Value of Security Assessment - Extensions and Applications

A thesis submitted to

the University of Manchester Institute of Science and Technology

for the degree of

Doctor of Philosophy

2003

Dilan Supun Jayaweera

Department of Electrical Engineering & Electronics

Declaration

No portion of the work referred to in the thesis has been submitted in support of an application for another degree or qualification of this or any other university, or other institution of learning.

Acknowledgement

I express my profound gratitude to my supervisor Prof. Daniel Kirschen. His invaluable advice, suggestions, guidance, and helps were main sources for the successful completion of this research project.

I would thank Prof. Ron Allan for offering invaluable advice and suggestions. Prof. Goran Strbac and Prof. Nick Jenkins are acknowledged with gratitude for their helps.

I would extend my gratitude to Dr. Keith Bell, Dr. Doug Warne, and Dr. Syed Ahmed for suggestions and advice given at the project meetings.

A very special thanks goes to National Grid Transco (UK) and UMIST for funding this research project.

Friends are also acknowledged for their supports.

I express my sincere thanks to sister Deepthi and brothers Dimuthu, Roshan, and Nirosh, for their continuing encouragement.

I would gratefully dedicate this thesis to my parents.

Abstract

This thesis proposes a novel tool to warn system operators when the level of stress in a power system becomes excessive. This tool is called probabilistic indicator of system stress. The thesis also proposes adaptive deterministic security criteria. These criteria assess the security of a power system on a deterministic basis but take into account the probabilistic nature of outages and their consequences. Both strands of this research focus on static security analysis.

The proposed indicator of system stress is calibrated using two calibrating techniques. The first technique creates a set of reference cases by increasing the system load. The second technique creates reference cases by taking out of service some components, de-rating and up-rating plants, and then adjusting the system load accordingly. These reference cases are used as the tick marks on the indicator of stress. Real time operating conditions are used to test the calibrated scale. The Monte Carlo simulation is used to estimate the absolute values in this design and Correlated Sampling is used to compare new operating situations with the reference cases. Stratified sampling is extended and applied to the Monte Carlo simulation to reduce the variance of the estimate. The indicators of stress were tested on the 24-bus IEEE Reliability Test System and on the 1085-bus model of the NGT (UK) system. The proposed indicator of system stress measures the system stress quantitatively and it is designed to be used in power system operation.

The deterministic and probabilistic security criteria are reviewed by applying the concepts of these two criteria to the modified 24-bus IEEE Reliability Test System. Probabilistic security assessment is also used to investigate the influence of weather conditions and system blackouts on the cost of security. These weather conditions include fair, average and adverse. The probabilistic cost of security is estimated using the Monte Carlo simulation, which relies on extended stratified sampling to reduce the variance of the estimate and speed up convergence.

Adaptive deterministic security criteria (ADSC) use deterministic security boundary and the probabilistic cost of security to determine adaptive deterministic security boundary (ADSB). Three types of ADSBs are proposed to test the criteria and to identify the best type of the ADSB. These types include single-line, rectangular and tri-line. At first, the reference contour plot is identified using the costs of security along the deterministic security boundary. The reference ADSB is calculated using the reference contour plot. Then, the families of ADSB are calculated and they are used to determine the initial group of ADSB. The system ADSB is determined by constructing more groups of ADSB to distribute them over the system feasible operating region. The concepts of ADSC are applied to the modified 24-bus IEEE Reliability Test System. ADSB adapts to the operating conditions in a power system. It determines the level of security in a power system on a deterministic basis but more accurately than traditional deterministic security criteria.

The issues and difficulties encountered in the design of this indicator and these criteria are addressed in detail. The use of these tools in power system operation and the benefits that they offer to power system operators are also discussed.

List of Publications

Parts of the research outcomes were published in international journals and conferences. They are listed below.

[a] D S Kirschen, D Jayaweera, D P Nedic, R N Allan, "Probabilistic Indicator of System Stress" in Proceedings of PMAPS'2002 - 7th International Conference on Probabilistic Methods Applied to Power Systems, Naples, Italy, September 2002.

[b] M A Rios, D S Kirschen, D Jayaweera, D P Nedic, R N Allan, "Value of Security: Modelling Time-Dependent Phenomena and Weather Conditions", IEEE Transaction on Power Systems, Vol. 17, No. 3, August 2002, pp. 543-548.

[c] D S Kirschen, K R W Bell, D P Nedic, D Jayaweera, R N Allan, "Computing the Value of Security," IEE PSMC conference, London, April 2002.

[d] D S Kirschen, K R W Bell, D P Nedic, D Jayaweera, R N Allan, "Computing the Value of Security," IEE Proceedings – Generation, Transmission and Distribution, Vol. 150, No. 6, November 2003, pp. 673-678.

[e] D S Kirschen, D Jayaweera, D P Nedic, R N Allan, "Probabilistic Indicator of System Stress" submitted to IEEE Transaction on Power Systems (under review).

List of Contents

Chapter 4 – Probabilistic Indicator of System Stress

List of Figures

Chapter 5

Chapter 6

List of Tables

Chapter 1

Introduction

1.1 Objective and Motivation

Power systems are operated with a significant margin to ensure that faults and other unscheduled outages do not immediately trigger consumer disconnections or the collapse of at least part of the system. Since the introduction of competition in the electricity supply industry, the cost to the suppliers of providing this security margin has become much more apparent. Consequently OFGEM (Office of Gas and Electricity Markets) has questioned whether the criteria used to set this margin produce an appropriate level of security. But, what is "an appropriate level of security"? Power system operators are well aware that, by generating electric power closer to the major load centre, one can reduce the frequency and severity of customer outages. The value of such security measures is equal to the cost to society of the customer disconnections that they prevent. The benefits of such security can only be estimated in a probabilistic sense since it is aimed at protecting the power system against unpredictable events.

The review of security standards performed in1994 by NGT (National Grid Transco) for OFGEM showed that the traditional empirical security standards would, in some cases, result in excessive security expenditures. In other situations, these criteria may be strict enough to prevent economically disastrous incidents.

Power system security is the term used to describe the ability of a power system to withstand unpredictable but unavoidable disturbances, such as the sudden loss of transmission lines due to lightning-induced failures or the outage of a major power plant due to a mechanical failure. Because of the extreme importance of electric power for economic activity and daily life, power system operators, such as the National Grid Transco, must carefully monitor the level of security of their system.

Traditionally, deterministic security criteria have been used for security assessment. A power system is usually said to be "secure" if it satisfies deterministic security criteria. These criteria usually state that no operating limit should be violated in the event of a probable contingency. Probable contingencies are defined as the outage of a single component of the system or of two related elements, such as two transmission lines located on the same set of towers. Security is checked using contingency analysis tools that simulate the effect of each of the "probable" contingencies using power system analysis programs. Power system analysis programs perform power flow, voltage stability of transient stability computations.

The idea behind the deterministic approach to security is that it avoids the cascading outages that lead to major incidents. For example, if a line outage results in an overload in another line, this second line is likely to trip, causing further outages and possibly load disconnections or a system collapse. While the deterministic criteria are simple and robust, they may not be economically optimal. Under some situations, they may enforce a level of security that is not justified by the benefit that they provide in terms of avoided customer disconnections. In other cases, for example during severe weather conditions, these deterministic criteria may not reflect the actual risk of major outages.

The main limitation of the deterministic approach is that it assumes that only "probable" contingencies will occur. While this is usually the case, a number of major incidents have resulted from contingencies that were assumed to have a low probability of occurrence.

The concept behind probabilistic security analysis is that one should look beyond an arbitrarily defined set of "probable" contingencies and study what could happen to the system in the case of unlikely events. If we do not limit ourselves to "probable" contingencies, the state of the system cannot be defined as secure or non-secure because most combinations of contingencies will cause some violations of operating limits. Taking preventive actions to avoid constraint violations that might be caused by unlikely events is not possible because it would be extremely costly. One simply cannot

secure the system against all possible contingencies. Another measure of security must be adopted if we are going to look beyond the probable contingencies.

1.2 Achievements and Conclusions of the First Project

The project "A method for computing the value of security in power system operations" was initiated by Prof. Daniel Kirschen in 1997. This project is also called in this thesis as the "first project." Dr. K. Bell developed the software codes necessary for this computation. Later Dr. M. Rios further developed this software and applied to a model of the NGT (UK) system. Following are the achievements and conclusions of the first project.

- A software tool that embodied a method for estimating power system outage costs for specified operating plans using Monte Carlo simulation was developed. This tool is called Value of Security Assessor (VaSA). The VaSA was extensively and successfully tested on a model of the NGT (UK) system. The results of tests are encouraging.

- Six variance reduction techniques and several variants were tested and compared to the results obtained with naïve Monte Carlo simulation. A Correlated sampling technique that makes possible a reliable comparison of operational schedules was also developed.

- A model consisting of five "weather states" was developed. One of these states corresponds to "normal weather" (i.e., fair weather) while other four correspond to conditions that usually result in a much higher than average number of faults. The testing showed that adverse weather does not affect the choice of operational plan.

- A knowledge-based system modelling operator-initiated corrective actions was developed and integrated within the VaSA. Techniques for modelling the probability of transient instability and the like hood of cascading and sympathetic trippings were developed and tested.

The VaSA is capable of calculating the value of security not only for a snapshot of the state of the system, but also for an operational plan covering 24 hours and taking into account the reaction time of the operator.

1.3 Aim of the Research

A study of major network outages carried out as part of the first project found that incidents occur even when the system is apparently operating within its normal security criteria. In some cases, these incidents are caused by a consequence of independent events that was considered too unlikely to be worth considering. In other cases, the system collapsed because a protection mal-operation unnecessarily removed from service a critical piece of equipment and caused cascading outages. Assuming that unexpected outages are independent events can therefore lead to widely optimistic conclusions regarding the security of the system.

Describing a system simply as secure or insecure because it satisfies or does not satisfy a deterministic security criterion can thus be misleading. Charting the unknown territory that lies beyond the deterministic criterion is essential if one wants to quantify how secure a system is. This is particularly true of systems where power transfers are close to their limits. On the other hand, in many cases operators have the opportunity to take corrective actions to rescue the system following unexpected events. The ability (or inability) to take such actions should be considered when describing the security of a power system.

Conversations with operators suggest that, rather than describing security in binary terms, they would like to have a continuous indication of the level of security (or its reciprocal, the degree of stress) of their power system. The VaSA is an ideal engine for calculating such an index because it does not limit itself to single or double contingencies and because it models complex phenomena such as cascading and sympathetic trippings.

Therefore, the first aim of this thesis is the designing a Probabilistic Indicator of System Stress based on an estimate of the amount of energy that may not be served if the system were to be operated under given operating conditions.

Probabilistic indicator of system stress should satisfy the design requirements. It should measure the system stress quantitatively. The indicator shall be calibrated with a set of reference cases that span regularly over the feasible operating limits of the power system. Real time operating conditions shall be used for testing. Monte Carlo simulation and Correlated Sampling are the main mechanisms that are used to calibrate and test the proposed indicator of stress.

Probabilistic indicator can be used to signal operators of the current level of stress under which the system is operating. If the indicator shows that the system is slightly stressed, no action is required. On the other hand if the level of stress as measured by the indicator is high, the operators may want to take measures to reduce the consequences of such operations.

It is often said that power systems are currently operating closer to their limits than in the past. The proposed indicator of stress could be used to provide a quantitative assessment of this statement.

On the other hand the probabilistic approaches are widely regarded in academic circles as more rigorous than deterministic criteria. However, power system operators have been reluctant to adopt them. Their reservations are easy to understand: in the high pressure, high responsibility environment of a control centre, operators do not want to be told that there is an X% probability that the system might collapse. They want straight answers to simple questions: Do I need to do something? Is my plan of action acceptable? How much power can I let flow through this line?

The traditional deterministic security criteria such as ‘N-1’ or ‘N-D’ provide a simple basis on which these questions can be answered. However, the resulting operating plans will, in some cases, be too conservative while under different conditions, they may

subject the system to unacceptable risks. On the other hand, the level of risk can be fixed if the operating plans are evaluated and adjusted on a probabilistic basis.

Unfortunately, this form of probabilistic assessment is not easily integrated with the tools that operators use to design their plans. Unless probabilistic security can be expressed in a simple form that is easy to understand and apply, operators will resist its application.

Therefore, the second aim of this thesis is the defining Adaptive Deterministic Security Criteria based on a probabilistic assessment of the system's security.

Adaptive deterministic security criteria use deterministic security boundary and probabilistic cost of security to calculate the adaptive deterministic security boundary. Unlike deterministic security boundary, the adaptive deterministic security boundary adapt to the operating conditions in a power system and determine the level of security in a power system more accurately than the 'N-1' or 'N-D' security criteria.

Adaptive deterministic security boundary provides a deterministic solution in a probabilistic framework and can be used by system operators to identify, feasible, secure, and economical operating conditions in a power system.

1.4 Outline of the Thesis

Chapter 2 reviews the literature relevant to this research project. This review begins with the fundamental concepts of power system security and progresses through security assessments of different time frames. The deterministic and probabilistic approaches to security assessment are addressed and the limitations of each of these approaches are highlighted. The literature on the risk-based security assessments is also reviewed. Alternative approaches, such as hybrid techniques that combine deterministic and probabilistic assessments, are also discussed. The chapter concludes with a critical review of the existing research and further highlights the benefits of the outcomes of the work described in this thesis.

Chapter 3 describes the work done in the project "A method for computing the value of security in power system operations", which this project continues. The main deliverable of that project was the development of Value of Security Assessor (VaSA) program, which was heavily used in this project. After reviewing the motivation and aims of this expansion, the chapter describes the concepts of the value of security assessment, the power system model used for this assessment and the functions of the computer program used in this assessment. The chapter briefly describes the Monte Carlo simulation that is used in the Value of Security Assessment and the variance reduction techniques that have been implemented. The computation of the cost of security is also detailed. The chapter ends with a summary of the conclusions of this first project.

Chapter 4 describes the Probabilistic Indicator of System Stress. The design requirements, the possible stress metrics and the design methodology are presented in the initial part of the chapter. The application of Monte Carlo simulation, the variance reduction techniques and the convergence criteria together with the auxiliary convergence criterion for stopping the Monte Carlo simulation are then described. The difficulties encountered in achieving convergence of the Monte Carlo simulation for a large power system are discussed in details and the techniques used to solve this problem are presented. Test results obtained on a small test system and a large real power system through are analysed. This chapter also discusses the results for these two power systems with two calibrating techniques. The chapter concludes with a discussion on how this Probabilistic Indicator of System Stress could be used and the benefits it would provide to operators.

Chapter 5 compares the deterministic and probabilistic security criteria. At the beginning of the chapter the steps of the deterministic and probabilistic security assessments are described. Then the steps in these assessments are applied to the modified 24-bus IEEE Reliability Test System (1996). Probabilistic security assessment is also used to investigate the influences of weather conditions and system blackouts on cost of security. These weather conditions include fair, average, and adverse. Influence of system blackouts is investigated by considering system blackouts for the estimation

of cost of security and ignoring them. The results of all the investigations are graphically presented. The drawbacks and benefits of each of these criteria are discussed. It is also shown that the agreement between the deterministic security boundary and the probabilistic cost of security contours is poor. The results of the deterministic and probabilistic security assessments are brought forward to chapter 6 to explore the adaptive deterministic security criteria.

Chapter 6 explores the Adaptive Deterministic Security Criteria (ADSC). Three types of adaptive security boundaries (ADSBs) are proposed. They are single line, rectangular and tri-line. At first, the reference contour plot is identified. The reference ADSB is calculated using the reference contour plot. The reference ADSB is used to calculate families of ADSB. Families of ADSB are combined to determine the initial group of ADSB. Then, the system ADSB is determined by constructing more groups of ADSB that distribute over the system feasible operating region. The chapter concludes with a discussion of how this approach could be used in power system operation and benefits offered by ADSB.

Chapter 7 summarises the major findings of this research project and presents recommendations for further research. In particular, the importance of testing the adaptive deterministic security criteria to a real power system is highlighted.

Chapter 2

Literature Review

2.1 Introduction

The fundamental objective of an electric power system is to supply its customers with electrical energy as economically as possible and with a reasonable assurance of continuity and quality. To maintain such security standards the power systems are required to be reliable.

Power system reliability reflects the adequacy and security in a power system [1], [2]. Adequacy with regard to composite generation and transmission relates to the existence of both sufficient generation capacity to supply the energy demand and of the associated transmission facilities required to transport the energy to the major system load points. Security relates to the ability of the system to withstand unexpected failures and continue operating without interruption of supply to the consumers [3], [4]. Security assessment is a major concern in planning and operation of electric power systems.

The following sections of this chapter, review the literature relevant to this exploration of security issues. In particular, it covers the fundamental concepts of power system security, the deterministic and probabilistic approaches to security, and the techniques used in adequacy and security assessments. It focuses mainly on the probabilistic framework for system security, in the context of power system operation. At the end of the chapter, the main weaknesses of proposed techniques that are relevant to this research project and the strength of the research components proposed by this thesis are presented. Links between the first project (i.e., "A method for computing the value of security in power system operations") and other approaches that have been published recently are also highlighted.

2.2 Power System Security

Power system security is usually assessed on the basis of security standards, i.e., the relationship between outages of generation and transmission plant and the level of any acceptable loss of demand. An 'N-1' security standard requires the system to work satisfactorily following loss of any one of its N elements. [5]

Loading on transmission system under normal operating conditions must be limited to levels that permit any "credible contingency" to occur without exceeding acceptable power quality, component or system limits.[5]

Contingencies may be external or internal events (for instance, faults subsequent to lightning versus operator-initiated switching sequences) and may consist of small/slow or large/fast disturbances (for example, random behaviour of the demand pattern versus generator or line tripping). [6]

Usually, numerical simulation of the contingency scenario is used to assess the effect of a contingency on a power system in a given state. However, the non-linear nature of the physical phenomena and the growing complexity of real-life power systems make security assessment difficult. For example, monitoring a power system every day calls for fast sensitivity analysis to identify the salient parameters driving the phenomena, and suggestions on how to act on the system so as to increase its level of security. [6]

On the other hand, increasing economic and environmental pressures make the conflicting aspects of security and economy even more challenging as instead of building of new transmission lines and generation facilities, operators tend to operate power systems more closer to the critical limits[6].

Every small change in load is a disturbance that causes a change in system conditions. However, system security is assessed for larger changes that cause major changes in system conditions. These changes are mainly caused by contingencies. Most commonly contingencies result in relay operations that are designed to protect the system from

faults or abnormal conditions. Typical relay operations result in the loss of a line, transformer, generator, or major load. [7]

Various components in a power system respond to changes that occur and may reach an equilibrium condition that is acceptable according to some criteria. Mathematical analysis of these responses and the new equilibrium condition is called security analysis. [7]

The decision drivers of security can be classified as shown in Figure 2.1 and the corresponding time frames for making security related decision are given in Table 2.1 [7].

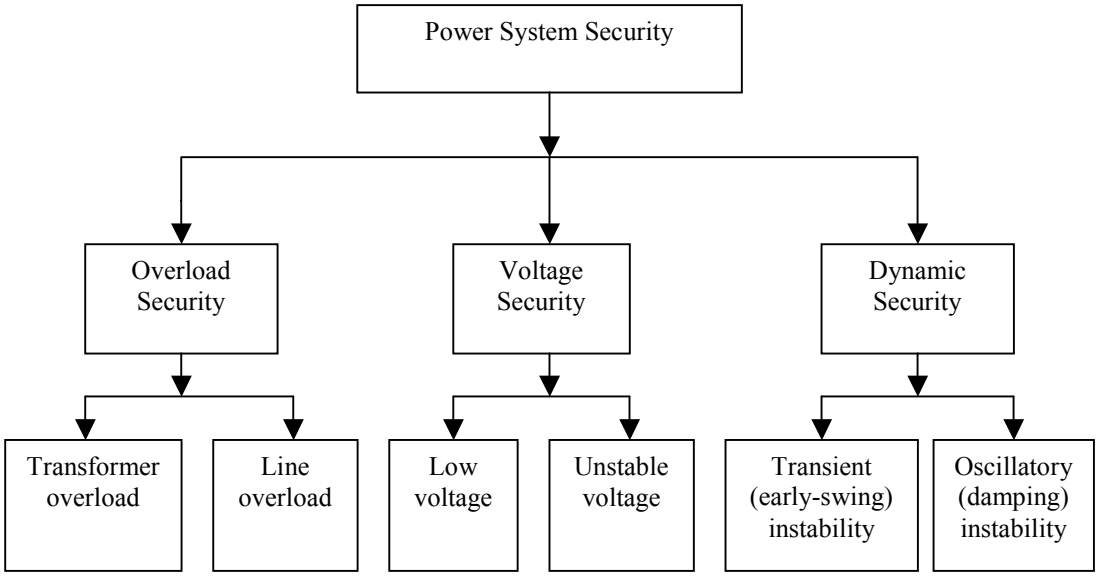

Figure 2.1: Decision drivers of power system security [7].

Table 2.1: Security related decisions [7].

Time-frame	Decision-maker	Decision	Basis for decision
On-line assessment (Minutes to hours)	Operator	How to constrain the economic operation to maintain the normal state?	Operating rules, online assessment, and cost
Operational planning (Hours to months)	Analyst	What should be the operating rules?	Minimum operating criteria, reliability, and cost
Planning (Months to years)	Analyst	How to reinforce/maintain the transmission system?	Reliability criteria for system design and cost

If the analysis evaluates only the expected post disturbance equilibrium condition (steady-state operating point), then it is called Static Security Assessment (SSA). Static or steady state security is the ability of the system to supply load without violating operating conditions and load curtailment [8],[9].

If the analysis evaluates the transient performance of the system as it progresses after the disturbance, then it is called Dynamic Security Assessment (DSA) [10],[11],[12]. Further, the DSA has been formally defined by the IEEE, Power Engineering Society (PES) working group on DSA as an evaluation of the ability of a certain power system to withstand a defined set of contingencies and to survive the transition to an acceptable steady state condition. Dynamic security considers the ability of the system to supply the load against system dynamic problems of early swing, transient instability and oscillatory instability[8], [13].

