Risk Assessment of Power System Catastrophic Failures and Hidden Failure Monitoring & Control System

Qun Qiu

Dissertation submitted to the Faculty of the

Virginia Polytechnic Institute and State University

in partial fulfillment of the requirements for the degree of

Doctor of Philosophy
In
Electrical Engineering

Lamine M. Mili, Chair
Arun G. Phadke
Jaime De La Ree
William H. Tranter
Joel A. Nachlas

December 2003
Blacksburg, Virginia

Keywords: Power System, Catastrophic Failures, Power System Protection, Hidden Failures, Risk Assessment, Dynamic Event Tree, Production Simulation, Hidden Failure Monitoring, Hidden Failure Control, Adaptive Dependability/Security Protection, Misoperation Tracking Database

Risk Assessment of Power System Catastrophic Failures and a Hidden Failure Monitoring & Control System

Qun Qiu

Abstract

One of the objectives of this study is to develop a methodology, together with a set of software programs that evaluate, in a power system, the risks of catastrophic failures caused by hidden failures in the hardware or software components of the protection system.

The disturbance propagation mechanism is revealed by the analysis of the 1977 New York Blackout. The step-by-step process of estimating the relay hidden failure probability is presented. A Dynamic Event Tree for the risk-based analysis of system catastrophic failures is proposed. A reduced 179-bus WSCC sample system is studied and the simulation results obtained from California sub-system are analyzed. System weak links are identified in the case study. The issues relating to the load and generation uncertainties for the risk assessment of system vulnerabilities are addressed.

A prototype system—the Hidden Failure Monitoring and Control System (HFMCS)—is proposed to mitigate the risk of power system catastrophic failures. Three main functional modules—*Hidden Failure Monitoring, Hidden Failure Control* and *Misoperation Tracking Database*—and their designs are presented. Hidden Failure Monitoring provides the basis that allows further control actions to be initiated. Hidden Failure Control is realized by using Adaptive Dependability/Security Protection, which can effectively stop possible relay involvement from triggering or propagating disturbance under stressed system conditions.

As an integrated part of the HFMCS, a Misoperation Tracking Database is proposed to track the performance of automatic station equipment, hence providing automatic management of misoperation records for hidden failure analysis.

Acknowledgments

In the past four years, I have gained a true appreciation for the effort involved in research and the compromises many researchers make in their lives to bring about positive change. My committee, family, friends, and coworkers have all contributed in meaningful ways to getting my goals accomplished.

I am grateful to my advisor, Dr. Lamine M. Mili, not only for his valuable guidance and advices, but also for providing me with inspiration and support throughout one of the most difficult challenges of my life.

I want to acknowledge my committee members, Dr. Arun G. Phadke, Dr. Jaime De La Ree, Dr. William H. Tranter, and Dr. Joel A. Nachlas, for generously contributing time and technical advice in the completion of this work. Without their contributions, my graduate degree would not have been a success.

I would like to express my gratitude to Dr. Yilu Liu for her help during the past four years. Special thanks also go to Carolyn Guynn and Glenda Caldwell of the Center for Power Engineering for their continuous support.

My sincere appreciation to Mike Higgins and Daniel Recker for providing me the working opportunities in the protection and control area. I also want to thank Terrence Liptak, Charles Jones, Robert Albanese, Henry Miller, John Burger, and Carson Taylor for their valuable discussions on various aspects of protection and control, substation automation/integration and Human Machine Interface.

Many other friends have been supportive as well. My thanks to my power lab fellows for their support and friendship over the past four years.

I thank my parents for providing me with numerous opportunities and continuous support throughout my life. I would also like to thank my parents-in-law, my sister, and my brothers for sharing my joy and sadness throughout this grueling process.

Not to be forgotten are my wife, Wei Sun, and my son, Jiajia, for the long lonely nights they spent while I was busy with this research. Without your love and support, this degree would not have been possible.

Acknowledgments

Finally, I would like to acknowledge the support of U.S. Department of Defense (DoD) and Electric Power Research Institute (EPRI) through the Complex Interactive Networks/Systems Initiative, WO 8333-01 for this research work.

For my wife: Wei

my son: Jiajia

We cannot stop a disaster from striking, but we can certainly help minimize its impact, improve response, and speed the recovery process.

■ Karl Stahlkopf, *vice president, EPRI, 2000*

Table of Contents

List of Figures

List of Tables

List of Acronyms and Symbols

ACM – Alarm Control Module
ADSP – Adaptive Dependability/Security Protection
AEP American Electric Power
BPA – Bonneville Power Administration
CB – Circuit Breaker
CC – Carrier Current
CMC – Centralized Monitoring/Control
CT – Current Transformer
DAS – Data Acquisition System
DC – Direct Current
DCB – Directional Comparison Blocking
DCUB – Directional Un-Blocking Scheme
DET – Dynamic Event Tree
DFR – Digital Fault Recorder
DMC – Distributed Monitoring/Control
DMS – Distributed Monitoring System
DoD – U.S. Department of Defense
DOE – U.S. Department of Energy
DTT – Direct Transfer Trip
DAWG – Disturbance Analysis Working Group
EEI – Edison Electric Institute
EHV – Extra High Voltage
EMI – Electromagnetic Interference
EMS – Energy Management System
EPRI – Electric Power Research Institute
ET – Event Tree
ETMSP – Extended Transient Midterm Stability Program
FERC –Federal Energy Regulatory Commission
GE – General Electric Company
GPS – Global Position System
GTOC – Ground Time Over-Current relay
HF – Hidden Failure
HFC – Hidden Failure Control
HFM – Hidden Failure Monitoring
HFMCS – Hidden Failure Monitoring and Control System
HMI – Human Machine Interface
IDS – Intrusion Detection Systems
IEEE – Institute of Electrical and Electronics Engineers
IED – Intelligent Electronic Device
ISO – Independent System Operator
IT – Information Technology
LAN – Local Area Network
LOP – Loss of Power

MA – Maintenance Action
MTD – Misoperation Tracking Database
MTTF – Mean Time To Failure
NERC – North American Electric Reliability Council
OA – Operating Action
P&C – Protection and Control
PLC – Programmable Logic Controller
PMU – Phasor Measurement Unit
PMRM – Partitioning Multi-objective Risk Method
POTT – Permissive Overreaching Transfer Trip
PSRC – Power System Relay Committee
PUTT – Permissive Under-Reach Transfer Trip Scheme
PT – Potential Transformer
RCC – Regional Control Centers
RFI – Radio Frequency Interference
RTU – Remote Terminal Unit
RWG – Relay Working Group
SCADA – Supervisory Control and Data Acquisition
SCC – System Control Center
SEL – Schweitzer Engineering Laboratories, Inc.
SF – System Failure
SOC – Self-Organized Criticality
SONET – Synchronous Optical Network
SPID – Strategy Power Infrastructure Defense
TSIN – Transmission Services Information Networks
TT – Transfer Trip
UCA – Utility Communications Architecture
UR – Universal Relay
WAN – Wide Area Network
WSCC – Western Systems Coordinating Council

P_{Bi} – Probability that a circuit breaker of the faulty line i does not open in time

P_{Ri} – Probability that the circuit breakers of the faulty line i do not reclose following a temporary fault

P_{HPi} – Probability of system failure due to relay hidden failure given the occurrence of a permanent fault

P_{HTNi} – Probability of system failure due to relay hidden failure given the occurrence of a temporary fault and the non-reclosing of the faulty line

P_{HTRi} – Probability of system failure due to relay hidden failure given the occurrence of a temporary fault and the successful reclosing of the faulty line

P_{LPi} – Probability of system failure due to line overloads given the occurrence of a permanent fault

P_{LTNi} – Probability of system failure due to line overloads given the occurrence of a temporary fault and the non-reclosing of the faulty line

P_{LTRi} – Probability of system failure due to line overloads given the occurrence of a temporary fault and the reclosing of the faulty line

Chapter 1 Introduction

1.1 Motivation of the Study

1.1.1 The Power System as a Critical Infrastructure

Critical infrastructures are defined as “those physical and cyber-based systems essential to the minimum operations of the economy and government.” [1] They are regarded as the backbone of the economy of both developed and developing countries throughout the world since they provide the crucial support for the delivery of basic services to almost all segments of a society.

As one of the nation’s most complex, large-scale networked systems, electric power has become increasingly automated in the past three decades due to technological advances. On the other hand, these same advances have created new vulnerabilities to equipment failures, human errors, weather and other natural causes, and physical and cyber attacks. The ever-increasing system scale and the strong reliance on automatic devices may turn a local disturbance into a large-scale failure via cascading events. This kind of wide-area failure may have a catastrophic impact on the whole society. Unfortunately, the risk of such a disastrous domino effect is growing in the U.S. because of the current trend to operate power systems closer to their stability or capacity limits. One compelling reason for this practice is, of course, economics. Providing power systems with some degree of robustness comes at a price, which is entailed by the required level of redundancy in the equipment that needs to be achieved. This is all the more true since the expansion of electric transmission systems does not keep pace with the rapid growth of the demand.

The importance of protecting our critical infrastructures, such as the power system, and strengthening our emergency response capabilities is clearly addressed in the Presidential Decision Directive 63 [1] issued by the Clinton administration in 1998. The Presidential Commission on Critical Infrastructure Protection, which was established in July 1996, called for the development of a coordinated national response to threats against critical infrastructures, based on an analysis of their vulnerabilities. Addressing these vulnerabilities will necessarily require evolutionary approaches that protect this critical infrastructure so that it can function properly and continuously.

1.1.2 Purpose of the Study

The challenge to the security, robustness, reliability, and efficiency of large-scale networks becomes an important issue for network planners and operators, who must identify and develop appropriate and effective means in advance to protect critical civilian infrastructures such as the electric power grid. Major blackouts are rare events, but their impact can be catastrophic. Highly reliable electricity supply systems are vital to national security, the well-being of our economy, and the quality of life in an era marked by increasing technological sophistication.

In order to maintain system reliability while responding to the growing demand for transmission service in an open, volatile electricity marketplace, there exists urgent need to construct new transmission lines and/or upgrade existing transmission facilities; however, the environmental restrictions and huge upfront capital costs limit this clear-cut solution. Power system operation has entered a more competitive economic era with a smaller stability margin, and is approaching levels beyond which the system is vulnerable to costly impacts resulting from possible outage events. Reliability and competition in the electricity industry can be compatible, but this result will not be achieved automatically.

Disturbances to the electric power system are presented all the time, but they are not of equal likelihood, or of equal impact. Large disturbances, such as blackouts, that are unlikely to occur, but would have dire consequences if they did, tend to be of more interest to power system engineers, and deregulation is pressing for more comprehensive and accurate risk assessment tools.

The investigations of major blackouts (briefly introduced in Section 2.3.2) and the analysis of NERC (North American Electric Reliability Council) disturbance reports [2] show that multiple contingencies leading to catastrophic failure may not be quite as improbable as one would expect if we take into account the possible relay *hidden failures*[1] [3] exposed to the initial trigger event. The effect of relay hidden failures is particularly significant for high-order contingencies, since the likelihood can be increased by several orders of magnitude, and is considerably greater than that for similar contingencies caused by independent overlapping outages.

The time has come to direct our attention to managing the risk that comes from the market-driven operation. The key to the success of deregulation is to integrate risk-based assessment into power system planning and operation in such an environment.

To understand such risks, we must weigh the risk against the potential for economic benefit. In response to many of these issues, the Electric Power Research Institute (EPRI) and the U.S. Department of Defense (DoD) have sponsored a joint 3-year, $30 million research program, "The Complex Interactive Networks/Systems Initiative (CIN/SI)," since 1999. With the objective of addressing the key technologies needed to build a robust power delivery infrastructure, the initiative aims to "significantly and strategically advance the robustness, reliability, and efficiency of the interdependent energy, communications, financial, and transportation infrastructures … to develop new tools and techniques that will enable large national infrastructures to self-heal in response to threats, material failures, and other destabilizers. Of particular interest is how to model enterprises at the appropriate level of complexity in critical infrastructure systems." [4]

The growing concern about wide-area power system disturbances and their impact on power systems has reinforced interest in a new generation of system protection tools. This dissertation is part of that research effort, aiming to devise a systematic method for the analysis of system failures, as well as a prototype system capable of mitigating the risk of wide-area disturbance and future full-scale applications.

---

[1] *A hidden failure is defined as "a permanent defect that will cause a relay or relay system to incorrectly and inappropriately REMOVE a circuit element(s) as a direct consequence of another switching event." [5] All the analysis of hidden failures for different relay schemes in the study is based on this definition.*

1.2 Differences between the Proposed Study and Related Research

In recent years, there has been considerable interest in risk assessment applications in power systems. Most of these studies focus on operating limits for system components, such as transformers or the thermal limit of transmission lines. For example, in the research conducted at Iowa State University, efforts have been placed on the analysis of expected operating costs in stressed conditions suffered by power system facilities under a reasonable likely scenario. J.D. McCalley et al. proposed a composite risk as a function of operating conditions [6]. The composite risk takes into account the risks of transformer loading capability [7], the overload limit of transmission lines, voltage collapse, voltage out-of-limit, and transient instability. The probabilistic nature of time-varying loads and ambient temperature is also included in identifying component (e.g. transformer, transmission line) risks associated with operating limits.

Additional research by Drs. Dai & McCalley [8] first proposed a method to identify the power system trajectory over a studied period with appropriate balancing of the model complexity and accuracy with computation efforts, and then focused on developing a framework to calculate cumulative risk for one year based on the predicted trajectory. Both the adequacy and security were considered to get the composite risk index; however, their research was confined to only thermal overload risk assessment and power flow infeasibility risk assessment; the risk due to simultaneous outage of multiple components was not addressed.

Other similar research efforts reported by Thorp's group at Cornell University applied Importance Sampling techniques to the simulation of cascading events leading to system blackout [10][11]. The major disadvantage of Importance Sampling is that it has to simulate each sequence of events many times in order to estimate its probability. A more recent effort by Wang and Thorp is the development of a random search algorithm based on power system heuristics for faster search of important blackout paths [12]. However, the computation cost is still very high; for example, the simulation had to be run on a 256-processor Intel cluster for a NYPP 3000-bus system. Such high-cost computation cannot be justified for utilities. Moreover, the simulation was based on a preset operating point, and load and generation uncertainties were not addressed in the simulation.

It is difficult to identify one dynamic methodology as clearly superior to the rest. Each methodology has advantages and disadvantages depending on the system under consideration and the objectives of the study; however, they all suffer from computational limitations on system size. Therefore, some system size reduction technique is usually used in conjunction with these methods.

This dissertation focuses on the risk assessment of catastrophic failures due to relay hidden failures and corrective actions to prevent the propagation of cascading outages. In exploring the mechanism of propagation, a Dynamic Event Tree approach is proposed. A Hidden Failure Monitoring and Control System (HFMCS), including Misoperation Tracking Database, is developed. Under the framework of risk assessment, the following issues were investigated:

- *How can hidden failures in protection and control systems lead to catastrophic failures?*
    - *How can the probability of relay hidden failures be evaluated?*
    - *How can hidden failures contribute to system vulnerability?*
    - *What is the mechanism of catastrophic failure?*
- *What is the framework for global system vulnerability assessment?*
    - *Why risk assessment instead of reliability evaluation?*
    - *How to evaluate the probability of catastrophic failure? (Event and fault tree for large-scale systems)*
    - *How to identify the system weak link? (risk index)*
    - *How to incorporate the uncertainties of load-generation profile in the risk assessment framework? (production simulation)*
- *How to strengthen the weak link?*
    - *How to monitor and control relay hidden failures? (Architecture of the HFMCS)*

- *How to allow protective devices adapting to changing system conditions by using intelligent adaptive protection and control techniques*
- *How to implement a Misoperation Tracking Database?*

1.3 Contributions of the Dissertation

The following key contributions have been made by answering the above questions.

Mechanism of catastrophic failure in power system

By analyzing the 1977 New York Blackout, we exhibit how relay hidden failures can contribute to system vulnerability: These relay misoperations exacerbate the stressed conditions of the power network, and may in turn cause more lines overloaded and tripped. This sequence of events finally led to the 1977 New York Blackout, the 1996 WSCC (Western Systems Coordinating Council) Blackout, and other power system catastrophic failures. Based on the analysis, the disturbance propagation mechanism is revealed, and it projects an efficient means to evaluate the risk of power system catastrophic failures.

Risk assessment framework to identify system weak link

As part of the effort to set up the risk assessment framework, a statistical analysis of disturbance reports based on the NERC disturbance database was presented to illustrate the disturbances profile in power systems, then the methodology to evaluate the probability of relay hidden failure was discussed.

By introducing a Dynamic Event Tree, probability of power system catastrophic failures due to relay hidden failures can be evaluated. A power flow program is used to determine the consequence of each trigger event. By combining the probability and impact index, the risk assessment framework for global system vulnerability assessment is established.

Under the proposed framework, a continuation power flow program is first used to fast-screen a list of locations most probably leading to system failures, which greatly alleviates the computation efforts needed. A detailed production simulation model addressing the load and generation uncertainties is developed.

Hidden Failure Monitoring and Control System

One of the significant contributions of this study is the development of a Hidden Failure Monitoring and Control System (HFMCS). Three main functional modules–*Hidden Failure Monitoring, Hidden Failure Control,* and *Misoperation Tracking Database*–and their designs are presented. Hidden Failure Monitoring provides the basis that allows further control actions to be initiated. Hidden Failure Control is realized by using Adaptive Dependability/Security Protection, which can effectively stop possible relay involvement from triggering or propagating disturbance under stressed system conditions or some abnormal conditions (e.g. relay hidden failures) in relay systems. These abnormal conditions are alarmed by the Hidden Failure Monitoring module. By enabling the Voting Scheme or temporarily disabling the questionable relay functional unit in the adaptive protection logic, security of the protection system is in favor and the risk of system catastrophic failures is minimized.

As an integrated part of the HFMCS, a Misoperation Tracking Database is proposed to track the performance of automatic station equipment, hence facilitating the risk assessment of catastrophic failures to develop a prioritized list of system weak links for the deployment of monitoring and control modules. It will also assist decision-makers in efficiently prioritizing and matching available resources with the many needs of the utility's system.

Adaptive Dependability/Security Protection

The intelligent adaptive protection and control techniques developed in this dissertation allow protective devices to adapt to changing system conditions, thus minimizing the risk of system catastrophic failures. As the core of the Hidden Failure Control module, three layers of ADSP logic have been developed, i.e. *Adaptive Primary Protection*, *Adaptive Backup Protection*, and *Adaptive Emergency Load Protection*. They are applicable for different scenarios. Adaptive Primary Protection is used to prevent the hidden failure modes of Zone-1 distance elements (reach or timer) and carrier current elements, while Adaptive Backup Protection mainly works against the defects of Zone-2/3 distance fault detectors or timers. Adaptive Emergency Load Protection is suitable for preventing relay from misoperating under unexpected heavy load conditions. The Voting Scheme inside these adaptive logics will be activated respectively upon meeting certain pre-defined criteria.

1.4 Organization of the Dissertation

The remainder of this dissertation is organized as follows. Chapter 2 provides an extensive literature review of related research, especially in the areas of protection system reliability, relay hidden failures, catastrophic failure prevention, reliability engineering, and risk assessment of dynamic systems. In addition, the importance of the power system as a critical infrastructure is emphasized by a brief review of major blackouts in North America. The deregulation effects and the challenges to maintain system reliability in today's competitive electricity market, as well as the differences between this study and related research, are also presented in Chapter 2. The mechanism of cascading system failures is examined in Chapter 3 through the analysis of the 1977 New York Blackout. Chapter 4 presents a systematic method for evaluating the probability of relay hidden failures. The Dynamic Event Tree for the risk-based analysis of system catastrophic failures that take into account the relay hidden failures is also elaborated in Chapter 4. As a test case of the risk assessment framework, a reduced 179-bus WSCC system is studied, and the simulation results obtained from a California sub-system are analyzed in Chapter 5. System weak links were identified in the case study.

Going one step further, Chapter 6 addresses the issues relating to the load and generation uncertainties for the risk assessment of system vulnerabilities. Detailed simulation flowcharts for four different types of generating units (i.e. thermal, hydro, nuclear, and pump-storage) are developed and implemented in Fortran language.

Chapter 7 proposes a prototype system to monitor and control relay hidden failures–the Hidden Failure Monitoring and Control System (HFMCS). Hardware and software architecture as well as considerations of implementation/deployment are discussed. Implementations of Adaptive Dependability/Security Protection (ADSP) and the Misoperation Tracking Database (MTD) are also illustrated. A summary of the contributions, implications, and limitations of the study and future research directions is given in Chapter 8.

Some key terms related to the study are defined in Appendix A. A statistical analysis of disturbance reports based on the NERC disturbance database is given in Appendix B. Detailed simulation processes on a 7-bus system are reported in Appendix C. Appendix D lists the load flow input data for a reduced WSCC system. Short circuit calculation results of the reduced WSCC system are documented in Appendix E.

Chapter 2 Literature Review

2.1 Introduction

In the first part of this chapter, the technological advances in computer relaying will be briefly introduced; these advances are crucial to the implementation of the HFMCS proposed in Chapter 7. In the subsequent sections, we will discuss the reliability of protection systems: dependability and security, the failure modes of protection systems, causes of relay misoperation, and catastrophic failures in power systems. This chapter will provide the reader with the appropriate theoretical background critical to understanding the approach in evaluating the risk of catastrophic failures due to relay hidden failures. Historical works in related areas such as security analysis, event tree analysis, and catastrophic failures prevention will be investigated with the intention of drawing conclusions on the advantages and disadvantages of the methods.

2.2 Failure of Protection Systems

2.2.1 History of Power System Protections

The first generation of electromechanical protection equipment features relatively primitive functions with limited capability. Analog electronic equipment gradually emerged by emulating the single function of its electromechanical precursors. Both of these technologies required expensive cabling and auxiliary equipment to produce functioning systems. For example, for a line protection package with three distance zones and overcurrent protections, we may need three phase distance relays and one ground distance relay for each zone protection, plus three phase overcurrent relays and one ground overcurrent relay for time delay and instantaneous protections, respectively. The number of relays used in the package exceeds twenty without counting the auxiliary relays (e.g. timer relays, directional relays, breaker failure relays, reclosing relays, lockout relays, etc.). All of these relays need to be wired to their current transformers (CTs) and potential transformers (PTs), accounting for considerable labor cost and susceptibility to a high risk of wiring error.

Originating in the 1960s, computer relaying offers many advantages, including the ability to process a significant amount of information, the ability for secure and reliable exchange of digital information with remote locations, the ability to continuously monitor protection relay integrity by self-supervision and auto-diagnostics, the ability to be reprogrammed easily, and the ability to tackle troublesome issues such as very high impedance arcing faults. The first generation microcomputer-based digital relay was either single function or had very limited multi-function capability, and did not significantly reduce the cabling and auxiliary equipment required.

After more than twenty years of development, more recent digital relays [17] have become quite multi-functional, reducing cabling and auxiliaries significantly. The second generation digital relays were introduced in the early 90s and have evolved into so-called Intelligent Electronic Devices (IEDs) due to their broad functions available to the relay engineer. These IED devices offer a wide array of protection, control, monitoring, metering, and communications functions in a flexible, scalable, and cost effective manner. This modular architecture (both hardware and software) of IED devices feature the latest technological innovations including open Utilities Communications Architecture (UCA) technology that allows IEDs to communicate with existing legacy devices, as well as easy 'upgradeability' and future technological enhancements.

For example, the 2nd generation digital relay (e.g. the GE UR series D60 relay [17]) use waveform sampling of current and voltage inputs with protection algorithms to provide complete transmission line protection. They not only provides four zones of phase and ground mho distance functions, together with directional phase and ground instantaneous and timed overcurrent, breaker failure and auto-reclosing functions, but also include built-in logic for the five common pilot-aided schemes. For distance functions, user may choose either mho or quadrilateral characteristics. Depending on the cost and desired protection schemes for different voltage transmission systems, some IEDs may just provide primary distance protection, while others may provide high performance protection with high speed open standard peer-to-peer communications. Typical operating time of GE UR relays is between one and 1 1/2 cycles, and SEL 421 relays claim to operate within one cycle [18].

With more and more functions built into a single module, the amount of cabling and auxiliary equipment installed in stations has been further reduced, to 20% to 70% of the levels common in 1990, which has achieved large cost reductions. Most electric utilities have embraced numeric multifunction protection technology as a means of surviving in an industry that has changed dramatically in the last ten years. Led by restructuring and shrinking resources, protection engineers are continuing the move to multifunction protection technology as a means of reducing cost and maintaining operating performance with fewer personnel.

More recently, these devices also transfer data to central control facilities and Human Machine Interfaces (HMIs) using electronic communications. IEDs with this capability will provide significantly more power system data, enhance operations and maintenance, and permit the use of adaptive system configuration for protection and control systems.

The new generation of IEDs will also be easily incorporated into automation systems, at both the station and enterprise levels. Some features offered by the new generation protection IEDs are summarized below:

- Sub-cycle operating time
- High-speed communication capability
- Support of multiple protocols such as Telnet, FTP, and UCA2
- Adaptive system control based on pre-fault/after-fault conditions
- Self-checking and monitoring
- Incorporated Phase Measurement Function (PMU) [19]
- Human Machine Interface capability
- Fully integrated complete breaker protection and control

By upgrading to these digital relays for new and retrofit installations, utilities can extend the lifetime, security, and reliability of an existing power system.

According to Newton-Evans Research Company’s 2002 survey of protective relays used in the power industry, the percentage of digital relays in the mix of all protective relays used by utilities continues to increase. Nearly 40% of all generator and transmission line relays installed in North America are now digital units. The majority of new and retrofit units being purchased are also digital relays. The ever-growing population of digital relays and the technological advances will provide the necessary physical platform to implement the HFMCS proposed in Chapter 7.

2.2.2 Reliability of Protection Systems

In general, reliability is the probability that a system will perform its specified functions at an acceptable level under given conditions for a specified period. More specifically, reliability may be interpreted as the conditional probability that the system will perform its intended function(s) throughout an interval, given that it was functioning correctly at time t_0. Reliability terminates with a failure — i.e. unreliability occurs.

In a different context, reliability may have more specific implications. In data communication, reliability has been succinctly defined as “Data is accepted at one end of a link in the same order as was transmitted at the other end, without loss and without duplicates.” However, what does reliability mean regarding power protection systems? Reliability of power protection systems is a double-edged sword because it involves both dependability of operation and security from false operation in the protective relaying world. According to IEEE standard C37.2-1979, security “relates to the degree of certainty that a relay or relay system will not operate incorrectly”; Dependability is defined as “the degree of certainty that a relay or relay system operate correctly.” More specifically, dependability means that each relay sends a trip signal when a fault is present in its zone. Security means that no relay sends a trip signal if no fault is present in its zone. Since no human invention is perfect, and the protective relay system is no exception, compromise between dependability and security is inevitable.

The recent economic downturn and wrong market signals have triggered a race to cut costs, with minimum attention to the consequences for overall system reliability. Responding to competitive pressure and shrinking capital and O&M budgets while maintaining protection reliability is not an easy job. [20]

Protection system reliability studies in the past three decades have produced fruitful results due to the efforts of many researchers such as R. Allan [21], C. Singh [22], R. Billinton [23], etc. The recent advances in digital relays bring new interest in evaluating its reliability performance. Research work [23] shows that built-in monitoring and self-checking facilities within the relay can improve the reliability of a protection relay. By identifying a selected group of reliability factors that impact both non-digital relays (electromechanical and solid state relays) and digital relays, Johnson [24] evaluated the reliability of digital multifunction protection systems against predecessor technologies, and discussed in detail the impact of various engineering, operating, training, maintenance, and economic factors on the reliability of digital protection. He also suggested that application and maintenance philosophies must be reviewed on a regular basis to ensure that they are meeting both current and long-term protection reliability needs.

2.2.3 Security verse Dependability

The objectives of protection systems require that the protective relay system must perform correctly under adverse system and environmental conditions. In other words, it must perform accurately and dependably: The protection system is not required to function during normal power system operation, but must be called upon to operate immediately to isolate the trouble area or block correctly for a trouble outside the protection zone [25]. Lack of dependability will lead to the failure of isolation of faulty components, unless backup protection is active (which usually involves a considerable time delay to allow coordination between backup and primary relays).

Historically, an accidental loss of a single piece of equipment due to relay misoperations will not have system-wide significance, while failing to clear a fault in time will cause severe damage to the protected equipment. Excess heat during a fault will cause the sag of line conductor, eventually requiring the replacement of the whole line conductor; it is very time-consuming and expensive to replace the sagged line. Other equipments, such as transformers and generators, are also very expensive. With the prohibitive replacement cost in mind, the design and application of protection systems in the power system are biased toward dependability at the expense of security to minimize damage to system components; hence, protection systems have traditionally been designed to include a high level of dependability, which was achieved by redundancy and diversity. This design philosophy for protection systems ensures that no single failure of a protective device or a protection system will lead to a fault remaining connected to the network for an unacceptable period of time.

For example, line protection in practice for 138kV and 345kV consists of a primary scheme and a backup scheme. The primary scheme uses either a Directional Comparison Blocking (DCB) or a Permissive Overreaching Transfer Trip (POTT) [25]-[28] for instantaneous protection over 100% of each protective zone, while the backup system uses instantaneous protection for a portion, say 50%-90%, of the protective zone and time delay protection for the remaining portion and overreaching into the next zone. For even higher voltage transmission line protection, e.g. the 500kV and 765kV systems, practices are very similar to the 138kV and 345kV systems; however, there will have a secondary primary system using a set of distance relays in the DCB or POTT arrangement, thereby providing two independent instantaneous protective schemes, giving 100% zone protection. These two primary systems should, preferably, be supplied by different manufacturers; for example, the line protection package consists of digital relays from GE and SEL in the recent practices of many utilities in North America.

CT, PT and DC control and tripping power will also be duplicated to provide independent and redundant sources to operate relays and trip circuit breakers for critical extra high voltage (EHV) systems. Each breaker will have two separate trip coils connected to separate batteries with similarly associated separation of auxiliary equipment.

For important transmission lines, local breaker failure protection will also be provided to ensure that all tripping elements are supervised and all necessary local and remote trips are initiated upon the failure of a tripping element. All of these designs contribute to a much more dependable protection system at the cost of its security. This approach is appropriate when a system is in normal operating conditions with sufficient margins.

On the other hand, lack of security means that false trips may occur, leading to cascading outages of transmission lines, widespread uncontrolled customer interruptions, even catastrophic system failures. While a system is already in its stressed state due to unexpected outages of transmission lines, or excessive load demand in abnormal weather conditions, or the system is operating closer to its limits, relay misoperation will no longer be tolerated due to the higher risk leading to catastrophic failure, and system security becomes a larger and more important issue.

Much of the art of protective relaying arises because of the tension between dependability and security. A typical problem is choosing between two available protection schemes, one having better dependability and worse security, the other having better security and worse dependability.

The prevailing design philosophy of the existing protection system, with its multiple zones of protection, leans toward dependability even at the cost of global system security. Hence, a vast majority of relay misoperations are unwanted trips, which have been shown to propagate major disturbances.

Dependability can be tested relatively easily in the laboratory or during field application. Security, on the other hand, is much more difficult to check. A true test of system security would have to measure responses to an almost infinite variety of potential transients and counterfeit trouble indications in the power system and its environment.[25]

2.2.4 Failure Modes of Protection Systems

Considering the vast number of relays existing on a power system, protection systems are highly reliable; however, 100 percent reliability is realistically unattainable. Incorrect or unwanted relay operations have occurred in the 1965 Northeast Blackout, the 1977 New York Blackout, and the 1996 WSCC events [29], and they will continue to contribute to future major disturbances.

The performance of protection systems can be classified into the categories of *Correct Operation*, which accounts for relays performing correctly based on the input signals, and

Incorrect Operation, which results from a failure to perform its planned functions [22]. In the Correct Operation category, we should be aware of *Unwanted Operation*, even when the protection system responds correctly to the system conditions; this scenario was demonstrated by the 1965 Northeast Blackout (see section 2.3.2).

There are two modes of possible improper relaying. The first, failure to operate for a legitimate internal fault within the zone of protection relegates tripping to backup relaying (*Incorrect Operation*). The longer the fault clearing time, the greater the potential for line or equipment damage as well as system instability. The second mode is false operation for a fault outside of the protected zone *(Undesired Tripping)*. This can cause incorrect isolation of a no-trouble area. Undesired tripping could be triggered by a heavy loading condition in the absence of a fault or in post-fault conditions, or by mis-coordination between primary relays and backup relays due to whatever reason, such as CT/PT errors, settings without enough margin, and/or hidden failures of relay components. Many utilities have experienced this type of failure.

Different types of relays may have different probabilities of undesired tripping. The electromechanical and static protection relays used in transmission systems become a major risk as their level of reliability decreases. Even if checked periodically, these relays often cause misoperations, leading to cascading outages.

One typically insecure relay with regard to line protection is the relaying equipment used at the majority of EHV lines—a non-electromechanical relay package called static relaying. The static relaying interfaces with traditional currents via transducers that convert the analog information to a digital quantity. The digital data is then input to the static relaying logic. The logic determines whether tripping should occur. This technology had some problems in the past, including susceptibility to false operation due to electrical transients caused by station switching operations. The first static protective relays were put into in service on a 765kV line in the mid 1970s, there were 29 instances of false tripping of 765kV circuits by static relays (28 faulty cards, 1 bad solder connection) in the first four and half years among the 25 static relay terminals in service then. On average, there were about 6.5 false trips per year. Among the 29 false trips, seven trips occurred due to external faults. In one case, a static relay defect contributed to the loss of a generating unit. In another instance, two 765kV circuits tripped falsely for a fault on a third. It is obvious that static relays were dependable but not very secure.

Another cause of relay misoperation is the aging of electromechanical relays. Electromechanical relays have a good reputation of being reliable. For example, GE's GCX17 relay has been widely used to provide high-speed directional protection for single-phase to ground and three-phase faults. They also provide time-delayed protection for phase-to-phase and double-phase to ground faults for transmission and sub-transmission systems. In some schemes, the same relays are used for both carrier starting primary systems and non-carrier step-distance back-up systems for the same terminal; however, aging capacitors in the relay cause changes in the electrical characteristics, which, in turn, change the settings of the relay, producing over/under-reaching misoperations. GE stopped production on this type of relay around 1965, and replacement parts are no longer available. These relays are being phased out, but there still exist many GCX relays in service (e.g. more than 200 terminals in a Midwest utility), which pose a great threat to system reliability, and may cause cascading failures in the system.

The impact of protection system failure depends on the condition of the power system when it occurs. Power system operation is greatly affected by these two different failure modes, and they have significant effects on the system reliability evaluation due to their differences in the number, order, and likelihood of contingencies [22]. In either of the above cases, customers and utilities can experience problems resulting from misoperations in the transmission system. State and federal governments are closely watching the operation of transmission systems, and improper relaying could cause some adverse public exposure for utilities.

The Relay Working Group (RWG) of the Western Systems Coordinating Council reviewed all 11 disturbances in 1998 and 10 disturbances in 1999 in WSCC systems [30]. The system protection and special protection problems in those disturbances were categorized as either a security or dependability issue. In this analysis, a security issue is defined as a false or inappropriate trip, and a dependability issue is defined as a failure to trip when required. The definitions here comply with the discussion in previous sections.

According to the WSCC Relay Working Group, the behavior of relay systems involved in each disturbance was analyzed to determine its degree of involvement and contribution to the triggering and development of the disturbance. The roles of the protection system in the disturbance were classified into three main categories:

1) *Primary Cause* if the protection system directly caused the disturbance to occur
2) *Secondary Cause* if the disturbance was caused by some other action and the protection system promoted the disturbance
3) *No Contribution* if the protection equipment did not contribute to the disturbance and functioned properly

If the disturbance was triggered by actions other than that of protection system, the impact of relay malfunction on the severity of the disturbance was further divided into major contribution or minor contribution in the Secondary Cause. Table 2.1 summaries the finding of RWG disturbance review [30]. As shown in Table 2.1, 12 out of 21 disturbances were either triggered or promoted due to the malfunction of the protection system, accounting for 57% of all disturbances. Relay security problems are more than twice as common as dependability problems.

The Relay Working Group of the WSCC concluded that that the protection system and special protection security was an issue in nine of these disturbances, while only four disturbances raised concerns regarding system dependability, and both dependability and security played a role in two disturbances.

Table 2.1 Summary of RWG Disturbance Review

	1998 Disturbances	1999 Disturbances	1998-1999Total
Number of Disturbances	**11**	**10**	**21**
Protection Problems Reported	**7**	**4**	**11**
RWG Verified Protection Problems	**6**	**5**	**11**
Primary Cause	**5**	**1**	**6**
Secondary Cause	**2**	**4**	**6**
Major Contribution	**1**	**1**	**2**
Minor Cause	**1**	**3**	**4**
No Problems Reported	**4**	**5**	**9**
Security Problem	**5**	**4**	**9**
Dependability Problem	**2**	**2**	**4**

2.2.5 Causes of Relay Misoperation

Four main causes contributing to incorrect operations are: 1) inappropriate design or application of relay schemes; 2) inappropriate settings for some specific system condition; 3) human error; and 4) component malfunction [25]. Since the first three factors are hard to quantify, they tend to be more related to the policy, practice, and the management of individual utilities, and thus are hard to control from the point of view of relay engineers; we are more interested in quantitative analysis of the equipment malfunction.

The above four categories may not be all-inclusive, but these are the major factors involved in the misoperation of a protective system. Other classifications may be used by different systems; for example, the WSCC groups the failures of protection system into six categories [30]:

1) Communications: problem with the communications channel, line trap, turning equipment, etc.
2) Components: a failure of a part or module of a relay or a component relay.
3) Settings: inappropriate relay settings, either calculated or applied.
4) Design: design errors or inappropriate design of circuit.
5) Procedures: Improper procedures include problems caused by maintenance procedures, test and installation procedures; this also includes switching or operational procedures.

6) Scheme: An inappropriate protection scheme is used.

Based on this classification, Relay Working Group of the WSCC investigated the relay misoperation causes of disturbances happening in 1998~1999. The misoperation causes are listed in Table 2.2.

Table 2.2 Relay Misoperation Causes

	1998 Disturbances	**1999 Disturbances**	**1998-1999 Total**
Inadequate installation test procedures	2	0	2
Trouble during commissioning, relays disabled	2	1	3
Maintenance	3	1	4
Setting/Coordination error	1	0	1
Procedural error	1	1	2
Equipment/Hardware trouble	1	3	4
Communications/TT equipment	2	1	3
Design practices	0	1	1
Total	**12**	**8**	**20**

If we group the misoperations caused by Equipment/Hardware trouble and Communications/TT equipment as misoperations due to component malfunction, component malfunctions are blamed for more than one-third of all relay misoperations. The ARG group also concluded that "Component failures and setting errors appear to be the primary cause of security (overtripping) problems." [30]

2.2.6 Relay Component Failure

Any component of a protection system, including CT, communication channel, relay timers, relay contact, may malfunction, leading to incorrect operation. Abnormal loading conditions exceeding relay loadability, failure of communication channel, CT/PT saturations, and inappropriate polarizing signals are among the most common causes of relay misoperations leading to cascading outages. Among those causes, relay loadability is frequently involved in cascading outages on power systems due to inappropriate Zone-3 (or Zone-2) distance settings of back-up protection systems. Hence, the performance of the protection system during abnormal system events plays a vital role in eliminating or mitigating cascading outages. [29]

The majority of 765/500/345kV static line protection equipment has been in service for over twenty years. The static line protection equipment has a modular design with many sub-boards that plug into a chassis. Each chassis is then tied to other chassis through interconnecting wiring. Static line relaying reliability concerns have been raised over the last several years. There are several areas of concern:

1) The "seating" of the cards. The card edge connection loosens and dust builds up on connector.
2) The wiring insulation has become brittle. This could result in shorts to ground on the chassis or to other wires.
3) Component aging. Each of the boards is comprised of discrete components. Over the life of this equipment, aging has caused changes in the value of capacitors and resistors. A small change in component value in a logic circuit could cause a deviation in operational parameters from the circuit design.

Loose connections, cold solder joints, loose screw terminals, broken wires, and incorrect cable wiring have been found and documented. Any of these problems could cause a failure of the protection system. The manufacturers have validated these concerns. For example, GE projected a twelve-year life expectancy for static relaying equipment and questioned the reliability of this equipment still in service.

In addition, calibration, a preventative maintenance task, is no longer performed on the static line relaying in some utilities because of the risk of damage to the relaying equipment, and this is becoming a common practice among utilities because the procedure usually creates problems, delaying the relay's return to service. During the calibration procedure, power to the equipment is turned off and back on, which leads to transients and thermal changes. These stresses result in component failures. Protection & Control personnel are not comfortable with the relaying in this condition since no guarantees for proper operation can be made.

2.2.7 Relay Hidden Failure

From the 1965 Northeast blackout to the 1977 New York Blackout to the 1996 WSCC Blackout, relay hidden failures have been blamed for either triggering disturbances or propagating cascading events leading to system blackouts. In the past decade, especially since the 1996 WSCC Blackout, relay hidden failures have been gaining more and more attention. [3][10][11][29][31][32] We are at a point in the evolution of the technology where we need to step back and ask some questions about protection reliability.

According to a NERC study of major disturbances that occurring between 1984 and 1988, more than two-thirds of disturbances involved the misoperation of protective relays. The defects of the involved relays were not detected until exposed to abnormal conditions such as neighboring faults, overloads, or reverse power flows. These hidden failures (defects) prevented the involved relays from performing their designed functions, and even worse, they helped propagate the disturbance. A research group headed by Phadke at Virginia Tech has investigated extensively the hidden failure modes of relays with high-vulnerability indices. More than a dozen hidden failure modes [5][33] have been identified so far. These research efforts provide insight into possible countermeasures [32], such as adaptive protection, to reduce the likelihood of hidden failure.

2.2.8 Adaptive Protection

Adaptive protection is a protection philosophy that "permits and seeks to make adjustments in various protection functions automatically in order to make them more attuned to prevailing power system conditions" [36].

Adaptive protection is a real-time feedback system, which allows the enabling/disabling of certain relay functions [37], and changing online relay settings, relay characteristics, or logic adapting to external signals and conditions in the power system [38]. With the help of phasor measurement units (PMU) located at key substations across the system, adaptive out-of-step protection has been proposed by carrying out the calculation of angular difference between two buses or two sub-systems. Indicating the degree of stability or risk of instability between systems, this angular difference can be used to enable or disable the out-of-step protection scheme [39].

Advances in high-speed reliable communication networks (e.g. SONET allows fast latency times and reliability of communication) provide the opportunities for wide area adaptive protection and have drawn considerable attention from researchers in the U.S. The most recent efforts are demonstrated by M.J. Damborg, et al. [40]-[42]. A communication and control structure operating in anticipatory and responsive modes is proposed to avoid or reduce the impact of misoperations of protection devices [41][42]. A similar concept was also suggested by J. C. Tan et al [43].

As already mentioned in section 2.2.3, the prevailing protection system design philosophy in the relay community is in favor of dependability. Although some researchers and engineers promoted the idea of changing relay trip logic in response to external conditions, no detailed logic design and implementation have been given. In this study, the adaptive protection concept was further advanced by proposing the detailed logic design of Adaptive Dependability/Security Protection to mitigate the risk of catastrophic failure. By integrating the concept into the HFMCS, the protection system behavior can be altered to emphasize security under abnormal conditions.

2.3 Failure of Power Systems

2.3.1 Effects of Deregulation

A typical example of the critical infrastructures that undergo rising vulnerability to catastrophic failure is the electric power transmission network. There are several reasons for such a situation to prevail. First, in developed countries, including the U.S., there has been very slow expansion of the high voltage transmission grid during the last decades due to stringent regulations put forward in response to environmental concerns. For example, it took American Electric Power Company (AEP) more than 10 years to get required certificates from state commissions and approval from federal agencies to build a 57 mile (Wyoming - Jacksons Ferry) 765kV transmission line. The proposed line was determined to be needed by 1998 when existing facilities would no longer meet customer demand if there were a major line failure [44]. Due to the delayed construction of the 765kV line, AEP had to implement interim contingency plans to minimize the economic and safety impacts that could result from outages.

Secondly, there are the profound structural reforms that the power industry has embarked on, which are geared toward the emergence and consolidation of competitive energy markets [45]-[49]. In 1996, the Federal Energy Regulatory Commission (FERC) issued its landmark Orders 888 and 889 [50] that required utilities to provide nondiscriminatory access to utility transmission systems by non-utilities, or independent power producers. In Europe [45], in South America [46], in the Pacific [47], and now in North America [48][49], governmental institutions have issued new regulations to transform the once vertically integrated utilities into independent generation, transmission, and distribution companies.

Traditionally, the power industry has operated as a non-competitive, regulated monopoly, with its emphasis on reliability (and security) at the expense of economy, and power systems have been operated very well for many years within the boundaries of operating limits imposed by safe but conservative reliability criteria [51][52][53]. In the last two decades, however, the energy industry has undergone major changes. Power systems have been restructuring from operating in a conventional vertically integrated environment to operating in a competitive, deregulated environment. More and more utilities have been separated into three isolated segments: generation, transmission, and distribution. These changes affect how our energy infrastructure operates.

Deregulation demands a better, faster, and cheaper way to conduct business, thus the power industry is being reorganized to allow power to be traded freely. In the emerging competitive electricity markets, generation companies are competing with each other to sell power in auction markets where customers can buy electric energy at the best price. The wholesale market is the first to flourish and expand at a rapid rate, boosted by open access transmission and great variability in electricity prices between U.S. states. For example, in the states of New Hampshire and New York, the price of electricity ranges between 9 to 12 cents per kWh, while in the states of Washington, Montana, and Idaho, the range is only 4 to 5 cents per kWh. This price discrepancy has resulted in a growing amount of bulk power being transferred over long distances throughout the transmission grid.

On the other hand, the transmission system was built for limited transfers of bulk power from region to region, not to serve an electricity market place. The power system infrastructure has failed to keep pace with the changing requirements of the power system. Due to the uncertainties in the market environment, incentives to investment in upgrading the power system infrastructure are lacking. The annual investments in transmission have been declining by almost $120 million a year for the past 25 years. An Edison Electric Institute (EEI) statistical yearbook shows that transmission investments in 1999 were less than half of what they had been 20 years earlier. As a result, the electricity transmission system has been constrained by insufficient capacity since the mid-eighties. With deregulation worsening a shortage of reserve margin, the power system is pushed to operation closer to its stability limit, with a smaller security margin imposed by both economic and environmental pressures; consequently, blackouts and brownouts in the Eastern and Western parts of the country are increasing in number at an alarming rate over the last few years [2][54]. For example, in July of 1996, a series of blackouts struck the western part of the United States, leaving 2.2 million customers without electricity. One month later, islanding and blackouts affected eleven U.S. Western states and two Canadian provinces. In December 1998, the Bay area of San Francisco experienced a series of blackouts, and in July of 1999, it was the turn of New York City to suffer from the same type of cascading failures. More recently, California has been struck by rolling blackouts initiated by the utilities to overcome a severe shortage of generation during peak hours. The reader is referred to the report prepared for the Transmission Reliability Program of the Department of Energy [54] for an exhaustive account of these blackouts.

There is growing evidence that the U.S. transmission system is in urgent need of modernization. Our economy has been paying and will continue to pay a high price for overlooking this need. According to Federal Energy Regulatory Commission (FERC)

Chairman Pat Wood, the cost to California electricity customers was $222 million for congestion alone between September 1999 and December 2000. Costs of congestion for four Independent System Operators (ISOs) today are estimated to be at least $500 million annually.

According to the May 2001 report on national energy policy released by the Vice President's task force in, electricity consumption has increased by 2.1% annually since 1989; however, the transmission capacity has increased by only 0.8% annually during the same period. Figure 2.1, taken from a report prepared for the Edison Electric Institute by Hirst and Kirby, shows average annual growth rates in U.S. transmission capacity and summer peak demand for 1979-1989, 1989-1999, and projections for 1999-2009 [55]. As an example, AEP last reinforced the 765kV transmission system that delivers electricity to its southern West Virginia, Virginia, and eastern Kentucky customers in 1973. Since then, the area's peak demand for electricity has increased more than 135%. Although the use of power electronic devices can increase the flow of power through the existing transmission lines, it is inevitable that demand growth will lead to the need for increased capacity available only by constructing more lines when the existing transmission lines have reached their thermal/stability limits.

Over the next ten years, the demand for electric power is expected to increase by about 25 percent. NERC has estimated the need for $56 billion in investment over the course of the next 10 years to eliminate the growing problem of congestion on transmission lines, but the electric transmission capacity will increase by only 4 percent under current plans. The yawning gap between the growing demands made on the transmission system and the money spent to improve it is getting larger and larger; this trend could exacerbate the existing transmission congestion and reliability problems [56]. The chronic under-investment in the electricity infrastructure has lead to shrinking reserves with the system operating at the stability edge, electricity outages, power disturbances, and price spikes.

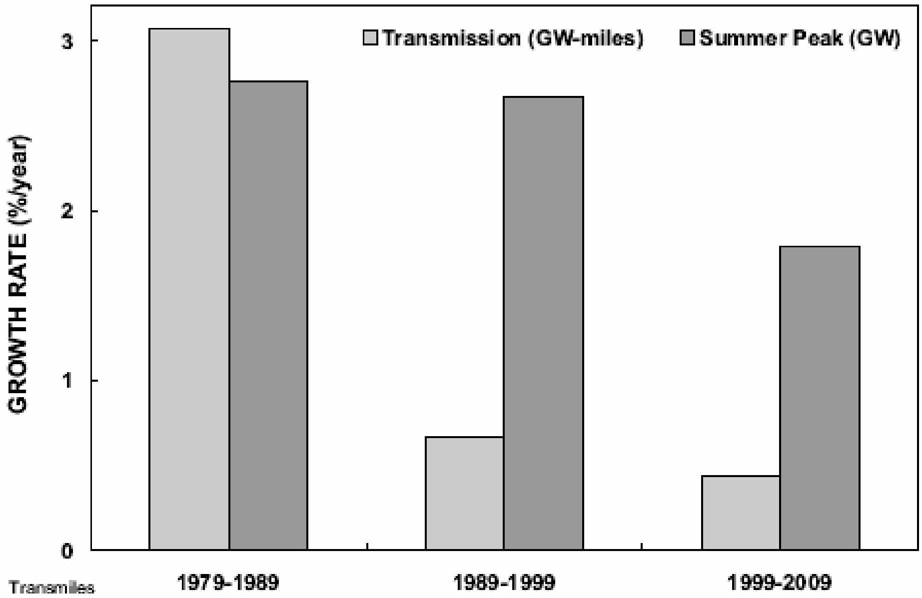


Figure 2.1 Average Annual Growth Rates in U.S. Transmission Capacity and Summer Peak Demand for 1979-1989, 1989-1999, and Projections for 1999-2009. (Eric Hirst and Brendan Kirby)

The growing unreliability of power delivery, including the potential for major blackouts, places the benefits of electric utility restructuring at risk, and threatens U.S. productivity, prosperity, and future well-being as demonstrated by the California power crisis. According to an EPRI White Paper [57] issued in June 2001, the direct losses to the nation due to power interruptions and inadequate power quality exceed $100 billion per year, based on a conservative estimate, and widespread catastrophic failures are more likely to happen than before.

