time metrics that estimate modes from PMU measurements could be applicable and suitable for a control response framework [157]. Subsequently, a stability criterion, such as requiring positive damping and above 3% damping ratio in the system, can be integrated and/or developed [158].

Trudnowski [159] presented a theoretical connection between the eigenvector properties of a system and measurable spectral properties. In particular, he described how the mode shape could be estimated using only system measurements. Although modal damping provides direct assessment of a mode's stability, the mode shape provides information on where the particular oscillation is most energetic [160]. Thus, it helps the control decision-making for mitigating a modal oscillation. Methods were proposed to achieve the application of this approach in near real-time [159].

Additionally, an interesting and related research direction would be to perform similar controller and support group analysis in terms of stability for a distributed controller set. Stability control is challenging and requires sophisticated solutions; perhaps insight into the device set can enhance strategies.

Lastly, improving power system machine learning applications by leveraging domain-specific analyses and known behaviors has promising results, as demonstrated by both the support vector machine and neural network studies. In particular, methods using power system knowledge (i.e., localized voltage impact, system modes) can be developed to enable systematic use of machine learning algorithms, specifically to enhance the "learning" component. Instead of relying on excessive training and very large data sets to construct effective models, the aim should be to incorporate power system analyses that already discover certain patterns. The combination of these patterns with the training would facilitate grounded, efficient, and more powerful machine learning applications in power systems.

10.3 Final Remarks

The power system is rapidly changing and is an amalgamation of various algorithms, components, and individuals. It is composed of cyber and physical layers that employ a variety of operational tools such as monitoring and control to enable a united implementation. Distributed controllers are pervasive in and pertinent to this execution, and as such, must maintain their objectives and integrity. The challenges to that commitment are inadvertent failures and increasing cyber-physical attacks that can compromise controllers. Resilient and dynamic defenses are needed that understand the vulnerabilities and risks present and respond quickly and effectively. This dissertation directly contributes to this effort by analytically gaining insight into the distributed controller set, employing those insights to respond to compromise or failure, and developing control action verification and classification techniques. The proactive strategies for responding to distributed controller compromise are a crucial part of protecting the power grid and just one piece of the puzzle for comprehensive system defense. The solution of this puzzle requires interdisciplinary and cyber-physical approaches from various perspectives and continuous validation and improvement. This dissertation is a part of that effort and helps realize a more resilient, efficient, and robust power grid.

REFERENCES

[1] S. Bennett, "A brief history of automatic control," *IEEE Control Systems Magazine*, vol. 16, no. 3, pp. 17–25, 1996.

[2] J. C. Maxwell, "On governors," *Proceedings of the Royal Society of London*, vol. 16, pp. 270–283, 1867.

[3] R. Bellman, "Dynamic programming and Lagrange multipliers," *Proceedings of the National Academy of Sciences*, vol. 42, no. 10, pp. 767–769, 1956.

[4] R. Kalman, "On the general theory of control systems," *IRE Transactions on Automatic Control*, vol. 4, no. 3, pp. 110–110, 1959.

[5] E. Hayden, M. Assante, and T. Conway, "An abbreviated history of automation & industrial controls systems and cybersecurity," *SANS analyst white papers*, 2014.

[6] G. S. Vassell, "The northeast blackout of 1965," *Public Utilities Fortnightly (United States)*, vol. 126, no. 8, 1990.

[7] G. W. Stagg, M. Adibi, M. Laughton, J. E. Van Ness, and A. J. Wood, "Thirty years of power industry computer applications," *IEEE Computer Applications in Power*, vol. 7, no. 2, pp. 43–49, 1994.

[8] M. Abrams and J. Weiss, "Malicious control system cyber security attack case study–Maroochy Water Services, Australia," McLean, VA: The MITRE Corporation, 2008.

[9] J. Slay and M. Miller, "Lessons learned from the Maroochy water breach," in *International Conference on Critical Infrastructure Protection.* Springer, 2007, pp. 73–82.

[10] K. R. Fall and W. R. Stevens, *TCP/IP Illustrated, Volume 1: The Protocols.* Addison-Wesley, 2011.

[11] C. C. Liu, A. Stefanov, J. Hong, and P. Panciatici, "Intruders in the grid," *IEEE Power and Energy Magazine*, vol. 10, no. 1, pp. 58–66, Jan. 2012.

[12] N. Falliere, L. O. Murchu, and E. Chien, "W32.Stuxnet dossier," Symantic Security Response, Tech. Rep., Oct. 2010.

[13] M. Assante, "Bad new world: Cyber risk and the future of our nation," September 2011. [Online]. Available: {http://www.csoonline.com/article/2129606/employee-protection/bad-new-world--cyber-risk-and-the-future-of-our-nation.html}

[14] EY's 19th Global Information Security Survey 2016-17, "Path to cyber resilience: Sense, resist, react," 2017. [Online]. Available: http://www.ey.com/gl/en/industries/power---utilities/ey-the-path-to-cyber-resilience-sense-resist-react

[15] M. Andreasson, D. V. Dimarogonas, H. Sandberg, and K. H. Johansson, "Distributed pi-control with applications to power systems frequency control," in *2014 American Control Conference*. IEEE, 2014, pp. 3183–3188.