Voltage security is the ability of a system, not only to operate in a stable manner, but also to remain stable (maintenance of system voltage) following any reasonable credible contingency or adverse system change [8],[4]. Voltage security analysis is performed to investigate whether any contingency triggers a voltage collapse [8].

SSA can be used quickly to determine if a system is insecure by simply looking at the static outcome of each contingency. However, to know whether the system is fully secured, DSA must be performed. It determines if the associated dynamics of each contingency are acceptable.

A power system always resides in one of four states called normal, alert, emergency, and restorative. The emergency state can be extreme, temporary, or controlled [14]. The importance of the four security states is that they provide a conceptual basis for making security-related decisions. This basis rests on the assumption that any normal state is acceptable and any other state is unacceptable. Figure 2.2 shows the power system states and the corresponding actions.

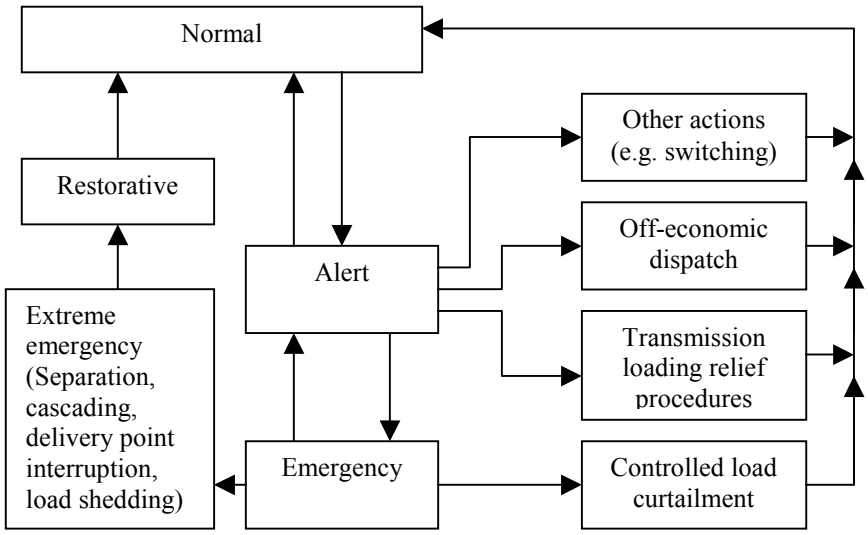

Figure 2.2: Power system states and actions [7].

The system planner and operator always have to consider security. Planning standards are more rigorous than operational standards. For example, the uncertainty in demand is not considered in operational standards.

Traditionally, security-related decisions in both operations and planning have been made with the criterion being that the power system should remain in the normal state at all times [13]. The fundamental drawback of this approach is that it does not reflect the quantitative difference that can exist between two states that are considered secure.

While security assessment explores the three main areas shown in Figure 2.1, these assessments must be performed in a critical time frame. Figure 2.3 shows the time frames that are applicable to emergency control actions [15].

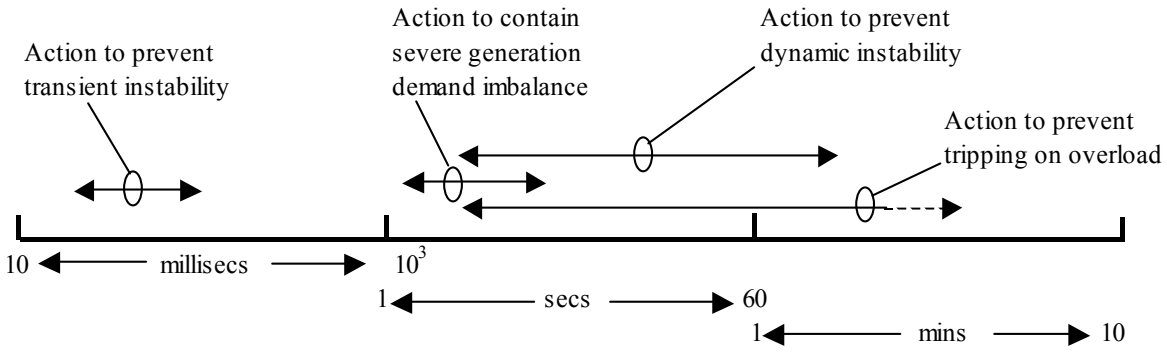

Figure 2.3: Time scales in emergency control actions [15].

The introduction of competitive supply and the accompanying opening of the transmission network have resulted in more highly stressed operating conditions, more vulnerable networks, and an increased need to identify the operational security level of the transmission system.

The determination of the security level, for given operating conditions, has been done traditionally using deterministic method where an operating condition is identified as secure or insecure according to whether each and every contingency in a pre-defined set (the contingency set) satisfies specified network performance criteria. If one or more contingencies cause violations of these operating conditions, then action is taken to move the security level into the secure region. If no contingencies cause violations, then no action need to be taken, or actions can be taken to enhance the economic efficiency of the delivery of energy to end users[16].

Security assessment approaches can be mainly classified either as deterministic or probabilistic. Deterministic methods provide very simple rule for use in making decisions. However, with the industry's emphasis on economic competition, and with the associated increased network vulnerability, researchers have looked for other techniques that can indicate whether the system is sufficiently secure while operating as economically as possible [17].

2.3 Steady State Security Assessments

2.3.1 Deterministic Approach

The current and traditional practice uses deterministic methods with safety margins to cover all the possible unknown uncertainties [13]. In the deterministic security assessment there are six basic steps in constructing a deterministic security boundary. They are [16] ,[18]:

I. Develop a power flow base case corresponding to the time-period (year, season) and loading conditions (peak, partial peak, off peak). Unit commitment is selected based on typical unit availability for the chosen time-period. The

topologies selected are normally all circuits in service. Sometimes sensitivity studies are also performed for a few weakened topologies. In addition, short-term operational studies are often performed with the explicit purpose of identifying limits for topologies expected in the near future.

II. Select the contingency set. Normally this set consists of all 'N-1' events, although some particularly credible 'N-2' events may be included (e.g. two circuits on the same towers). This may be shortened to only include events resulting in performance that is affected by operating conditions or facilities pertinent to the goals of the study. Traditionally, this has been done based on experience and knowledge of the system.

III. Identify the study parameters, which are to be maximised and the study range of operating conditions. These study parameters are typically generation levels for specific generators and power transfers over specific transmission paths.

IV. Identify the event or events that "first" violate the performance evaluation criteria as operational stress is increased within the study range. These events are referred to as the limiting contingencies. If there are no such violations within the study range, the region is not security constrained, and the study is complete.

V. Identify the set of operating conditions within the study range where a limiting contingency "first" violates the performance evaluation criteria. This set of operating conditions constitutes a line that partitions the study range when we consider two study parameters, a surface when there are three study parameters or a hyper surface for more than three study parameters. This line, surface, or hyper-surface is the security boundary.

VI Condense the security boundary into a set of plots or tables that are easily understood and used by the operator. Nomograms are one of the common ways of expressing the security boundaries.

2.3.2 Probabilistic Approach

The power systems have shifted from a regulated system to a competitive uncertain market environment. This has led operators to face more pressure, from economic imperatives in the market place, to operate the power systems with lower security margins. To operate the system closer to the traditional deterministic limits, or even beyond them, more refined methods for power system security assessment are needed that account for the probabilistic nature of uncertain variables in the decision-making environment.[13]

Some researches use analytical approaches (sometimes called contingency enumeration) to solve probabilistic problems, while others use Monte Carlo simulation for the same purpose. Analytical methods based on conditional probability, however, are computationally intensive when applied to a system with many components [9]. Monte Carlo simulation however is suitable for analysis of complicated systems.

In a probabilistic security assessment, steps of I to III and VI remain as in section 2.3.1. However, steps IV and V have to be modified as follows [16, 18]:

IV Evaluate the probabilistic index throughout the study range. Decide on a particular threshold level beyond which operation is deemed unacceptable.

V. Identify the set of operating conditions within the study range that have an index evaluation equal to the threshold level. This set of operating conditions constitutes the line (for two study parameters), a surface (for three) or a hyper surface (for more than three) that partitions the study range. This line surface, or hyper surface represents the security boundary; it delineates between acceptable regions of operation.

2.3.3 Comparison of the Probabilistic and Deterministic Approaches

It is known that probabilistic methods constitute powerful tools for use in many kinds of decision-making problems. Probabilistic assessments play an important part when an outcome is associated with uncertainties. [19]

The acceptance of probabilistic approaches is slow, mainly because they have not acquired the level of credibility, which is accorded to the much simpler and more transparent deterministic methods [20].

There are also several drawbacks with the deterministic approach: [20], [16]

- It ignores the variability in input data.
- The selection of credible contingencies does not include events like cascading tripping of lines or sympathetic tripping. Apparently unlikely conditions may be under estimated.
- The assumption of no failure risk in plans satisfying traditional criteria is misleading; in fact, the approach provides no idea on how safe the operating plan actually is.
- It does not signal on severity of risk beyond the deterministic security boundary.
- It ignores the effects of uncertainty in operating conditions.

These drawbacks can be alleviated with the probabilistic approach because [16]:

- It considers the probability of the possible outages.
- It captures the increased risk caused by multiple constraints as it sums risk associated with all contingencies and problems.
- It can reflect the risk associated with the insecure region.
- It does consider the uncertainty in near future operating conditions.

Therefore, it is also vital to investigate alternative security assessment tools that combine the positive properties of deterministic and probabilistic security indications.

2.4 Dynamic Security Assessment

Dynamic security assessment is the primary concern in systems that are constrained by stability limits. Such assessments are performed at three stages: on-line, operation planning and expansion planning [11].

A real time (on-line) dynamic security assessment: [12]

- Provides the system operator the information on the security status of the system.
- Determines the relevant operating limits (interface flow limits, generation limits) to ensure the dynamic security of the system in the event of occurrence of any critical contingencies.
- Identifies the limiting contingencies and computes indices quantifying the degree of stability or instability for each case.

There are sets of criteria that are to be satisfied with the dynamic security assessment. They are [12]:

- Initial transient stability (plant mode and area mode; single and multi swing).
- Voltage excursions (dip or rise) beyond specified threshold level and duration.
- Relay margin criteria.
- Minimum damping criteria for a designated short list of contingencies.

The security function in a dynamic security assessment computes the interface flow limits that ensure dynamic security of the system for severe contingencies. The interface flows are calculated by performing a series of power flow and time domain simulations.

The basic steps to calculate the interface flow are [12]:

I. Select a desired interface flow

II. Change the generation and load in the appropriate control areas to obtain the

desired interface flow. Solve the power flow. Selection of the generators to change depends on the practices of the utility. Generators are typically dispatched economically.

III. Using time domain analysis (numerical methods such as the implicit trapezoidal method to discretize the differential equations at each time step and iteratively solve the machine equations and the network equations) with early termination, simulate the contingency and compute the transient stability index (TSI). If TSI is within the prescribed (marginally stable) threshold, then the limiting interface flow has been found. Otherwise go to IV step.

IV. Reduce interface flow if unstable (TSI is negative), or increase it if stable (if TSI is positive). Repeat the II and III steps.

The security function captures the interface flow for which TSI is very small and within specified tolerance. The operating guidelines are established based on the most limiting interface flow [12]. If any of the contingencies results in instability, then the operator is notified immediately to take corrective actions.

2.5 Risk Based Probabilistic Approaches in Power System Security

Today, transmission and generation owners are keen to fully utilize their facilities to maximize the return on their investment. Deterministic assessment does not provide sufficient information on insecurity beyond the deterministic boundary. To alleviate such limitations reference [13], proposes a risk based security index that can captures the security level and recognises the likelihood and monetary impacts of unlikely events. The index proposed in [13], measures the system's exposure to failure considering load interruption, equipment damage, and opportunity costs due to equipment outages.

The basic mathematical formulation for calculating the risk is given by Equation (2.1) [13] .

$$\begin{aligned} Risk(\mathrm{Im}|X_t) &= E(\mathrm{Im}(X_{t+1}|X_t) \\ &= \int_{X_{t+1}} \int_{E_i} \Pr(E_i, X_{t+1}|X_t) \times Risk(\mathrm{Im} \mid E_i, X_{t+1}) dE_i dX_{t+1} \end{aligned} \tag{2.1}$$

Where Im denotes the impact or cost-consequences associated with load interruption, equipment damage, or opportunity cost due to equipment unavailability. The risk associated with the pre-contingency operating condition X_t (e.g. loading, dispatch, voltage profile) is given by the expected values of the monetary impact of the operating condition in the next time period X_{t+1} (the next hour) given the current operating condition, i.e., $E(\mathrm{Im}(X_{t+1}) \mid X_t)$. This expectation is the integral of the product of probability of the uncertain event, defined by E_i (the contingency state) and X_{t+1} (operating condition in the next time step) times its corresponding impact over the set of all possible events.

The risk based security assessment proposed in [13] considers the impact of a specified contingency state E_i for a specified operating condition X_{t+1}. Its result is denoted by $Risk(\mathrm{Im} \mid E_i, X_{t+1})$. The set of contingency states $\{E_i, \forall i = 0, N\}$ includes the possibility that the current state remains the same, i.e., an outage does not occur.

The uncertainty associated with the impact depends on the nature of the impact. For line overload, the uncertainty is with the ambient temperature, wind speed and direction, and solar flux [21]. For transformer overload, it is the ambient temperature and transformer's loading cycle [22]. For voltage security it is the interruption voltage level of the loads at each bus [23]. For dynamic (angle) security, it is in the fault type and fault location of the outaged circuit corresponding to contingency state E_i [24],[25].

Reference [13] claims that the following benefits can be achieved using the risk based security assessment when applied to security problems in a power system:

- Since the risk based security assessment is performed through the expected cost due to possible insecurity problems, it can signal the security and economy against a

particular operating condition. Such information is vital in security/economy decision-making as the operator has the option to trade off security with economy.

- Since the risk index may carry the information that may be related to the next minutes, hours, weeks, or years, such information can be used for preventive decisions against future operating conditions.
- Since the risk is assigned considering the problems due to each contingency and each component, it provides vital information to identify particularly risky components or operating conditions.
- Since the proposed risk-based security assessment can be used to calculate a risk index for over load, voltage and dynamic (angle) security problems, it can reflect the composite security level in the region.
- Risk can also be calculated for a time-period by summing over all the time instances for each operating condition. Such information on cumulative risk may be useful in assessing the influence on the security level of a particular facility plan.

2.6 Risk Assessment Techniques in Power System Adequacy

2.6.1 Operating Reserve Risk Assessment

The two broad categories of reserve assessment in composite power systems are the deterministic and probabilistic approaches. Deterministic criteria include considerations such as percentage of system load or operating capacity, fixed capacity margins, and the largest unit loading. Such an approach does not specifically recognize the probability of component failures.

A probabilistic approach can be used to recognize the stochastic nature of system components and incorporate these phenomena in a consistent evaluation of the required operating reserve. The magnitude of the operating reserve and the actual spinning requirement can be determined on the basis of system risk.

This risk has been defined in [26],[27] as the probability that the system will fail to meet the load or be able to just meet the load during a specified time in the future. This

duration is known as the lead time and failed generating units are normally not replaced or restored to service during this time period. In addition, the availabilities and un-availabilities of major system elements are all functions of the studied time period, i.e., the lead-time. The calculated system operating risk is, therefore, a function of the lead-time.

In the basic approach to operating capacity reserve assessment, each generating unit is represented by a two state model as shown in Figure 2.4, which includes an operating state and a failed state. In this model λ and μ are the unit failure and repair states.

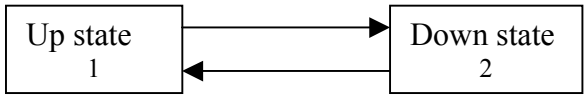

Figure 2.4: Component two state model.

The time dependent availabilities and un-availabilities of the generating units are used to create the capacity outage probability table. The availability and unavailability of a generating unit at lead-time T are given by Equations (2.2) and (2.3) respectively.

$$P_1(T) = \frac{\mu}{\lambda+\mu} + \frac{\lambda}{\lambda+\mu} e^{-(\lambda+\mu)T} \tag{2.2}$$

$$P_2(T) = \frac{\lambda}{\lambda+\mu} - \frac{\lambda}{\lambda+\mu} e^{-(\lambda+\mu)T} \tag{2.3}$$

In addition, the transmission facilities can also be represented by the two-state model that is same as shown in Figure 2.4. The time-dependent state probabilities of these components can therefore be calculated using Equations (2.2) and (2.3). The combined outages of both generation and transmission facilities can then be obtained assuming that these outages are independent.

Risk assessment of composite systems can consider a number of additional constraints such as acceptable voltages at load busses, transmission line load carrying capacities and real and reactive power considerations. In order to calculate the operating capacity risk, the composite power system can be categorised using a group of mutually

exclusive operating states designated in terms of the degree to which the security constraints are satisfied. These operating states include normal, alert, emergency, extreme emergency and restorative.

The composite system risk assessment procedure involves two basic steps: identifying events that lead to each of the operating states and calculating the probabilities of each states resulting from the identified events. According to the definitions of composite system operating states no constraints are violated or load curtailed in either the normal or alert state and therefore the system is not at risk in either of these two states.

A Composite System Operating State Risk ($CSOSR$) can therefore be calculated by Equation (2.4) [27]:

$$CSOSR = 1.0 - P_n - P_a \tag{2.4}$$

Where, P_n and P_a are the probabilities of normal and alert states respectively.

The summation of the two probabilities of the normal and alert states provides an assessment of the favourable conditions associated with the system. The complement of the sum of these two probabilities represents the unfavourable conditions and hence constitutes the system risk level. In this approach the continuous Markov model [28], which can be represented as a discrete process moving in small steps, is used to calculate the required time dependent state probabilities.

2.6.2 Risk Based Assessments of Available Transfer Capability

The knowledge of available transfer capability (ATC) is vital in order to guide the implementation and to make competition effective and reasonable [29].

Mathematically ATC can be represented as in Equation (2.5):

$$ATC = TTC - B\text{ase\_Case\_Flow} - TRM - CBM \tag{2.5}$$

Where, TTC is the total transfer capability, TRM is the transmission reliability margin, and CBM is the capacity benefit margin.

TTC is the largest value of power transfer that causes no violations, with or without contingency. *TRM* accounts for the inherent uncertainty in system conditions and the need for operating flexibility to ensure reliable system operation as system conditions change.

Among the various probabilistic approaches the Monte Carlo simulation has been proposed in [29]. *CBM* is the transfer capability reserved by load serving entities to ensure access to generation from interconnected systems to meet generation reliability requirements.

The general procedure using a combination of Monte Carlo simulation and Repeated Power Flow (RPF),[30, 31] to determine *TTC*/ *TRM* is shown in Figure 2.5.

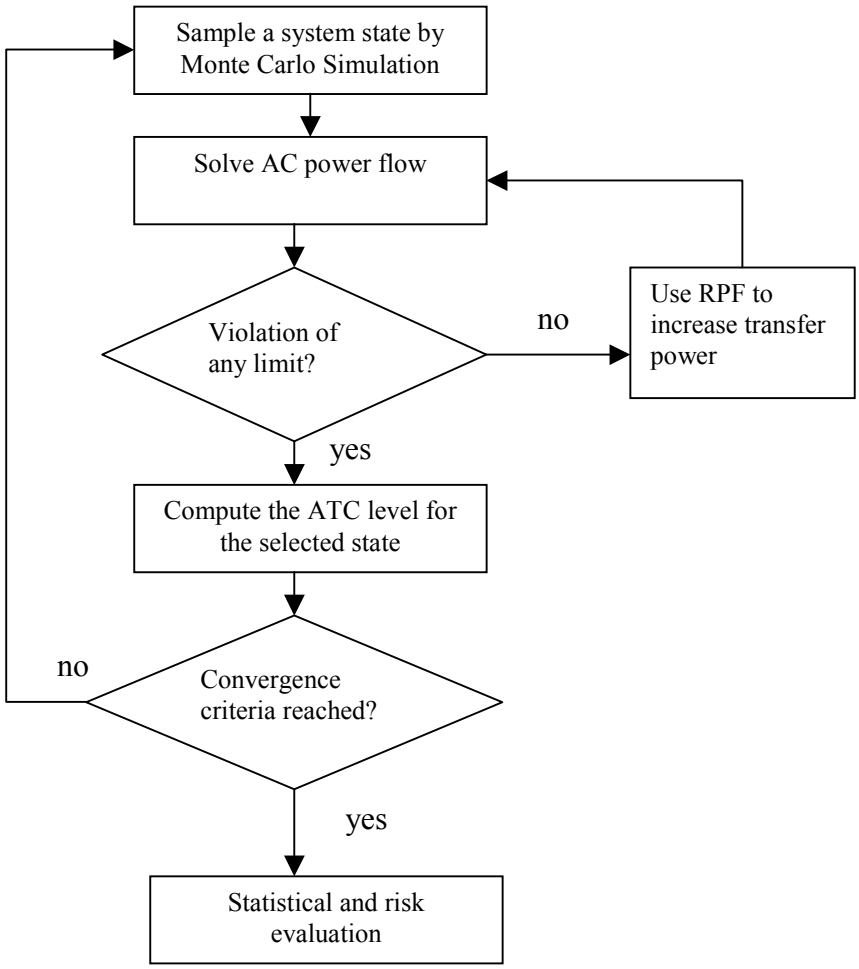

Figure 2.5: General procedure for calculating ATC [29].

In this assessment the risk is defined as [29] :

$$risk(T) = \frac{N(ATC(i) \le T)}{N} = probability(ATC(i) \le T) \qquad (2.6)$$

Where T represents the level of transfer and N represents the number of sampled states and $ATC(i)$ represents ATC level for system state i.

The percentile of a probabilistic variable can be defined as:

$$probability(ATC(i) \le value) = percentile \qquad (2.7)$$

Therefore, reference [29] suggests to use percentile to judge risk.

