1996

Risk-based operating limits for dynamic security constrained electric power systems

Agustín A. Irizarry-Rivera
Iowa State University

INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps. Each original is also photographed in one exposure and is included in reduced form at the back of the book.

Photographs included in the original manuscript have been reproduced xerographically in this copy. Higher quality 6" x 9" black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.

UMI

A Bell & Howell Information Company
300 North Zeeb Road, Ann Arbor MI 48106-1346 USA
313/761-4700 800/521-0600

Risk-based operating limits for dynamic security constrained electric power systems

by

Agustín A. Irizarry-Rivera

A dissertation submitted to the graduate faculty

in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Major: Electrical Engineering (Electric Power)

Major Professor: James D. McCalley

Iowa State University

Ames, Iowa

1996

Graduate College
Iowa State University

This is to certify that the Doctoral dissertation of

Agustín A. Irizarry-Rivera

has met the dissertation requirements of Iowa State University

Signature was redacted for privacy.

Committee Member

Signature was redacted for privacy.

Committee Member

Signature was redacted for privacy.

Committee Member

Signature was redacted for privacy.

Committee Member

Signature was redacted for privacy.

Major Professor

Signature was redacted for privacy.

For the Major Program

Signature was redacted for privacy.

For the Graduate College

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 OVERVIEW

1.1 Introduction

In this chapter we present the objective of this work, namely, to develop the foundation for a risk-based approach to security assessment in electric power systems operations to determine operating limits based on risk. Particular emphasis is placed on security constraints associated with dynamic system performance. We present the need for risk management in today's electric energy competitive market and how risk management may be used to balance system reliability and costs.

1.2 Power system security; operational planning

Our objective, to develop a risk-based approach to security assessment in electric power systems operations, is motivated by a perception that today's deterministic approach to security assessment often results in costly operating restrictions that are not justified by the corresponding low level of risk. Use of a risk-based approach to security assessment is therefore attractive because it offers the potential to allow operating practices that more equitably balance the tradeoff between cost and security, resulting in substantial savings from use of less costly energy resources.

Security problems most commonly manifest themselves in one of three different forms. Thermal overload of a circuit occurs when current exceeds the ratings of a circuit, and the circuit overheats due to the I^2R losses, resulting in circuit loss of life and subsequent

damage. Voltage instability occurs when there is insufficient reactive power supply and can lead to unacceptably low voltages. The third form, rotor angle instability, is concerned with the system dynamic response following a disturbance in terms of the generators' ability to remain in synchronism. In this research we focus on thermal overloads and rotor angle instability.

In general, security assessment in an operational planning environment seeks to determine operating limits for a given system situation characterized by:

1. *system configuration:* network topology and unit commitment
2. *operating conditions:* generation levels, line flows and voltage levels (observable and controllable) and load levels (observable only)
3. *contingency set:* a list of outage events
4. *performance measure:* post-contingency system performance criteria

Because a single study requires an explicit choice of configuration, conditions and contingency, and because the number of each is quite large, the number of possible studies is overwhelming. To reduce the possibilities to a manageable size and still obtain useful results, studies are limited using a credibility criterion: only credible system configurations, operating conditions and outage events are considered. This criterion is not usually applied statistically but rather using rules of thumb and judgment. Second, a severity criterion is applied: here the analyst tries to identify the system configuration, operating conditions, and outage event which result in the most severe system performance. Because this approach generally identifies a single event which drives the resulting decision, it is often called the deterministic approach. The deterministic approach is widely accepted in industry. It should be noted that the basic underpinings of the approach are probability (credibility) and consequence (severity), if only in a qualitative way. Therefore, the philosophy behind the deterministic approach is to appraise

the system situation using qualitative risk. In this work we develop the means of determining operating limits using quantitative risk. where we measure the credibility of events using probability and assess its severity via its economic impact.

In our method we still choose system configuration and operating conditions based on their credibility[1]. using engineering judgment. but we provide that the basis for decision making should be influenced by all credible events having potential to result in economic impact. and not just the most severe event. We replace the traditional performance measures. e.g.. stable or unstable for transient instability and overloaded or not for thermal problems. with expected cost over an interval of time or risk. The resulting acceptable operating region includes all operating conditions having risk below a specified threshold.

1.3 Deterministic security assessment: how it works and the need to enhance it

For a given network configuration (which circuits are in service and which generators are on line). system stability performance following a particular contingency is dependent on (1) the fault attributes: type. location. and duration. and (2) the operating conditions previous to initiation of the fault. The operating conditions are characterized by load levels. which the operator can monitor but not control. and generation power outputs. transmission flows and voltage levels which the operator can both monitor and control. The operational planner makes an assessment of the system security level based on the current operating conditions by asking a series of "what if" questions. e.g.. "What if a three phase fault occurs on the circuit from bus 10 to bus 20. and it is removed". Normally. the questions to be posed are predetermined off-line by using computer sim-

[1]In operational planning. studies are normally done only weeks or months ahead of the time frame for using the results. Thus. because of the short lead time. it is easy to predict which configuration and operating conditions are credible.

ulation to identify credible contingencies having potential to cause instability. These contingencies are referred to as the *defined contingency set.* A credible contingency usually includes any contingency resulting in loss of a single component (called an $N-1$ contingency), and in special cases, contingencies resulting in simultaneous loss of two components ($N-2$).

There are two levels of security assessment: classification and boundary determination. Classification involves identifying a particular operating condition as secure or insecure, depending on whether the postcontingency system performance is acceptable or not, for all contingencies in the set. Classification does not, however, quantify *proximity* of the operating condition to insecure conditions. For this we need boundary determination. Boundary determination involves identifying the frontier between secure and insecure operating regions.

Boundaries are represented by constraints imposed on parameters characterizing precontingency operating conditions. We call these operating parameters the critical parameters (CPs). If the boundary is given as a function of two critical parameters, e.g., the real power flow of two transmission lines, a nomogram may be used to illustrate the situation, as indicated on Figure 1.1.

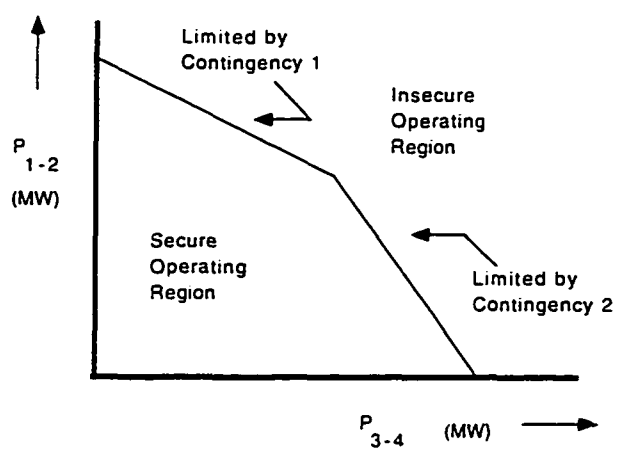

Figure 1.1 A nomogram

In practice, boundaries are often dependent on more than two CPs. Therefore, many nomograms are constructed for various combinations of the CPs not used on the axes of the two-dimensional graphs. Because this work is highly specialized, requiring considerable expertise, and is also labor intensive, it must be done off-line. An approach has evolved in the industry for developing nomograms, and we refer to this as the deterministic approach. The deterministic approach typically adheres to the following steps:

1. *Study Parameters:* Identify one or more study parameters for which a limit is desired.

2. *Base Case Model:* Develop a base case model of the planned operating system for the period under consideration.

3. *Credible Contingency List:* Develop a credible contingency list for each study parameter identified in Step 1 [1].

4. *Most Limiting Contingency:* Identify the most limiting contingency, or contingencies[2], from the list, for each study parameter.

5. *Critical Parameter Set:* For each most limiting contingency, identify the critical parameters, i.e., the precontingency conditions that most influence the postcontingency system performance.

6. *Boundary Determination:* Identify the boundary for each critical parameter as the level where system performance following the most limiting contingency first violates minimum operating reliability criteria.

The criterion for judging operating point acceptability is then based on the identified limit. An operating point beyond this limit is unacceptable. Therefore, in theory, the

[2]One contingency may be most limiting under some operating conditions whereas another contingency may be most limiting under different operating conditions.

deterministic approach *tolerates no risk*. i.e.. the limits are hard. In practice. operating engineers sometimes decide to violate the limits. particularly if there is strong economic incentive to do so. It is this kind of decision which we want to quantitatively frame: the following example will illustrate the point.

Consider that the deterministic approach requires that a very efficient 1000 MW unit costing $40/MWhr is constrained to operate below a limit of 900 MW for the next hour. due to a stability problem resulting from a certain contingency. The cost of replacing the 100 MW is $80/MWhr. Thus, the cost of adhering to the constraint for 1 hour is the difference between the production cost with and without the constraint:

$$([900 \times 40 + 100 \times 80] - [1000 \times 40])1 \text{ hr} = \$4.000.$$

On the other hand. consider that the plant is operating at 1000 MW. the contingency occurs. and the plant loses synchronism. but the remainder of the system remains intact. i.e.. there are no cascading effects. Assume it will take 10 hours to resynchronize the plant. During this time. it will be necessary to replace the energy at a cost of $80/MWhr for the first 100 MW and $90/MWhr for the remaining 900 MW. The direct cost (there are other costs. but we ignore them here for simplicity) of the instability is the difference between production costs with and without the instability:

$$([100 \times 80 + 900 \times 90] - [1000 \times 40])10 \text{ hrs} = \$490.000.$$

The decision of whether to operate at 900 MW or 1000 MW requires an additional piece of information: What is the probability of instability over the next hour when the plant operates at 1000 MW? Let the probability of instability over the next hour be 0.008 such that the expected cost of instability. or risk. is $0.008 \times \$490.000 = \$3.920$. In this case because $\$3.920 < \$4.000$. the best decision is to operate beyond the limit. We conclude that. depending on the relation between the risk[3]. defined as the product of

[3]The *expected monetary value* [2] of a "gamble" with several possible outcomes is the sum of the

probability of instability and the *consequences of instability* [3]. and the expected benefit. it may be advantageous to violate the deterministic limit by operating at 1000 MW.

1.4 Need for risk management: system reliability and its cost

The electric energy industry is expected to economically supply energy on demand without local failures or large-scale blackouts. To achieve this objective engineers need to assess and maintain or improve the reliability[4] of the electric power system while balancing reliability cost and reliability worth. Any player of today's competitive electric energy market which can adequately assess and balance its system reliability cost and reliability worth will have an advantage over its competitors since this player will be able to answer the question: "How much and in what way should money be spent in order to optimize the level of reliability ?". The answer to this question allows achieving a reliable level of operation at reasonable costs. Failure to answer the question results in short-term savings at the expense of lower reliability or excessive expenditures to achieve an unnecessarily high level of reliability: the former may undermine customers trust in the company's ability to serve its needs. the latter will divert the company's resources from more profitable activities.

We use the risk of operating at a given operating point. i.e. the expected cost of operating at a given operating point. to evaluate system reliability cost/reliability worth. Our measure of reliability is indirect since we calculate the probability of failure rather

products of monetary worth of each possible outcome and its probability. The probability of instability j equals the probability of suffering the impact associated with instability j. Therefore. the expected benefit minus the composite risk. the sum of the products of the impact associated with instability j. in dollars. and the probability of suffering that impact gives the expected monetary value of operating at point p for instability j.

[4]Reliability is the probability of a device or system performing its purpose adequately for the period of time intended under the operating conditions encountered [4]. Reliability. in a bulk power electric system. is the degree to which the performance of the elements of that system results in power being delivered to consumers within accepted standards and in the amount desired. The degree of reliability has been measured by the frequency. duration. and magnitude of adverse effects on consumer service. It is commonly thought to include two main components: adequacy, which is the ability to supply the demand. and security. which is the ability to respond to disturbances in an acceptable fashion [5].

than the probability of successful operation and use the economic impact of this failure to appraise the cost of unreliability. Economic impact is a major component of our method and is concerned with all costs: generation owner costs. transmission owner costs. customers costs and societal costs.

1.5 Risk-based security assessment

Risk is defined as the product of probability and impact

$$R = P \times I \tag{1.1}$$

Higher values of R indicate higher values of risk.

The risk-based approach builds from the deterministic approach in that steps 1. 2 and 3 are retained. However. the risk-based approach departs from the deterministic approach in the following fundamental way. Whereas the deterministic approach develops limits based on the most severe contingencies. the risk-based approach develops limits based on a composite measure computed from a risk contribution from all contingencies in the list. where risk is the product of probability and consequence. Therefore. in the risk-based approach. analysis is required for all contingencies in the list and not just the most severe. Although this requirement could result in additional labor. this is a reasonable price to pay to gain the benefits associated with a more quantitative assessment of the security versus economy tradeoff.

The main difference in the two approaches resides not in the methods used to obtain results regarding system performance following a specific contingency; indeed the same methods are required in both approaches. Instead. the main difference in the two approaches resides in the criterion used to judge operating point acceptability. Whereas one uses a deterministic criterion (secure or insecure for most severe contingency under worst-case disturbance scenario). the other uses a criterion based on probability and

consequence (composite risk level from all contingencies). Therefore the risk-based approach does not necessarily replace the deterministic approach: *it extends it.* One of the appeals of this approach is ease of transition for system operators: the change is transparent to the operators except for new graphs and tables.

1.6 Work done in this dissertation

In this work we develop a method that provides risk-based security assessment in an operating environment considering any type of security violation. Particular emphasis is placed on security constraints associated with dynamic system performance. Our work is motivated by a perception that today's deterministic approach to security assessment often results in costly operating restrictions that are not justified by the corresponding low level of risk. A risk-based approach to security assessment is attractive because it balances the system's reliability cost and reliability worth.

Our method allows determination of operating limits based on the risk of insecurity at a given operating point. We characterize the operating point in terms of pre-contingency controllable parameters, the *critical parameter set*, that most influence the postcontingency system performance. Total risk at a given operating point is obtained summing over all the individual risk associated with defined security violations and their corresponding triggering events. We develop risk expressions that account for fully reliable conventional protection equipment and for main breakers passive and active failures.

This dissertation introduces the concept of limiting operating point functions, curves that give limiting values of the critical parameter for various fault locations on a line and characterize the dependency of operating limit on fault type and fault location. The limiting operating point functions combine system stability performance and probability of instability information. This dissertation includes a detailed study on how excitation systems and other parameters affect limiting operating point functions. We also develop,

using probability theory. expressions to calculate the conditional probability of insecurity given a fault occurs for thermal overloads and two approaches for computing probability of transient instability: one based on Law of Total Probability and the other on Cartesian products.

Finally. we use a modified version of the IEEE Reliability Test System to illustrate risk-based electric power system security assessment and to compare it with traditional deterministic security assessment. We determine operating limits using iso-risk contours drawn in the space of pre-contingency controllable parameters. effectively creating nomograms based on risk. The contours of constant risk in the space of operating parameters provide a risk management tool that allows managers to justify decisions to operate beyond deterministic operating limits when it is economically advantageous to do so. The tool may also be useful in providing justification of constraints enforced to maintain security levels when these are challenged by a participant penalized as a result of them.

1.7 Organization of this dissertation

This dissertation is organized as follows: chapter 1 presents an overview of the work. chapter 2 is a literature survey. in chapter 3 our method to calculate the risk of an operating point is presented. chapter 4 presents the limiting point functions and their effect on probability of instability. chapter 5 presents a risk management example using a modified IEEE Reliability Test System and chapter 6 provides conclusions and suggestions for future work.

2 LITERATURE SURVEY

2.1 Introduction

This chapter presents a review of previous work on probabilistic security assessment and protective equipment reliability.

2.2 Probabilistic stability assessment

A review of previous work on probabilistic stability assessment indicates a considerable amount of literature is available: a sample of the main approaches dealing with security are referenced in what follows.

Anderson, Bose, and colleagues [6, 7] outlined a procedure to obtain a transient stability probability function through unspecified non-linear transformations of the probability distributions, or densities, of disturbance location, type and sequence. Conceptually, an n^{th} order joint density function of the random process is obtained via this transformation but the authors preferred to employ Monte Carlo simulation in their computation [8].

Billinton and Kuruganty [9, 10, 11] compute probability of stability based on reliability of fault clearing devices, the time needed for successfully clearing a fault being less than the critical clearing time, and probabilistic representation of fault location and fault type. A similar approach is followed by Hsu and Chang [12] who obtain the probability of system instability as the probability of critical clearing time of a certain fault event being less that the actual clearing time for that fault event.

Wu et al. [13] propose an approach based on a time to insecurity. In this approach the dynamic security region with respect to a fault is the set of injections for which the system is transiently stable. The time to insecurity is the first instant at which the injection leaves the corresponding security region. The probability distribution of the time to insecurity is expressed in terms of the configuration of the system at time t and the transition probabilities to other possible states. Although theoretically sound, at the moment of applying it, the approach requires determining the steady-state and dynamic security regions for each point of operation. The derivation of the probability function of time to insecurity requires knowledge of these regions. This is a major difference from our approach, we use probability of instability to determine operating security regions, i.e., to determine operating limits.

Leite da Silva et al. [14] develop a framework for integrating adequacy and security assessment, resulting in computation of probabilistic indices for predisturbance conditions. In their work system states are classified according to the impact of a disturbance and transition rates between states (Markovian) are used to characterize the stochastic nature of how each state is reached. Security is measured in terms of the probability of clearing a fault before critical clearing time is reached. This method uses the impact of the disturbance to classify the states of the system, thus incorporating impact of the disturbance within the probability of insecurity calculation. We use impact of the disturbance to calculate risk of an operating point, the probability of the event and its impact are decoupled up to the point of calculating risk.

Counan et al. [15] devise a defense plan against extremely low probability but very severe system collapse mechanisms. Such a defense plan may be complementary to the risk based security strategy proposed here in order to account for the extremely low probability events which may result in very severe impacts.

The IEEE PES APM Working Group [16] presents a broad assessment of trends and needs in reliability practices: one of the needs identified was a risk assessment index for

power system operation.

2.3 Protective equipment reliability

A secure system may only be achieved via reliable protective equipment. Defective, poorly-maintained or mis-calibrated protective equipment may cause severe security violations costing up to hundred of millions dollars. In our work we study the effect of protective equipment reliability on risk. Most security assessment studies assume fully reliable protective equipment, thus we provide a risk expression that follows this assumption. We also consider the possibility of protective equipment failure, resulting in higher impact for the same triggering event, and provide a risk expression for this situation as well. The following is a representative sample of protective equipment reliability literature.

The IEEE APM Task Force Report on Protective Systems Reliability [17] identified two types of protection schemes: conventional (component protection) and special (system protection). The report focus on the first and identifies two major failure modes of breakers or protection systems: failure to operate when the operation is called for and false tripping operation. Four methods for evaluating the effects of protection system malfunctions on the operation of power systems are briefly reviewed. These are: 1) adjusting the failure rates of protected components, 2) circuit breaker models, 3) event tree method, and 4) Monte Carlo method.

Kuruganty and Billinton [18] use probability density functions of the operating times associated with the components of the protection system such as relays, breakers, etc. These are assumed and used in conjunction with the reliabilities of the main and backup protection schemes to obtain the pdf of the fault clearing time. These densities are used together with the critical clearing time, conceivably for any fault type and location, to obtain a probability index for transient instability.