2.3.2 Catastrophic Failures in Power Systems

As one of the most critical infrastructures, the electric power system is essential to the new digital society and quality of life. System failure can result in loss of life or dollars as well as decreased operational efficiency. Widespread catastrophic failure is so disruptive to our society that it may lead to near whole community chaos (e.g. the 1977 New York Blackout).

The following brief description of major blackouts that have occurred in U.S. provides readers some idea of how significant the impacts of catastrophic failure would be, and what role relays played in these cascading events. A detailed study of the 1977 New York Blackout will be presented in Chapter 3 to reveal the mechanism of wide-spread catastrophic failure.

1965 Northeastern Blackout

The first major failure hit New York City and much of the northeastern United States during evening rush hour (5:16p.m. on a Tuesday) in 1965. The protective relay that triggered the Northeast Blackout by an unexpected flow of power was in one of five transmission lines transporting power north from the Beck plant on the Niagara River to the load center in Toronto, Ontario. The pickup setting of the backup relay was set below the unusually high loadings due to the emergency outages of the nearby Lakeview plant. The unexpected heavy load condition caused the circuit breaker to trip this unfaulted line, leading to the transfer of its power to the four remaining lines, each of which, in turn, became overloaded and tripped out in cascade in 2.7 seconds. The separation of the Toronto load caused the excess power to surge back into the New York transmission system, resulting in transient instabilities and leading to that cascading failure.

Within 12 minutes of the initial event, 30 million people over an area of 80,000 square miles, including parts of eight northeastern U.S. states and most of Canada's Ontario, were left without electricity for 13 hours. At the height of the homebound rush hour, hundreds of thousands of people were trapped in crowded subway trains, elevators, unlighted halls, and stairways. Planes heading for New York had to be diverted as far away as Bermuda as airports were plunged into darkness.

1977 New York Blackout

From 20:37 through 21:29 on July 13, 1977, a series of lightning strikes, transient or permanent faults, and protective relay malfunctions put six high capacity 345kV transmission lines to go out of service. The remaining two 138kV transmission lines became severely overloaded, and protective relaying also tripped them out of service. These cascading events finally led to the entire load of the Con Edison system being lost. New York City was plunged into darkness. Service to more than 8 million people was interrupted for periods ranging from 5 to 25 hours. The direct economic loss was estimated in excess of 350 million dollars, and the impact of this blackout was greatly exacerbated by widespread looting, arson, violence, and malicious property damage. According to one report, 50 cars were stolen from a car dealership in the Bronx. The police made 3,776 arrests, but many thousands escaped before being caught. About 500 policemen were injured on their duties. Over 1,000 fires burned throughout the city, six times the average rate.

One of the Con Edison's main conclusions drawn from their self-analysis of the 1977 New York Blackout was that there had been a "failure to appreciate the increased vulnerability of the system under conditions of high energy imports during thunderstorms" [58].

1996 WSCC Blackout

Two major outages hit the Western Interconnection in the summer of 1996 [54][59][60][61]. On July 2, 1996, a flashover to a tree on the Jim Bridger – Kinport 345kV line exposed a hidden failure in an electromechanical relay on the parallel Jim Bridger – Goshen 345kV line, taking out of service two of three 345kV outlet lines of the Jim Bridger power plant. This triggering event initiated a chain of events breaking the Western Interconnection system into five islands, and resulting in cascading outages.

One month later, an even more disruptive power failure struck the WSCC system again. On August 10, 1996, faults in Oregon at the Keeler-Allston 500 kV line and the Ross-Lexington 230 kV line, protective device malfunctions, inadequate voltage support, etc., led to islanding and blackouts in 11 U.S. states and 2 Canadian provinces with a loss of 30,390 MW of load. More than 7 million customers were affected, with the estimated economic loss at $1.5 to $2 billion.

2.3.3 Catastrophic Cascading System Failure Prevention

Although power engineers have recognized that relay hidden failures have played significant roles in the propagation of catastrophic failures, the mechanism of relay hidden failures leading to catastrophic failures and its impact on overall system reliability has not been well studied.

However, efforts have been made in developing techniques and methodologies for preventing catastrophic cascading system failure. H. You et al [62] proposed an intelligent adaptive load-shedding scheme using a Reinforcement Learning technique. When a system is on the edge of collapse, the scheme provides a self-healing strategy to prevent catastrophic failures by dividing the system into smaller islands based on the system vulnerability analysis.

In another paper by J.C. Tan, et al [63], a Sequential Tripping Strategy based on Certainty Factor was described for a wide-area back-up protection expert system (BPES). The BPES is designed to prevent the occurrence of wide-area blackouts by providing selective and secure back-ups to a region of a transmission network when the main protection has failed to clear a fault. By locating the line most likely to contain the fault, Sequential Tripping Strategy can clear a fault at minimized risk to the network; however, the authors failed to address the implementation issue of this scheme, and how the communications between several stations could be set up to meet the fast relay operation requirements remains an issue to be addressed.

2.4 Reliability Engineering and Risk Assessment

2.4.1 Security Analysis

As we know, reliability refers to the probability that a component or system will operate satisfactorily under a given set of criteria either at any particular instant at which it is required or for a certain length of time. According to NERC criteria [51][52], all Control Areas shall operate so that instability, uncontrolled separation, or cascading outages will not occur as a result of the most severe single contingency, or multiple outages of a credible nature specified by Regional policy. Utilities are mandated to operate their systems within a secure region, where "the grid can continue to operate at or above certain minimum performance levels despite the loss of any one major component" [52]. This region is defined by carrying out so-called N-1 contingency analysis, considering the various combinations of representative load demands, generation allocation, and network configuration [64][65]. Occasionally, limited N-2 security analysis is employed in some stringent cases; however, it is implemented not via an exhaustive search, but rather via a partial assessment of the system reserves over a small portion of the transmission network. One advantage of the traditional security analysis is that the calculation of operating margins is quite straightforward and has been widely accepted by utilities; however, this deterministic way to perform security assessment in bulk power transmission system planning and operation, although widely used, is overly subjective.

N-k security analysis for $k > 1$ is perceived as being impossible to achieve due to the huge number of cases that need to be investigated. In fact, it would require checking the effect on the system reserve margins of the loss of every k out of N pieces of equipment, which yields a very large number of possible operating contingencies to be checked that grows exponentially with N. On the other hand, unpredictable combinations of unusual and undesired N-k ($k>1$) events (for example, multiple lightning strikes during severe weather combined with relay hidden failures and/or human error) can stress even the best-planned system beyond the acceptable limits.

Obviously, this conventional reliability assessment methodology neglects the different likelihoods for different components going out of service under a specific set of conditions. Other uncertainties such as the weather conditions are also excluded from the analysis. The difference in risk plays no role in this approach, and thus it provides a limited amount of useful information regarding risk to the utilities and the public in terms of formulating an efficient and cost-effective regulatory strategy. This is a worst-case analysis in the sense of only one component out of service, giving the priority to security at the expense of economy. In general, it is a conservative approach; however, it may lead to aggressive conclusions due to the limitation of excluding risk factors. For example, some N-2 and above contingencies may have higher probability in certain settings as well as more serious consequences, and it is *these cases* that lead to the catastrophic failures, and are excluded in the normal contingency analysis practice. Unfortunately, the exclusion may lead to unrealistic characterization or understatement of potential risks to the system.

2.4.2 Risk Assessment

The traditional way to perform the security analysis is static in nature and has potential weaknesses when applied to a dynamic process system like a power system. In today's more competitive, deregulated environment, the limitations of the traditional security analysis seem to exceed its advantages. As a result, risk-based security assessment has been extensively studied and its applications have been found in power system operations and planning. Risk-based security assessment provides power system engineers with additional insight into how likely the power system is to go wrong, and what it will cause as a consequence under a certain disturbance, say, a three-phase fault. More specifically, risk-based assessment can provide quantitative inputs for power system operations.

In general, risk is defined in the IEEE Standard Dictionary as the simple product of the probability and consequence of associated events. Thus, a likely event with an insignificant result would not be considered risky, whereas a likely event with a serious consequence would be. Probabilistic risk-based approaches to security have been used for decades in many fields, including the airline and nuclear industries. Risk has different aspects with respect to the emphasized area of interest. For example, there are different types of risk assessments of power systems in terms of time frame. Real time operation risk assessment evaluates the risks of the power system operating in real time. The time frame for this kind of assessment is usually within one hour, i.e. it computes the risks for the power system for the next several minutes up to the next hour. In this dissertation, risk assessment focuses on catastrophic failure of the power system, falling into the category of short-term/long-term risk assessment.

By analyzing relay performance and how it interfaces with operating conditions, we may recognize the mechanisms of catastrophic failures in the power system, and thus may identify the risks and weak links in the system. Hence, a Hidden Failure Monitoring and Control System (HFMCS) can be developed to minimize the potential risk.

Normally, three steps can be taken to avoid or mitigate catastrophic failures in power system:

1) Avoid or eliminate failure cause in the first place (Risk assessment + HFMCS)
2) Detect and control failure early (HFMCS)
3) Reduce impact/consequence of failures (Future research)

This study will only target the first two stages of the issue – preventing the failure and controlling its propagation. Stage 3 falls mainly into the research area of the power system restoration.

2.4.3 Risk of Power System Catastrophic Failures

Most complex systems involve minimizing costs, maximizing benefits, and minimizing risks of various kinds. A power system is a complex system that involves minimizing risks of load flow infeasibility, thermal overload, steady-state instability, transient instability, and dynamic instability.

Partitioning Multi-objective Risk Method (PMRM) [66]-[68] separates extreme events from other non-catastrophic events, thereby providing decision-makers with additional valuable information. In addition to using traditional expected values, the PMRM generates a number of conditional expected-value functions, termed risk functions, which represent the risk, given that the damage falls within specific probability ranges (or impact ranges).

In the risk assessment of power systems, the disturbance events may be partitioned into three impact ranges: high probability of minor events that have slight consequences; medium probability of average events that have some impact; and low probability of extreme events with catastrophic implications. Accordingly, the impact axis may be partitioned into three impact ranges.

2.4.4 Dynamic Event Tree

A classic method for assessing the reliability of a system is the event tree method. The event tree methodology is an analytical technique for systematically modeling the time sequence of events (scenarios) and identifying potential outcomes of a known *triggering event*. The *triggering event* is anything that begins a series of actions. For example, it can be a short-circuit fault (permanent or temporary) on a bus/transmission line/transformer, a piece of equipment failure, or a line overload. Starting from a triggering event, the event tree details the possible sequences of events in terms of success or failure of a system (e.g. protection system) designed to mitigate the effects of the disturbance. In event tree analysis, one tries to imagine all triggering events and tries to follow through the possible consequences thereof to an ultimate end. Great care is required in identifying and quantifying dependencies between the failure events. This procedure, called *Probabilistic Risk Assessment* (PRA), was initially developed for understanding nuclear power accidents. It has been successfully applied in many areas, from identifying ways in which a system can fail, to quantifying system performance (e.g. unreliability), finding system failure probabilities, and identification of system weaknesses. Many different approaches fall into the category of PRA, but which method is best depends on the nature of the systems and the objectives involved.

Probabilistic Risk Assessment, focusing on the analysis of catastrophic failures, consists of the three following key questions:

1) What can go wrong with the system and what are the likelihoods of the triggering events? (Appendix B)
2) What kinds of factors help propagate the cascading failures leading to the catastrophic failures? (Chapter 3)
3) How do we evaluate the probabilities and consequences of these cascading events? (Chapter 4); this constitutes scenario modeling and analysis

This dissertation will address the above three issues with emphasis on the last two.

The event tree analysis is probably the most widely recognized and adopted method for assessing the reliability characteristics of a system [70]. As an example in the power system protection reliability evaluation, Ferreira et al [73] developed a reduced event tree for the unit feeder protection scheme and discussed the application of an event tree model to evaluate the dependability and security of the overall protection system.

The event tree methodology is well-suited in the situations for finding interrelationships between failure components and top events; however, the methodology has some potential weaknesses when quantifying the risk associated with a large-scale interconnected system like a power system, for which the system dynamic behavior is a significant factor.

A power system consists of a huge number of closed-loop feedback control subsystems. An important characteristic of a power system is that it behaves dynamically, i.e. its response to an initial triggering event evolves over time as system components interact with each other locally (e.g. excitation systems or governor systems response to local voltage or frequency and the proper operations of protection systems) or remotely (e.g. appropriate control actions via high-speed communications). Correspondingly, the system states[2] change continuously. The developments of the dynamic sequence of events are strongly affected by automatic control systems or operator actions.

The well-known event tree analysis, on the other hand, frequently does not address this characteristic of the power system. This conventional analysis of the system risk and reliability treats scenarios as static sets of hardware successes and failures; it does not literally simulate system response to a triggering event. The structure of the event tree is fixed and all-inclusive. The effects of dynamic progression of a triggering event and the response of automatic control equipment are not incorporated in the event tree analysis

---

[2] The system state is generally defined implicitly in terms of the system components; in the context of catastrophic failure analysis in the dissertation, the system state is defined by the states of relays, which in turns define the line states: on or off.

since many of the conditions affecting control system actions (e.g. causes to develop relay hidden failure) are not explicitly included in the model.

In this dissertation, the problem of risk assessment of the power system catastrophic failure is addressed using a so-called “Dynamic Event Tree” (DET) approach by incorporating line flow analysis and protection system performance into conventional event tree analysis. Although this DET approach has not enjoyed the support of power industry, the theoretical superiority of the Dynamic Event Tree approach over the classic event tree approach to risk assessment is obvious. DET extends the notion of an event tree to treat event sequences branching over time. This approach requires the explicit tracking of possible dynamic scenarios (a line tripping event is regarded as a dynamic scenario), which are determined by line flow analyses and the probability of relay hidden failure exposure. Each scenario track provides the contextual information needed to determine the likelihood of system state changes during any point in the sequence events.

The Dynamic Event Tree approach uses simulations to track branching in system evolution up to a specific number of depth levels following an initiating event. The simulations stop when a specified number of depth levels or a *Top Event* (System Failure) is reached. The sum of scenario track (event sequence) probabilities leading to a Top Event gives the probability of this Top Event.

The proposed Dynamic Event Tree method can treat both deterministic and stochastic component state transitions in a general manner. Relay hidden failure exposed due to fault or overload can be identified by a threshold (deterministic approach) or by a probability-distance or probability-overcurrent curve (stochastic approach). Detailed information is presented in Chapter 4 on the application of Dynamic Event Tree to the risk assessment of power system catastrophic failure.

2.5 Summary

Although the probability of relay misoperation is very small, and neglected in conventional contingency analysis, the consequence of relay misoperations is costly and may be disastrous. Thus, this kind of misoperation plays an important part in the risk assessment of power system catastrophic failure.

A structured risk management approach is critical to dealing with combined rare events with disastrous consequences. The purpose of this study is to establish a framework for evaluating the risk of catastrophic failures due to relay hidden failures, based on the internal relationships between cascading events. Under this framework, a methodology for evaluating the probability of relay hidden failures will be proposed, a continuous power flow program will be used for fast-screen purposes, the Dynamic Event Tree technique will be employed to compute system failure probability, and the severity index will be assessed by using a load flow program. However, the risk assessment framework is limited to use with only a static state approach (load flow) to evaluate the consequences of system disturbances. A Hidden Failure Monitoring and Control System (HFMCS) will be designed and detailed implementation considerations will be discussed. The implementation logic of Adaptive Dependability/Security Protection for primary and backup schemes will be presented. The adaptive algorithm to deal with unexpected emergency load conditions will also be developed. To facilitate the performance evaluation of automatic equipment within the substation, a Misoperation Tracking Database (MTD), together with the format of Event Report, will be proposed.

Chapter 3 Mechanism of Catastrophic Failures

3.1 Introduction

Many papers have been written to describe particular major power system blackouts and to analyze the causes of failure and the role played by power system protection in a catastrophic failure [120]. Catastrophic failure is an event, or series of events, which seriously disrupts normal activities. This definition implies a personal judgment about that what is serious and a debate about what activities are normal [121]. It is more appropriate if we can specify a quantitative definition such as economic damage so that in some sense a catastrophic failure is a failure of a particular magnitude; however, in practice, it is not easy to propose such a clear, quantitative definition on which most engineers agree.

In this study, catastrophic failure in a power system is defined as an event that occurred with either of the following consequences

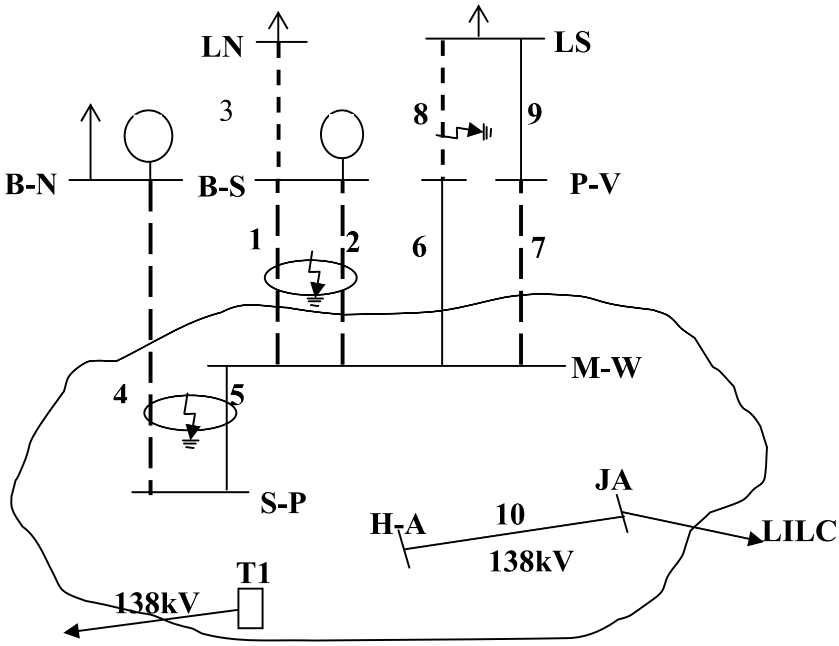
1) Large-scale loss of load
   - 1000 MW or more, or
   - 10% or more of system load
2) Other aspects of power system operations
   - Wide-area Voltage Collapse or/and
   - Large scale transient Instability

Catastrophic failure in a power system occurs when a complex set of external (e.g. high load demand) and internal (e.g. relay hidden failure, line overloading, etc.) interactions result in the power system being vulnerable; therefore, the power system is more susceptible to disturbance by relatively minor events such as short-circuit than when operating conditions are normal. The goal of the analysis of catastrophic failure is a systemic interpretation of a failure and its context that could, in turn, lead to some actions.

3.2 The 1977 New York Blackout

In order to develop an algorithm that calculates the probability of a system-wide disturbance due to cascading events following the legitimate tripping of a faulted line, we need to understand the mechanism of cascading catastrophic events. The 1977 New York Blackout is an interesting case that allows us to learn more about the mechanisms of multiple relay hidden failures and cascading catastrophic events.

As shown in Figure 3.1, the New York power system is connected to the northern neighboring systems through five 345-kV tie lines that imported a total power of 3375 MW before the blackout. It is connected from the south to Long Island Lighting Company and Public Service Electric and Gas through two 138-kV lines.



B-N – Buchanan North | LS – Leeds
B-S – Buchanan South | M-W – Millwood West
H-A – Hudson Ave. | P-V – Pleasant Valley
JA – Jamaica | S-P – Sprain Brook
LILC – Long Island Lighting Company | LN – Ladentown
PSE & G – Public Service Electric and Gas | T1 – Transformer

⟵ : denotes a connection with a neighboring system.

Figure 3.1 Simplified Schematic of the 345 kV System

The sequence of events that led to the blackout began with a lightning strike on the tower that supports Lines 1 and 2. Due to a hidden failure, the breaker failure relay of Line 2 at the Buchanan-South (BS) station sent a wrong signal to the relays of Line 3 at the Ladentown (LN) station, indicating that its circuit breaker had not opened in time, while it actually did. As a result, Line 3 was opened and locked out. About 19 minutes later, another lightning flashover occurred on Lines 4 and 5 placed on a common 345kV tower. Line 5 reclosed properly at both ends and hence was restored to service, while Line 4 did not reclose at Buchanan-North (BN) substation because of a large phase angle. At this time, large flows carried by Lines 1, 2, and 4 from the north transferred to Lines 6 and 7. This flow increase was beyond the Short Term Emergency (STE) thermal limit of Line 7 and resulted in currents of a magnitude large enough to trigger its overcurrent relay located at the Millwood-West (MW) station. Unfortunately, the contacts of this relay were permanently bent to a closed position during a testing procedure, causing Line 7 to open. So far, four out of the five tie-lines in the north were out of service. The cascading outages led to a 32% overload on Line 6 and a 6% overload on Line 8, with respect to their STE ratings. These thermal overloads led to line overheating and sag to the point where a short circuit occurred between Line 8 and a nearby tree. In summary, two relay hidden failures contributed to the New York Blackout.

In the above sequence, several hundred relays were involved in these protective actions. All the faults were cleared promptly by relays and circuit breakers, and most of the involved relays and circuit breakers operated as designed to remove equipment and circuits from service; however, several misoperations contributed to the catastrophic failure. Two hidden failures occurred that had significant consequences: One relay on Line 2 at the BS substation operated improperly, causing the unnecessary tripout of Line 3 (at LN side); and the damage relay on Line 7 at the MW substation caused the unnecessary tripout of the line following the short-circuits on Lines 4 and 5. Another two malfunctions occurred without significant impact on the system: The circuit breaker (CB1) at the MW substation failed to reclose Line 1 because of a problem in its pneumatic system, and the 138 kV Line 9 between HA and JA opened incorrectly at the HA substation as a result of a defective pilot wire relay circuit. All of these sequences of events finally led to the blackout of New York City.

Based on the above analysis, one typical scenario of multiple contingencies leading to system failure is as follows. The triggering event is a short-circuit that occurs on one of the transmission lines of the system. The relays of that line send tripping signals to its circuit breakers. Before the faulted line opens, the short-circuit current is sensed by a certain number of relays located within the *region of influence* of the fault. The latter region is defined as the union of the *regions of vulnerability* of all the relays whose hidden failures are exposed by the fault; consequently, each of these relays may unnecessarily open an unfaulted line if it suffers from a hidden failure. Hence, in addition to the faulted line, we may have two, three, or more simultaneous line openings, usually (but not necessarily) located in the vicinity of the fault. The power that used to pass through the tripped lines finds its way through other links in the network, which in turn may overload some of them. If any of the overload currents is larger than the setting of an overcurrent relay, or the apparent impedance seen by a distance relay falls into the relay's operating zone, then the corresponding relay will open the associated unfaulted line, putting additional stress on the network. In a domino effect, this sequence of line tripping followed by line overloading may propagate throughout the network until either the line overloading vanishes, or the stability limits or the voltage collapse limits are reached. It is clear that these chains of contingencies are dependent on one another. Moreover, several of them may cascade simultaneously; therefore, the probability of occurrence of these cascading failures is much higher than the probability of a random (i.e. independent) tripping of k out of N components of the system.

It is interesting to note that a system failure consists of a sequence of cascading line tripping that originates from the faulted line and spreads sequentially from one location to another one over an increasingly larger region of the network. A system failure consists also of the repetition of the same basic structure, which is the opening of a few lines located in the same neighborhood. This basic pattern repeats itself regardless of the size of the system failure, that is, regardless of whether it is a minor event that affects a small sub-network or a major event that results in the collapse of large segments of the network with dramatic consequences on millions of customers. Put differently, a system failure exhibits a *self-similar* geometric shape [122].

The above analysis of the 1977 New York Blackout focused on the causes of the relay hidden failures and the events that contributed significantly to system failure. These events are important in the probability estimation of hidden failure and system failure. It should be noted that the failure of the protective system to reclose a line due to hidden failure should also be analyzed. Although no hidden failure in the reclosing relays occurred in the events of the 1977 New York Blackout, it did happen according to statistics reported by the IEEE/PSRC Working Group 13 [74], which are presented next.

3.3 Some Statistics Reported by the IEEE/PSRC Working Group 13

IEEE/PSRC working group 13 reported statistics over a one-year period on relay and circuit breaker misoperations at a U.S. utility. [74] These statistics are summarized in Table 3.1. As seen from the table, there were seven failures to reclose and eight slow trips of lines; they amount to 14.6% and 17% of the total misoperations respectively, which need to be checked for hidden failures. There are two events under the "Unnecessary trip other than fault" subclass in the table, and this situation also happened in the 1977 New York Blackout due to an overload condition and a damage relay as analyzed in previous section.

The approach in [74] is used to evaluate relative performance of the protective system. It calculates the percentage of misoperations among the total number of protection system operations. It does not include all the relays involved, so it is not an evaluation of probability of relay misoperation or hidden failure.

Table 3.1 Statistics of Relay and Circuit Breaker Misoperations at a Utility (Taken from [74])

	Dependability			Security		System Restoration	Total Mis-operation
	Failure to trip	Failure to interrupt	Slow trip	Unnecessary Trip During Fault	Unnecessary Trip Other Than Fault	Failure to reclose	
Relay System	0	---	7	31	0	5	43
Circuit Break	0	0	1	---	2	2	5
Total Protective System	0	0	8	31	2	7	48
Incorrect Operation % (Relay System)	0%	0%	1.3%	5.6%	0%	0.9%	7.7%
Incorrect Operation % (Circuit Break)	0%	0%	0.2%	0%	0.4%	0.4%	0.9%
Incorrect Operation % (Protective System)	0%	0%	1.4%	5.6%	0.4%	1.3%	8.6%

3.4 Summary

It is usual practice in reliability and security analysis to neglect the effect of the protection systems; consequently, cascading failures leading to blackouts or brownouts are not investigated. Until recently, large-scale blackouts were considered to be sufficiently rare events to be disregarded from the analysis; however, at least in the U.S., ideas are evolving in this respect, prompted by the increasing number of major incidents that have plagued the U.S. power systems since mid-nineties. The frequency of major blackouts, which was about once per decade until 1996, has started to grow at an alarming rate since then.

During large disturbances, protection systems can play a detrimental role in the degradation of power system reliability. As revealed by an NERC study over a period from 1984 to 1988 [2], undetected failures of protection systems (i.e. relay hidden failures) aggravated disturbances by tripping unfaulted system components in 73.5% of the significant disturbances that were investigated. These undetected failures have helped the perturbation to propagate further, leading to cascading outages of transmission lines, eventually leading to catastrophic system failures. In other words, power system catastrophic failures are often the result of one or more hidden failures in protection systems acting in tandem.

One peculiarity of relay hidden failures is that they cannot be detected a priori; that is, they cannot be exposed before the system is perturbed. In particular, routine maintenance testing may not detect them or, even worse, may induce them by damaging relay components as was the case in the 1977 New York Blackout. Another source of hidden failures is the bad setting of relays, which occurred in the case of the 1965 Northeastern Blackout. The present practice favors dependability at the expense of security in that it ensures the isolation of a fault by allowing the tripping of unfaulted devices from time to time. However, this practice also contributes to the increasing risk of catastrophic failure in power system.

Chapter 4 Risk Assessment of Catastrophic Failures

4.1 Introduction

The U.S. electric system includes over 6,000 generating units, more than 500,000 miles of bulk transmission lines, approximately 12,000 major substations, and innumerable lower-voltage distribution transformers. Among them, the 115 kV and above extra-high voltage (EHV) network has 4000 buses; the total estimated number of relays is 6,000,000. Although relay hidden failure and catastrophic failure are rare events, the probability of these events is not negligible.

At this point, the question that arises is the following: where to reinforce the network in order to confine cascading failures to a small region? It is clear that the failures will propagate via the *weak links* in a system. Weak links may be defined as those lines of the network for which the probability of overloading and/or relay hidden failures is the largest; they are termed *hot spots* in the area of risk assessment and mitigation. This chapter will focus on the establishment of a risk assessment framework of power system catastrophic failures.

4.2 Hidden Failure Probability Evaluation

A hidden failure is defined to be "a permanent defect that will cause a relay or relay system to incorrectly and inappropriately *remove* a circuit element(s) as a direct consequence of another switching event" [5]. As implied by the definition, a hardware failure that results in the relay failing to operate a breaker and trip out a faulted line or device is not considered a hidden failure since redundant or backup protection or breaker failure systems must normally be provided for such a contingency.

The definition is based on the assumption that the protection system is designed for high dependability. However, if the primary protection system fails to detect a fault or send out a trip signal, and the backup protection (e.g. Zone-2 or Zone-3 or breaker failure protection) of the neighboring line(s) finally isolates the fault, there exists an undetected failure in the primary protection. Although this case is very rare, it can happen, and it has happened. Since cascading power system disturbances are also rare events, it is better to extend the definition of hidden failure to include such extreme cases and not to neglect their possibility. However, for the study in this dissertation, the above definition of hidden failure are strictly followed.

As is now well recognized, relay hidden failures contribute significantly to system cascading failure. The probability of relay hidden failure is the basis for the probability estimation of system failure. The following approach is proposed to estimate from historical data, the probabilities of relay hidden failures and systems failures. First, we need to group the relays into statistically homogenous classes with respect to their failure rates. Specifically, the relays are classified according to their type, their technology, and their age. The relay types are very diverse; they include overcurrent relays, distance relays, pilot relays, bus relays, and transformer relays, to cite a few; in addition, it is important to distinguish electromagnetic relays from solid state static relays and digital relays. Finally, age also matters because the failure rate during the debugging phase of a newly installed relay may be different from that of the mature operating phase and the wear out phase of this relay. The failure rate is expected to be high during the early and late operating periods and lower during the mature period of the relay. In other words, the reliability aging-curve of the relay has the well-known bathtub shape [64]. This may be especially true for the solid state static relays and digital relays.

Once the relay classification is performed, we may investigate a sample of relay-related events that have occurred in the U.S. transmission network. It is important that this sample, denoted by $\boldsymbol{S}$, be representative of the whole population of events. To this end, the events will be randomly selected. Obviously, they will have a broad range of degrees of severity. If the randomization is carried out properly, the sample $\boldsymbol{S}$ will thus include minor events that have little or no consequences, average events that have some impact, and extreme events with catastrophic implications. It is anticipated that the minor events form the bulk of system failures, while the catastrophic events are rare, since they have a very low probability of occurrence.

The probabilities of relay hidden failures are estimated as follows. Consider a given relay class, say the *i-th* class. Let n_i denote the total number of relays of that class involved in all the events of the sample S. Let m_i denote the total number of these relays whose hidden failures have been exposed. Then, an estimate of the probability p_i of hidden failures of the *i-th* relay class is defined as $p_i = m_i / n_i$.

Now, we intend to estimate the probability of occurrence of catastrophic system failures from the sample $\boldsymbol{S}$. To this end, we need to define a measure of severity for a system failure. Let X be such a measure. X may be defined as the cost in dollars suffered by the customers or the energy in MWh not delivered. X can be regarded as a random variable that takes a broad range of values, varying from zero to thousands of MWh (or millions of dollars). The probability distribution function of X may be estimated from the sample $\boldsymbol{S}$. Specifically, a histogram can be derived, and an empirical density function estimated from that sample. Hence, estimates of the probabilities of catastrophic events are given by the relative frequency of very large values of X. These probability estimates are very small and located in the tail of the probability density function.

The confidence intervals of the probabilities of both hidden failures and catastrophic system failures may be estimated by means of the nonparametric bootstrap method [79], [80]. Its main steps are outlined next.

4.2.1 The Nonparametric Bootstrap Method

The nonparametric bootstrap is a computationally intensive method that is based on the concept of sampling distribution. To explain this concept let us consider a parameter of a population probability distribution, γ, to be estimated by means of an estimator Γ using a sample drawn from that population. The sampling distribution of Γ can be thought of as the relative frequency distribution of all possible values taken by Γ calculated from an infinite number of random samples of finite size drawn from the population of the Γ values [79]. The estimate of this sampling distribution allows us to make inferences on the parameter γ.

The objective here is to estimate confidence intervals in which the true value of γ lies with a high probability.

While traditional parametric inference utilizes strong assumptions about the probability distribution of Γ, usually assumed to be normally distributed, the nonparametric bootstrap is distribution free, that is, no a priori distribution of Γ is made. The bootstrap method relies on the fact that the sampling distribution of Γ is a good estimate of the population distribution. How is this sampling distribution built? It is carried out by using Monte Carlo sampling, where a large number of samples of size n, called resamples, are randomly drawn with replacement from the original sample. Although each resample will have the same number of elements as the original sample, it may include some of the original data points more than once while some others are not included; therefore, each of these resamples will randomly depart from the original sample. In addition, because the elements in these resamples vary slightly, the statistic Γ^*, calculated from one of these resamples, will take on slightly different values. The central assertion of the bootstrap method is that the relative frequency distribution of these Γ^*'s an estimate of the sampling distribution of Γ.

The main steps of the nonparametric bootstrap procedure can be stated more formally as follows [79][80]. Consider a sample of values taken by a random variable, say the probability estimates previously defined. Let n be the size of this sample, called the original sample. Then, apply the following steps:

Step 1. From the original sample, draw M random samples of size n with replacement to obtain M resamples. The practical size of M depends on the statistical method to be applied to the sampling distribution. Typically, M is at least equal to 1000 when a confidence interval estimate of Γ is to be calculated.

Step 2. For each resample, calculate the statistic of interest, Γ^*. This may be the mean, the median, the mode estimator, or any other location or scale statistic.

Step 3. Order the M estimates of Γ^* by increasing values and assign a probability of $1/M$ to each of them. Identify the $[(1 - \alpha/2)\ M]$-*th* and the $[(\alpha/2)\ M]$-*th* quantiles of the sampling distribution, where α is a given level of confidence, say 0.95, and [x] denotes the largest integer smaller than the real number x. These quantiles are the lower and upper limits of the α-level confidence interval of the estimator Γ.

4.2.2 Probability of Relay Hidden Failure

By following the procedures presented in the previous section, the estimates of the probability of relay hidden failure can be based on the incomplete historical data of relay misoperations that have happened in a utility. The estimate criterion is that the resulting estimates of probability of relay hidden failure are unlikely to be underestimated. The conservatism has arisen from the fact that some information on relay misoperations is lacking. Unfortunately, since the estimate did not indicate the levels of conservatism that were used and there are no standards regarding the degrees of conservatism to follow, the risk assessors or risk managers may perform risk assessments inconsistently for different utilities. However, within the same system, by assuming the same probability of hidden failure for the same relay class, the estimates of risk for different areas may still be comparable.

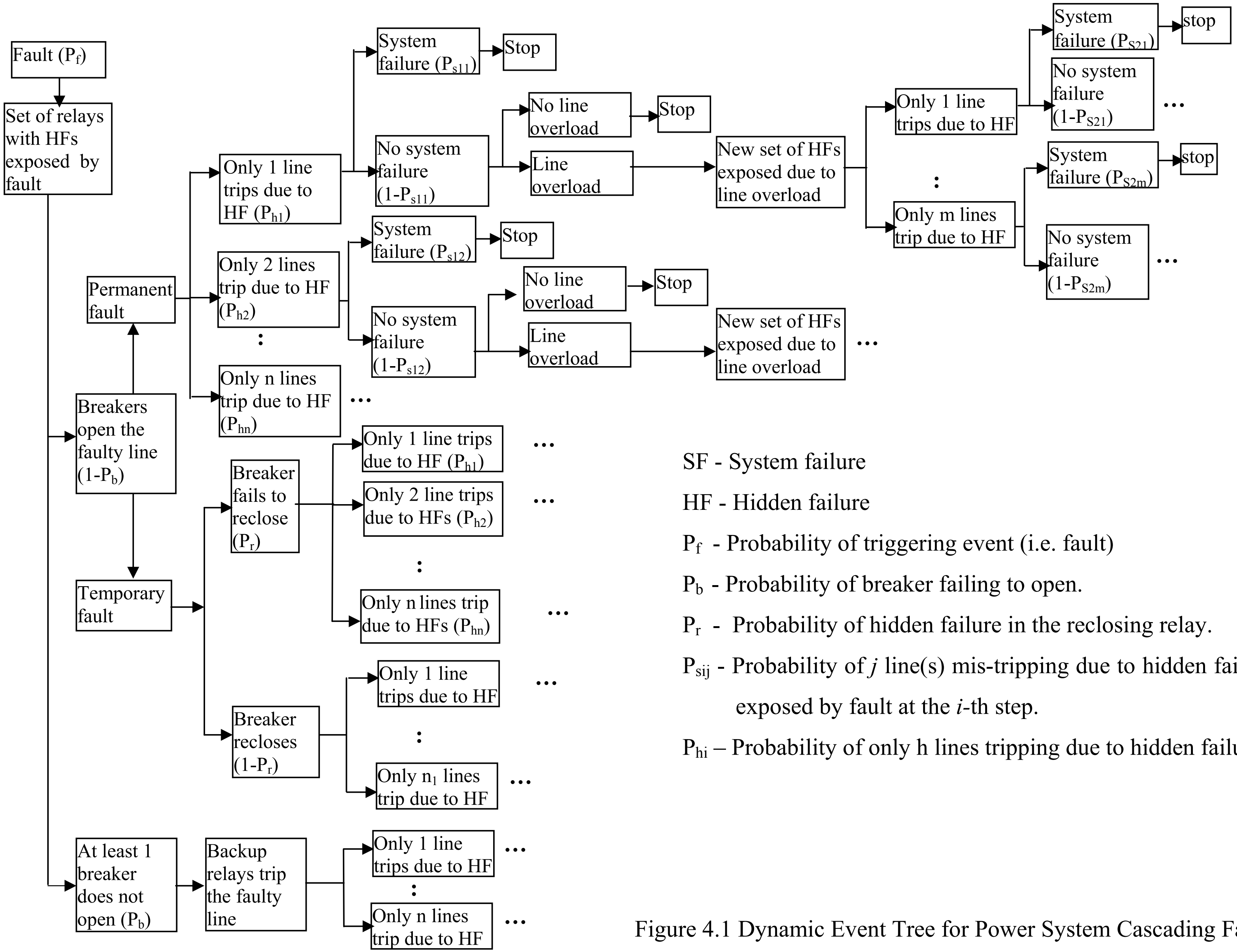
Many uncertainties contribute to the estimate errors of relay hidden failure probabilities. A lacking of statistical data is the main cause of the estimate errors. As more data and information are analyzed, uncertainty is reduced, and estimates become more accurate.

One disadvantage of the criterion is as follows: If the estimates of relay hidden failure probability are higher than they actually should be in order to overcome the uncertainties, the risks of some rare scenarios may be overestimated. However, since we are more concerned with the relative risks among different segments of the grid, the resulting estimates are still meaningful.

4.3 System Failure Probability Evaluation

In this section, a methodology is proposed for estimating the probabilities of catastrophic failures caused by hidden failures in the hardware or software components of the protection systems. A catastrophic failure is defined as the one that results in the outage of a sizable amount of load, say 10% of the peak load. It may be caused by dynamic instabilities in the system or the exhaustion of the reserve margins in transmission due to a sequence of line trippings leading to voltage collapse [81]. Only the static case of voltage collapse has been considered in this study.

The approach is based on a Dynamic Event Tree (DET) [82] introduced in section 2.4.3. The Dynamic Event Tree describes the probability of system failure (SF), that is, the probability of either load outages or voltage collapse. The triggering event is a short-circuit fault on a piece of equipment in the transmission network such as a line, a transformer, a bus, or a generator. The Dynamic Event Tree describing cascading outages due to a fault on a line, say line *i*, is depicted in Figure 4.1 and Figure 4.2. Figure 4.2 is an alternative version of the Dynamic Event Tree of Figure 4.1, and offers a succinct representation of the scenario. As shown in the DET, once the exposed relays are determined, the same procedure is followed to evaluate the probability of system failures, no matter what might cause the relays to be exposed. Hence, we can further reduce the size of the event tree by using the exposed relays as a constraint.



SF - System failure

HF - Hidden failure

P_f - Probability of triggering event (i.e. fault)

P_b - Probability of breaker failing to open.

P_r - Probability of hidden failure in the reclosing relay.

P_{sij} - Probability of *j* line(s) mis-tripping due to hidden failure exposed by fault at the *i*-th step.

P_{hi} – Probability of only h lines tripping due to hidden failure

Figure 4.1 Dynamic Event Tree for Power System Cascading Failures–I

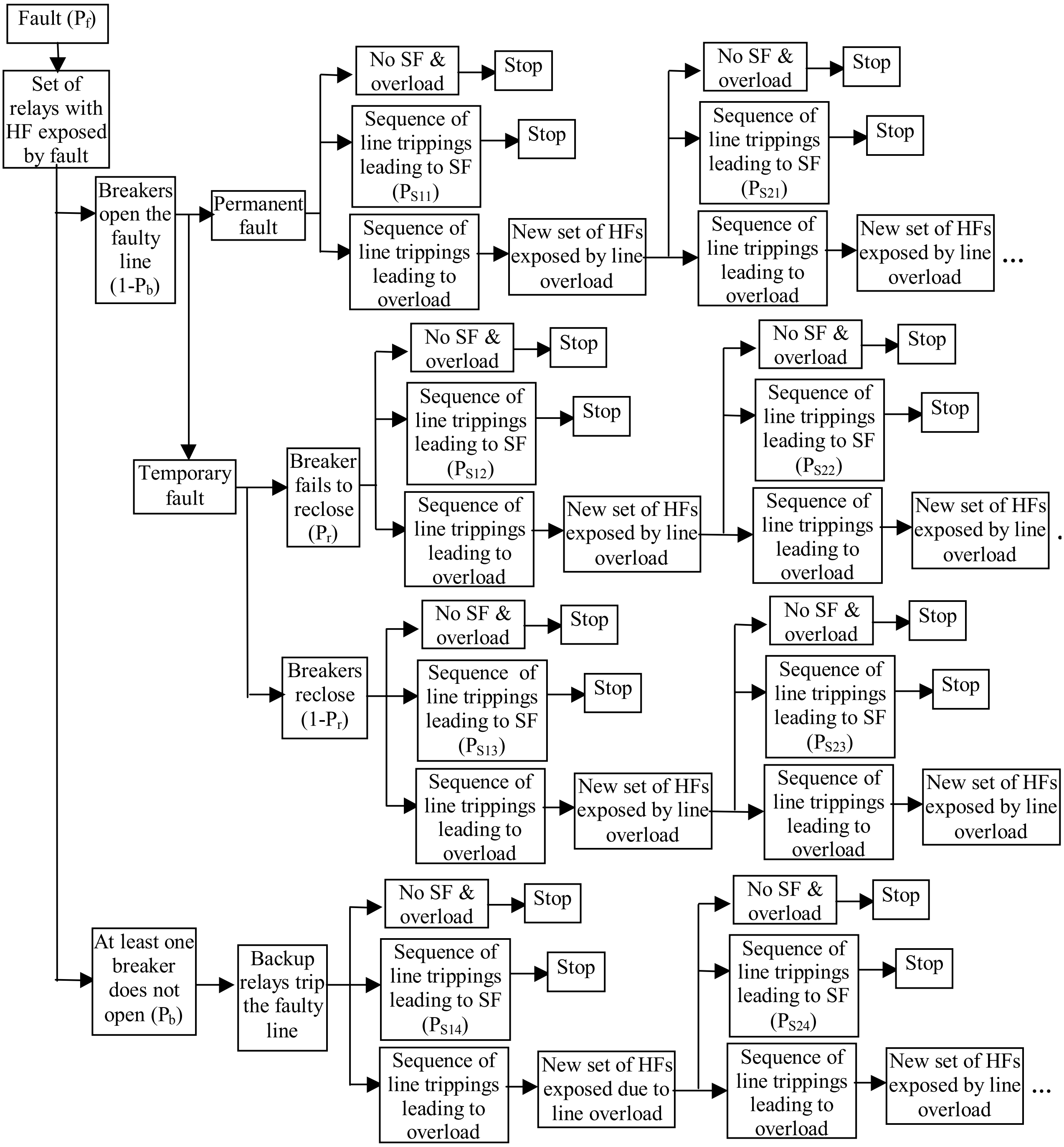


Figure 4.2 Dynamic Event Tree for Power System Cascading Failures – II

A Probabilistic Event Tree accounting for event probability has been developed to evaluate the probability of system failure based on the Dynamic Event Tree. As shown in Figure 4.3, there exist five levels in the Probabilistic Event Tree, which are "Trigger Event," "Breaker Status," "Fault Type," "Relay Reclosing Status," and "System Failure." Each branch in the probabilistic event tree will lead to a system failure (i.e. the end node of the tree). Therefore, the overall probability of system failure is the sum of all the probabilities of each branch. The system failure probability of one event branch in Figure 4.3 is the product of the probabilities of the five levels along the branch.

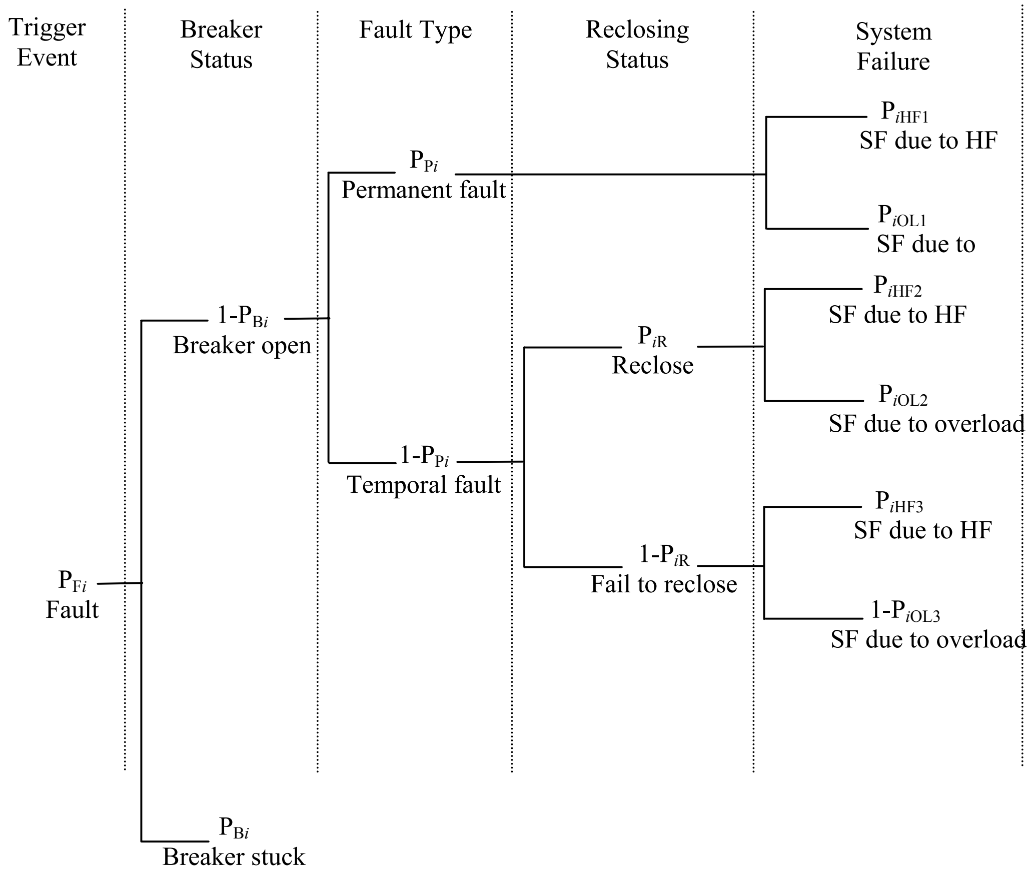


Figure 4.3 Probabilistic Event Tree

The probabilistic event tree consists of a collection of events and their associated probabilities that occur in the sequence as follows. First, the triggering event may be a permanent or a temporary short-circuit fault that affects one, two, or three phases with a probability $P_{Fi}(1 - P_{Bi})P_{Pi}$ and $P_{Fi}(1 - P_{Bi})(1 - P_{Pi})$, respectively. P_{Fi} is the probability of a fault, and this probability depends on the line length and environmental factors such as lightning frequencies, proximity of trees, etc… P_{Pi} is the conditional probability that the fault is permanent.

The normal practice to protect an EHV transmission line requires at least two different protection schemes. Several protection relays in different schemes at the faulty line will send tripping signals to the associated circuit breakers once a fault occurs on a line. Therefore, the circuit breakers on the faulty line should open to clear the fault. Although the probability that the circuit breaker fails to operate is very small, the circuit breaker may remain stuck in a closed position [74] and fail to open with a conditional probability P_{Bi} as shown in Figure 4.3. In this scenario, the breaker failure relay will send a transfer tripping signal to the neighboring relays to isolate the fault with a very high probability, which may be assumed to be one.

In the event of a temporary fault, the breakers should reclose after a brief instant, an event that may fail to occur with a conditional probability P_{Ri}. This claim is based on the statistical study of relay and circuit breaker misoperations conducted at a U.S. utility by the IEEE/PSRC working group 13 and reported in [74]. This study revealed that seven breakers failed to reclose on temporary faults over a one-year period, and the failures accounted for 14.6% of the total misoperations.