2.7 Risk Assessment Techniques in Power System Security

2.7.1 Risk of Transmission Line Overload

Power transfer in a transmission conductor is limited by the conductor's maximum design temperature, which determines the maximum sag of the conductor, and the rate of annealing. Annealing is the re-crystallisation of metal. The impacts of thermal overload is calculated considering sag and loss of strength of the conductor and the impacts of sag and loss of strength are given by Equation (2.8) and (2.9) respectively [21].

$$I_{sag}[\theta] = \begin{cases} I[Fault] & \theta > \theta_{\mathrm{L}} \\ 0 & otherwise \end{cases} \qquad (2.8)$$

$$I_{anneal}[\theta] = \begin{cases} \dfrac{\Delta t}{t_0} \times C_t & \theta > \theta_{\mathrm{MDT}} \\ 0 & otherwise \end{cases} \qquad (2.9)$$

Where,

$I_{sag}[\theta]$ = Impact of sag

$I[Fault]$ = Impact (or financial cost) corresponding to an outage of the overload circuit

θ_{L} = Limiting temperature

θ_{MDT} = Maximum design temperature

θ = Conductor temperature

$I[anneal]$ = Impact of annealing

Δt = Decrease in expected life of the conductor
t_0 = Expected remaining life of theconductor
C_t = Cost of re - conducting the circuit

$I[Fault]$ is dependent on operating conditions, and its quantification requires analysis with power flow and stability simulation.

For a given current I, the thermal overload risk can be expressed as the probability of the conductor temperature being greater than θ_{MDT} times its related impact. It is given by Equation (2.10) [21]:

$$R[I] = \int_{\theta > \theta_{mdt}} P[\theta \mid I] \times (I_{sag}[\theta \mid I]) d\theta \tag{2.10}$$

The conductor temperature θ is influenced by the conductor current I and the ambient conditions. $P[\theta \mid I]$ is the probability density function of θ for given I, $I_{sag}[\theta \mid I]$ is the impact of sag of θ for given I, and $R(I)$ is the risk of line overloading.

2.7.2 Risk of Transformer Loading

Reference [22], proposes a risk assessment technique for transformer loading capability, taking into account the probabilistic nature of time-varying loads and ambient temperature. In a transformer the loading capability is limited by the temperature of the winding and the insulation. This condition is characterised by the winding hottest spot temperature (HST).

In the analysis of risk, the load and ambient temperature can be considered as uncertainties and Monte Carlo simulation can be used to calculate the probabilistic distribution of the winding HST. Loss of life and the failure probability of the transformer are calculated based on the transformer HST. The total risk for the transformer is obtained by summing the product of probability and the corresponding consequences over all possible HST levels. Consequences are measured in terms of loss of life and transformer dielectric failure.

Figure 2.6 shows the risk calculation procedure of transformer loading.

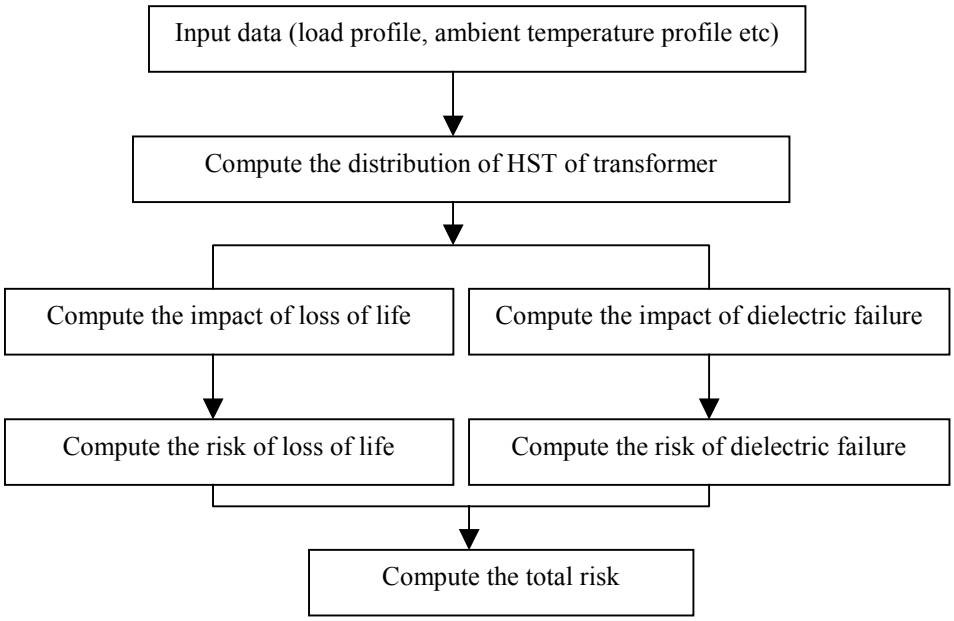

Figure 2.6: The procedure for calculation of transformer loading risk [22].

The probabilistic model proposed in [22] is based on the following assumptions:

- The load forecasting errors, and temperature uncertainty caused by weather forecasting error are assumed normally distributed.
- The loading profiles are correlated with ambient temperature profiles. For example in winter the correlation between load and temperature is negative and in summer it is positive.
- The distribution of ambient temperature and load over each hour is assumed multi-variate normal (MVN) [32].

The impact on loss of life is measured through the cost of re-winding the transformer and the expected percentage of transformer remaining life. The impact associated with transformer failure is calculated through the cost of replacing transformer capacity, which includes loss of load, loss in produced energy, and penalties.

The total impact of transformer thermal overloads includes the impact of both loss of life and failure. Under a specified operating condition X, which is a function of t, the risk over a period of T is calculated using Equation (2.11).

$$Risk(\mathrm{Im} \mid X) = Risk(\mathrm{Im}_1 \mid X) + Risk(\mathrm{Im}_2 \mid X) \tag{2.11}$$

Where, $Risk(\mathrm{Im} \mid X)$ is the risk corresponding to the operating condition X, $Risk(\mathrm{Im}_1 \mid X)$ is the risk of loss of life due to thermal overloading corresponding to the operating condition X, and $Risk(\mathrm{Im}_2 \mid X)$ is the risk of transformer failure corresponding to operating condition X.

The risk corresponding to loss of life due to thermal overloading is given by Equation (2.12).

$$Risk(\mathrm{Im}_1 \mid X) = \int_0^T \int_{\theta_0}^{\theta} \Pr(\theta \mid X) \times \mathrm{Im}_1(\theta) d\theta dt \tag{2.12}$$

Where, $\Pr(\theta \mid X)$ is the probability density function of θ (absolute temperature) given X (operating condition), and $\mathrm{Im}_1(\theta)$ is the impact due to loss of life of thermal overloading.

The risk corresponding to transformer dielectric failure is given by Equation (2.13).

$$Risk(\mathrm{Im}_2 \mid X) = \int_0^T \int_{\theta_0}^{\theta} \Pr(\theta \mid X) \times H(t \mid \theta) \times \Delta t \times \mathrm{Im}_2 d\theta dt \tag{2.13}$$

Where, Im_2 is the impact associated with transformer failure, $H(t \mid \theta)$ is the hazard function and Δt is the difference between transformer insulation loss of life at the hottest spot temperature (θ_0) and the absolute temperature (θ).

2.7.3 Annual Risk of Transmission Line and Transformer Overload

Reference [33] proposes a risk assessment method for overload security considering transmission lines and transformers. The cumulative risk of this effect is calculated using a sequential model where a series of hourly snap-shots, sequential in time is evaluated and summed to produce the resulting indices.

Trajectories of operating conditions are formed using the expected annual load curve by sampling on an hourly basis to arrange the maintenance and unit commitment schedules and then employing time invariant variances to represent normally distributed load uncertainties.

Figure 2.7 shows the procedure of trajectory development and annual thermal overload risk assessment framework.

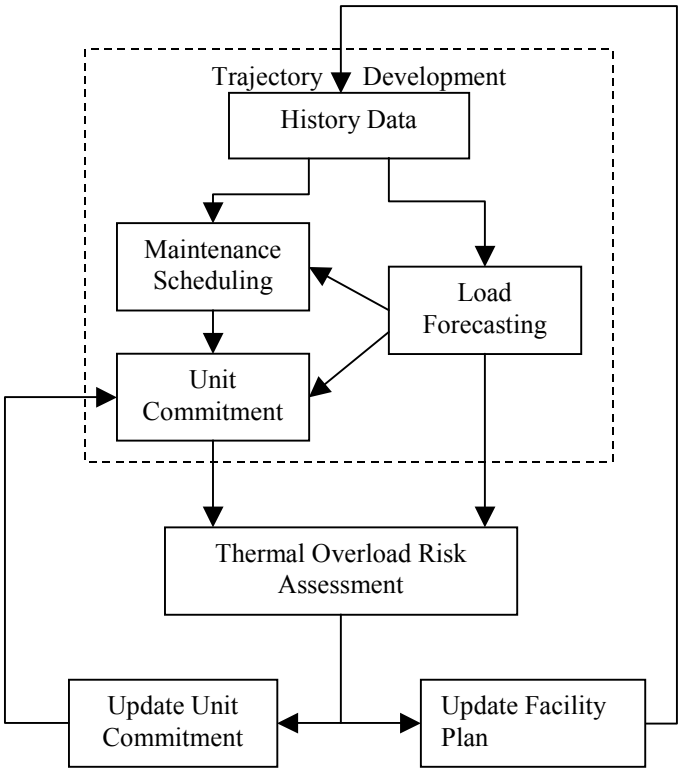

Figure 2.7: Annual thermal overload risk assessment framework [33].

The proposed approach models a series of 8760 samples, one per hour over a year, knowing the committed generation units, their despatch and probability density function (pdf) for the load.

Then the thermal overload risk (TOL) for a particular contingency state s in hour h can be calculated using the Equation (2.14).

$$Risk(TOL \mid h,s,b,\Omega) = \int_{-\infty}^{\infty} \Pr(I_b \mid h,s,\Omega) \times Risk(TOL \mid I_b) dI_b \qquad (2.14)$$

Where, Ω denotes 8760 samples, h denotes a single hour, b denotes a single branch, $\Pr(I_b \mid h, s, \Omega)$ denotes probability density function for the current flow on branch b, and $Risk(TOL \mid I_b)$ gives the expected monetary impact of each flow I_b on branch b.

The total risk for this branch in hour h over all contingency states is:

$$Risk(TOL \mid h, b, \Omega) = \sum_{s} \Pr(s) Risk(TOL \mid h, s, b, \Omega) \tag{2.15}$$

Where, $\Pr(s)$ is the probability density function of current flow at contingency state s.

Then the total cumulative risk for of all hours in all branches can be calculated using Equation (2.16).

$$Risk(TOL \mid \Omega) = \sum_{h} \sum_{b} Risk(TOL \mid h, b, \Omega) \tag{2.16}$$

The component risk, $Risk(TOL \mid I_b)$, can be calculated using the Equation (2.17).

$$Risk(TOL \mid I_b) = \int_{\theta} f(\theta \mid I_b)[I_{m_{L1}}(\theta) + I_{m_{L2}}(\theta)]d\theta \tag{2.17}$$

Where $I_{m_{L1}}(\theta)$ and $I_{m_{L2}}(\theta)$ express the monetary impact on the transmission line of sag and annealing respectively, as a function of conductor temperature θ. $f(\theta \mid I_b)$ is the probability density function for conductor temperature θ.

The probability density function of currents can be identified by probabilistic load flow methods [34],[35],[36],[37]. In this approach the system is linearised around the operating point at every hour and then a convolution method is used to obtain probability density function of current flows of all lines and transformers. Then these probability density functions are combined with component risk curves to get the decomposition risk assessment for every line and every transformer in every hour.

2.7.4 Risk of Special Protection Systems

Special protection schemes (SPS) are designed to detect abnormal system conditions and to use corrective action to mitigate the consequence of the abnormal conditions. SPS can provide rapid corrective actions and are often used to increase the transfer

capability of the network because with that the system can securely operate at a higher level of stress than it can operate if the system is in danger. However, excessive reliance on SPS can result in increased risk because SPS are normally armed only under stressed conditions and when their failure would result in very severe consequences. Another risk with SPS is the risk caused by failure to operate when required.

Figure 2.8 shows the basic steps used in risk assessment of SPS [38].

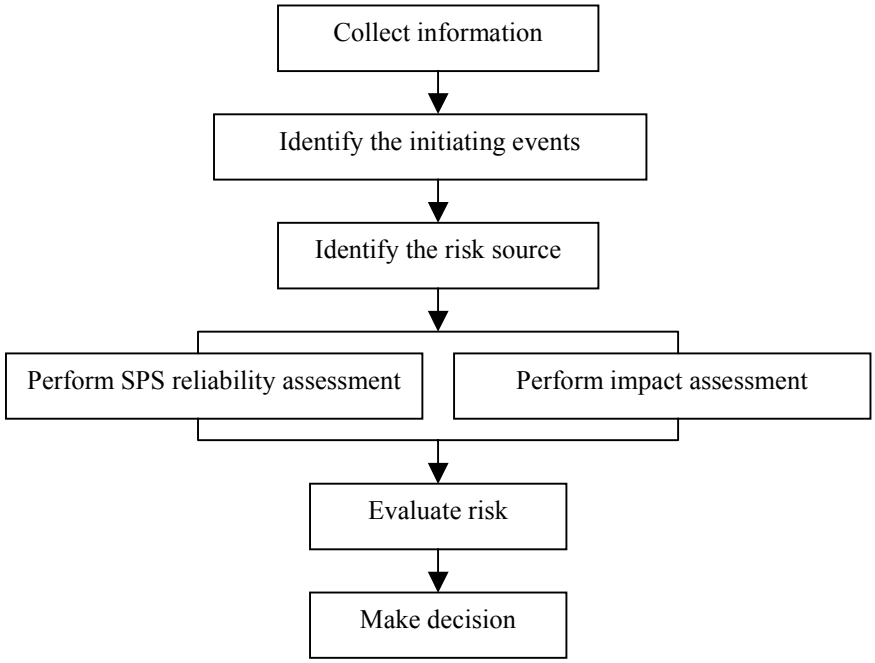

Figure 2.8: Procedure for SPS risk assessment [38].

At first, the information on physical layout of power system, operating logic, functions of each physical part, location, success criteria, embedded software information as well as maintenance and test procedures are gathered. The initiating events considered in this assessment are line outages, generator trippings, and load dropping. Sources of risk are hardware failure, fault design logic, software failure and human error. Markov modelling is used for SPS reliability assessment as the Markov modelling can incorporate independent and common cause failures, partial and full repairs, maintenance and diagnostic coverage.

Consequences due to SPS failure need to be estimated in terms of financial losses, i.e., the total cost associated with the SPS failure. The impact can be equipment damage, equipment outage, load interruption and penalties. Under evaluation of risk, both risk with and without SPS is calculated using the product of probability and impact concept and a decision is made on when and whether to arm the SPS.

2.7.5 Voltage Security Assessment

Voltage collapse typically occurs in power systems, when they are heavily loaded, weakened by transmission outages, or subjected to reactive power shortages. Reference [23] proposes a method to calculate the risk of voltage insecurity for a given short term operating condition.

There are two situations where the system either may reach a voltage collapse condition or it may remain voltage stable after disconnecting some of the system loads. In the case of no-collapse condition, the system suffers a load disconnection by responding to under voltage condition. On the other hand under some conditions, the system may approach a voltage collapse although all voltages are close to their nominal values.

Considering both of these conditions, the risk can be expressed as [23]:

$$\begin{aligned} R(X_0) &= E[I \mid X_0] \\ &= P(Collapse \mid X_0) \times E[I(Collapse)] + [1.0 - P(Collapse \mid X_0)] \times E[I(NoCollapse)] \end{aligned} \tag{2.18}$$

Where, X_0 stands for the current operating condition, I stands for the impacts, $P(Collapse \mid X_0)$ stands for the probability of collapse at operating point X_0, $E[I(Collapse)]$ stands for the expected impacts of collapse, $E[I(NoCollapse)]$ stands for the expected impact of no voltage collapse.

Under a given topology determined by a contingency, when both the load level L and the maximum loadability L_{mi} are random, the probability of voltage collapse is the probability that the load margin $M_i = L_{mi} - L$ is negative. Since L and L_{mi} are both

normally distributed, the resultant load margin M_i will also be normal, with a mean of μ_{mi} and a variance σ_{mi}. Therefore, the probability of collapse at the occurrence of i^{th} contingency E_i is given by [23]:

$$P(Collapse \mid E_i) = P(M_i < 0 \mid E_i) \tag{2.19}$$

$$M_i \sim N(\mu_{mi}, \sigma_{mi}^2) \tag{2.20}$$

The total probability of voltage collapse under the system exposed to uncertain contingencies is given by [23]:

$$P(Collapse) = \sum_{E_i} P(Collapse \mid E_i) \times P(E_i) \tag{2.21}$$

Where, $P(E_i)$ is the probability of occurrence of contingency i.

The issues highlighted with voltage collapse and no-collapse must also be considered for calculating the impacts. The service interruption at a bus occurs when the bus voltage is beyond the sustainable range of the individual load. With $K_{bus,c}$ as the percentage share of a load class c at a particular bus, the impact on the interrupted load is its service interruption cost multiplied by its interruption amount.

Therefore, the impact on the interrupted load is given by [23]:

$$I_{bus}(V_{bus}) = P_{bus} \sum_{c} C_{bus,c} \times K_{bus,c} \times I(V_{L,C} > V_{bus} \mid V_{bus}) \tag{2.22}$$

Where,

P_{bus} = Forecasted amount of load at a particular bus

$C_{bus,c}$ = Interruption cost associated with the load class c at the bus

$V_{L,C}$ = Lower limit of the sustainable voltage class c

$I(V_{L,C} > V_{bus} \mid V_{bus})$ = A zero to one indicator function that equals one when $V_{L,C} > V_{bus}$ holds or zero otherwise.

Then the expected impact on load with a given voltage is given by [23]:

$$E[I_{bus} \mid V_{bus}] = E[P_{bus}] \sum_{c} E[C_{bus,c}] \times K_{bus,c} \times P(V_{L,C} > V_{bus} \mid V_{bus}) \tag{2.23}$$

Where, the independence of $P_{bus}, C_{bus,c}$, and $V_{L,C}$ is assumed. $E[P_{bus}]$ is the expected value of the forecasted load at the corresponding bus.

Under the exposure to the uncertain load level and contingencies, the expected impact of voltage out-of-limits, when the voltage does not collapse is given by [23]:

$$E[I(NoCollapse)] = \sum_{E_i}(\int_{L} E[I \mid L, E_i] \times P(L)dL)P(E_i) \tag{2.24}$$

Where, $P(L)$ is the probability of load level, $P(E_i)$ is the probability of a contingency, and $E[I \mid L, E_i]$ is the expected voltage impact for a study system with a given load level and given contingency.

For the impact when voltage does collapse, it is assumed that the voltage collapse results in a system blackout. Then, the expected impact due to entire system load-interruption is [23]:

$$E[I(Collapse)] = \sum_{bus}(P_{bus}\sum_{c} C_{bus,c} \times K_{bus,c}) \tag{2.25}$$

Where, $K_{bus,c}$ is the % load sharing of load sector c.

2.7.6 Risk of Transient Instability

Transient stability is the ability of the power system to maintain synchronism when subjected to a severe transient disturbance such as a fault on a transmission facilities, a large change in interface flow or loss of a large load [10],[39].

Reference [24] describes a probabilistic index of system risk that reflects the probability of instability due to single-phase, two-phase and three-phase faults on a transmission system. The proposed method also recognises the risk as the product of probability of instability and the consequences.

The probability of occurrence of an event over a time-period can be expressed as:

$$P(K_{jip}) = P(E_i) \times P(K_{jip} / E_i) \tag{2.26}$$

Where,

K_{jip} = Event instability *j* due to event *i* at operating point *p*

$P(K_{jip})$ = Probability of occurrence of this event over a specified time period.

E_i = Event line outage over transmission circuit *i* over a time period

$P(E_i)$ = Probability of this event

To calculate the conditional probability of instability, assume that a fault may occur anywhere on a line with the same probability of occurrence. Therefore, using a uniform probability distribution function, the probability of instability *j* given that event *i* (outage of event *i*) is caused by an *n*-phase ($n\phi$) fault on circuit *i*, is given by:

$$P(K_{jip} / n\phi\_fault) = \int_{l_{jip}} \frac{1}{L_i} dx = \frac{l_{jip,n\phi}}{L_i} \tag{2.27}$$

$l_{jip,n\phi}$ is the maximum distance from the worst case location for which an *n*-ϕ fault results in an unstable response (Or minimum distance from the worst case location for an *n*-ϕ fault result in a stable response).

For a transient instability problem, the worst-case location is normally the bus nearest to the machine at risk of losing synchronism. Figure 2.9 illustrates the maximum distance function for a 3ϕ fault.

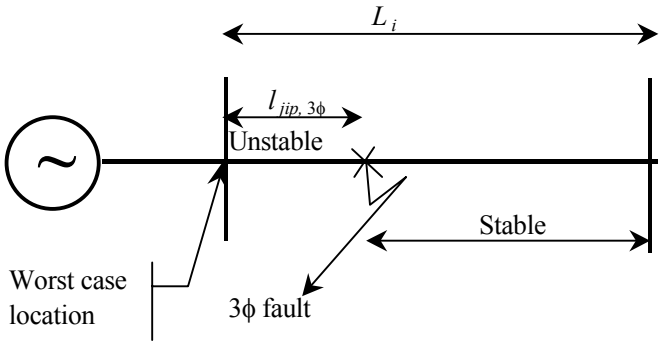

Figure 2.9: Illustration of maximum distance function $l_{jip,3\phi}$.