P.M. Anderson [19] measures reliability of a protection system as the probability of successful operation of the system. Failures are divided into operational failure, a failure to operate when it should, and security failure, initiating an unnecessary or unwanted operation when there is no fault in the relay's protective zone. Anderson uses basic series and parallel systems reliability calculations to model redundant relay-breaker configurations as well as different typical power system relay and circuit breaker control configurations.

Anderson's paper represents, in our opinion, the best reference on how to calculate the probability of protection system failure taking into account components reliability and system configuration: it uses failure modes and effect analysis method. Later in this work we include the probability of protection system failure in our risk expression and suggest the use of the method presented by Anderson to calculate the necessary probabilities. The following is a summary of Anderson's paper.

2.3.1 Failure modes and effect analysis of conventional protection systems

A fully redundant protection system installation is shown in Figure 2.1. A more common protective system configuration for high voltage transmission systems is similar to that of Figure 2.2-1, where parallel redundancy is employed in the relays but a single circuit breaker trip coil and breaker trip mechanism is used.

In order to perform analysis, a system configuration must be assumed. We consider three control configurations, with different degrees of redundancy, shown in Figure 2.2. Each control configuration assumes a single battery supply, a single breaker mechanism, and parallel redundant relays. Control configuration #2 provides redundant current transformers (CT) and potential transformers (PT). Control configuration #3 provides redundant circuit breaker trip coils, in addition to the redundancies of configuration #2. These three control configurations are considered typical of industry practice.

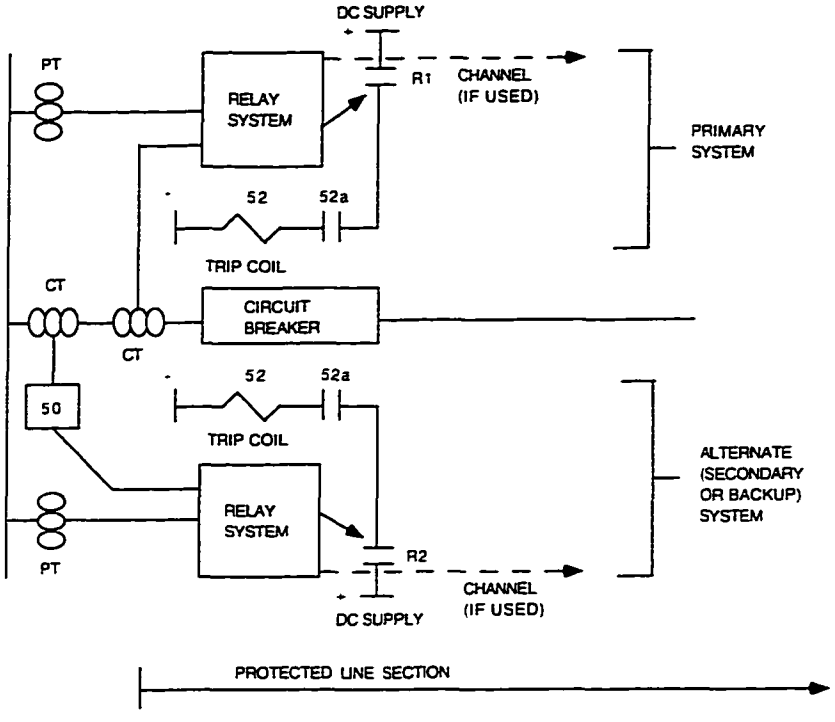

Figure 2.1 Transmission line protection with maximum practical redundancy

In [19] the author considers two backup systems. Local Backup System (LBS) and a Remote Backup System (RBS). A simplified LBS is shown in Figure 2.3. The main protective relay (MPR) contacts close upon fault recognition and pick up contacts 62x or 62y in addition to the trip coil (52T). Relay 50 is an overcurrent relay: the contacts remain closed as long as the fault is uncleared, thus allowing coil 62 to energize a timer. When the timer completes its cycle, contacts 62 close, energizing the breaker failure relay 86. Relay 86 has multiple contacts that initiate tripping on all breakers adjacent to the failed system. These breakers adjacent to the failed system are located on the same transmission switching station. Faults may be cleared by the LBS without taking other lines out of service depending on the transmission switching station arrangement.

Now consider a protective system strategy for a power system that incorporates all three relay systems: the Main Protective System (MPS), the Local Backup System

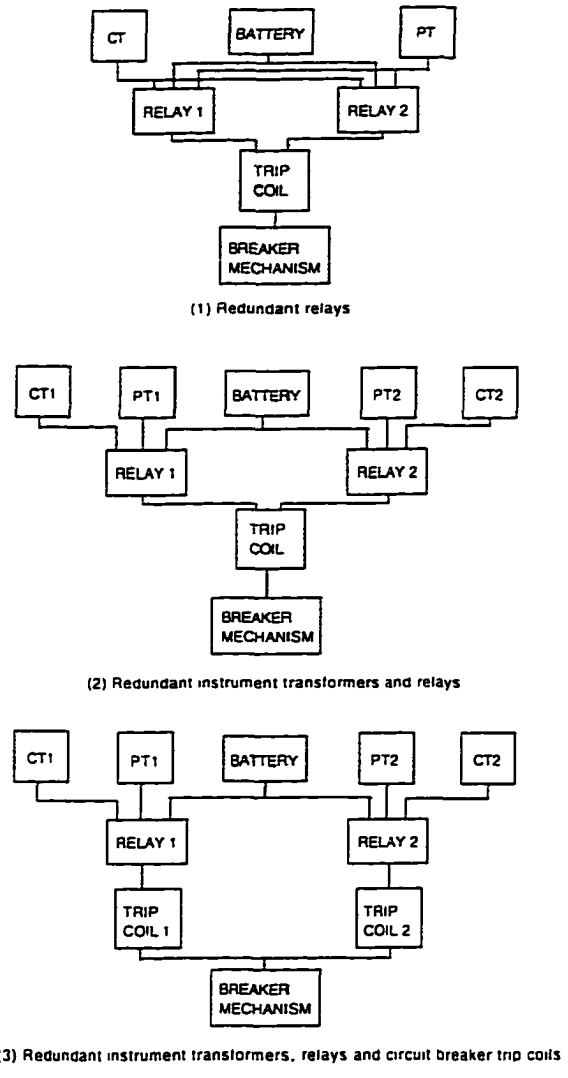

Figure 2.2 Block diagram of typical power system relay and circuit breaker control configuration

(LBS), and the Remote Backup System (RBS). It is further assumed that these systems will only fail by operational mode failure, i.e., failure to operate when called upon to do so.

The three protective systems under consideration will usually have a control configuration similar to one of those illustrated in Figure 2.2. Backup systems may be simpler than these general arrangements due to the omission of redundant elements. In any case, we note the series logic of these systems. The logical pattern is always

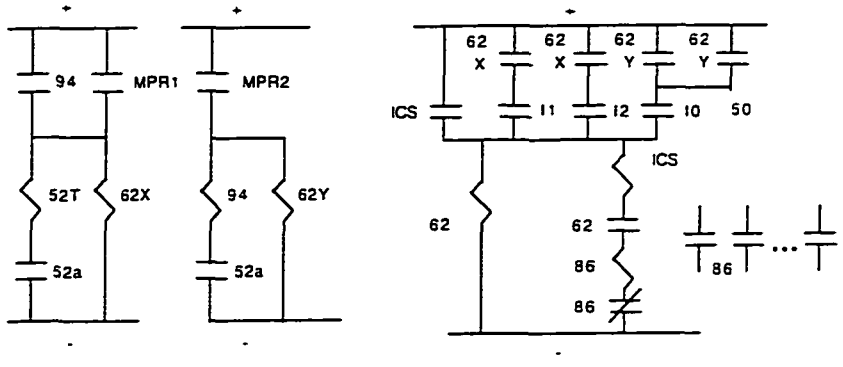

Figure 2.3 Simplified DC protection schematic for breaker failure and local backup protection

1. instrument transformers and battery

2. relays

3. trip coil(s)

4. breaker mechanism.

For analysis. we group these components into two groups. a protective relay (electrical) group and a circuit breaker (mechanical) group. Somewhat arbitrarily we include 1. 2. and 3 in the relay group. and 4 in the circuit breaker group. This simplifies the notation for computing reliabilities.

We now define the event SFC = Successful Fault Clearing and compute the protective system reliability as

$$R = P(SFC) \tag{2.1}$$

To compute 2.1 we compute the reliability of each subsystem. and combine the results. Let MCB stand for main circuit breaker.

In order to simplify the notation. we write

$$\begin{aligned} P_{MPS} &= P(MPSworks) \\ &= P(MPRworksandMCBworks) \\ &= P_{MPR}P_{MCB} \end{aligned} \tag{2.2}$$

since MPR and MCB are independent systems.

We also define

$$\begin{aligned} Q_{MPS} &= P(MPSfails) = 1 - P_{MPS} \\ &= Q_{MPR} + Q_{MCB} - Q_{MPR}Q_{MCB} \end{aligned} \tag{2.3}$$

The LBS and RBS have definitions similar to 2.2 and 2.3. with only the subscripts changed.

To compute the system reliability 2.1. we evaluate the probabilities associated with both the local systems and the remote systems. Clearly. one or the other must work correctly for successful fault clearing. If we let LPS designate the "local protective systems" and RBS the "remote backup systems" we may write

$$R = P(SFC) = P_{LPS} + P_{RBS} - P_{LBS}P_{RBS} \tag{2.4}$$

The LPS consists of both the main protective system and the local backup system. Now. the local backup system depends on successful primary relay operation. This gives the logic diagram of Figure 2.4. for which we compute

$$P_{LPS} = P_{MPR}(P_{MCB} + P_{LBS} - P_{MCB}P_{LBS}) \tag{2.5}$$

where

$$P_{LBS} = P_{LBR}P_{LCB} \tag{2.6}$$

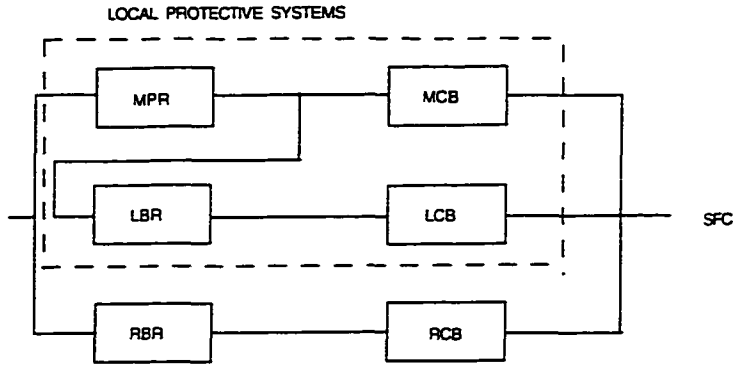

Figure 2.4 Logic diagram of successful fault clearing

and MPR stands for main protective relay. MCB stands for main circuit breaker. LBR stands for local backup relay and LCB stands for local circuit breaker.

Combining 2.5 and 2.6 we compute. after some algebraic manipulation.

$$R = P(SFC) = P_{MPR}P_{MCB} + P_{MPR}Q_{MCB}P_{LBS} + P_{MPR}Q_{MCB}Q_{LBS}P_{RBS} + Q_{MPR}P_{RBS} \tag{2.7}$$

In some case it is more convenient to work with the probability of system failure. i.e..

$$Q = 1 - R = Q_{MPR} + Q_{MCB}Q_{LBS} - P_{MPR}Q_{RBS} \tag{2.8}$$

Eq. 2.8 gives the probability of unsuccessful fault clearing.

2.4 Risk in general engineering literature

The mere act of living involves risk. It is the responsibility of engineers to design. build and operate systems that benefit society without significantly increasing risk above the inherent everyday risks of life. To achieve this objective it is necessary to quantify

and weight the benefit and risk of a variety of systems. from the very simple to the very complex. this is achieved via risk analysis. There are several industries that heavily rely on risk assessment for decision making. among these are: construction. transportation. chemical. nuclear. aerospace and insurance. Among these risk analysis takes a variety of names and it has been extensively discussed in the literature. The following is a representative sample of these sources.

Terje Aven [20] presents general methods for analysis of reliability and risk. His book focuses on analysis of repairable systems. with most applications taken from offshore petroleum activities.

J.D. Andrews and T.R. Moss [21] focus on the risk and reliability assessment of process plant. It describes the main probabilistic methods employed in reliability and risk assessment. particularly fault tree analysis and failure mode and effect analysis and their derivatives.

Richard B. Jones [22] presents techniques to achieve risk reduction. "an industrial-strength version of continuous improvement". His risk-based management is based on reliability-centered maintenance (RCM). RCM's fundamental premise is to maintain system function by analyzing how a system functions and how it can functionally fail.

2.5 Summary

Our work is oriented toward power systems security and operations. This orientation allow us to represent the precontingency operating conditions deterministically. since it is precisely those conditions that an operator must know when assessing risk in real time. It also requires that we compute risk as a function of precontingency operating conditions. The vast majority of previous efforts have been concerned with planning and adequacy and most contemporary reliability assessment methods are limited to static (power flow) assessments. There is a clear need for methods and indices to evaluate system reliability

at the operations level. i.e.. to perform probabilistic security assessment. Previous work that dealt with probabilistic security or stability faced one or more of the following problems:

- They required an extensive amount of statistical data. data that was normally unavailable to practitioners. Several previously developed methods assume that a certain amount and type of statistical data was available or "could be obtained" and then proceeded to develop methods based on these presumably available data. Our method uses a minimum amount of statistical data. the frequency of faults and their type on a circuit. data known to be available to most utilities.

- They used clearing time being less than critical clearing time as stability performance measure. this measure may provide practical and valuable upper bounds on limits as well as insight into the behavior of a system. but its application to real systems is limited since clearing time is fixed by protection systems set-up. For the transient stability problem our system performance measure is a composite evaluation of stability limits for all fault types and locations calculated using time-domain simulation. For the thermal overload problem our system performance measure is whether or not the-post contingency flow on the circuit at risk of thermal overload exceeds its short-time emergency rating.

- Analytical structures to calculate probability of instability or insecurity were presented but Monte Carlo. or other numerical methods. were used to actually calculate the desired probability. We present a simple method that is tractable thus avoiding the need of calculating probabilities using computationally intensive methods.

Also. previous work on probabilistic stability assessment differs from our work in that our purpose of calculating probability of instability is to use it with the impact of

instability. i.e. to calculate risk of operating at a specific operating point. Calculating probability of instability is only one step towards the use of risk as a decision making tool. a management tool.

Calculating probability of instability is an interesting problem that once solved provides us with little information on how to evaluate the operating conditions associated with this probability. For example. knowing that the probability of instability over the next hour is 0.75 may lead to operating decisions to reduce this high probability of instability condition. but is this a sound economic decision ? Is the cost of operating at this high probability of instability condition greater than the benefit ? Probability alone can not answer this question. Accounting for impact of instability leads to the development of a concise statement of the security-economics tradeoff problem.

3 RISK OF INSECURITY

3.1 Introduction

Our goal is to determine operating limits based on the risk of insecurity at a given operating point. In this chapter we show how to quantify this risk. We characterize the operating point in terms of pre-contingency controllable parameters, the *critical parameter set*, that most influence the postcontingency system performance. In general, several parameters will influence the postcontingency system performance: thus the operating point should be characterized in terms of all these. For the transient stability problem we simplify the analysis using only one parameter in our critical parameter set, real power generation on the machines at risk of losing synchronism. Thermal overloads are characterized by pre-contingency flows on the circuits that are at risk of overloading and generation changes that affect the post-contingency flows on such circuits.

We use $R(s_t)$ to represent the risk at operating point s_t, where we use the subscript t to emphasize the time dependence of the operating point. At any given operating point s_t we may have a security violation j due to a fault on line i [1]. Total risk at a given operating point s_t is obtained summing over all defined security violations and their corresponding triggering events.

$$R(s_t) = \sum_{\forall j} \sum_{\forall i} R_{ji}(s_t) \tag{3.1}$$

[1] We assume that the elementary event that triggers a security violation is a fault on circuit i, this may be generalized to "malfunction of component i" to include other possible ways of initiating a security violation.

As mentioned in chapter one risk is the product of probability and impact. thus $R_{ji}(s_t) = P_{ji}(s_t)I_{ji}(s_t)$. We assume that the impact of a security violation is known or that a good estimate is available. The following section presents how to obtain the probabilities needed to calculate risk.

3.2 Probability of security violations

In this work we consider two security violations. transient instability and thermal overload. We use probability theory to develop two approaches for computing probability of transient instability and a simpler approach to compute probability of thermal overload [2]. We present the concept of limiting operating point functions. curves that characterize the dependency of operating limits on fault type and location. and we use these curves to compute probability of instability.

3.2.1 Assumptions, definitions and notation

We wish to determine the probability of insecurity j due to a fault on circuit i at operating point s_t over the next hour. To simplify the discussion we restrict the problem with the assumptions below: however. the theory developed in this chapter is flexible enough to allow these assumptions to be lifted if desired. In fact. we consider the effect of lifting assumptions 1 and 2. i.e. the effect of unreliability of protection equipment later in this chapter.

1. Every sustained fault on transmission circuit i will be followed by fault clearing. i.e.. line outage. This implies that we do not account for momentary faults which do not result in line clearing nor do we account for a stuck breaker condition.

[2]It is possible to define the event of interest to be "economic impact" and use the probability of this event to assess risk. since the economic impact event can not occur without occurrence of the security violation. This alternative definition of the event of interest allows risk evaluation of remedial action schemes where successful operation of the equipment results in controlled economic impact.

2. Every fault clearing is preceded by a sustained fault: therefore we do not account for breaker misoperation.

3. A fault may occur anywhere on a line with the same probability of occurrence.

Let K_j denote the event insecurity j. $P(K_j)$ denotes the probability of this event. Let F_i denote the event fault on transmission circuit i over the next hour. $P(F_i)$ denotes the probability of the event fault on transmission circuit i over the next hour.

Occurrence of F_i does not imply that insecurity j will occur. e.g., an outage on the line from bus 10 to bus 20 will cause rotor angle instability on a nearby machine A only if operating point s_t for machine A is beyond the limiting operating point for that outage. In general, the probability of insecurity j due to fault on line i at operating point s_t is the product of the probability of fault on line i at operating point s_t and the conditional probability of insecurity j given a fault occurs at operating point s_t, i.e.

$$P(K_j) = P(F_i \cap S_t)P(K_j/F_i \cap S_t) \tag{3.2}$$

S_t represents the event "operating point s_t". The subscript t refers to a given time, the time at which we are evaluating system security. In this work we consider two security violations: transient instability and thermal overload. We use what we call the Law of Total Probability approach and the Cartesian product approach to calculate the conditional probability of instability given a fault occurs. We assume that instability j may only occur due to an outage of a transmission circuit. We use an indicator function to calculate the conditional probability of thermal overload given a fault occurs. The following sections explain these methods.