In addition to the relays of the faulty line, other relays may also sense the fault current. Unlike the former relays, the latter should not open the lines under their control unless the relays on the faulty line fail to isolate the fault in time; however, one or several of them may each suffer from a hidden failure (HF) with a small probability P_{Hi} and thereby trip the associated non-faulty line. This sequence of line trippings may result in either a system failure or line overloads.

The short-circuit current exposes the hidden failures of all the relays whose zones of vulnerability include the faulty line. If there are k exposed hidden failures, their associated lines will trip with a probability. Now, these line trippings will change the pattern of the power flow in the system and thereby may induce the overload of a certain number of lines in the system. When the overload is large enough, the relay hidden failures of the overloaded lines will be exposed, and the associated lines will trip. In this case, another sequence of line trippings due to relay hidden failures may lead to system failure or more line overloads and so forth. This sequence of line trippings may continue until a major system failure such a brownout or a blackout occurs as typified by the 1977 New York Blackout described in Chapter 3.

Based on the Probabilistic Event Tree, the probability of system failure due to a triggered event *i* can be evaluated as follows:

$$P_{Si} = P_{Fi}\,(1\text{-}P_{Bi})\ \{P_{Pi}\,(P_{HPi} + P_{LPi}) + (1\text{-}\ P_{Pi})\ [P_{Ri}\ (\ P_{HTNi} + P_{LTNi}) + (1\text{-}\ P_{Ri})\ (P_{HTRi} + P_{LTRi})]\} \qquad (1)$$

where

P_{Bi} : Probability that a circuit breaker of the faulty line *i* does not open in time

P_{Ri}: Probability that the circuit breakers of the faulty line *i* do not reclose following a temporary fault

P_{HPi} : Probability of system failure due to relay hidden failure given the occurrence of a permanent fault

P_{HTNi}: Probability of system failure due to relay hidden failure given the occurrence of a temporary fault and the non-reclosing of the faulty line

P_{HTRi}: Probability of system failure due to relay hidden failure given the occurrence of a temporary fault and the successful reclosing of the faulty line

P_{LPi}: Probability of system failure due to line overloads given the occurrence of a permanent fault

P_{LTNi}: Probability of system failure due to line overloads given the occurrence of a temporary fault and the non-reclosing of the faulty line

P_{LTRi}: Probability of system failure due to line overloads given the occurrence of a temporary fault and the reclosing of the faulty line

Let us now derive the expression of the probability of system failures given a permanent fault, which is denoted by P_{HPi}. To this end, let us define S_C as the set of all sequences of line outages leading to system failure due to hidden failures exposed by the short-circuit current. Let us also define P_j as the probability of the j-th sequence. Then, we have

$$P_{HPi} = \sum_{j \in S_c} P_j \qquad S_C = \{S_{C1}, S_{C2}, \ldots, S_{Ck}\} \tag{2}$$

The probability P_j is the product of: (i) the probabilities $\{p_m$ for all m $\in S_{CTj}\}$ of all tripped lines in the j-th failure mode leading to system failure, and these tripping lines form the subset S_{CTj} of S_{Cj}; (ii) the probabilities $\{(1-p_n)$ for all n $\in \overline{S}_{CTj}\}$ of all the remaining lines that do not trip, and these in-service lines form the subset $\overline{S}_{CTj}$ of S_{Cj}. Hence, we have

$$P_j = \prod_{m \in S_{CTj}} p_m \prod_{n \in \overline{S}_{CTj}} (1 - p_n) \tag{3}$$

where

$$S_{Cj} = S_{CTj} \cup \overline{S}_{CTj} \tag{4}$$

Detailed explanation on probability evaluation of the system failure is illustrated by a 7-bus test system in Appendix C. In this demonstration, for each trigger event, we evaluated the probabilities of different combinations of exposed relay hidden failure modes leading to system failures.

Similarly, we can derive the expressions of P_{HTNi} and P_{HTRi} as well as the expressions of the probabilities of system failure due to line overloads, P_{LPi}, P_{LTNi}, and P_{LTRi}. For example,

$$P_{LPi} = \sum_{j \in S_L} P_j \qquad S_L = \{S_{L1}, S_{L2}, \ldots, S_{Lk}\} \tag{5}$$

where
$$P_j = \prod_{m \in S_{LTj}} p_{ml} \prod_{n \in \bar{S}_{LTj}} (1 - p_{nl}) \tag{6}$$

and
$$S_{Lj} = S_{LTj} \cup \bar{S}_{LTj} \tag{7}$$

Here, S_{Lj} *i*s the set of sequence of line events leading to system failure due to hidden failures exposed by line overloads, and S_{LTj} is the subset of S_{Lj} that consists of all tripped lines in the *j*-th failure mode leading to system failure. In addition, p_m denotes the probability that Line m trips due to a hidden failure exposed by line overloads.

For a large power system, it is a formidable task to evaluate the probability of system failure induced by a fault on every branch of the network; therefore, a fast screening method must be used beforehand to identify the regions of the network that may include weak links. The search can then concentrate only on the identified areas with the smallest reserve margins in transmission and/or generation. Note that the *weak links* are the *minimal cut sets* of the event tree, in that they lead to system failure with the smallest number of line trippings, implying that they lead to the highest probabilities of system failure.

Once the probability of system failures has been evaluated, it is important to assess the system failure significance (i.e. risk index) that accounts for both the probability and severity of a system failure, which is defined as

$$R_i = P_i * S_i * w_i \tag{8}$$

where

R_i: Risk Index for *i*-th trigger event

P_i: Probability of system failure due to *i*-th trigger event.

S_i: Severity Index for system failure due to *i*-th trigger event.

w_i: Weighting factor, which is used to account for the importance of loss load, loss of key substation, or other stability issues

Different system failures have different consequences. The severity of system failure can be represented by either the number of customers disconnected, the amount of power curtailed, the amount of energy non-delivered, or the amount of dollars lost by the customers. We denote this by so-called Severity Index (S_i), which is a measure of severity of system failure. This severity index should account for various factors that a utility should deal with. In the analysis, we may just simply weight the loss of power in MW. The weight coefficient accounts for the relative importance of a tripped load or a disconnected substation. Obviously, hospitals, governmental buildings, and major industries should be assigned more weight than residential customers.

4.4 Implementation of Risk Assessment of Catastrophic Failures

Based on the foregoing methodology, a package of software programs has been developed that includes a continuation power flow program, a short-circuit program, a power flow program, and a probability calculation program. The probabilities of relay hidden failures as well as the power generations and loads at all buses are given as inputs to the program. Only the power system's steady stability is investigated to indicate if a system failure occurs or not. In Chapter 6, the uncertainties of power generation and loads will be accounted for. These programs are run sequentially as depicted in Figure 4.4.

In the first step, the continuation power flow program is executed to rank the load buses by increasing reactive reserve margins to voltage collapse. The rank allows us to identify the heavily loaded regions of the system with the smallest reserve margins. Obviously, the incident branches to those load buses with the smallest reactive reserves are probably going to be weak links in the system with respect to voltage collapse. Cascading failures in these regions are likely to occur with the highest probability since few line trippings due to relay hidden failures may result in the disconnection of large segments of the loads.

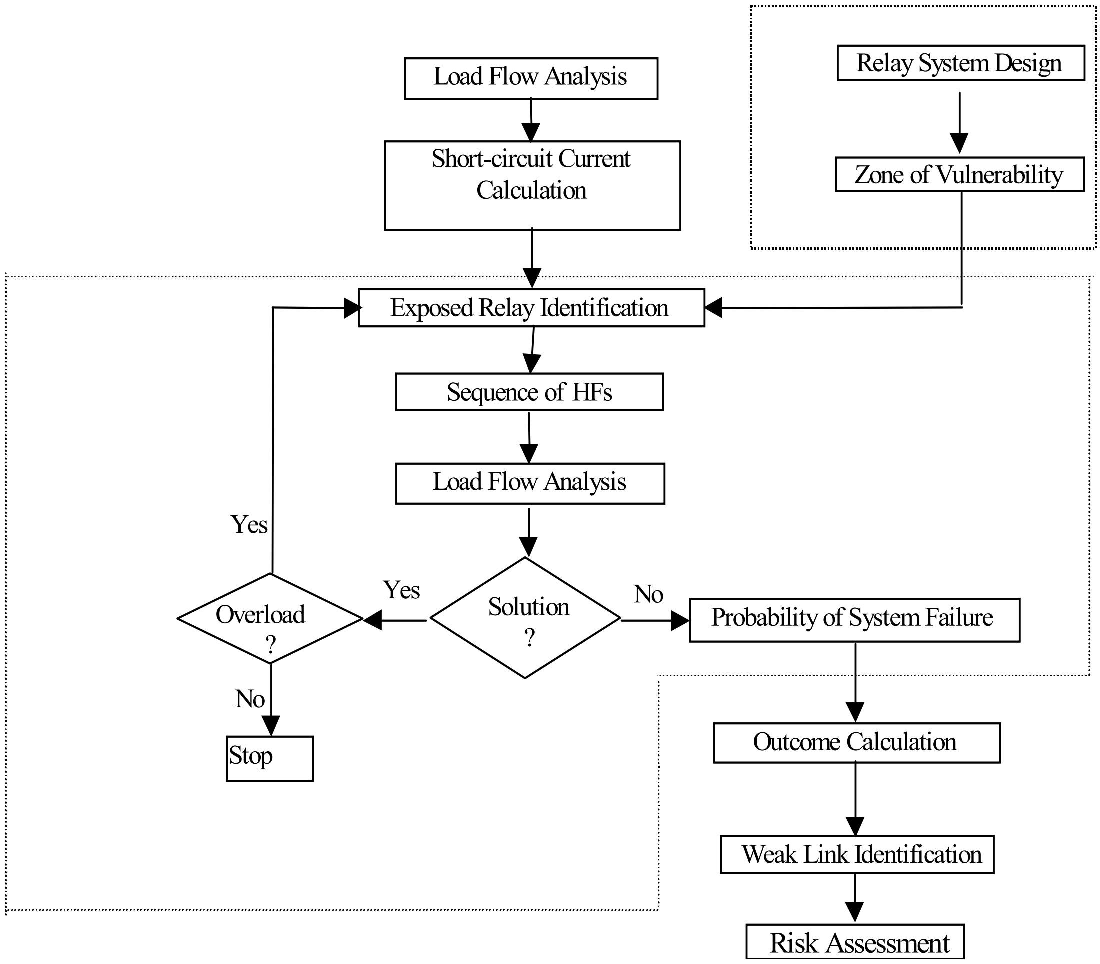


Figure 4.4 Flowchart for Risk Assessment Algorithm of Catastrophic Failure

In the second step, a three-phase short-circuit is applied sequentially to every branch of these regions, and in each case, all those relays that are seeing a large short-circuit current are pinpointed via the short-circuit program; then, these fault currents are compared with the pickup settings of the overcurrent relays. If the magnitude of a fault current exceeds the pickup setting of an overcurrent relay, then the relay is said to be exposed to relay hidden failure, and a hidden failure probability is assigned to the relay. For every combination of relay trippings, all the lines that become heavily overloaded are singled out through the load flow program. The hidden failures of their relays may be exposed, resulting in the tripping of another set of lines, and so forth. This sequence of events continues until either a sufficiently large amount of load is being disconnected or a voltage collapse has occurred. In the last step, the probability of system failure is calculated. The flowchart for probability calculation of system failure is given in Figure 4.5.

The implemented procedures include the following steps:

1) Run the continuation power flow program to calculate the reactive reserves at every load bus of the studied system
2) Apply a short-circuit to a branch within a region having the smallest reactive reserve
3) Run the short-circuit program to identify all exposed relays
4) Form the combinations of line trippings due to the exposed relay hidden failures
5) For each combination of line tripping, calculate the amount of load that is shed due to bus isolation or system separation. If the loss of load is larger than a given threshold, label the case as system failure and go to Step 8; otherwise continue
6) Run load flow program to check if the load flow converges; if the load flow does not converge, go to Step 8; otherwise continue
7) If the load flow converges, check to determine whether there are any overloaded lines. If the answer is positive, establish the new set of line tripping combinations due to the exposed relay hidden failures and go back to Step 4; if not, go to Step 10
8) Compute the probability of the system failure
9) Compute the risk associated with this tripping sequence
10) Check to determine if all the combinations of line tripping have been exhausted. If the answer is negative, repeat Steps 4-9; otherwise go to Step 2 to evaluate next fault location
11) Output the results.

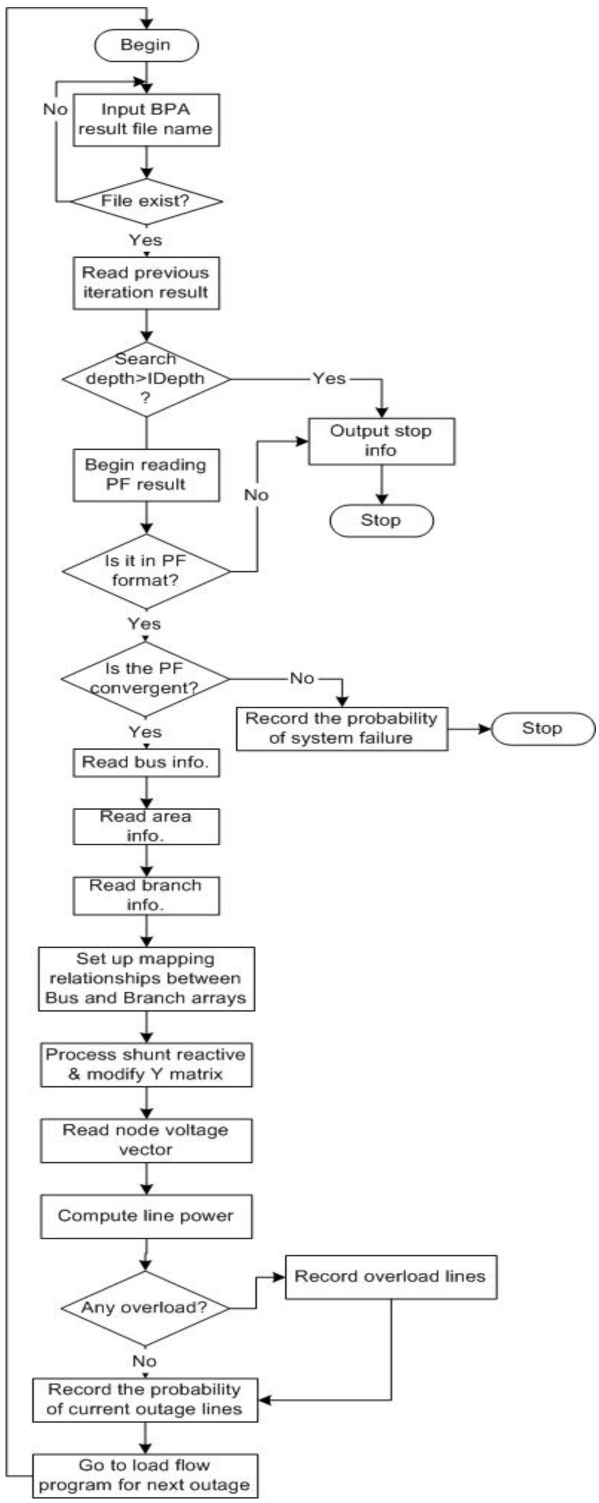


Figure 4.5 System Failure Probability Calculations

4.5 The Continuation Power Flow Method

Due to the considerable burden of conducting load flow study of huge numbers of combinations of line trippings, instead of considering all the possible trigger events in a system, the continuation power flow method provides a powerful vehicle to identify the most vulnerable areas that may lead to catastrophic failures in a system.

As a first screening, a Continuation Power Flow (CPF) program is executed to identify the regions that have the smallest reactive reserves in the system. Starting from a power flow solution, say at peak load, the CPF algorithm traces the power flow solution curves as the reactive power injections of the load buses are increased up to the saddle-node bifurcation point (refer to Figure 4.6) [83][84]. The latter is defined as the point where the power flow Jacobian matrix becomes singular, also termed the point of voltage collapse.

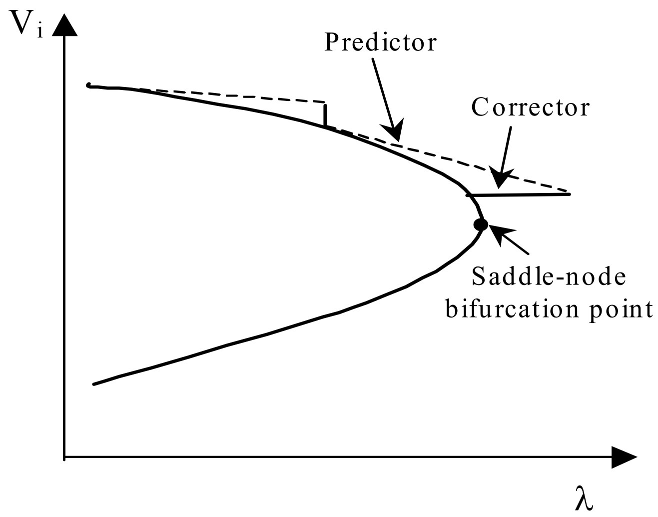


Figure 4.6 Predictor-Corrector Scheme

Several continuation schemes have been proposed in the literature for power system applications [84]-[86]. In this research project, we have used the predictor-corrector scheme initiated by Kubicek [87] in conjunction with the local parameterization method proposed in [88] for the prediction step. As depicted in Figure 4.6, the predictor finds a point along the tangent of the V-Q curve in the direction of the saddle-node bifurcation point, while the corrector uses this point as an initial condition to seek, via a Newton-Raphson algorithm, a solution to a set of parameterized power flow equations. The latter are expressed as

$$P_{Gi} - P_{Li} - P_i = 0 \text{ and } Q_{Gi} - Q_{Li} - Q_i = 0, \text{ for } i = 1, \ldots, N, \tag{9}$$

where the subscripts G and L stand for generator and load, respectively, and P_i and Q_i are the real and reactive power flows through the lines incident to Node i. In the prediction step, a load reactive power Q_{Li} injected into Node i is increased from an initial value, Q_{Li0}, via a load parameter λ and a load factor k_{Li} according to

$$Q_{Li} = Q_{Li0} + \lambda\, k_{Li}\, \Delta Q. \tag{10}$$

If $F(z) = 0$, with $z^t = [\theta^t, V^t, \lambda]$, denotes the foregoing set of parameterized equations, then the prediction of the next solution along the tangent vector $dz^t = [d\theta^t, dV^t, d\lambda]$ is the solution to $(\partial F / \partial z)\, dz = 0$. By expanding the Jacobian matrix $\partial F / \partial z$ with one additional row vector e_k, whose elements are all equal to zero except for the *k-th* element, which is equal to 1, we get a square nonsingular matrix that can be inverted to solve for the tangent vector dz in

$$\begin{bmatrix} \partial F / \partial z \\ e_k \end{bmatrix} dz = \begin{bmatrix} 0 \\ \pm 1 \end{bmatrix}. \tag{11}$$

Here, the k-th element of dz is set to -1 or +1 depending on whether the point of voltage collapse has been passed or not. The associated state variable z_k is called the continuation parameter because, during the correction phase, it will be fixed to its predicted value. Now which of the entries of z is picked as the continuation parameter? Obviously, it is the one that has the largest rate of change around the corrected solution, that is, the one that has the largest absolute component of the tangent vector, dz.

4.6 Summary

One of the objectives of this study is to develop a methodology together with a set of software programs that calculate, in a power system, the probabilities of catastrophic failures caused by hidden failures in the hardware or software components of the protection systems.

The programs consist of a continuation power flow program, a short-circuit program, a power flow program, and a probability calculation program. These programs are run sequentially as follows. In the first step, the continuation power flow program is executed to identify the heavily loaded regions of a system with the smallest reserve margins. Cascading failures in these regions are likely to occur with the highest probability since few line trippings due to relay hidden failures may result in the disconnection of large segments of load. In the second step, a three-phase short-circuit is applied sequentially to every branch of these regions, and in each case, all those relays detecting a large short-circuit current are pinpointed via the short-circuit program. Then, for every combination of relay trippings, all the lines that become overloaded are singled out through the load flow program. The hidden failures of their relays may be exposed, resulting in the trippings of another set of lines, and so forth. This sequence of events continues until either a sufficiently large amount of load is being disconnected or a voltage collapse has occurred. In the latter case, the load flow Jacobian matrix is singular. In the last step, the probability of system failure is calculated.

Chapter 5 Simulation Results

5.1 WSCC Sample System Overview

The one-line diagram of the WSCC 179-bus sample system is shown in Figure 5.1. The detailed data is listed in Appendix D. In this system, there are 29 generators, 179 buses, 246 transmission lines at 110kV and above, and 53 transformer branches, with a generation of about 61400 MW. After being eliminated all the buses dividing a line into different segments in the input data, the 179-bus WSCC system is reduced to a system with 126 buses and 162 branches. The total load is 60785 MW, and the system loss is 615 MW.

Since the severity of a system failure depends heavily on the load and generation profiles that are considered, a large sample of these operating conditions should be investigated. Production simulation methods may be used to solve this problem. A much simpler method would be to consider only different load-generation profiles as listed in Table 5.1. To be more specific, we carry out the study for two seasons, namely, the summer and the winter seasons, which have significant differences with respect to the load-generation profile. For each season, three load conditions (most frequent load, peak load, and off-peak load) will be selected, and three different generation profiles under each load condition will be considered. Hence, for each year, a total of 18 cases will be evaluated. This should cover a broad range of operating conditions of the system under study.

Table 5.1 Load-Generation Profiles

Load profile	Generation profile	Load profile	Generation profile
Summer		Winter	
Peak Load	Normal case	Peak Load	Normal case
	Worst case		Worst case
	Alternative case		Alternative case
Off-Peak Load	Normal case	Off-Peak Load	Normal case
	Worst case		Worst case
	Alternative case		Alternative case
Most frequent Load	Normal case	Most frequent Load	Normal case
	Worst case		Worst case
	Alternative case		Alternative case

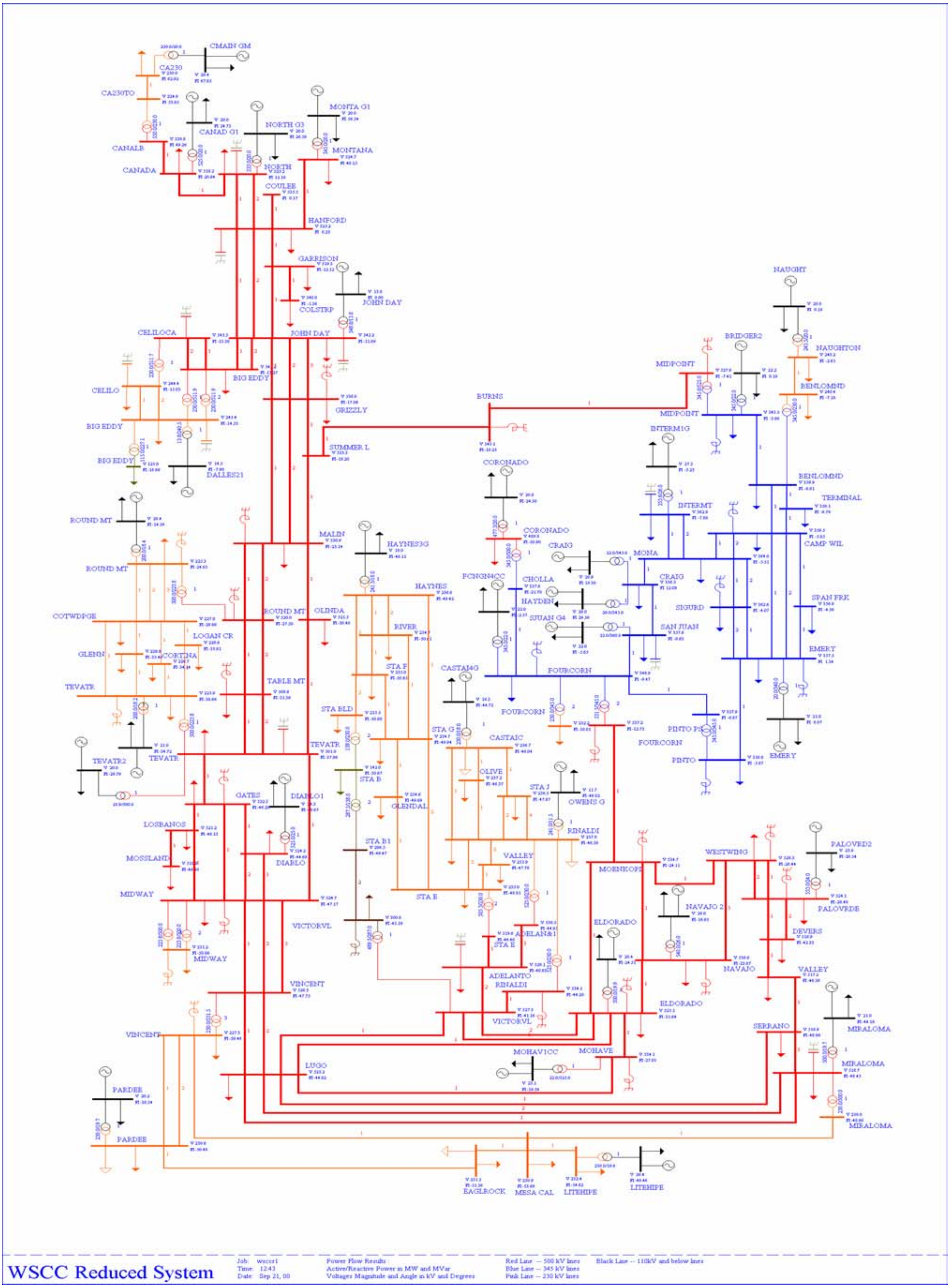


Figure 5.1 One-line Diagram of the WSCC 179-Bus Sample System

Once we obtain the system failure probabilities for each of these different cases, we can combine them to get a more robust estimation of the system failure probabilities.

There are two common types of input signals used by relay schemes. One is voltage; the other is current magnitude. Since there are many different relaying schemes in transmission systems, for the sake of simplicity, only the third zone distance relay is being considered in the relay hidden failure and system failure investigation.

There are two assumptions for the Zone-3 relay scheme:

1) Zone-3 relays can only sense the fault forward
2) The setting of the Zone-3 is to cover the entire line plus 1.2 of the longest line behind the remote bus.

5.2 Simulation Results Obtained on the California 61-bus Subsystem

For demonstration purposes, the software programs that implement the proposed methodology have been applied to the California subsystem of the WSCC 179-bus reduced system. Its one-line diagram is sketched in Figure 5.2. This subsystem includes 61 buses and 83 branches at voltage levels of 500kV, 230 kV, and 110 kV, and serves a total load of 21,576 MW. The main area of this sub-network is the tightly connected Los Angeles area that is comprised of 41 buses and 52 branches. The major tie lines include the California-Oregon Intertie (COI) from Malin to Round Mountain (Olinda) to Table Mountain to Tevatra, and down south to Vincent in the Los Angeles area. Los Angeles also connects to Las Vegas through three 500kV lines from Victorville/Lugo to Eldorado and one 500kV tie line from Denvers to Palo Verde in Arizona.

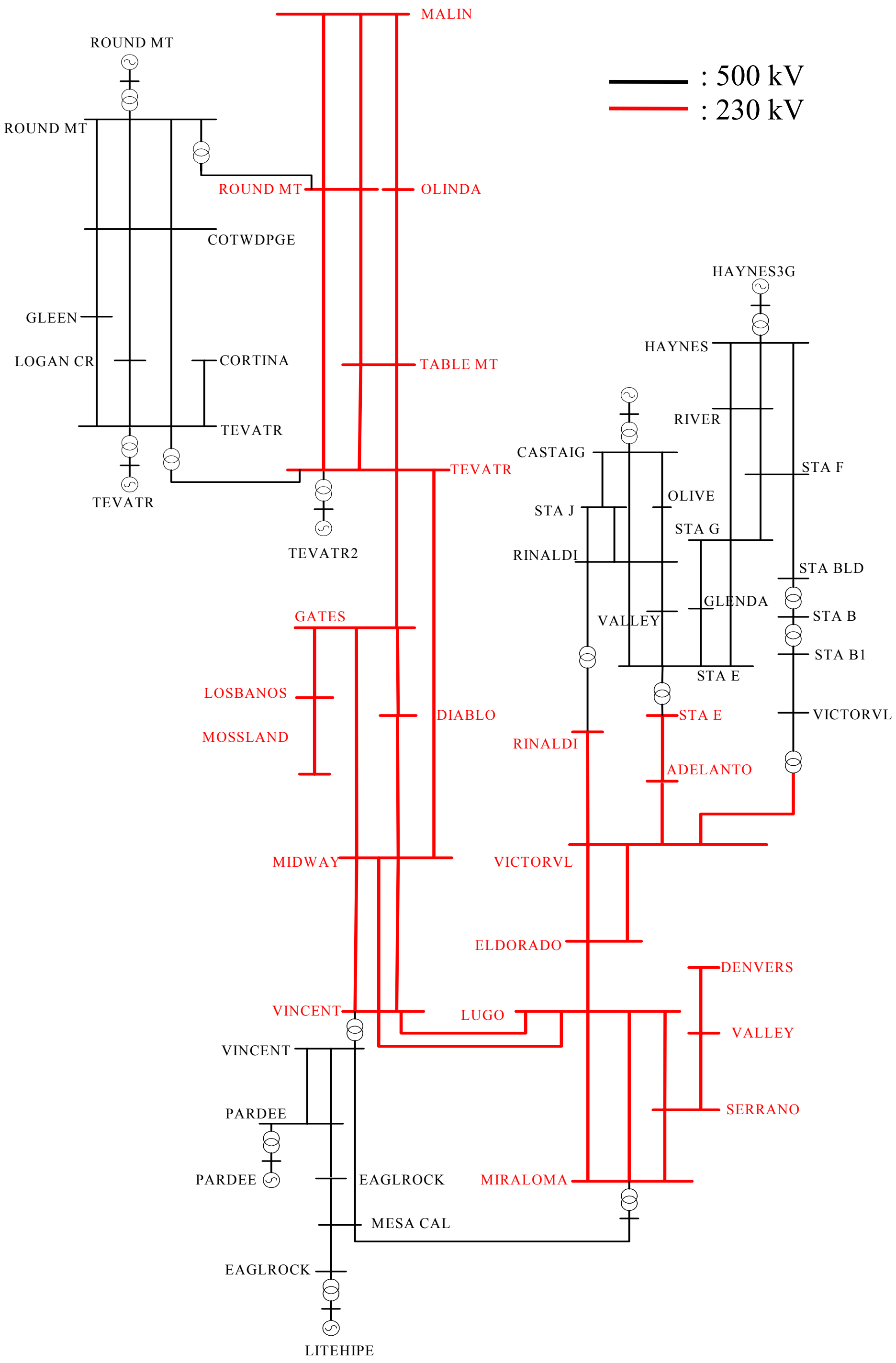


Figure 5.2 One-line Diagram of the California Sub-System

The objective here is to assess the risk of catastrophic failure of this subsystem. A major failure is defined as being either a loss of a large amount of load, say larger than 400 MW, or a voltage collapse. To this end, the continuation power flow was first executed sequentially at each of the 34 load buses of the subsystem to assess their respective reactive power margins to voltage collapse. We may rank the load buses by increasing reserve margins, and identify the regions of the network that may include weak links.

As an example, Figure 5.3 displays the Q-V curve of Bus 34, named Cortina 200, whose reactive reserve was found to be equal to 395 MVar. The reserve margins grouped by voltage level while being ordered by ascending magnitude are listed in Table 5.2. In other words, for every voltage level, the buses with the smallest reserves are located at the top of the list; therefore, the areas in their vicinities are likely to include the weak links of the subsystem.

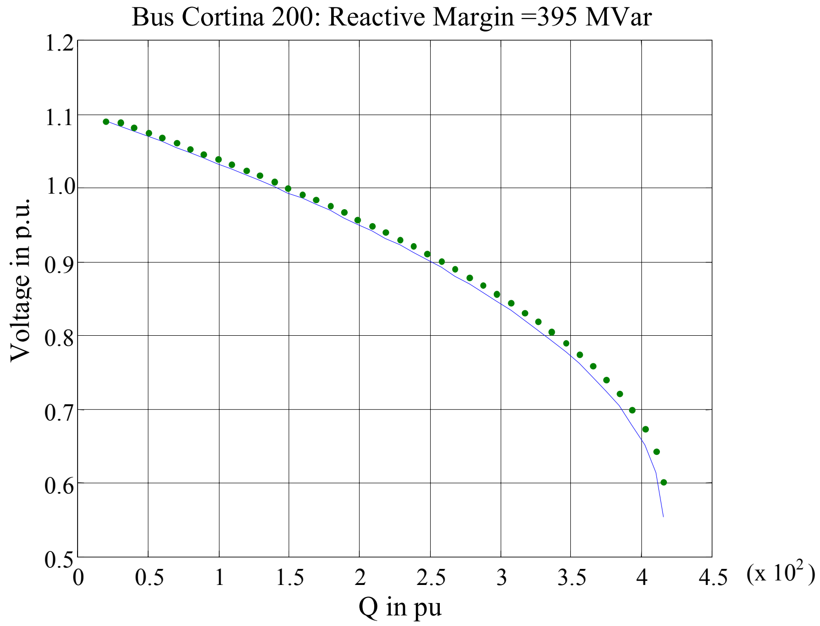


Figure 5.3 Q-V Curve at Bus 34 (Cortina 200)

Table 5.2 Voltage Stability Margins at the Load Buses of the California Sub-System

Bus No.	Bus Name	Voltage (kV)	Base case ($x10^2$MW, $x10^2$MVar)	Margin ($x10^2$MVar)	Margin from the Base Case ($x10^2$Mvar)
44	LUGO	500	-9.07+j0.952	8.35	7.40
31	VALLEY	500	4.06+j0.41	11.50	11.09
6	LOSBANOS	500	2.65+j0.14	17.80	17.66
13	ROUND MT	500	-19.2-j0.94	19.50	20.44
30	SERRANO	500	12.3+j0.728	28.50	27.77
36	ADELANTO	500	-18.62+j0.59	29.90	29.31
27	VICTORVL	500	0.0+j0.0	31.50	31.50
3	GATES	500	3.05+j0.834	33.00	32.17
18	TEVATR	500	56.61+j19.91	66.10	46.19
24	MIRALOMA	500	30.98+j7.89	60.10	52.21
26	VICTORVL	287	-1.69+j1.402	10.15	8.75
53	STA BLD	230	1.38+j0.28	13.45	13.17
43	EAGLROCK	230	1.75+j 0.18	15.60	15.42
56	STA F	230	1.17+j0.24	17.20	16.96
49	RIVER	230	3.2+j0.65	18.40	17.75
40	GLENDAL	230	1.35+j0.2	19.05	18.85
57	STA G	230	1.21+j0.25	20.90	20.65
61	VALLEY	230	2.052+j0.176	23.80	23.62
45	OLIVE	230	-0.728-J0.17	24.10	24.27
54	STA E	230	8.078+j1.321	26.10	24.78
22	MESA CAL	230	3.774+j0.645	25.60	24.96
58	STA J	230	8.877-j0.062	27.60	27.66
33	VINCENT	230	10.66+j1.79	34.50	32.71
47	RINALDI	230	1.21+j0.25	35.30	35.05
59	SYLMARLA	230	-27.71-j4.92	30.80	35.72
60	SYLMAR S	230	4.01+j0.806	37.00	36.19
29	PARDEE	230	31.18+j0.78	41.10	40.32
20	LITEHIPE	230	31.91+j6.3	73.40	67.10
34	CORTINA	200	-0.443+j0.2	4.15	3.95
35	COTWDPGE	200	2.104-j0.77	10.70	11.47
12	ROUND MT	200	1.48+j1.18	21.00	19.82
16	TEVATR	200	8.84+j0.868	32.50	31.63
8	MIDWAY	200	7.776+j1.626	37.25	35.62
50	STA B	138	2.372-j0.632	10.00	10.63

As a second step of the method, based on the ranked list, we may carry out multiple-contingency analysis on the buses and incident lines with the smallest reserve margins of the California subsystem. Here, a three-phase short circuit is applied, and a short-circuit calculation is carried out for every incident line. This calculation allows us to identify the exposed relay hidden failures, which are listed in the third column of Table 5.3.

Let p_f denote the probability of a three-phase short-circuit on a given branch, and let p denote the probability of an exposed relay hidden failure that will trip the associated line, where q is the probability of an exposed line that will not trip ($q = 1 - p$). For $p_f = 10^{-3}$, and $p = 10^{-4}$, the probabilities of catastrophic failure are calculated. Table 5.3 lists the probability of catastrophic failure due to faults on major 500kV transmission lines in California.

It is observed that the probabilities range from 10^{-3} to 0. As shown in the table, if there is three-phase short-circuit fault on the lines of MALIN – OLINDA or OLINDA – TEVATR, the probability leading to catastrophic failure may be as high as 10^{-3}; if the fault happens on the lines of GATES – LOSBANOS or GATES – DIABLO, it will not cause catastrophic failure in the system. Note that all but Cases 10, 14, and 15 lead to voltage collapse. Case 10 results in a loss of load of 1230 MW, and neither Cases 14 nor Case 15 leads to a catastrophic failure. It is observed that the weak links of the California subsystem are the first eight branches listed in Table 5.3, since the highest probabilities of voltage collapse are associated with them. It turns out that the first seven of these branches are tie lines of the California subsystem, five of them being heavily loaded. Based on the probability index, we may find the weak link in the studied system.

Table 5.3 Probability of Voltage Collapse

(Fault on major 500kV transmission lines)

No	Faulty Line	Lines with Exposed Relay HFs		Probability of Voltage Collapse	Probability of VC for $p_f = 10^{-3}$, $p=10^{-4}$.
1	MALIN - OLINDA	MALIN GRIZZLY GRIZZLY MALIN MALIN	SUMMER L MALIN (1) MALIN (2) ROUND MT (1) ROUND MT (2)	$p_f(1-3pq^4)$	$\approx 10^{-3}$
2	OLINDA - TEVATR	TEVATR GATES TABLE MT TABLE MT MALIN	MIDWAY TEVATR TEVATR (1) TEVATR (2) OLINDA	$p_f(1-q^5)$	$\approx 10^{-3}$
3	TABLE MT - TEVATR (1)	ROUND MT ROUND MT TABLE MT GATES MIDWAY OLINDA	TABLE MT (1) TABLE MT (2) TEVATR (2) TEVATR TEVATR TEVATR	$p_f(p+pq+p^2q^2+p^2q^4)$ $\approx p_f p\,(1+q)$	$\approx 2\text{x}10^{-7}$
4	MALIN - ROUND MT (1)	MALIN ROUND MT ROUND MT GRIZZLY GRIZZLY MALIN MALIN	ROUND MT (2) TABLE MT (1) TABLE MT (2) MALIN (1) MALIN (2) SUMMER L OLINDA	$p_f(p+pq+p^2q^2(1+2p^2-p^3))$ $\approx p_f p\,(1+q)$	$\approx 2\text{x}10^{-7}$
5	TEVATR - MIDWAY	OLINDA TABLE MT TABLE MT GATES MIDWAY MIDWAY MIDWAY MIDWAY MIDWAY MIDWAY MIDWAY	TEVATR TEVATR (1) TEVATR (2) TEVATR DIABLO (1) DIABLO (2) GATES LOSBANOS VINCENT (1) VINCENT (2) VINCENT (3)	$p_f(p+pq+p^2q^2+p^4q^4+ p^6q^5)$ $\approx p_f p(1+q)$	$\approx 2\text{x}10^{-7}$
6	TEVATR - GATES	TEVATR TABLE MT TABLE MT TEVATR GATES GATES GATES	OLINDA TEVATR (1) TEVATR (2) MIDWAY LOSBANOS MIDWAY DIABLO	$p_f(p+pq+p^2q^2)$ $\approx p_f p\,(1+q)$	$\approx 2\text{x}10^{-7}$
7	ROUND MT - TABLE MT (1)	MALIN MALIN TABLE MT TABLE MT ROUND MT	ROUND MT (1) ROUND MT (2) TEVATR (1) TEVATR (2) TABLE MT (2)	$p_f(p+p^2q+p^2q^3)$ $\approx p_f p$	$\approx 10^{-7}$

No	Faulty Line	Lines with Exposed Relay HFs		Probability of Voltage Collapse	Probability of VC for p_f $=10^{-3}$, $p=10^{-4}$.
8	MIRALOMA - SERRANO	SERRANO SERRANO MIRALOMA MIRALOMA	VALLEY LUGO LUGO (1) LUGO (2)	$p_f(p+p^2q)$ $\approx p_f p$	$\approx 10^{-7}$
9	VALLEY - DEVERS	DEVERS DEVERS VALLEY	PALOVRDE (1) PALOVRDE (2) SERRANO	$p_f p^2$	$\approx 10^{-11}$
10	SERRANO - VALLEY	VALLEY SERRANO SERRANO	DEVERS LUGO MIRALOMA	$p_f p^2$	$\approx 10^{-11}$
11	VINCENT - LUGO (1)	VINCENT (1) VINCENT (2) VINCENT (3) LUGO LUGO LUGO LUGO LUGO LUGO	MIDWAY MIDWAY MIDWAY VINCENT (2) ELDORADO MIRALOMA (1) MIRALOMA (2) SERRANO MOHAVE	$p_f(p^3+p^3q)$	$\approx 2\text{x}10^{-15}$
12	DIABLO - MIDWAY (1)	DIABLO DIABLO MIDWAY MIDWAY MIDWAY MIDWAY MIDWAY MIDWAY	MIDWAY (2) GATES LOSBANOS GATES TEVATR VINCENT (1) VINCENT (2) VINCENT (3)	$p_f(p^3+p^4q+p^3q^2+p^3q^2)$ $\approx p_f P^3$	$\approx 10^{-15}$
13	MIDWAY – VINCENT (1)	MIDWAY MIDWAY LOSBANOS GATES DIABLO DIABLO TEVATR LUGO LUGO	VINCENT (2) VINCENT (3) MIDWAY MIDWAY MIDWAY (1) MIDWAY (2) MIDWAY VINCENT (1) VINCENT (2)	$\approx p_f p^6$	$\approx 10^{-27}$
14	GATES - LOSBANOS	GATES GATES GATES LOSBANOS LOSBANOS	TEVATR MIDWAY DIABLO MIDWAY MOSSLAND	0	0
15	GATES - DIABLO	TEVATR LOSBANOS GATES DIABLO DIABLO	GATES GATES MIDWAY MIDWAY (1) MIDWAY (2)	0	0

Table 5.4 shows an example of the process of probability evaluation of system failure due to relay hidden failure. In this example, one of the incident lines (VALLEY 500 – SERRANO 500) to the bus Valley 500kV (the 2nd bus listed in Table 5.2) was picked, and a three-phase fault was applied at the line. Then three 500 kV lines (DEVERS – VALLEY, MIRALOMA – SERRANO, LUGO – SERRANO) were identified to be exposed to the fault. Based on the exposed lines, we have different tripping combinations. Table 5.4 only shows the tripping combinations leading to loss of load. As shown in the table, those tripped lines are checked with an X, and the probability of the line tripping is assumed to be *p*. For example, the first tripping combination in the table shows only one line (DENVERS – VALLEY) was tripped, and this combination has a conditional probability of $p(1-p)^2$ and a loss of load of *406+j41.0*. In this way, we can find all the probabilities of system failure due to different triggering events.

Table 5.4 System Failure Probability Evaluation

(Faulty Line: VALLEY 500 SERRANO 500 1)

DEVERS VALLEY 500	MIRALOMA SERRANO 500	LUGO SERRANO 500	Probability	Loss of Load
X			$p(1-p)^2$	406.0+j41.0
X	X		$p^2(1-p)$	406.0+j41.0
X		X	$p^2(1-p)$	406.0+j41.0
	X	X	$p^2(1-p)$	1230+j72.8
X	X	X	p^3	1636+j113.8

5.2.1 Case Analyses

Case 1:

If OLINDA-MALIN is tripped due to a fault on the line and MALIN-ROUND MT (1) (or MALIN-ROUND MT (2)) is also tripped due to hidden failure, then the system will collapse. If any two or more of the exposed lines are tripped, the voltage collapses. The only three situations that will *not* lead to voltage collapse are listed in the following:

1) If only MALIN-SUMMER L trips, the other four lines do not trip. ($\boldsymbol{pq^4}$)
2) If only GRIZZLY-MALIN (1) trips, the other four lines do not trip. ($\boldsymbol{pq^4}$)

3) If only GRIZZLY-MALIN (2) trips, the other four lines do not trip. (***pq^4***)

Therefore, the total probability is ***$p_f(1-pq^4)$***

Case 2:

If any one of the five exposed lines, together with the faulty line (OLINDA - TEVATR), trips, the system collapses. If none of the five exposed lines trips, the system is fine. Therefore, the total probability is ***$p_f(1-q^5)$***

Case 14:

The power carried by each of these exposed lines is as follows:

Line	Active power P(MW)	P/P_{max}% (P_{max}= 1600MW)
TEVATR-GATES	590.5	37%
GATES-LOSBANOS	176.4	11%
GATES-MIDWAY	264.7	16.5%
DIABLO-GATES	159.2	10%
MIDWAY-LOSBANOS	129.1	8.1%
LOSBANOS-MOSSLAND	40.0	2.5%
Power flow in this local area	610.0	38.5%

As shown in the above table, the load flow is light compared to the thermal limit of a 500kV transmission line. The net power flowing in this area is about 610MW, only 38.5% of the thermal limit of 500kV transmission line. If all of these lines are tripped, the power transfer to neighboring lines is still small (less than 610 MW), so it will not cause voltage collapse, nor overload lines. (The typical thermal limit for 500kV line is about 2600MW, I use a much smaller value here.)

From the above analysis, it would seem reasonable to say that there exists an increased likelihood of catastrophic failure triggered by a fault along the 500kV transmission corridor compared with that in the Los Angeles area. Although knowing this at the time would not allow the day and time or the precise trigger event for the blackout to be predicted, the identification of possible system weak links provides decision-makers with a quantitative justification for efficiently prioritizing the use of available resources as necessary to strengthen the power system.

Chapter 6 Production Simulations of the Load-Generation Uncertainties

6.1 Introduction

The proposed risk assessment of catastrophic failures in the power system is based on a specific load-generation profile (snapshot). A simplified approach is to conduct the risk assessment for several load-generation profiles as demonstrated in previous chapter, i.e. summer peak/normal and winter peak/normal load conditions. However, it is impractical for these few cases to capture all the possible scenarios that may lead to catastrophic failures; therefore, a more accurate and practical way is needed to deal with the load-generation uncertainties.

To address this issue, a simulation scheme is proposed to provide more diversified load-generation profiles for the studied period (e.g. one year). This chapter explains in details the approach of using production simulations [64] to generate the load-generation profile for risk assessment of power system catastrophic failures. The objective of the production simulation is to meet the system load demand at minimum operating cost while satisfying the security constraints of the system. For a given load profile under a certain configuration, the simulation generates a series of unit commitments corresponding to different time segments in the studied period. During a specific time frame, we may evaluate the risks of catastrophic failures corresponding to that specific operation point.

In the production simulation, four types of generating units—hydro-station, pumped-storage station, nuclear unit, and thermal unit—are considered, and each of the generating units has specific operating characteristics. The dispatch of the different types of units may follow different criteria, and each dispatch will be checked against the transmission line constraints.

For the assessment of the risk of catastrophic failures, transmission losses may be neglected in the production simulation; the operation and maintenance costs are not considered separately and may be reflected in the fuel cost instead. Other operating constraints, such as the unit minimum uptime/down-time, also may be excluded from this analysis.

In summary, the production simulation for the risk assessment of power system catastrophic failures includes the following steps:

1) Give the first priority to the must-run units[3] serving the security purpose (the area protection rule)
2) Dispatch the units with the minimum cost in the priority list (the economic criteria)
3) Ensure that the sum of the minimum technical ratings of all committed thermal units does not exceed the minimum daily load while ensuring, also, that the sum of the maximum ratings of the committed units meets the maximum daily load plus the reliable spinning reserve (the technical requirements)
4) Ensure that the interchanging power between two zones does not exceed the capacity limit of the tie lines (the transmission constraints)

The detailed simulation procedures for various types of generating units are presented in the following sections. Some key issues, such as the load modeling for sub-systems and transmission line capacity limits, are briefly discussed. Simulation flowcharts are also provided.

The production simulation framework presented here may also be used to analyze the costs/benefits of planning power plants or transmission lines. With appropriate modifications, it may also find other applications, such as simulating the bidding process in the current competitive market environment.

[3] must run units are those generators designated to operate at specific outputs and not available for dispatch

6.2 Load Modeling

6.2.1 Special Considerations

An hourly load-model representation is used in the production simulation. For an accurate modeling, the 8760 hourly load representation is needed in the simulation during a one-year study period; however, for the risk assessment of catastrophic failures, a less accurate load modeling may be acceptable. The simulation is based on a typical day/week load profile for each month. This compromise makes the study more manageable without discrediting the results.

A typical week load profile may be further simplified by only considering the average weekday and weekend load profile in the simulation. In a somewhat more accurate model, four day types are considered: Saturday, Sunday, peak weekday, and average weekday.

In order to consider the transmission line capacity constraints or to simulate an interconnected system, the studied area needs to be divided into several sub-systems, termed zones; in addition, the load profile of each zone needs to be given. The constraints of transmission lines are accounted for by modifying the sub-system load-duration curves. In some applications, the hourly power exchange through each tie line is known beforehand; then, the modifications of load curves are carried out directly by superposition.

If the sub-systems belong to different utilities, and only typical day load profiles are given for each month (this is the normal situation in the planning phase), careful measures need to be taken when merging the load profiles to form an overall load profile representing the studied system. On the other hand, if both the system load profile and the sub-system load profiles are given, appropriate modifications to either the sub-system load profiles or the system load profile are needed to match them.

In the simulation, the load-duration curves are revised when each unit is dispatched. Each successful dispatch is checked against the transmission line loading constraints. Once a transmission capacity limit is reached, any thermal/nuclear unit or hydro-station causing the overload of the transmission line will not be committed even it may have a cheaper marginal cost.