[16] A. N. Venkat, I. A. Hiskens, J. B. Rawlings, and S. J. Wright, "Distributed MPC strategies with application to power system automatic generation control," *IEEE Transactions on Control Systems Technology*, vol. 16, no. 6, pp. 1192–1206, 2008.

[17] A. Atputharajah and T. K. Saha, "Power system blackouts-literature review," in *2009 International Conference on Industrial and Information Systems (ICIIS)*. IEEE, 2009, pp. 460–465.

[18] A. S. Debs, *Modern Power Systems Control and Operation*. Springer Science & Business Media, 2012.

[19] S. K. Khaitan, J. D. McCalley, and C. C. Liu, *Cyber Physical Systems Approach to Smart Electric Power Grid*. Springer, 2015.

[20] J. Zhang and A. D. Dominguez-Garcia, "On the failure of power system automatic generation control due to measurement noise," in *2014 IEEE PES General Meeting — Conference Exposition*, July 2014, pp. 1–5.

[21] M. Vrakopoulou, P. M. Esfahani, K. Margellos, J. Lygeros, and G. Andersson, "Cyber-attacks in the automatic generation control," in *Cyber Physical Systems Approach to Smart Electric Power Grid*. Springer, 2015, pp. 303–328.

[22] H. Lin, A. Slagell, Z. Kalbarczyk, P. W. Sauer, and R. K. Iyer, "Semantic security analysis of SCADA networks to detect malicious control commands in power grids," in *Proceedings of the First ACM Workshop on Smart Energy Grid Security*. ACM, 2013, pp. 29–34.

[23] S. Hossain, S. Etigowni, K. Davis, and S. Zonouz, "Towards cyber-physical intrusion tolerance," in *2015 IEEE International Conference on Smart Grid Communications (SmartGridComm)*. IEEE, 2015, pp. 139–144.

[24] E. A. Lee, "Cyber physical systems: Design challenges," in *2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC)*, May 2008, pp. 363–369.

[25] S. S. Sunder, M. Torngren, E. A. Lee, D. Broman, and P. Asare, "Cyber-physical systems," 2012, UC Regents. [Online]. Available: http://cyberphysicalsystems.org/

[26] R. R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, "Cyber-physical systems: the next computing revolution," in *Proceedings of the 47th Design Automation Conference*. ACM, 2010, pp. 731–736.

[27] W. Bolton, *Programmable Logic Controllers*. Newnes, 2015.

[28] S. Etigowni, S. Hossain-McKenzie, M. Kazerooni, K. Davis, and S. Zonouz, "Just-ahead-of-time controller recovery," *IEEE Transactions on Dependable and Secure Computing*, 2016 (Under Review).

[29] S. McLaughlin and S. Zonouz, "Controller-aware false data injection against programmable logic controllers," in *Smart Grid Communications (SmartGridComm), 2014 IEEE International Conference on*, Nov. 2014, pp. 848–853.

[30] M. Hong and C.-C. Liu, "Complete controllability of power system dynamics," in *Circuits and Systems, 2000. Proceedings. ISCAS 2000 Geneva. The 2000 IEEE International Symposium on*, vol. 4, 2000, pp. 241–244.

[31] B. Satchidanandan and P. Kumar, "Dynamic watermarking: Active defense of networked cyber-physical systems," *arXiv preprint arXiv:1606.08741*, 2016.

[32] T. Kailath, *Linear Systems*. Prentice-Hall Englewood Cliffs, NJ, 1980, vol. 156.

[33] A. Hamdan and A. Elabdalla, "Geometric measures of modal controllability and observability of power system models," *Electric Power Systems Research*, vol. 15, no. 2, pp. 147–155, 1988.

[34] A. Hamdan and A. Nayfeh, "Measures of modal controllability and observability for first-and second-order linear systems," *Journal of Guidance, Control, and Dynamics*, vol. 12, no. 3, pp. 421–428, 1989.

[35] M. Hong, C.-C. Liu, and M. Gibescu, "Complete controllability of an n-bus dynamic power system model," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 46, no. 6, pp. 700–713, June 1999.

[36] A. Messina and M. Nayebzadeh, "An efficient placement algorithm of multiple controllers for damping power system oscillations," in *Power Engineering Society Summer Meeting, 1999. IEEE*, vol. 2. IEEE, 1999, pp. 1280–1285.

[37] N. K. Sharma, A. Ghosh, and R. K. Varma, "A novel placement strategy for facts controllers," *IEEE Transactions on Power Delivery*, vol. 18, no. 3, pp. 982–987, 2003.

[38] F. Gubina and B. Strmcnik, "Voltage collapse proximity index determination using voltage phasors approach," *IEEE Transactions on Power Systems*, vol. 10, no. 2, pp. 788–794, 1995.