3.2.2 Law of Total Probability approach

Our goal is to compute risk corresponding to a specific operating point s_t: therefore $S_t = s_t$ and $P(S_t = s_t) = 1$. Assume that having a fault on circuit i is independent of

the system operating point. Thus.

$$P(F_i \cap S_t) = P(F_i)P(S_t) = P(F_i) \tag{3.3}$$

We define $3o$. $2o$. and $1o$ to ground faults to be the set of all possible faults.[3] and we assume that only one of these faults occur at a time. Let events a_1. a_2 and a_3 represent single phase to ground fault. two phase to ground fault and three phase to ground fault. respectively. This constitutes a collection of mutually exclusive and exhaustive events. Therefore. starting with the identity $F_i = F_i \cap F_i$.

$$\begin{aligned} F_i &= F_i \cap (a_3 \cup a_2 \cup a_1) \\ P(F_i) &= P(F_i \cap a_3) + P(F_i \cap a_2) + P(F_i \cap a_1) \end{aligned} \tag{3.4}$$

From the above and the definition of conditional probability [23. pp. 18] we can derive the probability of instability j due to a fault on circuit i at operating point s_t.

$$\begin{aligned} P(K_j/F_i) &= \frac{P(K_j \cap F_i)}{P(F_i)} = \frac{\sum_{n=1}^{3} P(K_j \cap F_i \cap a_n)}{P(F_i)} \\ &= \frac{\sum_{n=1}^{3} P(F_i \cap a_n)P(K_j/F_i \cap a_n)}{P(F_i)} \\ &= \sum_{n=1}^{3} P(a_n/F_i)P(K_j/F_i \cap a_n) \end{aligned} \tag{3.5}$$

Let $\mathcal{L}$ be a continuous random variable. denoting fault location on a line and let L be the line length. The uniform probability density function (uniform pdf) indicates that all locations on line i have equal probability of sustaining a fault given a fault occurs.

[3]The severity of line to line faults on transient instability typically lies between $2o$ to ground faults and $1o$ to ground faults. If the probability of occurrence of line to line faults is comparable to the probability of $3o$. $2o$. and $1o$ to ground faults then line to line faults must be included in the set of all possible faults. This can be done with no loss of generality.

The pdf is given by

$$\begin{aligned} f(l:0.L) &= \frac{1}{L} \quad . \; 0 < l < L \\ &= 0 \quad . \; otherwise \end{aligned} \tag{3.6}$$

If we let $l = l_{jis_t.a_n}$. where $l_{jis_t.a_n}$ is the length of circuit i for which an *no* fault results in instability j at operating point s_t then

$$P(K_j/F_i \cap a_n) = \int_{l_{jis_t.a_n}} \frac{1}{L_i} dx = \frac{l_{jis_t.a_n}}{L_i} \tag{3.7}$$

gives the probability of instability j given an *no* fault occurs on circuit i. The integration path is taken over the portion of circuit i length for which an *no* fault results in instability j at operating point s_t. If this portion of circuit i consists of two or more non-consecutive segments. then Eq. 3.7 must be interpreted as a sum of integrals. one for each segment.

The probability of the event occurrence of a *no* fault given a fault occurs on line i at operating point s_t over the next hour. $P(a_n/F_i)$ is obtained from historical data.

3.2.2.1 Length of circuit i for which an *no* fault results in instability, $l_{jis_t.a_n}$

The parameter $l_{jis_t.a_n}$ indicates the length of circuit i for which an *no* fault results in unstable response.

If the generation level is at or below its deterministic limit (e.g.. the maximum generation level for which the generator response is stable for a 3*o* at the machine terminals). then $l_{jis_t.a_3} = 0$. implying that the generator response is stable for a 3*o* fault located anywhere on the line. In this case. we would expect $l_{jis_t.a_2} = l_{jis_t.a_1} = 0$. also. At some generation level above the deterministic limit. however. it would be true that $l_{jis_t.a_3} \geq x$. implying that the generator response is unstable for a 3*o* fault located within a distance x from the generator terminals. At the generation level where $l_{jis_t.a_3} = x$.

$0 > l_{jist.a_2} \geq x$ and $0 > l_{jist.a_1} \geq x$ depending on excitation system type and x, i.e., single phase to ground and double phase to ground faults may or may not be stable for faults closer to the generator terminals than x depending on the excitation system used on the machine at risk of losing synchronism and fault location.

3.2.3 Cartesian product approach

One difference in the Cartesian approach relative to the Law of Total Probability approach is that we discretize the inherently continuous random variable fault location. This step, and the notion of independence, allow us to use a Cartesian product to easily combine the pdf for fault type and pdf for fault location into one joint pdf. The joint pdf for fault type and location is used to assess the conditional probability of instability j given a fault on line i occurs. We use the limiting operating point functions to do this assessment.

3.2.3.1 Limiting operating point functions

It is possible to obtain data characterizing the dependency of operating limit on fault type and location by using time domain simulation or other techniques to find the limiting values of the critical parameter for various fault locations on the line. We call the resulting functions the limiting operating point functions.

For a transient instability problem the limiting generation level for a $3o$ fault would be likely to increase as the fault is moved away from the bus closest to the machine at risk of losing synchronism, or as the fault is changed from a $3o$ fault to a $2o$ or a $1o$ fault, because these changes cause the impedance seen by the fault to increase. Limiting operating functions showing the previously discussed behavior are illustrated in Figure 3.1. In Chapter 4 we show how excitation system types, network topology and sequence impedances can influence the limiting operating point functions.

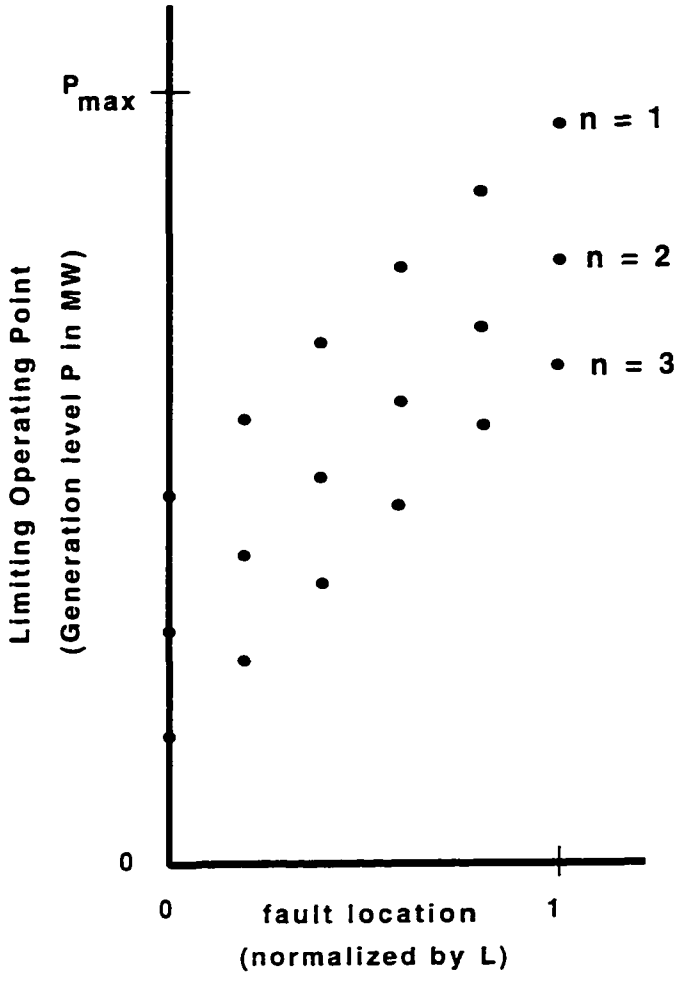

Figure 3.1 Limiting operating point functions

3.2.3.2 Relation between the length of circuit i for which an *no* fault results in instability, $l_{jis_t.a_n}$, and limiting operating point functions

Given any [fault type. fault location] pair on circuit i we can always obtain a limiting value for the critical parameter. generation level in this case. but there is no guarantee that there is a [fault type. fault location] pair for which a given generation level is a limit. Therefore. it is necessary to choose the [fault type. fault location pair] and use time domain simulation. or other techniques. to obtain the corresponding unique value of the critical parameter. This is how we generate the limiting operating point functions.

If there are operating points for which a fault located at a point on the line could result in more severe stability performance than that of a fault closer to the generator terminals. then the limiting operating point functions are not monotonically increasing. In this case there are some operating points for which the integration path in Eq. 3.7 consists of more than one consecutive segment; we use the following procedure to obtain $l_{jis_t.a_n}$ from the limiting operating point functions.

1. Draw a horizontal line corresponding to the current operating point s_t on the limiting operating point vs. fault location plane.

2. Identify the segments of circuit i associated with values of the limiting operating points below the horizontal line drawn in step 1.

3. The sum of the segment lengths identified in step 2 is equal to $l_{jis_t.a_n}$.

This procedure also applies if stability performance always improves as the fault moves further along the line from the generator terminals so that the limiting operating point functions are monotonically increasing. In this case the integration path in Eq. 3.7 consists of a single segment.

3.2.3.3 Conditional probability of instability

We use the limiting operating point functions to calculate $P(K_j)$, the probability of instability j. If a [fault type, fault location] pair occurs which requires an operating limit for stability less than s_t the system will be unstable. In other words, $P(K_j)$ is the probability of occurrence of faults on circuit i over the next hour for which the current operating point s_t is beyond the operating limit for stability required by these faults. The conditional probability of the event instability j given a fault on line i occurs is

$$P(K_j/F_i) = P(P_{lim_{j,i}}(n,l) \leq s_t). \tag{3.8}$$

Equation 3.8 indicates that $P_{lim_{j,i}}$, the stability limit for certain [fault type, fault location] pair on a given circuit i over the next hour, is a random variable. $P_{lim_{j,i}}$ depends on l and n, the discretized random variables corresponding to fault location and fault type, respectively[4].

3.2.3.4 Probability density function for fault type

Let $\mathcal{A}$ be the fault type sample space, i.e., the set of all possible fault types. $\mathcal{A}$ is a countable set with elementary events a_1, a_2 and a_3 (single phase to ground fault, two phase to ground fault and three phase to ground fault, respectively). Let N be the discrete random variable for fault type and let n be the integer values it may take. We denote the pdf for fault type as $f_n(n)$ and show its graph in Figure 3.2.

3.2.3.5 Probability density function for fault location

Let $\mathcal{B}$ be the fault location sample space, i.e., the set of all possible fault locations. $\mathcal{B}$ is a countable set with elementary events b_0, b_1, ...

[4]The random variable n is inherently discrete. The random variable l is inherently continuous but we discretized to obtain the joint pdf.

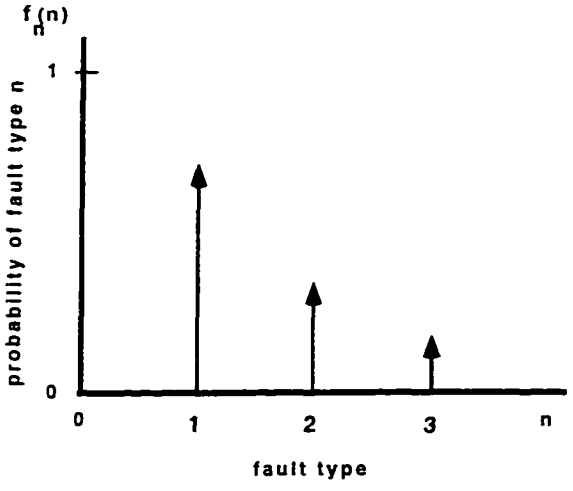

Figure 3.2 Probability density function for fault type $f_n(n)$

We assume that a fault may occur anywhere on the line with the same probability. therefore. we use a discrete uniform distribution function to model fault location.

Discrete uniform distribution: *A discrete random variable X has the discrete uniform distribution on the integers 0. 1. 2. .... M if it has a pdf of the form*

$$f(x) = \frac{1}{M+1} \tag{3.9}$$

for $x = 0. 1. 2. .... M.$

Let $\mathcal{L}$ be the discrete random variable for fault location and let l be the integer values it may take. We denote the pdf for fault location as $f_l(l)$ and show its graph in Figure 3.3. Each interval in Figure 3.3 has length L/M.

3.2.3.6 Joint PDF and Cartesian products

We assume the events fault type and fault location to be independent events. Physically we mean that any type of fault may occur anywhere on a transmission line. Probabilistically we mean that $\mathcal{L} = l$ and $\mathcal{N} = n$ are independent [24. pp. 31]. i.e..

$$P(\mathcal{L} = l. \mathcal{N} = n) = P(\mathcal{L} = l)P(\mathcal{N} = n). \tag{3.10}$$

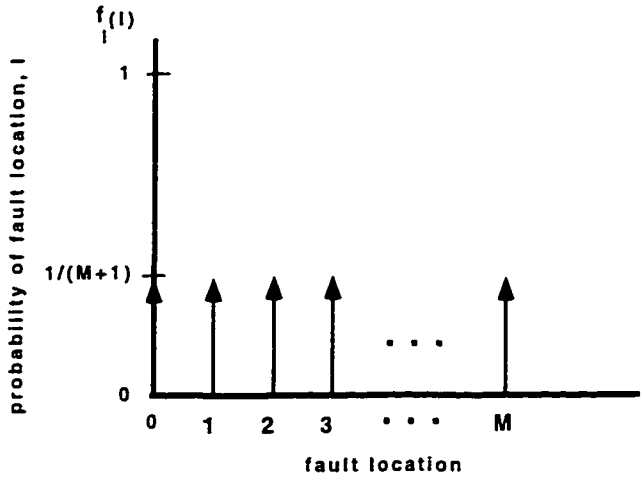

Figure 3.3 Probability density function for fault location $f_l(l)$

In this definition, the events a_n and b_l are subsets of the same probability space, $\mathcal{S}$. We defined $\mathcal{A}$ as the fault type sample space and $\mathcal{B}$ as the fault location sample space. To satisfy the probability definition of independence we construct a space $\mathcal{S}$ having as subsets the sets $\mathcal{A}$ and $\mathcal{B}$ using the Cartesian product of these sets.

Cartesian products [24, pp. 38]: *Given two sets $\mathcal{A}$ and $\mathcal{B}$ with elements a_i and b_i respectively, we form all ordered pairs $[a_i, b_i]$ where a_i is any element of $\mathcal{A}$, and b_i is any element of $\mathcal{B}$. The Cartesian product of the sets $\mathcal{A}$ and $\mathcal{B}$ is a set $\mathcal{S}$ whose elements are all such pairs.*

The space $\mathcal{S}$ is shown in Figure 3.4-B. If the events fault type and fault location are independent events the joint pdf of these events is the product of their individual pdf: i.e. $f_{n,l}(n,l) = f_n(n)f_l(l)$.

Figure 3.4 shows the relation between the space $\mathcal{S}$ and the limiting operating point functions. The points on the limiting operating point functions which are less than s_t, the white points in Figure 3.4-A, are those points associated with [fault type, fault location] pairs which cause instability. Identification of these pairs results in identification of the region D on the probability space $\mathcal{S}$, the white points in Figure 3.4-B. This region D includes all fault type and fault location combinations which make $P_{lim_j} \leq s_t$, implying

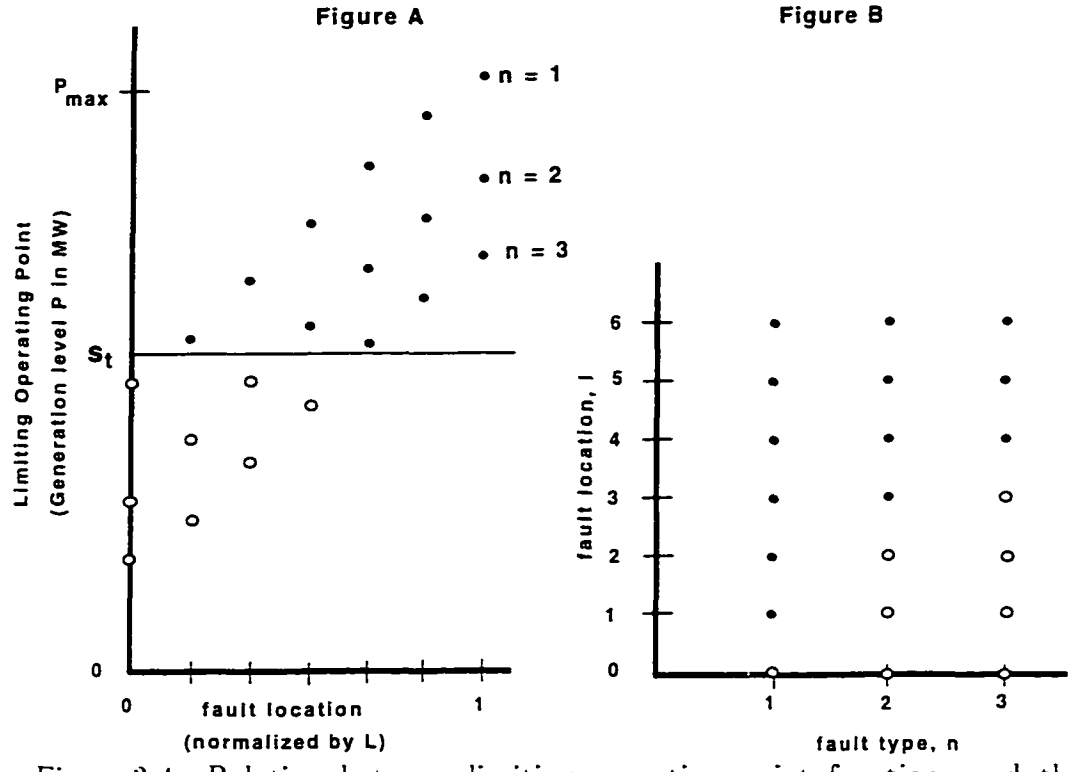

Figure 3.4 Relation between limiting operating point functions and the space $\mathcal{S}$

that operating point s_t would result in instability if any of these [fault type, fault location] pairs occur.

This relation suggests the following procedure to calculate $P(K_j/F_i)$ using the limiting operating point functions:

1. Draw a horizontal line corresponding to the current operating point s_t on the limiting operating point vs. fault location plane.

2. Identify the [fault type, fault location] pairs associated with values of the limiting operating points below the horizontal line drawn in step 1.

3. Calculate and add the probability of occurrence of these pairs using the joint pdf for fault type and fault location. This is numerically equal to $P(K_j/F_i)$.

The probability of rotor angle instability, $P(K_j)$, due to a fault on line i at s_t over the next hour is

$$P(K_j) = P(F_i)P(P_{lim_j}(n,l) \leq s_t) \tag{3.11}$$

3.2.4 Probability of occurrence of a fault on line i

Transient instability or thermal overload normally occur as the result of an initiating event that induces a disturbance in the system. We assume this initiating event to be a fault on line i and use a Poisson process to model its probability of occurrence[5]. In this section we describe the Homogeneous, Non-Homogeneous and Compound Poisson processes.

3.2.4.1 Homogeneous Poisson process

We assume that we have historical data which provides the number of outages per unit of time and, following traditional security assessment practices, assume noncredible events to have probability equal to zero. We relate the rate of occurrence of event i to the probability of occurrence of event i using a homogeneous Poisson process (HPP) [23, pp. 105]. Let $X(t)$ [6] denote the number of events that occur in a given interval $[0,t]$, and suppose that the following additional assumptions hold.

- *Stationary increments:* The probability that an event will occur in a given short interval $[t, t+\Delta t]$ is approximately proportional to the length of the interval, Δt, and

[5]Other models, such as Markov processes, may be suitable also. For instance, limits, characterized by operating parameters, are associated with a given topological state of the system: when the state changes, new limits are used [25]. Assuming that the topological state of the system is known with probability equal to one and assuming noncredible events have probability zero the probability of state transition from one state to the next is equal to the probability of occurrence of the event.

[6]$X(t)$ is, in general, a counting process since $X(t)$ represents the total number of "events" that have occurred up to time t [26, pp. 208].

does not depend on the position of the interval. This means that the probability of occurrence of an event in an interval increases as the interval increases.