Assume that the events are mutually exclusive and exhaustive events. Using the law of total probability, the probability of instability *j* due to event *i* at point *p* is given by:

$$\begin{aligned} P(K_{jip}) &= \sum_{n=1}^{3} P(n\phi\_fault) \times P(K_{jip} / n\phi\_fault) \\ &= \sum_{n=1}^{n=3} P(n\phi\_fault) \frac{l_{jip,n\phi}}{L_i} \end{aligned} \tag{2.28}$$

$$\begin{aligned} P(n\phi\_fault) &= P(E_i) \times P(n\phi\_fault / E_i) \\ &= P(E_i) f_{n\phi} \end{aligned} \tag{2.29}$$

Substituting Equation (2.29) in Equation (2.28) gives:

$$P(K_{jip}) = P(E_i) \sum_{n=1}^{3} f_{n\phi} \left(\frac{l_{jip,n\phi}}{L_i} \right) \tag{2.30}$$

The impact of instability is defined in terms of energy not supplied and the social political impacts of such an event.

The energy not supplied can be modelled as:

$$B_{jip} = \frac{P_{lost_{jip}} \times T_{lost_{ji}}}{P_{peak}(1hour)} \tag{2.31}$$

Where, $P_{lost_{jip}}$ = Generation level of unit lost

P_{peak} = Peak load of the system

$T_{lost_{ji}}$ = Time required to synchronise and load the lost units

The per-unit base of this analysis is defined as the energy supplied to the entire system for an hour under peak condition.

The Social/ Political impacts can be modelled as:

$$C_{ji} = \sum_{s \in i} C_{jis} \tag{2.32}$$

Where, C_{jis} = Impact factors giving the percentage increase over the energy replacement impact for a specific impact s.

Therefore, the total impact of instability j resulting from a contingency i at operating point p is the energy impact increased by the percentage 100 (C_{ji}) %, i.e.,

$$I_{jip} = B_{jip}\,(1+C_{ji}) \tag{2.33}$$

The $(1+C_{ji})$ social/political weighting is based on a subjective assessment and is approximate.

The composite risk can be given by:

$$R_{jp} = \sum_{i=1}^{M} R_{jip} \tag{2.34}$$

Where, R_{jp} = Composite risk at an operating point p associated with a particular instability j.

Therefore,

$$R_p = \sum_{j=1}^{N} R_{jp} = \sum_{j=1}^{N} \sum_{i=1}^{M} R_{jip} \tag{2.35}$$

Where, N = Different instabilities

M = Different events

R_p = Composite risk at an operating point p, associated with several different instabilities.

This computed risk index is useful for making decisions related to operating limits or it can be used to compare alternatives for enhancing stability performance. It also enables dynamic security to be assessed and compared together with overload and voltage security.

2.7.7 Composite Risk of Power System Security

The composite risk can be calculated using the risk of transmission line overload [21], risk of transformer overload [22], voltage collapse [23], voltage out-of-limit [23], and transient instability [24],[40] for defined operating conditions by summing each of the risk as all of these risks have the same unit of $/hr [22]. Such an evaluation is useful to system operators for monitoring the overall system stress.

2.7.8 Risk Based Approach for Maintenance and Scheduling

Reference [41] proposes a method for estimating the cumulative long-term risk of maintenance allocation and scheduling of transmission equipments including plants in large power systems. This approach considers equipment failure probability, equipment damage as well as the consequences of outage in terms of overload and voltage security. The objective is to optimise economic resources and maintenance activities in a bulk transmission system to mitigate the consequences of component failures.

A cumulative risk assessment is useful in evaluating the system from an operation planner's perspective. It performs a sequential, hourly simulation over a long term (e.g. an year), and it evaluates security levels in terms of quantitative indices, reflecting the risk of overload, of cascading overload, of low voltage, and of voltage instability. The risk index R is an expectation of severity, computed as the product of probability $p(c)$ of contingency c with contingency severity $sev(c \mid m,t)$, where m indicates the m^{th} maintenance activity (and thus the network configuration in terms of network topology and unit commitment), and t indicates the hour (and thus the operating conditions in terms of loading and despatch), given by $R(c,m,t) = p(c)sev(c \mid m,t)$. The severity function captures the contingency severity in terms of overload, cascading overload, low voltage, and voltage instability.

The risk associated with any given network configuration and operating condition is computed by summing over the no-contingency condition $(c = 0)$ and all N contingencies as:

$$R(m,t) = \sum_{c=0}^{N} p(c)sev(c \mid m,t) \tag{2.36}$$

Figure 2.10 shows the functions of integrated maintenance scheduler and selector where the risk reduction calculations are performed after the maintenance activity as the approach assumes that maintenance decreases the probability of failure of that equipment. It also assumes that during the maintenance there is a possibility for an increase in risk due to out of service equipment due to maintenance as they can limit

system resources. These calculations are performed until the end of the study period (e.g. a year).

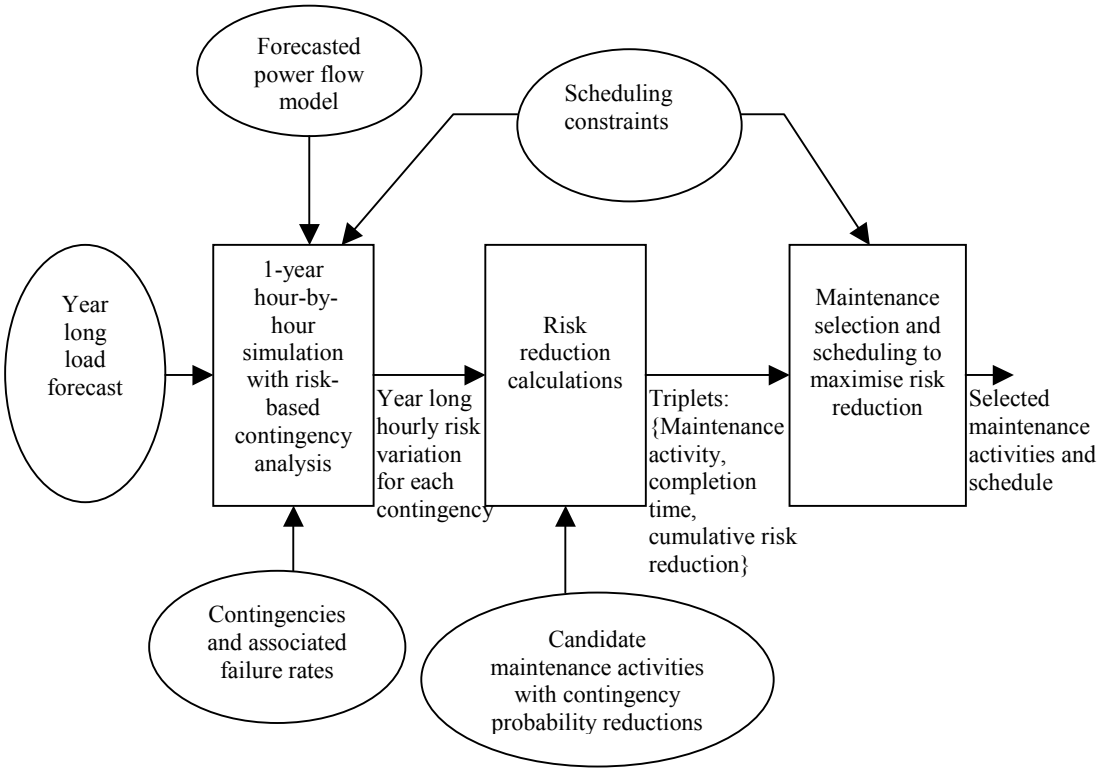

Figure 2.10: Integrated maintenance selector and scheduler [41].

Risk maximisation in Figure 2.10 is achieved by an optimisation where the inputs are maintenance activity, completion time and risk reduction. The optimisation problem formulation has flexibility in scheduling the maintenance activities for generation and transmission equipments simultaneously or sequentially. Simultaneous scheduling is more attractive because it results in a global optimum. Sequential scheduling reduces complexity.

2.7.9 Online Risk-Based Security Assessment

Reference [42] proposes an on-line risk-based security assessment to provide rapid online quantification of the security level associated with an existing or forecasted operating condition. This approach also condenses contingency like hood and severity into indices that reflect probabilistic risk. The proposed approach performs using the

analysis for near future operating conditions whereas the traditional online security assessment performs the analysis considering the past conditions.

In this approach the assessments are limited to overload security (flow violations and cascading overloads) and voltage security (voltage magnitude and voltage instability).

Figure 2.11 illustrates the basic online risk based security assessment process.

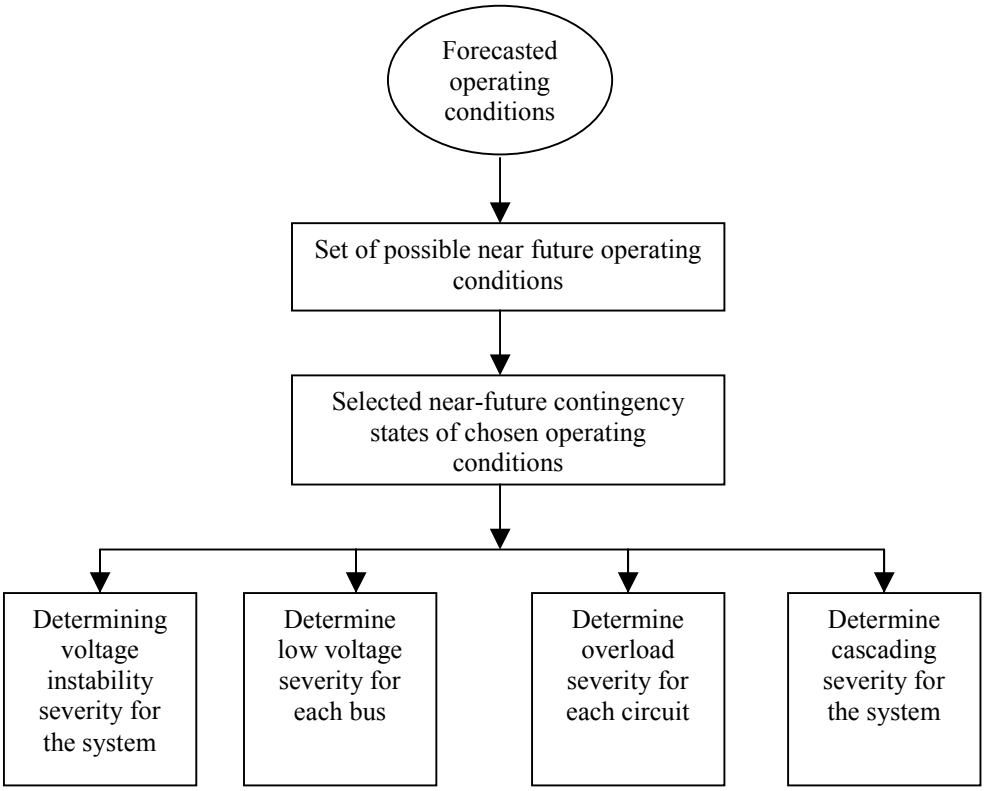

Figure 2.11: Illustration of basic online risk based security assessment process [42].

In Figure 2.11, if the probabilities are assigned to each state, then the probability of each terminal state is the product of the probabilities assigned to each state that connect the initial state to that terminal state. If the severity values to each terminal state is assigned, the risk can be calculated as the sum over all terminal states of their product of probability and severity as shown in Equation (2.37).

$$Risk(X_{t,f}) = \sum_i \Pr(E_i)(\sum_j \Pr(X_{t,j} \mid X_{t,f}) \times Sev(E_i, X_{t,j})) \qquad (2.37)$$

Where, $X_{t,f}$ is the forecasted condition at time t, $X_{t,j}$ is the j^{th} possible loading condition, $\Pr(X_{t,j} \mid X_{t,f})$ is the probability of load forecasted uncertainty, E_i is the i^{th} contingency and $\Pr(E_i)$ is its probability. $Sev(E_i, X_{t,j})$ quantifies the severity, or consequences of the i^{th} contingency occurring under j^{th} possible operating condition. It represents the severity for overload, low voltage, voltage instability, and cascading overload.

Reference [42] proposes several severity functions. They are:

- Severity function for low voltage (the voltage magnitude of each bus determines the low-voltage severity of that bus). Under this there are three types of severities. The discrete severity function assigns one if the voltage magnitude is lower than the low voltage rating, and zero otherwise. It can reflect only that violations exist and not the extent of the violation. The percentage severity function measures the voltage magnitude with respect to the lower voltage level and estimates a percentage of violation. In the continuous severity function a fall in voltage magnitude linearly increases the severity.
- Severity function for overload determines the power flow with respect to the rating of transmission line or transformers.
- Severity function for voltage instability is a system-wide severity function. It uses a loadability corresponding to the system bifurcation point to determine the voltage instability severity.
- Severity function for cascading overloads: Cascading is a sequential succession of dependent events. With the assumption that a circuit will be outaged if its MVA flow exceeds *K* times its emergency overload rating, following steps are used to calculate the severity function for cascading overloads.

  I Identify all circuits having flows exceeding *K* times their emergency overload rating.

  II Remove these circuits, and resolve the power flow

  III Repeat steps I and II until one of the following conditions are met.

  a) No circuits are identified in step I

  b) The power flow solution procedure diverges in step II

c) The procedure exceeds a pre-specified number of iterations of step I and II

2.7.10 Further Aspects of Risk Based Approaches

Another important part of power system security is the security constrained optimum power flow. In a traditional optimum power flow, the criteria that is minimised is the generation cost subject to power flow equations, generation limits, branch flow & bus voltage constraints together with other security constraints. In a risk-constrained optimum power flow it is necessary to integrate the risk in to the equality and inequality constraints. The problem then takes the following form [7]:

Minimise: a (generation cost) + b (total system risk)
Subject to:

- Power flow equations
- Generation limits
- Regional risk constraints

Where a and b represents the multipliers of generation cost and total system risk respectively. The risk-integrated Optimum Power Flow is still under the research and no publications are yet available.

2.8 An Alternative Form of Probabilistic Approach

Traditionally, system security is assessed by simulating a set of contingencies without regard to the numerical probabilities of the contingencies. The relative like hood of contingencies is considered loosely by recognising that single outages 'N-1' are more likely than double outages 'N-2' and that generator outages are more likely than line or transformer outages. Therefore, to limit the contingency analysis to a reasonable number, typically single outages and some limited set of double or multiple outages are used [43].

Reference [43] proposes an alternative probabilistic risk assessment method that can provide an objective basis for trading off reliability with economics via a risk-based power system operation. In [43], the risk is defined as:

$$RI = \sum_{i \in \{simulated\_situations\}} P_i \times I_i \tag{2.38}$$

In Equation (2.38) the P_i represents the situation probability and I_i represents the impact.

In Equation (2.38) the situation probability describes the probability of initiating events or contingencies that could lead to violations of operating security limits causing impacts.

Proposed technique in [43] calculates separate security boundaries for outage of each elements in the power system. Each of these boundaries has a situation probability that is determined by the outage of corresponding element. These situation probabilities are used to calculate the situation probability of a particular boundary that is constrained by outage of corresponding elements in the power system.

For example in a power system if only Line A and Line B are the possible outages and if line A and Line B have the outage probabilities of 0.01 and 0.05 respectively then the probability of all lines are in service becomes 0.9405 (=0.99x0.95). The probability of outage of Line A and in-service of Line B becomes 0.0095 (=0.01x0.95). The probability of in-service of Line A and outage of Line B becomes 0.0495 (=0.99x0.05). The probability of outage of both lines becomes 0.0005 (=0.01x0.05). In this way, the probability of no constraint violation at the deterministic security boundary results as 1.0 (i.e., 0.9405+0.0095+0.0495+0.0005=1.0) or in other words the situation probability of deterministic security boundary is zero.

Impacts are calculated through the economic value of reliability of operating conditions that violate security constraints.

Risk indices together with study parameter (e.g. load level and amount and directions of power transfers that take place across the study area) are represented in a contour plateau.

Reference [43] claims that with this approach the operator can consciously trade off risk with dollars (i.e., how is increased risk associated with heavier use of facilities offset by the corresponding increase in benefit [23]) in operating beyond the conservative and deterministic contingency criteria.

2.9 Discussion

There is limited number of publications available in the area of power system security with the emphasis on power system operations exploring the probabilistic approaches to catch uncertain system events that affect system security. In some of these publications the system security is analysed through risk-based approaches where the risk is measured through constraint violations. Such approaches do not indicate complete system security. For example an under-voltage condition will not necessarily result in a voltage collapse condition.

On the other hand, weather conditions also play a vital role with regards to power system security. The published risk assessment approaches related to power system operational security have not considered or have neglected this influence. In addition, reflecting the risk as product of probability of events and their impacts does not necessarily reflect system security, as the concept is erroneous under certain circumstances. For example the probability of a system blackout is very low, however, its impacts disastrous. If the concept of product of probability and impact is applied to measure the risk, then the same risk can also be achieved with a high probabilistic event that has lower consequences, as the risk formulation is linear. In reality these two situations are entirely different in terms of social and financial impacts.

It is more appropriate to measure the impact of a contingency by the actual damage that it produces, i.e. by the amount of load disconnection that it might cause; as such an

approach can incorporate various external influence for assessing the power system security. [3]

The other way of assessing system security is through the value of security/benefit approach taking into account probability of various random events [44]. Such an approach uses the amount of load disconnection and incorporates weather conditions. The importance of such assessments is highlighted in [45].

The first project (i.e., "A method for computing the value of security in power system operations") assessed the level of security in a power system through costs of security. Cost of security is estimated with random distribution of contingencies using the Monte Carlo simulation. This project set out to demonstrate that a probabilistic method capable of estimating the expected cost of outages and hence comparing various levels of security could be developed [46],[47].

Cost of security is a realistic way of measuring the power system security particularly in an operational time frame as it reflects the actual damage imposed on the connected customers.

The research project that is described in this thesis is an extension of the first project (i.e., "A method for computing the value of security in power system operations"). It investigates the security tools that can warn system operators against stressed operating conditions. Probabilistic assessment techniques that are published in the literature do not quantitatively measure the level of stress in a power system. Use of indices, which do not indicate levels of stress in a power system quantitatively are not capable of warning operators on stressed operating conditions. In this context, a power system can reach a very problematic state undetected by the operator. This highlights the importance of security tools that can measure the system stress quantitatively. Probabilistic indicator of system stress proposed in Chapter 4 measures the system stress quantitatively. Monte Carlo simulation and Correlated Sampling mainly involve in calibrating and testing the indicator of stress.

On the other hand probabilistic tools are complicated for system operators to work with due to their complex interpretation of system security. Tools that operate adaptively to operating points, but still reflect the system security in deterministic terms are certainly worth investigating. To provide operators with a probabilistic measure of security similar to the deterministic security criteria, adaptive deterministic security criteria are proposed in chapter 6. These criteria integrate the probabilistic cost of security and deterministic security boundary for the calculation of adaptive deterministic security boundary (ADSB). The ADSB adapts to operating conditions in a power system. The power system operators can use ADSB to identify feasible, secure and economical operating conditions.

Some of the routes for establishing the contour plot of index of risk in [43] and the contour plot of cost of security established in chapter 5 are similar. However, the formulation used in [43] (i.e., Equation (2.38)) is erroneous as the product of probability and impacts does not always reflect the risk in a power system. With the approach proposed in [43], the risk within the deterministic security boundary results as zero. However, there is a value for cost of security along the deterministic security boundary. A clear evidence of this fact is presented in chapter 5.

Use of dynamic security assessment for the estimation of costs of security requires detailed modelling of dynamic nature of contingencies in a power system. Detailed modelling of dynamic contingencies demands significantly high CPU time. This is because it increases the complexity for a precise estimation of costs of security through the Monte Carlo simulation.

In an operational time frame, the processing time is a crucial fact, and the operators are to be signalled on the level of system security in a shortest possible time to avoid disastrous consequences. Dynamic security assessment indicates whether a system is fully secured demanding a significantly high CPU time where as the static security assessment provides an outcome in a relatively lower CPU time and the static outcome also provides a measure of the level of security in a power system.

Since the indicator of stress proposed in chapter 4, comparison of deterministic and probabilistic security criteria presented in chapter 5, and the adaptive deterministic security criteria proposed in chapter 6 base power system operation the research in this thesis focuses on static security assessment.

2.10 References

[1] R. Billinton and W. Li, *Reliability Assessment of Electrical Power Systems Using Monte Carlo methods,* New York; London: Plenum Press, 1994.

[2] R. Billinton, M. F. Firuzabad, and S. Aboreshaid, "Power System Health Analysis," *Electric Power Systems Research*, vol. 55, pp. 1-8, 1997.

[3] D. S. Kirschen, "Power System Security," *Power Engineer*, vol. 16, pp. 241-248, 2002.

[4] U. G. Knight, *Power Systems in Emergencies: From Contingency Planning to Crisis Management,* England: John Wiley & Sons Ltd, 2000.

[5] G. Strbac, "MSc Course Materials on Power System Security," University of Manchester Institute of Science and Technology, Manchester, UK, March 2001.

[6] L. Wehenkel, "Machine Learning Approaches to Power System Security Assessment," in *IEEE Intelligent Systems Magazine*, vol. 12, 1997, pp. 60-72.

[7] J. D. McCalley, "Security Assessment: Decision Support Tools for Power System Operators," Iowa State University, Ames, Iowa, 5th September 2000.

[8] D. Kirschen, "MSc Course Materials on Power System Operation - Introduction and Overview," University of Manchester Institute of Science and Technology, Manchester, UK, March 2001.

[9] Y. H. Kim and C. Singh, "Probabilistic Security Analysis Using SOM Monte Carlo Simulation," *IEEE Transactions on Power Systems*, vol. 2, 2002.

[10] L. L. Grigsby, *The Electric Power Engineering Handbook*. USA: A CRC Handbook Published in Cooperation with IEEE Press, 2001.

[11] A. M. L. D. Silva, J. L. Jardim, A. M. Rei, and J. C. O. Mello, "Dynamic Security Risk Assessment," *IEEE Transactions on Power Systems*, pp. 198-205, 1999.