[39] H. C. Leung and T. S. Chung, "Optimal placement of FACTS controller in power system by a genetic-based algorithm," in *Power Electronics and Drive Systems, 1999. Proceedings of the IEEE 1999 International Conference on*, vol. 2, 1999, pp. 833–836.

[40] K. M. Rogers, R. Klump, H. Khurana, A. A. Aquino-Lugo, and T. J. Overbye, "An authenticated control framework for distributed voltage support on the smart grid," *IEEE Transactions on Smart Grid*, vol. 1, no. 1, pp. 40–47, 2010.

[41] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, "Catastrophic cascade of failures in interdependent networks," *Nature*, vol. 464, no. 7291, pp. 1025–1028, 2010.

[42] A. Berizzi, "The Italian 2003 blackout," in *IEEE Power Engineering Society General Meeting*, June 2004, pp. 1673–1679.

[43] B. Chen, K. Butler-Purry, and D. Kundur, "Impact analysis of transient stability due to cyber attack on FACTS devices," in *North American Power Symposium (NAPS), 2013*, Sept. 2013, pp. 1–6.

[44] Y. Xiang, Y. Zhang, L. Wang, and W. Sun, "Impact of UPFC on power system reliability considering its cyber vulnerability," in *T & D Conference and Exposition, 2014 IEEE PES*, April 2014, pp. 1–5.

[45] H. Gawand, A. Bhattacharjee, and K. Roy, "Control aware techniques for protection of industrial control system," in *India Conference (INDICON), 2014 Annual IEEE*, Dec. 2014, pp. 1–6.

[46] P. de Lima and G. Yen, “Accommodating controller malfunctions through fault tolerant control architecture,” *Aerospace and Electronic Systems, IEEE Transactions on*, vol. 43, no. 2, pp. 706–722, April 2007.

[47] K. R. Davis, K. L. Morrow, R. Bobba, and E. Heine, “Power flow cyber attacks and perturbation-based defense,” in *Smart Grid Communications (SmartGridComm), 2012 IEEE Third International Conference on*. IEEE, 2012, pp. 342–347.

[48] L. Xie, Y. Mo, and B. Sinopoli, “Integrity data attacks in power market operations,” *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 659–666, 2011.

[49] L. Jia, R. J. Thomas, and L. Tong, “Impacts of malicious data on real-time price of electricity market operations,” in *HICSS*, 2012, pp. 1907–1914.

[50] A. Teixeira, H. Sandberg, G. Dán, and K. H. Johansson, “Optimal power flow: Closing the loop over corrupted data,” in *2012 American Control Conference (ACC)*. IEEE, 2012, pp. 3534–3540.

[51] P. Srikantha and D. Kundur, “Denial of service attacks and mitigation for stability in cyber-enabled power grid,” in *2015 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, Feb. 2015, pp. 1–5.

[52] P. Kundur, J. Paserba, V. Ajjarapu, G. Andersson, A. Bose, C. Canizares, N. Hatziargyriou, D. Hill, A. Stankovic, C. Taylor et al., “Definition and classification of power system stability IEEE/CIGRE joint task force on stability terms and definitions,” *IEEE transactions on Power Systems*, vol. 19, no. 3, pp. 1387–1401, 2004.

[53] S. Amini, F. Pasqualetti, and H. Mohsenian-Rad, “Dynamic load altering attacks against power system stability: Attack models and protection schemes,” *IEEE Transactions on Smart Grid*, 2016.

[54] P. Antsaklis and A. Michel, *A Linear Systems Primer*. Birkhäuser Boston, 2007. [Online]. Available: https://books.google.com/books?id=WyWBPV6Cu9QC

[55] J. Wirfs-Brock, “The realities of cybersecurity at a rural utility,” *Inside Energy*, September 2015. [Online]. Available: http://grid.insideenergy.org/cybersecurity/

[56] R. M. Lee, M. J. Assante, and T. Conway, “Analysis of the cyber attack on the Ukrainian power grid,” *SANS Industrial Control Systems*, 2016.

[57] Y. Yuan, Q. Zhu, F. Sun, Q. Wang, and T. Basar, "Resilient control of cyber-physical systems against denial-of-service attacks," in *Resilient Control Systems (ISRCS), 2013 6th International Symposium on*, Aug 2013, pp. 54–59.

[58] J. P. Hespanha, *Linear Systems Theory.* Princeton University Press, 2009.

[59] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. J. Overbye, "Detecting false data injection attacks on dc state estimation," in *Preprints of the First Workshop on Secure Control Systems, CPSWEEK*, 2010.

[60] A. Gomez-Exposito and A. Abur, "Generalized observability analysis and measurement classification," *Power Systems, IEEE Transactions on*, vol. 13, no. 3, pp. 1090–1095, Aug 1998.

[61] O. Kosut, L. Jia, R. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *Smart Grid, IEEE Transactions on*, vol. 2, no. 4, pp. 645–658, Dec. 2011.

[62] M. Dahleh and I. Diaz-Bobillo, *Control of Uncertain Systems: A Linear Programming Approach.* Prentice Hall, 1995.