- *Independent increments:* The occurrences of events in non-overlapping intervals[7] are independent.

- *Negligible multiple events:* The probability of occurrence of two or more independent events in a short interval $[t, t + \Delta t]$ is negligible.

The probability of occurrence of r events in a given interval $[t, t + \Delta t]$ is.

$$P(X(t) = r) = \epsilon^{-\lambda t}\frac{(\lambda t)^r}{r!}, r = 0, 1, \ldots . \lambda > 0 \tag{3.12}$$

Using Eq. 3.12 and recalling that F_i is the event one line outage on transmission circuit i over the next hour[8] we obtain the probability of one outage on transmission circuit i over the next hour (r=1,t=1).

$$P(F_i) = \lambda_i \epsilon^{-\lambda_i}, \lambda_i > 0 \tag{3.13}$$

The proportionality constant λ_i reflects the rate of occurrence or intensity of the Poisson process, and it may be estimated using the sample mean [23, pp. 571] of the observed number of outages over the number of observation intervals.

3.2.4.2 Non-homogeneous Poisson process

A non-homogeneous, also called non-stationary, Poisson process is obtained by allowing the arrival rate, the rate of occurrence, at time t to be a function of time [26, pp. 237]. If we let $m(t) = \int_0^t \lambda(s)\,ds$, then it can be shown that

[7] Non-overlapping intervals are intervals that do not share any points, in this case time points.

[8] We compute risk off-line and compare the relative risk of different candidate limits. We may use any time interval to calculate probabilities as long as we are *consistent* at the moment of comparing risks. We choose a time period of one hour to be consistent with the fact that the operating conditions for which we are calculating risk are not likely to exist past one hour. If we were to compare risk vs. benefits we will also need to use consistent time periods when calculating risks and benefits.

$$P(X(t+s)-X(t)=r)=\epsilon^{-(m(t+s)-m(t))}\frac{(m(t+s)-m(t))^r}{r!}.r\geq 0 \qquad (3.14)$$

In other words. $X(t+s)-X(t)$ is Poisson distributed with mean $m(t+s)-m(t)$. Thus $X(t)$ is Poisson distributed with mean $m(t)$. and for this reason $m(t)$ is called the *mean value function* of the process. The importance of the non-homogeneous Poisson process resides in the fact that we no longer require the condition of stationary increments. Thus we now allow for the possibility that events may be more likely to occur during certain time periods. We may use this model to conveniently account for the non-uniformity of outage rates. i.e.. let $\lambda(t)$ vary with season and weather. For example. an area that expects to be hit by a hurricane may choose to use an intensity function $\lambda(t)$ given by

$$\begin{aligned}\lambda(t) &= a+bt\ .\ 0\geq t\geq t_1\\ &= c\quad\ .\ t_1\geq t\geq t_2\\ &= c-bt\ .\ t_2\geq t\geq t_3\end{aligned} \qquad (3.15)$$

where the parameters a.b.c and times depend on hurricane trajectory and speed.

3.2.4.3 Compound Poisson process

A stochastic process $Z(t).t\geq 0$ is said to be a *compound Poisson process* if it can be represented as

$$Z(t)=\sum_{i=1}^{X(t)}Y_i.t\geq 0 \qquad (3.16)$$

where $X(t).t\geq 0$ is a Poisson process. and $Y_n.n\geq 0$ is a family of independent and identically distributed random variables which are also independent of $X(t).t\geq 0$.

Suppose several lines emanate from a generating station and a model for the total number of line outages over time is required. If we assume that data is available on the number of outages on line i and a Poisson process $X(t)$ may be used to model the event line outage then the total number of line outages for all the lines is given by $Z(t)$. If we let $X(t)$ be a non-homogeneous Poisson process then $Z(t)$ becomes a non-homogeneous compound Poisson process.

3.2.5 An indicator function to calculate probability of thermal overload

The conditional probability of thermal overload depends on pre-contingency flows on the circuits that are at risk of overloading, the monitored circuits, and generation changes that affect the post-contingency flows on such circuits, but it does not depend on the type of fault or fault location. We will have thermal overload with probability equal to unity if the post-contingency flow on the monitored line, $\hat{f}$, is above its short term emergency (STE) rating.

$$\begin{aligned} P(K_j/F_i) &= 0 \ . \ \hat{f} \leq STE \\ &= 1 \ . \ \hat{f} > STE \end{aligned} \tag{3.17}$$

It is interesting to note that the STE can be expressed as a probabilistic function of weather statistics, but doing so is outside the scope of this dissertation.

3.3 Impact of insecurity

Significant interest exists in assessing the impact of disturbances resulting in violation of reliability criteria in bulk transmission systems. Quantification of the cost of system disturbances and using these impacts in computing risks associated with an operation point is an important aspect of the risk-based security assessment method since it links the operating limits with the costs of the disturbances that affect the operating limit.

3.3.1 Quantification of impact of instability

The impact of security violation j due to event i at operating point s_t can be expressed as

$$I_{ji}(s_t) = IS_{ji}(s_t) + IT_{ji}(s_t) + ID_{ji}(s_t)$$

where $IS_{ji}(s_t)$ is the impact on the suppliers (mainly replacement energy costs and cost of resynchronization). $IT_{ji}(s_t)$ is the impact on the owner of the transmission facilities affected by the security violation (costs to repair equipment and reenergize facilities). and $ID_{ji}(s_t)$ is the impact on the demand served by the affected suppliers (replacement energy costs and/or cost of service interruption). This formulation is attractive because it facilitates identification of *who* is taking risk and how much when "no-risk" operating limits are exceeded. This identification will become more critical as the electric power industry undergoes organizational separation based on function[9]. The ultimate goal is to develop methods of expressing these impact components in dollars.

The costs associated with the impact on supply and transmission can be quantified. as associated techniques and data are usually available. Quantitative assessment of other costs. however. such as those associated with the impact on the demand or those associated with regulatory actions precipitated by nuclear generation trip or load interruption can be difficult to do with precision because these costs are dispersed and extremely variable. and in some cases. historical data is either not available or hard to gather [27. 28]. A simple. subjective method of evaluating these impacts is to assign to each consequence a discrete level (like 1.2.3) corresponding to the severity [29]. For example. a logarithmic scale could be developed where one could assign to each demand

[9]The 1978 Public Utilities Regulatory Policy Act (PURPA) provided for non-utility generation. and the 1992 National Energy Policy Act required that utilities provide transmission service at a fair price to any generation owner wishing to sell on the wholesale energy market. Currently. many state legislatures are considering extending this requirement to include retail energy sales as well. Thus. traditional rate-base regulation of the utilities is giving way to a competitive. multi-participant bulk power market. and organizational separation seems likely in order to ensure no competitive participant can utilize the market power inherent to operation of the transmission system.

impact a discrete impact level α between 0 and 20, such that an increase in α of 1 indicates an increase in dollar impact by a factor of 10. The dollar impact is then 10^{α}. This is attractive because although it can be difficult to subjectively estimate impact in terms of absolute dollar values, it is usually not difficult to estimate relative differences between various impacts in terms of orders of magnitude. For instance, in [25] impact factors are used to account for socio/political costs, costs that are included as a percentage increase over the energy replacement costs. The socio/political weighting factors are based on subjective assessment and are approximate, but the point is that they represent real impacts having effects that must be included in risk calculation.

To better quantify economic impact more data is required, particularly for security violations such as oscillatory instability, voltage instability and thermal overloads. A survey has been recently developed [30] to extract information from a large number of industry experts regarding the economic impact of various system instabilities. This survey will quantify the economic cost impact of bulk transmission disturbances to the various owners of power system facilities.

3.3.1.1 Impact approximations used in this dissertation

In Chapter 5 we use a modified version of the IEEE Reliability Test System to illustrate risk-based electric power system security assessment. In this example we consider transient instability and thermal overload to be the only security violations of interest. We account for the impact of these security violations using estimates of the economic consequences of suffering such violations.

In the event of transient instability it is estimated that a generation plant consisting of three 350 MW units would be out of service for 10 hours. We assume that energy can be replaced at a cost of 37.5 \$/MWh[10], startup fixed costs are estimated at \$45,000

[10]The average sale for resale revenue per kWh in 1994 was 3.7 cents according to "The Electric Power Annual 1994 Volume II Operational and Financial Data" a report from the Energy Information Administration.

for all three machines and maintenance and repairs costs are estimated at $36.225 for all three machines[11]. These costs are direct costs to the energy producer. we assume that no load is shed due to this outage. thus there are no direct or indirect costs to the customer.

The impact of thermal overload is divided into maximum and partial impact. Maximum impact refers to the total cost of reconductoring the line. this is needed when the flow on the line exceeds short-time emergency rating. Maximum impact is estimated at $108.000 per mile[12]. Appendix 2 includes material and construction costs data from ComEd and PG&E. Partial impact is the impact of thermal overload for flows above continuous rating and below short-time emergency rating. Partial impact is assumed. for simplicity. to follow a linear curve[13] as shown in Figure 3.5. a maximum partial impact of one third the total cost of reconductoring the line is assumed to generate the impact vs. limiting parameter curve. This figure is arbitrary. the point being that there is a deterioration on the line that must be accounted for when flows are above continuous rating and below short-time emergency rating.

3.4 Risk expressions

This section summarizes how we obtain expressions that allow quantification of the risk of operating at a given operating point as a function of those pre-contingency parameters (the *critical parameter set*) that most influence the postcontingency system performance. We present risk expressions that consider (1) fully reliable conventional protection systems and (2) unreliability of conventional protection systems.

[11]Maintenance costs are estimated at 3.45 Mills/kWh according to data from "Energy Information Administration/Historical Plant Cost and Annual Production Expenses for Selected Electric Plants 1987". Startup costs are estimates from actual data confidentially supplied by a utility.

[12]This estimate includes conductor and tower work only. The estimate is guided by a 1992 Commonwealth Edison Company. Chicago IL. reconductoring project.

[13]This implies a linear deterioration of the line as the MVA flow increases.

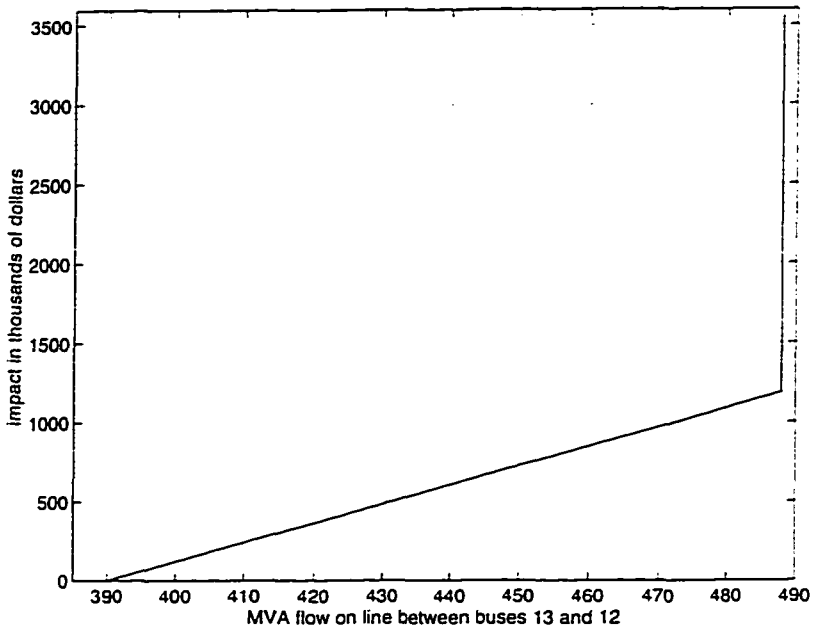

Figure 3.5 Thermal overload impact as a function of MVA flow for the line between Buses 13 and 12, modified RTS-96

3.4.1 Risk assuming fully reliable protection system

If we assume that a fault on circuit i is always cleared by the main protection system the risk of operating at operating point s_t is:

$$R(s_t) = \sum_{\forall j} \sum_{\forall i} P(F_i) P(S_t = s_t) P(K_j / F_i \cap S_t = s_t) I(K_j / F_i \cap S_t = s_t) \qquad (3.18)$$

In Eq. 3.18 $S_t = s_t$ because the event operating point is not random, it is known. Our expression calculates risk of a given, deterministic, operating point. If we were calculating risk for a random operating point, as we will do in planning, then the left hand side of Eq. 3.18 will be $R(S_t)$: risk will be a function of the random variable S_t instead of s_t.

3.4.2 Effect of conventional system protection reliability on risk

Consideration of the reliability of conventional system protection requires identification and assessment of the different impacts that an elementary event, a fault on circuit i in this case, may have. We desire a risk expression that integrates reliability of system protection with risk-based security assessment. We use the probability of satisfactory or unsatisfactory performance of conventional system protection and consider three conditions following a fault on line i with different impacts:

1. fault occurs on circuit i, and it is cleared by the main protection mechanism, i.e., $F_i \cap M \cap S_t$
2. fault occurs on circuit i, the main protection mechanism fails to clear the fault (this is an active failure), and the fault is cleared by the backup protection mechanism $F_i \cap \bar{M} \cap B \cap S_t$
3. no fault occurs, circuit i is lost due to undesired operation of the protection system (this is a passive failure) $\bar{F}_i \cap M_0 \cap S_t$

where M denotes main protection mechanism works, $\bar{M}$ denotes main protection mechanism fails due to active failure, M_0 denotes main protection mechanism fails due to passive failure, B denotes backup protection works, $\bar{F}_i$ denotes undesired operation of the protection system and S_t denotes system is operating at operating point s_t. Then the risk at operating point s_t is given by:

$$\begin{aligned} R(s_t) &= \sum_{\forall j}\sum_{\forall i}[P(F_i)P(M)P(S_t)P(K_j/F_i \cap M \cap S_t)I(K_j/F_i \cap M \cap S_t) \\ &+ P(F_i)P(\bar{M})P(B)P(S_t)P(K_j/F_i \cap \bar{M} \cap B \cap S_t)I(K_j/F_i \cap \bar{M} \cap B \cap S_t) \\ &+ P(\bar{F}_i)P(M_0)P(S_t)P(K_j/\bar{F}_i \cap M \cap S_t)I(K_j/\bar{F}_i \cap M_0 \cap S_t)] \end{aligned} \tag{3.19}$$

In all cases the conditional probabilities of insecurity are obtained using the set of limiting operating point functions that correspond to the conditions following the fault

on line i.

3.5 Summary

In this chapter we provide a foundation to calculate probability of insecurity from which the risk-based security assessment approach for determining operating limits may be extended.

Two approaches have been presented for computing probability of instability: one is based on Law of Total Probability and the other on Cartesian products. Both approaches use the same basic data and result in the same probability values: however, the Law of Total Probability approach does not require independence between the fault type and fault location events.

We use an indicator function to obtain the conditional probability of insecurity given a fault occurs for thermal overloads.

Finally, we present expressions to calculate the risk associated with a given operating point s_t considering fully reliable conventional protection systems and unreliable conventional protection systems providing a unified framework for identifying operating points that equitably balance risk with operating costs.

4 LIMITING OPERATING POINT FUNCTIONS

4.1 Introduction

We show that the limiting operating point functions introduced in Chapter 3 cannot be expressed in closed form. We attempted to express the limiting parameter, generation in this case, as a function of fault type and location and tried two different approaches, using an expression from the transient energy function (TEF) and a simple one-machine to infinite bus using the equal area criterion. Because TEF requires angles and speeds at fault clearing the approach proved infeasible since these angles and speeds may only be obtained via numerical integration and are not available in closed form. The one-machine to infinite bus using the equal area criterion results in an expression that requires an iterative solution and it does not serve the need of identifying basic factors which influence the limiting operating point functions.

We used time domain simulation to study variation of limiting operating point functions with fault location and fault type on a simple test system, a 500 kV system local to the Navajo Power Plant in Arizona. We show how excitation system types, network topology and sequence impedances can influence the limiting operating point functions.

4.2 Investigation of analytical expressions for limiting operating point functions

Our goal in developing a closed form expression for these functions is not to use it in calculation, since considerable modeling simplification is necessary, but to illuminate the basic properties of the limiting operating point functions.

4.2.1 Analytical expression using Transient Energy Function (TEF)

The limiting operating point curves (lopc) are graphs of limiting parameters, e.g., generation level at a specific machine or machines or real power flow over a set of lines, vs. fault location. The limiting parameter is a pre-disturbance observable parameter. Each point in the lopc is the maximum level that the parameter may reach for stability in the event of having a specific type of fault at a given location. Conceptually each point in the lopc corresponds to a disturbance scenario with a normalized energy margin of zero, $\Delta V_n = 0$ [31, pp. 86].

$$\begin{aligned}\Delta V_n = 0 = \; & -\frac{1}{2}M_{eq}\tilde{\omega}_{eq}^{cl\,2} - \sum_{i=1}^{n} P_i(\theta_i^u - \theta_i^{cl}) \\ & - \sum_{i=1}^{n-1}\sum_{j=i+1}^{n}\left[C_{ij}(cos\theta_{ij}^u - cos\theta_{ij}^{cl}) - D_{ij}\frac{\theta_i^u - \theta_i^{cl} + \theta_j^u - \theta_j^{cl}}{(\theta_{ij}^u - \theta_{ij}^{cl})}(sin\theta_{ij}^u - sin\theta_{ij}^{cl})\right]\end{aligned} \tag{4.1}$$

where $(\theta^{cl}, \tilde{\omega}^{cl})$ are the conditions at the end of the disturbance and $(\theta^u, \mathbf{0})$ represents the controlling unstable equilibrium point. $\Delta V_n = 0$ is in terms of post-disturbance equilibrium parameters, i.e., $\Delta V_n(\theta^{cl}, \tilde{\omega}^{cl}, \theta^u)$. Of these, θ^{cl} and $\tilde{\omega}^{cl}$ are functions of fault attributes and pre-disturbance parameters, i.e., $\theta^{cl}(n, l, P_{lim})$, $\tilde{\omega}^{cl}(n, l, P_{lim})$, where n, l, and P_{lim} denote fault type, fault location and limiting parameter (e.g. generation level), respectively. The connection between these post-disturbance parameters $\theta^{cl}, \tilde{\omega}^{cl}$ and the pre-disturbance operating parameters (n, l, P_{lim}) is obtained via numerical integration of the system equations, i.e., time domain simulation. There is no simple analytical, closed-

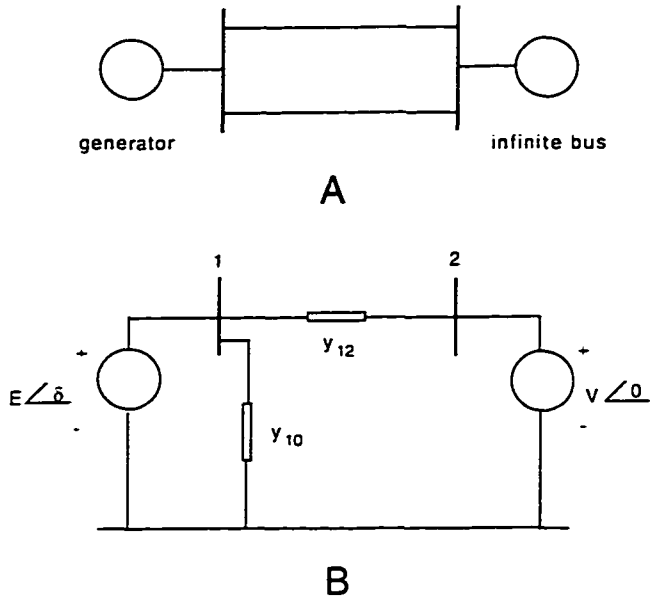

Figure 4.1 One machine connected to an infinite bus through two transmission lines (A) one-line diagram. (B) equivalent circuit.

form connection between pre-disturbance conditions and post-disturbance parameters in TEF or any other direct stability assessment method.