6.2.2 Implementation of Load Modeling

The simulation procedures related to load modeling are as follows:

1) Input the month-type, day-type, and hour-type load-demand profile for the system and each zone (sub-system), as well as the forecasting maximum or actually-occuring loads for the system and each zone
2) Form the daily load-duration curves of the system (if the related system load pattern is given) and each zone during the studied period
3) If the system daily load-duration curve is known, modify the daily load-duration curve of each zone to match the pattern of the system daily load-duration curve, and go to step 5
4) If the system daily load-duration curve is not known, form the system daily load duration curve of the studied area based on the zone's daily load-duration curves, and check against the maximum system load (if given)
5) If there are power exchanges with outside systems, modify the system load-duration curve based on the pre-set limit or the contract
6) Modify the revised load-duration curves of each zone based on the planned power exchange contract between zones
7) Modify the load-duration curve of the corresponding zone based on the pumped-storage station (if present) dispatching results within each zone (Please refer to Section 6.3.2 Pumped-Storage Station for more details)
8) Update the system daily load-duration curve and related zone's daily load-duration curve for each unit commitment

The flowchart for the above load modeling is shown in Figure 6.1

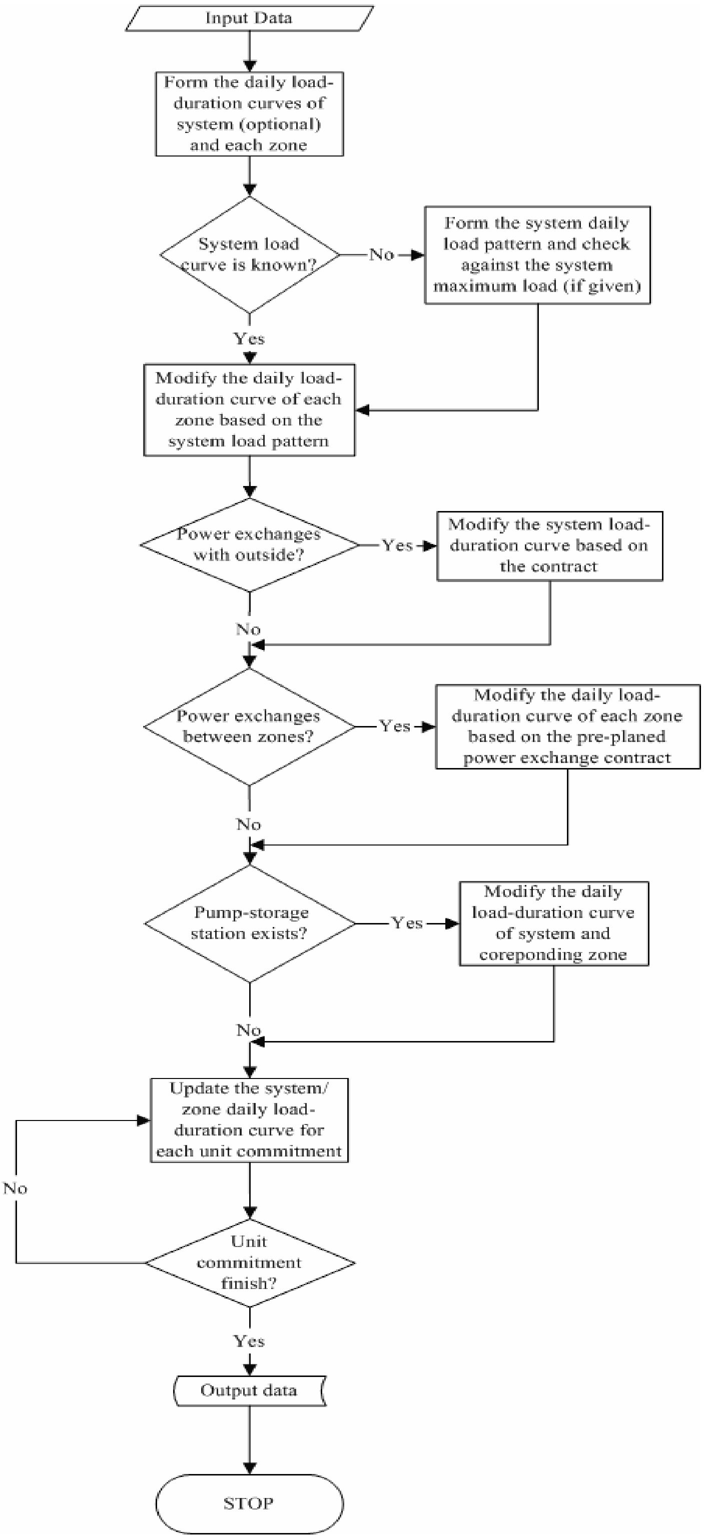


Figure 6.1 Implementation of Daily Load-Duration Curve Model

6.3 Production Simulation for Different Types of Units

In this section, the dispatch criteria for the four types of generating units—hydro-station, pumped-storage station, nuclear unit, and thermal unit—are discussed, and the simulation procedures are explained in details followed by corresponding flowcharts.

6.3.1 Hydro-Station Simulation

The production simulation of a hydro-station is more complicated than that of a thermal unit. Since the operating cost of a hydro-station is less than that of a thermal unit, the dispatch of the hydro-station normally has priority over the thermal units. Moreover, due to its rapid load-tracking capability, the hydro-station often assumes the peak load of the system. In addition, this arrangement will lower the total cost of the system operation, since the thermal unit will incur a higher operation cost (and is less efficient) to trace the peak load variations.

The dispatch simulation of a hydro-station is normally conducted on a monthly time frame—the summation of hourly output during the studied month will be subjected to a given electricity constraint. This monthly electricity is determined by the water inflow, the out-going down-stream requirement, and the reservoir capacity, as well as the coordination with other hydro-stations along the same river. Different weather conditions will also affect the monthly electricity capacity.

Anther consideration in the hydro-station simulation is the proper assignment of adjustable capacity factors of different types of hydro-stations. Regarding water storage capacity, four kinds of hydro-stations are considered: a non-adjustable water storage capacity station, a seasonal adjustable capacity station, a yearly-adjustable capacity station, and a multi-year adjustable capacity station. The run-of-river hydro-station falls into the category of non-adjustable capacity stations, whose hourly output power is totally determined by the inflow water. For this kind of station, the adjustable capacity factor assigned is one.

For the latter three kinds of hydro-stations, monthly electricity capacity factors vary in certain ranges; the range is 0.95-1.05 for seasonal adjustable stations, 0.9-1.1 for yearly-adjustable stations, and 0.8-1.2 for multi-year adjustable stations. Table 6.1 lists the adjustable factors for the four types of hydro-stations

Table 6.1 Adjustable Factors for Different Types of Hydro-Stations

Types	Run-of-river station	Seasonal adjustable station	Yearly-adjustable station	Multi-year adjustable station
Adjustable Factor Range	1.0 (fixed)	0.95-1.05	0.90-1.10	0.80-1.20

Data Requirements

The following data are needed for the hydro-station simulation.

Monthly Available Capacity (ACH)

The available capacity is the installed capacity minus the maintenance capacity in a station. In a probabilistic production simulation, the forced outage capacity (versus planned outage capacity due to maintenance scheduling) also needs to be deducted.

Monthly Electricity (EH)

This is determined by inflow water, storage capacity of a reservoir, and weather conditions. Normally, three different sets of data are provided, corresponding to three different weather conditions: normal year data, flood year data, and dry year data. For a given data set, adjustments may be applied for some monthly data in the simulation by multiplying an appropriate adjustable factor from Table 6.1.

Monthly Forced Base Loading (FBL)

This data corresponds to the minimum flow restriction due to irrigation, navigation, or environmental considerations. It may also be affected by the coordinated operation of several hydro-stations along the same river.

Monthly Maintenance Schedule

This is the planned outages during the studied period. Several key factors are considered in maintenance scheduling. These factors include the seasonal load-demand profile, the total number of units needing to be scheduled in the studied period, the size of a generating unit, the average time spent on maintenance for each unit, and the maximum maintenance capacity in a station at the same time. Another factor that may be taken into account is the time a unit has been in service. A new or very old unit may need to schedule outages more frequently than others. In general, every hydro unit requires an overhaul every three years, which lasts about 25 days, and two inspections every year, lasting one week each. Operations maintenance scheduling requires more specific information such as the availability of maintenance crews, the elapsed time from the last maintenance, etc.

Monthly Expected Maximum Output Power (EMP)

This is determined by the following factors: the unit's monthly maximum available capacity, monthly electricity, monthly forced base loading, the adjustable factor, and the daily load-duration curve for each month. It is the maximum output power in a day that a hydro unit/station assumes in the simulation. For the run-of-river type hydro-station, the monthly expected maximum output power equals to or is less than its monthly forced base loading.

Effective Capacity Coefficient (ECC)

This coefficient determines the dispatching order of hydro-stations, thus determining the operating positions in the daily load-duration curve. It is computed in this way:

$$ECC=EMP/(EH*FA/24/DM)$$

where

ECC Effective Capacity Coefficient

EMP Monthly Expected Maximum Output Power

EH Monthly Electricity

FA Adjustable Factor shown in Table 6.1, its initial value is one.

DM Days in the month (29, 30, or 31)

A larger coefficient means more peak-loading capability of a hydro-station, and higher priority given to the station. This consideration ensures that the system can take full advantage of the peak-loading capability of hydro-stations.

Simulation Flowchart

The simulation procedures of the hydro-station consist of the following steps:

1) Input the hydro-station data (capacity, monthly electricity, monthly forced base loading, adjustable factor, monthly maintenance schedule, etc.)
2) Compute the monthly available capacity for each station
3) Compute/adjust the monthly spinning reserves for each station
4) Compute the monthly expected maximum output power for each station
5) Rank the dispatching order based on the effective capacity coefficients
6) Dispatch the forced base loading of each hydro-station (and update the system and corresponding zone's daily load-duration curves)
7) Compute the loading positions for each hydro-station based on the dispatching order
8) Check for possible loss of electricity due to a mismatch between the load pattern and too great an inflow water, if there exists loss of electricity, modify the adjustable capacity/electricity factors and repeat Steps 3-8
9) Output the dispatched positions for each hydro-station and other statistical data for each zone

The flowchart for the hydro-station simulation is shown in Figure 6.2.

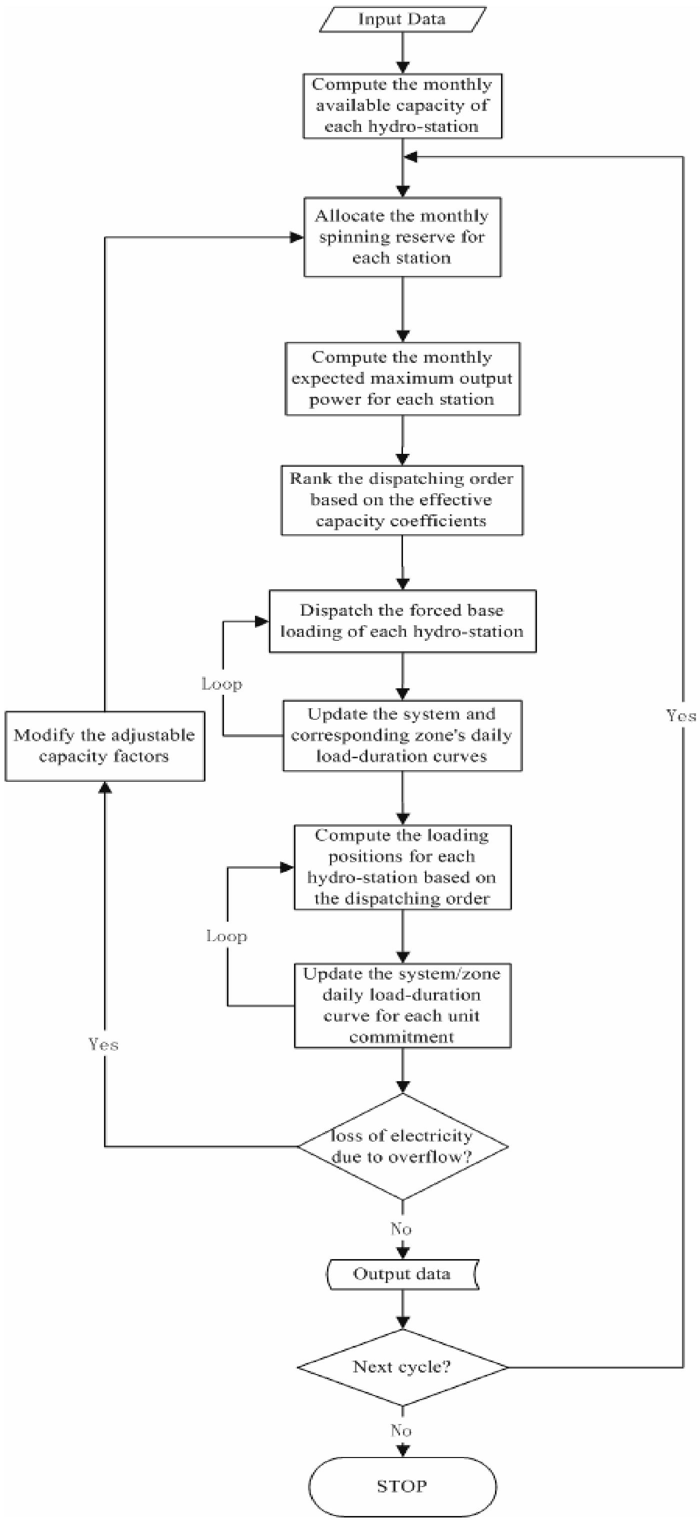


Figure 6.2 Hydro-Station Simulation

6.3.2 Pumped-Storage Station Simulation

Several factors affect the operation of a pumped-storage station. These factors include generating capacity, pumping capacity, water storage capacity, efficiency, daily load demand pattern, and marginal cost of other units (thermal and nuclear). For the sake of simplicity, we may assume that the pumped-storage station has better economic performance than thermal units (e.g. gas units). This is true in a system where thermal units comprise most of the generating capacity. Based on the above assumption, a different approach from [64] to dispatch pumped-storage station is proposed below. (In [64], Stoll proposed to simulate a thermal station before the simulation of a pumped-storage station, and his approach may lead to more iterations than the proposed simulation here)

1) Develop the cumulative load curve from the daily load-duration curve
2) In the cumulative load curve, find the MW position (P_p) corresponding to the given pumped-storage station generating electricity (E_p); subtracting P_p from the maximum daily load (PL_{max}) will give the maximum capacity (P_{pmax}) that can be assumed by the pumped-storage station subject to the electricity constraint
3) Compare the generating capacity (C_{pump}) of the pumped-storage station with the P_{pmax} obtained in previous step, if $C_{pump} > P_{pmax}$, go to Step 8
4) Since $C_{pump} < P_{pmax}$, compute the electricity (denoted by E_{mis}) between the C_{pump} and P_{pmax} in the cumulative load curve
5) Modify the daily load-duration curve by reducing (flattening) all the hourly loads above the position (PL_{max} - C_{pump})
6) Form the new cumulative load curve based on the updated daily load-duration curve
7) Substitute E_p with E_{mis} obtained in Step 4; repeat Steps 2-7
8) Calculate the consumed electricity E_c when the station runs in pumping mode (E_c may also be given a priori)
9) Follow similar procedures to modify the daily load curve by increasing the valley-load

10) Output the new daily load-duration curve for dispatching nuclear stations. (Please refer to Section 6.3.3 Nuclear Unit Simulation).

The flowchart for the pumped-storage station simulation is shown in Figure 6.3

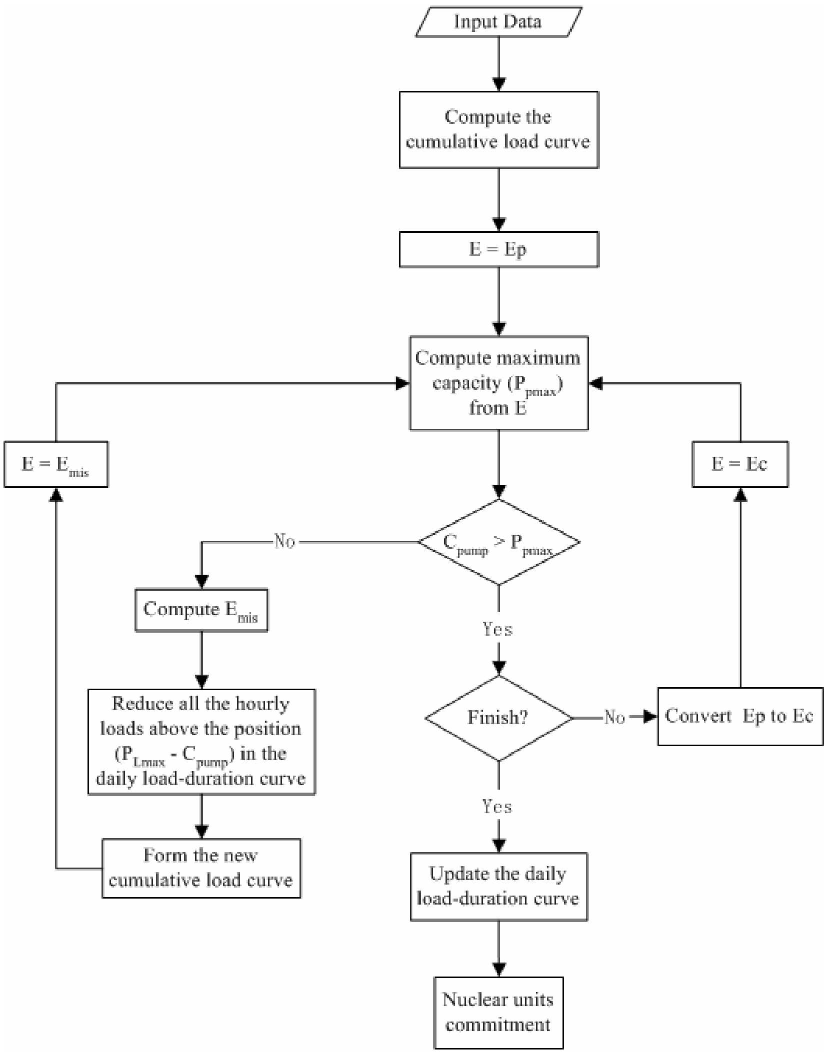


Figure 6.3 Pumped-Storage Station Simulation

6.3.3 Nuclear Unit Simulation

The commitment of nuclear units is relatively simple when compared with other types of generating units. In most cases, nuclear units are economical and they are expected to assume the base area in the daily load-duration curve. This is also desirable for safety purposes. In addition, the design of the nuclear station limits its peak-load tracing ability. In this simulation, we may treat a nuclear unit like a thermal unit, which is discuss below.

6.3.4 Thermal Unit Simulation

The objective of a production simulation is to meet the system load demand at minimum operating cost as well as the security constraints. The simulation procedures for the thermal unit commitment are briefly discussed below:

1) Commit the list of must-run units first; for each must-run unit, do the following:
    a. Check to determine if the committed unit's cumulative minimum rating is greater than the system minimum daily load; if yes, print an error message and stop
    b. Check to determine if the committed unit's cumulative minimum rating is greater than the corresponding zone's minimum daily load plus the tie-line capacity; if yes, print an error message and stop
    c. Update the system and zone daily load-duration curves based on the must-run unit's minimum rating
2) Rank all the available thermal units (including the must-run units) in a priority queue based on the full-load operating cost
3) Process the first unit in the priority queue, if it was not committed before, do the following:
    a. Check to determine if the cumulative minimum rating plus the unit's minimum rating is greater than the system's un-served minimum load; if yes, proceed to the next unit in the queue
    b. Check to determine if cumulative minimum rating plus the unit's minimum rating is greater than the corresponding zone's minimum load plus the tie-line capacity; if yes, proceed to the next unit in the queue
    c. Update the system and the zone daily load-duration curve based on the unit's minimum rating

4) Cumulate the maximum rating of the unit with those committed in the same zone; check to determine if the cumulative maximum rating is greater than the corresponding zone's maximum load plus the tie-line capacity. The following two scenarios are possible:
   a. If no, check to determine if the system cumulative maximum rating is greater than the system's maximum load plus spinning reserve requirement; if yes, the thermal unit commitment succeeds, and go to Step 5. If no, commit this unit, update the system and the zone daily load-duration curve, proceed to the next unit in the queue, and repeat Steps 3-4
   b. If yes, calculate the hourly dispatch, which is subject to the tie line capacity; proceed to the next unit in the queue, and repeat Step 3~4
   c. If there is no unit in the priority queue, print out a warning message and the hourly load curtailment
5) Output the unit commitment results

The flowchart for the thermal unit simulation is shown in Figure 6.4

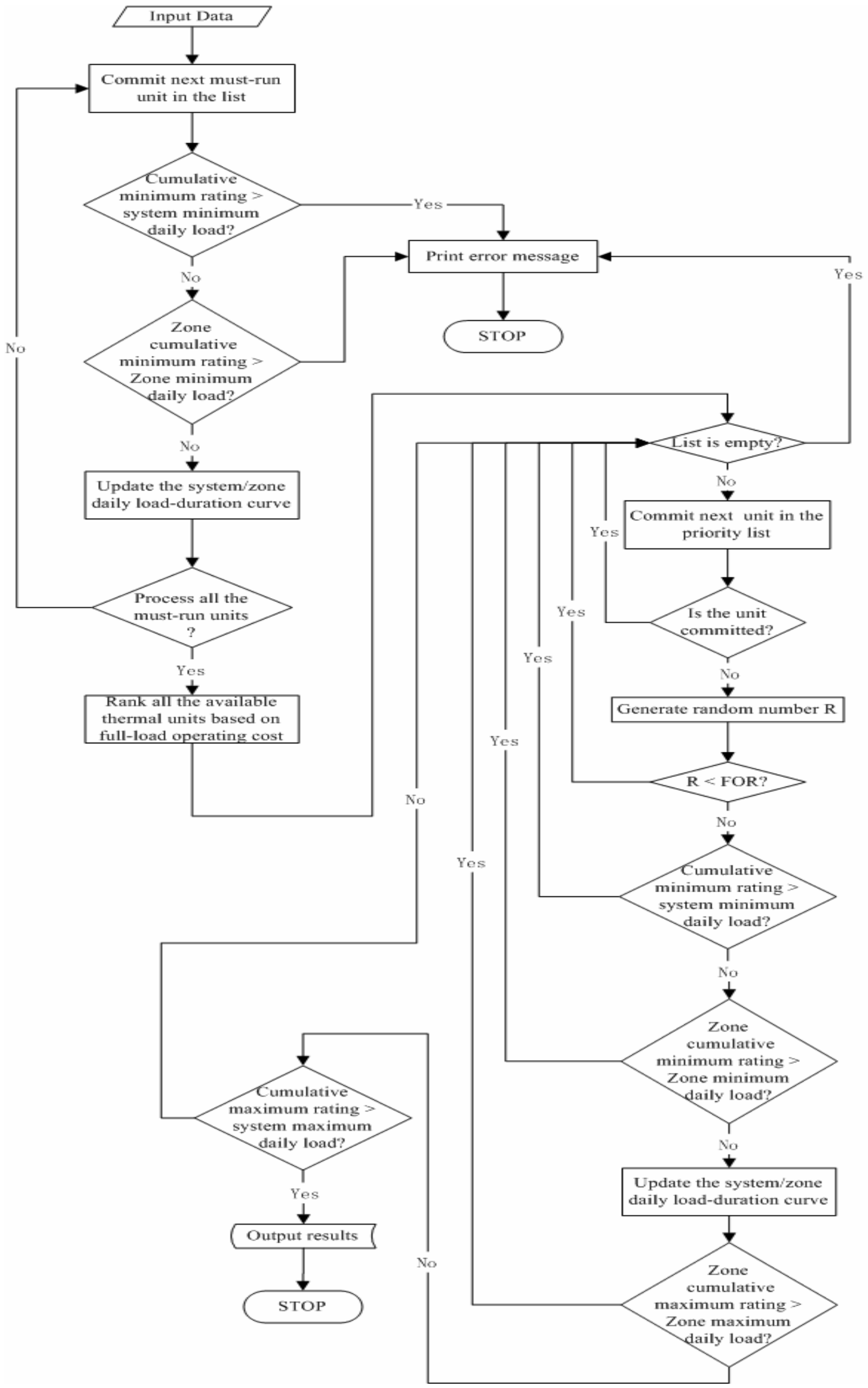


Figure 6.4 Thermal Unit Simulation

6.4 Other Considerations

6.4.1 Spinning Reserve

In general, a spinning reserve of 3%-8% of load demand is required. For a large system, 3% may be enough, while 8% is probably needed for a small system.

Spinning reserve will first be dispatched proportionally between hydro (including pumped-storage) units and thermal units. The spinning reserve ratio assumed by hydro units and thermal units varies among utilities. It depends on the characteristics of the hydro/thermal units in the system and the utility practice as well. Spinning reserve will be shared among all the committed thermal units proportionally to their capacity. For hydro units, the spinning reserve will normally be shared in proportion to their maximum expected output powers. The spinning reserve allocation between hydro units and thermal units may be transferred in either direction within a range when some conditions are met. For example, in a flood year, the thermal units may provide more spinning reserve to let hydro units generate more electricity. This flexibility may avoid possible loss of electricity due to overflow.

6.4.2 Area Protection Rule

In a large interconnected system, the generating sources for security purposes are important to the system reliability and the local critical loads. The minimum amount of committed generating units (capacity) must be assigned in the heavy load center to ensure voltage stability. This area protection requirement often imposes some constraints on the dispatch during off-peak load periods. Tradeoffs must be made to balance the economic objectives and security concerns.

6.5 Summary

The proposed production simulation framework for risk assessment of catastrophic failures may also be applied to other interesting areas such as electric market simulation and cost/benefit analysis of power plants and transmission lines after appropriate modifications.

Chapter 7 The Hidden Failure Monitoring and Control System

7.1 Introduction

Customer service reliability and the security of an electric transmission system depend heavily on the proper performance of substation protective relaying and automatic control systems. Ever-rising customer expectations, reduced maintenance schedules, and increased demands on the transmission system require an effective and reliable monitoring and control system to ensure the correct operation of relays, circuit breakers, switches, alarm systems, SCADA, and other automatic equipment found at the substations.

Due to technological advances in high-speed reliable communication networks and the availability of powerful IED devices with self-supervision, auto-diagnostics features and integrated communications capabilities, the Hidden Failure Monitoring and Control System (HFMCS) can be one of the most promising risk mitigation actions to prevent power system catastrophic failure involving relay hidden failure. In this chapter, the implementation of the Hidden Failure Monitoring and Control System is developed. The risk assessment of system failure and relay hidden failure will provide a prioritized substation list for the deployment of the HFMCS.

The proposed architecture aims to implement a straight forward, efficient, cost-effective HFMCS, which can be integrated into SCADA and station automation designs. The HFMCS framework facilitates template-driven SCADA and station automation applications, and complies with the needs of the Integrated/Automated Substation [89]-[93]. The integrated Misoperation Tracking Database will provide automatic management of misoperation records for hidden failure analysis.

7.2 HFMCS Architecture

The proposed HFMCS consists of three main functional modules shown in Figure 7.1: *Hidden Failure Monitoring*, *Hidden Failure Control,* and *Misoperation Tracking Database*. Hidden Failure Monitoring provides a basis that allows further controls to be initiated. Hidden Failure Control will be implemented based on *Adaptive*

Dependability/Security Protection. A Misoperation Tracking Database can facilitate the risk assessment of system failures and hidden failures, and provide a prioritized deployment of the monitoring and control modules at substations identified as system weak links during the risk assessment.

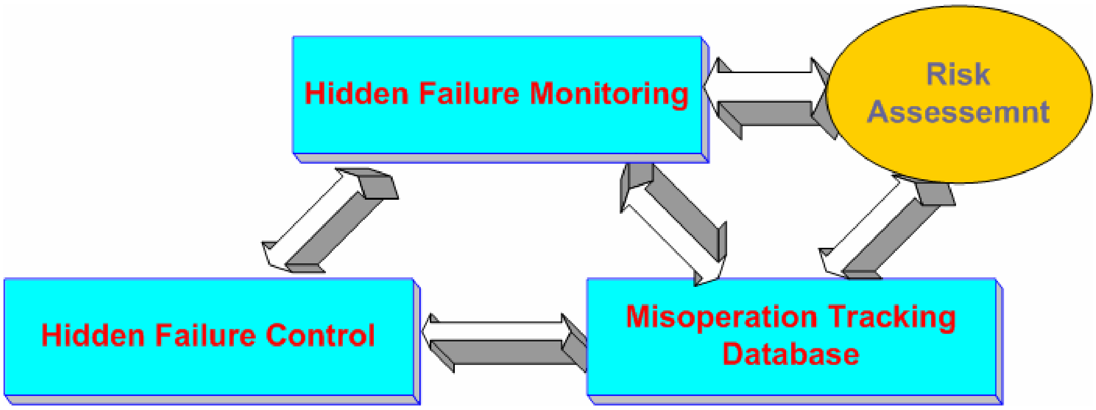


Figure 7.1 Functions of the Hidden Failure Monitoring & Control System

The HFMCS is a substation-based, dedicated, and secure corporate-wide area network. There are two layer networks within the HFMCS: the substation level network—*Distributed Monitoring/Control (DMC) Network*—and the corporate level network—*Centralized Monitoring/Control (CMC) Network.*

7.2.1 Centralized Monitoring/Control Network

The Centralized Monitoring/Control (CMC) Network is comprised of a System Control Center (SCC), a few Regional Control Centers (RCCs), and a large number of Distributed Monitoring/Control (DMC) networks located at key substations. Figure 7.2 demonstrates the configuration of a Centralized Monitoring/Control (CMC) Network. The number of Regional Control Centers depends on a company's geographical service territories and practice, etc. The Misoperation Tracking Database (MTD) normally will be located at the system control center, and connected to the backup server of SCC to minimize the interventions to other key functions of the SCC, such as monitoring and control functions. The MTD may be accessed by authorized users from the corporate WAN. Internal firewalls and a secure router between the corporate WAN and the SCC are used to secure the CMC network. The access points from the corporate WAN should be limited. Other network security measures such as Intrusion Detection Systems (IDS), authentication, encryption, and strong access restrictions must be in place to minimize the risks of unauthorized access. Remote access from laptops should be limited to those necessary personnel, for example, the developer of the HFMCS or the field protection and control (P&C) specialist who is responsible for the maintenance of a substation's DMC network. The P&C specialist should only be granted access to those stations under his direct responsibility.

The connection between a substation and the regional control center should be redundant, and the dedicated connection between the substation and the regional control center should ensure the transmission of real-time monitoring and control data with first priority. Other non time-critical data, such as event logs and oscillography data, will be polled regularly by the MTD.

The RCC is responsible for monitoring critical automated equipment status (e.g. IEDs) for all stations within its territory. Various equipment status signals will be polled regularly. If critical equipment at a station is in an abnormal condition, it will send a message via the Distributed Monitoring/Control (DMC) network at the substation to the RCC and an alarm signal will display on the monitor at the RCC to alert the operator. A more detailed explanation will be presented in section 7.3.

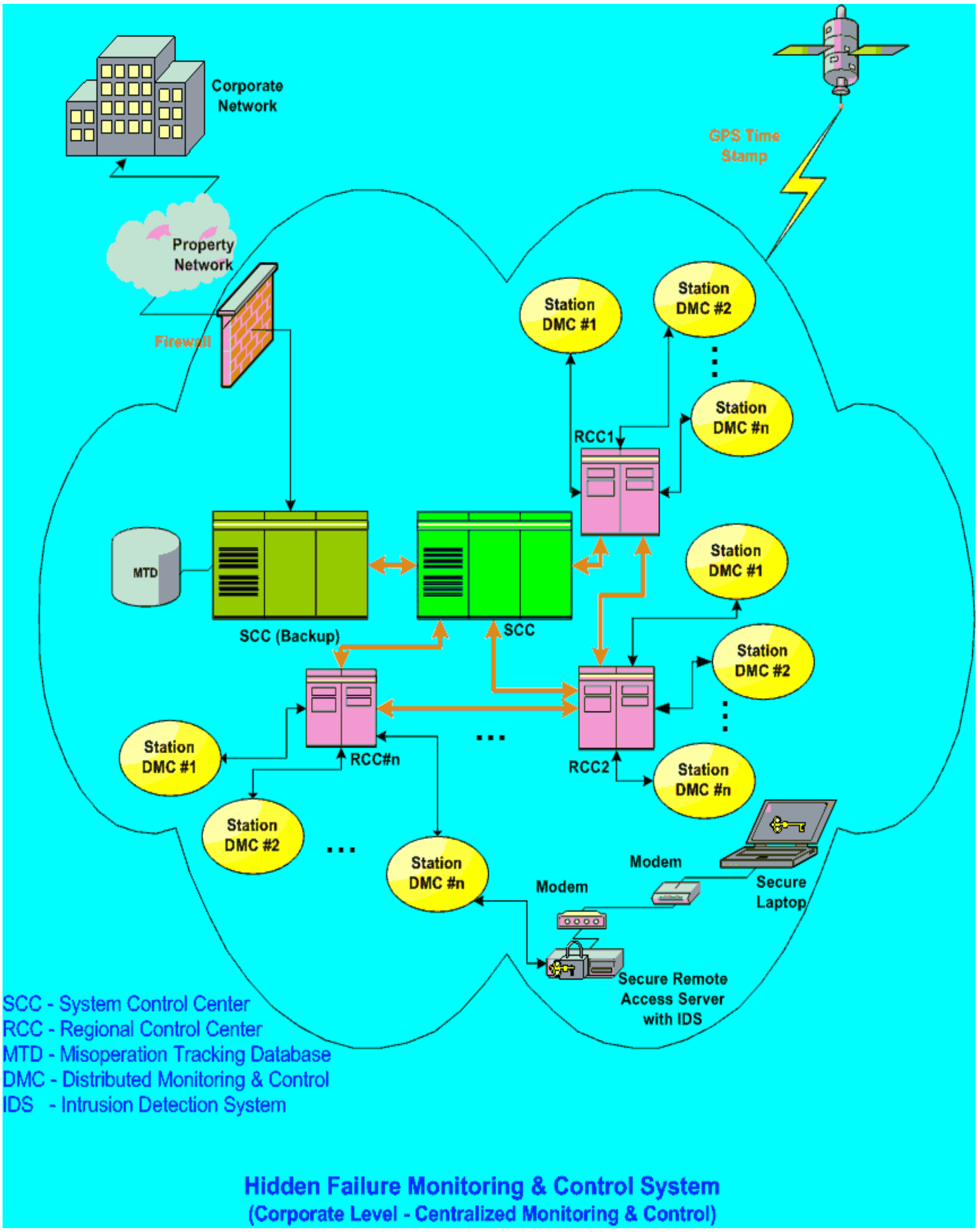


Figure 7.2 Centralized Monitoring & Control System

7.2.2 Distributed Monitoring/Control Network

Distributed Monitoring/Control (DMC) provides the monitoring and control functions locally for substation automated equipment. DMC is an integrated Ethernet Local Area Network (LAN) designed to allow communications between the Station PC/Data Concentrator and station IEDs (digital protective relays, meters, Remote Terminal Units, etc.) It allows both local and remote access of the station IEDs attached to the Substation LAN.

The foundation of the DMC network is the Station PC/Data Concentrator, the Ethernet Switch and the communication server (e.g. Schweitzer SEL2030) used to communicate with vendors' IEDs. Figure 7.3 shows the DMC network for the HFMCS.

The functions provided by the Station PC include Local Station Control, Data and Alarm Annunciation, Oscillography, and SCADA, along with other features. A second Station PC/Data Concentrator can be installed if needed, to provide a backup at important 345kV and above stations.

In order to minimize the up-front cost of building a HFMCS, it is advisable that a substation LAN and Ethernet switches be deployed before a station PC is in service. In such a case, this system will not provide the full features of the local system monitoring and control, but will allow direct local and remote access to the station IEDs.

All devices with network capability (Station PC, network-compatible IEDs, etc.) are tied together through an *Ethernet switch*. Some other devices that lack network capability (e.g. all SEL relays except SEL 421[www.selinc.com]) but do support serial communications will connect to a communication server. In Figure 7.3, a *multiport device server* is also provided for communications to some legacy IEDs, such as the ALPS, DLP, and RFL9300 (w/o MODBUS option). Some A/D I/O adaptors are deployed for supervisory data, such as breaker trip signals for old circuit breakers as well as miscellaneous alarms.

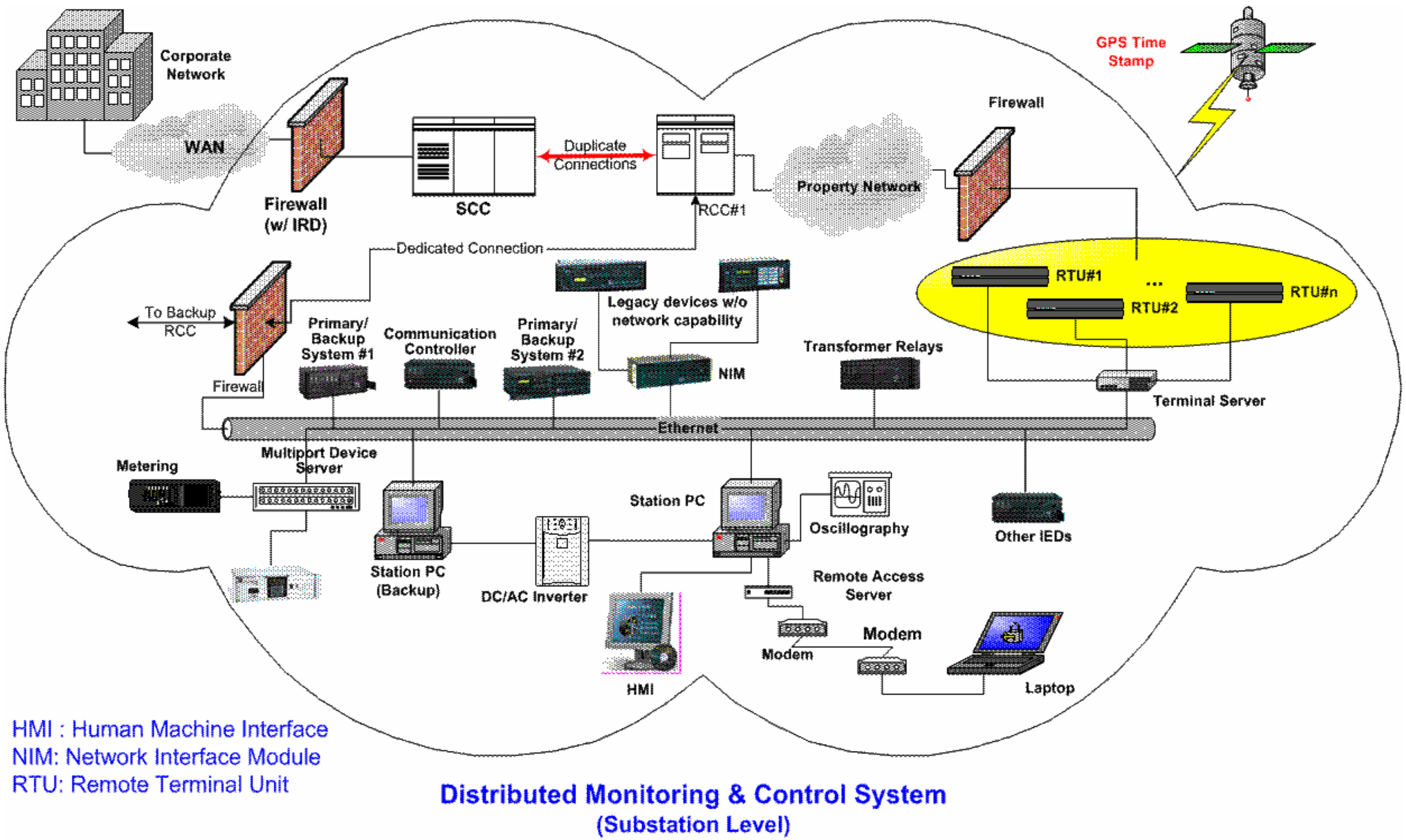


Figure 7.3 Distributed Monitoring & Control (DMC) System

Not all the DMC networks are able to connect to a utility's corporate WAN due to the prohibitive cost for such preferred connections. In such cases, a dial-up connection has to be established, in which case a *remote access server* and associated *modem* have to be set up.

Whenever possible, fiber optic cable is recommended to connect DMC devices to eliminate electrical noise and surge problems; however, not all devices support fiber optic connections. If Cat5 cable is to be used to connect a device to the Ethernet switch, surge protectors need to be installed at the Ethernet switch and at the remote device. If Cat5 cable is used, it must be twisted pair/shielded. The Cat5 cable must be routed away from the control cable, as much as is practical.

A reliable DC/AC inverter is required to power the Station PC/Data Concentrator, backup station PC, the multiport device server, A/D I/O adaptors, the remote access server, and the modem in the DMC network.

7.2.3 Software Architecture

The Station PC uses real-time monitoring software to present various data/control displays to the station operator and P&C personnel; in addition, other communications software, such as UCA I/O Server, Modbus Ethernet I/O Server, OPCLINK, or the utility's proprietary SCADA protocol translator, are needed to support the integrated process. The IED vendor's integration software is also used, e.g. SEL5040, which performs automatic polling of SEL relays for oscillography. Other data retrieving and remote access software, such as an oscillography viewer and Carbon Copy, are provided. OEM software packages can be used to communicate with legacy IEDs.

Oscillography from GE UR relays is automatically polled from the real-time monitoring software. Human Machine Interface (HMI) screens available on the Station PC include Station One-Line, Breaker Control Panel, Line Control Panel, Alarm Annunciator, Relay Panel, Meter Panel, Carrier Current Panel, and Transfer Trip Panel.

For demonstration purposes, a pseudo-simplified station one-line screen of a DMC Human Machine Interface is shown in Figure 7.4. The Station One-Line panel shows the configuration of major devices monitored by the DMC. The circuit breaker (CB) icon (e.g. A1, B1, etc.) also represents the relay systems that control the CB. The CB icon in green denotes its open status; it will change to red if the associated CB closes.

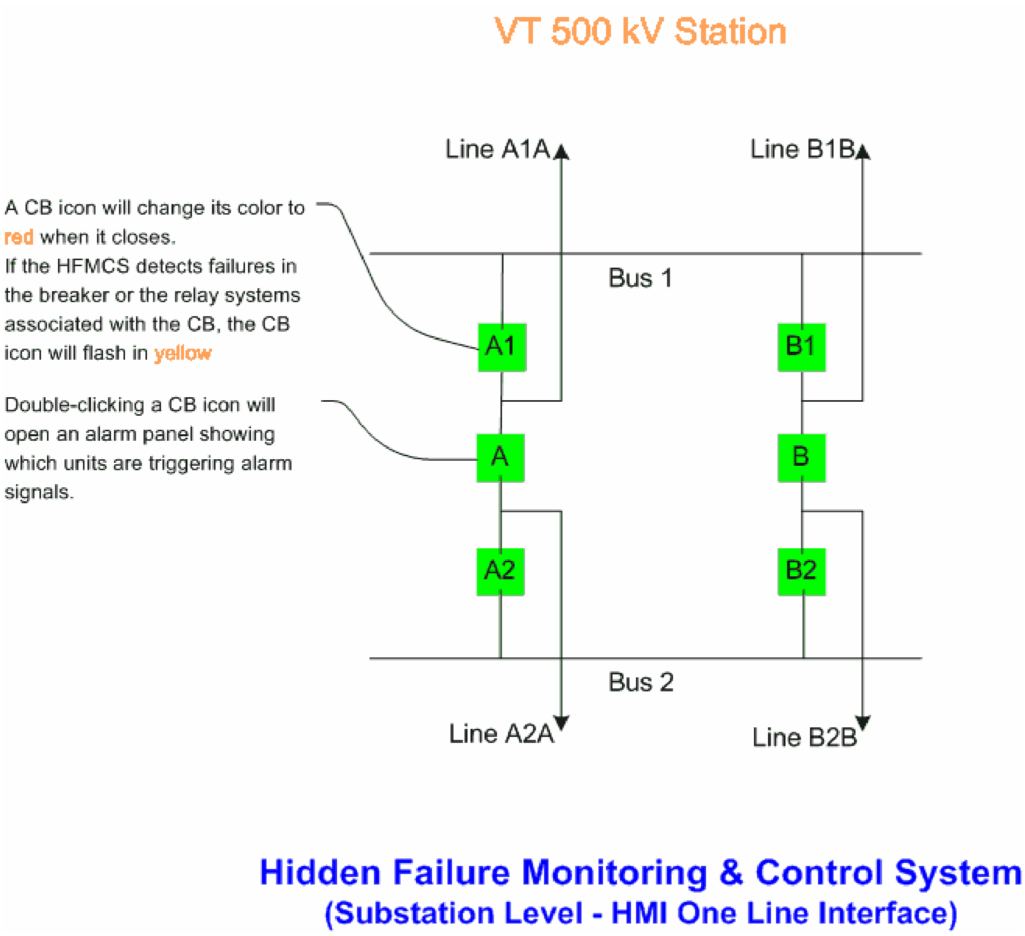


Figure 7.4 HMI of the HFMCS – Station One-Line Diagram

If the DMC system detects abnormal conditions in the circuit breaker or in the relay systems associated with the circuit breaker, the CB icon will flash in yellow. Double-clicking the CB icon will cause an alarm panel to pop up to show which functional unit is issuing the alarm. Figure 7.5 shows a sample alarm panel. Detailed alarm signals to be captured by the alarm module will be discussed in section 7.3.

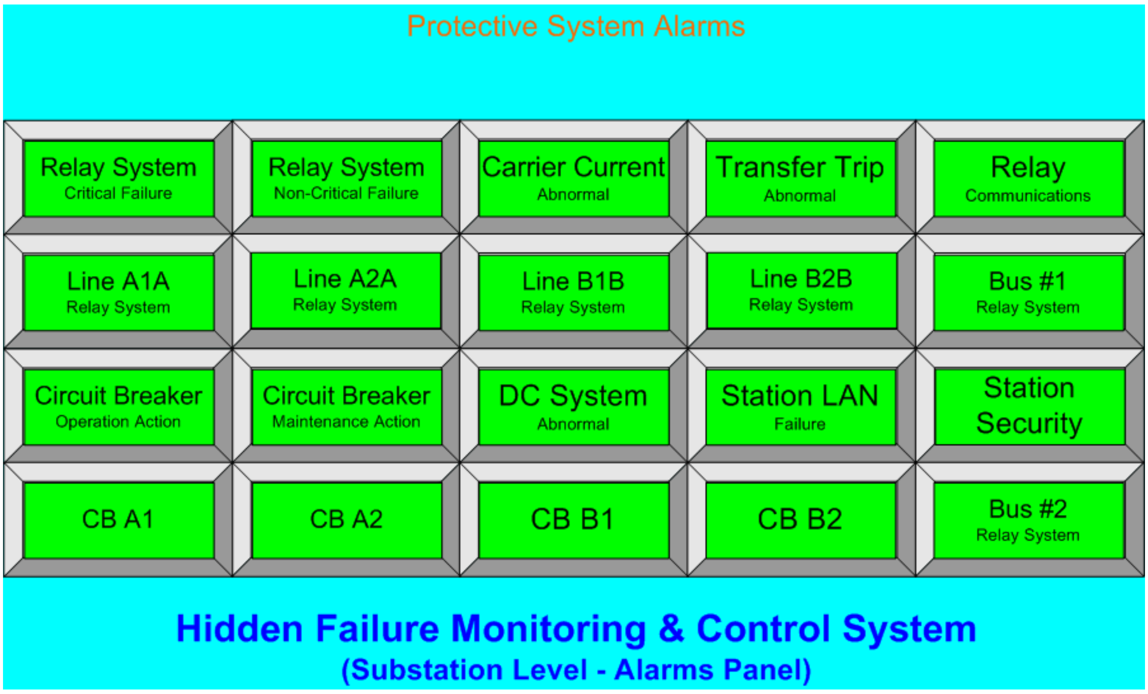


Figure 7.5 HMI of the HFMCS – Protective System Alarm Panel

7.3 Hidden Failure Monitoring

The Hidden Failure Monitoring (HFM) system collects, displays, and stores information about various automated devices at a station. The information is collected from various RS232 or RS485 compatible IEDs using various IED specific protocols. Each data point is tagged with date and time. This data may be retrieved periodically via modem or network. The data format must comply with that of the Human Machine Interface. The HMI will reformat the collected data and present the data to its user.

The HFM system is a substation LAN-based monitoring system that provides a broad range of monitoring functions for all important devices within a substation. Various alarm signals will be generated for abnormal conditions that may contribute to the failure of protection systems. These alarm signals can be separated into two categories: *Critical Alarm Signals* and *Non-critical Alarm Signals*. Critical alarm signals are those needing to be addressed immediately; otherwise, the failure of the protection system is inevitable once some triggering conditions are met.

The core of the HFM system is the *Alarm Control Module (ACM)*. All alarms associated with a transmission line, transformer, or bus will be brought to the ACM on the Station PC, and displayed on the corresponding HMI screens (e.g. Station One-Line panel and Protective System Alarm panel). The critical alarm signals will also be sent to the Regional Control Center (Figure 7.2) and the System Control Center. The operator at the Regional Control Center then may kick in appropriate control measures, either dispatching a protection & control technician to the station to address the problem or issuing a command to activate the *Adaptive Dependability/Security Protection* Scheme (Refer to Figure 7.6-Figure 7.9), which is discussed in Section 7.4.

As shown in Figure 7.5, the ACM collects the following line/bus/circuit breaker alarm information:

- Relay System Critical Failure Alarms
- Relay System Non-Critical Failure Alarms
- Carrier Current (CC) Abnormal Alarms (primary system #1&2)
- Transfer Trip (TT) Abnormal Alarms (Optional)
- Relay Communications Alarms
- Circuit Breaker Operating Action Alarms
- Circuit Breaker Maintenance Action Alarms
- Breaker Failure Alarms
- DC System Abnormal Alarms
- Station LAN Failure Alarms
- Station Security Alarms

The button in the *Protective System Alarms* panel will flash in yellow if an alarm signal associated with the button is activated. For example, the button labeled "*Relay System Critical Failure*" will be activated by any one of the following alarm signals:

- Protective Relay Critical Alarms
- Relay Loss of Potential

- 551x LOR Trip Coil
- OA/Int/Lead Transformer Differential LOR Trip Coil
- Reactor Differential LOR Trip Coil
- Bus Differential LOR Trip Coil
- Hydran Monitor Critical Alarm
- Qualitrol TR Temperature Monitor Critical Alarm

The "*Relay System Non-Critical Failure*" button will flash if any one of the below alarm signals presents:

- Carrier Current Check Back Disabled
- Protective Relay Loss of GPS (IRIG-b) Clock Signal
- Cable-To-Ground Abnormal
- Loss of Communication to a Station IED from the Station PC.