[63] SmartWireGrid, "Minnesota power deploys smart wires to optimize its grid and save customers money," September 2016, Online, SmartWires Incorporated. [Online]. Available: http://www.smartwires.com/category/press-release/

[64] D. Divan, "Improving power line utilization and performance with D-FACTS devices," in *Power Engineering Society General Meeting, 2005. IEEE.* IEEE, 2005, pp. 2419–2424.

[65] D. M. Divan, W. E. Brumsickle, R. S. Schneider, B. Kranz, R. W. Gascoigne, D. T. Bradshaw, M. R. Ingram, and I. S. Grant, "A distributed static series compensator system for realizing active power flow control on existing power lines," *IEEE Transactions on Power Delivery*, vol. 22, no. 1, pp. 642–649, Jan. 2007.

[66] H. Johal and D. Divan, "Design considerations for series-connected distributed FACTS converters," *IEEE Transactions on Industry Applications*, vol. 43, no. 6, pp. 1609–1618, Nov. 2007.

[67] K. M. Rogers and T. J. Overbye, "Power flow control with distributed flexible ac transmission system (D-FACTS) devices," in *41st North American Power Symposium*, Oct. 2009, pp. 1–6.

[68] K. Rogers, R. Klump, H. Khurana, and T. Overbye, “Smart-grid - enabled load and distributed generation as a reactive resource,” in *Innovative Smart Grid Technologies (ISGT), 2010*, Jan. 2010, pp. 1–8.

[69] J. A. Hartigan and M. A. Wong, “Algorithm as 136: A k-means clustering algorithm,” *Journal of the Royal Statistical Society. Series C (Applied Statistics)*, vol. 28, no. 1, pp. 100–108, 1979.

[70] H.-S. Park and C.-H. Jun, “A simple and fast algorithm for k-medoids clustering,” *Expert Systems with Applications*, vol. 36, no. 2, pp. 3336–3341, 2009.

[71] MathWorks, “Hierarchical Clustering,” 2015, http://www.mathworks.com/help/stats/hierarchical-clustering.html.

[72] M. T. Heath, *Scientific Computing.* McGraw-Hill, New York, 2002.

[73] J. M. Lim and C. L. DeMarco, “Model-free voltage stability assessments via singular value analysis of PMU data,” in *Bulk Power System Dynamics and Control - IX Optimization, Security and Control of the Emerging Power Grid (IREP), 2013 IREP Symposium*, Aug 2013, pp. 1–10.

[74] M. Gavish and D. Donoho, “The optimal hard threshold for singular values is $\frac{4}{\sqrt{3}}$,” *IEEE Transactions on Information Theory*, vol. 60, no. 8, pp. 5040–5053, Aug. 2014.

[75] G. Golub and W. Kahan, “Calculating the singular values and pseudo-inverse of a matrix,” *Journal of the Society for Industrial and Applied Mathematics Series B Numerical Analysis*, vol. 2, no. 2, pp. 205–224, 1965.

[76] P. J. Rousseeuw, “Silhouettes: A graphical aid to the interpretation and validation of cluster analysis,” *Journal of Computational and Applied Mathematics*, vol. 20, pp. 53–65, 1987.

[77] J. Chen and A. Abur, “Placement of PMUs to enable bad data detection in state estimation,” *Power Systems, IEEE Transactions on*, vol. 21, no. 4, pp. 1608–1615, Nov. 2006.

[78] G. Peters and J. H. Wilkinson, “The least squares problem and pseudo-inverses,” *The Computer Journal*, vol. 13, no. 3, pp. 309–316, 1970.

[79] PowerWorld Corporation, “Exercises for Students,” 2016, http://www.powerworld.com/solutions/excercises.

[80] “Electric power system resiliency: Challenges and opportunities,” Electric Power Research Institute (EPRI), Tech. Rep., Feb. 2016.

[81] A. B. Birchfield, T. Xu, K. M. Gegner, K. S. Shetye, and T. J. Overbye, "Grid structural characteristics as validation criteria for synthetic networks," *IEEE Transactions on Power Systems*, 2017 (to be published).

[82] "Texas 2000-June 2016," Online, Illinois Center for a Smarter Electric Grid (ICSEG). [Online]. Available: \url{http://icseg.iti.illinois.edu/synthetic-power-cases/texas2000-june2016/}

[83] PowerWorld Corporation, "D-FACTS Quick-Start Tutorial," 2016, http://www.powerworld.com/knowledge-base/d-facts-quick-start-tutorial.

[84] "PowerWorld Simulator," 2015, PowerWorld Corporation. [Online]. Available: http://www.powerworld.com/products/simulator/overview

[85] R. Fletcher and M. J. Powell, "A rapidly convergent descent method for minimization," *The computer journal*, vol. 6, no. 2, pp. 163–168, 1963.

[86] P. W. Sauer and M. Pai, *Power System Dynamics and Stability.* Stipes Publishing Co., 1998.