We conclude that development of an analytical expression using TEF cannot be done without obtaining a relationship between pre-disturbance conditions and end-of-disturbance conditions.

4.2.2 Analytical expression using equal area criterion

We explored the possibility of developing an analytical expression for the lopf using a simple one-machine-infinite-bus system. Here we attempted to use the generator classical model and equal area criterion [32. pp.26-33] to link fault reactance (due to an specific fault type. fault location pair) and maximum pre-disturbance generation level (the limiting parameter of the lopc in this case).

Figure 4.1 shows a system where one machine is connected to an infinite bus through two transmission lines. From network theory we can show that the power at node 1 is

given by

$$P_1 = E^2 Y_{11} cos(\theta_{11}) + EVY_{12} sin(\delta - \theta_{12} + \frac{\pi}{2}) \tag{4.2}$$

where all symbols are defined as in [32. pp. 27]. The swing equation for the generator is

$$\frac{2H}{\omega_R}\frac{d^2\delta}{dt^2} = P_m - P_1 \tag{4.3}$$

where P_m is mechanical power input to the generator. Any fault anywhere on this circuit will be represented in this mathematical model via $Y_{12}\angle\theta_{12}$. the negative of the transfer admittance. $-y_{12}$. between nodes 1 and 2 resulting from the fault ($Y_{11}\angle\theta_{11}$ also changes). Since fault clearing time is fixed P_1 will be a limiting generation. $P_1 = P_{lim} = P_m$. if $\delta(t = t_{clearing}) = \delta_{critical}$. $\delta(t = t_{clearing})$ is obtained integrating the swing equation from t=0 (when the fault is applied) to $t = t_{clearing} = t_c$.

$$\delta(t_c) = \frac{\omega_R}{2H} P_m t_c^2 - \frac{\omega_R}{2H}\int_0^{t_c}\int_0^{t_c} E^2 Y_{11f} cos(\theta_{11f}) + EVY_{12f} sin(\delta(t) - \theta_{12f} + \frac{\pi}{2}) dt dt \tag{4.4}$$

and $\delta_{critical}$ is given by the equal area criterion [32. pp. 31].

$$\delta_{critical} = \arccos(\frac{1}{r_2 - r_1}[(\frac{P_m}{P_M})(\delta_m - \delta_0) + r_2 \cos\delta_m - r_1 \cos\delta_0]) \tag{4.5}$$

where

- P_M = peak of the prefault power-angle curve ($P_M = EVY_{12}$)
- r_1 = ratio of the peak of the power-angle curve of the faulted network to P_M
- r_2 = ratio of the peak of the power-angle curve of the network with the fault cleared to P_M
- $\delta_0 = \arcsin(\frac{P_m}{P_M}) = \arcsin(\frac{P_{lim}}{P_M})$
- $\delta_m = \arcsin(\frac{P_m}{r_2 P_M}) = \arcsin(\frac{P_{lim}}{r_2 P_M})$.

The relation between fault type and location (given by $Y_{11f}\angle\theta_{11f}$ and $Y_{12f}\angle\theta_{12f}$) and predisturbance limit (generation level $P_1 = P_m = P_{lim}$) is.

$$\arccos\left(\frac{1}{r_2 - r_1(\cdot)}\left[\left(\frac{P_{lim}}{P_M}\right)(\delta_m(\cdot) - \delta_0(\cdot)) + r_2\cos\delta_m(\cdot) - r_1(\cdot)\cos\delta_0(\cdot)\right]\right) \tag{4.6}$$
$$= \frac{\omega_R}{2H}P_{lim}t_c^2 - \frac{\omega_R}{2H}\int_0^{t_c}\int_0^{t_c} E^2 Y_{11}cos(\theta_{11}) + EVY_{12f}sin(\delta(t) - \theta_{12f} + \frac{\pi}{2})dtdt$$

where the notation $\delta_m(\cdot)$, $\delta_0(\cdot)$, etc is used to emphasize the dependence of these parameters on P_{lim}. The only practical way of solving Eq. 4.6 to find P_{lim} in terms of $Y_{11f}\angle\theta_{11f}$ and $Y_{12f}\angle\theta_{12f}$ is numerically. This defeats the purpose of having a closed form relation between fault type and location and limiting parameter.

4.3 Time domain simulation study of the limiting operating point functions

The limiting operating point functions characterize the dependency of operating limit on fault type and location by using time domain simulation to find the limiting values of the critical parameter for various fault locations on the line.

We have developed probability of instability in terms of the limiting operating point functions. These functions are critical to the assessment procedure because embedded within them is information on operating point, probability, and stability performance. Our investigation indicates that these functions are influenced by

- sequence impedances seen from the fault point for unbalanced faults
- excitation system type for the "at risk" generator, and
- network topology.

4.4 Study system and analysis of results

Simulation studies were performed on a simple test system, a 500 kV system local to the Navajo Power Plant in Arizona, to illustrate how excitation system types, network topology and sequence impedances can influence the limiting operating point functions. A one line diagram of the study system and the system data are given in Appendix A. The system configuration represents the Navajo-McCullough 500 kV line out of service due to either forced or scheduled outage. It is assumed that there is no series compensation in the Navajo-Westwing, Navajo-Moenkopi, Moenkopi-Westwing, and Moenkopi-Eldorado 500 kV lines. Generators in the study area are represented using a two axis model with exciter, power system stabilizer, and turbine-governor representation. Real power loads are represented as constant current, and reactive power loads are represented as constant impedance. This example does not include the effects of remedial actions that would normally be used under these conditions.

Eleven graphs are presented in Appendix A. Figures A.2 thru A.7 present limiting operating point functions (lopf) for the following exciter types: DC, AC and Static. These graphs are grouped by fault type and exciter type. The parameters for the excitation systems used are included in Appendix A.

Figures A.8 thru A.10 present how network topology affect the lopf. Here the impedance magnitude of the Navajo-Moenkopi line is changed by $\pm 20\%$ to model the effect of electrical distance on the "returning path" between fault location and machine at risk of losing synchronism. We use an AC excitation system for this portion of the study.

Figures A.11 and A.12 present how variation of sequence impedances seen from the fault point affect the lopf. Here we changed the zero and negative sequence reactances at all fault points by $\pm 20\%$. We use an AC excitation system for this portion of the study. The values used for the zero and negative sequence reactances are given in Appendix A.

The analysis of the graphs follow.

1. Static limits > AC limits > DC limits. i.e.. generation limits for units with static excitation systems are higher (less restrictive) than generation limits for units with AC excitation system. Generation limits for units with AC excitation systems are higher (less restrictive) than generation limits for units with DC excitation system. This effect. shown in Figures A.2 thru A.4. is due to the higher initial response characteristics (higher ceiling voltage and time response) of the static and AC alternator exciters.

   Influence on probability of instability: Since limits corresponding to static and AC alternator excitation systems are virtually the same when the fault is at the far-end of the circuit. for a given fault rate. circuits having a higher concentration of faults at the far-end causes diminished benefit from higher response excitation system performance.

2. All limiting operating point functions for all fault types and for all excitation system types have the same shape. concave downward. The largest 3σ. 2σ (all exciters) and 1σ (DC exciter) fault limit is obtained in the segment $0.5 < L < 0.8$. where L is the normalized line length. or equivalently. in the segment $0.03 < X < 0.046$. where X is per unit line reactance. The largest 1σ fault limit is obtained in the segment $0.2 < L < 0.3$. ($0.012 < X < 0.017$) for AC and Static exciters.

   Influence on probability of instability: The downward concavity indicates that faults closer to the machine terminals are not necessarily more severe than faults distant from the machine terminals. This contradicts the commonly accepted assumption that stability performance of the machine under study improves as faults become more distant from that machine terminals. This also implies that probability of instability is lower for circuits having a higher concentration of faults in the middle rather than at the ends.

3. As expected, three phase faults, for all excitation types, incur the most restrictive limit when the fault is located at the terminals of the machines, but three phase faults at the far-end of the circuit may be less severe than two phase to ground or one phase to ground faults at the same location. For example, in Figures A.6 and A.7 generation limits for different fault types at $L \geq 0.4$ ($X \geq 0.023$) indicate that $1o$ faults are more limiting than $3o$ faults for AC and Static exciters. This is due to slower excitation system response to $1o$ faults at $L \geq 0.4$. Consequently probability of instability is heavily dependent on the fault type distribution and studying stability performance only for three phase faults yields a poor indication of actual risk associated with a given operating point.

Table 4.1 Comparison of fault severity as a function of excitation system (faults at Navajo, L=0)

Excitation system	limits
DC	$1o > 2o > 3o$
AC	$1o > 2o > 3o$
Static	$1o > 2o > 3o$

Table 4.2 Comparison of fault severity as a function of excitation system (faults at Westwing, L=1)

Excitation system	limits
DC	$1o > 2o > 3o$
AC	$3o > 2o > 1o$
Static	$3o > 2o > 1o$

Influence on probability of instability: Use of static or AC exciters decrease the probability of instability, since lopf limits increase. Although single line to ground faults have higher probability of occurrence their influence does not tend to raise limits under risk-based security assessment because single line to ground faults are more limiting than other fault types for the far-end 50-60% of the circuit.

4. The limits for all fault types decrease by approximately 100 MW (or 0.05 per unit change from the "base" case) when the Navajo-Moenkopi line impedance magnitude increases by 20%. The limits for all fault types increase by approximately 100 MW (a 0.05 per unit change from the "base" case) when the Navajo-Moenkopi line impedance magnitude decreases by 20%. The lopf shapes remain unchanged as line impedance changes: this is shown in Figures A.8 thru A.10.

   The $\pm 20\%$ change in line impedance magnitude results in a $\mp 5\%$ change in limits. i.e., the limits change little with line impedance magnitude changes.

   Influence on probability of instability: The probability of instability decreases as line impedance decreases.

5. A $\pm 20\%$ change in X_0 and X_2 result in a negligible change in limits. The observed change is of the same magnitude as the tolerance used to bracket the limits (10 MW): this is shown in Figures A.11 thru A.12.

   Influence on probability of instability: Changes in positive or negative sequence reactances have negligible influence on the probability of instability since there is no discernible change in lopf characteristics.

4.5 Summary

In this chapter we investigated analytical expressions of the limiting value of generation as a function of fault type and fault location. Two approaches were investigated. In approach A, we explored using an expression from the transient energy function (TEF). Because TEF requires angles and speeds at fault clearing, this approach proved infeasible since these angles and speeds may only be obtained via numerical integration and are not available in closed form. In approach B we investigated a simple one-machine to infinite bus system using the equal area criterion. This approach results in an expression

that requires an iterative solution procedure and as such does not serve well the need of identifying basic factors which influence the limiting operating point functions. We conclude that factors influencing the limiting operating point functions are best identified using simulation.

In studying the limiting operating point function we have investigated two items: system stability performance as a function of fault type and fault location and the effect on the probability of instability of sequence impedances seen from the fault point for unbalanced faults. excitation system type for the at "risk" generator and network topology. The significance of the limiting operating point functions study can be summarized in:

- Conclusions on stability performance:
  - Generation limits for units with static excitation systems are higher (less restrictive) than generation limits for units with AC excitation system. Generation limits for units with AC excitation systems are higher (less restrictive) than generation limits for units with DC excitation system.
  - All limiting operating point functions for all fault types and for all excitation system types have the same shape. concave downward. The downward concavity indicates that faults closer to the machine terminals are not necessarily more severe than faults distant from the machine terminals. This contradicts the commonly accepted assumption that stability performance improves as faults become more distant from machine terminals.
  - As expected. three phase faults. for all excitation types. incur the most restrictive limit when the fault is located at the terminals of the machines. but three phase faults at the far-end of the circuit may be less severe than two phase to ground or one phase to ground faults at the same location.

- Conclusions on probability of instability:
  - The downward concavity of the limiting operating point functions implies that probability of instability is lower for circuits having a higher concentration of faults in the middle rather than at the ends.
  - Use of static or AC exciters decrease the probability of instability, since lopf limits increase. Although single line to ground faults have higher probability of occurrence their influence does not tend to raise limits under risk-based security assessment because single line to ground faults are more limiting than other fault types for the far-end 50-60% of the circuit.
  - The probability of instability decreases as line impedance decreases.
  - Changes in positive or negative sequence reactances have negligible influence on the probability of instability since there is no discernible change in lopf characteristics.

5 RISK MANAGEMENT EXAMPLE

5.1 Introduction

We use a modified version of the IEEE Reliability Test System to illustrate risk-based electric power system security assessment and to compare it with traditional deterministic security assessment. We determine operating limits using iso-risk contours drawn in the space of pre-contingency controllable parameters, effectively creating nomograms based on risk. Details on the the risk-based security assessment are given and a numerical example is presented.

5.2 Selected scenario

We have chosen the IEEE Reliability Test System (IEEE-RTS) [33] to illustrate the risk-based security assessment approach. We have done so to allow comparison of our method with other reliability assessment methods and techniques as well as for the intrinsic value of illustrating our approach using a well known and available IEEE standard system. The IEEE-RTS is a generic system, in the sense that it does not represent an existing power system, but we believe that when properly modeled studies performed on it provide valuable general results and guidelines applicable to real systems.

We have chosen a scenario where each of three different events, outage of a transmission line in all cases, have potential to provoke one of two different security violations: transient instability of machines at a nearby plant and thermal overload on a line ad-

jacent to an outaged circuit. This multiplicity of triggering events and outcomes allow illustration of composite risk at a given operating point. The following section provides more information on the IEEE-RTS.

5.2.1 IEEE reliability test system

The IEEE Reliability Test System (IEEE-RTS) is a standardized electric generation and transmission system used to test and compare methods and results from reliability analysis of various types of power systems. It has been used in bulk power system reliability studies since it was first published in 1979 by the Application of Probability Methods (APM) Subcommittee of the IEEE Power System Engineering Committee. In this work we modify and use the most recent version of this system, which was published in 1996, called RTS-96. RTS-96 has the capability of being up to a three area RTS, depending on user specification determined by the application.

5.3 Numerical example

The modified one area IEEE-RTS, shown in Figure 5.1, is used to illustrate the risk-based security assessment approach. The base case has a total system load of 3192 MW and the line between Bus 13 and Bus 11 is considered out of service due to either forced or scheduled outage. All generators are represented using the classical machine model except for those at Bus 13 which are represented using two axis machine model with exciter. There are three identical machines at Bus 13, each having a maximum generation capacity of 350 MW. Real power loads are represented as constant current, and reactive power loads are represented as constant impedance.

The critical parameter set, parameters that most influence the postcontingency system performance, are real power generation at Bus 13 and pre-contingency flow on the line between buses 12 and 13. We define the credible contingency list to be: (event

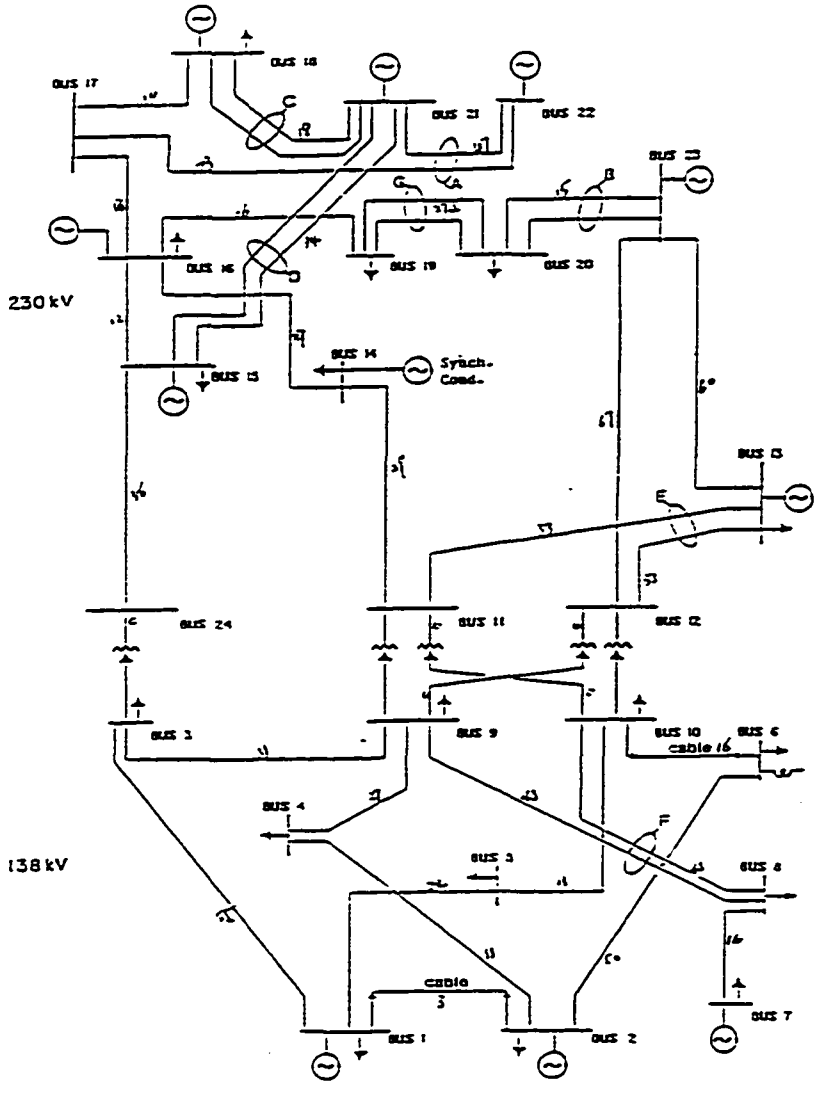

Figure 5.1 IEEE - One area RTS-96

1) loss of line between Bus 12 and Bus 13. (event 2) loss of line between Bus 13 and Bus 23 and (event 3) loss of line between Bus 12 and Bus 23. These events may cause two different types of security violations: transient instability to generators at Bus 13 (caused by events one and two) and thermal overload on the line between Bus 12 and Bus 13 (caused by event three).

The deterministic limits for acceptable transient stability performance are based on a worst-case disturbance scenario. In this case the scenario consists of: 1) a three phase, four cycle fault at Bus 13 removed by clearing the line between Bus 12 and Bus 13; here

the limit is 202 MW/machine and 2) a three phase, four cycle fault at Bus 13 removed by clearing the line between Bus 13 and Bus 23: here the limit is 204 MW/machine. In both cases the deterministic stability limit was identified using time domain simulation.

Limits to avoid thermal overload depend on three parameters: generation at Bus 13, pre-contingency flow on the line between Bus 12 and Bus 23 (outaged line) and pre-contingency flow on the line between Bus 12 and Bus 13 (monitored line). Given a set of feasible generations at Bus 13 and flows on these lines we use generation shift factors and line outage distribution factors [34, pp. 363-366] to calculate post-contingency flow on the line monitored for thermal overload, the line between buses 12 and 13. The flow on the line between Bus 12 and Bus 13 after the line between Bus 12 and Bus 23 is outaged is our post-contingency performance measure for the thermal overload problem. Explicitly,

$$\hat{f}_l = f_l^* + d_{lk} f_k^* \tag{5.1}$$

where

- $d_{lk} = \frac{\Delta f_l}{f_k^*}$ is the line outage distribution factor when monitoring line l after outage on line k.
- Δf_l is the change in MW flow on line l.
- f_k^* is the flow on line k before it is outaged.
- f_l^* is the flow on line l before it is outaged.
- and $\hat{f}_l$ is the flow on line l after line k is removed.