[12] G. C. Ejebe, C. Jing, J. G. Waight, V. Vittal, G. Pierper, F. Jamshidian, P. Hirsch, and D. J. Sobajic, "Online Dynamic Security Assessment in an EMS," *IEEE Computer Applications in Power*, vol. 11, pp. 43-47, 1998.

[13] J. D. McCalley, V. Vittal, and N. Abi-Samra, "An Overview of Risk Based Security Assessment," *Proceedings of the IEEE Power Engineering Society Summer Power Meeting*, pp. 173-178, 1999.

[14] L. Fink and K. Carlsen, "Operating Under Stress and Strain," *IEEE Spectrum*, vol. 15, pp. 48-53, 1978.

[15] U. G. Knight, "The Implementation of Emergency Control," *CIGRE IFAC Symposium on Control Applications*, Paper 207-05, 1983.

[16] J. McCalley, M. Bhavaraju, R. Billinton, A. Breipohl, H. Chao, J. Chen, J. Endrenyi, R. Fletcher, C. Grigg, G. Hamoud, R. Logan, A. P. Meliopoulos, N. Rau, M. Schilling, Y. Ychlumberger, A. Schneider, and C. Singh, "Comparison Between Deterministic and Probabilistic Study Methods in Security Assessment for Operations," *A task force organized by the IEEE PES Reliability, Risk, and Probability Applications Subcommittee*, 2001.

[17] L. Fink, "Security: Its Meaning and Objectives," *Proceedings of the Workshop on Power System Security Assesment*, pp. 35-41, 1988.

[18] J. Chen and J. D. McCalley, "Comparison Between Deterministic and Probabilistic Study Methods in Security Assessment for Operations," *6th International Conference on Probabilistic Methods Applied to Power Systems*, 2000.

[19] D. J. Sobajic, "Enhancing Reliability of the North American Transmission Grid," presented at Power Delivery EPRI, 2001.

[20] J. Endrenyi, "Power System Reliability Concepts," Ontario Power Technologies, Toronto 2000.

[21] H. Wan, J. D. McCalley, and V. Vittal, "Increasing Thermal Rating by Risk Analysis," *IEEE Transactions on Power Systems*, vol. 14, pp. 815-823, 1999.

[22] W. Fu, J. D. McCalley, and V. Vittal, "Risk Assessment for Transformer Loading," *IEEE Transactions on Power Systems*, vol. 16, pp. 346-353, 2001.

[23] H. Wan, J. D. McCalley, and V. Vittal, "Risk Based Voltage Security Assessment," *IEEE Transactions on Power Systems*, vol. 15, pp. 1247-1254, 2000.

[24] J. D. McCalley, A. A. Fouad, B. L. Agrawal, and R. G. Farmer, "A Risk-Based Security Index for Determining Operating Limits in Stability-Limited Electric Power Systems," *IEEE Transactions on Power Systems*, vol. 12, pp. 1210-1217, 1997.

[25] V. Vital, J. D. McCalley, A. V. Acker, W. Fu, and N. Abi-Samra, "Transient Instability Risk Assessment," *Proceedings of the IEEE Power Engineering Society Summer Power Meeting*, pp. 206-211, 1999.

[26] R. Billinton and R. Allan, *Reliability Evaluation of Power Systems,* New York: Plenum Press, 1984.

[27] G. Lian and R. Billinton, "Operating Reserve Risk Assessment in Composite Power Systems," *IEEE Transactions on Power Systems*, vol. 9, pp. 1270-1276, 1994.

[28] R. Billinton and R. Allan, *Reliability Evaluation of Engineering Systems*. New York: Plenum Press, 1983.

[29] Y. Ou and C. Singh, "Calculation of Risk and Statistical Indices Associated with Available Transfer Capability," *IEE Proceedings on Generation Transmission and Distribution*, vol. 150, pp. 239-244, 2003.

[30] Y. Ou and C. Singh, "Improvement of Total Transfer Capability Using TCSC and SVC," presented at Proceedings of IEEE PES Summer Meeting, Vancouver, Canada, 2001.

[31] Y. Ou and C. Singh, "Assessment of Available Transfer Capability and Margins," *IEEE Transactions on Power Systems*, vol. 17, pp. 463-468, 2002.

[32] G. Casella and R. L. Berger, *Statistical Inference,* Belmont, California: Duxbury Press, 1990.

[33] Y. Dai, J. D. McCalley, N. Abi-Samra, and V. Vittal, "Annual Risk Assessment for Overload Security," *IEEE Transactions on Power Systems*, vol. 16, pp. 616-623, 2001.

[34] B. Borkowska, "Probabilistic Load Flow," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-93, 1974.

[35] O. A. Klitin, "Stochastic Load Flows," *IEEE Transaction on Power Apparatus and Systems*, vol. PAS-94, 1975.

[36] R. Allan, "Probabilistic Load Flow Using Multilinearizations," *IEE Proceedings - C*, vol. 130, pp. 165-171, 1983.

[37] H. R. Sirisena and E. P. M. Brown, "Representation of Non-Gaussian Probability Distribution in Stochastic Load Flow Studies by the Method of Gaussian Sum Approximations," *IEE Proceedings - C*, vol. 130, pp. 165-171, 1983.

[38] W. Fu, S. Zhao, J. D. McCalley, V. Vittal, and N. Abi-Samra, "Risk Assessment for Special Protection Systems," *IEEE Transactions on Power Apparatus and Systems*, vol. 17, pp. 63-72, 2002.

[39] P. Kundur, *Power System Stability and Control,* New York; London: McGraw-Hill Inc., 1994.

[40] J. D. McCalley, V. Vital, A. V. Acker, and N. Abi-Samra, "Risk Based Transient Stability Assessment," presented at IEEE PES Summer Meeting, Edmonton, Canada, 1999.

[41] Y. Jiang, M. Ni, J. D. McCalley, and T. V. Voorhis, "Risk-based Maintenance Allocation and Scheduling for Bulk Electric Power Transmission System Equipment," presented at Proceedings of the Fifth International Conference on Systems Engineering, Las Vegas, 2002.

[42] M. Ni, J. D. McCalley, V. Vittal, and T. Tayyib, "Online Risk Based Security Assessment," *IEEE Transactions on Power Systems*, vol. 18, pp. 258-265, 2003.

[43] S. T. Lee and S. Hoffman, "Industry-wide Power Delivery Reliability Initiative Bears Fruit," in *IEEE Computer Applications in Power*, 2001.

[44] R. Allan and D. Kirschen "Assessment of Value of Security - Case for Support," presented at Tech. Rep., Manchester Centre for Electrical Energy, UMIST, Manchester, UK, 1994.

[45] NGC, "A Review of Transmission Security Standards," National Grid Company (UK), August 1994.

[46] K. Bell, M. Rios, D. Kirschen, and R. Allan, "Computation of the Value of Security: Final Report - Volume I," University of Manchester Institute of Science and Technology, Manchester, UK, October 1999.

[47] M. Rios, D. Kirschen, and R. Allan, "Computation of the Value of Security: Final Report - Volume II," University of Manchester Institute of Science and Technology, Manchester, UK, November 1999.

Chapter 3

Value of Security Assessment

3.1 Background

National Grid Transco (NGT, formerly National Grid Company) initiated a review of the transmission security standards in October 1992 following a formal request from the Office of Gas and Electricity Markets (OFGEM, formerly the Office of Electricity Regulation). In making the request, OFGEM indicated their concern that high levels of constraint costs arose during maintenance and other outages when the risk of a double circuit fault was low.[1]

OFGEM further suggested that the security standards might [1]:

- Consider single circuit faults ('N-1') rather than double circuit faults ('N-D')
- Be re-formulated in probabilistic terms
- Use cost/benefit techniques
- Consider the possible use of derogation

In this review the UK's National Grid Transco's conclusions were [1]:

- Changing the standards to consider only single circuit faults would be unacceptable because although this saves the constraint costs, there would be an increase in unreliability.
- It would be possible to re-formulate the security standards using cost/ benefit techniques and probability.
- While derogations from the existing planning and operational standards are used at present, their extended use would mean justifying each variation from the normal standards on a cost/benefit or probabilistic basis.

In a cost benefit approach, the principles underlying the planning and operation of the system should be founded on the costs and benefits to the users of the system. The cost is reflected in the payments made to the generators. The benefit is related to the consequences of stochastic events, which can only be estimated in a probabilistic sense. According to economic theory, the security should be tightened up to the point where its incremental cost equals the incremental cost of the avoided outages. Therefore, using such a cost-benefit analysis the optimal level of security can be determined.

Finally the review concluded that although the cost/ benefit techniques might be useful when applied to either planning or operation, these techniques have disadvantages:

- The techniques are significantly more complicated and time-consuming than deterministic security standards
- The results are variable and dependent on assumptions about the generator bids and the value of lost load.

3.2 Value of Security Assessor

The project 'A method for computing the value of security in power system operations' is initiated by Prof. Kirschen in 1997. This project aimed at developing a technique for calculating the value of security in power system operation. Dr. K. Bell developed the software necessary for this computation. This developed program is called Value of Security Assessor (VaSA). Later Dr. M. Rios further developed this software and applied to a model of the NGT system. VaSA is the basis for designing Probabilistic Indicator of System Stress, Comparison of Deterministic and Probabilistic Security Criteria, and defining Adaptive Deterministic Security Criteria which are presented in chapters 4, 5, and 6 respectively.

VaSA computes various types of costs involved in power system operations. Costs of operation can be categorised into deterministic and probabilistic costs. Cost of energy is a deterministic cost and cost of security is a probabilistic cost. Cost of energy is almost consistent against operating conditions and cost of security is affected.

Following are the components that contribute for the cost of energy and they can be separately estimated using VaSA.

- Base case generation cost
- Generation outage cost
- Generation rescheduling cost

Following are the components that contribute for the cost of security and they can be separately estimated using VaSA.

- Cost of load bus outages
- Cost of line tripping/outages that disconnect load busses
- Cost of load disconnection for maintaining system feasibility (e.g. frequency)
- Cost of emergency load shedding
- Cost of load disconnection due to operator action

Computation of the value of security involves the analysis of the system's behaviour over a period of time (for example 1 hour or 24 hours). The basis of the value of security assessment is a sequential Monte Carlo simulation. The reason for use sequential simulation for the value of security assessment is in an operational time frame the present system operating condition is a result through the previous operating condition. In addition it also requires detailed modelling of random disturbances.

The value of security should be computed over a planned generation schedule with un-planned events such as generation unit failure, line outages, double circuit outages, bus outages, compensating device failures, cascade tripping of lines, sympathetic tripping, and transient instability tripping of generators.

The Monte Carlo simulation used in VaSA is embodied with the following functions.

- A.C. Load flow
- Random number generator
- Weather modelling
- Operator action

- Sensitivity analysis
- Variance Reduction techniques
- Cost computation

Figure 3.1 shows the processing done in a single trial in the Monte Carlo simulation for the computation of costs.

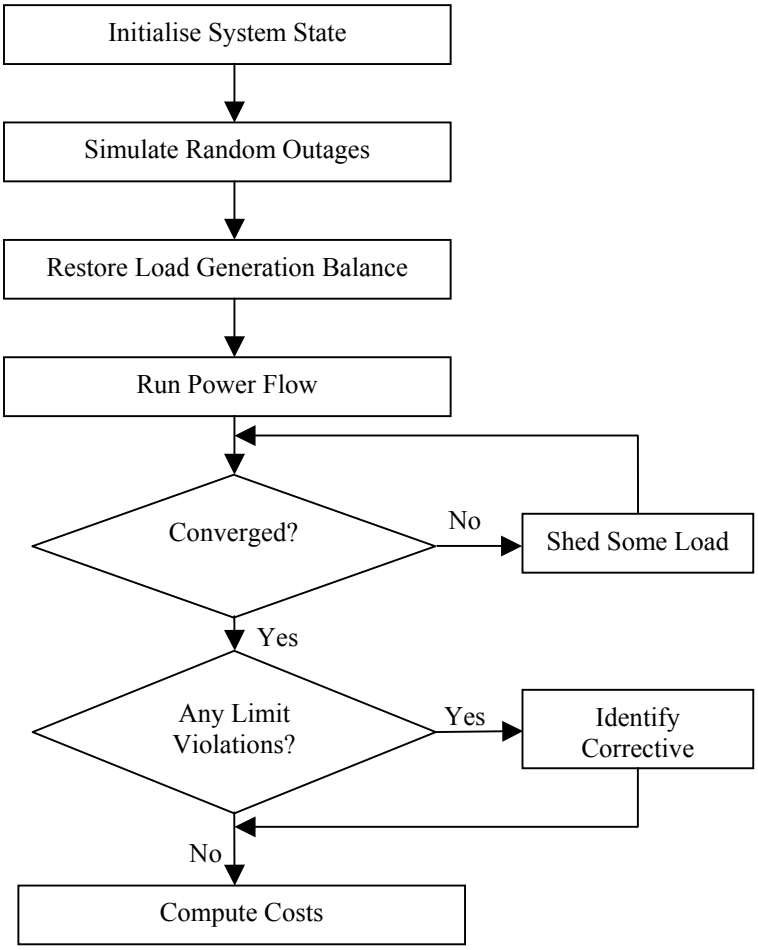

Figure 3.1: Processing done in a single trail of the Monte Carlo simulation [2].

In an operational time scale, weather can be predicted. The effects of predicted weather patterns can be reflected in the probabilities of different random events. VaSA can also model weather effects and generate weather dependent failure rates. VaSA models the weather effects by adjusting the failure rates for overhead transmission lines.

Figure 3.2 shows how the processing shown in Figure 3.1 is modified to take time-dependent phenomena into account.

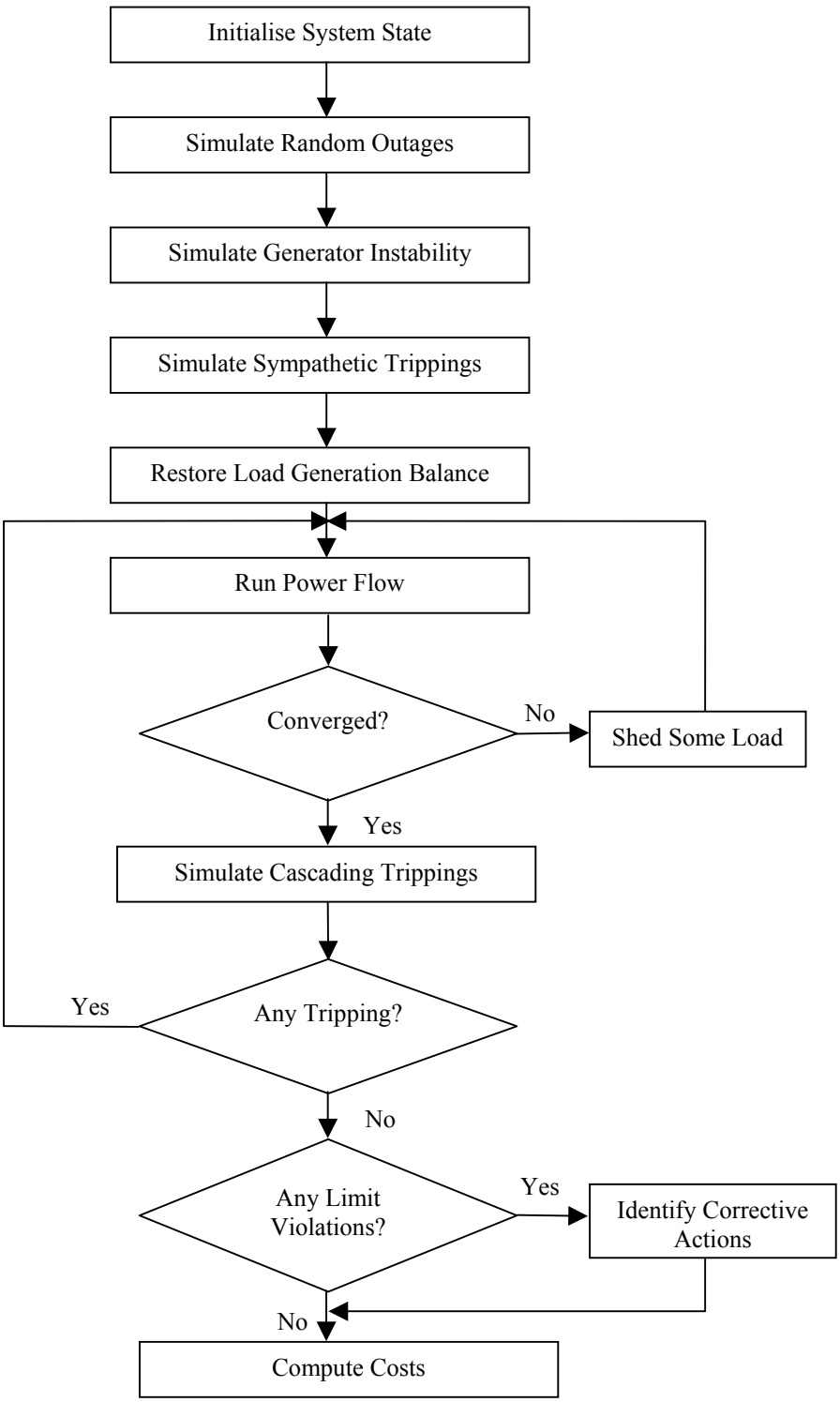

Figure 3.2: Processing done in each trial of the Monte Carlo simulation when modelling the time dependent phenomena [2].

Detailed modelling descriptions of the functions shown in Figures 3.1 and 3.2 are given in the section 3.3 of this chapter.

Variance reduction techniques are proposed to reduce the variance of the estimated parameter of the Monte Carlo simulation. Detailed descriptions of the types of variance reduction techniques and how they are used in VaSA are given in section 3.6 of this chapter.

3.3 Modelling in the Value of Security Assessor

3.3.1 Modelling the Network

VaSA requires the following data regarding the power system under study:[3]

- The initial network state given by the network topology and load demand.
- The network parameters required for a conventional power flow computation.

Bus data:

Bus number, bus name, area number, zone number, type of the bus (i.e., PV, PQ, Slack, bus with SVC), specified voltage, specified voltage angle, active load at the bus, reactive load at the bus, base voltage of the bus, shunt conductance, shunt susceptance, maximum voltage of SVC buses, minimum voltage of SVC buses.

Line data:

Line connected busses, area number, zone number, circuit number of the line (e.g. if single line then 1, if double line then 1 for the first line and 2 for the second line), type of the line (e.g. a transmission line, fixed tap transformer, on load transformer, phase shifter), series resistance, series reactance, shunt suceptance, short term emergency rating, medium term emergency rating, long term emergency rating, tap-ratio, phase shifter angle, minimum tap, maximum tap, tap step, status (i.e., in-service or out of service).

Generator data:

Generator name, connected bus name, generator type (e.g. frequency responsive, CCGT, OCGT, pumped storage, hydro, inter-connector, nuclear, synchronous condenser, etc.), scheduled active generation, maximum active power output, minimum stable generation, run-up rate, run-down rate, maximum reactive output, minimum reactive output, marginal price at the scheduled output.

- Planned generation schedule. This also known as a particular generation scenario.
- Probabilistic data to assess the component's states against random disturbances, i.e. the failure rates of components (e.g. lines, transformers, busses, compensation devices, generation plants), the probability of sympathetic tripping of lines, probability of transient instability etc.
- Load restoration data, i.e. the rate of restoration of disconnected loads. There are two methods available to model the restoration of disconnected loads. The first method continuously restores the load at a constant rate and the second method restores in steps at an increasing rate.
- Cost computation data, i.e., the data required for computing the Value of Lost Load (VOLL) such as Sector Customer Damage Function (SCDF), sector weighting factor, etc.
- Weather data, i.e. proportion of failures (F_i), normalised duration of weather (T_{n_i}), inter-regional lines, etc.

3.3.2 Checking for Equilibrium

With those input data, at first an a.c. load flow is performed to check the network equilibrium (i.e., convergence of the power flow) in the base case of the particular scenario. To estimate the value of security the a.c. load flow should converge and there should be no constraint violations in this base case. If the base case is set successfully then the Monte Carlo simulation begins.

3.3.3 Modelling Random Disturbances

Next, the random number generator generates random numbers for assessing the component states against random disturbances. The random number generator used in the routine of VaSA is 'g05caf' which is extracted from the NAG Fortran Library [4]. In this random generator, the default random seed is the real time at which the Monte Carlo simulation begins (i.e., an integer derived from computer's date and time). In addition the program has flexibility in defining a new random seed. Each item of plant receives a separate random number between zero and one. If the random number corresponding to a particular item of plant is less than the calculated probability of failure then the corresponding equipment is deemed to have failed. Otherwise the equipment is deemed to be in service. The probability of failure of an item of plant in the network is calculated using the Poisson distribution. Therefore, the probability $p_i(t)$ of item of plant i suffering a fault at time t is calculated using the Equation (3.1) [5].

$$p_i(t) = 1 - e^{-\lambda_i t} \tag{3.1}$$

Where, λ_i is the failure rate of plant item i per year. λ_i is assumed to be constant during the estimation time-period t.

3.3.4 Modelling Weather Conditions

Five weather states have been defined for the calculation of value of security. They are: 1) normal weather; 2) thunderstorm; 3) freezing rain/wet; 4) high winds; 5) dry spell followed by fog. These weather states can also be categorised into two states: normal (non-adverse) weather and adverse weather. Weather states can be specified on a regional basis in order to model different weather conditions within the system. The proportion of failures of network element n occurring in each weather state is given by [5],

$$F_i^n = \frac{T_i}{T} \times \frac{\lambda_i^n}{\overline{\lambda^n}} \tag{3.2}$$

Where,

F_i^n Proportion of failures for component n in weather state i

$\overline{\lambda^n}$ Average failure rate of component n

λ_i^n Failure rate of component n in weather state i

T_i Duration of the weather state i

T Equal to the sum of all weather state durations.