[87] *PowerWorld Simulator Help Manual*, PowerWorld Corporation, March. [Online]. Available: https://www.powerworld.com/WebHelp/

[88] North American Electric Reliability Corporation, "Proposed Definition of "Remedial Action Scheme"," *NERC Reliability Standards.* [Online]. Available: http://www.nerc.com/pa/Stand/Prjct201005_2SpclPrtctnSstmPhs2/Proposed%20RAS%20Definition_10262014_clean.pdf

[89] A. P. Meliopoulos and A. G. Bakirtzis, "Corrective control computations for large power systems," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-102, no. 11, pp. 3598–3604, Nov. 1983.

[90] P. M. Anderson and B. K. LeReverend, "Industry experience with special protection schemes," *IEEE Transactions on Power Systems*, vol. 11, no. 3, pp. 1166–1179, Aug. 1996.

[91] C. F. Henville and E. Struyke, "RAS and streched power system," *Western Protective Relaying Conference*, 2006.

[92] R. Ramanathan, B. Tuck, and J. O'Brien, "BPA's experience of implementing remedial action schemes in power flow for operation studies," in *2013 IEEE Power Energy Society General Meeting*, July 2013.

[93] S. C. Pai and J. Sun, "BCTCs experience towards a smarter grid—increasing limits and reliability with centralized intelligence remedial action schemes," in *Electric Power Conference, 2008. IEEE Canada*, Oct. 2008, pp. 1–7.

[94] A. A. Fouad, A. Ghafurian, K. Nodehi, and Y. Mansour, "Calculation of generation-shedding requirements of the B.C. hydro system using transient energy functions," *IEEE Power Engineering Review*, vol. PER-6, no. 5, pp. 31–32, May 1986.

[95] Y. Zhang and K. Tomsovic, "Adaptive remedial action scheme based on transient energy analysis," in *Power Systems Conference and Exposition, 2004.* IEEE, 2004, pp. 925–931.

[96] W. Shao and V. Vittal, "Corrective switching algorithm for relieving overloads and voltage violations," *IEEE Transactions on Power Systems*, vol. 20, no. 4, pp. 1877–1885, 2005.

[97] S. Wang and G. Rodriguez, "Smart RAS (remedial action scheme)," in *2010 Innovative Smart Grid Technologies (ISGT)*, Jan. 2010, pp. 1–6.

[98] H. Atighechi, P. Hu, J. Lu, G. Wang, and S. Ebrahimi, "A fast load shedding remedial action scheme using real-time data for BC hydro system," in *2016 IEEE Power and Energy Society General Meeting (PESGM)*, July 2016, pp. 1–5.

[99] L. Hitachi America, "Introduction to online RAS (remedial action scheme)," April 2016. [Online]. Available: \url{https://www.wecc.biz/Administrative/RAS%20Arming%20-%20Hitachi%20America.pdf}

[100] M. Kazerooni, "Enhanced power system resiliency to high-impact, low-frequency events with emphasis on geomagnetic disturbances," Ph.D. dissertation, University of Illinois at Urbana-Champaign, 2016.

[101] Energy Information Administration (EIA), "Electric generator dispatch depends on system demand and the relative cost of operation," 2012.

[102] H. Song, B. Lee, and V. Ajjarapu, "Control strategies against voltage collapse considering undesired relay operations," *IET Generation, Transmission & Distribution*, vol. 3, no. 2, pp. 164–172, 2009.

[103] I. Genc, R. Diao, V. Vittal, S. Kolluri, and S. Mandal, "Decision tree-based preventive and corrective control applications for dynamic security enhancement in power systems," *IEEE Transactions on Power Systems*, vol. 25, no. 3, pp. 1611–1619, Aug. 2010.

[104] D. Ruiz-Vega and M. Pavella, “A comprehensive approach to transient stability control. ii. Open loop emergency control,” *IEEE Transactions on Power Systems*, vol. 18, no. 4, pp. 1454–1460, Nov. 2003.

[105] M. J. Assante, “Confirmation of a coordinated attack on the Ukrainian power grid,” *SANS Industrial Control Systems*, January 2016. [Online]. Available: ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid

[106] “D-FACTS devices in PowerWorld simulator.” [Online]. Available: \url{http://www.powerworld.com/files/clientconf2014/07Weber_DFACTS.pdf}

[107] M. Dahleh and I. Diaz-Bobillo, *Control of Uncertain Systems: A Linear Programming Approach.* Prentice Hall, 1995.

[108] Information Trust Institute, “IEEE 24-Bus System,” University of Illinois at Urbana-Champaign. [Online]. Available: \url{http://icseg.iti.illinois.edu/ieee-24-bus-system/}

[109] G. Hug-Glanzmann and G. Andersson, “Decentralized optimal power flow control for overlapping areas in power systems,” *IEEE Transactions on Power Systems*, vol. 24, no. 1, pp. 327–336, 2009.

[110] W. F. Tinney and C. Hart, “Power flow solution by newton’s method,” *Power Apparatus and Systems, IEEE Transactions on*, vol. PAS-86, no. 11, pp. 1449–1460, Nov 1967.

[111] D. Van Hertem, J. Verboomen, K. Purchala, R. Belmans, and W. Kling, “Usefulness of DC power flow for active power flow analysis with flow controlling devices,” in *AC and DC Power Transmission, 2006. ACDC 2006. The 8th IEE International Conference on*, March 2006, pp. 58–62.