The pre-outage flows on lines l and k, f_l^* and f_k^* respectively, are a function of generation level at Bus 13 and other injections. We model the dependency on generation

at Bus 13 explicitly and use a consistent set of feasible flows on these lines as to reflect the influence on post-contingency flow of other injections on the network.

$$f_l^* = f_l^0 + a_{li}(P_i - P_i^0) \tag{5.2}$$

$$f_k^* = f_k^0 + a_{ki}(P_i - P_i^0) \tag{5.3}$$

where

- $a_{li} = \frac{\Delta f_l}{P_i - P_i^0}$ and $a_{ki} = \frac{\Delta f_k}{P_i - P_i^0}$ are the generation shift factors representing the sensitivity of the flow on line l or k to a change in generation at bus i.
- Δf_l and Δf_l are the changes in MW flow on line l or k.
- $P_i - P_i^0$ is the change in generation at bus i.
- f_l^0 and f_l^0 are the flow on line l or k before the generation change at bus i.
- and f_l^* and f_k^* are the flows on line l or k after the generation change at bus i.

Substitute Eq. 5.2 into Eq. 5.1 to obtain

$$\hat{f}_l = f_l^0 + a_{li}(P_i - P_i^0) + d_{lk}(f_k^0 + a_{ki}(P_i - P_i^0)) \tag{5.4}$$

Eq. 5.4 is used to calculate the post-contingency flow on the line between Bus 12 and Bus 13 when the line between Bus 12 and Bus 23 is outaged for a range of values of P_i. The reason for making this calculation as a function of P_i is so we can express the post-contingency performance indicator, and therefore risk, as a function of a precontingency parameter that is both controllable by an operator and influential towards the risk corresponding to the event. Thermal overload on the line between Bus 12 and Bus 13 occurs if:

- the line between Bus 12 and Bus 23 is outaged. $\hat{f}_{12-13} > 488$ (488 MVA is the Short Term Emergency (STE) rating)
- under no outage conditions. $f^{-}_{12-13} > 390$. from Eq. 5.2. 390 is the minimum continuous rating of line 12-13

5.3.1 Probability data

The following conditional probabilities of having a *no* fault when a fault occurs were assumed for events one and two: 0.01. 0.19. and 0.8. for 3o. 2o. and 1o faults respectively. We model the occurrence of the event line outage using a homogeneous Poisson process with intensity. λ. of 45.8×10^{-6} outages/hour (or 0.40 outages/year $\times$ 365 $\times$ 24) for all lines. i.e. $P(F_1) = P(F_2) = P(F_3) = 45.8 \times 10^{-6}$. We assume that a fault may occur anywhere on the line with the same probability. therefore. we use a discrete uniform distribution function to model fault location.

5.3.2 Limiting operating point functions

Limiting operating point functions for each fault type. 3o. 2o. and 1o. can be determined for outage on the lines between Bus 13 and Bus 12 and between Bus 13 and Bus 23 using time domain simulation to identify limits for faults located at various locations on the line to be cleared. The limiting operating point functions used in this case are illustrated in Figures 5.2 and 5.3. The limiting parameter is real power generation at Bus 13.

These limiting point functions (lopf) differ from those shown in Appendix A. These lopf exhibit a behavior similar to those illustrated in Figure 3.1. they are monotonically increasing. i.e.. the limiting generation level of a *no* fault increases as the fault is moved away from the bus closest to the machine at risk of losing synchronism. We can also see that as the fault type changes from a 3o fault to a 2o to a 1o fault the limiting

generation level increases. Both of these effects occur because these changes cause the impedance seen by the fault to increase.

The lines between Bus 12 and Bus 13 and between Bus 13 and Bus 23 are considerably shorter than those studied in Chapter 4. It seems that the diminishing benefits of a high response excitation system, i.e., more restrictive limits at the far end of the line, are associated with line length. Verification and possible quantification of this effect is worthy of future investigation.

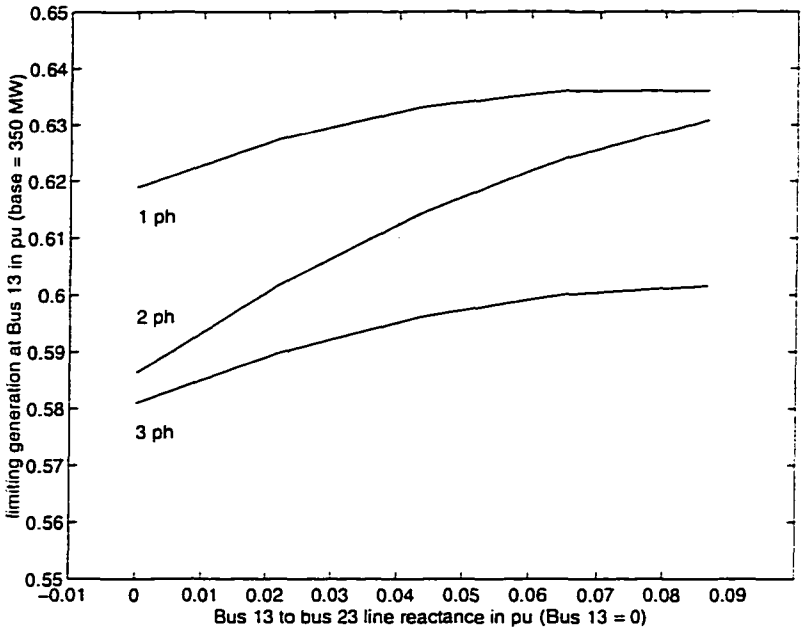

Figure 5.2 Limiting operating point functions for an outage on the line between Buses 13 and 23, modified RTS-96

5.3.3 Impact

In the event of transient instability it is estimated that the three 350 MW units at Bus 13 would be out of service for 10 hours. We assume that energy can be replaced at a cost of 37.5 $/MWh, startup fixed costs are estimated at $18,000 for all three machines

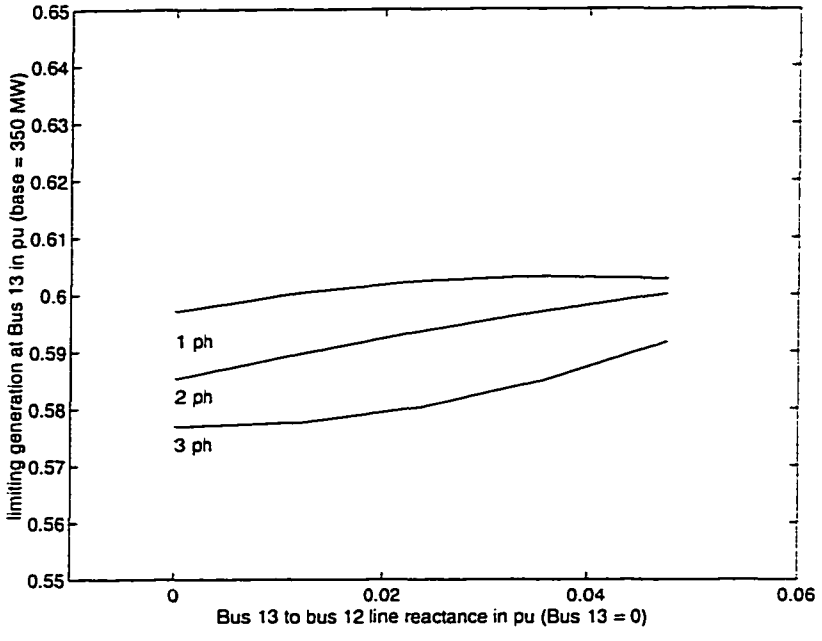

Figure 5.3 Limiting operating point functions for an outage on the line between Buses 13 and 12, modified RTS-96

and maintenance and repair costs are estimated at $36.225 for all three machines[1]. These costs are direct costs to the energy producer, we assume that no load is shed due to this outage, thus there are no direct or indirect costs to the customer.

The impact of thermal overload is divided into maximum and partial impact. Maximum impact refers to the total cost of reconductoring the line, this is needed when the flow on the line exceeds short-time emergency rating. Maximum impact is estimated at $108.000 per mile[2]. Partial impact is the impact of thermal overload for flows above continuous rating and below short-time emergency rating. Partial impact is assumed, for simplicity, to follow a linear curve as shown in Figure 5.4, a maximum partial impact of one third the total cost of reconductoring the line is assumed to generate the impact vs. limiting parameter curve. This figure is arbitrary, the point being that there is a deterioration on the line that must be accounted for when flows are above continuous

[1]See Chapter 3 for the source of these estimates

[2]See previous footnote

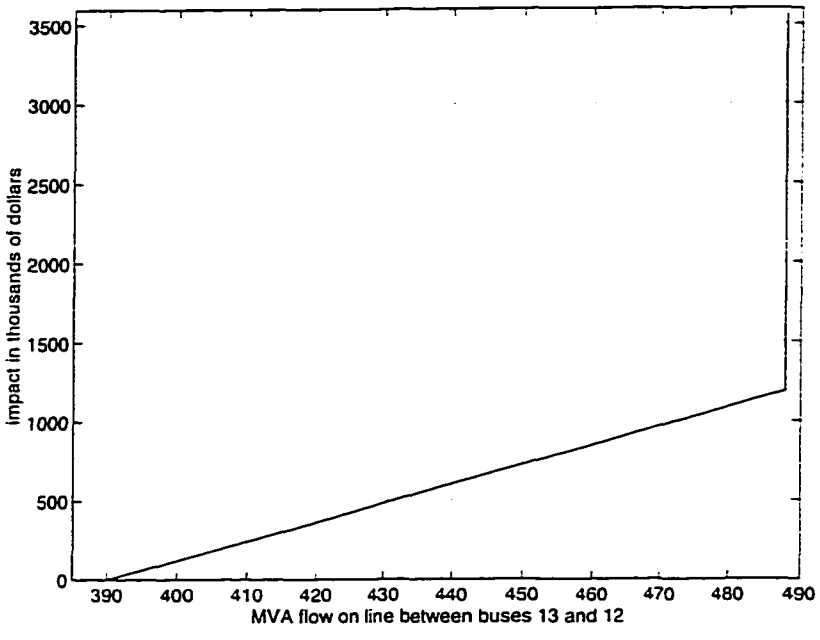

Figure 5.4 Thermal overload impact as a function of MVA flow for the line between Buses 13 and 12. modified RTS-96

rating and below short-time emergency rating.

5.3.4 Risk based nomograms

Let $i = 1.2.3$ denote: (event 1) loss of line between Bus 12 and Bus 13. (event 2) loss of line between Bus 13 and Bus 23 and (event 3) loss of line between Bus 12 and Bus 23. respectively. Security violation $j = 1$ denotes transient instability to generators at Bus 13 (caused by events one and two) and security violation $j = 2$ denotes thermal overload on the line between Bus 12 and Bus 13 (caused by event three).

Risk of transient instability due to event one and two is denoted by $R_{11}(s_t)$ and $R_{12}(s_t)$ respectively. Risk of thermal overload is denoted by $R_{23}(s_t)$. Risk of transient instability is a function of generation at Bus 13 only. $R_1(P_{13}) = R_{11}(P_{13}) + R_{12}(P_{13})$. Risk of thermal overload is a function of generation at Bus 13 as well as other injections. the influence of which we capture as pre-existing flows on the outaged and monitored

lines f_l^0 and f_k^0 in Eq. 5.4. $R_2(P_{13}, f_{12-13}^0, f_{12-23}^0) = R_{23}(P_{13}, f_{12-13}^0, f_{12-23}^0)$. The sum of these two risks give the composite risk of operating at point s_t. i.e., the total risk of operating at s_t. $R(s_t) = R_1(s_t) + R_2(s_t)$.

We want to draw contours of constant risk in the space of operating parameters. i.e., $R(s_t) = K$. Our operating parameters, the critical parameter set, are real power generation at Bus 13 and pre-contingency flow on the line between buses 12 and 13[3]. Generation at Bus 13 is an independent parameter, the pre-contingency flow on the line between buses 12 and 13 depends on the generation at Bus 13 as well as other injections.

We have written a computer program to draw contours of constant risk. The algorithm that controls this program follows:

1. read a set of feasible generations at Bus 13, P_{13}^0, and flows that reflect the influence of other injection on lines 12-13 and 13-23 f_{12-13}^0 and f_{13-23}^0.

2. select a generation level at bus 13, P_{13}

3. calculate risk of transient instability using the limiting operating point functions information shown in Figures 5.2 and 5.3 and impact of transient instability

4. calculate the flows on lines 12-13 and 13-23 for the selected generation level at bus 13 using Eq. 5.4 and compute risk of thermal overload

5. calculate total risk adding risk of transient instability and thermal overload: save the result

6. repeat steps 2 to 5 for different generations at bus 13

7. select a level of risk K

[3]We could have chosen flow on the line between buses 12 and 23 instead of flow on the line between buses 12 and 13. We use only one flow because we wish to generate two-dimensional nomograms. However, the resulting nomogram, though given in the space of P_{13} and f_{12-13}, accounts for the influence of f_{12-23} and for the dependency of both flows on P_{13}. See Eq. 5.4.

8. solve the equation $R(s_t) = K$ for pre-contingency parameters

9. draw the solution of $R(s_t) = K$ in the space of pre-contingency parameters

Figure 5.5 shows contours of constant risk, the output of our computer program, for an initial flow on line 12-13 of 365.4 MVA. Four iso-risk curves are shown, at risk levels 0, 30, 100 and 170. The risk levels have units of dollars over the next hour, i.e., the expected cost over the next hour in dollars. Regions under an iso-risk curve represent generation-flow combinations that result in risk below the risk associated to the iso-risk curve. Notice that we obtain a considerable increment of the security region, and consequently substantial increase in equipment utilization, if we allow operation beyond the zero risk level, the deterministic level.

5.3.5 Operating limits development

We have a tool to draw nomograms based on risk: we require criteria to determine a threshold risk value that will define the region of acceptable operation. The boundary of this region consists of the operating limits corresponding to the threshold risk contour.

Reference [16] suggests three different methods of identifying thresholds for a new index, as follows.

1. Use judgment or experience based on what has previously been defined as acceptable operating points in the past.

2. Compute a criterion for the index in terms of other indices for which criteria are clearly established.

3. Perform a cost/benefit analysis, and choose a criterion that minimizes total costs of providing reliability plus the costs of instability.

Method 1 could be applied by computing risk for acceptable operating points where system response to a contingency is stabilized by applying remedial action to trip a unit, an action which gives a "controlled impact".

Method 2 is attractive if other criteria for stability limitations can be established. For example, one might propose that loss of the plant at Bus 13 (681 MW, generation at economic dispatch) for 10 hours once per year is acceptable, but loss of the plant for 10 hours twice per year is unacceptable, so that the threshold level is bracketed between $R = P \times I = 0.27 \times ((681)(10)(37.5\text{-}19.95) + 18.000 + 36.225) = \$46.910$ and $2 \times \$46.910 = \$93.820$ [4]. As another example, if the security problem was undamped oscillations that continued unmitigated, they could result in an out of step condition, generation tripping, and subsequent load shedding via underfrequency relays. This would enable direct quantification of the impact in terms of the shed load. A risk threshold could be identified by "working backwards" from a threshold in terms of MW-hrs/year interrupted or customer-hrs/year interrupted.

Threshold determination by method 3 could be interpreted as an optimization problem where one desires to simultaneously minimize the sum of the operating costs plus the risk. Equivalently, a decision can be made on the basis of *expected monetary value* [2] of the risk vs. no risk "gamble". Impact, in dollars, of the risk alternative may be compared against the operating costs of the no risk alternative, using a decision tree where the alternatives are weighted using their corresponding probability of occurrence. For example, the deterministic limit to avoid transient instability is 202 MW/machine at Bus 13. Operating at 202 MW/machine represents a penalty in operation costs since the un-restrained economic dispatch indicates that machines at Bus 13 should be operated at 227 MW/machine. Assume these machines are constrained at 202 MW/machine for 10 hours every day and further assume that the cost of buying the 25 MW/machine

[4]The cost of replacing the energy is assumed to be 37.5 $/MWh. The cost of producing the energy is 19.95 $/MWh, the incremental cost.

is 37.5 $/MWh. the cost of producing the energy is 19.95 $/MWh. the incremental cost. The cost of adhering to the deterministic limit over one hour is. (25)(3)(37.5-19.95) = $1.316. Now. assume we choose to ignore the deterministic limit and operate the plant at 227 MW/machine. In the event of transient instability we will loose the plant for 10 hours incurring in a cost of (227)(3)(37.5-19.95)(10) + 18.000 + 36.225 = $173.740. Assuming the occurrence of faults follow an homogeneous Poisson process with intensity of 45.8×10^{-6} outages/year the probability of having no outages over the next hour is $P(r = 0) = e^{-45.8\times10^{-6}} = 0.99995$. the probability of one outage is $P(r = 1) = 45.8 \times 10^{-6}$. The expected costs of the risk vs. no risk gamble are $7.96 and $1.316 respectively. Clearly the expected costs of adhering to the deterministic limit exceed those of ignoring it[5].

Deciding which level of risk is acceptable is a management decision that will be dictated by company policy. Which method will be used to determine an acceptable risk threshold will depend on the company's policy towards risk.

Once this decision is made the system operator will receive new nomograms that indicate the operating limits to be maintained. Figure 5.6 show contours of constant risk. risk level = 30. for different initial flows on line 12-13. $f3 > f2 > f1$. An operator will use this graph in the following manner.

1. Identify the current operating point. The operating point is determined by real power generation at Bus 13 and existing flow on line 12-13.

2. Identify the iso-risk contour corresponding to the existing flow.

3. If current generation at Bus 13 and existing flow on line 12-13 exceed the desired

[5]A risk averse decision maker may doubt the results of the economic analysis we have presented based on the idea that it does not take into account events of extremely low probability but very severe system collapse mechanism. A defense plan against these events is presented in [15]. implementation of a similar plan may be an economically feasible way to complement the risk based security strategy proposed here since it will account for the extremely low probability events which may result in very severe impacts.

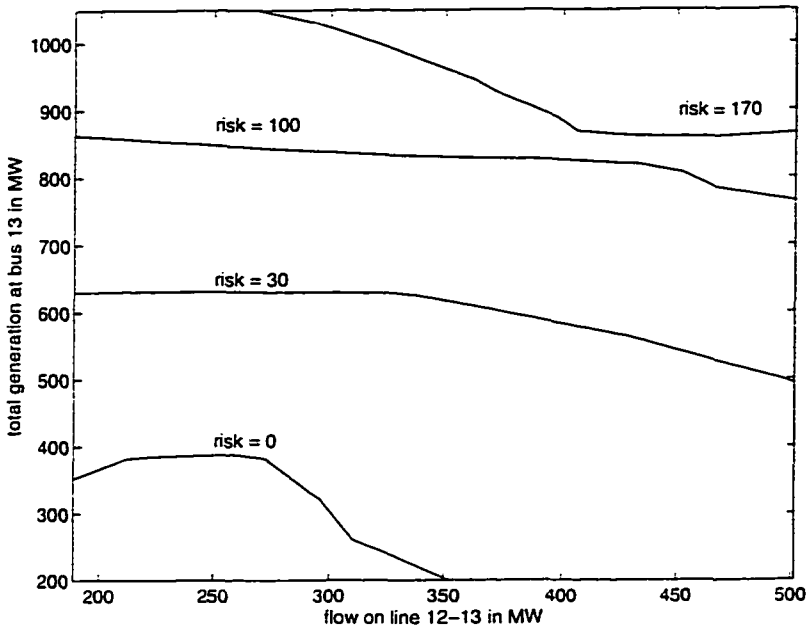

Figure 5.5 Contours of constant risk for operating point 1: $P_0 = 680$. $f_{12-13} = 365.4$. $f_{13-23} = 168.5$

risk level adjust generation at Bus 13 to move the operating point inside the security region.