F_i^n is usually not available for each individual component. Only an average value (F_i) for each class of components (e.g. lines at 400kV) can be obtained from the data collected for most systems. Therefore, a particular λ_i^n is computed from equation (3.3).

$$\lambda_i^n = \frac{1}{F_i} \times \frac{T_i}{T} \times \overline{\lambda^n} = w \times f_i \times \overline{\lambda^n} \tag{3.3}$$

Hence, the average failure rate is adjusted by the factor $w \times f_i$ to obtain a weather-dependent failure rate. This adjustment is only applied to overhead lines since they are the only type of component whose performance is significantly affected by the weather. Each region that a line crosses may have a different weather condition and thus a different adjustment factor $w \times f$ is applied.

The failure rate of a line therefore depends on the length of the line and the weather in each region, which this line crosses.

$$\lambda^n = \overline{\lambda^n} \sum_{j=1}^{m} \left(\frac{l_j}{L} \times w \times f_i \right) \tag{3.4}$$

Where,

m Number of regions that the line crosses

l_j Length of the line in region j

L Total length of the line

In this way, the weather dependent failure rates are developed and apply for the computation of value of security.

3.3.5 Checking for Islanding

Once the random disturbances have been "created", the network is fully checked for any islands that might have been caused by these contingencies. To identify the islands, when busses are involuntarily disconnected from the network their network association status with the network is set as un-associated. Islands are identified by re-building the network with only the components that are in service. The initial state of the network considers as the island number of zero. Then the network rebuilding begins and identifies the busses that are associated with the original network and in service. In this way, at first the island with the largest number of busses is built. Then the remaining un-associated busses, which are in service, are assigned separate island numbers. Likewise, if there are n numbers of in-service busses that are un-associated with the largest island, then the network comprises $(n+1)$ islands.

3.3.6 Checking for Equilibrium in Each Island

An a.c. load flow is performed for each island to check the equilibrium. There are three possible outcomes of each of power flow computation.

- The power flow converges and the resulting state of the system does not exhibit any violation of normal operating limits (i.e., thermal limit violations, or voltage limit violations). This contingency state therefore does not require any corrective action. However, if there are some loads that are not served due to outages of busses or tripping of line causing the de-energisation of busses and hence the disconnection of loads, then there will be a cost of security. Otherwise the cost of security is zero.

- The power flow converges but there are some violations of normal operating constraints. Corrective actions must be taken to bring the system back within acceptable limits. For example, generation may be re-dispatched, gas turbines may be started, or, as a last resort, loads may be shed to correct line overloads.

- The power flow diverges. This is taken to indicate that the occurrence of this contingency state would result in severe problems. In such situations, as an emergency measure, load shedding is carried out to prevent a complete voltage collapse in the system. Based on conversations with experienced operators, a heuristic technique has been developed to determine the ways and percentage of load that is typically dropped to restore the network equilibrium.

  According to the heuristic approach, the load shedding is carried out in 5% block of the load in the zone where the bus with the largest mismatch is located. Load shedding is carried out until convergence is achieved. The situation is also deemed as an emergency. If the load shedding is carried out 20 times the zone is blacked out. Then the load disconnections extend to the neighbouring zones where they proceed again in blocks of 5% of the area load. If the convergence has not been achieved after 100 load-shedding steps, the system is deemed to have collapsed.

3.3.7 Operator Action

When the system has reached an equilibrium point (i.e., when convergence of the load flow has been achieved), the resulting state of the system may exhibit violations of normal operating limits. Corrective actions must be taken to bring the system back within acceptable limits. Corrective actions include re-dispatching generation, changing voltage set points, and tap ratios. Load is not shed to remove violations of operating limits if these violations can be corrected using normal controls, i.e., active and reactive despatch. A fuzzy expert system with embedded power flow and linear sensitivity analysis [6] determines the extent and location of these corrective actions.

There are three types of controls available in eliminating violations with the fuzzy expert system in VaSA. They are:

- Active dispatch

  — Dispatches settings of active power generation, shedding of loads (active and reactive components in proportion) and changes to phase shifter settings in order to relieve overloads of transmission lines

- Reactive dispatch

  — Dispatches settings of reactive control devices in order to correct violations of voltage limits
- Dispatch of active controls for correction of voltage problems

  — This is activated to change the active generation and, if necessary, shed load in order to remove any outstanding violations of voltage limits. However, this type of control measure is very costly and is the last option among control actions.

In setting the dispatch in each island, the operator's judgement is simulated by balancing the criteria of control effectiveness, control margin, cost, simplicity and the possibility of unwanted secondary effects.

At first the expert system checks the sensitivity of the control measure in eliminating or reducing the violations. If it is successful in eliminating or reducing the violations then the corresponding control measure is applied. Effectiveness of the control actions are always checked by applying a control action and then performing an a.c. load flow.

3.3.8 Modelling Time Dependent Phenomena

Cascading tripping of lines, sympathetic tripping and transient instability of generators are due to the results of time dependent phenomena. VaSA is capable of modelling these types of outages and the corresponding modelling strategies are described in the following sections.

Cascading tripping of lines is modelled in VaSA assuming that the overloaded lines are tripped in r% of the situations encountered [7] where the r is the probability that the operator is unable to eliminate the overloads before the protection operates [2].

Sympathetic tripping is modelled in VaSA using the probability of malfunction of the element's protection system when a failure occurs in its vulnerability region. The vulnerability region defines as the region of the system where a fault may provoke the

tripping of the element. A Monte Carlo trial indicates whether a line is tripped by sympathy using the probability of sympathetic tripping.

Random sampling using the set of probabilities (i.e., probability of stability due to a fault on line k) determines whether a fault provokes instability in the system. If a stability problem is simulated, it is necessary to determine the affected generators. Offline stability studies are used to determine the vulnerability region associated with the stability of each generator. Thus, if a fault on line k provokes instability and this line is in the vulnerability region of a generator, then this generator is disconnected.

3.3.9 Checking for New Equilibrium

On the basis of models described above, these additional time-dependent outages can also be simulated in a probabilistic manner. Then an ac load flow is performed and, if required, further loads are disconnected to achieve the new equilibrium (i.e., convergence of the power flow)

3.3.10 Load Restoration

Estimating the load restoration time in the Value of Security Assessor takes into account two phases. They are:

- The control phase
    - — In this phase the operator takes corrective actions to try to stabilise the system and to decide on a restoration strategy. Load reconnections are not carried out during this phase.
- The load restoration phase
    - — This phase involves the reconnection of the load that was disconnected or voluntarily removed during the control phase.

The heuristic model that has been built in the VaSA divides the restoration process into these two phases. The restoration duration is measured from the moment when the initial load disconnection is carried out. It is reasonable to assume that the duration of the first phase is proportional to the severity of the outage and therefore it is modelled as shown in Equation (3.5).

$$t_1 = T \times P_{shed} / P_T \tag{3.5}$$

Where, t_1 is the duration of the first phase. T is the expected duration of this first phase for a system blackout to experience. Thirty minutes being a reasonable value for T. The basis of this time duration is accounted from [8].

The duration of the second phase or restoration phase is calculated using the Equation (3.6) where P_{shed} and P_T are the disconnected and the total load of the system respectively. t_2 is the duration of the second or restoration phase and R_{rest} is the rate of restoration in MW/ min.

$$t_2 = P_{shed} / R_{rest} \tag{3.6}$$

3.4 Calculation of Operation Cost

Costs of operation are the cost of security and cost of energy. The amount of active generation of plants and the system marginal price are required to calculate the cost of energy in a particular trial. The amount of disconnected load, the time to restoration of disconnection load and the value of lost load are required to calculate the cost of security in a particular trial of the Monte Carlo simulation.

3.4.1 Customer Damage Functions

For any feeder network, the procedure for evaluating customer outage costs (COC) involves the convolution of load, system and cost models. The annual energy consumed or peak demand for each customer sector (i.e., Residential, Commercial, Industrial and Large users) constitutes the load model while the system's attributes, operating procedure and reliability indices form the system model. For a given service area, the

cost model is a series of values referred to as the composite customer damage function (CCDF) and defines as the normalised costs (normalised either by annual energy consumed or peak demand) due to supply interruptions expressed as a function of interruption duration for the customer mix supplied. These normalised costs are grouped according to classes of consumers and the average values for a class obtained. These are, in turn, appropriately weighted to yield a series of sector values referred to as sector customer damage function (SCDF). For each sector y and its load factor LF_y, the value corresponding to interruption duration t_j is denoted by $C_y(t_j)$ and is given by Equation (3.7). [9]

$$C_y(t_j) = \frac{C_{Ly}(t_j)}{LF_y \times 8.76} \quad \text{£/MWh} \tag{3.7}$$

Where $C_{Ly}(t_j)$ is the SCDF value without giving due regard to the load factor.

The definition of SCDF is similar to the CCDF but refers to a sector rather than the entire customer mix. SCDF values are appropriately weighted to give CCDF values. Equation (3.8) shows the formula for evaluating the CCDF, values through $C_y(t_j)$ for an interruption duration t_j, with weighting in proportion to the respective sector annual energy consumption.[9]

$$C(t_j) = \sum_{y}^{ny} C_y(t_j) \times \left(\frac{E_y}{\sum_{y}^{ny} E_y} \right) \quad \text{£/MWh} \tag{3.8}$$

Where E_y is the annual energy consumed by sector y, and ny is the number of sectors connected to the system under review. In Equation (3.8) the energy consumption is used as the moderating factor due to its information being readily available; otherwise contribution at peak demand could also be used. In instances where difficulties in disaggregating the load and therefore obtaining the load factors may be encountered, the Equation (3.9), which uses supply point's load factor (LF) can be used [10].

$$C(t_j) = \sum_{y \in ny} C_{L,y}(t_j) \left(\frac{E_y}{\sum_{y \in ny} E_y} \right) \left(\frac{1}{LF \times 8.76} \right) \quad \text{£/MWh} \tag{3.9}$$

3.4.2 Cost of Security

The cost of security is calculated using Value of Lost Load (VOLL). VOLL suggest the value of an average consumer puts on an unsupplied kWh [10]. The starting point for the evaluation of the VOLL is the SCDFs for the sectors surveyed.

Two approaches are available in VaSA for calculating the VOLL. The first assumes that individual sector load factor information is unavailable, i.e., only the overall load factor of the customer mix (i.e., only the bus load factor) is available while the second assumes that sector load factors of each bus (E.g. residential (35%), commercial (27%), industrial (34%) and large users (4%)) are known. In the value of security assessment SCDFs are classified into seven duration of interruptions: momentary; one minute; 20 minutes; one hour; 4 hours; 8 hours; and 24 hours. A momentary is assumed to have a duration of one minute for the calculation of cost of security.

In the first approach the SCDF values are appropriately weighted to give the CCDF values (refer Equations 3.8 and 3.9), which are in turn used to calculate the corresponding VOLL for each duration, t_j (hours) as shown in Equation (3.10).[10]

$$VOLL(t_j) = \frac{C(t_j)}{t_j \times LF} \quad \text{(£/kWh)} \tag{3.10}$$

Where LF refers to the load factor of the customer mix considered

In the second approach, from the SCDF value a value of lost load attribute to each sector for the corresponding outage duration is derived. The formula for the VOLL corresponding to a duration t_j (hours) for a general sector y is given by Equation (3.11).[10]

$$VOLL_y(t_j) = \frac{C_{L,y}(t_j)}{LF_y \times t_j} \quad \text{(£/kWh)} \tag{3.11}$$

For the computation of cost of security in a trial, this thesis uses the second approach. Therefore, the cost of security in a trial is computed using Equation (3.12).

$$C_s = \sum_{j=1}^{n} (VOLL_y(t_j) \times t_j \times P_{shed}(j)) \tag{3.12}$$

Where,

C_s Cost of security in a particular trial

$VOLL_y(t_j)$ Value of Lost Load for interruption duration t in the interval j for sector y

t_j Total interruption duration (i.e., $t_1 + t_2$) corresponding to time interval j

P_{shed} Amount of disconnected load

t_1 Duration of the first phase (control phase) of the restoration

t_2 Load restoration phase where reconnecting of disconnected load takes place.

n Number of intervals

3.4.3 Cost of Energy

The cost of energy in time interval j is the product of system marginal price (SMP) and the total active generation after responding to random disturbances (i.e., total active generation after getting the system back to normal), where the SMP is the price of the most expensive generating unit required to meet the forecasted demand in each half hour [11]. Equation (3.13) gives the formulation of the cost of energy for a particular time interval j in a trial.

$$C_{e_j} = P_{G_j} \times (SMP) \tag{3.13}$$

Where,

C_{e_j} Cost of energy in a particular interval j in a trial

P_{G_j} Total active generation of the corresponding time interval in the trial

3.5 Stopping Criteria

The estimation process described in Figure 3.1 is for a single trial of the Monte Carlo simulation. When the simulation progresses for number of trials, there must be some means of terminating the simulation once a sufficiently accurate estimate of the value of security has been obtained. The criteria that is used for terminating the Monte Carlo Simulation process upon achieving the expected certainty of the estimate is called stopping criteria.

Four criteria have been devised to decide when the estimate produced by VaSA is within the expected accuracy. The first criterion sets the minimum number of trials that should be performed by the Monte Carlo simulation. The second criterion checks whether experience at least a system blackout. VaSA can also skip this criterion as a similar result can alternatively be achieved using the minimum number of trials set by the first criterion. The third criterion checks whether the estimation is within the confidence interval limit with the expected degree of confidence (γ).

The confidence interval (L) is given by the Equation (3.14) where $\overline{X}$ is the estimated value, σ_X is the standard deviation of the estimation, and α is the factor that corresponding to the postulated normal distribution of the degree of confidence (γ).

$$L = [\overline{X} - \alpha \times \sigma_X, \overline{X} + \alpha \times \sigma_X] \tag{3.14}$$

Therefore, to meet the third criterion, the following inequality constraint should be satisfied.

$$\sigma_X < \frac{\overline{X}}{\alpha} \times L \tag{3.15}$$

However, if the simulation cannot meet both the second and third criteria, it is terminated by the fourth criterion, which sets maximum number of trials.

Additional auxiliary criterion that is developed for the indicator of system stress is described in Chapter 4.

3.6 Variance Reduction Techniques

The value of security in networks with a small number of components can be estimated using a naïve Monte Carlo simulation because convergence can be achieved quickly enough without variance reduction techniques (VRTs). However, this is not always true and in many cases one or more variance reduction techniques have to be used to achieve convergence. This situation is particularly true with larger networks. With a VRT the estimated mean is pushed further towards the population mean by reducing the variance of the estimate.

Every VRT does not perform well for every type of estimation and the appropriate VRT must be identified for each particular application. This can be done by performing a set of preliminary estimations with VRTs and validating the results.

Several Variance Reduction Techniques have been integrated within the VaSA [12]:

- Antithetic Variates
- Dagger Sampling
- Stratified Sampling
- Control Variates
- Correlated sampling
- Importance Sampling

In Antithetic Variates two negatively correlated samples are used to estimate the parameter. Negatively correlated samples are created using the generated random numbers and reproducing another set of random numbers so as to correlate them negatively. In other words, if the generated set of random numbers is U then for creating negatively correlated samples, the random numbers are generated with $(1-U)$. Thus, the average of two trials will be approaching the population mean. If many such pairs of trials are performed, the variance of the averages of the pairs will be low or in other words the variance of the sample will be reduced. Obviously this takes twice the CPU time required which is a drawback of this technique.[12]

Dagger sampling requires an appropriate choice of the length of the system dagger cycle. For example if component a has outage probability of 0.1 then its dagger cycle length is 10. If component b has outage probability of 0.33, its dagger cycle length is 3. If the component c has an outage probability of 0.15 then its dagger cycle length is 6. If we choose the system dagger cycle length as 6 then plant c requires a single random number to decide the status of the plant for 6 trials. Plant b requires two random numbers to decide the status of two cycles. Therefore, with plant b only two events will be occur in 6 trials. However, for component a the dagger cycle needs to be truncated. I.e., one random number determines its status for 10 trials, however, after the 6^{th} trial a new random number is generated and used it for assessing the status of a for the next 6 trials. In this way the average of the outcomes of those effective trials are close to the population mean, and reduces the sample variance for number of such sets of 6 trials. Therefore, in dagger sampling selecting the system dagger cycle length is a key issue as it affects the accuracy of the estimation. [12]

In Stratified Sampling a heterogeneous population is divided into homogeneous subpopulations and these subpopulations are called strata. In a stratum the observations vary very little and the mean can be precisely estimated. Such precisely estimated stratum means are then combined to get the precise estimate of the population mean. Strata are established according to the stratification variable. If the stratification variable is positively correlated with the parameter to be estimated then the precision and the convergence of the estimation of population mean further improves. In VaSA stratification can be performed with any of the following stratification variables. [12].

- Cost
- MVA flow of lines
- MW/MVAr of the system

Comprehensive details of the stratified sampling and extended descriptions of stratification variables are described in Chapter 4.

Control Variates is also known as regression sampling. This technique replaces the direct estimation of parameters with an estimate of the difference between the parameter

to be estimated and some analytical models. The technique is more suitable when one is able to estimate a part of the problem using an analytical method (enumeration). In Control Variate a random variate C is a control variate for Y if it is correlated with Y and if its expectation μ_C is known [13]. In VaSA either generation outages or transmission outages can be used as the control variate (i.e., regression variable).

The cost of control variate is simultaneously evaluated using enumeration and Monte Carlo simulation. The cost to be estimated is also estimated using the Monte Carlo simulation. Equation (3.16) shows the basic establishment of this technique.

$$C = \overline{C}_{T_m} + \overline{C}_{c_e} - \overline{C}_{c_m} \tag{3.16}$$

Where,

C Estimated cost by reducing the variance of the estimate with control variate technique

$\overline{C}_{T_m}$ Estimated cost using Monte Carlo simulation

$\overline{C}_{c_m}$ Estimated cost of control variate using Monte Carlo simulation

$\overline{C}_{c_e}$ Evaluated cost of control variate using enumeration

Since the difference between the variability of the cost of control variate that is calculated using enumeration and the cost of control variate that is estimated using the Monte Carlo simulation is negative, this technique also achieves a faster convergence than naïve Monte Carlo simulation. [12]

Correlated sampling is particularly useful when comparing two scenarios where each scenario uses the same set of random numbers. The aim of correlated sampling is to produce a high positive correlation between two similar processes so that the variance of the difference is considerably smaller than it would be if the processes were statistically independent. Comprehensive details of this technique are given in Chapter 4.[12]

The basic idea of importance sampling is to disturb the original sampling process completely by replacing the original process by another one. This distortion is corrected

by a weighting of the observations from the new sampling process, so that the average of the corrected observations is still an unbiased estimator of the mean of the original process. Importance sampling in VaSA focuses on biasing individual plant outages and expected number of outages per trial of each plant type. Then it tallies the outcome of the trial that is generated from the biased outages with the expected cost and scales back to compensate for bias. [12].

3.7 Conclusions of the First Project

The first project set out to develop a probabilistic method for estimating the expected cost of outages and hence comparing various levels of security. According to the results of this project, the Value of Security Assessor can be used in two ways. They are:

- To compare different operating scenarios
- To calculate the value of security in a power system

The project has also shown that the comparisons of different scenarios can be realised using computed total costs or using the correlated sampling method. Out of these two methods, the correlated sampling method provides a better way of selecting the best operating scenarios due to high CPU demand with the other method.

The results further suggested that[14]:

- The effect of adverse weather increases cost of security. The best scenario can be changed depending on the weather condition.
- An increase in the failure rate of one or more components increases the cost of security.
- Consideration of sympathetic tripping would also increase the cost of security.
- Most of the Variance Reduction Methods and Correlated Sampling perform well for reducing number of trials in a Monte Carlo simulation for small power systems. However with large power systems the reduction of variance with variance reduction techniques does not considerably reduces number of Monte Carlo trials. The best variance reduction technique also depends on the parameter to be estimated.

The results also show that the cost of corrective actions is much smaller than the social cost of outages [2]. Modelling corrective actions demands considerably high CPU time due to high processing time in the sensitivity analysis process. Therefore, the research components presented in chapters 4, 5, and 6 ignored the loads disconnection in the Monte Carlo simulation due to operator action.

3.8 Extended Facilities of VaSA

VaSA was originally developed for calculating the value of security under the project "A method for computing the value of security in power system operations". The existing facilities of VaSA [3] have been extended for the development of the Probabilistic Indicator of System Stress and Adaptive Deterministic Security Criteria.

Following are the extended facilities that are embodied with the VaSA.

With regard to Value of Security Assessment:

- Separately estimating the value of security caused by outage of each type of elements in the network. E.g. single line, double line, cascading tripping, sympathetic tripping, and transient instability.

With regard to Probabilistic Indicator of System Stress:

- Estimating Expected Energy Not Served (EENS) through Monte Carlo simulation
- Correlating more than two cases
- Applying extended stratified sampling to reduce the variance of Monte Carlo simulation.
- New stopping criterion for Monte Carlo simulation.
- Statistical tests.

With regard to Adaptive Deterministic Security Criteria:

- Changing generation pattern in a power system according the criteria given in [15] and estimating the cost of security.

3.9 Deterministic Security Assessor (DSA)

A deterministic security assessor (DSA) program has been developed for contingency analysis and to calculate deterministic security boundary. This program uses power flow and 'N-1' and/or 'N-D' level contingencies to calculate the secure levels of generation and transmission line flows at the specified plants and lines respectively. These levels are maximised by this program using the study criteria, which are described in chapter 5 of this thesis.

3.10 References

[1] NGC, "A Review of Transmission Security Standards," National Grid Company (UK), August 1994.

[2] M. Rios, D. S. Kirschen, D. Jayaweera, D. P. Nedic, and R. N. Allan, "Value of Security: Modelling Time-Dependent Phenomena and Weather Conditions," *IEEE Transactions on Power Systems*, vol. 17, pp. 543-548, 2002.

[3] K. Bell and M. Rios, "Value of Security - User Guide," Manchester Centre for Electrical Energy, Manchester, UK, October 1999.

[4] Numerical-Algorithm-Group-Ltd., "Nag Fortran Library Manual," Oxford 1993.

[5] R. Billinton and R. N. Allan, *Reliability Evaluation of Power Systems*, 2nd ed. New York; London: Plenum Press, 1996.