Some of the other important alarm groups include:

- Carrier Current (CC) Abnormal Alarms (primary system #1&2):

  Loss of Power, Communication Path Failure, Carrier Set Failure, Carrier Low Level, etc.
- Transfer Trip (TT) Abnormal Alarms:

  Loss of Guard, Loss of Power, Transmitter (TX) Power Fail, Low Level, DTT LOR Trip Coil, etc.
- DC System Abnormal Alarms:

  Breaker Control DC/Trip Coil Monitor, Station Battery Alarms, Station Battery Charger Alarms, Station Inverter Alarms, Battery Room Combustible Gas High, Battery Room Combustible Gas Very High

Most of the devices attached to the DMC network depend on the DC system for their power source. Without the DC power, these devices cannot perform their functions. The substation LAN will also be monitored to prevent any network failure resulting improper functioning of the DMC system.

The HFM system can also measure the CT cable insulation resistance to ground. The measurement is performed once per day automatically. If the measured resistance is less than 50K ohms, then an alarm (CTG Abnormal) is produced. The test can also be initiated manually via a pushbutton located on the relay.

In addition to capturing transmission line protection alarms, the ACM can be expanded to provide transformer protection alarms, plus transformer monitoring and diagnostics, such as associated Sudden Pressure Trip, Low Side Overloads and Low Side Analog SCADA.

The Alarm Control Module also provides annunciation of the alarms using programmable LEDs located on the front of the relay. There are touchpads available on the front of the relay to enable or disable each alarm. The changed status will be captured by HMI on the Station PC.

Another important function implemented in ACM is to retrieve sequence of event information and oscillography event information from various IEDs, and store these data in the Station PC. From the Station PC, a field technician can view detailed alarm information and enable/disable alarm points. One important feature of the HFM system is that an intermittent alarm will be recorded, and it can facilitate the post-fault analysis of possible relay hidden failures.

Other than monitoring the operations of IEDs during abnormal conditions, another aspect of HFM system is its self-diagnostic capability. Self-diagnostic features of IED devices (e.g. primary system #1&2) include an event record that tags events with time and date. This precise time stamping allows for a determination of the sequence of events throughout a system. Events can also trigger oscillography records that consist of a 64 sample/cycle record of analog signals and digital flags, as well as a snapshot of protection settings. These records will be polled into the Station PC.

7.4 Hidden Failure Control

The Hidden Failure Monitoring system provides a powerful tool for detecting abnormal conditions in automated devices and for initiating proper remedies via Hidden Failure Control (HFC). HFC can also be activated directly by system abnormal conditions. The core of Hidden Failure Control is the Adaptive Dependability/Security Protection (ADSP). [29][40][94]-[98]

7.4.1 Adaptive Dependability/Security Protection

Normally, there exist two sets of protection systems at each terminal for a HV or EHV line. For example, it may use one set as high-speed primary protection and one set as back-up for a 138kV line. For a 345kV line, it may either use dual high-speed primary systems or one primary and one backup with a single battery system. For 500kV and 765kV lines, it almost always uses dual high-speed primary systems with dual battery systems to protect the backbone of the bulk transmission system.

Individual utilities have several options for their primary system: a directional blocking scheme (DCB), a directional un-blocking scheme (DCUB), a permissive over-reach transfer trip scheme (POTT), or a permissive under-reach transfer trip scheme (PUTT) scheme. The DCB and POTT schemes are more favored by some utilities than others. The primary schemes are always accompanied by back-up schemes using zone 2 and/or zone 3 distance elements together with ground time overcurrent relays. Phase instantaneous relays may also be used. Thus, for some fault locations, there may be four to six functional units within a line protection package that sense the fault. For example, for a close-in fault, the zone-1's of protection systems #1 and #2, the DCB schemes of primary systems #1 and #2, and the instantaneous overcurrent units of overcurrent relays #1 and #2 will be able to "see" the fault. Each of the functional units indicating a fault will issue a command to the CB trip coil to clear the fault. Even for a fault outside the protection range of the primary system, e.g. for a remote bus fault, the zone-2's of protection systems #1 and #2 and the time overcurrent units of protection systems #1 and #2 will detect the fault, and arm the trip logic, hence, it is highly likely that a fault will be cleared in time.

In the above conventional schemes, if any relay unit indicates a fault within its protection zone, it will issue a command to its associated breaker(s) to trip the faulted line. However, this high dependability may also hurt the system at the cost of security because of the increasing probability of undesired tripping, especially when the system is stressed and the security of the protection system is favored. Thus, under stressed conditions, we may want to alter the trip logic, requiring two or three relay functional units to indicate a fault simultaneously before sending out a trip signal to the breaker(s). Another scenario is, when Hidden Failure Monitoring observes some abnormal conditions in relay systems, it is desirable to trigger Hidden Failure Control to temporarily disable the questionable protection sub-system or enable the Voting Scheme proposed in the next section. Through this approach, the bias is toward security and stopping possible relay involvement in the disturbance triggering or propagation.

7.4.2 Implementation of Adaptive Dependability/Security Protection

Adaptive Primary Protection Implementation

There are two independent functions for the primary protection of an EHV transmission line: 1) Zone 1 distance and instantaneous overcurrent protection, and 2) High-speed pilot scheme (carrier current function). The proposed Adaptive Primary Protection logic is shown in Figure 7.6 (Part 1) and Figure 7.7 (Part 2). These functions are highly dependable (during normal conditions) yet adaptive (during stressed conditions). The adaptability of this design is realized via the control block "Voting Scheme" shown in the logic diagrams. The voting scheme will only be enabled when pre-defined criteria are met during stressed conditions.

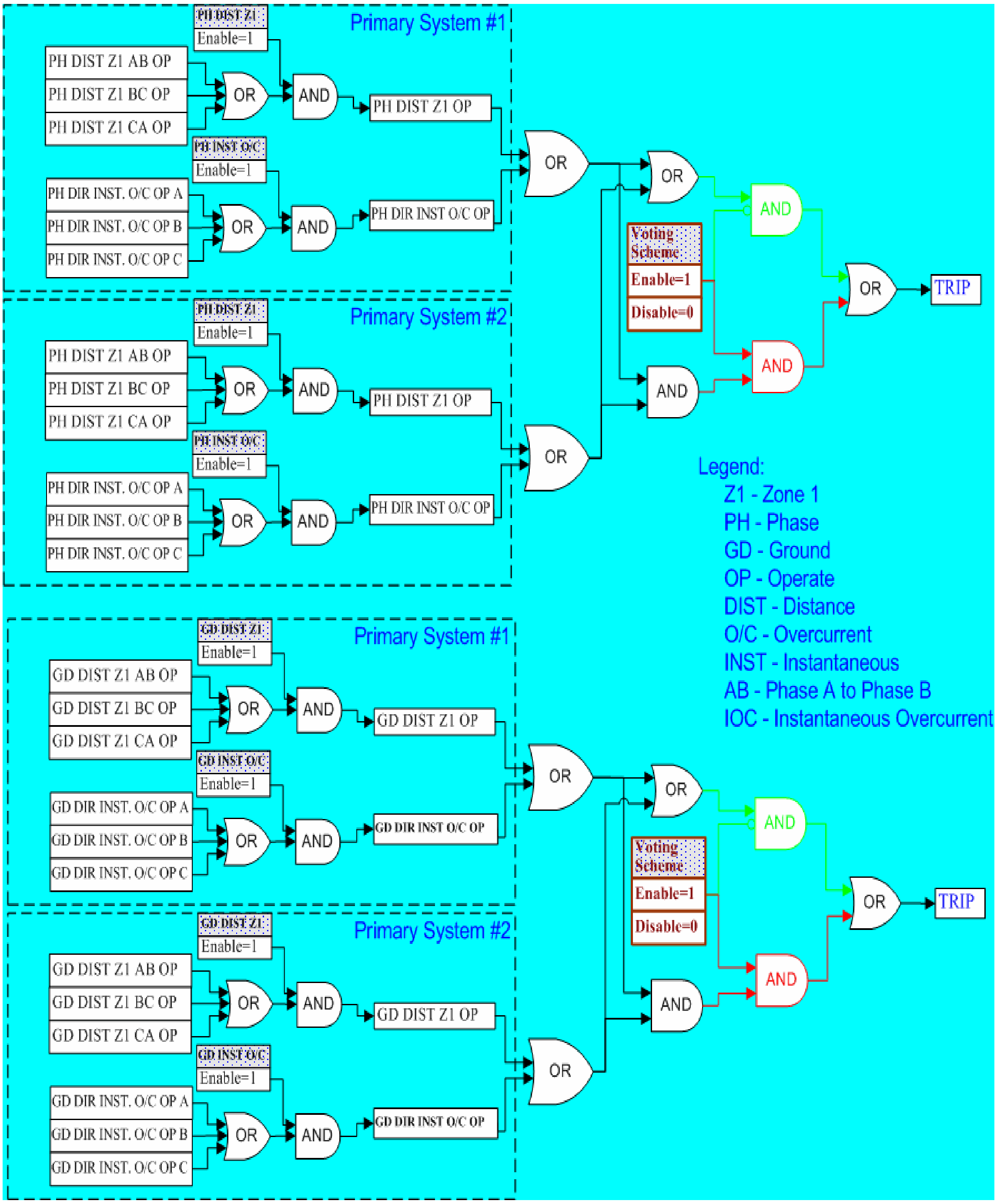


Figure 7.6 Adaptive Primary Protection Logic - Part 1:

Distance & Overcurrent Function

1) Normal operating conditions

The ADSP logic of Zone 1 distance and instantaneous overcurrent primary protection is presented in Figure 7.6. When a power system operates at normal forecast conditions, the voting scheme will be de-activated. Circuit breakers will be controlled by the upper AND gate (displayed in Green) in each primary system, which provides a highly dependability-oriented protection. As shown in Figure 7.6, two sets of primary systems with identical functions are used in this scheme; however, they are normally supplied by different vendors to minimize the risk of common failure modes due to the same design or production procedure problem.

For each type of fault (phase or ground fault), two types of fault detectors (Zone-1 Distance and Instantaneous Overcurrent) in each primary system will respond to a fault within their respective protection zones and send an independent trip command to the circuit breaker(s) immediately. This function layer will provide up to four levels of overlapping protections for 50%-90% of the transmission line.

Co-existing with the distance and instantaneous overcurrent functions in Figure 7.6, dual sets of carrier current functions (DCB scheme) employed in Figure 7.7 can each provide high-speed protection for 100% of the subject line. Each set uses its own fault detectors, which are also independent from the fault detectors used in Part 1 of implementation of the primary scheme. In total, we have four independent sets of 100% line fault detections for ground faults and two independent sets for phase faults in the Part 2 deployment.

Normally, a Zone-3 element in a distance relay is used as the fault detector for the DCB scheme. A fault within its zone of protection will arm the relay but will be blocked from tripping until a carrier current signal is received from the remote end, indicating a fault is on its protected line instead of on a downstream line. More detailed information on the mechanism of pilot schemes (DCB etc.) can be found in a number of textbooks. [25]-[28]

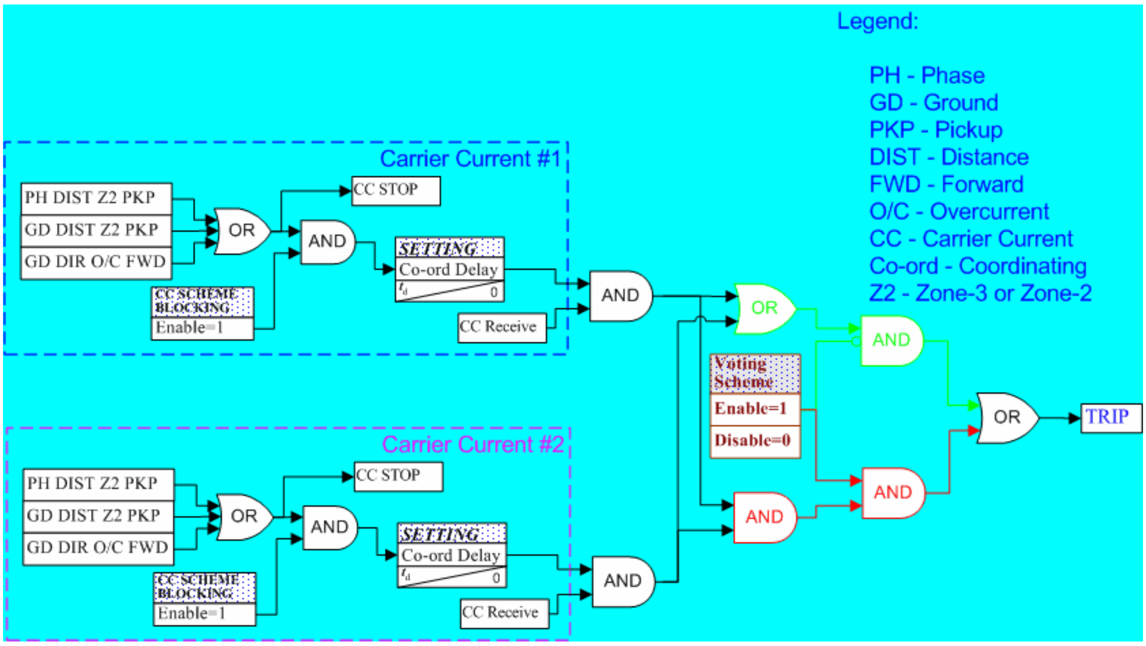


Figure 7.7 Adaptive Primary Protection Logic - Part 2:
Carrier Current Function

2) Stressed/emergency operating conditions

If there is a fault or outage occurring in a neighboring line, the voltage/current magnitude and/or load flow direction will change. These external signals will be fed into the Voting Scheme block to determine whether the carrier current protection scheme needs to be more secure to avoid a false trip. Several levels of security can be achieved based on a set of pre-defined rules. A lookup table is provided to facilitate the decision-making. This lookup table will be site-specific and determined by off-line simulation of various multiple contingencies and desirable protection needs at a substation.

Once the Voting Scheme is activated, the circuit breaker will be controlled by a trip signal flowing through the lower AND gate (in Red) as shown in Figure 7.6 and Figure 7.7. A trip signal will not be issued to the circuit breaker(s) until the elements with identical function (e.g. distance Zone-2 fault detector) in both primary systems sense the fault and send out a trip command. This design will ensure that any single defective element with hidden failure will not misoperate the line and exacerbate an already stressful condition. Since it is highly unlikely that the elements of similar function from two different vendors would experience the identical failure mode, this Voting Scheme will effectively prevent line misoperation due to relay hidden failure, thus stopping the propagation of system disturbances and preventing wide-area system failures.

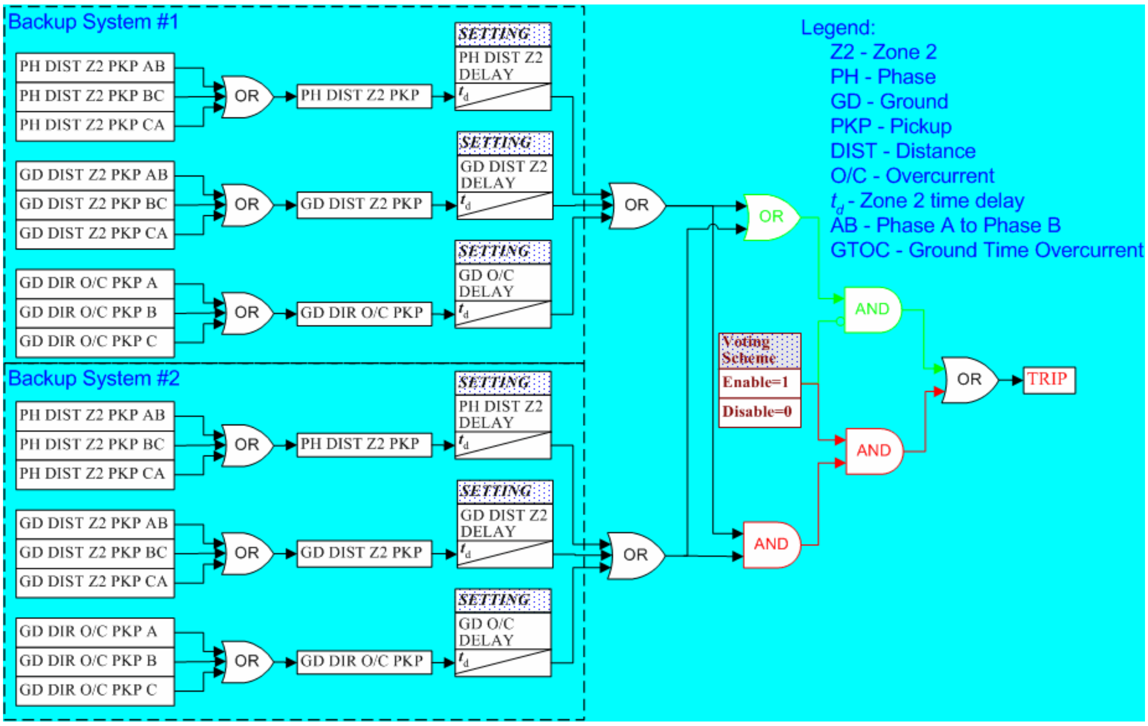


Figure 7.8 Adaptive Zone 2/GTOC Backup Protection Logic

Adaptive Backup Protection Implementation

Different types of relay schemes have different susceptibilities to hidden failures, hence different possibilities of misoperations. Zone-2 or 3 distance schemes are normally used as backup protection for transmission or sub-transmission lines. Due to their open zone protection nature, they are the most likely schemes that may cause misoperations.

For backup Zone-2 & Ground Time Overcurrent (GTOC) and Zone-3/GTOC protection schemes, similar adaptive implementations are proposed in Figure 7.8 and Figure 7.9. As shown in Figure 7.8 and Figure 7.9, each design also consists of two sets of backup systems chosen from different vendors such as GE, SEL or ABB etc.

For each sub-system within the dashed box in the figures, three protection functions are provided by a Phase Distance Unit, a Ground Distance Unit, and a Ground Directional Overcurrent Unit against phase or ground faults. No Phase Directional Overcurrent Unit is integrated, although commonly used in sub-transmission systems (69kV and below) among utilities. Since protection zones of backup functions extend to the downstream lines, the backup units are prone to over trip and cause undesired outages. The ADSP design provides the most benefits in backup function relays.

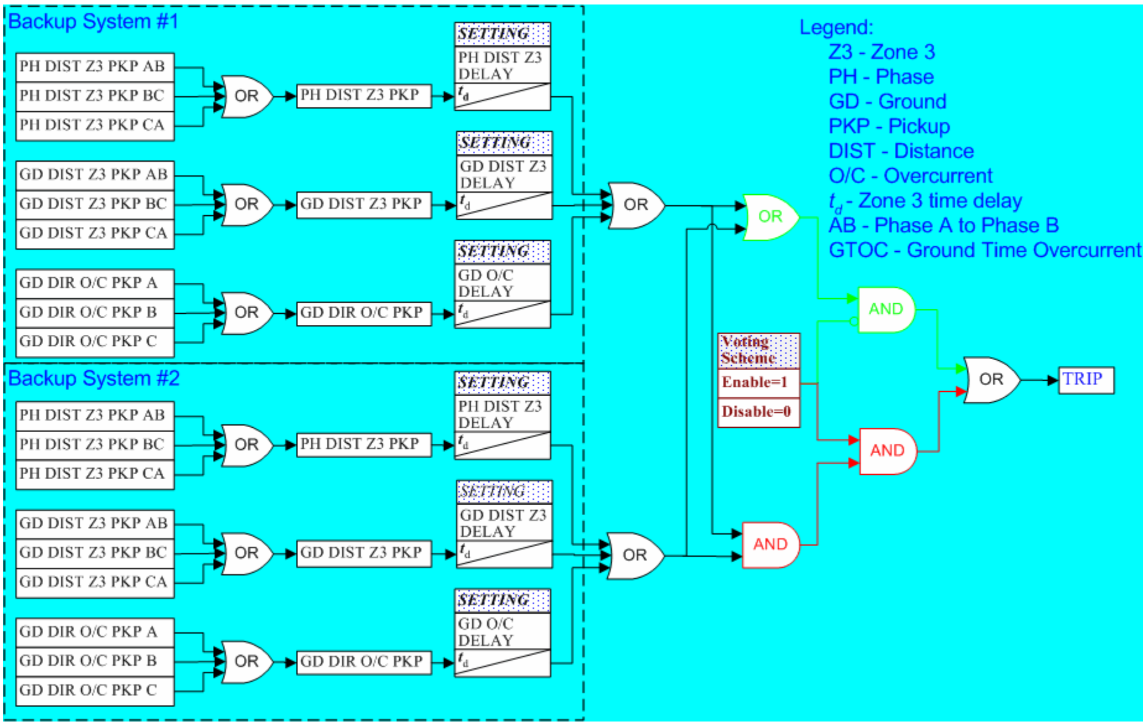


Figure 7.9 Adaptive Zone-3/GTOC Backup Protection Logic

As explained in the previous section, the proposed backup protection logic will also adapt to prevailing conditions by being highly dependable during normal system conditions and being more secure during abnormal system conditions when the Voting Scheme is activated.

Adaptive Emergency Load Protection Implementation

Another scenario causing relay misoperations results from unexpected load re-dispatching following faults and/or equipment outages. To deal with this situation, an adaptive algorithm is proposed as follows.

Normally, the pickup setting of Zone-3 with the mho distance characteristic should be guaranteed not to trip with maximum possible load flow under normal conditions. The emergency load during abnormal conditions may exceed the maximum possible load flow under normal conditions. Sometimes, it is not desirable to limit Zone-3 pickup by the minimum load impedance corresponding to emergency load condition. One obvious reason for this is that it may cause Zone-3 being set too low to provide necessary backup protection for downstream lines, especially when the remote end station is a strong source with a lot of infeed. More commonly, we may not know what the maximum emergency load is, or the load magnitude may be deemed highly unlikely when setting the Zone-3 relay.

Although most modern digital relays provide a *Load Encroachment Function* [17], which is used for heavy load conditions, we may not want to use this function for emergency load conditions, since the Load Encroachment Function may limit the relay's capability of tripping a high resistance fault, which may fall into the operating range of load encroachment shown in Figure 7.10.

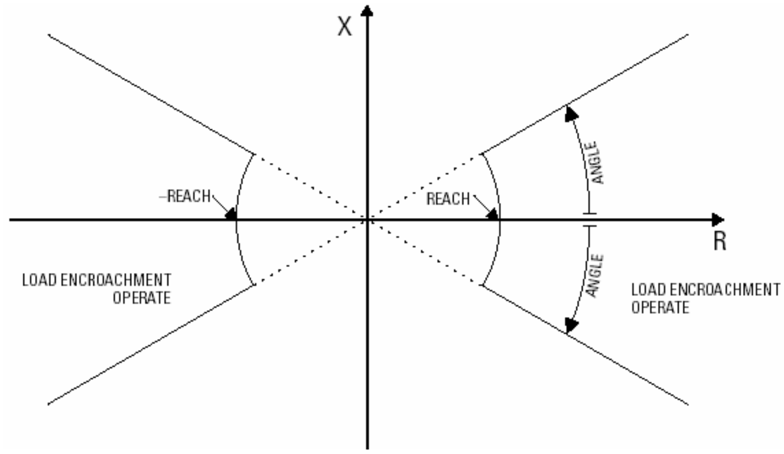


Figure 7.10 Adaptive Load Encroachment Characteristics

One appropriate solution may be to use the load encroachment function when we need it, i.e. enable this function only when a favorable condition justifies it. The triggering conditions can be either the outage of an adjacent line or other preset abnormal conditions.

However, a better approach may be to make the reach of load encroachment characteristics adaptable by continuously monitoring the load flow existing on the line. The reach is initially set based on the minimum load impedance (maximum possible load) that the relays might see under normal conditions, and then adjusted automatically based on load impedance and a supervising voltage threshold. The supervising voltage is used to distinguish a fault scenario from an emergency load condition.

This adaptive algorithm can further relax the reach limit imposed by the expected maximum load flow under normal conditions. The reach is set based on the actual line flow rather than the expected maximum load flow. This provides the maximum resistive coverage while maintaining a safe margin from the load impedance.

It should be noted that all of the above adaptive logics are designed to respond to local control signals, e.g. voltage and/or current signals; however, the Voting Scheme and adjustable reach of load encroachment function can also react to remote control signals from remote stations or a Regional Control Center. It is not clear at this moment if the remote control signal is reliable enough to be brought into the adaptive protection logics. We must ensure that any remote control signal is trustworthy before using it.

7.5 The Misoperation Tracking Database (MTD)

Misoperation data availability is critical to the probability evaluation of relay hidden failure and the deployment of the HFMCS. The IEDs in a substation capture sequences of events and oscillography during fault or other abnormal conditions, and the Data Concentrator polls these data periodically from all involved IEDs in the events. These data are valuable to the performance analysis of relays and other automatic devices at a substation when misoperation occurs. The Misoperation Tracking Database (MTD) for the HFMCS on a central file server at Control Center polls these misoperation data from Data Concentrators across the whole system and archives them in a data warehouse for future analysis. The MTD serves as a consistent access point for documenting and tracking automatic equipment operations. The retrieval of these data can be separated from the dedicated and secure Hidden Failure Control and SCADA network. The MTD will be connected to the SCADA network via firewall and to the corporate network, so it can be accessed by authorized users connected to the corporate network.

This central repository not only furnishes information to protection and control (P&C) personnel, station equipment specialists, supervisors, power quality investigators, system planners, marketing personnel, distribution engineers, and power plant personnel, but also provides a powerful tool for hidden failure analysis. By conducting statistic analysis on the data from the MTD, relay engineers or decision-makers will be able to identify vulnerabilities or bad designs in the protection systems; hence, corresponding countermeasures can be deployed. MTD data also helps to identify problem areas requiring maintenance attention, or to spot trends in protection system malfunctions and equipment failures, which assists decision-makers in efficiently prioritizing and matching available resources with to system needs. Further, the LAN-based nature of the Misoperation Tracking Database facilitates the prompt dissemination of automatic equipment investigation information during times of transmission system emergencies, customer service disruptions, or serious protective system malfunctions.

7.5.1 Structure of the MTD

Level One

The design of the MTD database can be implemented in two levels. Level 1 is a pool of every misoperation and all operations initially investigated as a potential misoperation; however, every operation in the transmission system should be examined to confirm that automatic station equipment is performing as intended. Conducting this analysis is especially important, as extended maintenance intervals and reduction of the frequency of actual site visits are becoming common practices among utilities. It is realized that varying amounts of information are available to the operation analyst in each situation. Sometimes records from Digital Fault Recorder (DFR) are plentiful, sometimes not. Sometimes relay targets are quickly available, sometimes not. Likewise, Data Acquisition System (DAS) information may or may not be available. The important point is that an operation should be analyzed with what information is available and, where appropriate, an MTD record (see section *7.5.2 Event Report*) should be prepared (it should be noted that most operations are proper and do not necessarily require preparation of an MTD record). Finally, documenting the proper (or improper) performance of automatic schemes enables relay engineers to draw comparisons between areas and to take corrective action where necessary. This information provides a key index for prioritizing new installations or upgrades when deploying the HFMCS.

Level Two

After filtering out the normal operations of automatic station equipment, each misoperation should be categorized based on the equipment type and further sub-categorized at the component level. For example, the cause of a misoperation should be investigated, and the involved equipment should be identified as one of the following:

- Circuit Breaker/Switch

- Relaying (Contact, timer, seal-in circuit, etc.)
- Carrier Set (Receiver, transmitter, tuning unit, line trap, etc)
- Current Transformer
- Capacitor Voltage Transformer (Coupling capacitor, …)
- Communication Channel (Pilot wire, fiber optical equipment, etc.)
- DC Battery
- SCADA
- Cable
- Others

7.5.2 Event Report

The basic record in the MTD database is a misoperation report—an Event Report—on protection and control automatic equipment in the substation. Each record documents a misoperation event. A misoperation event is an instance where station equipment (such as relaying, or circuit breakers) operated automatically in response to some initiating cause. The Working Group on Protective Relaying Performance Criteria of the IEEE Power System Relaying Committee defined a standardized protective relaying performance reporting system in 1992 [99]. The misoperation report for the MTD contains valuable information for risk assessment of hidden failure and the deployment of the HFMCS:

- Time and date of the misoperation
- System and weather conditions (e.g. any lighting, any overload) when misoperation occurs
- Cause and consequences of the misoperation
- Customer outages
- Relay targets
- Equipment involved in the misoperation event
- Equipment information (manufacturer, model, serial number, year manufactured)
- Components failed and failure mode

- A brief description and analysis of the nature of failure
- Others

The component failure mode in the MTD record is used to identify/classify the failure modes of various components. The data are vital to evaluating the past performance of each component and helping predict the performance of future designs. Similarly, information on resulting customer outages (if any) will also be useful for future system impact evaluation under the risk assessment framework.

Each misoperation can be individually identified as *Improper but Desired*, *Improper & Undesired*, *Engineering Error*, *Design Error*, *Component Failure*, etc., in its Operation Category. A sample misoperation report is shown in Figure 7.11.

Misoperation Report Format

Report Status:______________ **Date of Report:**__________________

Company: __________________________________ **Region:** ___________ **Area:** ________

Date of Failure:_____________ **Time:** ____________ **Events:** ______

Station: ___________________ **Circuit:** ____

Weather Condition: _________________________________ **Lighting?** _____________

System Condition: __________________________________ **Overload?** _____________

Fault Cause: _______________________________________ **Faulted Phase** __________

Equipments: ____

MFR _______________ **S/N** ______________ **TYPE** ____________ **kV** __________

Manufactured Year ____________________ **Other** _________________________

Operation Category ____________________ **Customer Outage** _______________

Consequence ____

Component Failed ____

Component Failure Mode ____

Relay Targets ____

Other Equipments Involved ____

____

Remarks (Nature of trouble, Analysis, etc.) ______________________________________

____

____

____

____

Action Taken/Required ____

____

____

Follow Up ____

____

Reported By ____________________ **Title** _________________ **Phone** ______________

Figure 7.11 Format of Sample Misoperation Report

7.5.3 Implementation Considerations for the MTD

It is advisable to prepare a misoperation report as soon as possible following the initial analysis of an equipment operation. Having the information immediately available in the MTD database will likely be an aid to other personnel participating in an investigation. Regional and senior management may also be interested in prompt information on automatic operations, particularly for high-profile system failures.

Multiple Misoperations in a Single Misoperation Report

Since it is not unusual for two or more protective schemes to activate for a single abnormal event, the entry screen for the MTD should facilitate reporting multiple associated misoperations triggered by the same event, so multiple records may be assigned the same event number.

Successive Misoperations in Separate Misoperation Reports

This is a judgment call that depends on factors such as the overall time span, whether DFR records are available for the various operations, whether relay targets were retrieved during the course of events, and simple common sense. In the case of a permanent transmission line fault (due, perhaps, to a broken insulator), a single MTD report might suffice to describe the fault and the misoperations. On the other hand, a single report would not be appropriate if a storm moved through an area and caused multiple operations on a transmission circuit over a period of minutes (or hours). Here, if DFR records and HFM information are reasonably available, separate event reports should be prepared to document each known misoperation.

Trip Check Errors

The MTD database is chiefly intended as a means for analyzing hidden failures and deploying the HFMCS, as well as keeping and distributing information on automatic equipment operations, on whether those operations were proper or not, desirable or not, and whether customer service was impacted (particularly for misoperations). Normally, trip check errors themselves are not to be characterized as a misoperation in utilities;

however, most trip check errors do result in subsequent automatic equipment operations which, in turn, may either be proper or improper (that is, a misoperation). For the purposes of the MTD system, it is desirable to document whether the subsequent control system action was proper or not. It is also recommended to include a full explanation of the error itself in the MTD record, and the error and its cause should be thoroughly investigated by the responsible engineer for future hidden failure prevention.

Reports Generation

Accessing the MTD database can provide a tabular listing of all reported equipment misoperations for each region. The misoperation report can be sorted by Date, Location, Voltage Level, Trigger Event, or Relay System Involved; it can show at a glance whether multiple misoperations occurred, whether a customer outage resulted, and whether the report is preliminary or final. Details for any particular equipment operation listed in the tabular listing can be obtained by double-clicking on the record of interest.

Quarterly reports can also be generated automatically for managerial use from data maintained in the MTD system. Such reports summarize and broadly classify the number of misoperations and the customer outage impact occurring each quarter. Comparisons can be made between regions and between areas, and trend reports can be used to show the changes in key measures over time.

Naming Conventions for IED Files

There are many stations and many IEDs in each station, and some of the station names are the same. Therefore, it is important to create unique IED file names based on some specified information such as state, utility owned or not, voltage level, station name, IED's manufacturer, device ID in station, etc. This will help users quickly find the information of interest.

Database Access

Though it is assumed that database access will take place through a LAN, it should also be capable of supporting remote dial in access.

7.6 Implementation Considerations for the HFMCS

The implementation of a system-wide HFMCS is a capital-intensive project to any utility. It cannot be rolled out in a large scale. For a new build substation, it is recommended to include all the functions proposed in this chapter; therefore, this project type requires installing the complete set of the Distributed Monitoring and Control (DMC) modules. For substation work other than a new build, such as a line relay replacement or circuit breaker replacement, the DMC can be built to "integrate as you go." In other words, for a line relay replacement, the implementation will allow integrating only the modules for that particular line. The rest of the substation remains untouched until future work is performed. The approach will result in some functionality loss of the DMC system for the existing substation; if the risk assessment of catastrophic failures indicates that a higher risk of system failure is associated with the malfunction of a line at the substation, a fully functional DMC system should be implemented regardless.

To minimize the cost of equipment, spare parts, engineering and design, training, and installation, the proposed DMC can share with SCADA some hardware, such as transducers, or use an existing Data Concentrator used by SCADA as the Station PC for the DMC. This will minimize the installation of HFMCS specific equipment; the HFMCS shall not decrease the reliability or performance of the SCADA system. Through this approach, reliability can be improved at a manageable cost.

7.7 Security of the HFMCS

As already mentioned in previous sections, the HFMCS is devised to improve the reliability of protection systems. Since the HFMCS is required to operate in an indoor or outdoor (harsh) environment, which includes wide temperature ranges, dusty environments, electrical noise (EMI, EMC, and RFI), etc., the HFMCS, in turn, depends on the reliability of the hardware infrastructure. What is more, the HFMCS, like the SCADA network, also faces a myriad of threats from both external and internal sources.

A major issue related to network connected stations is obviously security. With more and more information sharing across the corporate WAN, increased remote access through public communication services (e.g. leased phone line), and popular use of network compatible equipment within substations, the rising threat of electronic intrusions[4] against a utility or substation has been a growing concern among utilities, since these intrusions may cause regional and possibly even widespread power outages. Due to the nature of the HFMCS and its direct interface with IEDs, the security of the HFMCS against electronic intrusions is becoming even more important.

Similarly to the SCADA network, the most vulnerable link in the HFMCS is the remote access point, either via dial-in or a network access point. This connection creates a pathway to another network (e.g. Corporate WAN), which introduces security risks from the Internet. It is advised to limit these kinds of access to the HFMCS from the corporate WAN as much as possible.

The security of the SCADA network has been widely addressed and implemented in the power industry. [104]-[109] These techniques and procedures used by SCADA, such as strong access restrictions, audit logs, authentication, encryption, internal firewalls, intrusion detection systems (IDS), and network topologies, can also benefit the HFMCS and reduce risk to a tolerable level. Secure routers will serve as interfaces to the network connected stations. MTA database access restrictions and disk mirroring techniques can be used to minimize these security vulnerabilities. Different tiers of authorized users will be assigned corresponding privileges to limit the risk of exposure of critical functions.

---

[4] *Electronic Intrusions – Entry into the substation via telephone lines or other electronic-based media for the manipulation or disturbance of electronic devices. These devices include digital relays, fault recorders, equipment diagnostic packages, automation equipment, computers, PLC, and communication interfaces. [102]*

Chapter 8 Conclusions and Future Research

A major power system disturbance is mitigated via protection and control actions; however, the present protection and control practices are not designed for cascading outage of power apparatuses. Additionally, power system deregulations present new challenges to relay engineers. They require that relay engineers work more closely with planning and operating engineers to ensure that the drive to maximize profits does not sacrifice the reliability of power system operations.

How to stop the propagation of cascading outages and minimize the impact of the disturbance has drawn considerable interest from government agencies, electric utilities, and manufacturers, as well as academic researchers. The risk assessment framework for catastrophic system failures and the Hidden Failures Monitoring and Control System established in this dissertation provide promising tools for utilities to embrace the challenges in a competitive electricity market.

The risk assessment framework is capable of identifying possible system weak links, while the HFMCS provides bottom line benefits by accurately tracking and predicting the substation equipment performance. Information about system weak links and apparatus performance is the cornerstone of the decision-making process.

8.1 Contributions of the Dissertation

In Chapter 1, the following major questions were asked in response to the challenges imposed on utilities in today's digital society:

- ✓ *How can hidden failures in protection and control systems lead to catastrophic failures?*
- ✓ *What is the framework for global system vulnerability assessment?*
- ✓ *How to strengthen the weak link?*

Several key contributions have been made by answering those questions.

1. Mechanism of catastrophic failure in power system

As shown in the analysis of the 1977 New York Blackout in Chapter 3, several hundreds of relays may be involved in a large disturbance in a power system, and most of the involved relays and circuit breakers operated properly to protect equipment from damage and maintain the healthy portion of the power system to continue safe operation. However, relays exposed to hidden failures may unnecessarily trip unfaulted lines. Hence, in addition to the faulted line, we may have two, three, or more simultaneous line openings, usually (but not necessarily) located in the vicinity of the triggering event.

These misoperations exacerbate the stressed conditions of the power network, and may, in turn, cause more lines overloaded and tripped. This sequence of events finally led to the 1977 New York Blackout, 1996 WSCC Blackout, and other catastrophic failures. The 1977 New York Blackout analysis exhibits how hidden failures can contribute to system vulnerability. Based on the analysis, the disturbance propagation mechanism is revealed, which projects an efficient means to evaluate the risk of catastrophic failure.

2. ***Risk assessment framework to identify system weak link***

As part of the effort to set up the risk assessment framework, a statistical analysis of disturbance reports based on the NERC disturbance database was presented to illustrate the disturbances profile in power systems, then the methodology to evaluate the probability of relay hidden failure was discussed.

By introducing the Dynamic Event Tree/Probabilistic Event Tree, the probability of power system catastrophic failures due to relay hidden failures can be evaluated. A power flow program is used to determine the consequence of each trigger event. By combining the probability and impact index, the risk assessment framework for global system vulnerability assessment is established.

Under the proposed framework, a continuation power flow program is first used to fast-screen a list of locations most probably leading to system failures, which greatly alleviates the computation efforts needed. The issues relating to the load and generation uncertainties for the risk assessment of system vulnerabilities are addressed. Detailed simulation flowcharts for four different types of generating units (i.e. thermal, hydro, nuclear, and pump-storage) are developed and implemented in Fortran language.

3. Hidden Failure Monitoring and Control System

One of the significant contributions of this study is the development of the HFMCS. Three main functional modules–*Hidden Failure Monitoring, Hidden Failure Control* and *Misoperation Tracking Database*–and their designs are presented. Hidden Failure Monitoring provides the basis that allows further controls to be initiated. Hidden Failure Control is realized by using Adaptive Dependability/Security Protection, which can effectively stop possible relay involvement in the disturbance triggering or propagating under stressed system conditions or some abnormal conditions (e.g. relay hidden failures) in relay systems. These abnormal conditions are alarmed by the Hidden Failure Monitoring module. By enabling the Voting Scheme or temporarily disabling the questionable relay functional unit in the adaptive protection logic, security of protection system is maintained, and the risk of system catastrophic failures is minimized.

As an integrated part of the HFMCS, a Misoperation Tracking Database is proposed to track the performance of automatic station equipment, hence facilitating the risk assessment of catastrophic failures to develop a prioritized list of system weak links for the deployment of monitoring and control modules. It will also help decision-makers efficiently prioritize and match available resources with the many needs of the utility's system.

4. Adaptive Dependability/Security Protection

The intelligent adaptive protection and control techniques developed in this dissertation allow protective devices to adapt to changing system conditions, thus minimizing the risk of system catastrophic failures. As the core of the Hidden Failure Control module, three layers of ADSP logic have been developed, i.e. *Adaptive Primary Protection*, *Adaptive Backup Protection*, and *Adaptive Emergency Load Protection*. They are applicable for different scenarios. Adaptive Primary Protection is used to prevent the hidden failure modes of Zone-1 distance elements (reach or timer) and carrier current schemes, while Adaptive Backup Protection mainly works against the defects of Zone-2/3 distance fault detector or timer. Adaptive Emergency Load Protection is suitable for preventing relay from misoperating under unexpected heavy load conditions. The Voting Scheme inside these adaptive logics will be activated respectively upon meeting certain pre-defined criteria.

8.2 Implications, Limitations and Suggestions for Further Research

The risk assessment proposed in the study in place of reliability evaluation for catastrophic failure can evaluate the likelihood of subsequent protection misoperations following a triggering event. It will help system planning engineers and/or decision-makers answer questions like how, where, and when to reinforce systems at a minimum cost. It can also assist system operators in determining what and where actions should be taken to avert problems and prevent cascading failures, thus improving customer service reliability and enhancing customer satisfaction.

The proposed risk assessment framework and the HFMCS can also benefit infrastructure systems such as information, telecommunications, transportation, health care, finance, water supply, and the oil and gas distribution network; however, the technology would need further development to tailor it to the needs of a specific area.

The severity index evaluation is currently subjected to static state consideration. The impact of a disturbance is assessed by running a load flow program. The loss of load is determined if a node (bus) is isolated from other parts of the system. If the load flow program does not converge, it is assumed that the studied scenario experienced a voltage collapse, which is not quantified. For the sake of simplicity, voltage collapse is treated as a loss of the whole system. This may not be true if we take into account the Special Protection System actions such as load shedding, system islanding, etc. Voltage collapse scenarios indicated by a load flow program will not necessary occur in actual system operation. Since a power system is a large-scale closed-loop feedback system, an initial unfavorable condition (e.g. the reactive/active power unbalance due to line outage) will be continuously corrected by numerous control systems. For example, voltage sag may be corrected by an automatic tap-changing transformer or adjusted by the excitation system of nearby generation units to maintain system voltage within its required range. The impact of load-resource unbalance due to generation rejection or line outage may also be temporarily absorbed by load frequency characteristics. These are all beyond the limit of a load flow program. Combining this work with the work on transient stability by Drs. De La Ree and Elizondo would be a productive extension of this study.

Due to the limited scope of the study, the production simulation does not consider the force outage rate of tie lines between two areas; however, it does have the capability to consider plan outages (for maintenance purposes) of units, and the scheduled outage of tie lines can be given as input to the program. The simulation also assumes that no congestion exists within each sub-area. If congestion does exist, the program has to divide the area into two sub-systems and treat the congested line as a tie line. It may be relatively easy to enhance the production simulation by simulating the forced outage of units randomly. Currently, the program adopted a trade-off approach by modifying the Effective Unit Capacity using a unit's forced outage rate.

The current risk assessment process requires running several stand-alone programs. It may be more efficient to combine them to evaluate a system automatically. However, combining them and making the program run smoothly on a large-scale system (commercial grade) is not an easy task.

Another promising expansion to the study may be to take advantage of the phase measuring capability of the newest IEDs, such as SEL 421. Integrating real-time measurements of system state based on PMU and accurate measurement synchronization techniques derived from GPS into the HFMCS will enable the Hidden Failure Control module to respond to distant major events. Adaptive out-of-step protection is an example of such applications. [32]

In the mid-1980s, EPRI sponsored the research and deployment of a disaster-related technology known as the "National Lightning Detection Network (NLDN)," which consists of hundreds of electromagnetic sensors across the country that trace the cloud-to-ground lightning, generating real-time lightning field data, which are sent to a control center via communication satellites and shared by participated power companies to avert lightning outage. The timely lightning data, displayed in a map of United States, prepare the power companies with adequate lead time for possible lightning strikes on the grid.

Similarly, combined with the risk assessment framework proposed in the dissertation, a Geographic Information System (GIS) could be a great asset in analyzing and mapping vulnerability. It could also be used to train system operators, planning engineers, and others who are responsible for response to catastrophic failures.

Bibliography

[1] White Paper, The Clinton Administration's Policy on Critical Infrastructure Protection: *Presidential Decision Directive 63*. [On line]. Available: http://www.fas.org/irp/offdocs/paper598.htm.

[2] NERC Disturbance Data. [On line]. Available: http://www.nerc.com/dawg/.

[3] A.G., Phadke, J.S. Thorp, “Expose Hidden Failures To Prevent Cascading Outages [in power systems],” *IEEE Computer Applications in Power*, Vol. 9 Issue 3, July 1996, pp20-23.

[4] M. Amin, “Toward Self-healing Energy Infrastructure Systems,” *IEEE Computer Applications in Power*, Volume 14, Issue 1, Jan. 2001.

[5] S. Tamronglak, *Analysis of Power System Disturbances due to Relay Hidden Failures*, Dissertation submitted to the Faculty of the Virginia Tech, Department of Electrical Engineering, in partial fulfillment for the degree of Doctor of Philosophy, March 1994.

[6] J. D. McCalley, A. A. Fouad, V. Vittal, A. A. Irizarry-Rivera, B. L. Agrawal, and R. G. Farmer, “A risk-based security index for determining operating limits in stability-limited electric power systems.” *IEEE Transactions on Power Systems*, Vol. 12, No. 3, August 1997, pp. 1210-1219.

[7] W. Fu, J. D. McCalley, V. Vittal, “Risk Assessment for Transformer Loading,” *IEEE Transactions on Power Systems*, Vol. 16, No. 3, August 2001, pp. 346-353.

[8] Y. Dai, *Framework for Power System Annual Risk Assessment*, Ph.D. dissertation, Ames, Iowa: Iowa State University, 1999.

[9] S. Zhao, *Influence of Generator Rejection System Reliability on Risked-based Security Assessment*, M.S. thesis, Ames, Iowa: Iowa State University, 1998.

[10] J. S. Thorp, A.G. Phadke, S.H. Horowitz, and C. Tamronglak, “Anatomy of Power System Disturbances: Important Sampling,” *International Journal of Electrical Power & Energy Systems*, vol. 20, No. 2, February 1998, pp. 147-152.

[11] K. Bae and J.S. Thorp, "A Stochastic Study of Hidden Failures in Power System Protection," *Decision Support Systems*, Vol. 24, No. 3&4, January 1999, pp. 259-268

[12] H. Wang and J. S. Thorp, "Optimal Locations for Protection System Enhancement: A Simulation of Cascading Outages," *IEEE Transactions on Power Delivery*, Vol. 16, No. 4, October 2001

[13] G. Cauley, P. Hirsch, A. Vojdani, T. Saxton, and F. Cleveland, "Information Network Supports Open Access," *IEEE Computer Applications in Power*, July 1996, pp. 12-19.

[14] B. R. Barkovich and D. V. Hawk, "Charting a New Course in California," *IEEE Spectrum*, July 1996, pp. 26-31.

[15] J.-P. Gingras, "1998 Quebec Storm," Presentation made at the NSF workshop on Mitigating the Vulnerability of Critical Infrastructures to Catastrophic Failures, Alexandria, VA, Sept. 10-11, 2001. [On line]. Available: http:/www.ari.vt.edu/workshop.

[16] B.K., Duncan and B.G., Bailey, "Protection, metering, monitoring and control of medium voltage power systems," *2003 IEEE Technical Conference on Industrial and Commercial Power Systems*, May 4-8, 2003, pp121–128.

[17] GE Power Management, *D60 Line Distance Relay – UR Series Instruction Manual*, ON Canada, 2002.

[18] Schweitzer Engineering Laboratories. [On line]. Available: http://www.selinc.com/sel-421.htm.

[19] A.G. Phadke, "Synchronized Phasor Measurements-A Historical Overview," *Transmission and Distribution Conference and Exhibition 2002: Asia Pacific*. IEEE/PES, Vol. 1, Oct. 6-10 2002, pp 476 -479.

[20] P.K.C. Wong, "A Privatised Utility's Response to Protection Reliability," IEE Seventh International Conference on Developments in Power System Protection, April 9-12 2001, pp. 343 -346.

[21] R. N. Allan and A. N. Adraktas, "Terminal Effects and Protection System Failures in Composite System Reliability Evaluation," *IEEE Transactions on PAS,* Vol. 101, 1982, pp. 4557-4562.

[22] C. Singh, A. D. Patton, "Models and Concepts for Power System Reliability Evaluation Including Protection-system Failures,"

[23] R. Billinton, M. Fotuhi-Firuzabad, T.S. Sidhu, "Determination of the Optimum Routine Test and Self-Checking Intervals in Protective Relaying using a Reliability Model," *IEEE Transactions on Power Systems*, Vol. 17, Issue 3, August 2002, pp 663–669.

[24] G. F. Johnson, "Reliability Considerations of Multifunction Protection," *IEEE Transactions on Industry Applications*, Vol. 38, Issue 6, Nov.-Dec. 2002, pp1688–1700.

[25] Westinghouse Electric Corporation, *Applied Protective Relaying*, 1982.

[26] S. H. Horowitz, A. G. Phadke, *Power System Relaying*, 2nd edition, New York: John Wiley & Sons INC., 1996.

[27] P. M. Anderson, *Power System Protection*, IEEE Press Series on Power Engineering, IEEE Press and McGraw Hill, 1999.

[28] J. Lewis Blackburn, *Protective Relaying*, Marcel Dekker, Inc, 1987.