5.3.6 Effect of conventional system protection reliability on risk-based nomograms

Eq. 3.19 gives the risk at an operating point s_t considering unreliability of conventional protection equipment. We will use Eq. 3.19 and assume maximum impact, i.e., loss of all generators at the generating plant, in all events to calculate the risk at a given operating point and compare it to the risk assuming fully reliable protection equipment. The impact in all cases is $I = I(K_j/F_i \cap M \cap S_t) = I(K_j/F_i \cap \bar{M} \cap B \cap S_t) = I(K_j/\bar{F}_i \cap M_0 \cap S_t) = (10)(37.5) \times P_{gen} + 54.225$. Also $P(s_t) = 1$, $P(F_i) = 45.8 \times 10^{-6}$ and $P(\bar{F}_i) = 1 - P(F_i) = 0.9999542$.

We obtain the probability of succesful breaker operation, $P(M)$, probability of active

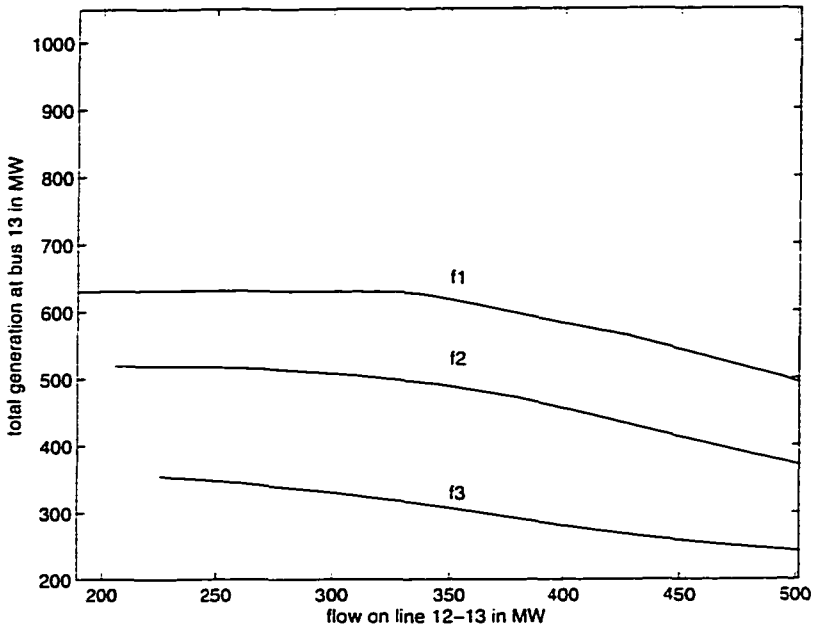

Figure 5.6 Contours of constant risk. risk level = 30. for different initial flows on line 12-13

breaker failure. $P(\bar{M})$. and probability of passive breaker failure. $P(M_0)$ using a Markov chain [26. pp. 137-161]. We chose a Markov chain to model breaker reliability because of the stand-by nature of the conventional protection system. The breaker is not under continuous operation: it is required to operate at a certain moment. and its success or failure will depend on its operating condition. *its state*. The Markov chain has three states: 0 - succesful operation. 1 - active failure and 2 - passive failure. The transition rates between these states are given by the active. λ_1. and passive. λ_2. failure rates of the breaker[6]. The breaker may: remain in state 0. the initial state. transit from state 0 to state 1 or transit from state 0 to state 2 [7]. The transition matrix. B. for the breaker

[6]According to the test data for the IEEE RTS the active failure rate of a breaker is 0.0066 failures/year. the passive failure rate of a breaker is 0.0005 failures/year.

[7]This is worst case scenario since we do not allow transition from the failure states to the successful operation state. i.e.. we assume there is no inspection of the breaker during its service period.

is:

$$B = \begin{vmatrix} 1-\lambda_1-\lambda_2 & \lambda_1 & \lambda_2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{vmatrix}$$

The transition matrix corresponding to one hour transition intervals is:

$$B = \begin{vmatrix} 0.99999919 & 753.42 \times 10^{-9} & 57.08 \times 10^{-9} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{vmatrix}$$

The probabilities of being at each possible state after one year are $P_{8760} = P_0 \times B^{8760} =$ (0.9997 0.0003 0.0000). Thus. $P(M) = 0.9997 = P(B)$. $P(\bar{M}) = 0.0003$ and $P(M_0) =$ 0.0000. Substitution of these values into Eq. 3.19 results in

$$R(s_t) = \sum_{\forall j} \sum_{\forall i} I \times 45.8 \times 10^{-6} \tag{5.5}$$

The same calculation assuming fully reliable protection equipment yields

$$R(s_t) = \sum_{\forall j} \sum_{\forall i} I \times 45.8 \times 10^{-6} \tag{5.6}$$

There is no discernible increment in probability of insecurity. and therefore on the risk. This is because of the high reliability of conventional protection systems.

How unreliable must the conventional protection system be to influence the risk of an operating point ? Assuming an active failure rate as 0.066 and a passive failure rate as 0.005 failures /year. respectively (an order of magnitude increment [8]) the probabilities of being at each possible state after one year become $P_{8760} = P_0 \times B^{8760} =$ (0.997 0.0028 0.0002). Thus. $P(M) = 0.997 = P(B)$. $P(\bar{M}) = 0.0028$ and $P(M_0) =$ 0.0002. Substitution of these values into Eq. 3.19 results in

[8]This is equivalent to 66 breakers out of a 1000 failing when required to operate over the next year. Increasing the unreliability level of these devices by another order of magnitude will be unrealistic since an active failure rate of 0.66 failures/year implies that 660 breakers out of a 1000 will fail when required to operate over the next year. Such unreliable devices will not be put to use.

$$R(s_t) = \sum_{\forall j} \sum_{\forall i} I \times 45.9 \times 10^{-6} \tag{5.7}$$

The increment in probability of insecurity is in the order of 1×10^{-7}. Assume a maximum impact of $200.000. then $R(s_t) = 9.18$ dollars over the next hour for unreliable protection systems and $R(s_t) = 9.16$ dollars over the next hour for fully reliable protection systems. The risk based nomograms obtained considering unreliability of conventional protection equipment will be indistinguishable from those considering fully reliable protection equipment.

5.4 Summary

We have used the IEEE Reliability Test System to illustrate how to quantify the risk associated with a given operating point. Using contours of constant risk in the space of operating parameters we provide a risk management tool that allows corporate managers to justify decisions to operate beyond deterministic operating limits when it is economically advantageous to do so. New nomograms based on risk rather than deterministic limits are produced and the change is transparent to the system operator. An important feature of the risk-based nomogram is that we can automatically draw them accounting for dependencies between critical parameters. Our analysis of the effect of conventional system protection unreliability on risk-based nomograms shows that these are indistinguishable from those considering fully reliable protection equipment. Therefore assuming fully reliable protection equipment simplifies risk calculations and yields an acceptable risk value.

6 CONCLUSIONS AND SUGGESTIONS FOR FUTURE WORK

6.1 Contributions of this work

We have developed a method that allows risk-based security assessment in an operating environment considering any type of security violation. This method explicitly calculates the risk of an operating point and permits, if desired, the inclusion of reliability of protection equipment in the risk calculation.

An integral part of the risk-based security assessment method is the calculation of probability of insecurity. We have developed, using probability theory, expressions to calculate the conditional probability of insecurity given a fault occurs for thermal overloads and two approaches for computing probability of transient instability: one based on Law of Total Probability and the other on Cartesian products. Our method to calculate probability of insecurity uses a minimum amount of statistical data, the frequency of faults and their type on a circuit, data known to be gathered by utilities. We present a simple method that is tractable thus avoiding the need of calculating probabilities using computationally intensive methods.

Also, in contrast with previous work on probabilistic stability assessment, our purpose of calculating probability of instability is to use it with the impact of instability, i.e. to calculate risk of operating at a specific operating point. Calculating probability of instability is only one step towards the use of risk as a decision making tool, a management tool. Accounting for impact of instability leads to the development of a

concise statement of the security-economics tradeoff problem.

We introduced the concept of limiting operating point functions, curves used to calculate probability of transient instability that include within them information on operating point, probability and system stability performance. We investigated how excitation systems and other parameters affect the limiting operating point functions.

Using our risk-based security assessment method we can draw contours of constant risk in the space of operating parameters. These contours can be used as a risk-management tool, allowing managers to justify decisions to operate beyond deterministic operating limits when it is economically advantageous to do so. Once an acceptable level of risk is identified we can generate nomograms based on risk rather than deterministic limits. The change from deterministic to risk-based operating limits is transparent to system operators since they just see new nomograms or tables.

Finally, we provided an example illustrating how to implement the risk-based security assessment method using a modified version of the IEEE-Reliability Test System 1996.

6.2 Suggestions for future work

In this work we developed a general method to perform risk-based security assessment in operating environment and focused on transient instability and thermal overloads as the security violations of interest. It will be of great interest to include voltage and oscillatory instability problems in this scheme.

The effect of special protection scheme (SPS) reliability on risk of transient instability is currently under investigation at Iowa State University. Other promising topics of investigation are calculating risk for planning purposes, where the operating points for which risk is calculated are not deterministic but follow a probability distribution, and obtaining risk when the critical parameters set has high cardinality.

In our study of limiting operating point functions we did not consider the effect of

changing the voltage profile of the study area. These variations in the voltage profile may influence the behavior and characteristics of the limiting operating point functions and may prove worthy of future investigation.

We suggest further work to enhance the determination of a threshold risk value that would provide for identification of the desired operating limits by calculation of the appropriate iso-risk contours. In order to determine a risk threshold it may be benefitial to identify thresholds on probability and impact. i.e.. to have three threshold values:

- Probability threshold: Identify a minimum probability threshold below which the effects of the contingency would be excluded from the composite risk calculation used to determine operating limits. This implies that we do not include the effects of low probability events. regardless of the impact.

- Impact threshold: Identify a maximum impact threshold for events with nonnegligible probability (as identified by the probability threshold). Examples of impact which would exceed this impact threshold may be those which will result in loss of life. heavy equipment damage or trip of a nuclear unit. An operating point is unacceptable if an event with nonnegligible probability would cause an impact that exceeds this threshold. Contingencies with impact greater than this threshold will have zero-risk (deterministic) limits.

- Risk threshold itself: A threshold to be applied to those events with probability greater than the probability threshold and impact less than the impact threshold.

It should be noted that selection of a probability (minimum) threshold and an impact (maximum) threshold does not determine the risk threshold. The probability and impact thresholds are set without regard to the benefits associated with an operating condition: the risk threshold is. however. operating point dependent. Efforts to standarize these

thresholds. or the procedures to identify them. may prove benefitial for the entire electric power industry.

Finally. assuming that actual line outage data can be obtained. a goodness of fit study on different possible models to find another distributions for the occurrence of line outages (possible probabilistic models are Weibull. Log normal. Log logistic) is recommended. This effort may prove beneficial if we consider the possibility of using hazard functions to reconcile statistical data collection on a yearly basis and use of this data on an hour basis.

APPENDIX A LIMITING OPERATING POINT FUNCTIONS STUDY RESULTS

Study system

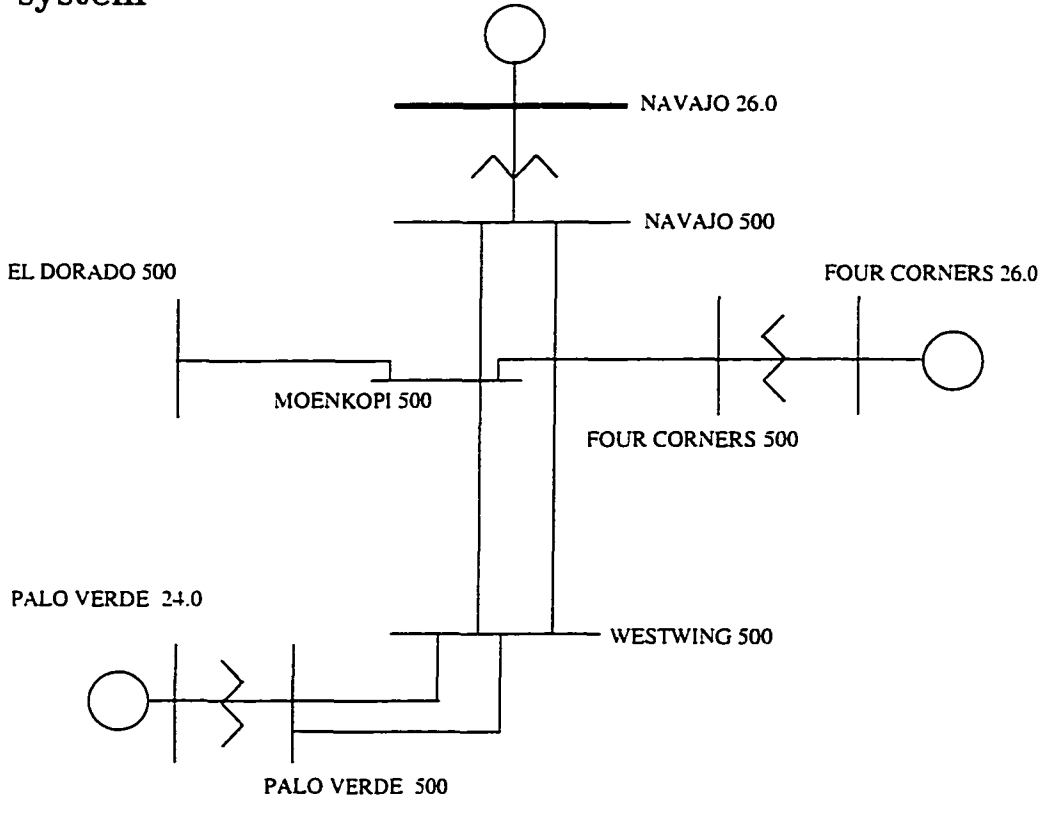

Figure A.1 One-line diagram of the study system: a 500 kV system local to the Navajo Power Plant in Arizona

Table A.1 Line impedances of the study system

line	impedance
FOURCORNERS-MOENKOPI	0.00180 + j 0.04189
NAVAJO-MOENKOPI	0.00078 + j 0.01815
WESTWING-MOENKOPI	0.00184 + j 0.04244
ELDORADO-MOENKOPI	0.00222 + j 0.04959
PALOVERDE-WESTWING	0.00040 + j 0.00960 (2 lines)
NAVAJO-WESTWING	0.00255 + j 0.05865

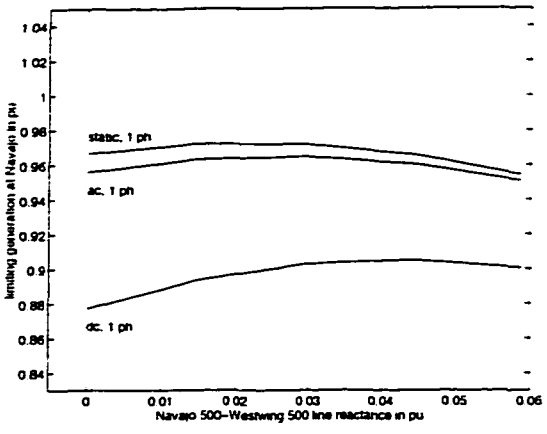

Figure A.2 Comparison of limiting operating point funtions. three excitation system types and 1σ faults

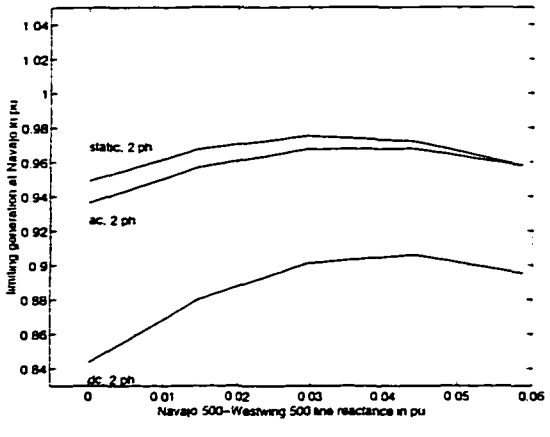

Figure A.3 Comparison of limiting operating point funtions. three excitation system types and 2σ faults

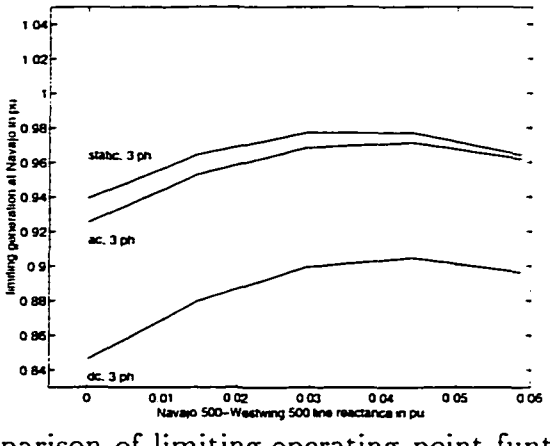

Figure A.4 Comparison of limiting operating point funtions. three excitation system types and 3σ faults

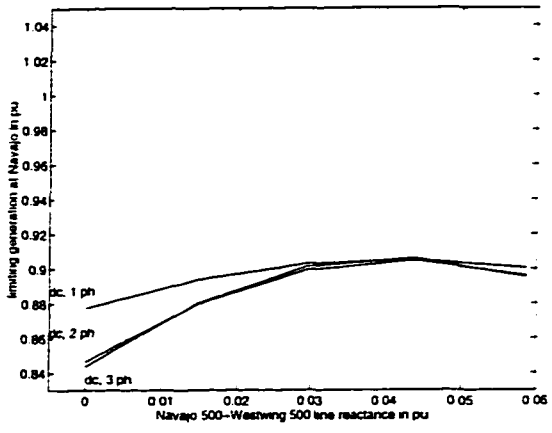

Figure A.5 Comparison of limiting operating point funtions. three fault types and DC exciter system

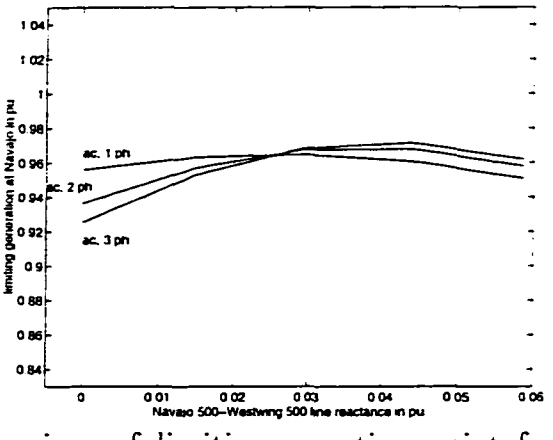

Figure A.6 Comparison of limiting operating point funtions. three fault types and AC exciter system