[112] B. Stott, J. Jardim, and O. Alsac, “DC power flow revisited,” *Power Systems, IEEE Transactions on*, vol. 24, no. 3, pp. 1290–1300, Aug 2009.

[113] B. Stott and O. Alsac, “Fast decoupled load flow,” *Power Apparatus and Systems, IEEE Transactions on*, vol. PAS-93, no. 3, pp. 859–869, May 1974.

[114] T. J. Overbye, “Power system analysis, lecture 14: Power flow,” October 2011. [Online]. Available: https://courses.engr.illinois.edu/ece476

[115] S. Lu, N. Zhou, N. Kumar, N. Samaan, and B. Chakrabarti, "Improved DC power flow method based on empirical knowledge of the system," in *Transmission and Distribution Conference and Exposition, 2010 IEEE PES*, April 2010, pp. 1–6.

[116] J. Glover, M. Sarma, and T. Overbye, *Power System Analysis and Design.* Cengage Learning, 2011.

[117] T. Overbye and R. Baldick, "EE 369, Power system analysis, lecture 12: Newton-Raphson power flow," University of Texas at Austin. [Online]. Available: http://users.ece.utexas.edu

[118] S. Kim and T. Overbye, "Hybrid power flow analysis: Combination of AC and DC models," in *Power and Energy Conference at Illinois (PECI), 2011 IEEE*, Feb. 2011, pp. 1–4.

[119] A. Phadke, "Synchronized phasor measurements in power systems," *Computer Applications in Power, IEEE*, vol. 6, no. 2, pp. 10–15, April 1993.

[120] B. Xu and A. Abur, "Observability analysis and measurement placement for systems with PMUs," in *Power Systems Conference and Exposition, 2004. IEEE PES*, vol. 2, Oct. 2004, pp. 943–946.

[121] L. De Moura and N. Bjørner, "Z3: An efficient SMT solver," in *Proceedings of the Theory and Practice of Software, 14th International Conference on Tools and Algorithms for the Construction and Analysis of Systems*, ser. TACAS'08/ETAPS'08. Berlin, Heidelberg: Springer-Verlag, 2008. [Online]. Available: http://dl.acm.org/citation.cfm?id=1792734.1792766 pp. 337–340.

[122] M. B. Cain, R. P. O'Neill, and A. Castillo, "History of optimal power flow and formulations," *FERC*, 2012.

[123] S. McLaughlin, S. Zonouz, D. Pohly, and P. McDaniel, "A trusted safety verifier for process controller code," *Networks and Distributed Systems Symposium (NDSS)*, 2014.

[124] M. Kezunovic, L. Xie, and S. Grijalva, "The role of big data in improving power system operation and protection," in *2013 IREP Symposium Bulk Power System Dynamics and Control - IX Optimization, Security and Control of the Emerging Power Grid*, Aug. 2013, pp. 1–9.

[125] E. Styvaktakis, M. Bollen, and I. Gu, "Classification of power system events: voltage dips," in *Harmonics and Quality of Power, 2000. Proceedings. Ninth International Conference on*, vol. 2, 2000, pp. 745–750.

[126] P. Alluri, S. Solanki, J. Solanki, and T. Menzies, "Power system state recognition using data mining algorithms," in *North American Power Symposium (NAPS), 2013*, Sept. 2013, pp. 1–6.

[127] M. Kazerooni, H. Zhu, and T. J. Overbye, "Dynamic modeling and filtering in geomagnetically induced current validation," in *North American Power Symposium (NAPS)*, Sept. 2014.

[128] O. Ipinnimo and S. Chowdhury, "ANN-based classification system for different windows of voltage dips in a power network," in *Power Engineering Conference (UPEC), 2013 48th International Universities'*, Sept. 2013, pp. 1–6.

[129] H. Li, D. Wang, G. Hu, J. Chen, and L. Zhao, "A method to recognize transient voltage disturbance in power system," in *Power Electronics and Motion Control Conference (IPEMC), 2012 7th International*, vol. 2, June 2012, pp. 1464–1468.

[130] K. Seethalekshmi, S. Singh, and S. Srivastava, "A classification approach using support vector machines to prevent distance relay maloperation under power swing and voltage instability," *Power Delivery, IEEE Transactions on*, vol. 27, no. 3, pp. 1124–1133, July 2012.

[131] K. Seethalekshmi, "SVM based power swing identification scheme for distance relays," in *Power and Energy Society General Meeting, 2010 IEEE*, July 2010, pp. 1–8.

[132] U. Parikh, B. Das, and R. Maheshwari, "Combined wavelet-SVM technique for fault zone detection in a series compensated transmission line," *Power Delivery, IEEE Transactions on*, vol. 23, no. 4, pp. 1789–1794, Oct. 2008.

[133] A. Megahed, A. Monem Moussa, and A. Bayoumy, "Usage of wavelet transform in the protection of series-compensated transmission lines," *Power Delivery, IEEE Transactions on*, vol. 21, no. 3, pp. 1213–1221, July 2006.