[29] A. G. Phadke, S. H. Horowitz, J. S. Thorp, "Aspects of Power System Protection in the Post-Restructuring Era," 2002.

[30] WSCC Relay Work Group, "Review of WSCC Disturbances—1998-1999," [Online] Available: http://www.wecc.biz/committees/OC/TOS/RWG/documents/RWG-Review_WSCC_Disturbances_1998-99.pdf.

[31] A. G. Phadke, S. H. Horowitz, J. S. Thorp, *Anatomy of Power System Blackout and Preventive Strategies by Rational Supervision and Control of Protection Systems,* ONRL/Sub/19X-SD630C, prepared by Virginia Polytechnic Institute and State University for Oak Ridge National Laboratory, Martin Marietta Energy Systems, Inc., Oak Ridge, Tennessee, January 1995.

[32] A.G. Phadke, "Hidden Failures in Protection Systems," Power Systems and Communications Infrastructures for the Future, Beijing, September 2002.

[33] D. Elizondo, *Hidden Failures in Protection Systems and its Impact on Power System* Wide-area Disturbances, MS thesis, Virginia Tech, April, 2000.

[34] IEEE PES Task Force on Applications of Probability Methods, "Bulk Power System Reliability Criteria and Indices: Trends and Future Needs," *IEEE Transactions on Power Systems*, Vol. 9, February 1994, pp. 181-190.

[35] R. N. Allan, "Effects of Protection Systems Operation and Failures in Composite System Reliability Evaluation."

[36] *CIGRE* Working Group 34.02, A.G. Phadke, et al, "Adaptive Protections and Local Control."

[37] E. M. Martínez and J. J. López Márquez, "Application of Phasor Measurement Units in the Adaptive Protection of Interconnected Systems," International conference on power systems and communication systems infrastructures for the future, Beijing China, September 23-27, 2002.

[38] G.D. Rockefeller, C.L. Wagner, J.R. Linders, et al, "Adaptive transmission relaying concepts for improved performance," *IEEE Transactions on Power Delivery*, Vol. 3, Issue 4, Oct. 1988, pp. 1446–1458.

[39] J.S. Thorp, A.G. Phadke, S.H. Horowitz, M.M. Begovic, "Some Applications of Phasor Measurements to Adaptive Protection," *IEEE Transactions on Power Systems*, Vol. 3, Issue 2, May 1988, pp. 791-798.

[40] M. J. Damborg, M. Kim, et al, "Adaptive Protection as Preventive and Emergency Control," *Proceedings, IEEE PES Summer Meeting*, Seattle WA, Vol. 2, July 2000, pp. 1208-1212.

[41] M. J. Damborg, S.S. Venkata, et al, "Examples of Adaptive Transmission System Protection Using Rapid Communication and Control," *Proceedings, MEPCON'2001*, Egypt, 2001.

[42] M. Kim, M. J. Damborg, et al, "Wide-Area Adaptive Protection Using Distributed Control and High-Speed Communications.," 14th PSCC, Sevilla, June 24 – 28, 2002

[43] J.C. Tan et al, "Intelligent Wide Area Back-up Protection and its Role in Enhancing Transmission Network Reliability," *Developments in Power System Protection, Seventh International Conference on IEE*, 2001, pp. 446-449.

[44] AEP proposes building a 765-kilovolt (kV) transmission line, [On line]. Available: http://www.aep.com/about/localissues/default.htm.

[45] R. T. Tabors, "Lessons from the UK and Norway," *IEEE Spectrum*, Aug. 1996, pp. 45-49.

[46] H. Rudnick, "Pioneering Electricity Reform in South America," *IEEE Spectrum*, Aug. 1996, pp. 38-44.

[47] M. Einhorn and R. Siddiqi, (Editors.) *Electricity Transmission Pricing and Technology*. Kluwer Academic Publishers, 1996.

[48] S. Hunt and S. Shuttleworth, "Unlocking the Grid," *IEEE Spectrum*, July 1996, pp. 20-25.

[49] M. Ilic, F. Galiana, and L. Fink, (Editors.) *Power Systems Restructuring: Engineering and Economics*. Kluwer Academic Publishers, 1998.

[50] Federal Energy Regulatory Commission Orders 888 and 889, 1996. [On line]. Available: http://www.ferc.gov/news/rules/data/rm95-9003.txt.

[51] NERC, Planning Standards, September 1997.

[52] NERC, Operating Manual, January 1998. [On line]. Available: http://www.nerc.com/~oc/pds.html.

[53] Western Systems Coordinating Council Reliability Criteria, March 1997.

[54] J. Hauer and J. E. Dagle. Consortium for Electric Reliability Technology Solutions *Grid of the Future White Paper on Review of Recent Reliability Issues and System Events*. Office of Power Technologies, Assistant Secretary for Energy Efficiency and Renewable Energy, U.S. Department of Energy, December 1999.

[55] E. Hirst and B. Kirby, *Transmission Planning for a Restructuring U.S. Electricity Industry*, prepared for Edison Electric Institute, June 2001.

[56] Vice-president's Task Force, *Report of the National Energy Policy Development Group*, May 2001.

[57] EPRI White Paper, *The Western States Power Crisis: Imperatives and Opportunities*, June 2001.

[58] Federal Energy Regulatory Commission, U.S. Department of Energy, *The Con-Edison Power Failure, July 13 and 14, 1977, Staff Report*, Washington, DC.

[59] WSCC Disturbance Report for the Power System Outages that Occurred on the Western Interconnection on July 2 & 3, 1996.

[60] C. W. Taylor and D. C. Erickson, "Recording and analyzing the July 2 Cascading Outage," *IEEE Computer Application in Power*, pp. 26-30, Vol. 10, Issue 1, January, 1997.

[61] D. N. Kosterev, C. W. Taylor, and W. A. Mittelstadt, "Model Validation For The August 10, 1996 WSCC System Outage," *IEEE Transactions on Power Systems*, Vol. 14, Issue 3, Aug. 1999.

[62] H. You, V. Vittal, et al, "An Intelligent Adaptive Load Shedding Scheme," 14th PSCC, Sevilla, 24-28 June 2002.

[63] J. C. Tan, P.A. Crossley, et al, "Sequential Tripping Strategy for a Transmission Network Back-Up protection Expert System," *IEEE Transaction On Power Delivery*, Vol. 17, No. 1, January 2002.

[64] H. G. Stoll, *Least-cost Electric Utility Planning*, John Willey & Sons, 1989

[65] P. Haase, "Charting Power System Security," *EPRI Journal*, pp. 27-31, September/October, 1998.

[66] Y. Y. Haimes, *Risk Modeling, Assessment and Management*, John Willey & Sons, 1998.

[67] Y. Haimes, D. Li, and V. Tulsiani, "Multi-objective Decision Tree Analysis," *Risk Analysis* 10(1), pp. 111-129, 1990.

[68] V. Chankong, Y. Haimes, *Multiobjective Decision Making: Theory and Methodology*, New York: Elsevier-North Holland, 1983.

[69] E. Henley and H. Kumamoto, *Probabilistic risk assessment: reliability engineering, Design and analysis*, New York: IEEE Press, 1992.

[70] T. Aldemir, N. O. Siu, A. Mosleh et al, *Reliability and Safety Assessment of Dynamic Process Systems*, Springer-Verlag, 1994.

[71] V. R. Lalli, H. A. Malec, and M. H. Packard (Eds), *Reliability and Maintainability (RAM) Training*, NASA/TP-2000-207428, July 2000.

[72] L. C. Wolstenholme, *Reliability Modeling–A Statistical Approach*, Chapman and Hall, 1999.

[73] L. R. Ferreira, J. Pugh, P. A. Crossly, R. N. Allan, and J. Goody, "Design and Reliability of Integrated Protection and Control Schemes," *Power System Control and Management*, April 16-18, 1996.

[74] IEEE/PSRC Working Group 13, "Transmission Protective Relay System Performance Measuring Methodology," September 1999.

[75] G. L. Wilson, P. Zarakas, "Anatomy of a Blackout," *IEEE Spectrum*, Vol. 15, No. 2, February 1978, pp. 38-46.

[76] P. Whwatanadate, *The Exact Probabilistic Approach for Propagation of Uncertainties*, Ph.D. dissertation, Pittsburgh, Penn.: University of Pittsburgh, 1998

[77] Glossary of Terms Task Force, North American Electric Reliability Council, August, 1996. [On line]. Available: http://www.nerc.com/glossary/.

[78] J. S. Thorp and A. G. Phadke, "Protecting Power Systems in the Post-Restructuring Era," *IEEE Computer Applications in Power*, Jan. 1999, pp. 33-37.

[79] B. Efron and R. J. Tibshirani. *An Introduction to the Bootstrap*. Chapman and Hall, 1993.

[80] C. Z. Mooney, R. D. Duval. *Bootstrapping: a Nonparametric Approach to Statistical Inference*. Sage Publications, 1993.

[81] C. W. Taylor, *Power System Voltage Stability*, New York: McGraw-Hill, 1994.

[82] H. Kumamoto and E. J. Henley. *Probabilistic Risk Assessment and Management for Engineers and Scientists*. 2nd Edition, IEEE Press, 1996.

[83] A. H. Nayheh and B. Balachandran. *Applied Nonlinear Dynamics: Analytical, Computational, and Experimental Methods*. Wiley Interscience, 1995.

[84] C. A. Canizares and F. L. Alvarado, "Point of Collapse and Continuation Methods for Large Scale AC/DC Systems," *IEEE Transactions on Power Systems*, Vol. 8, No. 1, February 1993, pp. 1-8.

[85] G. D. Irisarri, X. Wang, J. Tong, and S. Mokhtari, "Maximum Loadability of Power Systems Using Interior Point Non-Linear Optimization Method," *IEEE Transactions on Power Systems*, Vol. 12, Feb. 1997, pp. 162-172.

[86] H-D. Chiang, K. S. Shah, and N. Balu, "CPFlow: A Practical Tool for Tracing Power System Steady-State Stationary Behavior due to Load and Generation

Variations," *IEEE Transactions on Power Systems*, Vol. 10, No. 2, May 1995, pp. 623-634.

[87] M. Kubicek and M. Marek. *Computational Methods in Bifurcation Theory and Dissipative Structure*. Springer-Verlag, 1983

[88] V. Ajjarapu and C. Christy, "The Continuation Power Flow: A Tool for Steady State Voltage Stability Analysis," *IEEE Transactions on Power Systems*, Vol. 7, No. 1, Feb. 1992, pp. 416-423.

[89] J. D. McDonald, "Substation Automation: IED Integration and Availability of Information," *IEEE Power & Energy*, Vol. 1, No. 2, March/April 2003, pp. 22-31.

[90] S. Haacke, S. Border, D. Stevens, and B. Uluski, "Plan Ahead for Substation Automation" *IEEE Power & Energy*, Vol. 1, No. 2, March/April 2003, pp. 32-41.

[91] T. Nissen and D. Peterchuck, "Substation Integration Pilot Project" *IEEE Power & Energy*, Vol. 1, No. 2, March/April 2003, pp. 42-49.

[92] M. Pesin, J. Orth and D. Yuill, "Substation data integration at Tacoma Power," *Utility Automation*, Vol. 8, No. 2, March/April, 2003

[93] D. Moryc, "Automation through Integration: A New Direction for Waterloo North Hydro," *Utility Automation*, Vol. 8, No. 2, March/April, 2003

[94] S. H. Horowitz, A. G. Phadke, J. S. Thorp, "Adaptive Transmission System Relaying," IEEE PES Summer Meeting, San Francisco, July 12–17, 1987

[95] G. D. Rockefeller, C. L. Wagner, J. R. Linders, K. L. Hicks, and D. T. Rizy, "Adaptive Transmission Relaying Concepts for Improved Performance," *IEEE Transactions on Power Delivery*, vol.3, no.4, October 1988, pp. 1446-1456.

[96] L. L. Mankoff and G. D. Rockefeller, "EPRI R & D Programs With Digital Systems For Hierarchical Integrated Protection And Control," *EPRI*, Vol.17, No.1, 1989, pp. 77-87.

[97] B. Stedall, P. Moore, A. Johns, J. Goody, M. Burt, "An investigation into the use of adaptive setting techniques for improved distance back-up protection," *IEEE Transactions on Power Delivery*, Vol. 11, Issue 2, April 1996, pp. 757-762.

[98] A. G., Phadke, "Computer Relaying: Its Impact on Improved Control and Operation of Power Systems," *IEEE Computer Applications in Power*, Vol. 1 Issue 4, October 1988, pp. 5-10.

[99] Protective Relaying Performance Criteria Working Group, IEEE PES Power System Relaying Committee, U.S.A., "Protective Relaying Performance Reporting," *IEEE Transactions on Power Delivery*, Vol. 7, Issue 4, October 1992, pp. 1892-1899.

[100] The White House Office of the Press Secretary, White House Communications on Critical Infrastructure Protection, October 22, 1997. [On line]. Available: http://www.julieryan.com/Infrastructure/IPdoc.html.

[101] U.S. National Institute of Standards and Technology, Introduction to Computer Security: The NIST Handbook, NIST, Dept. of Commerce, July 20, 1994.

[102] *IEEE Guide for Electric Power Substation Physical and Electronic Security*, IEEE Standard 1402-2000, New York: IEEE, April 4, 2000.

[103] National Security Telecommunications Advisory Committee Information Assurance Task Force, *Electric Power Risk Assessment*, March 1997. [On line]. Available: http://www.ncs.gov/n5_hp/Reports/EPRA/electric.html

[104] R. I. Williams, "SCADA Security: Turning Control and Automation Systems into Hard Targets," *Utility Automation* Vol. 8, Issue 1, January/February 2003.

[105] J. Falco, K. Stouffer, et al, "IT Security for Industrial Control Systems," National Institute of Standards and Technology (NIST), [On line]. Available: http://www.isd.mel.nist.gov/documents/falco/ITSecurityProcess.pdf.

[106] "Understanding SCADA System Security Vulnerabilities," Riptech, [On line]. Available: http://www.riptech.com/industry/energy.html.

[107] P. Oman, E. Schweitzer, and J. Roberts, "Protecting the Grid from Cyber Attack Part I: Recognizing Our Vulnerabilities," *Utility Automation* Vol. 6, Issue 7, November/December 2001.

[108] P. Oman, E. Schweitzer, and Jeff Roberts, "Protecting the Grid from Cyber Attack, Part II: Safeguarding IEDs, Substations and SCADA systems," *Utility Automation* Vol. 7, Issue 1, January/February 2002.

[109] P. Oman, E. Schweitzer, and J. Roberts, “Safeguarding IEDs, Substations, and SCADA Systems against Electronic Intrusions,” [On line]. Available: http://www.selinc.com/techpprs/6118.pdf.

[110] L. A, Kojovic, J. McCall and T. Newton, “Modular Relay Architecture Unifies Protection and Control,” *IEEE Computer Applications in Power*, Vol. 11 Issue 3, October 1998, pp. 30-35.

[111] L. Mili, Q. Qiu, et al, *Task 4-5 Yearly Report of DoD/EPRI project for 2000*, November 2000.

[112] H. E. Hurst, “Long-term Storage Capacity of Reservoirs,” *Trans. Am. Soc. Civil Eng*, vol. 116, 1951, pp. 770.

[113] B. A. Carreras, D. E. Newman, I. Dobson, and A.B. Poole, “Initial Evidence for Self-Organized Criticality in Electric Power System Blackouts,” in *Proceedings of the 33rd Annual Hawaii International Conference on System Sciences*, 2000, pp. 102.

[114] P. Bak, C. Tang, and K. Wiesenfeld, “Self-Organized Criticality. An explanation of *1/f* Noise.” *Physics Review Letters*, 59, 1987, pp. 381-384.

[115] P. Bak, *How Nature Works: The Science of Self-Organized Criticality*, Copernicus, New York: Springer, 1996.

[116] P. Bak and K. Chen, “Self-Organized Criticality,” *Scientific American*, 264, 46, 1991.

[117] P. Bak, C. Tang, and K. Wiesenfeld, “Self-Organized Criticality," *Physical Review,* A38, 364, 1988.

[118] P. Bak and C. Tang, “Earthquakes as a Self-Organized Critical Phenomenon," *Journal of Geophysical Research*. B94, 15635, 1989.

[119] L. Mili, Class notes, ECPE 5714 *Robust Estimation and Filtering*, Spring 2001.

[120] J. W. Evans, “Influence of Power System Protection on System Blackouts,” in IEE Colloquium on Measures to Prevent Power Blackouts, pp. 3/1-3/3, May 27 1998.

[121] J. Fortune and G. Peters, *Learning from Failure: The System Approach*, John Wiley & Sons, 1995.

[122] J. Beran, *Statistics for long-memory processes*, New York: Chapman & Hall, 1994.

Appendix A Definitions of Key Terms

Adequacy

The ability of the electric system to supply the aggregate electrical demand and energy requirements of the customers at all times, taking into account scheduled and reasonably expected unscheduled outages of system elements.

Availability

Measure of time that a generating unit, transmission line, or other facility is capable of providing service, whether or not it actually is in service. Typically, this measure is expressed as a percent available for the period under consideration.

Bulk Power System

The portion of an electric power system that encompasses the generation resources, system control, and high-voltage transmission system.

Cascading

The uncontrolled successive loss of system elements triggered by an incident at any location. Cascading results in widespread service interruption, which cannot be restrained from sequentially spreading beyond an area predetermined by appropriate studies.

Catastrophic Failure (Disaster)

System failures with such immense impact that they inevitably receive widespread public attention and are almost always the subject of investigation.

Circuit Breaker

A mechanical switching device capable of making, carrying, and breaking currents under normal circuit conditions, and also, making, carrying, for a specified time, and breaking currents under specified abnormal circuit conditions, such as those of a short-circuit.

Contingency

The unexpected failure or outage of a system component, such as a generator, transmission line, circuit breaker, switch, or other electrical element. A contingency also may include multiple components, which are related by situations leading to simultaneous component outages.

Curtailment

A reduction in the scheduled capacity or energy delivery.

Disturbance

Unplanned event that produces an abnormal system condition.

Dynamic Event Tree

The Dynamic Event Tree approach uses simulations to track branching in system evolution at a specific number of sequence events following an initiating event. The simulations stop when a specified number of sequence events or a Top Event (System failure) is reached. The sum of scenario (event sequence) probabilities leading to a Top Event gives the probability that this Top Event will occur during the specified number of sequence events.

Event Tree Analysis

An analytical technique for systematically identifying potential outcomes of a known initiating event. An "initiating event" is anything that begins a series of actions.

Federal Energy Regulatory Commission (FERC)

Independent federal agency within the U.S. Department of Energy that, among other responsibilities, regulates the transmission and wholesale sales of electricity in interstate commerce.

Forced Outage

Removal from service availability of a generating unit, transmission line, or other facility for emergency reasons or a condition in which the equipment is unavailable because of unanticipated failure.

Hidden Failure

A hidden failure is defined to be "a permanent defect that will cause a relay or relay system to incorrectly and inappropriately *remove* a circuit element(s) as a direct consequence of another switching event."[5] All of the analyses of hidden failures for different relay schemes in the study are based on this definition.

Intelligent Electronic Device (IED)

Any device incorporating one or more processors with the capability to receive or send data/control from or to an external source (e.g. electronic multifunction meters, digital relays, controllers).

Installed Capability

Seasonal (i.e. winter and summer) maximum load-carrying ability of a generating unit, excluding capacity required for station use.

Interruptible Rate

Electricity rate that, in accordance with contractual arrangements, allows interruption of consumer load by direct control of the utility system operator or by action of the consumer at the direct request of the system operator. It usually involves commercial and industrial consumers. In some instances, the load reduction may be affected by direct action of the system operator (remote tripping) after notice to the consumer in accordance with contractual provisions.

Island

A portion of a power system or several power systems that is electrically separated from the interconnection due to the disconnection of transmission system elements.

Load

A consumer of electric energy; also the amount of power (sometimes called demand) consumed by a utility system, individual customer, or electrical device.

Load Duration Curve

A non-chronological, graphical summary of demand levels with corresponding time durations using a curve, which plots demand magnitude (power) on one axis and percent of time that the magnitude occurs on the other axis.

Load Pocket

Geographical area in which electricity demand sometimes exceeds local generation capability and in which there is an electricity import limitation due to transmission constraints.

Load Shedding

The process of deliberately removing (either manually or automatically) pre-selected customer demand from a power system in response to an abnormal condition in order to maintain the integrity of the system and minimize overall customer outages.

Must-Run Resources

Generation designated to operate at a specific level and not available for dispatch.

Nonspinning Reserve

Generation capacity that is not being utilized but that can be activated and used to provide assistance with little notification.

North American Electric Reliability Council (NERC)

A not-for-profit company formed by the electric utility industry in 1968 to promote the reliability of the electricity supply in North America. NERC consists of 10 Regional Reliability Councils and one Affiliate whose members account for virtually all the electricity supplied in the United States, Canada, and a portion of Baja California Norte, Mexico. The members of these Councils are from all segments of the electricity supply industry—investor-owned, federal, rural electric cooperative, state/municipal, and provincial utilities, independent power producers, and power marketers. The 10 NERC Regional Reliability Councils are East Central Area Reliability Coordination Agreement (ECAR), Electric Reliability Council of Texas (ERCOT), Florida Reliability Coordinating Council (FRCC), Mid-Atlantic Area Council (MAAC), Mid-America Interconnected Network (MAIN), Mid-Continent Area Power Pool (MAPP), Northeast Power Coordinating Council (NPCC), Southeastern Electric Reliability Council (SERC), Southwest Power Pool (SPP), and Western Systems Coordinating Council (WSCC). The Affiliate is the Alaskan Systems Coordination Council (ASCC).

Operable Capability

The portion of installed capability of a generating unit that is in operation or available to operate in the hour.

Operating Reserve

That capability above firm system demand required to provide for regulation, load forecasting error, equipment forced and scheduled outages, and local area protection. It includes both spinning and nonspinning reserve.

Operating Reserve – Spinning

The provision of resource capacity in excess of current and anticipated demand that is synchronized to the system and deployable for Peak Demand or Load—The greatest demand that occurs during a specified period of time.

Probabilistic Risk Assessment (PRA)

PRA is a technical analysis that systematically answers:

- What can go wrong (accident scenario)
- How likely is it to occur (probability, frequency)
  - ✓ Event tree and fault tree used to quantify likelihood
- What will be the outcome (consequences)
  - ✓ Quantification of loss of load and customer disconnected

Protection System

The electric and mechanical devices and circuitry, from sensors of the process variable to the actuation device input terminals, involved in generating those signals associated with the protective function.

Relay

An electric device that is designed to interpret input conditions in a prescribed manner and, after specified conditions are met, to respond to cause contact operation or a similar abrupt change in associated electric control circuits.

Static Relay

A relay in which the designated response is developed by electronic, solid state, magnetic, or other components without mechanical motion. A relay that is composed of both static and electromechanical units in which the designed response is accomplished by static units may be referred to as a static relay.

Reliability

The degree of performance of the elements of the bulk electric system that results in electricity being delivered to customers within accepted standards and in the amount desired. Reliability may be measured by the frequency, duration, and magnitude of adverse effects on the electric supply. Electric system reliability can be addressed by considering two basic and functional aspects of the electric system: *Adequacy* and *Security*.

Reserve

Electric power generating capacity in excess of the system load projected for a given time period. It consists of two sources: *spinning reserve* and *supplemental reserve*.

Risk

Risk is the product of likelihood and severity. Thus, a likely event with an insignificant result would not be considered risky, whereas a likely event with a serious consequence would be.

Risk Assessment

In this dissertation, risk assessment is concentrated on power system catastrophic failures.

Security

The ability of the electric system to withstand sudden disturbances such as electric short circuits or unanticipated loss of system elements.

Spinning Reserve

Ancillary service that provides additional capacity from electricity generators that are on line, loaded to less than their maximum output, and available to serve customer demand immediately should a contingency occur.

Stability

Ability of an electric system to maintain a state of equilibrium during normal and abnormal system conditions or disturbances.

Substation Integration

Integration of protection, control, and data acquisition functions into a minimal number of platforms to reduce capital and operating costs, reduce panel and control room space, and eliminate redundant equipment and databases.

Substation Automation

Deployment of substation and feeder operating functions and applications ranging from supervisory control and data acquisition (SCADA), and alarm processing to integrated volt/var control in order to optimize the management of capital assets and enhance operation and maintenance (O&M) efficiencies with minimal human intervention.

System Failure

Failures arising from sets of related activities.

Unit Commitment

Process of determining which generators should be operated each day to meet the daily demand of the system.

Voltage Collapse

An event that occurs when an electric system does not have adequate reactive support to maintain voltage stability. Voltage collapse may result in outage of system elements and may include interruption in service to customers.

Vulnerability

The probability of the system's declined ability to absorb disturbances. A result of exposure to risk factors—such as faults and load fluctuations—and also of underlying system status which reduces the system's ability to cope. Thus, vulnerability can be viewed as follows:

$$\text{Vulnerability} = \text{exposure to risk} + \text{inability to cope}$$

Vulnerability is usually assessed as a probability.

A simple and straightforward interpretation of vulnerability is the system's ability to absorb disturbances. More specific, vulnerability can be defined as the probability of a part of the network (e.g. a transmission line, a transformer, a segment of a transmission corridor, or a load center, etc.) being damaged by an abnormal condition occurring in the power system.

The following factors may influence vulnerability:

- Design philosophy associated with the specific portion of the network
- System state (Unfavorable operating condition)
- Component status and maintenance practice (Out-of-data or poorly maintained equipments)
- Emergency preparedness/Remedy (Inadequate preparations for emergencies)
- External factors such as weather, landscape, human activities, etc.

Protection systems may be at an increased level of vulnerability under stressed conditions.

Appendix B Disturbance Report Analysis

B.1 Introduction

Risk assessment of catastrophic failures [111] based on a Dynamic Event Tree has been proposed to estimate, from historical data, the probability of system failures; however, this approach requires the investigators have sufficient knowledge of the studied system.

From a global point of view, large disturbances that happen from time to time in power systems are not totally uncorrelated. This kind of global system dynamics may be intrinsic to the characteristics of the system topologies, operating practices and reliability criterion. Thus, large-scale disruptions exhibit some kind of long-time correlation. How to trace the correlation between the frequencies of the disturbances as a function of their magnitude (e.g. the loss of power, the affected area, or the energy unserved) is an important issue in long-term risk assessment of power systems.

The global dynamic properties of large power systems may be understood through the correlation analysis of long time series of historical disturbance data. Normally, the causes for individual disturbance are random. But large disturbances caused by a sequence of equipment failures (such as relay hidden failures) may have long-range dependence, and the autocorrelation function may fall off asymptotically as a power law. The Hurst exponent [112] was proposed to measure autocorrelations (serial correlations) in a time series. For $1 > H > 0.5$, there are long-range time correlations, and for $0.5 > H > 0$, the series has long-range anti-correlations. If $H = 1.0$, the process is deterministic. When the data is uncorrelated, the Hurst exponent is 0.5.

However, it is difficult to determinate such dependence due to the noise and the availability for data of thousands of events that occurred over long periods. Rescaled range statistics (R/S statistics) and scaled window variance techniques have been developed to determine dependence by suppressing the interference of noise. The Hurst exponent can be determined by applying these techniques.

Examining correlations in a time series of power system blackouts [113] shows that the large blackouts tend to correlate with large blackouts after a long time interval. The analysis also shows the existence of long-range time correlations in the power system disturbances as indicated by Hurst exponents greater than 0.5, for example; the Hurst exponent for energy unserved is near 0.7.

The results suggest that blackouts in power systems may be considered Self-Organized Criticality (SOC) phenomena [114]-[118].

In this appendix, the NERC disturbance reports [2] are analyzed in order to obtain the statistic profile of these disturbances and unveil the intrinsic relationships, hence to gain some insights into the global dynamic characteristics of a power system. Also of interest are questions such as:

- *Do the power system disturbances have long-range dependence?*
- *Do the power system disturbances follow a certain distribution, such as Exponential, Cauchy or other distribution?*
- *Can we predict the probability of catastrophic failure globally based on the historical data?*

A robust technique such as projection statistics is used to reject the extreme outliers. The bounded influence GM estimator is applied to the parameter estimation of linear regression. The analysis suggests the intrinsically unstable dynamics of power systems.

B.2 Self-Organized Criticality

In physics, a critical state is a state at which a system changes its behavior or structure radically, for instance, from solid to liquid. Physicists have noted the possibility of a “critical state,” in which independent microscopic fluctuations can propagate so as to give rise to instability on a macroscopic scale.

In a “sub-critical" state, previous changes in the system have a sufficiently weak effect upon the current state and the system states in different times are correlated only over a short period of time. The correlation falls off exponentially with time lag. On the other hand, when some parameter of the system is “tuned" to an appropriate value, a “critical" state may be reached, in which the correlation between different times ceases to decay exponentially with time lag, and in which spontaneous macroscopic fluctuations may be observed in a system.

In standard critical phenomena, there is a control parameter which an experimenter can vary to obtain this radical change in behavior. For example, in the case of melting, the control parameter is temperature. Self-organized critical phenomena, by contrast, are exhibited by driven systems which reach a critical state by their intrinsic dynamics, independently of the value of any control parameter. These dynamics of large interactive systems have been much studied by physicists.

Per Bak and his colleagues proposed a theory of Self-Organized Criticality (SOC) that provides additional insights into the evolution of complex dynamic systems [114]. They recognized that the most complex state of dynamic systems does not lie in a chaotic region but rather lies at the border between predictable periodic behavior and unpredictable chaos [115]. This state came to be known as the “critical” state, with self-similarity being its defining characteristic. Power laws are observed in complex systems exactly at this state. The surprise came when physicists realized that very different systems turned out to behave in exactly the same way close to their critical points. And what was more surprising: extremely simple models of these systems provided exact theories of their behavior. The theory of critical phenomena became a powerful framework for understanding phase transitions, and introduced the concept of “universality.” Universality means that systems sharing a small number of basic features behave identically at the critical point. Even though the theory of SOC can provide useful insights into models of socioeconomic systems, most of the progress in this field remained within the physics community.

The prototypical example of such “self-organized criticality" is a sand pile [116]. Sand is slowly dropped onto a surface, forming a pile. As the pile grows, the avalanche carrying sand from the top to the bottom of the pile occurs. The existence of the self-organized critical state is robust not only to perturbations of the initial shape of the pile, but also to changes in the type of sand used (although differently shaped grains will change the value of the critical slope). This sort of robustness makes such a state a plausible model of spontaneous macroscopic instability in systems observed in nature.

Self-organized criticality is observed in many complex systems. SOC systems have been proposed as models of a variety of physical phenomena, including earthquakes [118], volcanic eruption, and turbulence. The concept of SOC tries to explain the “repeatability” of phenomena in nature, which can obviously be observed in power laws. Such large dynamic systems as power system are driven by highly non-linear behavior, where a small external perturbation could generate a large-scale phenomenon at a critical state of the system.

Whether the power system demonstrates some kind of evidence of correlations between disturbances is an interesting question. In this chapter, a time series of power system disturbances from 1984 to 1999 that occurred in North America are examined to find the possible long time internal correlations, which may lead to new approaches to analysis and control of large disturbances. This study may also lead to the development of generic estimates of failure rates, the development of statistics on rare events such as catastrophic failures, and a better understanding of the nature and general profile of the power system disturbances in North America.

B.3 Robust Estimation Techniques

As we know, the parametric estimation theory founded by Fisher assumes an exact and a priori knowledge of the probability distribution of the residues. The maximum likelihood estimators based on this theory, such as the least squares estimator, are vulnerable to the violation of these assumptions. To deal with this problem, Huber developed the robust estimation theory in 1964. Robustness implies insensitivity to small deviations from the assumptions. Hampel expanded the theory by initiating the concepts of influence function and breakdown point. Robust estimation techniques, such as the projection statistics and bounded influence GM estimator used in the analysis of power system disturbances, are summarized briefly in the following section.

B.3.1 Projection Statistics

The projection statistics [119] are given by

$$PS_i = \max_{\|\underline{v}\|=1} \frac{\left| \underline{h}_i^T \underline{v} - \underset{j}{med}(\underline{h}_j^T \underline{v}) \right|}{C1.4826 \, \underset{k}{med} \left| \underline{h}_k^T \underline{v} - med(\underline{h}_j^T \underline{v}) \right|}$$

In order to identify outliers in the multidimensional factor space, the following steps are proposed to compute the projection statistics.

Consider the regression model $\underline{z} = \underline{H}\,\underline{x} + \underline{e}$,

$$\underline{H} = \begin{bmatrix} h_{11} & h_{12} \cdots h_{1n} \\ h_{21} & h_{22} \cdots h_{2n} \\ \cdots & \cdots \\ h_{m1} & h_{m2} \cdots h_{mn} \end{bmatrix} = \begin{bmatrix} h_1^T \\ h_2^T \\ \vdots \\ h_m^T \end{bmatrix} \qquad \underline{h}_i = \begin{bmatrix} h_{i1} \\ h_{i2} \\ \vdots \\ h_n \end{bmatrix}$$

each $\underline{h}_i$ defines a point in an *n*-dimensional space called the design space or factor space. $\{h_1 \ldots h_m\}$ are *m* realizations of a random vector $\underline{h}$.

1. Calculate the coordinate wide median

$$\underline{M} = \left(\underset{j=1,\ldots,m}{med} (h_{j1}), \ldots, \underset{j=1,\ldots,m}{med} (h_{jn}) \right)$$

2. Take all $\underline{v}_i$ of the form.

$$\underline{v}_j = \underline{h}_j - \underline{M}\,; \quad j = 1,\ldots,m$$

3. Normalize $\underline{v}_j$ by

$$\underline{\upsilon}_j = \frac{\upsilon_j}{\|\upsilon_j\|} = \frac{\underline{\upsilon}_j}{\sqrt{\upsilon_{j1}{}^2 + \upsilon_{j2}^2 + \cdots + \upsilon_{j2}^2}}$$

4. Calculate the standardized projection of $\{\underline{h}_1, \underline{h}_2, \cdots, \underline{h}_m\}$ on $\underline{v}_j$, then we have m scales Z_i, ~ Z_m

$$\begin{cases} Z_1 = \underline{h}_1^T \cdot \underline{v}_j \\ Z_2 = \underline{h}_2^T \cdot \underline{v}_j \\ \vdots \\ Z_m = \underline{h}_m^T \cdot \underline{v}_j \end{cases}$$

Z_i is an orthogonal projection, and the standard projection along the $\underline{v}_j$, direction

$$\hat{Z}_{median} = median(Z_1, \cdots Z_m)$$

$$\begin{cases} r_1 = Z_1 - \hat{Z}_{med} \\ r_2 = Z_2 - \hat{Z}_{med} \\ \vdots \\ r_m = Z_m - \hat{Z}_{med} \end{cases}$$

and

$$MAD = 1.4826 \times \underset{i=1,\dots m}{med} |r_i|$$

$$\begin{cases} P_{j1} = \dfrac{Z_1 - \hat{Z}_{med}}{MAD} = \dfrac{r_1}{MAD} \\ \vdots \\ P_{jm} = \dfrac{Z_m - \hat{Z}_{med}}{MAD} = \dfrac{r_m}{MAD} \end{cases}$$

So far, we have $P_j = \{p_{j1}, \cdots, p_{jm}\}$ for $\underline{v}_j$

5. Repeat Step 4 for $j=1,\dots m$, then we have

$$\begin{cases} v_1 : p_{11}, p_{12}, \dots p_{1m} \\ v_2 : p_{21}, p_{22}, \dots p_{2m} \\ \vdots \\ v_n : p_{n1}, p_{n2}, \dots p_{nm} \end{cases}$$

$\{P_{i1}, P_{i2}, \dots, P_{im}\}$ is a standard projection for h along $\{\underline{v}_1, \underline{v}_2 \dots \underline{v}_m\}$

6. Calculate the projection statistics of ($h1$, $h2$, ... hm); obtain

$$
\begin{aligned}
PS_1 &= \max\{p_{11}, \cdots, p_{n1}\} \\
PS_2 &= \max\{p_{12}, \cdots, p_{n2}\} \\
&\vdots \\
PS_m &= \max\{p_{1m}, \cdots, p_{nm}\}
\end{aligned}
$$

By using the above algorithm, the bad leverage point (extreme event) is successfully identified in the disturbance data.

B.3.2 Bounded Influence GM Estimator

As we know, the M-estimator is given by

$$\underline{x}^{(k+1)} = \left(\underline{H}^T \underline{Q}^{(k)} \underline{R}^{-1} \underline{H}\right)^{-1} \underline{H}^T \underline{Q}^{(k)} \underline{R}^{-1} \underline{z} \qquad (1)$$

for the given linear regression model $\underline{z} = \underline{H}\ \underline{x} + \underline{e}$ by minimizing the objective function

$$J(\underline{x}) = \sum_{i=1}^{m} \rho\left(\frac{r_i}{\sigma_i}\right)$$

The above M-estimator is robust as long as there is no leverage point. Here we introduce

$$W_i = \min\left(1, \left(\frac{d}{PS_i}\right)^2\right)$$

to deal with the case with a leverage point in the sample. d is the threshold.

Then we have

$$q\left(\frac{r_i}{\sigma_i \omega_i}\right) = \frac{\psi\left(\frac{r_i}{\sigma_i \omega_i}\right)}{\frac{r_i}{\sigma_i \omega_i}}$$

and we still use equation (1), except the only difference is the Q function.

Now we minimize

$$J(\underline{x}) = \sum_{i=1}^{m} \omega_i^2 \rho\left(\frac{r_i}{\sigma_i \omega_i}\right)$$

For the leverage point, ω_i is small. If it is a good leverage point, r_i is small, and $\frac{r_i}{\sigma_i \omega_i}$ is also small, then

$$\omega_i^2 \left(\frac{r_i}{\sigma_i \omega_i}\right)^2 = \left(\frac{r_i^2}{\sigma_i^2}\right)$$

The relationship between ω_i and PS_i is shown in Figure B.1

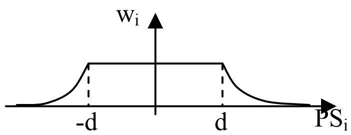


Figure B.1 ω_i versus PSi

B.4 Disturbance Data Analysis

In this section, a detailed analysis of power system disturbances is provided. The results here also help give some idea of how accurately the disturbance sizes follow the power law.

B.4.1 Scope and Sample Size of the Disturbance Data

The power system disturbance data come from the Disturbance Analysis Working Group (DAWG) Database [2]. The DAWG database summarizes disturbances that occur on the bulk electric systems of the electric utilities in North America. The Department of Energy (DOE) requires electric utilities to report system emergencies that include electric service interruptions, voltage reductions, acts of sabotage, and other unusual occurrences that can affect the reliability of the bulk electric systems. When a utility experiences an electric system emergency that it must report to DOE, the utility sends a copy of the report to its Regional Council, which then sends a copy to NERC. The disturbance data analysis here is based on major electric utility system disturbances gathered by NERC.

There are a total of 451 events from 1984 to 1999 in the database, which fall into the following four categories defined by NERC.

- Electric service interruptions
- Voltage reductions
- Unusual occurrences that can affect the reliability of the bulk electric systems
- Public appealing

Among the 451 events, there are 292 interruption events. The average loss of load of these interruption events is 713MW, and the median is 295MW. The maximum loss of load is 19,400 MW, which occurred on March 13, 1989 in the NPCC-HQ system.

Another severity index is the average number of customers disconnected. The average number of customers disconnected is 196,130, and the median is 41,848. The maximum number of customers disconnected is 7,500,000, which occurred on August 10, 1996 in the WSCC system.

B.4.2 Causes of Disturbance

The causes are very diverse, but severe weather, faults and equipment failure comprise the majority of the triggering events, accounting for 25%, 25% and 20%, respectively (Table B.1). The remaining 30% are due to accidents (e.g. fires, birds, etc.), human error, relay malfunction, sabotage, and unusual occurrences (earthquakes, solar magnetic disturbances).

Table B.1 Causes of Initial Fault

Causes	Severe Weather	Fault	Equipment Failure	Others
Percentage	25%	25%	20%	30%

B.4.3 Time Series of the Disturbances and Data Histogram

The time series of the power loss of all interruption events (1984 ~ 1999) is shown in Figure B.2. The time span is from January 3, 1984 to June 17, 1999, with corresponding time lag from 5645 to 1 in days shown on the x-axis. A similar time series of the number of customers disconnected is shown in Figure B.3.

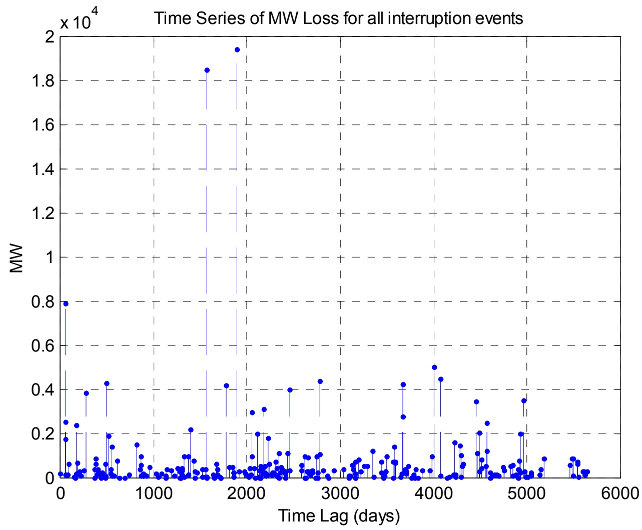


Figure B.2 Time Series of Disturbances (Loss of Power)

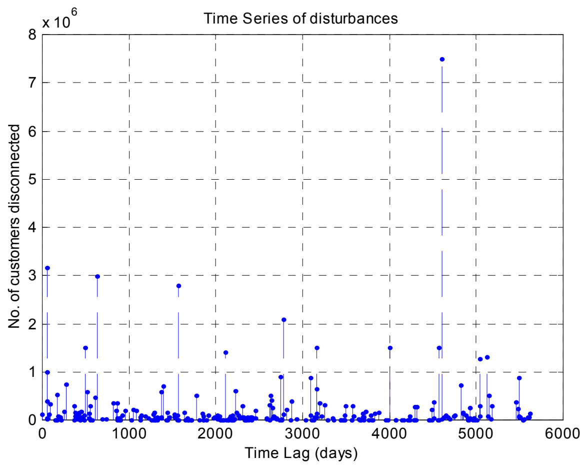


Figure B.3 Time Series of Disturbances (Customers Disconnected)

A histogram is a useful tool for exploring the shape of the distribution of the values of a variable. Histograms may be used for screening of outliers, checking normality, or suggesting another parametric shape for the distribution. The histograms of the frequency of events versus loss of load in MW and number of customers disconnected are shown in Figure B.4. It seems the distribution of the disturbance data has a "thick tail" different from the one observed in a Gaussian distribution. Hence, a Cauchy distribution is suggested to check against the disturbance data by using Q-Q plot.

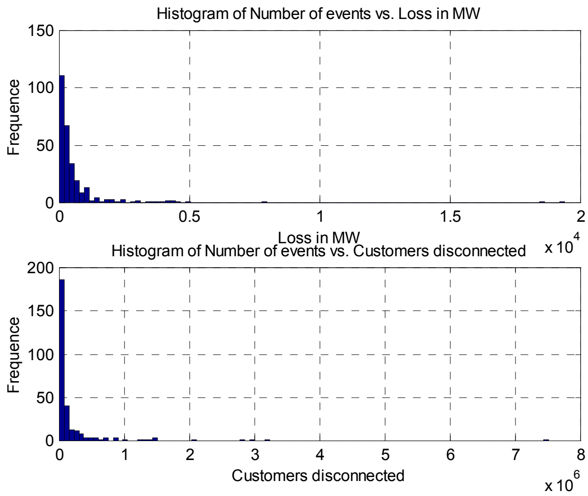


Figure B.4 Histogram of Disturbance Events

B.4.4 Mean Time to Failure

Among all of these disturbance events, the number of events with loss of power (LOP) of 100MW and above is 243, and the mean time to failure is once every 23 days; 97 events occurred with a LOP of 500MW and above, accounting for once every 58 days. There are 47 events with a LOP of 1,000MW and above, which is once every 122 days; Four events happened with the LOP exceeding 5,000 MW during the past 15 years, with a frequency of once every 3.86 years, and two catastrophic failures occurred approximately once every eight years with the LOP over 10,000 MW. Table B.2 shows the statistics of these events.

Table B.2 Statistics of Disturbance Events with Respect to Loss of Power

Scale (MW)	≥ 100	≥ 500	≥ 1,000	≥ 5,000	≥ 10,000	Total
No.	243	97	47	4	2	438
Percentage	55.5%	22.1%	10.7%	0.9%	0.5%	100%
MTTF	23 days	58 days	122 days	3.86 yrs	7.73 yrs	13 days

Similarly, the statistics with respect to the customer disconnected is given in Table B.3. As shown in the table, the average number of customers disconnected are about 1.5-3 times with respect to the thresholds of the scale, with the lower threshold having higher multiplier, for example, the average number of customers disconnected is about three times the thresholds for the scales of 50,000 and 100,000.

Table B.3 Statistics of Disturbances with Respect to Customer Disconnected

Scale ($x10^3$)	≥ 50	≥ 100	$\geq 1,000$	$\geq 5,000$	Total
Avg.($x10^3$)	149	300	2,250	7,500	
No.	156	103	17	1	441
Percentage	35.4%	23.4%	3.9%	0.2%	100%
MTF	23 days	54.8 days	332 days	15 yrs	13 days

Comparing Table B.3 with Table B.2, we find that the 50,000scale of the number of customers disconnected corresponds to the scale of LOP of 100 MW, and 100,000 corresponds to 500 MW. The total numbers of events in these two tables are slightly different due to some events with incomplete data (e.g. no LOP given), which thus are excluded from the statistics. The catastrophic failures consist of no more than 0.5% of all the events, with an occurrence of approximately once per ten years.

B.4.5 Power Law of Disturbances

Researchers at Caltech provide some interesting results on the correlations of a cumulative number of natural disasters with respect to the monetary loss per event, shown in Figure B.5.

It is interesting to ask the question: In an artificial system, is there a similar relationship between the frequencies and the scale of the disturbances? Do the power system disturbances also follow the power law?

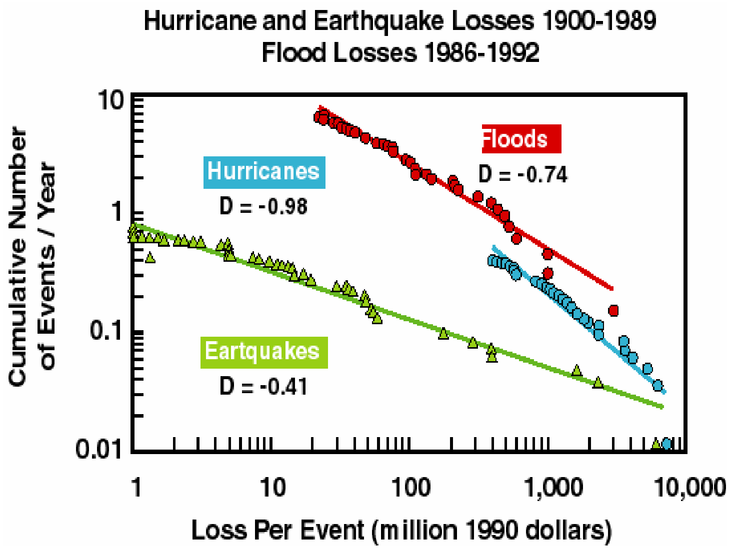


Figure B.5 Power Law of Natural Disasters

Figure B.6 shows the cumulative frequency magnitude relation of power system disturbances, i.e. the cumulative number of disturbances versus the LOP.

Over three orders of magnitude in LOP, the distribution follows a power law as required for SOC. The straight line shows the best fitted power law. By using the bounded influence GM estimator, the slope of the fitted line is about –0.7.

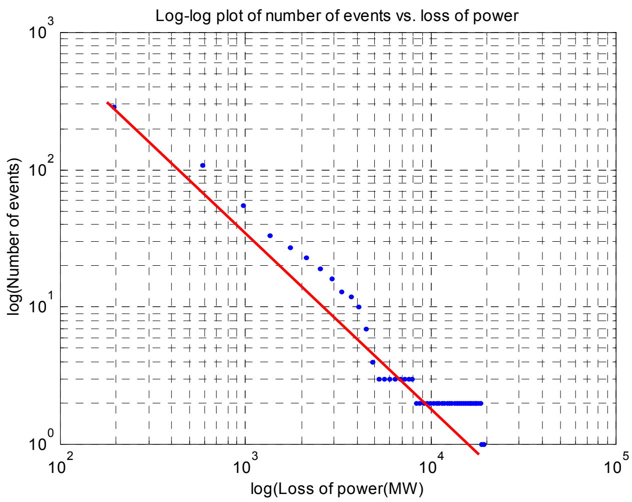


Figure B.6 Cumulative Number of Events Versus LOP

Figure B.7 shows a similar relationship between the number of disturbances and the scale of the disturbances (i.e. the number of customers disconnected). The slope of the fitted line is –1.365.

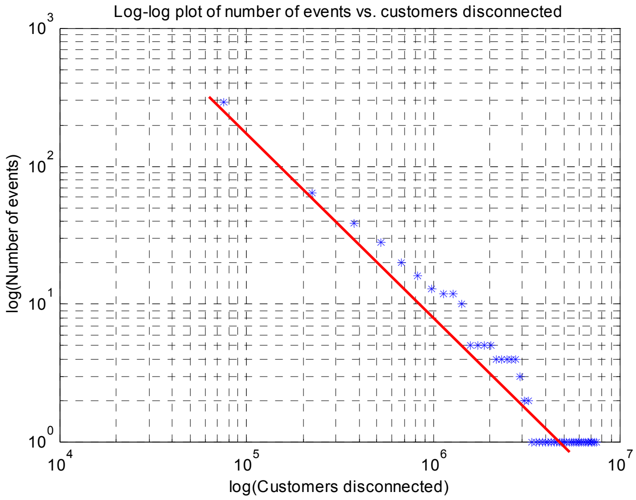


Figure B.7 Cumulative Number of Events versus Number of Customers Disconnected

B.4.6 Autocorrelation

Another question one may ask: Are there any correlations between these disturbances in the power system? Autocorrelation plots are a commonly-used tool for checking randomness in a data set. This randomness is ascertained by computing autocorrelations for data values at varying time lags. If random, such autocorrelations should be near zero for any and all time lag separations. If non-random, then one or more of the autocorrelations will be significantly non-zero.