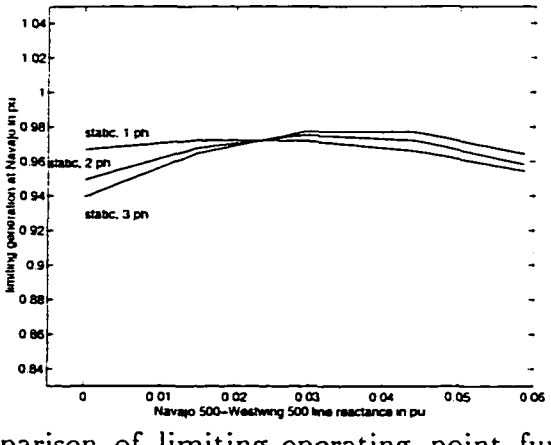

Figure A.7 Comparison of limiting operating point funtions. three fault types and Static exciter system

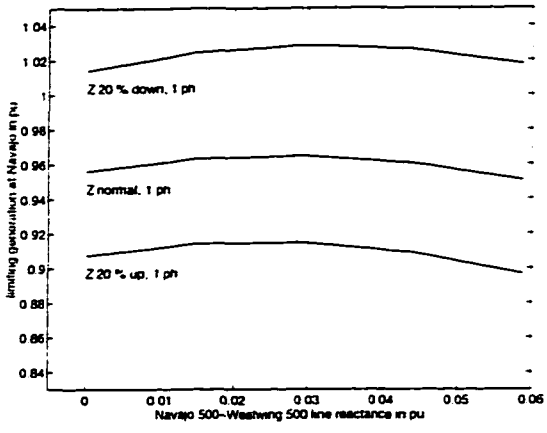

Figure A.8 Comparison of limiting operating point funtions. Navajo 500 - Moenkopi 500 impedance change and 1σ faults

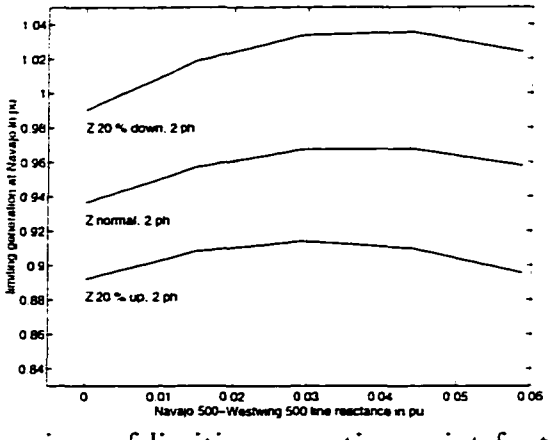

Figure A.9 Comparison of limiting operating point funtions. Navajo 500 - Moenkopi 500 impedance change and 2σ faults

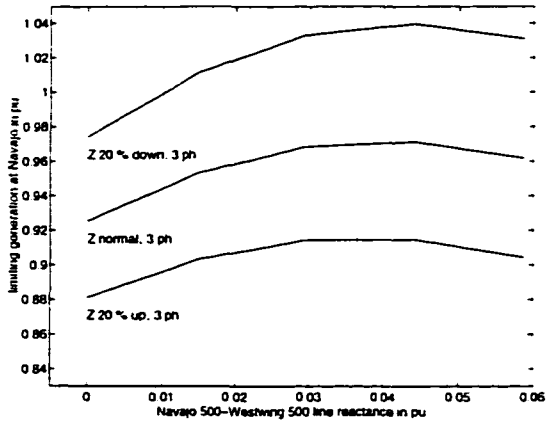

Figure A.10 Comparison of limiting operating point funtions. Navajo 500 - Moenkopi 500 impedance change and 3σ faults

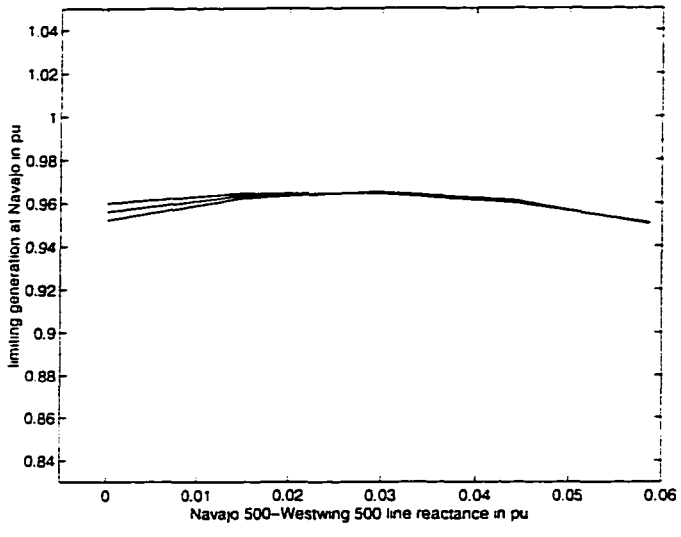

Figure A.11 Comparison of limiting operating point funtions. zero and negative sequence impedance change and 1σ faults

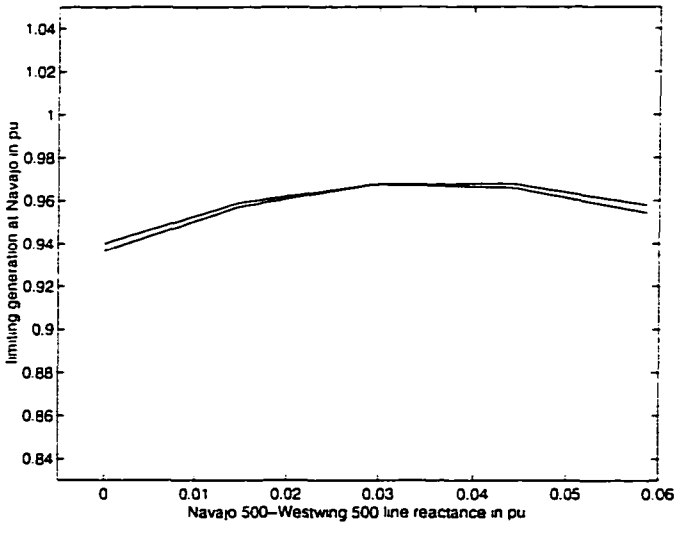

Figure A.12 Comparison of limiting operating point funtions. zero and negative sequence impedance change and 2σ faults

Parameters used in the study

Table A.2 DC commutator exciter parameters (Type DC1A)

$K_A = 46.0$	$T_A = 0.06$	$V_{RMAX} = 1.00$
$V_{RMIN} = -0.9$	$T_E = 0.46$	$SE_1 = 0.33$
$SE_2 = 0.1$	$E_{FD1} = 3.10$	$K_F = 0.10$
$T_F = 1.0$		

Table A.3 Alternator supplied controlled-rectifier exciter parameters (Type AC4A)

$K_A = 200.00$	$T_A = 0.015$	$V_{RMAX} = 4.58$
$V_{RMIN} = -3.67$	$V_{IMAX} = 0.300$	$V_{IMIN} = -0.30$

Table A.4 Potential or compound source controlled-rectifier exciter with field voltage control loop parameters (Type ST3A)

$K_A = 7.93$	$T_A = 0.04$	$V_{RMAX} = 10.000$
$V_{RMIN} = -10.00$	$V_{IMAX} = 0.20$	$V_{IMIN} = -0.200$
$K_I = 0.00$	$K_P = 6.15$	$K_{BMAX} = 6.900$
$K_C = 0.20$	$K_G = 1.00$	$X_L = 0.081$
$V_{GMAX} = 5.80$		

All data taken from "IEEE Recommended practice for excitation system Models for Power System Stability Studies". IEEE Standard 421.5-1992.

Note: ETMSP and IEEE Standard follow different notation.

T_A (ETMSP) = T_M (IEEE Standard)

K_A (ETMSP) = K_M (IEEE Standard)

K_J (ETMSP) = K_A (IEEE Standard)

The values of X_0 and X_2 at Navajo 500 and Moenkopi 500 were provided by Arizona Public Service planning engineers. Intermediate values were calculated assuming a linear distribution of these parameters over the Navajo-Westwing line.

Table A.5 Zero and negative sequence reactances at different points over the Navajo 500 - Westwing 500 line ($L = 0$ at Navajo 500, $L = 1$ at Westwing 500)

location	$L = 0$	$L = 1/4$	$L = 1/2$	$L = 3/4$	$L = 1$
X_0	0.0033	0.0038	0.0042	0.0047	0.0051
X_2	0.0049	0.0046	0.0044	0.0041	0.0038

APPENDIX B RECONDUCTORING COSTS

Information from Commonwealth Edison Company

In 1992 ComEd reconducted a 138kV, L11609, 300 Kcmil copper conductor to 1113 Kcmil 45/7 ACSR conductor, from Electric Junction to Frontenac, a distance of 4.5 miles for an increase in capacity requirement[1].

The following material and construction costs are based on this project.

Table B.1 ComEd reconductoring project: material and construction costs (reconductoring only)

materials	conductor = 75,000 feet	$100,000
	hardware = clamps, arm steel, dampers, shackles, etc.	$20,000
	Total	$120,000
construction	conductor removal and disposal, no salvage	$40,000
	conductor installation includes: guard poles temporary dead-ends arm reinforcements, etc.	$50,000 × 4.5 = $224,870
	Total	$264,870

Therefore the total cost to reconduct a 4.5 mile line (assumes 8 structures per mile) = $384,870. The cost per mile is approximately $86,000 (conductor only).

The following additional items were installed also: two dead end towers at each end

[1]This information was provided by R.P. Schlueter, Commonwealth Edison Company, 125 South Clark Street, P.O. Box 767, Chicago IL 60690-0767 via correspondence with Glenn Hillesland, Adjunct Professor, Iowa State University on July, 18 1996.

of the line. This was required to provide additional capacity to carry higher tension to meet NESC regulations for clearances. All existing porcelain insulators were changed to 138kV polymer insulators (silicon type) plus grounding and static wire replacement.

The cost for materials and construction for doing this work was:

Table B.2 ComEd reconductoring project: material and construction costs (dead end towers installation)

two tower foundations two towers	$60.000 $42.000
insulators ($120 a piece)	$12.000
Change of static wire from 134.6 Kcmil ACSR to 7#8 Alwd.. installation materials (for 4.5 miles)	 $55.000 $16.000
Ground rods reinstallation	$30.000

Total costs of the project were:

Table B.3 ComEd reconductoring project: material and construction costs (Total)

conductor only	$384.870
tower work	$102.000
insulator work	$12.000
static wire and grounds	$71.000
Total (This cost does not include switching or inspection costs. usually 5% or 6% of total cost of the project.)	$569.870

All work was completed in 4 calendar months. The project was performed by outside contractors with ComEd inspection. All materials supplied by ComEd.

The total cost of the project was 126.638 dollars/mile.

Information from Pacific Gas and Electric Company

PG&E planning engineers inform that per unit costs do not address the cost to reconductor a line since it can vary significantly if towers need to be strengthened or

poles interset. For the more straightforward jobs. they suggest about 100-150 thousand dollars per circuit mile[2]. Approximate costs of building new lines and costs of replacing termination equipment when reconducting follow.

Table B.4 PG&E costs of building new lines

60 and 70 kV single circuit wood pole - 397.5 kcmil	
No underbuild	$125.000/mile
Underbuild	$166.000/mile
Overbuild	$196.000/mile
60 and 70 kV single circuit wood pole - 715.5 kcmil	
No underbuild	$133.000/mile
Underbuild	$173.000/mile
Overbuild	$204.000/mile
115 kV single circuit wood pole - 715.5 kcmil	
No underbuild	$142.000/mile
Underbuild	$188.000/mile
Overbuild	$218.000/mile
115 kV DCTL - 715.5 kcmil	
One circuit installed	$251.000/mile
Two circuits installed	$318.000/mile
Install second circuit	$84.000/mile
230 kV DCTL - 1113 kcmil Al	
One circuit installed	$364.000/mile
Two circuits installed	$463.000/mile
Install second circuit	$117.000/mile
230 kV DCTL - 1113 Al (2 conductor bundled)	
One circuit installed	$533.000/mile
Two circuits installed	$708.000/mile
Install second circuit	$195.000/mile

[2]This information was provided by Chifong Thomas and Robert Jenkins from Pacific Gas and Electric Company. Transmission Planning Department. via electronic mail to James McCalley. Assistant Professor. Iowa State University on July. 24 1996.

Table B.5 PG&E costs of line termination

60 or 70 kV single conductor up to 1113 kcmil AA conductor	$842.000
115 kV single conduction up to 2300 kcmil AA conductor	$1.317.000
230 kV DCTL up to 1113 kcmil AA single conductor	$1.793.000
230 kV DCTL up to 2 conductor bundled 1113 kcmil AA	$1.828.000

BIBLIOGRAPHY

[1] "Analytical methods for contingency selection and ranking for dynamic security analysis." EPRI Final Report TR-104352. Project RP 3103-3. 1994.

[2] H. Raiffa. *Decision Analysis: Introductory Lectures on Choices under Uncertainty.* Reading. Massachusetts: Addison-Wesley. 1968.

[3] "The new IEEE standard dictionary of electrical and electronic terms." New York. New York: IEEE Press. 1993.

[4] R. Billinton and R. Allan. *Reliability Evaluation of Engineering Systems: Concepts and Techniques.* New York. New York: Plenum Press. second ed.. 1992.

[5] "Regional reliability criteria." North American Electric Reliability Council Report. Princeton. New Jersey: NERC. 1994.

[6] P. Anderson and A. Bose. "A probabilistic approach to power system stability analysis." *IEEE Transactions on Power Apparatus and Systems.* vol. PAS-102. pp. 2430–2439. August 1983.

[7] P. Anderson. A. Bose. K. Timko. and F. Villaseca. "A probabilistic approach to stability analysis." EPRI Report EL-2797. Electric Power Research Institute. 1983.

[8] K. Timko, A. Bose, and P. Anderson, "Monte carlo simulation of power system stability," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-102, pp. 3453–3459, Oct 1983.

[9] R. Billinton and P. Kuruganty, "A probabilistic index for transient stability," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-9, pp. 195–206, Jan/Feb 1980.

[10] P. Kuruganty and R. Billinton, "A probabilistic assessment of transient stability," *International Journal of Electric Power and Energy Systems*, vol. 2, pp. 115–119, April 1980.

[11] R. Billinton and P. Kuruganty, "Probabilistic evaluation of stability in multimachine power systems," *IEE Proceedings*, vol. 126, no. 4, pp. 321–326, 1980.

[12] Y.-Y. Hsu and C.-L. Chang, "Probabilistic transient stability studies using the conditional probability approach," *IEEE Transactions on Power Systems*, vol. 3, pp. 1565–1572, November 1988.

[13] F. Wu, Y. Tsai, and Y. Yu, "Probabilistic steady-state and dynamic security assessment," *IEEE Transactions on Power Systems*, vol. 3, pp. 1–9, February 1988.

[14] A. L. da Silva, J. Endrenyi, and L. Wang, "Integrated treatment of adequacy and security in bulk power system reliability evaluations," *IEEE Transactions on Power Systems*, vol. 8, pp. 275–282, February 1993.

[15] C. Counan, M. Trotignon, E. Corradi, M. Stubbe, and J. Deuse, "Major Incidents on the French Electric System: Potentiality and Curative Measures Studies," *IEEE Transactions on Power Systems*, vol. 8, pp. 879–886, August 1993.

[16] 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. PWRS-9. pp. 181–190. February 1994.

[17] APM Task Force Report on Protection Systems Reliability. "Effect of protection systems on bulk power reliability evaluation." *IEEE Transactions on Power Systems*. vol. 9. pp. 198–204. February 1994.

[18] P. Kuruganty and R. Billinton. "Protection system modelling in a probabilistic assessment of transient stability." *IEEE Transactions on Power Apparatus and Systems*. vol. PAS-100. pp. 2163–2170. May 1981.

[19] P. Anderson. "Reliability modeling of protective systems." *IEEE Transactions on Power Apparatus and Systems*. vol. PAS-103. pp. 2207–2214. August 1984.

[20] T. Aven. *Reliability and Risk Analysis*. Essex. England: Elsevier Applied Science. 1992.

[21] J. Andrews and T. Moss. *Reliability and Risk Assessment*. Essex. England: Longman Scientific & Technical. 1993.

[22] R. B. Jones. *Risk-Based Management: A Reliability-Centered Approach*. Houston.Texas: Gulf Publishing Company. 1995.

[23] L. Bain and M. Engelhardt. *Introduction to Probability and Mathematical Statistics*. Belmont. California: PWS-KENT Publishing Company. second ed.. 1992.

[24] A. Papoulis. *Probability. Random Variables. and Stochastic Processes*. New York. New York: McGraw-Hill Book Company. second ed.. 1984.

[25] J. McCalley. A. Fouad. V. Vittal. A. Irizarry-Rivera. B. Agrawal. and R. Farmer. "A risk-based security index for determining operating limits in stability limited

electric power systems." Presented at IEEE-PES Summer Meeting. 1996. Paper 96 SM 505-8 PWRS.

[26] S. M. Ross. *Introduction to Probability Models.* San Diego. California: Academic Press. Inc.. fifth ed.. 1993.

[27] G. Wacker and R. Billinton. "Customer cost of electric service interruptions." *Proceedings of the IEEE.* vol. 77. pp. 919–930. June 1989.

[28] C. Woo and R. Pupp. "Costs of service disruptions to electricity consumers." *Energy.* vol. 17. no. 2. pp. 109–126. 1992.

[29] "Application of safety instrumented systems for the process industries." Instrument Society of America (ISA) Standard ISA-S84.01-1996. February 1996.

[30] A. Nguyen. A. Irizarry-Rivera. J. McCalley. and V. Vittal. "Survey development for assessing impact of power system disturbances." Presented at the Fifth Annual Midwest Electro-Technology Conference. 1996.

[31] A. Fouad and V. Vittal. *Power System Transient Stability Analysis Using the Transient Energy Function Method.* Englewood Cliffs. New Jersey: Prentice Hall. Inc.. 1992.

[32] P. Anderson and A. Fouad. *Power System Control and Stability.* New York. New York: IEEE Press. 1994.

[33] Reliability Test System Task Force of the Application of Probability Methods Subcommittee. "The IEEE reliability test system - 1996." Presented at IEEE-PES Winter Meeting. 1996. Paper 96 WM 326-9 PWRS.

[34] A. Wood and B. Wollenberg. *Power Generation Operation and Control.* New York. New York: John Wiley and Sons. 1984.

ACKNOWLEDGMENTS

I would like to express my gratitude to my major professor Dr. James D. McCalley, under whose able guidance the work was conducted.

My sincere thanks to Drs. V. Vittal, G. Sheblé and J. Lamont and to Prof. G. Hillesland, for generously providing time and assistance in the completion of this work.

It has been a great pleasure to be a part of the power graduate students group at Iowa State University. Your camaraderie, support and the many hours we spent working, learning and laughing made my stay at Iowa State an unforgettable part of my life. I thank you all.

I am very grateful for the support and encouragement that my parents, Agustín and Lydia, and my sisters, Eca and Debbie, have offered me during my entire life. I thank my wife, Maribel, for her understanding, support and encouragement through my doctorate studies. To all of you *gracias*.

The author acknowledges the financial support of the Office of Minority Students Affairs, Iowa State University and the Electric Power Research Institute for this research work.