[134] C.-C. Chang and C.-J. Lin, "A practical guide to support vector classification," National Taiwan University, Tech. Rep., April 2010.

[135] C. Cortes and V. Vapnik, "Support-vector networks," *Mach. Learn.*, vol. 20, no. 3, pp. 273–297, Sept. 1995. [Online]. Available: http://dx.doi.org/10.1023/A:1022627411411

[136] C.-C. Chang and C.-J. Lin, "LIBSVM: A library for support vector machines," *ACM Transactions on Intelligent Systems and Technology*, vol. 2, pp. 27:1–27:27, 2011, software available at http://www.csie.ntu.edu.tw/~cjlin/libsvm.

[137] H. S. Hippert, C. E. Pedreira, and R. C. Souza, “Neural networks for short-term load forecasting: a review and evaluation,” *IEEE Transactions on Power Systems*, vol. 16, no. 1, pp. 44–55, Feb. 2001.

[138] A. Bahbah and A. Girgis, “New method for generators’ angles and angular velocities prediction for transient stability assessment of multimachine power systems using recurrent artificial neural network,” in *IEEE Power Engineering Society General Meeting*, vol. 1, June 2004.

[139] E. M. Voumvoulakis, A. E. Gavoyiannis, and N. D. Hatziargyriou, “Application of machine learning on power system dynamic security assessment,” in *2007 International Conference on Intelligent Systems Applications to Power Systems*, Nov 2007, pp. 1–6.

[140] R. Aggarwal and Y. Song, “Artificial neural networks in power systems. iii. examples of applications in power systems,” *Power Engineering Journal*, vol. 12, no. 6, pp. 279–287, Dec. 1998.

[141] M. A. Nielsen, *Neural Networks and Deep Learning.* Determination Press, 2015.

[142] M. Caudill, “Neural networks primer, part i,” *AI Expert*, vol. 2, no. 12, pp. 46–52, Dec. 1987. [Online]. Available: http://dl.acm.org/citation.cfm?id=38292.38295

[143] T. Xu, B. Venkatesh, C. Opathella, and B. N. Singh, “Artificial neural network model of photovoltaic generator for power flow analysis in PSS SINCAL,” *IET Generation, Transmission Distribution*, vol. 8, no. 7, pp. 1346–1353, 2014.

[144] A. Qian, S. Shande, and Z. Shouzhen, “Transient stability study using artificial neural networks models of generator, excitation system, governor,” in *Power System Technology, 1998. Proceedings. 1998 International Conference on*, vol. 2, Aug. 1998, pp. 1331–1335.

[145] G. Rogers, *Modal Analysis of Power Systems.* Boston, MA: Springer US, 2000, pp. 31–73. [Online]. Available: http://dx.doi.org/10.1007/978-1-4615-4561-3_3

[146] D. P. Kothari, “Application of neural networks to power systems,” in *Proceedings of IEEE International Conference on Industrial Technology 2000 (IEEE Cat. No.00TH8482)*, Jan. 2000, pp. 621–626.

[147] L. Thomas, M. Kumar, and B. Annappa, “Discovery of optimal neurons and hidden layers in feed-forward neural network,” in *2016 IEEE International Conference on Emerging Technologies and Innovative Business Practices for the Transformation of Societies (EmergiTech)*, Aug 2016, pp. 286–291.

[148] K. G. Sheela and S. N. Deepa, "Review on methods to fix number of hidden neurons in neural networks," *Mathematical Problems in Engineering*, 2013.

[149] M. D. Blechner, "Behavior of various machine learning models in the face of noisy data," Harvard-MIT Division of Health Sciences and Technology, Final Project, Tech. Rep., 2005.

[150] J. Hauer, "Application of prony analysis to the determination of modal content and equivalent models for measured power system response," *IEEE Transactions on Power Systems*, vol. 6, no. 3, pp. 1062–1068, 1991.

[151] P. Kundur, N. J. Balu, and M. G. Lauby, *Power System Stability and Control*. McGraw-Hill, New York, 1994.

[152] J. F. Hauer, C. Demeure, and L. Scharf, "Initial results in prony analysis of power system response signals," *IEEE Transactions on Power Systems*, vol. 5, no. 1, pp. 80–89, 1990.

[153] A. Cagnano, E. D. Tuglie, and F. Torelli, "Estimation of power system dominant modes," in *2009 IEEE Bucharest PowerTech*, June 2009, pp. 1–7.

[154] L. Ding, A. Xue, F. Han, J. Li, M. Wang, T. Bi, and J. Wang, "Dominant mode identification for low frequency oscillations of power systems based on prony algorithm," in *2010 5th International Conference on Critical Infrastructure (CRIS)*, Sept. 2010, pp. 1–6.

[155] H. T. Siegelmann, B. G. Horne, and C. L. Giles, "Computational capabilities of recurrent NARX neural networks," *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, vol. 27, no. 2, pp. 208–215, 1997.