[6] K. R. W. Bell, D. S. Kirschen, R. N. Allan, and P. Kelen, "Efficient Monte Carlo Assessment of Value of Security," presented at 13th Power System Computation Conference, Trondheim, Norway, 1999.

[7] A. Merlin and J. C. Dodu, "New Probabilistic Approach Taking into Account Reliability and Operation Security in EHV Power System Planning at EDF," *IEEE Transactions on Power Systems*, vol. 1, pp. 175-181, 1986.

[8] R. Kearsley, "Restoration in Sweden and Experience Gained from the Blackout of 1983," *IEEE Transaction on Power Systems*, vol. 2, pp. 422-428, 1987.

[9] K. K. Kariuki and R. N. Allan, "Applications of Customer Outage Costs in System Planning Design and Operation," *IEE Proceedings on Generation Transmission and Distribution*, vol. 143, pp. 305-312, 1996.

[10] K. K. Kariuki and R. N. Allan, "Evaluation of Reliability Worth and Value of Lost Load," *IEE Proceedings on Generation Transmission and Distribution*, vol. 143, pp. 171-180, 1996.

[11] OFGEM, "New Electricity Trading Arrangements." http://www.ofgem.gov.uk/elarch/atrading.htm.

[12] K. Bell, M. Rios, D. Kirschen, and R. Allan, "Computation of the Value of Security: Final Report - Volume I," University of Manchester Institute of Science and Technology, Manchester, UK, October 1999.

[13] R. Y. Rubinstein, *Simulation and Monte Carlo Method*: Wiley, 1981.

[14] M. Rios, D. Kirschen, and R. Allan, "Computation of the Value of Security: Final Report - Volume II," University of Manchester Institute of Science and Technology, Manchester, UK, November 1999.

[15] J. McCalley, M. Bhavaraju, R. Billinton, A. Breipohl, H. Chao, J. Chen, J. Endrenyi, R. Fletcher, C. Grigg, G. Hamoud, R. Logan, A. P. Meliopoulos, N. Rau, M. Schilling, Y. Ychlumberger, A. Schneider, and C. Singh, "Comparison Between Deterministic and Probabilistic Study Methods in Security Assessment for Operations," *A task force organized by the IEEE PES Reliability, Risk, and Probability Applications Subcommittee*, 2001.

Chapter 4

Probabilistic Indicator of System Stress

4.1 Introduction

Power system security has become a major concern of electric power utilities, as power systems become more and more complex and are operated closer to their transmission capacity limits with the introduction of competition of electricity markets. In a power system, faults and failures are unpredictable and unavoidable. However, a power system must be operated in such a way that these incidents should not normally result in the disconnection of some consumers or a collapse of the entire system. Traditionally, a deterministic security criterion is used to assess the security of the system. Traditional security criteria reflect the system security either as 'secure' or 'insecure' considering the credible events. On the other hand, the traditional security criteria do not take into account non-credible events. Losing two independent components at the same time is usually deemed "not credible" because the probability of two simultaneous independent faults or failures is very low. For example, in the UK, a loss of any double circuit line is considered a credible contingency because both circuits would be taken out of service simultaneously if the tower that supports them were to fail. On the other hand, the simultaneous loss of two separate lines is considered not credible. If a conventional security analysis program detects that one of the credible contingencies would result in violations of the normal operating limits, the operator is required to take preventive actions. These preventive actions should adjust the current operating state of the system in such a way that the post-contingency violations disappear. Such preventive actions are not required if suitable post-contingency actions are available.

The partition of the set of all possible contingencies into "credible" and "non-credible" subsets makes possible an unambiguous distinction between secure and non-secure operating states. This approach is very convenient from an operator's point of view

because it specifies clearly when action is required and when it is not. A problem that is fundamentally probabilistic has therefore been turned into a deterministic problem. The deterministic approach has drawbacks. It assumes that each system component has the same probability of outages and avoids consideration of cost effects, cascading tripping, sympathetic tripping, and influences of failures due to weather effects. The security in a deterministic approach indicates binarily and do not indicate the level of security quantitatively.

To investigate the system security level in a power system in an operational time frame a probabilistic approach is required as the events are triggered in a random nature and such an approach can be used for quantitative indication of level of security. This chapter presents a tool that measures the system security continuously against unpredictable and unavoidable events taking into account the probabilistic nature of power system events. This tool is called the Probabilistic Indicator of System Stress. It is a steady state security tool and can be used for stress measurements of power system operations. The Value of Security Assessor (VaSA) is the engine used in the Probabilistic Indicator of System Stress.

The following sections describe the design requirements, methodologies of the development, calibration and testing of indicators of stress for large and small networks. The chapter addresses major issues that arise throughout the design process and discusses the results of stress measurements. Method for measuring stress levels, and the benefits offered to operators are also discussed.

It is to be note that in the following sections a ‘reference case’ refers to a case that is used for calibrating the indicator of stress and a ‘new case’ refers to a case that represents a possible real time operating condition.

4.2 Design Requirements

A probabilistic indicator of system stress should obviously satisfy the usual requirement for validity, i.e. the ability to provide an accurate and reliable measure of the risk of customer disconnections in a power system. In addition, if this indicator is to be acceptable to operators, they should find it useful, practical, and intuitively correct. The computation of the indicator of stress should also be sufficiently fast to guarantee that it is still relevant to the current state of the system by the time it is available. The only point that needs to be stressed with regard to the validity requirement is that the model used in the calculation of the indicator of stress should take into account all the factors that significantly affect the operation of a power system. This means that the effect of the weather conditions on the probability of outages and the opportunity for the operator to react to problems as they develop should be taken into consideration [1].

The acceptability requirement deserves a more detailed discussion because it includes several aspects. First, several factors reduce the level of security in a power system: an increase in load, a large number of unavailable components (lines, generators, reactive compensation devices), a reduction in the available active or reactive reserve, and increased power transfers between regions. The indicator should obviously reflect the influence of each of these factors taken independently. More importantly, it should be able to balance the influence of various factors going in opposite directions at the same time. For example, the indicator should be able to reliably measure the level of stress in a power system if the load is fairly high and there is an unusual pattern of outaged lines but the reactive reserve is larger than usual. An indicator whose value increases linearly with the level of stress would also be more useful than a non-linear indicator. In this context, the binary secure/insecure classification achieved by the deterministic security criteria is a highly non-linear security criterion. Figure 4.1 shows the comparison between linear and non-linear indicators of system stress.

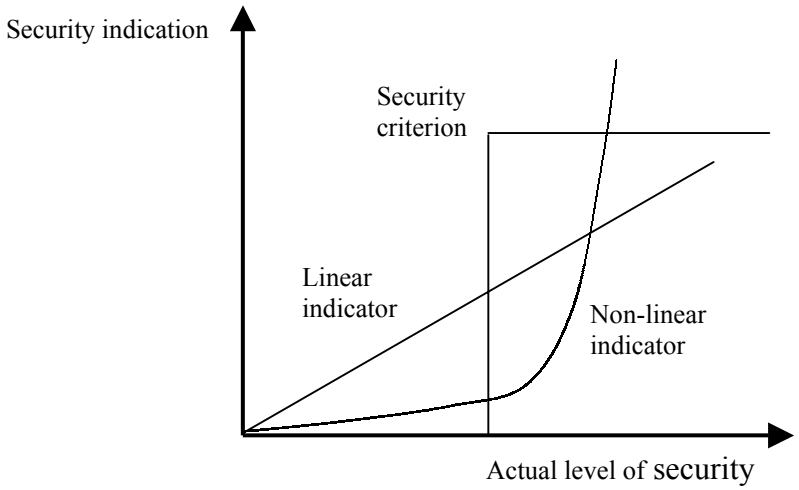

Figure 4.1: Comparison between linear and non-linear indicators of system stress.

The application of probabilistic methods to power system problems have often been hampered by their very large computational burden, particularly when they require a Monte Carlo simulation. This difficulty is significant when one attempts to apply probabilistic methods in power system operation. In this case the computations must be based on data gathered in real-time and the results should be available before changes in the state of the power system. Otherwise the results are obsolete and irrelevant. This highlight the operational tools that are processed through probabilistic methods must be designed to process the data in a very short time.

An analogy might clarify these design requirements and the developments of this indicator. Most parents have in their medicine cabinet a thermometer that they use to get a quick but reliable indication of how sick their child might be. A probabilistic indicator of stress should perform the same function for a power system. Just like the dilation of mercury in an old-fashioned thermometer shows the severity of an illness, the Expected Energy not Served (EENS) measured using a Monte Carlo simulation can indicate the level of stress in a power system.

To be useable a thermometer or any other measuring device it must be calibrated. This means that there must be labelled tick marks that make possible an easy reading of the temperature (referred to thermometer analogy). Rather than simply using the absolute value of EENS as calculated by the Monte Carlo simulation, it is proposed to measure it

by comparison with a set of known reference points. Measuring the EENS against a calibrated scale has two advantages. First, it facilitates the interpretation of the probabilistic indicator by the operators. Just like new parents are taught that if their child's temperature rises above 39°C they should call the doctor, operators will quickly learn that a reading of x for the probabilistic indicator of system stress is a sign of potential trouble and that action needs to be taken soon. The second reason to measure by reference to a calibrated scale is that it can be done very quickly using correlated sampling. Since correlated sampling is typically 5 to 10 times faster than naive Monte Carlo simulation, this form of relative measurement makes possible the use of a probabilistic indicator of system stress in an operational environment.

4.3 Why EENS?

There are several indices that are relevant to power systems [2]. These include Loss of Load Probability (LOLP), Loss of Load Expectation (LOLE), Expected Energy not Served (EENS), Load Interruption Index, Customer Interruption Frequency Index, Customer Interruption Duration Index, and Customer Curtailment Index. It is preferable that the index indicating the level of stress should be a function of the frequency, duration, and magnitude of the outage. Furthermore, such an indicator should reflect a zero level of stress when the system is healthy and should increase with increasing system stress. Since the EENS incorporates all these attributes, the EENS is used as the metric for the indicator. It is also to be highlighted that this design uses the EENS as a proxy to indicate the level of stress in power systems. Other metrics besides EENS could be used for stress measurement.

4.4 Design Methodology

4.4.1 Reference Cases

A set of reference cases spanning the entire range of possible values of EENS for the system must be selected. At the low end, the EENS is virtually zero because all the components of the system are in service and the load is so small that a very large number of components would have to be outaged before any load would need to be disconnected. At the high end, the stress is so high that a small increase in load causes a complete system collapse. Between these two extremes, reference cases must be created to obtain regularly spaced markers on the EENS scale. Given a base case with all system components in service, these cases can be generated by adjusting the total load in the system until the desired value of EENS is obtained. This choice of reference cases is clearly not unique. The same values of EENS can also be approached by disconnecting some system components, up rating or de-rating some of the generation, and adjusting the load accordingly. The method that uses increase in total system load to create a set of cases, which have regularly spaced EENS, is called the first calibration technique. The method, which uses disconnecting some system components, up rating or de-rating some of the generation, and adjusting the load accordingly to create a set of cases, is called the second calibration technique. In terms of scaling the indicator of stress, two reference cases are identical as long as they have the same values of EENS. Given the usual qualifications regarding the confidence interval and the degree of confidence, comparing a new situation to any reference cases using correlated sampling should give the same result, as long as the criteria for convergence of the Monte Carlo simulation are satisfied.

4.4.2 Monte Carlo Simulation

The calculation of the EENS requires a Monte Carlo simulation of the behaviour of the power system. This simulation must reflect accurately the way a power system is operated and the information that is available in the operational time frame. In particular, the following features have to be modelled [1],[3].

- Effect of the weather conditions on the probability of line faults
- Cascade and sympathetic tripping of lines
- Heuristic representation of generator instability
- Under-frequency load shedding
- Post-contingency re-dispatch of active and reactive resources
- Emergency load shedding to prevent a complete system collapse
- Time required for restoration

While the representation of these factors makes the Monte Carlo simulation more complex, it provides a more realistic estimate of the EENS. Each trial of the Monte Carlo simulation corresponding to application of a random single or multiple contingencies to the state of the power system to be assessed. Figure 4.2 illustrates the processing done for each trial of the Monte Carlo simulation. This processing is similar to what was used in the Value of Security Assessor described in the previous chapter, with the exception that the Energy Not Served is not translated into a cost.

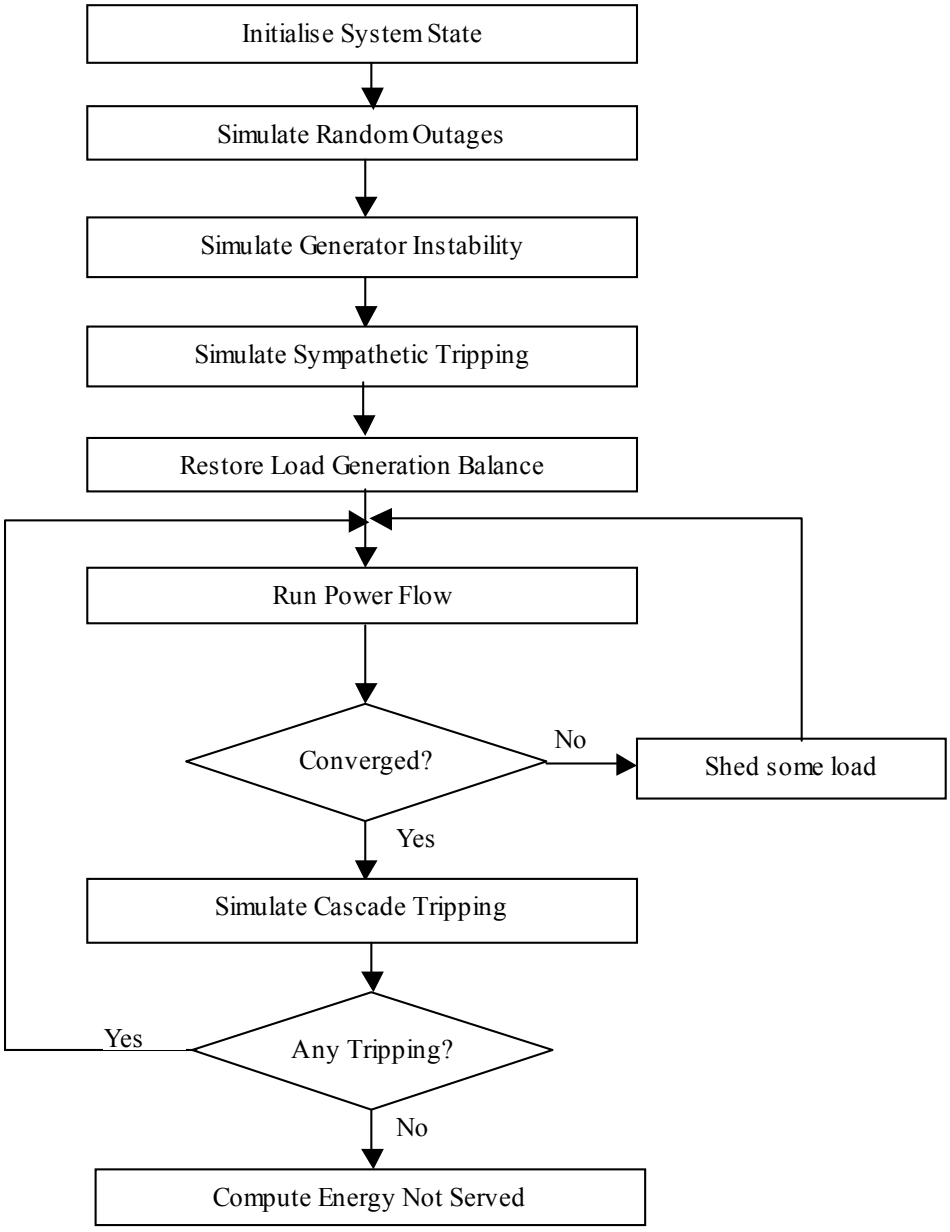

Figure 4.2: Flowchart of the Monte Carlo simulation for a particular trial for the calculation of energy not served (ENS).

Load can be disconnected for several reasons:

- Because the operator (or under-frequency relays) must react to restore the balance between production and consumption following an outage if generation cannot be ramped up sufficiently fast.
- Because the operator fears that a voltage collapse is unavoidable if load is not shed in a region, which is severely affected by transmission or generation outages.

- Because a bus fault or a set of line outages have isolated a load supply point
- Because the system voltage has collapsed.

If the Monte Carlo simulation encounters any of the above situations, a heuristic proportion of the load is shed. Load shedding begins from the largest mismatch zone in blocks of 5% of zone load and continues through the neighbouring zones until achieving the system equilibrium. Divergence of the power flow after 100 steps of load shedding indicates that the system has collapsed (a system blackout has occurred).

At the end of each trial, the amount of load disconnected is converted into the amount of energy not served using the model of load restoration in the VaSA [4]. When the simulation satisfies the criterion, which sets through the confidence interval and the degree of confidence of the Monte Carlo simulation, the estimation is terminated and the corresponding absolute value of EENS is used for the calibration of the indicator of stress.

4.4.3 Convergence Criteria

If μ represents the true population mean of energy not served and $\overline{X}$ is the mean energy not served estimated from a sample of *n* trials, the probability of the true mean lying within some interval $\overline{X} \pm L$ of the estimated mean is the degree of confidence γ, which is given by Equation (4.1).

$$\gamma = P\left(\overline{X} - L \le \mu \le \overline{X} + L\right) \tag{4.1}$$

If the sampling distribution is assumed normal, the confidence limit L is given by Equation (4.2).

$$L = t_{\alpha/2} \cdot \sigma_X \tag{4.2}$$

$$\gamma = 1 - \alpha \tag{4.3}$$

Where σ_X is the standard deviation of the estimate and $t_{\alpha/2}$ is found from the t-distribution with *n-1* degrees of freedom. When *n* is getting larger the t-distribution approximates the normal distribution (the standard normal distribution provides a good approximation to the t-distribution for sample size of 30 or more). Thus, given that the

estimate variance σ_X^2 is related to the variance of the population distribution σ^2 by Equation (4.4), we have:

$$\sigma_X^2 = \sigma^2 / n \tag{4.4}$$

For a pre-specified *L* and *γ,* the required number of trials may be found from Equation (4.5).

$$n = \left(\sigma^2 \; t_{\alpha/2}^2\right) / L^2 \tag{4.5}$$

Equation (4.5) shows that the number of trials required to achieve an answer within a given interval of confidence and with a given degree of confidence depends on the variance of the population. Since the population variance σ^2 is not known, it is replaced in Equation (4.5) by the sample variance s^2. (The sample variance is calculated at the end of each trial). Once a sufficient number of Monte Carlo trials have been analysed, the accumulated energy not served is divided by the number of trials to yield the expected energy not served.

In a naive Monte Carlo simulation, no special measure is taken to reduce the variance. A number of variance reduction techniques (VRTs) are used with the Value of Security Assessor (VaSA) to artificially reduce the estimated variance by pushing the value to be estimated towards the population mean [4]. Alternatively, VRTs reduce the number of trials and consequently the CPU time in a Monte Carlo simulation.

Another VRT has been developed for the calculation of the indicator of stress as with large power systems naïve Monte Carlo simulation doesn't converge due to significantly high load disconnections of system blackouts compared to the load disconnections of other events. The situation was unable to control with the existing VRTs in VaSA. The developed VRT is called extended stratified sampling.

4.4.4 Extended Stratified Sampling

In stratified sampling, a heterogeneous population is divided into homogeneous sub-populations. These homogeneous sub-populations are called strata. If each stratum is homogeneous, the measurements vary little from one trial to another. A precise estimate of the mean of any stratum can be obtained from a sample in that stratum. These estimates can then be combined into a more precise estimate for the whole population. The stratification variable can be chosen in accordance with a variable that has a positive correlation with the parameter to be estimated. In the case of the indicator of stress since the parameter to be estimated is EENS, the amount of load disconnection or in other words the shed load was used as the stratification variable as EENS is a function of disconnected loads.

In shed load stratification, the total system load is divided into a number of presumed strata. The optimum number of strata can be determined by testing the case with different number of strata and then observing the accuracy and the required numbers of trials as well as the CPU time. The span of the partition is determined by dividing the total system load by the squared value of the number of strata. This is because the performed experiments by dividing the system load by number of strata, squared value of number of strata and cubic value of number of strata showed that dividing by squared value of number of strata can best allocate EENS value avoiding emptying strata. Strata obviously cannot overlap. In large power systems, the load disconnections due to minor disturbances are quite small compared to the load disconnection due to a system blackout, as there are not many trials that give a value in between. Therefore, the proposed method for setting the number of strata can eliminate the empty strata. This type of partitioning distributes EENS values homogeneously within a stratum. When the simulation progresses, the value of Energy not Served (ENS) for each trial is allocated to the right stratum. Then the average and variance of the ENS are calculated for each stratum. These values are then combined to check the accuracy of the estimate. Convergence of the Monte Carlo simulation has been reached when the estimate has an accuracy satisfying the stopping rules.