In order to investigate the evidence of correlations of the power system disturbances over a long time scale, the autocorrelation function of the disturbance time series is plotted in Figure B.8. This autocorrelation function measures the strength of association between two disturbances that occurred at different times. The sample autocorrelation plot in Figure B.8 shows that the disturbance time series is not random, but rather has auto-correlation between observations. It seems to fall off exponentially with time lags.

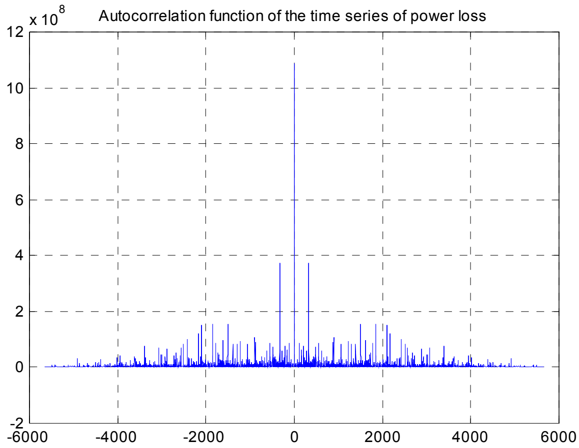


Figure B.8 Autocorrelation Function of LOP

Figure B.9 shows the log-log scatter-plot of the autocorrelation of the LOP time series. The events with zero LOP are differentiated from zero-padding samples by adding 1 MW.

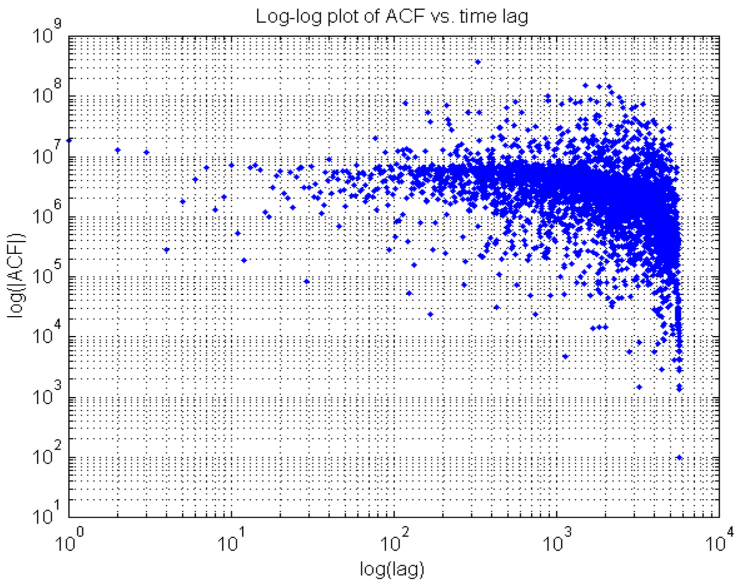


Figure B.9 Autocorrelation Function of LOP on Log-Log Scale w/ Zero Padding

For comparison, Figure B.10 shows the sample autocorrelation of LOP on a log-log scale without zero-padding.

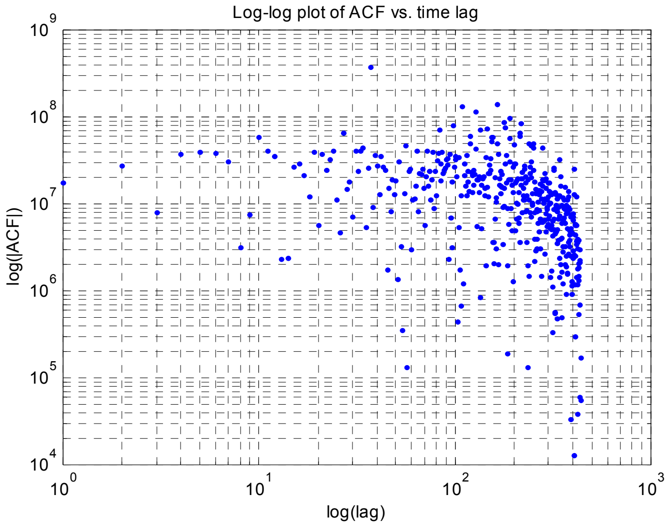


Figure B.10 Autocorrelation Function of LOP on Log-Log Scale w/o Zero Padding

B.4.7 Variance of Sample Mean on Log-Log Scale

Another useful plot to explore the correlations of a time series is the log-log plot of the variance of sample mean versus sample size. The steps to plot the log-log scatter-plot of variance of sample mean versus the sample size are summarized as follows:

1) Suppose the sample size is n, choose m<n (say m =10) to be the size of sub-sample (block), then for each m, there are n/m blocks with size of m for each block
2) Calculate the sample mean for the n/m blocks
3) Calculate the sample variance of these sample means
4) Repeat Steps 1-3 for m = 20, 30, ...
5) Plot the variance of sample mean versus the sample on a log-log scale.

Applying the above procedure to the disturbance data gives the log-log scatter-plot of variance of sample mean versus sample size shown in Figure B.11.

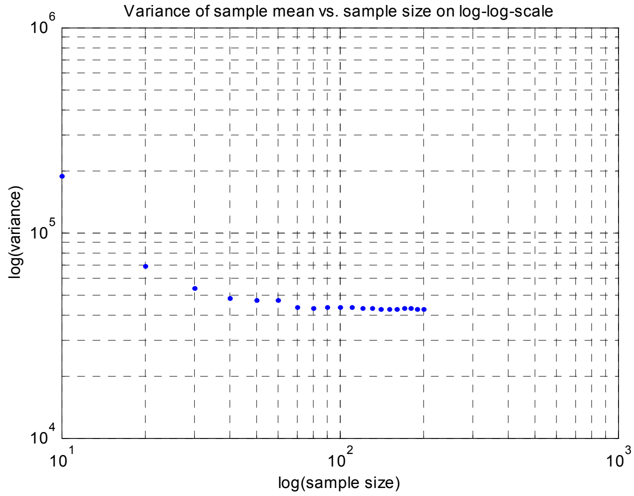


Figure B.11 Variance of Sample Mean vs. Sample Size on Log-Log Scale

By using the bounded influence GM estimator, the slope of the fitted line is –0.1143, which is displayed in Figure B.12.

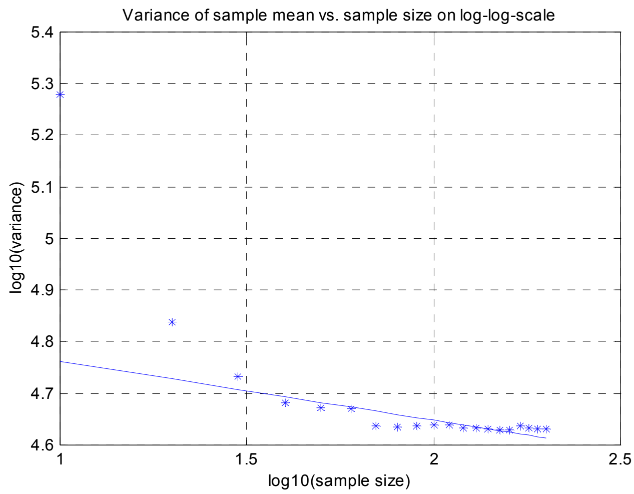


Figure B.12 Fitted Line Obtained by Bounded Influence GM Estimator

B.4.8 Q-Q Plot against Cauchy Distribution

The most useful tool for assessing whether a set of data follows some distribution is a quantile-quantile or QQ plot. This is a scatter plot with the quantiles of the scores (observations) on the horizontal axis and the expected scores on the vertical axis. A plot of these scores against the expected scores should reveal a straight line. The expected Cauchy scores are calculated by X = a * tan (pi*Y/2). Curvature of the points indicates departure from Cauchy distribution. This plot is also useful for detecting outliers, which appear as points that are far away from the overall pattern of points.

The steps in constructing the Q-Q plot are as follows:

1) Suppose $\{Z_1, Z_2, ..., Zn\}$ is the sample of system disturbances, sort the data from smallest to largest: $Z(1) < Z(2) < ... < Z(n)$
2) Let X be a conditional Cauchy random variable. X is the solution to X = a * tan(pi*Y/2), where Y takes values equal to {1/(n+1), 2/(n+1), ..., n/(n+1)} and a = median $(Z_1, Z_2, ..., Zn)$. The associated values of X are $X(1) < X(2) < ... < X(n)$
3) Do a scatter plot of Z versus X, where the points in the (X, Z) plane are {X(1), Z(1)}, {X(2), Z(2)}, ..., {X(n), Z(n)}, then join all of these points by a line.

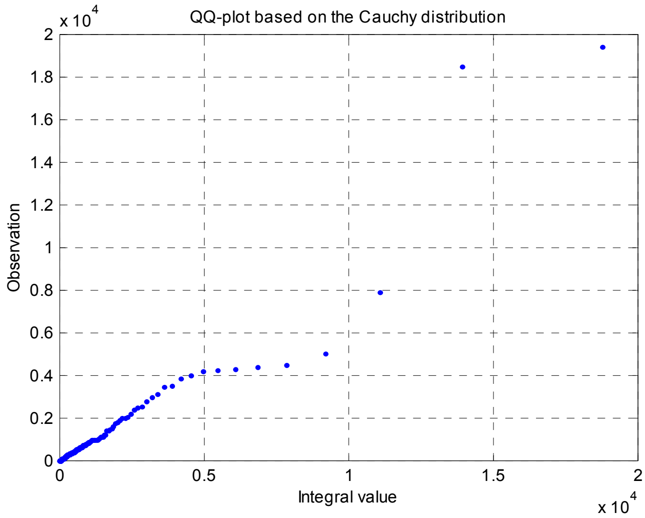


Figure B.13 Q-Q Plot of Disturbance Data (LOP)

Figure B.13 is the Q-Q plot of LOP based on Cauchy distribution. As shown in the figure, the LOPs of the disturbance data approximately follow the Cauchy distribution.

If we zoom in the first part of the plot (those majority samples with LOP less than 5,000 MW, displayed in Figure B.14; the correlation coefficient (r) of the fitted line for those scatter points indicates a value near 1, which slightly deviates from the perfect linearity (theoretical line).

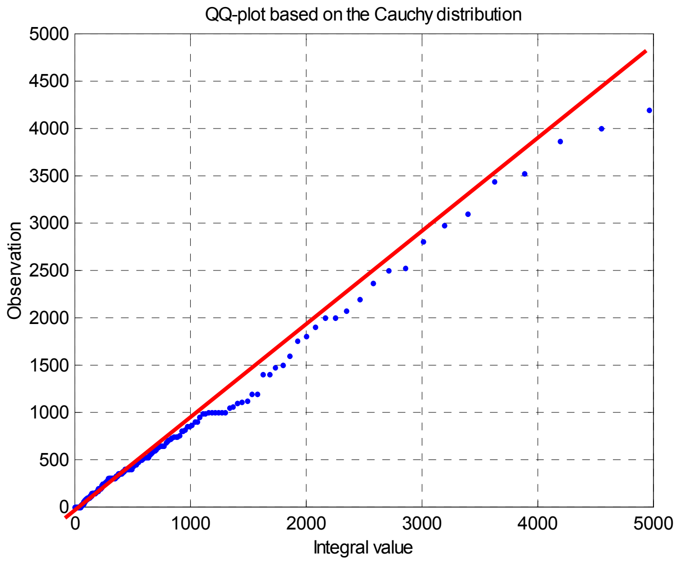


Figure B.14 Q-Q Plot of Samples with LOP less than 5,000 MW

B.5 Conclusion

The concept of SOC was introduced first by Bak et al.; it has been applied to phenomena in physics, biology, economics, and geosciences. A system exhibits SOC behavior if it tends to move into a critical state, where the distribution of event sizes (e. g., the LOP) is scale invariant, and where the temporal behavior is a 1/f (pink, flicker) noise.

SOC offers considerable insight into a wide range of phenomena, from forest fires, to earthquakes, to traffic jams. Despite the success of the SOC concept in some physical systems, it has not been established in applications of power systems (such as disturbance prediction) yet.

The alternative approach based on the analysis of the disturbance data globally studied here and in some recent work [113] proposes that power systems have intrinsically unstable dynamics, leading to deterministic fluctuations, such as catastrophic failure (blackout) in a limit cycle, or even deterministic "chaos."

As shown in the previous analysis, the frequency of disturbance occurrences as a function of their magnitude can be described by a power law. The power law distributions suggest that SOC may play an important part in the understanding and explanation of power system failures and in the prediction of catastrophic failures.

Once we can identify the intrinsic relationships and statistic characteristics of disturbances that occurr in a power system, we may confirm our approach and set up appropriate promising models to predict the probability of system failure as well as long-term risk assessment.

In order to investigate a phenomenon with respect to SOC, sample data over long periods with thousands of events should be collected. The most difficult part of this process is to gather enough disturbance data.

The statistical analysis initiated here may be extended to other sorts of applications in the power system such as long-term prediction of electricity prices and load forecasting.

As shown in the analysis, the LOP of the disturbance data approximately follows the Cauchy distribution; however, further analysis of the samples with the LOP between 5,000 and 10,000 MW reveals that these events occurred with a higher probability than that suggested by Cauchy distribution. These catastrophic failures (blackouts) happened more frequently than one would expect if we treat these events using traditional Gaussian distribution.

Appendix C Simulation Results Obtained on a 7-Bus System

A mechanism of cascading multiple failures in power systems has been unveiled through the analysis of the 1977 New York City Blackout in Chapter 3. For the sake of clarity, the mechanism of cascading failures represented by the event tree, along with the calculation of the associated failure probabilities, is illustrated in an example that makes use of short-circuit analysis and load flow calculations applied to a 7-bus system, whose one-line diagram is shown in Figure C.1.

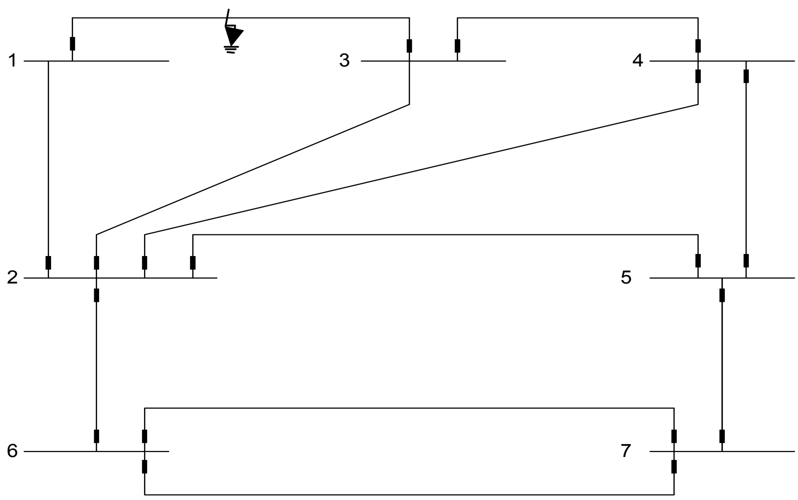


Figure C.1 One-line diagram for the 7-bus test system

Here, we assume that the network is protected only by zone 1, zone 2, and zone 3 distance relays. The proposed pickup settings are equal to 70% and 120% of the protected line for zone 1and zone 2 relays, respectively, and 100% of the protected line length plus 120% of the longest adjacent line for zone 3 relays. This example is also based on the following assumptions:

1) The triggering event is a permanent three-phase short-circuit on Line 1-3, which occurs with a probability P_f;
2) The faulty line is opened by its own circuit breakers, that is, there is no breaker stuck in the closing position;
3) All relays have the same hidden failure probability denoted by P_{HF};

4) The hidden failure of a relay is exposed whenever the associated line is overloaded; a system failure is supposed to occur whenever at least one bus is isolated from the rest of the network.

By using a short-circuit and a load flow program, we determine the list of cascading events on a power system following a legitimate tripping of a given line. The short-circuit program is run to identify all the exposed relay hidden failures and a load flow calculation is executed to identify the new set of relays whose hidden failures have been exposed due to overloaded lines.

The settings of the zone 3 relays are shown in Table C.1, where R_{ij} denotes the relay at the *i*-th end of Line *i-j*. Suppose that a three-phase fault is applied to the bus-3 end of Line 1-3. We calculate the short-circuit current at the fault point by assuming that all the pre-fault bus voltages are equal to one p.u. Then, we determine the voltage drops at all the buses. Using the principle of superposition, we obtain the fault-on voltages, which allow us to calculate the short-circuited current on every branch of the network. Finally, we determine the apparent impedance seen by each relay. Table C.2 displays the zone 3 relays with hidden failures exposed to fault. The flow chart of the general procedure to identify exposed relay is displayed in Figure C.2 . The apparent impedances seen by them are smaller than their settings. As a result, these relays may trip incorrectly. The voltages, short-circuited currents, and apparent impedances of the exposed relays are also listed in Table C.2. In the final step, a load flow program is executed to identify the overloaded lines following the tripping of those lines with exposed relay hidden failures and the probabilities of system failure are calculated.

The simulation results are displayed in Table C.3. Note that the lines exposed to hidden failures can trip individually or simultaneously as shown in the second column of Table C.3, which is entitled Step 2. Also, note that the steps of a sequence of trippings are numbered 1 through 6. For example, in the tripping sequence of case 1, Line 2-3 opens due to hidden failure in step 2, which in turn induces Line 3-4 to be overloaded and to disconnect in step 3. Finally, Line 2-5 trips for the same reason in step 4. Since no overloaded line is encountered after step 4, the line tripping sequence will stop. In some cases, there may be more than one line overloaded at the same time due to previous contingencies. For example, both Lines 3-4 and 2-5 are overloaded in step 3 of case 5; they will trip simultaneously at this step.

The system failure probabilities are given in the last column of Table C.3. Here, P_{ij} denotes the conditional probability that the overloaded Line *ij* is mis-tripped. We observe from Table C.3 that there are 14 sequences of line tripping that lead to a system failure.

Table C.1 Settings of Zone 3 Distance Relays

Relay	Setting (p.u.)	Relay	Setting (p.u.)
R_{12}	0.276	R_{21}	0.348
R_{13}	0.456	R_{31}	0.312
R_{34}	0.318	R_{43}	0.318
R_{45}	0.384	R_{54}	0.456
R_{57}	0.348	R_{75}	0.348
R_{23}	0.468	R_{32}	0.398
R_{24}	0.468	R_{42}	0.398
R_{25}	0.408	R_{52}	0.338
R_{26}	0.348	R_{62}	0.276
R_{67}	0.312	R_{76}	0.312

Table C.2 List of Exposed Zone 3 Relays

Exposed Relay	Setting (p.u.)	Apparent Impedance	Voltage (p.u.)	Current (p.u.)
R_{23}	0.468	0.18	0.5205	2.89
R_{24}	0.468	0.3025	0.52052	1.72
R_{43}	0.318	0.03	0.2108	1.4
R_{54}	0.456	0.3905	0.547	7.02

Table C.3 Probabilities of Cascading Failures for the 7-Bus System

Sequence	Step 2	Step 3	Step 4	Step 5	Step 6	
Case	Line Tripping(s) Due to HF	Line tripping(s) due to overload	Line tripping(s) due to overload	Line tripping(s) due to overload	Line tripping(s) due to overload	Probability of System Failure
1	2-3	3-4 (117%)	2-5 (102%)			$P_f P_{HF} P_{34} P_{25}$
2	2-4					$P_f P_{HF}$
3	3-4	2-3 (174%)	2-5 (102%)			$P_f P_{HF} P_{33} P_{25}$
4	5-4					$P_f P_{HF}$
5	2-3 & 2-4	3-4 (117%) 2-5 (140%)	2-6 (108%)	5-4 (120%)		$P_f P^2_{HF} P_{34} P_{25} P_{26} P_{54}$
6	2-3 & 4-3	2-5 (102%)				$P_f P^2_{HF} P_{25}$
7	2-3 & 5-4	3-4 (117%)	2-5 (113%)			$P_f P^2_{HF} P_{34} P_{25}$
8	2-4 & 3-4	2-3 (174%)	2-5 (132%)	2-6 (108%)	5-4 (120%)	$P_f P^2_{HF} P_{23} P_{25} P_{26} P_{54}$
9	2-4 & 5-4					$P_f P^2_{HF}$
10	3-4 & 5-4	2-3 (174%)	2-5 (113%)			$P_f P^2_{HF} P_{23} P_{25}$
11	2-3&2-4&3-4	2-5 (132%)	2-6 (108%)	5-4 (120%)		$P_f P^3_{HF} P_{25} P_{26} P_{24}$
12	2-3&2-4&5-4	2-5 (127%)	2-6 (108%)			$P_f P^3_{HF} P_{25} P_{26}$
13	2-3&3-4&5-4	2-3 (113%)				$P_f P^3_{HF} P_{23}$
14	2-4&3-4&5-4	2-3 (174%)	2-5 (127%)	2-6 (108%)		$P_f P^3_{HF} P_{23} P_{25} P_{26}$

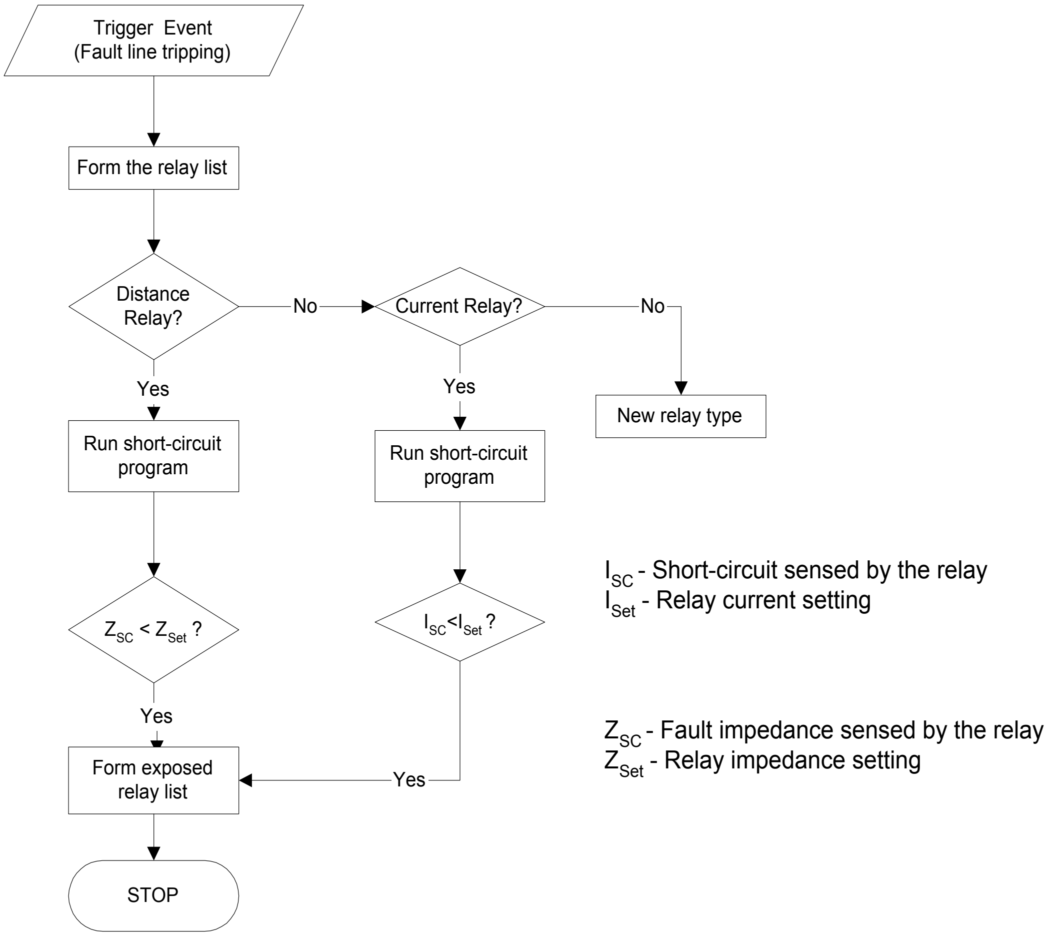


Figure C.2 Flowchart for the Determination of Exposed Relays

Appendix D Load Flow Data for the Reduced WSCC System

Table D.1 Load Data of the Reduced WSCC Sample System

(Sorted by voltage level)

No.	NAME	Voltage	P(MW)	Q(MW)	Voltage	Angle	Shunt
47	OWENS G	11.5	100.0	0	1.020	-47.3	
70	DALLES21	13.8	100.0	0	1.055	-7.9	
77	JOHN DAY	13.8	100.0	0	1.000	0.0	
40	CASTAI4G	18.0	100.0	0	1.020	-46.0	
43	HAYNES3G	18.0	100.0	0	1.000	-47.3	
4	CORONADO	20.0	100.0	0	1.040	-19.7	
11	HAYDEN	20.0	100.0	0	1.000	33.7	
30	CANAD G1	20.0	100.0	0	1.000	24.7	
35	CMAIN GM	20.0	100.0	0	1.020	67.8	
65	MONTA G1	20.0	100.0	0	1.000	56.6	
79	NORTH G3	20.0	100.0	0	1.000	26.6	
112	ROUND MT	20.0	100.0	0	1.020	-15.1	
116	TEVATR	20.0	100.0	0	1.050	-35.7	
118	TEVATR2	20.0	100.0	0	1.000	-30.8	
138	ELDORADO	20.0	100.0	0	1.020	-26.0	
140	LITEHIPE	20.0	100.0	0	1.020	-49.6	
144	MIRALOMA	20.0	100.0	0	1.050	-45.4	
149	PARDEE	20.0	100.0	0	1.010	-39.6	
159	EMERY	20.0	100.0	0	1.050	9.6	
162	NAUGHT	20.0	100.0	0	1.000	3.4	
6	CRAIG	22.0	100.0	0	0.950	23.6	
9	FCNGN4CC	22.0	100.0	0	1.000	2.2	
18	SJUAN G4	22.0	100.0	0	1.000	-0.9	
36	BRIDGER2	22.0	100.0	0	1.009	2.5	
148	MOHAV1CC	22.0	100.0	0	1.050	-21.0	
15	PALOVRD2	24.0	100.0	0	0.960	-21.7	
103	DIABLO1	25.0	100.0	0	0.980	-42.3	
13	NAVAJO 2	26.0	100.0	0	1.000	-17.8	
45	INTERM1G	26.0	100.0	0	1.050	0.3	
67	BIG EDDY	115.0	160.0	31.3	1.069	-16.9	0.00
51	STA B	138.0	237.2	-63.2	1.033	-51.9	0.00
100	CORTINA	200.0	-43.3	20.0	1.131	-35.0	0.00
101	COTWDPGE	200.0	210.4	-77.0	1.136	-30.5	0.00
105	GLENN	200.0	27.5	-0.1	1.141	-34.2	0.00
106	LOGAN CR	200.0	8.0	0.0	1.140	-34.6	0.00
109	MIDWAY	200.0	777.6	32.6	1.167	-51.4	-1.30
113	ROUND MT	200.0	148.0	0.0	1.124	-25.1	-1.28

No.	NAME	Voltage	P(MW)	Q(MW)	Voltage	Angle	Shunt
117	TEVATR	200.0	884.0	54.8	1.128	-39.6	-0.32
10	BENLOMND	230.0	139.7	23.8	1.007	-5.2	0.00
33	BIG EDDY	230.0	0.0	0.0	0.979	53.8	0.00
34	CA230	230.0	3600.0	700.0	1.001	62.9	0.00
39	CA230TO	230.0	0.0	0.0	1.032	-47.3	0.00
41	CASTAIC	230.0	135.0	27.0	1.023	-50.9	0.00
42	CELILO	230.0	0.0	0.0	1.031	-50.6	0.00
46	EAGLROCK	230.0	-72.8	-17.0	1.035	-47.6	0.00
48	FOURCORN	230.0	121.0	25.0	1.034	-47.8	0.00
50	GLENDAL	230.0	320.0	65.0	1.024	-51.8	0.00
54	HAYNES	230.0	138.0	28.0	1.027	-52.1	0.00
55	LITEHIPE	230.0	807.8	132.1	1.025	-50.1	0.00
57	MESA CAL	230.0	117.0	24.0	1.025	-51.9	0.00
58	MIRALOMA	230.0	121.0	25.0	1.024	-51.2	0.00
59	NAUGHTON	230.0	887.7	-6.2	1.031	-48.9	0.00
60	OLIVE	230.0	-2771.0	1654.0	1.038	-47.1	21.46
61	PARDEE	230.0	401.0	80.6	1.021	-48.2	0.00
62	RINALDI	230.0	205.2	17.6	1.029	-49.0	0.00
68	RIVER	230.0	-67.5	160.0	1.066	-14.6	5.77
71	STA BLD	230.0	3137.0	1681.0	1.062	-15.1	7.92
137	STA E	230.0	175.0	18.0	1.010	-52.8	0.00
141	STA F	230.0	3191.0	630.0	1.012	-55.8	0.00
143	STA G	230.0	377.4	64.5	1.007	-55.1	0.00
146	STA J	230.0	0.0	0.0	1.038	-50.1	0.00
150	SYLMAR S	230.0	3118.0	78.0	1.006	-51.7	0.00
154	SYLMARLA	230.0	1066.0	-10.8	0.995	-51.6	-1.90
157	VALLEY	230.0	148.0	-7.9	1.046	-4.0	0.00
161	VINCENT	230.0	255.0	100.0	1.045	0.6	0.00
52	STA B1	287.0	0.0	0.0	1.037	-50.7	0.00
63	VICTORVL	287.0	-129.0	32.2	1.052	-44.5	-1.08
3	BENLOMND	345.0	0.0	0.0	0.977	-17.0	0.00
5	CAMP WIL	345.0	2350.0	-127.0	0.975	16.3	0.00
8	CHOLLA	345.0	239.0	-56.0	1.009	-4.7	-1.55
17	CRAIG	345.0	840.0	5.0	1.036	-3.9	3.90
44	EMERY	345.0	2053.0	907.1	1.053	-4.4	4.30
85	FOURCORN	345.0	610.0	-414.0	0.999	-1.6	-8.70
155	INTERMT	345.0	457.7	81.7	1.043	-2.4	-0.60
156	MIDPOINT	345.0	33.9	11.9	1.045	-3.4	0.00
158	MONA	345.0	116.1	38.4	1.037	4.9	-2.20
160	PINTO	345.0	-62.0	12.8	1.056	-2.0	0.00
163	PINTO PS	345.0	0.0	0.0	1.037	-2.4	0.00
164	SAN JUAN	345.0	31.6	11.5	1.040	-1.4	-0.18
165	SIGURD	345.0	141.2	71.4	1.035	-1.1	0.00

No.	NAME	Voltage	P(MW)	Q(MW)	Voltage	Angle	Shunt
166	SPAN FRK	345.0	379.0	-43.0	1.052	-0.5	-0.50
167	TERMINAL	345.0	185.0	78.5	1.039	-3.4	0.00
2	ADELAN&1	500.0	1750.0	-56.0	0.980	-26.2	0.00
7	ADELANTO	500.0	0.0	0.0	1.068	-7.9	-1.13
12	BIG EDDY	500.0	90.0	70.0	1.072	-23.9	-1.90
14	BURNS	500.0	0.0	0.0	1.067	-24.8	-3.91
16	BURNS1	500.0	793.4	207.0	1.049	-29.6	-1.46
19	BURNS2	500.0	617.0	-69.0	1.056	-29.6	-4.27
20	CANADA	500.0	0.0	0.0	1.070	-22.8	0.00
21	CANALB	500.0	0.0	0.0	1.061	-25.9	0.00
22	CELILOCA	500.0	0.0	0.0	1.047	-22.1	0.00
23	COLSTRP	500.0	0.0	0.0	1.026	-31.4	0.00
24	CORONADO	500.0	0.0	0.0	1.056	-23.4	0.00
25	COULEE	500.0	0.0	0.0	1.041	-31.1	0.00
26	DEVERS	500.0	0.0	0.0	1.051	-15.5	0.00
27	DIABLO	500.0	0.0	0.0	1.047	-42.4	0.00
28	ELDORADO	500.0	0.0	0.0	1.066	-5.8	0.00
29	FOURCOR1	500.0	0.0	0.0	1.069	-28.0	0.00
31	FOURCOR2	500.0	4400.0	1000.0	1.036	20.9	0.00
32	FOURCORN	500.0	0.0	0.0	1.079	49.2	0.00
37	GARRISON	500.0	-1862.0	971.0	1.060	-42.1	9.12
38	GATES	500.0	0.0	0.0	1.081	-46.2	0.00
49	GATES1	500.0	0.0	0.0	1.072	-45.5	-0.80
56	GRIZZLY	500.0	0.0	0.0	1.043	-47.7	0.00
64	GRIZZLY1	500.0	0.0	0.0	1.059	-42.5	0.00
66	GRIZZLY2	500.0	1700.0	300.0	1.049	48.2	0.00
69	GRIZZLY3	500.0	-44.2	22.0	1.089	-13.3	0.00
72	GRIZZLY4	500.0	0.0	0.0	1.090	-13.4	4.62
73	GRIZZLY5	500.0	-1525.0	-50.0	1.079	-1.4	0.00
74	GRIZZLY6	500.0	0.0	0.0	1.070	0.2	0.00
75	GRIZZLY7	500.0	2584.0	394.0	1.037	-12.2	0.00
76	GRIZZLY8	500.0	3200.0	1100.0	1.083	-11.1	10.19
78	GRIZZLY9	500.0	3500.0	500.0	1.050	0.2	5.50
80	GRIZZLYA	500.0	5000.0	400.0	1.050	12.1	12.00
81	HANFORD	500.0	0.0	0.0	1.053	-19.6	-2.20
82	JOHN DAY	500.0	-66.6	-97.0	1.068	-17.2	-6.74
83	LOSBANOS	500.0	-339.0	-119.0	1.054	-23.3	-1.10
84	LUGO	500.0	0.0	0.0	1.062	-5.2	-2.20
86	MALIN	500.0	0.0	0.0	1.058	-18.2	0.00
95	MIDPOINT	500.0	0.0	0.0	1.079	-22.1	0.00
96	MIDWAY	500.0	0.0	0.0	1.069	-17.2	0.00
102	MIDWAY4	500.0	50.0	25.0	1.053	-46.1	0.00
104	MIDWAY5	500.0	305.0	-7.6	1.047	-47.7	-0.91

No.	NAME	Voltage	P(MW)	Q(MW)	Voltage	Angle	Shunt
107	MIDWAY6	500.0	265.0	14.0	1.049	-49.5	0.00
108	MIRALOMA	500.0	55.6	-329.0	1.059	-48.6	-3.27
110	MOENKOP1	500.0	40.0	21.5	1.046	-49.8	0.00
111	MOENKOP2	500.0	-189.0	61.5	1.037	-31.1	0.00
115	MOENKOP4	500.0	-0.7	118.5	1.014	-32.1	-0.91
119	MOENKOPI	500.0	5661.0	3491.0	0.998	-39.0	15.00
120	MOHAVE	500.0	0.0	0.0	1.050	-24.1	0.00
121	MONTANA	500.0	0.0	0.0	1.012	-38.0	0.00
122	MOSSLAND	500.0	0.0	0.0	1.028	-30.8	0.00
123	NAVAJO	500.0	0.0	0.0	0.981	-46.6	0.00
128	NORTH	500.0	0.0	0.0	1.013	-25.8	0.00
129	OLINDA	500.0	0.0	0.0	0.999	-45.3	0.00
134	PALOVRDE	500.0	0.0	0.0	0.972	-35.1	0.00
135	RINALDI	500.0	0.0	0.0	1.068	-50.0	0.00
136	ROUND MT	500.0	856.0	19.6	1.036	-43.5	0.00
139	ROUND1	500.0	902.3	-11.4	1.051	-33.1	-3.19
142	ROUND2	500.0	204.2	-28.2	1.055	-46.1	0.00
145	ROUND3	500.0	3098.0	1189.0	1.041	-49.7	4.00
151	SERRANO	500.0	1230.0	72.8	1.041	-50.1	0.00
152	STA E	500.0	406.0	41.0	1.037	-47.8	0.00
153	SUMMER L	500.0	0.0	0.0	1.061	-48.9	0.00
168	TABLE MT	500.0	0.0	0.0	1.061	-19.8	0.00
173	TEVATR	500.0	0.0	0.0	1.032	-37.1	0.00
177	VALLEY	500.0	0.0	0.0	1.055	-49.3	0.00
178	VICTORVL	500.0	0.0	0.0	1.046	-48.2	0.00
179	VINCENT	500.0	0.0	0.0	1.057	-49.3	0.00
180	WESTWING	500.0	0.0	0.0	0.984	-6.7	-2.20
	Total		57885	15351			

Table D.2 Generator Data of the Reduced WSCC Sample System

No.	NAME	Voltage	P(MW)	Q(MVar)	Q_{max}	Q_{min}	Voltage	Angle
36	BRIDGER2	22.0	1640.0	285.5	600	-525	1.009	2.5
30	CANAD G1	20.0	4450.0	1010.9	4000	-4000	1.000	24.7
40	CASTAI4G	18.0	200.0	-52.2	268	-134	1.020	-46.0
35	CMAIN GM	20.0	4480.0	1150.1	5320	-3500	1.020	67.8
4	CORONADO	20.0	800.0	123.0	300	-300	1.040	-19.7
6	CRAIG	22.0	1048.0	-132.9	400	-400	0.950	23.6
70	DALLES21	13.8	1301.0	430.7	692	-711	1.055	-7.9
103	DIABLO1	25.0	765.0	-206.4	330	-310	0.980	-42.3
138	ELDORADO	20.0	982.7	-128.8	300	-300	1.020	-26.0
159	EMERY	20.0	1665.0	-31.4	9999	-9999	1.050	9.6
9	FCNGN4CC	22.0	2160.0	-30.5	700	-500	1.000	2.2
11	HAYDEN	20.0	2050.0	464.8	900	-900	1.000	33.7
43	HAYNES3G	18.0	325.0	68.3	300	-220	1.000	-47.3
45	INTERM1G	26.0	1780.0	534.6	850	-440	1.050	0.3
77	JOHN DAY	13.8	5173.6	853.5	2649	-1850	1.000	0.0
140	LITEHIPE	20.0	3195.0	1032.7	2000	-900	1.020	-49.6
144	MIRALOMA	20.0	1690.0	593.5	900	-400	1.050	-45.4
148	MOHAV1CC	22.0	1680.0	446.6	700	-300	1.050	-21.0
65	MONTA G1	20.0	2910.0	952.7	1500	-1000	1.000	56.6
162	NAUGHT	20.0	445.0	91.7	9999	-9999	1.000	3.4
13	NAVAJO 2	26.0	1690.0	195.3	700	-280	1.000	-17.8
79	NORTH G3	20.0	9950.0	1852.5	5780	-2000	1.000	26.6
47	OWENS G	11.5	110.0	29.1	100	-100	1.020	-47.3
15	PALOVRD2	24.0	2640.0	378.8	1300	-900	0.960	-21.7
149	PARDEE	20.0	2200.0	393.7	600	-600	1.010	-39.6
112	ROUND MT	20.0	1057.0	25.5	400	-400	1.020	-15.1
18	SJUAN G4	22.0	962.0	148.8	300	-300	1.000	-0.9
116	TEVATR	20.0	594.0	192.1	300	-300	1.050	-35.7
118	TEVATR2	20.0	3467.0	1653.5	2500	-1000	1.000	-30.8
Total			61410	12325				

Table D.3 Transmission Lines of the WSCC Sample System

Bus i	Voltage	Bus j	Voltage	Cir#	R (p.u.)	X (p.u.)	C (p.u.)
CRAIG	345.0	MONA	345.0	1	0.00811	0.13690	1.21740
CHOLLA	345.0	FOURCORN	345.0	1	0.00179	0.01988	1.28800
FOURCORN	345.0	SAN JUAN	345.0	1	0.00050	0.00530	0.04410
SAN JUAN	345.0	CRAIG	345.0	1	0.00977	0.11000	1.00000
BENLOMND	345.0	TERMINAL	345.0	1	0.00160	0.02260	0.19050
CAMP WIL	345.0	TERMINAL	345.0	1	0.00080	0.01060	0.10195
BENLOMND	345.0	CAMP WIL	345.0	1	0.00240	0.03320	0.29245
CAMP WIL	345.0	MONA	345.0	1	0.00170	0.02250	0.19960
CAMP WIL	345.0	MONA	345.0	2	0.00210	0.02380	0.19225
EMERY	345.0	PINTO	345.0	1	0.00960	0.08780	0.71325
CAMP WIL	345.0	EMERY	345.0	1	0.00520	0.06020	0.50500
CAMP WIL	345.0	EMERY	345.0	2	0.00490	0.05370	0.44215
CAMP WIL	345.0	SPAN FRK	345.0	1	0.00120	0.01720	0.14935
EMERY	345.0	SIGURD	345.0	1	0.00340	0.03740	0.31040
EMERY	345.0	SIGURD	345.0	2	0.00340	0.03720	0.30910
MONA	345.0	SIGURD	345.0	1	0.00380	0.03400	0.29120
MONA	345.0	SIGURD	345.0	2	0.00320	0.03490	0.28610
BENLOMND	345.0	MIDPOINT	345.0	1	0.00620	0.06730	0.55780
INTERMT	345.0	MONA	345.0	1	0.00180	0.02450	0.21960
INTERMT	345.0	MONA	345.0	2	0.00180	0.02450	0.21960
PINTO PS	345.0	FOURCORN	345.0	1	0.00480	0.04360	0.35390
EMERY	345.0	SPAN FRK	345.0	1	0.00340	0.03920	0.32620
CANADA	500.0	CANALB	500.0	1	0.00350	0.07000	2.30300
CANADA	500.0	NORTH	500.0	1	0.00083	0.02390	1.65000
NORTH	500.0	HANFORD	500.0	1	0.00020	0.00820	0.65000
NORTH	500.0	HANFORD	500.0	2	0.00020	0.00820	0.65000
HANFORD	500.0	COULEE	500.0	1	0.00113	0.02069	0.92763
HANFORD	500.0	MONTANA	500.0	1	0.00070	0.07400	2.43500
GARRISON	500.0	HANFORD	500.0	1	0.00142	0.02258	0.94000
HANFORD	500.0	JOHN DAY	500.0	1	0.00120	0.02316	0.85760
HANFORD	500.0	JOHN DAY	500.0	2	0.00030	0.02000	1.80000
GARRISON	500.0	JOHN DAY	500.0	1	0.00196	0.03304	0.94000
GARRISON	500.0	COLSTRP	500.0	1	0.00179	0.01405	1.84000
BIG EDDY	500.0	CELILOCA	500.0	1	0.00001	0.00030	0.00717
BIG EDDY	500.0	CELILOCA	500.0	2	0.00001	0.00030	0.00922
BIG EDDY	500.0	JOHN DAY	500.0	1	0.00023	0.00451	0.16660
BIG EDDY	500.0	JOHN DAY	500.0	2	0.00020	0.00446	0.15250
GRIZZLY	500.0	JOHN DAY	500.0	1	0.00063	0.01412	0.54878
GRIZZLY	500.0	JOHN DAY	500.0	2	0.00109	0.02408	0.77771
GRIZZLY	500.0	JOHN DAY	500.0	3	0.00108	0.02409	0.77674
GRIZZLY	500.0	SUMMER L	500.0	1	0.00101	0.00513	0.87075
GRIZZLY	500.0	MALIN	500.0	1	0.00218	0.01676	1.59003
GRIZZLY	500.0	MALIN	500.0	2	0.00214	0.01587	1.55415
MALIN	500.0	ROUND MT	500.0	1	0.00103	0.00898	0.79020
MALIN	500.0	ROUND MT	500.0	2	0.00107	0.00890	0.76350
MALIN	500.0	SUMMER L	500.0	1	0.00084	0.00760	0.74749

Bus i	Voltage	Bus j	Voltage	Cir#	R (p.u.)	X (p.u.)	C (p.u.)
MALIN	500.0	OLINDA	500.0	1	0.00103	0.01230	1.39800
BURNS	500.0	MIDPOINT	500.0	1	0.00264	0.02686	2.64530
BURNS	500.0	SUMMER L	500.0	1	0.00122	-0.00300	1.10350
ROUND MT	500.0	TABLE MT	500.0	1	0.00143	0.00668	0.73750
ROUND MT	500.0	TABLE MT	500.0	2	0.00143	0.00668	0.73750
TABLE MT	500.0	TEVATR	500.0	1	0.00156	0.01169	1.15570
TABLE MT	500.0	TEVATR	500.0	2	0.00097	0.01022	0.71260
OLINDA	500.0	TEVATR	500.0	1	0.00158	0.01071	1.90435
TEVATR	500.0	MIDWAY	500.0	1	0.00168	0.03629	1.23870
TEVATR	500.0	GATES	500.0	1	0.00094	0.02544	0.69475
GATES	500.0	MIDWAY	500.0	1	0.00074	0.00600	0.54395
GATES	500.0	DIABLO	500.0	1	0.00079	0.01937	0.66425
LOSBANOS	500.0	GATES	500.0	1	0.00083	0.01985	0.00000
LOSBANOS	500.0	MIDWAY	500.0	1	0.00153	0.01470	0.00000
MOSSLAND	500.0	LOSBANOS	500.0	1	0.00053	0.01297	0.00000
DIABLO	500.0	MIDWAY	500.0	1	0.00087	0.02087	0.72855
DIABLO	500.0	MIDWAY	500.0	2	0.00087	0.02087	0.72855
MIDWAY	500.0	VINCENT	500.0	1	0.00123	0.00789	0.99350
MIDWAY	500.0	VINCENT	500.0	2	0.00123	0.00792	0.99440
MIDWAY	500.0	VINCENT	500.0	3	0.00112	0.00747	0.91793
LUGO	500.0	VICTORVL	500.0	1	0.00020	0.00410	0.14810
LUGO	500.0	MIRALOMA	500.0	1	0.00028	0.00753	0.25868
LUGO	500.0	MIRALOMA	500.0	2	0.00035	0.00750	0.27680
LUGO	500.0	VINCENT	500.0	1	0.00044	0.01125	0.41460
LUGO	500.0	VINCENT	500.0	2	0.00044	0.01125	0.41460
LUGO	500.0	MOHAVE	500.0	1	0.00190	0.03100	2.07010
ELDORADO	500.0	LUGO	500.0	1	0.00193	0.02779	2.33560
ELDORADO	500.0	VICTORVL	500.0	1	0.00179	0.02524	0.26773
ELDORADO	500.0	VICTORVL	500.0	2	0.00179	0.02524	0.26773
LUGO	500.0	SERRANO	500.0	1	0.00060	0.01280	0.47310
MIRALOMA	500.0	SERRANO	500.0	1	0.00021	0.00457	0.16168
SERRANO	500.0	VALLEY	500.0	1	0.00040	0.00930	0.34280
VICTORVL	500.0	RINALDI	500.0	1	0.00083	0.01884	0.83334
ADELANTO	500.0	ADELAN&1	500.0	1	0.00074	0.01861	0.70132
ADELANTO	500.0	STA E	500.0	1	0.00082	0.01668	0.59401
ADELANTO	500.0	VICTORVL	500.0	1	0.00000	0.00159	0.06001
ADELANTO	500.0	VICTORVL	500.0	2	0.00000	0.00159	0.06001
MOHAVE	500.0	ELDORADO	500.0	1	0.00056	0.01415	0.52145
DEVERS	500.0	VALLEY	500.0	1	0.00042	0.00905	0.33397
PALOVRDE	500.0	DEVERS	500.0	1	0.00259	0.02967	1.07650
PALOVRDE	500.0	DEVERS	500.0	2	0.00259	0.02967	1.07650
NAVAJO	500.0	ELDORADO	500.0	1	0.00280	0.02110	0.50970
NAVAJO	500.0	MOENKOPI	500.0	1	0.00077	0.00544	0.69921
NAVAJO	500.0	WESTWING	500.0	1	0.00241	0.03485	2.43280
MOENKOPI	500.0	WESTWING	500.0	1	0.00179	0.02584	1.69610
MOENKOPI	500.0	ELDORADO	500.0	1	0.00207	0.01359	1.97580
PALOVRDE	500.0	WESTWING	500.0	1	0.00040	0.00960	0.45190
PALOVRDE	500.0	WESTWING	500.0	2	0.00040	0.00960	0.45190
FOURCORN	500.0	MOENKOPI	500.0	1	0.00177	0.02149	1.67230