[156] "Matlab," 2015, MathWorks. [Online]. Available: http://www.mathworks.com/products/matlab/

[157] Task Force on Identification of Electromechanical Modes, "Identification of electromechanical modes in power systems," IEEE Power and Energy Society, Tech. Rep., June 2012.

[158] *Establishing System Operating Limits for the Operations Horizon*, 6th ed., California ISO, April 2017, operating procedure.

[159] D. J. Trudnowski, "Estimating electromechanical mode shape from synchrophasor measurements," *IEEE Transactions on Power Systems*, vol. 3, no. 23, pp. 1188–1195, 2008.

[160] L. Dosiek, N. Zhou, J. W. Pierre, Z. Huang, and D. J. Trudnowski, "Mode shape estimation algorithms under ambient conditions: A comparative review," *IEEE Transactions on Power Systems*, vol. 28, no. 2, pp. 779–787, 2013.

APPENDIX A

IEEE 118-BUS SYSTEM CONTROL SUPPORT GROUPS

Figure A.1 is a one-line diagram of the IEEE 118-bus system with lines colored according to cluster group. Each cluster represents a control support group; black lines indicate no support group and that the line/device is independently controlled.

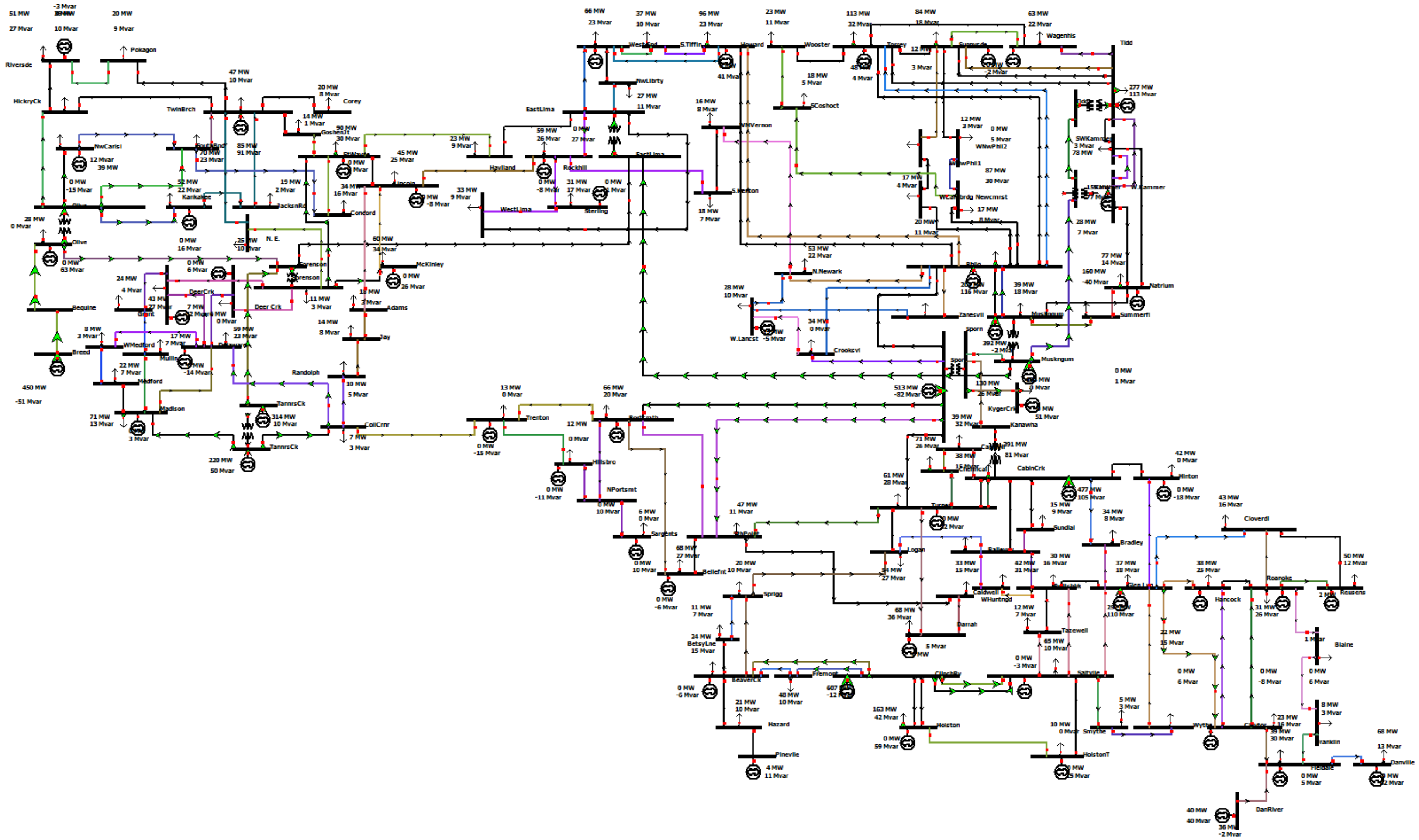


Figure A.1: One-line diagram of the IEEE 118-bus system with lines colored according to cluster group.