Bus i	Voltage	Bus j	Voltage	Cir#	R (p.u.)	X (p.u.)	C (p.u.)
CA230TO	230.0	CA230	230.0	1	0.00200	0.02000	0.40000
BIG EDDY	230.0	CELILO	230.0	1	0.00006	0.00131	0.00189
BIG EDDY	230.0	CELILO	230.0	2	0.00006	0.00116	0.00166
COTWDPGE	200.0	ROUND MT	200.0	1	0.01113	0.06678	0.03643
COTWDPGE	200.0	ROUND MT	200.0	2	0.01050	0.06540	0.03430
COTWDPGE	200.0	ROUND MT	200.0	3	0.01105	0.06642	0.03580
COTWDPGE	200.0	TEVATR	200.0	1	0.03903	0.27403	0.15536
COTWDPGE	200.0	CORTINA	200.0	1	0.02482	0.16938	0.10116
CORTINA	200.0	TEVATR	200.0	1	0.01480	0.10101	0.06033
COTWDPGE	200.0	GLENN	200.0	1	0.01382	0.09268	0.05530
GLENN	200.0	TEVATR	200.0	1	0.03058	0.20460	0.12236
COTWDPGE	200.0	LOGAN CR	200.0	1	0.01668	0.11381	0.06804
LOGAN CR	200.0	TEVATR	200.0	1	0.02235	0.16106	0.09171
STA B1	287.0	VICTORVL	287.0	1	0.01070	0.07905	0.18335
STA B2	287.0	VICTORVL	287.0	1	0.01070	0.07905	0.18335
STA E	230.0	GLENDAL	230.0	1	0.00047	0.00723	0.00812
STA E	230.0	STA G	230.0	1	0.00119	0.01244	0.01399
STA E	230.0	STA G	230.0	2	0.00119	0.01244	0.01399
STA F	230.0	HAYNES	230.0	1	0.00201	0.03074	0.03443
STA F	230.0	STA BLD	230.0	1	0.00073	0.01025	0.01279
STA F	230.0	STA BLD	230.0	2	0.00073	0.01025	0.01279
STA F	230.0	STA G	230.0	1	0.00110	0.01189	0.01257
VALLEY	230.0	STA E	230.0	1	0.00128	0.00979	0.01060
GLENDAL	230.0	STA G	230.0	1	0.00035	0.00536	0.00602
HAYNES	230.0	STA G	230.0	1	0.00281	0.04296	0.04824
RINALDI	230.0	VALLEY	230.0	1	0.00138	0.01116	0.01235
RINALDI	230.0	VALLEY	230.0	2	0.00138	0.01116	0.01235
RIVER	230.0	HAYNES	230.0	1	0.00220	0.03422	0.03858
RIVER	230.0	HAYNES	230.0	2	0.00238	0.03669	0.04142
RIVER	230.0	STA F	230.0	1	0.00037	0.00366	0.00415
RIVER	230.0	STA G	230.0	1	0.00055	0.00586	0.00623
RINALDI	230.0	STA E	230.0	1	0.00229	0.01583	0.01530
RINALDI	230.0	STA E	230.0	2	0.00229	0.01583	0.01530
CASTAIC	230.0	OLIVE	230.0	1	0.00221	0.03346	0.03669
CASTAIC	230.0	RINALDI	230.0	1	0.00290	0.03800	0.04120
CASTAIC	230.0	STA J	230.0	1	0.00309	0.04677	0.05040
CASTAIC	230.0	SYLMARLA	230.0	1	0.00226	0.03422	0.03753
RINALDI	230.0	OLIVE	230.0	1	0.00029	0.00434	0.00475
RINALDI	230.0	STA J	230.0	2	0.00071	0.00484	0.01940
RINALDI	230.0	STA J	230.0	4	0.00081	0.00486	0.01928
RINALDI	230.0	STA J	230.0	3	0.00161	0.00971	0.00964
RINALDI	230.0	SYLMARLA	230.0	1	0.00027	0.00393	0.00459
RINALDI	230.0	SYLMARLA	230.0	2	0.00027	0.00393	0.00459
RINALDI	230.0	SYLMARLA	230.0	3	0.00027	0.00393	0.00459
PARDEE	230.0	VINCENT	230.0	1	0.00285	0.03649	0.06328
PARDEE	230.0	VINCENT	230.0	2	0.00138	0.03399	0.05626
EAGLROCK	230.0	MESA CAL	230.0	1	0.00190	0.02580	0.04920
EAGLROCK	230.0	PARDEE	230.0	1	0.00845	0.07034	0.07977
LITEHIPE	230.0	MESA CAL	230.0	1	0.00110	0.01270	0.02400

Bus i	Voltage	Bus j	Voltage	Cir#	R (p.u.)	X (p.u.)	C (p.u.)
VINCENT	230.0	MESA CAL	230.0	1	0.00320	0.03950	0.07200
MIRALOMA	230.0	MESA CAL	230.0	1	0.00138	0.05399	0.07626
PARDEE	230.0	SYLMAR S	230.0	1	0.00065	0.01187	0.02336
PARDEE	230.0	SYLMAR S	230.0	2	0.00065	0.01187	0.02336
EAGLROCK	230.0	SYLMAR S	230.0	1	0.00140	0.02640	0.05100
BENLOMND	230.0	NAUGHTON	230.0	1	0.01080	0.09650	0.16480

Table D.4 Transformer Data of the WSCC Sample System

Bus i	Voltage	Bus j	Voltage	Cir#	R (p.u.)	X (p.u.)	Tap 1	Tap 2
ROUND MT	20.0	ROUND MT	200.0	1		0.02281	18.4	200.0
TEVATR	20.0	TEVATR	200.0	1		0.01815	18.2	200.0
LITEHIPE	20.0	LITEHIPE	230.0	1		0.00365	19.6	230.0
PARDEE	20.0	PARDEE	230.0	1		0.01026	19.7	230.0
ELDORADO	20.0	ELDORADO	500.0	1		0.01512	19.9	500.0
MIRALOMA	20.0	MIRALOMA	500.0	1		0.00516	19.7	500.0
TEVATR2	20.0	TEVATR	500.0	1		0.00448	18.9	500.0
MIDWAY	200.0	MIDWAY	500.0	1	0.00030	0.01740	223.8	500.0
MIDWAY	200.0	MIDWAY	500.0	2	0.00020	0.01190	223.8	500.0
ROUND MT	200.0	ROUND MT	500.0	1	0.00010	0.01740	223.8	500.0
TEVATR	200.0	TEVATR	500.0	1	0.00020	0.01250	223.8	500.0
NAUGHTON	230.0	NAUGHT	20.0	1	0.00050	0.01410	243.5	20.0
RINALDI	230.0	OWENS G	11.5	1	0.00499	0.11473	241.0	11.5
BIG EDDY	230.0	DALLES21	13.8	1		0.01034	240.5	13.8
CASTAIC	230.0	CASTAI4G	18.0	1	0.00050	0.02380	230.0	18.0
HAYNES	230.0	HAYNES3G	18.0	1	0.00058	0.02535	241.3	18.0
CA230	230.0	CMAIN GM	20.0	1		0.00200	230.0	20.0
BIG EDDY	230.0	BIG EDDY	115.0	1	0.00089	0.02990	227.1	115.0
STA BLD	230.0	STA B	138.0	2	0.00015	0.00668	230.0	138.0
SYLMARLA	230.0	SYLMAR S	230.0	1		0.00115	233.1	230.0
STA B1	287.0	STA B	138.0	2	0.00030	0.00746	287.5	138.0
CRAIG	345.0	HAYDEN	20.0	1		0.01500	345.0	20.0
EMERY	345.0	EMERY	20.0	1	0.00020	0.00580	340.0	20.0
CRAIG	345.0	CRAIG	22.0	1		0.01238	345.0	22.0
FOURCORN	345.0	FCNGN4CC	22.0	1		0.00590	345.0	22.0
MIDPOINT	345.0	BRIDGER2	22.0	1		0.00460	345.0	22.0
SAN JUAN	345.0	SJUAN G4	22.0	1		0.00600	360.0	22.0
INTERMT	345.0	INTERM1G	26.0	1		0.00520	353.6	26.0
BENLOMND	345.0	BENLOMND	230.0	1	0.00030	0.01810	345.0	230.0
FOURCORN	345.0	FOURCORN	230.0	2	0.00014	0.00693	345.0	230.0
PINTO	345.0	PINTO PS	345.0	1		0.01950	345.0	345.0
JOHN DAY	500.0	JOHN DAY	13.8	1		0.00375	548.8	13.8
CANADA	500.0	CANAD G1	20.0	1		0.00150	525.0	20.0
CORONADO	500.0	CORONADO	20.0	1		0.01730	477.3	20.0
MONTANA	500.0	MONTA G1	20.0	1		0.00500	545.0	20.0
NORTH	500.0	NORTH G3	20.0	1		0.00250	533.0	20.0
MOHAVE	500.0	MOHAV1CC	22.0	1		0.00980	525.0	22.0
PALOVRDE	500.0	PALOVRD2	24.0	1	0.00006	0.00495	553.0	24.0
DIABLO	500.0	DIABLO1	25.0	1		0.00980	525.0	25.0
NAVAJO	500.0	NAVAJO 2	26.0	1		0.00666	540.0	26.0
ADELAN&1	500.0	RINALDI	230.0	1	0.00013	0.00693	525.0	230.0

Bus i	Voltage	Bus j	Voltage	Cir#	R (p.u.)	X (p.u.)	Tap 1	Tap 2
BIG EDDY	500.0	BIG EDDY	230.0	1	0.00020	0.01181	511.9	230.0
BIG EDDY	500.0	BIG EDDY	230.0	2	0.00009	0.00735	511.9	230.0
CANALB	500.0	CA230TO	230.0	1		0.01000	550.0	230.0
CELILOCA	500.0	CELILO	230.0	1		0.00221	511.7	230.0
MIRALOMA	500.0	MIRALOMA	230.0	1		0.00500	500.0	230.0
RINALDI	500.0	RINALDI	230.0	1	0.00026	0.01386	525.0	230.0
STA E	500.0	STA E	230.0	2	0.00007	0.00693	505.3	230.0
VINCENT	500.0	VINCENT	230.0	3		0.00383	531.5	230.0
VICTORVL	500.0	VICTORVL	287.0	1	0.00020	0.02338	489.5	287.0
CORONADO	500.0	CHOLLA	345.0	1		0.01460	500.0	345.0
FOURCORN	500.0	FOURCORN	345.0	2		0.00550	531.5	345.0
MIDPOINT	500.0	MIDPOINT	345.0	1		0.00720	525.0	345.0

Table D.5 Input Data of the WSCC Sample System in BPA Format

```
( POWERFLOW,CASEID=WSCC1,PROJECT=WSCC )

. Concise version of wscc_r.dat, delete all ZERO fields
. Add thermal (current) limit on Midpoint-Burns-Summer Lines
./ P_OUTPUT_LIST,FULL \
/ P_OUTPUT_LIST,ZONES = ALL \
/ AI_LIST,FULL \
/ NETWORK_DATA \
./ P_INPUT_LIST,FULL \
./ P_INPUT_LIST,ZONES = ALL \
/ NEW_BASE,FILE = WSCCR.BSE \
/ PF_MAP,FILE = WSCCR.MAP \
/ P_ANALYSIS_REPORT,LEVEL=4 \
/ RPT_SORT = ZONE \

BQ    CANAD G120.0CN100.             9999 4450 4000-40001000
BQ    CMAIN GM20.0CN100.             9999 4480 5320-35001019
BQ    MONTA G120.0MT100.             9999 2910 1500-10001000
BQ    NORTH G320.0WA100.             9999 9950 5780-20001000
BS    JOHN DAY13.8OR100.             9999 5173 2649-18501000
BQ    DALLES2113.8OR100.             9999 1301 692.-711 1054
BQ    ROUND MT20.0CA100.             9999 1057 400.-400 1019
BQ    TEVATR  20.0CA100.             9999 594. 300.-300 1049
BQ    TEVATR2 20.0CA100.             9999 3466 2500-10001000
BQ    DIABLO1 25.0CA100.             9999 765. 330.-310  980
BQ    CASTAI4G18.0CA100.             9999 200. 268.-134 1019
BQ    PARDEE  20.0CA100.             9999 2200 600.-600 1009
BQ    OWENS G 11.5CA100.             9999 110. 100.-100 1019
BQ    LITEHIPE20.0CA100.             9999 3195 2000-900 1019
BQ    HAYNES3G18.0CA100.             9999 325. 300.-220 1000
BQ    MIRALOMA20.0CA100.             9999 1690 900.-400 1049
BQ    ELDORADO20.0NV100.             9999982.7 300.-300 1019
BQ    MOHAV1CC22.0NV100.             9999 1679 700.-300 1049
BQ    NAVAJO 226.0AZ100.             9999 1690 700.-280 1000
BQ    PALOVRD224.0AZ100.             9999 2640 1300-900  959
BQ    CORONADO20.0AZ100.             9999 800.300.0-300 1039
BQ    FCNGN4CC22.0NM100.             9999 2160 700.-500 1000
BQ    SJUAN G422.0NM100.             9999 962. 300.-300 1000
BQ    INTERM1G26.0UT100.             9999 1779 850.-440 1049
BQ    EMERY   20.0UT100.             9999 1665 9999-99991049
BQ    HAYDEN  20.0CO100.             9999 2050900.0-900 1000
BQ    CRAIG   22.0CO100.             9999 1048 400.-400  949
BQ    NAUGHT  20.0WY100.             9999 445. 9999-99991000
BQ    BRIDGER2  22ID100.             9999 1640600.0-525 1008
B     CANADA   500CN 4400 1000
B     CANALB   500CN
B     MONTANA  500MT 1700300.0
B     MIDPOINT 500ID             -220
B     NORTH    500WA 5000400.0    1200
B     COULEE   500WA
B     COLSTRP  500WA-1525-50.0
B     GARRISON 500WA 2584394.0
B     HANFORD  500WA 3500500.0     550
B     JOHN DAY 500OR 3200 1100    1019
B     BIG EDDY 500OR-44.222.00
B     GRIZZLY  500OR-66.6-97.0    -674
B     SUMMER L 500OR
```

```
B     BURNS    500OR              -440
B     CELILOCA 500OR               462
B     MALIN    500OR -339 -119    -110
B     ROUND MT 500CA               -91
B     OLINDA   500CA -18961.50
B     TABLE MT 500CA-.700118.5     -91
B     TEVATR   500CA 5661 3491    1500
B     LOSBANOS 500CA265.014.00
B     MOSSLAND 500CA40.0021.50
B     GATES    500CA305.0-7.60     -91
B     MIDWAY   500CA55.60 -329    -327
B     DIABLO   500CA50.0025.00
B     ADELANTO 500CA-1862971.0     912
B     ADELAN&1 500CA

B     VICTORVL 500CA
B     LUGO     500CA204.2-28.2
B     VINCENT  500CA
B     RINALDI  500CA               -80
B     STA E    500CA
B     MIRALOMA 500CA 3098 1189     400
B     SERRANO  500CA 123072.80
B     VALLEY   500CA406.041.00
B     DEVERS   500CA856.019.60
B     PALOVRDE 500AZ793.4207.0    -146
B     WESTWING 500AZ617.0-69.0    -427
B     MOENKOPI 500AZ              -391
B     NAVAJO   500AZ90.0070.00    -190
B     CORONADO 500AZ 1750-56.0
B     ELDORADO 500NV902.3-11.4    -319
B     MOHAVE   500NV              -196
B     FOURCORN 500NM              -113
B     MIDPOINT 345ID610.0 -414    -870
B     BENLOMND 345UT33.9011.90
B     TERMINAL 345UT185.078.50
B     CAMP WIL 345UT457.781.70     -60
B     SPAN FRK 345UT141.271.40
B     MONA     345UT-62.012.80
B     INTERMT  345UT 2053907.1     430
B     EMERY    345UT116.138.40    -220
B     SIGURD   345UT379.0-43.0     -50
B     PINTO PS 345UT
B     PINTO    345UT31.6011.50     -18
B     CRAIG    345CO 2350 -127
B     SAN JUAN 345NM840.05.000     390
B     FOURCORN 345NM239.0-56.0    -155
B     CHOLLA   345AZ
B     CA230    230CN 3600700.0
B     CA230TO  230CN
B     BIG EDDY 230OR-67.5160.0     576
B     BIG EDDY 115OR160.031.25
B     CELILO   230OR 3137 1681     792
B     ROUND MT 200CA148.0         -128
B     COTWDPGE 200CA210.4-77.0
B     GLENN    200CA27.50-.100
B     CORTINA  200CA-43.320.00
B     LOGAN CR 200CA8.010
B     MIDWAY   200CA777.632.60    -130
B     TEVATR   200CA884.054.80     -32
B     CASTAIC  230CA
```

```
B     VICTORVL 287CA -12932.20    -108
B     VINCENT  230CA 1066-10.8    -190
B     MIRALOMA 230CA
B     PARDEE   230CA 311878.00
B     OLIVE    230CA-72.8-17.0
B     RINALDI  230CA121.025.00
B     SYLMARLA 230CA-2771 1654    2146
B     SYLMAR S 230CA401.080.60
B     VALLEY   230CA205.217.60
B     EAGLROCK 230CA175.018.00
B     STA J    230CA887.7-6.20
B     STA B1   287CA
B     STA B2   287CA
B     STA B    138CA237.2-63.2
B     STA BLD  230CA138.028.00
B     STA E    230CA807.8132.1
B     STA F    230CA117.024.00
B     STA G    230CA121.025.00
B     RIVER    230CA320.065.00
B     MESA CAL 230CA377.464.50
B     LITEHIPE 230CA 3191630.0
B     HAYNES   230CA
B     GLENDAL  230CA135.027.00
B     FOURCORN 230NM139.723.80
B     BENLOMND 230UT148.0-7.90
B     NAUGHTON 230WY255.0100.0
L     CRAIG    345 MONA     3451      .00811.13690      1.2174
L     CHOLLA   345 FOURCORN 3451      .00179.01988      1.2880
L     FOURCORN 345 SAN JUAN 3451      .00050.00530      .04410
L     SAN JUAN 345 CRAIG    3451      .00977.11000      1.0000
L     BENLOMND 345 TERMINAL 3451      .00160.02260      .19050
L     CAMP WIL 345 TERMINAL 3451      .00080.01060      .10195
L     BENLOMND 345 CAMP WIL 3451      .00240.03320      .29245
L     CAMP WIL 345 MONA     3451      .00170.02250      .19960
L     CAMP WIL 345 MONA     3452      .00210.02380      .19225
L     EMERY    345 PINTO    3451      .00960.08780      .71325
L     CAMP WIL 345 EMERY    3451      .00520.06020      .50500
L     CAMP WIL 345 EMERY    3452      .00490.05370      .44215
L     CAMP WIL 345 SPAN FRK 3451      .00120.01720      .14935
L     EMERY    345 SIGURD   3451      .00340.03740      .31040
L     EMERY    345 SIGURD   3452      .00340.03720      .30910
L     MONA     345 SIGURD   3451      .00380.03400      .29120
L     MONA     345 SIGURD   3452      .00320.03490      .28610
L     BENLOMND 345 MIDPOINT 3451      .00620.06730      .55780
L     INTERMT  345 MONA     3451      .00180.02450      .21960
L     INTERMT  345 MONA     3452      .00180.02450      .21960
L     PINTO PS 345 FOURCORN 3451      .00480.04360      .35390
L     EMERY    345 SPAN FRK 3451      .00340.03920      .32620
.  500 kV lines
L     CANADA   500 CANALB   5001      .00350.07000      2.3030
L     CANADA   500 NORTH    5001      .00083.02390      1.6500
L     NORTH    500 HANFORD  5001      .00020.00820      .65000
L     NORTH    500 HANFORD  5002      .00020.00820      .65000
L     HANFORD  500 COULEE   5001      .00113.02069      .92763
L     HANFORD  500 MONTANA  5001      .00070.07400      2.4350
L     GARRISON 500 HANFORD  5001      .00142.02258      .94000
L     HANFORD  500 JOHN DAY 5001 1848 .00120.02316      .85760
L     HANFORD  500 JOHN DAY 5002 1848 .00030.02000      1.8000
L     GARRISON 500 JOHN DAY 5001 1848 .00196.03304      .94000
L     GARRISON 500 COLSTRP  5001 1848 .00179.01405      1.8400
```

```
L     BIG EDDY 500 CELILOCA 5001 1848 .00001.00030      .00717                  .0003983
L     BIG EDDY 500 CELILOCA 5002 1848 .00001.00030      .00922                  .0003983
L     BIG EDDY 500 JOHN DAY 5001 1848 .00023.00451      .16660                  .0002511
L     BIG EDDY 500 JOHN DAY 5002 1848 .00020.00446      .15250                  .0002511
. California - Oregon Intertie (COI)
L     GRIZZLY  500 JOHN DAY 5001 1848 .00063.01412      .54878                  .0003983
L     GRIZZLY  500 JOHN DAY 5002 1848 .00109.02408      .77771                  .0003487
L     GRIZZLY  500 JOHN DAY 5003 1848 .00108.02409      .77674                  .0003487
L     GRIZZLY  500 SUMMER L 5001 1848 .00101.00513      .87075                  .0003983
L     GRIZZLY  500 MALIN    5001 1848 .00218.01676      159003                  .0003487
L     GRIZZLY  500 MALIN    5002 1848 .00214.01587      155415                  .0003487
L     MALIN    500 ROUND MT 5001 1848 .00103.00898      .79020                  .0003487
L     MALIN    500 ROUND MT 5002 1848 .00107.00890      .76350                  .0003487
L     MALIN    500 SUMMER L 5001 1848 .00084.00760      .74749                  .0004156
L     MALIN    500 OLINDA   5001 1848 .00103.01230      1.3980
L     BURNS    500 MIDPOINT 5001 1732 .00264.02686      2.6453                  .0004156
L     BURNS    500 SUMMER L 5001 1732 .00122-.0030      1.1035                  .0004156
L     ROUND MT 500 TABLE MT 5001 1848 .00143.00668      .73750                  .0002766
L     ROUND MT 500 TABLE MT 5002 1848 .00143.00668      .73750                  .0002766
L     TABLE MT 500 TEVATR   5001 1848 .00156.01169      1.1557                  .0003079
L     TABLE MT 500 TEVATR   5002 1848 .00097.01022      .71260                  .0003079
L     OLINDA   500 TEVATR   5001 1848 .00158.01071      190435                  .0003079
. California - Oregon Intertie (COI)
L     TEVATR   500 MIDWAY   5001 1848 .00168.03629      1.2387                  .0002829
L     TEVATR   500 GATES    5001 1848 .00094.02544      .69475                  .0002829
L     GATES    500 MIDWAY   5001 1848 .00074.00600      .54395                  .0002829
L     GATES    500 DIABLO   5001 1848 .00079.01937      .66425                  .000.000
L     LOSBANOS 500 GATES    5001 1848 .00083.01985      .00000                  .0002829
L     LOSBANOS 500 MIDWAY   5001 1848 .00153.01470      .00000                  .0001801
L     MOSSLAND 500 LOSBANOS 5001 1848 .00053.01297      .00000                  .0002829
L     DIABLO   500 MIDWAY   5001 1848 .00087.02087      .72855                  .000.000
L     DIABLO   500 MIDWAY   5002 1848 .00087.02087      .72855                  .000.000
L     MIDWAY   500 VINCENT  5001 1848 .00123.00789      .99350                  .0004156
L     MIDWAY   500 VINCENT  5002 1848 .00123.00792      .99440                  .0004156
L     MIDWAY   500 VINCENT  5003 1848 .00112.00747      .91793                  .0004156
L     LUGO     500 VICTORVL 5001 1848 .00020.00410      .14810                  .000.000
L     LUGO     500 MIRALOMA 5001 1848 .00028.00753      .25868                  .0004156
L     LUGO     500 MIRALOMA 5002 1848 .00035.00750      .27680                  .0004156
L     LUGO     500 VINCENT  5001 1848 .00044.01125      .41460                  .0004156
L     LUGO     500 VINCENT  5002 1848 .00044.01125      .41460                  .0004156
L     LUGO     500 MOHAVE   5001 1848 .00190.03100      2.0701                  .0004156
L     ELDORADO 500 LUGO     5001 1848 .00193.02779      2.3356                  .0004156
L     ELDORADO 500 VICTORVL 5001 1848 .00179.02524      .26773                  .000.000
L     ELDORADO 500 VICTORVL 5002 1848 .00179.02524      .26773                  .000.000
L     LUGO     500 SERRANO  5001 1848 .00060.01280      .47310                  .0004156
L     MIRALOMA 500 SERRANO  5001 1848 .00021.00457      .16168                  .0004156
L     SERRANO  500 VALLEY   5001 1848 .00040.00930      .34280                  .0004156
L     VICTORVL 500 RINALDI  5001 1848 .00083.01884      .83334
L     ADELANTO 500 ADELAN&1 5001 1848 .00074.01861      .70132
L     ADELANTO 500 STA E    5001 1848 .00082.01668      .59401
L     ADELANTO 500 VICTORVL 5001 1848 .00000.00159      .06001                  .000.000
L     ADELANTO 500 VICTORVL 5002 1848 .00000.00159      .06001                  .000.000
L     MOHAVE   500 ELDORADO 5001 1848 .00056.01415      .52145                  .0004156
L     DEVERS   500 VALLEY   5001 1848 .00042.00905      .33397                  .0004156
L     PALOVRDE 500 DEVERS   5001 1848 .00259.02967      1.0765                  .0002078
L     PALOVRDE 500 DEVERS   5002 1848 .00259.02967      1.0765                  .0002078
L     NAVAJO   500 ELDORADO 5001 1848 .00280.02110      .50970                  .0001882
L     NAVAJO   500 MOENKOPI 5001 1848 .00077.00544      .69921
L     NAVAJO   500 WESTWING 5001 1848 .00241.03485      2.4328
L     MOENKOPI 500 WESTWING 5001 1848 .00179.02584      1.6961
```

```
L     MOENKOPI 500 ELDORADO 5001 1848 .00207.01359      1.9758
L     PALOVRDE 500 WESTWING 5001 1848 .00040.00960      .45190
L     PALOVRDE 500 WESTWING 5002 1848 .00040.00960      .45190
L     FOURCORN 500 MOENKOPI 5001 1848 .00177.02149      1.6723
L     CA230TO  230 CA230    2301      .00200.02000      .40000
L     BIG EDDY 230 CELILO   2301      .00006.00131      .00189                  .0007580
L     BIG EDDY 230 CELILO   2302      .00006.00116      .00166                  .0007580
L     COTWDPGE 200 ROUND MT 2001      .01113.06678      .03643                  .0002170
L     COTWDPGE 200 ROUND MT 2002      .01050.06540      .03430                  .0001737
L     COTWDPGE 200 ROUND MT 2003      .01105.06642      .03580                  .0002170
L     COTWDPGE 200 TEVATR   2001      .03903.27403      .15536                  .0002156
L     COTWDPGE 200 CORTINA  2001      .02482.16938      .10116                  .0002419
L     CORTINA  200 TEVATR   2001      .01480.10101      .06033                  .0002419
L     COTWDPGE 200 GLENN    2001      .01382.09268      .05530                  .0002156
L     GLENN    200 TEVATR   2001      .03058.20460      .12236                  .0002156
L     COTWDPGE 200 LOGAN CR 2001      .01668.11381      .06804                  .0002419
L     LOGAN CR 200 TEVATR   2001      .02235.16106      .09171                  .0002419
L     STA B1   287 VICTORVL 2871      .01070.07905      .18335                  .000.000
L     STA B2   287 VICTORVL 2871      .01070.07905      .18335                  .000.000
L     STA E    230 GLENDAL  2301      .00047.00723      .00812
L     STA E    230 STA G    2301      .00119.01244      .01399                  .000.000
L     STA E    230 STA G    2302      .00119.01244      .01399                  .000.000
L     STA F    230 HAYNES   2301      .00201.03074      .03443
L     STA F    230 STA BLD  2301      .00073.01025      .01279                  .000.000
L     STA F    230 STA BLD  2302      .00073.01025      .01279                  .000.000
L     STA F    230 STA G    2301      .00110.01189      .01257
L     VALLEY   230 STA E    2301      .00128.00979      .01060
L     GLENDAL  230 STA G    2301      .00035.00536      .00602
L     HAYNES   230 STA G    2301      .00281.04296      .04824
L     RINALDI  230 VALLEY   2301      .00138.01116      .01235                  .000.000
L     RINALDI  230 VALLEY   2302      .00138.01116      .01235                  .000.000
L     RIVER    230 HAYNES   2301      .00220.03422      .03858
L     RIVER    230 HAYNES   2302      .00238.03669      .04142
L     RIVER    230 STA F    2301      .00037.00366      .00415
L     RIVER    230 STA G    2301      .00055.00586      .00623
L     RINALDI  230 STA E    2301      .00229.01583      .01530                  .000.000
L     RINALDI  230 STA E    2302      .00229.01583      .01530                  .000.000
L     CASTAIC  230 OLIVE    2301      .00221.03346      .03669
L     CASTAIC  230 RINALDI  2301      .00290.03800      .04120
L     CASTAIC  230 STA J    2301      .00309.04677      .05040
L     CASTAIC  230 SYLMARLA 2301      .00226.03422      .03753
L     RINALDI  230 OLIVE    2301      .00029.00434      .00475
L     RINALDI  230 STA J    2302      .00071.00484      .01940
L     RINALDI  230 STA J    2304      .00081.00486      .01928
L     RINALDI  230 STA J    2303      .00161.00971      .00964                  .000.000
L     RINALDI  230 SYLMARLA 2301      .00027.00393      .00459                  .000.000
L     RINALDI  230 SYLMARLA 2302      .00027.00393      .00459                  .000.000
L     RINALDI  230 SYLMARLA 2303      .00027.00393      .00459                  .000.000
L     PARDEE   230 VINCENT  2301      .00285.03649      .06328                  .0005823
L     PARDEE   230 VINCENT  2302      .00138.03399      .05626                  .0005823
L     EAGLROCK 230 MESA CAL 2301      .00190.02580      .04920                  .0005823
L     EAGLROCK 230 PARDEE   2301      .00845.07034      .07977                  .0002911
L     LITEHIPE 230 MESA CAL 2301      .00110.01270      .02400                  .0005823
L     VINCENT  230 MESA CAL 2301      .00320.03950      .07200                  .0005823
L     MIRALOMA 230 MESA CAL 2301      .00138.05399      .07626                  .0005823
L     PARDEE   230 SYLMAR S 2301      .00065.01187      .02336                  .0007706
L     PARDEE   230 SYLMAR S 2302      .00065.01187      .02336                  .0007706
L     EAGLROCK 230 SYLMAR S 2301      .00140.02640      .05100                  .0007706
L     BENLOMND 230 NAUGHTON 2301      .01080.09650      .16480
T     CRAIG    345 HAYDEN  20.01            .01500            345. 20.00
```

```
T     CORONADO 500 CHOLLA   3451            .01460            500. 345.0
T     PALOVRDE 500 PALOVRD224.01      .00006.00495            553. 24.00        .0003066.000
T     CORONADO 500 CORONADO20.01            .01730            477.320.00
T     SAN JUAN 345 SJUAN G422.01            .00600            360. 22.00
T     FOURCORN 500 FOURCORN 3452            .00550            531.5345.0
T     FOURCORN 345 FCNGN4CC22.01            .00590            345. 22.00        .0003000.000
T     FOURCORN 345 FOURCORN 2302      .00014.00693            345. 230.0        .000 430.000
T     NAVAJO   500 NAVAJO 226.01            .00666            540. 26.00        .0002000.000
T     CANALB   500 CA230TO  2301            .01000            550. 230.0
T     CANADA   500 CANAD G120.01            .00150            525. 20.00
T     CA230    230 CMAIN GM20.01            .00200            230. 20.00
T     VICTORVL 500 VICTORVL 2871      .00020.02338            489.5287.0
T     INTERMT  345 INTERM1G26.01            .00520            353.626.00
T     MONTANA  500 MONTA G120.01            .00500            545. 20.00
T     MIDPOINT 500 MIDPOINT 3451            .00720            525. 345.0        .0001500.000
T     NORTH    500 NORTH G320.01            .00250            533. 20.00
T     CELILOCA 500 CELILO   2301            .00221            511.7230.0        .0002500.000
T     BIG EDDY 230 BIG EDDY 1151      .00089.02990            227.1115.0        .000 250.000
T     BIG EDDY 500 BIG EDDY 2301      .00020.01181            511.9230.0        .0001008.000
T     BIG EDDY 500 BIG EDDY 2302      .00009.00735            511.9230.0        .0001300.000
T     JOHN DAY 500 JOHN DAY13.81            .00375            548.813.80        .0005000.000
T     BIG EDDY 230 DALLES2113.81            .01034            240.513.80        .0002000.000
T     ROUND MT20.0 ROUND MT 2001            .02281            18.35200.0
T     ROUND MT 200 ROUND MT 5001      .00010.01740            223.8500.0        .000 840.000
T     TEVATR2 20.0 TEVATR   5001            .00448            18.90500.0
T     TEVATR  20.0 TEVATR   2001            .01815            18.18200.0
T     TEVATR   200 TEVATR   5001      .00020.01250            223.8500.0        .0001120.000
T     MIDWAY   200 MIDWAY   5001      .00030.01740            223.8500.0        .000 840.000
T     MIDWAY   200 MIDWAY   5002      .00020.01190            223.8500.0        .0001120.000
T     DIABLO   500 DIABLO1 25.01            .00980            525. 25.00
T     VINCENT  500 VINCENT  2303            .00383            531.5230.0        .0001120.000
T     ELDORADO20.0 ELDORADO 5001            .01512            19.92500.0
T     MOHAVE   500 MOHAV1CC22.01            .00980            525. 22.00
T     LITEHIPE20.0 LITEHIPE 2301            .00365            19.57230.0
T     MIRALOMA20.0 MIRALOMA 5001            .00516            19.69500.0
T     MIRALOMA 500 MIRALOMA 2301            .00500            500. 230.0
T     STA B1   287 STA B    1382      .00030.00746            287.5138.0
T     STA BLD  230 STA B    1382      .00015.00668            230. 138.0
T     STA E    500 STA E    2302      .00007.00693            505.3230.0
T     ADELAN&1 500 RINALDI  2301      .00013.00693            525. 230.0
T     HAYNES   230 HAYNES3G18.01      .00058.02535            241.318.00
T     RINALDI  500 RINALDI  2301      .00026.01386            525. 230.0
T     RINALDI  230 OWENS G 11.51      .00499.11473            241. 11.50
T     CASTAIC  230 CASTAI4G18.01      .00050.02380            230. 18.00
T     SYLMARLA 230 SYLMAR S 2301            .00115            233.1230.0
T     PARDEE  20.0 PARDEE   2301            .01026            19.74230.0
T     CRAIG    345 CRAIG   22.01            .01238            345. 22.00
T     EMERY    345 EMERY   20.01      .00020.00580            340. 20.00
T     PINTO    345 PINTO PS 3451            .01950            345. 345.0
T     BENLOMND 345 BENLOMND 2301      .00030.01810            345. 230.0
T     NAUGHTON 230 NAUGHT  20.01      .00050.01410            243.520.00
T     MIDPOINT 345 BRIDGER2  221            .00460            345. 22.00        .0002000.000
(END)
```

Appendix E Short Circuit Results for the Reduced WSCC System

The short-circuit current and apparent impedance of three-phase permanent fault on the reduced WSCC 179-bus sample system were calculated. The three-phase fault locations were selected based on the following criteria for this moment:

1) select fault location on 500 kV lines
2) select fault location on important tie lines
3) select fault location at different part of each state

The fault locations on the 500 kV lines are listed in Table E.1 below. All the faults were applied on the first end in the table, e.g. the fault was applied at the Grizzly end of line Grizzly 500 - Malin 500.

Table E.1 Fault Locations in the WSCC reduced system

Faulty line	Location
Hanford 500 – Coulee 500	Washington (Central)
John day500 – Garrison 500	Oregon(North)
Grizzly 500 – Malin 500	Oregon(Central)
Malin 500 – Round MT 500	Oregon(South)
Table mt500 – Tevatr 500	California (Central)
Tevatr 500 – Gates 500	California (South)
Lugo 500 - Miraloma 500	California (LA-South)
Moenkopi500 - Fourcorn 500	Arizona (North)
Palovrde500 – Devers 500	Arizona (Southwest)
Midpoint 500 – Burns 500	Idaho(South)

All the short-circuit calculations were based on the classic generator models. The pre-fault current and short-circuit currents together with the apparent impedances of these faults are shown in Table E.2. The results are sorted by the ratio of short-circuit current to pre-fault current (i.e. I2/I1 in the table). For the sake of simplicity, only those lines with a ratio greater than 2.0 are listed in the table following corresponding fault line.

We observe from Table E.2 that the apparent impedance of the neighboring lines reduced significantly following the fault. For example, there are 7 lines with a ratio greater than 2.0 due to fault on the line from Handford to Coulee. The apparent impedance of line John Day to Hanford changed from 302.6 Ohm to 59.2 Ohm, which may less than its zone

3 setting, hence exposed to the fault. If there is a hidden failure in its distance relay, this line may also misoperate.

Table E.2 500 kV Line Currents and Apparent Impedances

Fault line: DIABLO 500 - MIDWAY 500 (1) (Three-phase fault)

Bus I	Voltage	Bus J	Voltage	Cir #	Current I1 (A)	Current I2(A)	Ratio (I2/I1)	Apparent Impedance	
					(Pre-fault)	(During fault)		(Pre-fault)	(During-fault)
MIDWAY	500	VINCENT	500	3	171	1786	10.45	1790	82
MIDWAY	500	VINCENT	500	1	176	1696	9.66	1742	86
MIDWAY	500	VINCENT	500	2	175	1690	9.64	1744	86
DIABLO	500	MIDWAY	500	2	279	980	3.52	1093	100
MIDWAY	500	TEVATR	500	1	505	1271	2.52	606	115
GATES	500	DIABLO	500	1	191	1068	5.58	1588	141
GATES	500	MIDWAY	500	1	371	460	1.24	818	328

Fault line: GATES 500 - DIABLO 500 (Three-phase fault)

Bus I	Voltage	Bus J	Voltage	Circuit#	Current I1 (A)	Current I2 (A)	Ratio (I2/I1)	Apparent Impedance	
					(Pre-fault)	(During fault)		(Pre-fault)	(During-fault)
GATES	500	MIDWAY	500	1	371	2698	7.26	818	45
GATES	500	TEVATR	500	1	678	2023	2.98	448	60
DIABLO	500	MIDWAY	500	2	279	1238	4.45	1093	80
DIABLO	500	MIDWAY	500	1	279	1238	4.45	1093	80
LOSBANOS	500	GATES	500	1	194	464	2.40	1568	309

Fault line: GATES 500 - LOSBANOS 500 (Three-phase fault)

Bus I	Voltage	Bus J	Voltage	Circuit#	Current I1 (A)	Current I2 (A)	Ratio (I2/I1)	Apparent Impedance	
					(Pre-fault)	(During fault)		(Pre-fault)	(During-fault)
LOSBANOS	500	MIDWAY	500	1	148	2770	18.69	2049	25
GATES	500	MIDWAY	500	1	371	2656	7.15	818	50
GATES	500	TEVATR	500	1	678	1903	2.81	448	69
GATES	500	DIABLO	500	1	191	942	4.92	1588	140

Fault line: MIRALOMA 500 - SERRANO 500 (Three-phase fault)

Bus I	Voltage	Bus J	Voltage	Circuit#	Current I1 (A)	Current I2(A)	Ratio (I2/I1)	Apparent Impedance	
					(Pre-fault)	(During fault)		(Pre-fault)	(During-fault)
SERRANO	500	VALLEY	500	1	511	2233	4.37	588	13
LUGO	500	MIRALOMA	500	2	1031	2994	2.90	295	42
LUGO	500	MIRALOMA	500	1	1028	2984	2.90	296	42
LUGO	500	SERRANO	500	1	665	2965	4.46	458	42

Fault line: OLINDA 500 - MALIN 500 (Three-phase fault)

Bus I	Voltage	Bus J	Voltage	Circuit#	Current I1 (A)	Current I2(A)	Ratio (I2/I1)	Apparent Impedance	
					(Pre-fault)	(During fault)		(Pre-fault)	(During-fault)
MALIN	500	SUMMER L	500	1	1382	2689	1.95	222	44
TEVATR	500	OLINDA	500	1	1535	3961	2.58	189	44
MALIN	500	GRIZZLY	500	2	822	1768	2.15	373	66
ROUND MT	500	MALIN	500	2	1079	1560	1.45	278	89
ROUND MT	500	MALIN	500	1	1072	1546	1.44	280	90

Fault line: OLINDA 500 - TEVATR 500 (Three-phase fault)

Bus I	Voltage	Bus J	Voltage	Circuit#	Current I1 (A)	Current I2(A)	Ratio (I2/I1)	Apparent Impedance	
					(Pre-fault)	(During fault)		(Pre-fault)	(During-fault)
OLINDA	500	MALIN	500	1	1268	3740	2.95	238	14
TEVATR	500	TABLE MT	500	2	1321	1539	1.16	219	85
TEVATR	500	TABLE MT	500	1	1150	1339	1.16	252	98
GATES	500	TEVATR	500	1	678	1455	2.14	448	156
MIDWAY	500	TEVATR	500	1	505	1103	2.18	606	219

Fault line: ROUND MT 500 - TABLE MT 500 (1) (Three-phase fault)

Bus I	Voltage	Bus J	Voltage	Circuit#	Current I1 (A)	Current I2(A)	Ratio (I2/I1)	Apparent Impedance	
					(Pre-fault)	(During fault)		(Pre-fault)	(During-fault)
ROUND MT	500	MALIN	500	2	1079	2975	2.76	278	19
ROUND MT	500	MALIN	500	1	1072	2952	2.75	280	20
TEVATR	500	TABLE MT	500	2	1321	3491	2.64	219	42
TABLE MT	500	ROUND MT	500	2	1234	1309	1.06	239	42
TEVATR	500	TABLE MT	500	1	1150	3008	2.61	252	48

Fault line: SERRANO 500 - VALLEY 500 (Three-phase fault)

Bus I	Voltage	Bus J	Voltage	Circuit#	Current I1 (A)	Current I2(A)	Ratio (I2/I1)	Apparent Impedance	
					(Pre-fault)	(During fault)		(Pre-fault)	(During-fault)
MIRALOMA	500	SERRANO	500	1	191	5538	29.00	1572	29
DEVERS	500	VALLEY	500	1	971	2976	3.06	308	34
LUGO	500	SERRANO	500	1	665	2855	4.29	458	65

Fault line: TEVATR 500 - GATES 500 (Three-phase fault)

Bus I	Voltage	Bus J	Voltage	Circuit#	Current I1 (A)	Current I2(A)	Ratio (I2/I1)	Apparent Impedance	
					(Pre-fault)	(During fault)		(Pre-fault)	(During-fault)
GATES	500	MIDWAY	500	1	371	3127	8.42	818	47
TEVATR	500	OLINDA	500	1	1535	1779	1.16	189	109
TEVATR	500	TABLE MT	500	2	1321	1538	1.16	219	126
TEVATR	500	TABLE MT	500	1	1150	1353	1.18	252	143
GATES	500	DIABLO	500	1	191	1011	5.28	1588	144
MIDWAY	500	VINCENT	500	3	171	1298	7.60	1790	148
MIDWAY	500	TEVATR	500	1	505	491	0.97	606	391

Fault line: TEVATR 500 - MIDWAY 500 (Three-phase fault)

Bus I	Voltage	Bus J	Voltage	Circuit#	Current I1 (A)	Current I2(A)	Ratio (I2/I1)	Apparent Impedance	
					(Pre-fault)	(During fault)		(Pre-fault)	(During-fault)
TEVATR	500	OLINDA	500	1	1535	1722	1.12	189	124
TEVATR	500	TABLE MT	500	2	1321	1479	1.12	219	144
MIDWAY	500	VINCENT	500	3	171	1236	7.23	1790	161
TEVATR	500	TABLE MT	500	1	1150	1301	1.13	252	164
MIDWAY	500	VINCENT	500	1	176	1179	6.71	1742	169
MIDWAY	500	VINCENT	500	2	175	1175	6.70	1743	170
GATES	500	TEVATR	500	1	678	669	0.99	448	304
GATES	500	MIDWAY	500	1	371	408	1.10	818	499
DIABLO	500	MIDWAY	500	2	279	351	1.26	1093	607
DIABLO	500	MIDWAY	500	1	279	351	1.26	1093	607

Fault line: VINCENT 500 - LUGO 500 (1) (Three-phase fault)

Bus I	Voltage	Bus J	Voltage	Circuit#	Current I1 (A)	Current I2(A)	Ratio (I2/I1)	Apparent Impedance	
					(Pre-fault)	(During fault)		(Pre-fault)	(During-fault)
LUGO	500	VICTORVL	500	1	1906	3180	1.67	160	35
LUGO	500	MIRALOMA	500	2	1031	1688	1.64	295	66
LUGO	500	MIRALOMA	500	1	1028	1681	1.64	296	67
LUGO	500	MOHAVE	500	1	1144	1675	1.46	266	67
MIDWAY	500	VINCENT	500	3	171	1358	7.95	1790	89
MIDWAY	500	VINCENT	500	1	176	1279	7.28	1742	94
MIDWAY	500	VINCENT	500	2	175	1274	7.26	1743	95
LUGO	500	SERRANO	500	1	665	1053	1.58	458	106
ELDORADO	500	LUGO	500	1	1028	1384	1.35	295	148
LUGO	500	VINCENT	500	2	570	702	1.23	534	160

Fault line: VINCENT 500 - MIDWAY 500 (1) (Three-phase fault)

Bus I	Voltage	Bus J	Voltage	Circuit#	Current I1 (A)	Current I2(A)	Ratio (I2/I1)	Apparent Impedance	
					(Pre-fault)	(During fault)		(Pre-fault)	(During-fault)
MIDWAY	500	TEVATR	500	1	505	1863	3.69	606	35
GATES	500	MIDWAY	500	1	371	1960	5.28	818	49
LUGO	500	VINCENT	500	1	570	3035	5.32	534	53
LUGO	500	VINCENT	500	2	570	3035	5.32	534	53
MIDWAY	500	VINCENT	500	3	171	653	3.82	1790	101
MIDWAY	500	VINCENT	500	2	175	618	3.52	1744	106
DIABLO	500	MIDWAY	500	2	279	765	2.75	1093	137
DIABLO	500	MIDWAY	500	1	279	765	2.75	1093	137
LOSBANOS	500	MIDWAY	500	1	148	331	2.23	2049	236

Fault line: VALLEY 500 - DEVERS 500 (Three-phase fault)

Bus I	Voltage	Bus J	Voltage	Circuit#	Current I1 (A)	Current I2(A)	Ratio (I2/I1)	Apparent Impedance	
					(Pre-fault)	(During fault)		(Pre-fault)	(During-fault)
SERRANO	500	VALLEY	500	1	511	4953	9.69	588	35
PALOVRDE	500	DEVERS	500	2	971	1918	1.97	312	101
PALOVRDE	500	DEVERS	500	1	971	1918	1.97	312	101

Qun Qiu

Qun Qiu was born in Changting, Fujian province in southeast China. He received his B.S. degree from Zhejiang University and his M.S. degree from the graduate school of CEPRI (Beijing, China), both in electrical engineering. In 1989, he joined China Electric Power Research Institute (CEPRI) in Beijing, China as a research engineer, where he developed a load-resource balance program (1989-1990) and a dynamic stability (small signal stability) program (1992~1993), which have been purchased by more than a dozen utilities in China. In 1996, he went to Manitoba HVDC Research Center (Winnipeg, Canada) developing the High Speed Transient Stability program based on the Real Time Digital Simulator (RTDS); he implemented all IEEE excitation system models in the program—including 9 models published in 1968 and 12 models published in 1981. He has in-depth knowledge of BPA Load Flow and Transient Stability programs and working knowledge of ASPEN, PSS/E, EMTP, EPRI's PSAPAC (IPFLOW, ETMSP), WASP III, POWERSYM, PSCAD, GE's URPC, SEL's 5010/5020/5030, WonderWare, etc.

Qun Qiu also worked as a consulting engineer in assisting electric utilities in developing solutions for safe and reliable power system operations, providing training and technical support to power engineers in the following areas:

-Load flow analysis -Short circuit calculation
-Contingency analysis -EHV network planning (500kV/230kV)
-Production simulation -Power system modeling
-Dynamic stability analysis and PSS/excitation system tuning

Qun Qiu joined American Electric Power (AEP) in May 2002, where his duties include: corporate-wide protection and control standards development and production deployment, substation data network application development, process refinement, etc. He is the lead engineer of Motor Operated Air Breaker (MOAB) standard in AEP.

Other responsibilities include area protection coordination study for AEP's Indiana and Michigan network, substation automation/integration, Human Machine Interface development, PMU applications, and training and technical support to station design engineers, field protection and control engineers.

In April 2003, he completed an analysis on 765kV Capacitor Coupling Voltage Transformer (CCVT) failures and AEP 765kV CCVT design practice; his study led to a new 765kV CCVT design standard for line protection. The new design standard was in effect in June, 2003, and will have an immediate saving over $1.15 million in 2004 and about $3.85 millions savings in total for the next few years. He is currently working on the design of a MOAB automatic control logic that will be implemented late 2003. This is the first pilot project for this control package, which is more economical than AEP past MOAB Standards.

Qun Qiu is the author/co-author of more than 20 technical reports, conference papers and journal papers. His research interests include power system protection and control, power system operation and planning, relay hidden failures, reliability/risk assessment, substation automation/integration, phasor measurement applications.

He is a student member of the Institute of Electrical and Electronics Engineers.

Educations:

PhD, Electrical Engineering	July 1999 - September 2003 Virginia Tech, Blacksburg, Virginia
MS, Computer Engineering	August 2001 Virginia Tech, Blacksburg, Virginia
MS, Electrical Engineering,	May 1996 Graduate School of EPRI, Beijing China
BS, Electrical Engineering,	July 1989 Zhejiang University, Hangzhou, China

Selected projects:

- Solid State Breaker (SSB) and Dynamic Voltage Restorer (DVR) Simulations
  - Developed simulation schemes and conducted the performance analysis of SSB and DVR for the Siemens-Westinghouse Energy Management Division in Orlando, FL (1998~1999)
- Three Gorges Power System Real-time Simulation (1997~1998)
  - Developed and commissioned the equivalent circuit of the Three Gorges Power System on the Real Time Digital Simulator (RTDS)

- <u>Power System Planning and Operation Studies</u>
  - Supervised the 500kV network planning study of Hebei southern power grid (Supervisor, 1997)
  - Studied the optimal power dispatch of the Three Gorges Hydro-Station (18.2GW) among four utilities in Central China (Principal Investigator, 1995)
  - Evaluated the transmission schemes of the Ertang hydropower station (3300MW) to Sichuan Power Grid (PI, 1994)
  - Investigated the power capacity to be transmitted from Yunnan to Guangdong power grid (PI, 1993)
  - Performed the load-resource balance analysis for four utilities in Southern China AC/DC Interconnected Systems (PI, 1989~1990)
- <u>Power System Security Studies</u>
  - Investigated the dynamic stability behaviors of North-China Power Grid (41GW) and PSS application (Supervisor, 1997)
  - Performed the eigenvalue/eigenvector analysis of Southern China AC/DC Interconnected Systems (39GW) and PSS tuning (PI, 1995-96)
  - Conducted the security analysis (transient stability) of the transmission system from Three Gorges Hydro-Station to Sichuan power grid (PI, 1995)
  - Performed the contingency analysis on the Guangdong Provincial Power Company (31GW) and assisted the utility to develop control strategies (PI, 1993).
  - Integration field tests of TSQ-Guangdong 500 kV AC transmission lines (1992)