Following mathematical formulations exist in stratified sampling [5]:

The estimate of the variance of the sample (unbiased estimate) within a stratum is given by Equation (4.6).

$$s_h^2 = \frac{1}{n_h - 1}\sum_{i=1}^{n_h}(y_{hi} - \bar{y}_h)^2 \tag{4.6}$$

The estimate of the variance with stratified random sampling is given by Equation (4.7).

$$v(\bar{y}_{st}) = s^2(\bar{y}_{st}) = \frac{1}{N^2}\sum_{h=1}^{L} N_h(N_h - n_h)\frac{s_h^2}{n_h} \tag{4.7}$$

The estimate of the mean of the sample within a stratum is given by Equation (4.8).

$$\bar{y}_h = \frac{\sum_{i=1}^{n_h} y_{hi}}{n_h} \tag{4.8}$$

Then the estimate of the population mean through stratified sampling is given by Equation (4.9).

$$\bar{y}_{st} = \frac{\sum_{h=1}^{L} N_h \bar{y}_h}{N} \tag{4.9}$$

Where,

N = $N_1+N_2+ \cdots\cdots + N_L$ = Total number of units (trials)

L = Total number of strata (Number of partitions)

N_h = Total number of units (Total number of trials) in h^{th} stratum

n_h = Number of units in a sample (Number of trials in a sample) in h^{th} stratum

N_h / N = Stratum weight

y_{hi} = Value obtained for the i^{th} unit (ENS value for the i^{th} trial) in h^{th} stratum

h = Stratum

i = Unit number (trial number) in a stratum

st = Stratified

4.4.5 Correlated Sampling

Correlated sampling is another variance reduction technique, which is also built into the Value of Security Assessor (VaSA). This technique is particularly well suited for the probabilistic indicator of stress because it can achieve a considerable reduction in CPU time when comparing cases. As its name suggests, correlated sampling takes advantage of the correlation that arises between the estimates of two quantities when Monte Carlo trials are carried out in parallel using the same random numbers. For applying correlated sampling to the comparison of the level of security between two cases, the operating states of the power system to be compared are subjected to the same contingencies. For each trial, the difference in the amount of load disconnected is thus due to inherent differences in the security of the cases. Instead of accumulating the estimates of the energy not served for the two cases separately, the difference in energy not served is tallied and the expected difference in energy not served is estimated using Equation (4.10).

$$\overline{\Delta X} = \frac{1}{n}\sum_{i=1}^{n}\overline{\Delta X_i} \tag{4.10}$$

Where, $\overline{\Delta X_i}$ is the difference in energy not served at the i^{th} trial and n is the number of correlated trials.

By definition, the confidence interval L is such that the true population mean lies within $\overline{\Delta X} \pm L$ of the estimated mean with a degree of confidence γ. Therefore, if $\overline{\Delta X} > L$ (or $\overline{\Delta X} < L$) the expected energy not served of one of the cases is greater (or smaller) than the expected energy not served of the other with a degree of confidence γ. The variance used in the convergence test is the sample variance of the difference between the energy not served of the two cases.

4.4.6 Auxiliary Convergence Criterion

An auxiliary convergence criterion is introduced for the cases where the system is not stressed. In these cases, the system is quite robust when subjected to random disturbances. Calculating the absolute values of EENS of such "healthy" cases requires a large number of trials for a precise estimate of ENS. This is particularly true for large, well-designed networks. In 'healthy' cases most of the Monte Carlo trials do not experience any load disconnection

The auxiliary convergence criterion is also called as the fixed standard deviation criterion, and is satisfied if the simulation satisfies Equation (4.11).

$$\sigma_X < \sigma_{\text{fix}} \tag{4.11}$$

Where σ_X is the estimated standard deviation of EENS. The fixed standard deviation σ_{fix} is the standard deviation of a reference case, which converges in a highest number of trials that is less than the user defined maximum number of trials. The standard deviation of this case is considered as the fixed standard deviation of all reference cases and is set for all the cases. This convergence criterion is imposed in parallel with the convergence criterion, which sets through the degree of confidence γ and the confident limit *L*. This introduces flexibility in satisfying either of these criteria for the cases that are quite healthy against random disturbances. This type of fixed standard deviations is commonly used in instrumentation.

For example in Figure 4.3, the $eens_1$ to $eens_4$ ($eens_1<eens_2<eens_3<eens_4$) denote the EENS of the reference cases of A_1 to A_4 and the σ_{x1} to σ_{x4} ($\sigma_{x1} <\sigma_{x2} <\sigma_{x3} <\sigma_{x4}$) denote the corresponding standard deviations when they are converged.

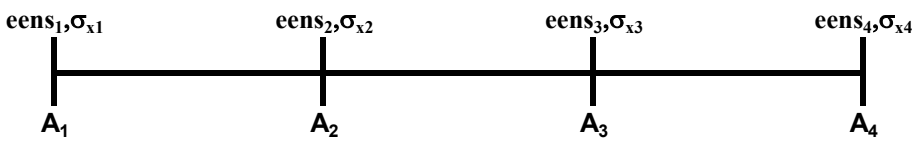

Figure 4.3: An example of levels of EENS of reference cases that are used for the clarification of the fixed standard deviation criterion.

Let the required number of trials to converge the cases A_1 to A_4 are n_1 to n_4 respectively ($n_1>n_2>n_3>n_4$). Cases A_1 and A_2 are assumed as healthy cases. If the maximum number of trials of the simulation is n_{max}, which is less than n_1 and n_2 and greater than n_3 and n_4 then the standard deviation of case A_3 (i.e., σ_{x3}) is considered as the fixed standard deviation for the cases A_1 and A_2 when need to force the convergence of cases A_1 and A_2 within n_{max} trails. Next, the Monte Carlo simulations are performed for the cases A_1 and A_2 considering the fixed standard deviation σ_{x3}. In other words, the required confident intervals of the cases A_1 and A_2 are widen to force the convergence of these two cases within n_{max} trials.

4.4.7 Statistical Tests

Three statistical tests are introduced for comparing the stress levels of new cases. These tests are performed using correlated sampling. The first test checks whether a new case has more stress than a reference case. The second test checks weather a new case has a less stress than a reference case. The third test checks whether a new case has about the same stress level as a reference case.

The first and second tests are performed with the correlated sampling as described in section 4.4.5.

In the third test, if the simulation achieves the degree of confidence γ at a particular trial and the confidence limit of this estimation at this trial is L with an estimated standard deviation of $\sigma_{X,}$ and if this confidence limit is less than half the resolution of the calibrated indicator of stress, then the simulation stops, indicating that the new case has about the same stress level as the reference case. Equation (4.12) shows the condition that is set for this test where $d_{resolution}$ is the resolution of the calibrated indicator of stress.

$$\left| t_{\alpha/2} \times \sigma_X \right| < 0.5 \times d_{resolution} \tag{4.12}$$

4.5 Calibration and Testing the Indicator of Stress

The proposed indicator of stress was calibrated and tested with both a small and a large network. The 24-bus IEEE Reliability Test System is considered as a small test system and a 1085-bus model of the NGT (UK) system is considered as a large network. This network is also a real power system.

4.5.1 24-bus IEEE Reliability Test System

The 24-bus IEEE Reliability Test System is shown in Figure 4.4 [6]. This is the base case for the small test system.

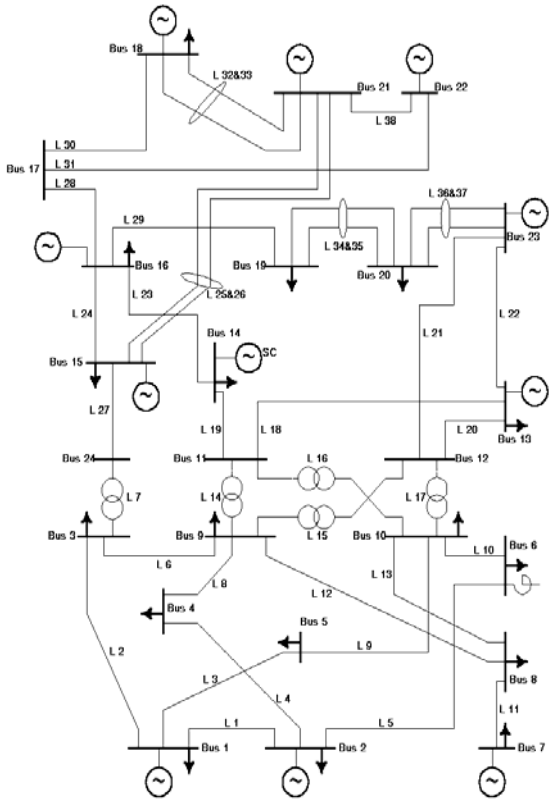

Figure 4.4: 24-bus IEEE Reliability Test System.

A first set of 9 reference cases, called reference scale A, was created by gradually and uniformly increasing the load from 57% of base load to 114% of base load in such a way that the resolution of the scale is about at 5MWh. The EENS of each of these cases

was calculated using naive Monte Carlo simulation. Since the ranking of these reference cases is more important than the absolute value of their EENS, their order was checked pair-wise using correlated sampling. Further, the ranking was also checked when the failure rates of the components was increased. These increased failure rates includes 10, 50 and 100 times the average failure rates of the system components. The purpose of this test was to verify whether the ranking remains robust when the number of large incidents increases. As expected, the values of EENS increased with higher failure rates, and the regular spacing of EENS between consecutive reference cases was lost. However, even with higher failure rates the ranking remained robust.

A second reference scale, called reference scale B, was created by taking out of service or de-rating some components and then adjusting the system load accordingly. Table 4.1 shows the changes of these reference cases with respect to the base case.

Table 4.1: Definition of the reference cases of scale B of 24-bus IEEE Reliability Test System

Case	**Changes with respect to base case**
B1	None
B2	L32, L33, L5 disconnected
B3	L36, L37, L2 disconnected
B4	L31, L3 disconnected
B5	L18 and 2 x 80 MW generation at bus 7 disconnected Remaining generator at bus 7 de rated to 60MW Generation at bus 1 up rated by 30 MW Generation at bus 2 up rated by 2 x 30 MW Generation at bus 23 up rated by 30 MW and 60 MW
B6	L6, L15, L30 disconnected
B7	L9 disconnected 40 MW of generation at bus 1 disconnected Generation at bus 23 up rated by 40 MW
B8	L29, L8 disconnected
B9	L14, L38 disconnected

To test the effectiveness of the proposed technique, four new cases corresponding to increasing amounts of system stress were created and evaluated using the two calibrated reference scales. Table 4.2 describes these new cases.

Table 4.2: Definition of the new cases of 24-bus IEEE Reliability Test System

Case	Description of the case
C1	Load ratio = 1.5 L2, L29, L25, L26 disconnected
C2	Same as case C1 plus: One generators at bus 2 is disconnected (40 MW) Compensated by additional 40 MW at bus 23
C3	Same as C2 plus: L18 disconnected
C4	Same as C3 plus: Generation at bus 7 decreased by 60 MW Generation at bus 1 decreased by 30 MW Generation at bus 15 increased by 15 MW Generation at bus 16 increased by 15 MW Generation at bus 23 increased by 60 MW

All tests were repeated three times. The minimum and maximum trials for calculating the absolute values of ENS through naive Monte Carlo simulation are 10,000 and 25,000 respectively. The minimum and maximum trials for positioning reference cases within the scale and also measuring up the stress levels of the new cases through the correlated sampling are 2000 and 25000 respectively. Degree of certainty of the results is 90% with a confidence limit of 10%.

The minimum number of trials of the naive Monte Carlo simulation was set considering the expected number of trials needed to experience at least one system blackout. Such an estimate can be obtained by running set of cases, which are used to calibrate the indicator of stress and then observing the average number of trials required to experience a system blackout. These investigations showed that running 10,000 trials leads to a very high probability of experiencing a system blackout. In correlated sampling the minimum number of trials was set considering the expected trials required to experiencing a load disconnection in all the cases that are correlated. These investigations showed that setting a minimum of at least 2000 trials leads to a very high probability of experiencing a load disconnection in a case.

Correlated sampling and the naive Monte Carlo simulation have the same number of maximum trials. Designing an indicator of stress for the 24-bus IEEE Reliability Test System did not require a variance reduction technique, as convergence could be

achieved with the naive Monte Carlo simulation in a reasonable number of trials. This is because in 24-bus IEEE Reliability Test System the loads disconnections due to system blackouts and due to other events are homogeneous.

4.5.2 1085-bus Model of the NGT (UK) System

The proposed indicator of stress has also been tested on a model of the NGT (UK) system based on the state estimator output at 17.56 hour on 1st September 2001. The state estimator output of this network model consists of 1085 busses, 1822 transmission lines and transformers, and 137 generating units. System maximum active and reactive generations at this snapshot are 56.2GW and 26.08GVAr respectively. State estimator output active and reactive demands are 33.28GW and 2.31GVAr respectively and the active and reactive power generation are 33.67GW and 5.74GVAr respectively. This snapshot represents typical operating conditions for the NGT (UK) system, neither particularly stressed nor particularly light. This network model is used as the base case for developing indicator of stress for the NGT (UK) system.

Scale A was calibrated by gradually and proportionally increasing the system active and reactive load from 58% of system base load to 124% of the base load to create 17 reference cases. It should be noted that this model is a snapshot of an output of the state estimator used at the NGT control centre. As such it reflects the operating conditions on that day. Therefore it does not reflect the full capacity of the NGT (UK) system because some lines, generators were not in service because they were not needed or were on scheduled or unscheduled outage.

During the calibration process of the probabilistic indicator of system stress on the NGT (UK) system model, the Monte Carlo simulation and stratified sampling with shed load stratification were used to calculate the absolute values of EENS for the reference cases. Investigations were also performed with the following VRTs [4]:

- Antithetic variate
- Control variate
- Importance sampling

- Stratified sampling with MVA stratification (I.e., Line flow is used as the stratification variable)
- Stratified sampling with MW/ MVAr stratification (I.e., System active and reactive power is used as the stratification variable)

None of these VRTs achieved the same level of performance as the stratified sampling with shed load stratification.

The reason why stratified sampling with shed load stratification was necessary is that, in the NGT (UK) system model, there is a very large difference between the average load disconnection due to minor events and the load disconnection caused by rare events such as system blackouts. These large differences in the magnitude of the load disconnection make convergence of the naive Monte Carlo simulation impossible. Stratified sampling must therefore be used because it allows the Monte Carlo simulation to converge for the two types of events separately before combining them into a single value of EENS.

This scheme reduced the variance considerably while maintaining the accuracy requirements compared to the naive Monte Carlo simulation. However, the number of trials required for convergence remains extremely large. System blackouts were thus ignored when estimating the absolute value of EENS.

Stratified sampling was applied by defining six strata. The first stratum contains the trials that do not experience load disconnections. The 6^{th} stratum contains the trials that lead to larger disconnections, such as partial blackouts, but not total system blackouts as they are ignored. The other four strata cover the remaining load disconnections. Stratified sampling is efficient if the variation between the strata means is sufficiently large compared with within-strata variation and if the stratification variable is positively correlated with the parameter to be estimated [7].

Through the first calibration technique, which uses a progressive increase in active and reactive demand to define the reference cases, the absolute EENS values of the reference cases were estimated. The number of Monte Carlo trials required to determine

the fixed standard deviation is considered as the reference of the maximum number of trials. Therefore, the maximum number of trials of the Monte Carlo simulations should be greater than the reference maximum number of trials. For the estimation of the absolute values of EENS for the reference cases, the minimum number of trials was set at 10,000 and the maximum at 100,000. The degree of certainty for convergence was 90% with a confidence limit of 10%. An additional criterion for convergence was also applied by introducing a fixed-standard deviation, which is same for all the reference cases. Therefore, estimating the absolute values has freedom to satisfy either:

- Criteria on certainty
- Criterion on fixed standard deviation

These reference cases were also compared using Correlated Sampling [8] to check that they are in the right order on the scale. In the case of correlated sampling, the minimum number of trials was set at 2,000 and the maximum number of trials was set at 25,000. The requirement for the degree of certainty was set to 90%. When testing the new cases on the calibrated indicator of stress the simulation stops either if it meets 90% certainty to reflect a new case has a more or less stress than a reference case or if the new case has the same stress level of stress as a reference case.

Correlated Sampling was performed by ignoring system blackouts as well as considering system blackouts to investigate the influences. The fidelity of the calibrated indicator of stress was tested with some of the new operating scenarios, which are made in ascending order of system stress. Five such new cases were used to test the calibrated indicator of stress.

System blackouts were ignored throughout the comparisons of these new cases as they compromise the convergence demanding significantly higher number of trials for a precise comparison.

Investigations performed using Correlated Sampling, by considering all load disconnections including system blackouts and then excluding system blackouts suggest that ignoring system blackouts has a very small probability of making a difference in

the conclusion of the comparison of new cases. For example when compare the cases with Correlated Sampling including and excluding system blackouts, 8 to 10 comparisons out of 10 comparisons remained in the same conclusion of stress level under both situations.

The indicator of stress was also calibrated using the second calibration technique where the reference cases are created by disconnecting some components, up-rating and de-rating plants, and adjusting the system load accordingly to obtain the same stress level of cases as in the first calibrating technique. The same process as in the first calibration technique was used to fit the reference cases on the scale and to compare new cases.

4.6 Results

4.6.1 24-bus IEEE Reliability Test System

Figures 4.5(a) and 4.5(b) show the probabilistic indicator of system stress calibrated using the first and second calibration techniques respectively.

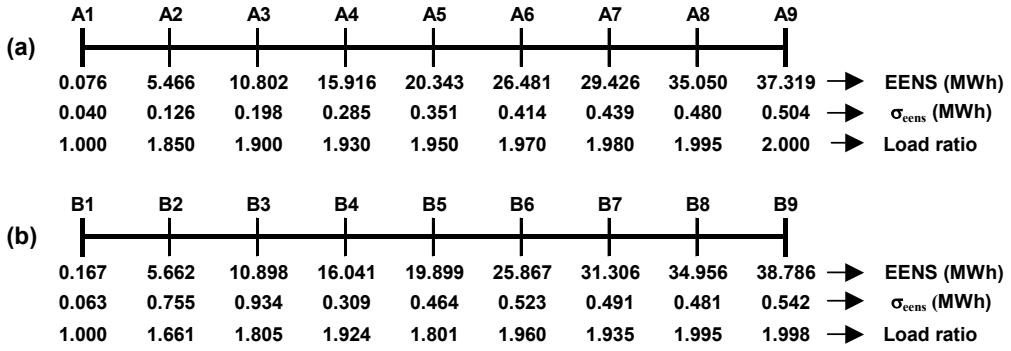

Figure 4.5: Scale A, Scale B and corresponding EENS, standard deviations of the estimates and load ratios of each of the reference cases. Figure 4.5(a) shows the calibrated scale A and Figure 4.5(b) shows the calibrated scale B. The load ratio is the load level with respect to the minimum feasible load (i.e., 0.57 x system base load).

Figure 4.6(a) and 4.6(b) show the stress levels of new cases measured using the calibrated indicators of system stress.

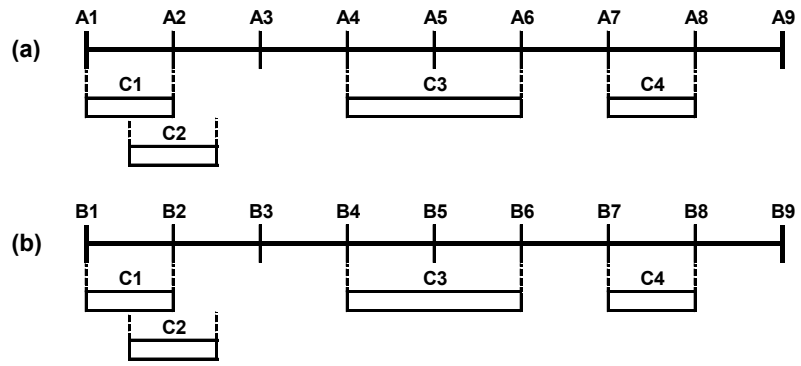

Figure 4.6: New cases measure up on scale A and scale B. Figure 4.6(a) corresponds to scale A and Figure 4.6(b) corresponds to scale B.

It is clear from Figures 4.5(a) and 4.5(b) that the relation between the loads level and the EENS is non-linear. Towards the top of the scale, a very small change in the overall loading has a much larger effect on the EENS than towards the bottom of the scale.

Tables 4.3 & 4.4 show the conclusion reached about the measured stress levels of the new cases. A comparison between Figures 4.5(a) and 4.5(b) suggests that the ways of calibrating the indicator of stress are not affecting the conclusions of stress level. The little black rectangles show the intervals within which the EENS of the new cases exist with 90% confidence. Stress level of any new case can be bounded by two reference cases or centred over a reference case on scale A or scale B.

For example referring to Figure 4.6(a), which represents the measurements with scale A, it can be stated with 90% certainty that the EENS of new case C1 is greater than the EENS of reference case A1 and smaller than the EENS of reference case A2. It can be stated with more than 90% certainty that the EENS of new case C2 is similar to reference case A2. The results of the comparison between new case C3 and reference case A5 are not conclusive. We can only say that the EENS of new case C3 is between the EENS of reference case A4 and the EENS of reference case A6. It can be stated

with 90% certainty that the EENS of new case C4 is greater than case A7 and smaller than case A8. Table 4.3 gives more details of the correlated sampling simulations of these comparisons.

Table 4.3: The measured stress levels of new cases on scale A of 24-bus IEEE Reliability Test System.

Test	**Δ*eens***	**$\Delta\sigma_{eens}$**	**Trials**	**Conclusion**	**Confidence**
A1-C1	-0.867	0.403	2808	A1 < C1	90%
	-1.225	0.62	2291	A1 < C1	90%
	-0.857	0.353	3902	A1 < C1	90%
A2-C1	5.244	0.783	2808	C1 < A2	90%
	4.313	0.98	2291	C1 < A2	90%
	4.312	0.637	3902	C1 < A2	90%
A1-C2	-6.042	3.071	2937	A1 < C2	90%
	-3.289	1.485	6089	A1 < C2	90%
	-5.986	2.484	3657	A1 < C2	90%
A2-C2	-0.751	1.05	25000	A2 ~ C2	91%
	-0.112	1.04	25000	A2 ~ C2	98%
	0.345	0.979	25000	A2 ~ C2	98%
A3-C2	1.807	6.32	5065	C2 < A3	90%
	3.142	8.325	2024	C2 < A3	90%
	2.505	5.27	3657	C2 < A3	90%
A4-C3	-12.39	7.244	3104	A4 < C3	90%
	-22.531	10.872	2016	A4 < C3	90%
	-4.995	3.025	12280	A4 < C3	90%
A5-C3	-0.513	2.21	25000	C3 ~ A5	64%
	0.269	2.183	25000	C3 ~ A5	70%
	7.122	4.314	3814	C3 < A5	90%
A6-C3	4.539	2.759	16112	C3 < A6	90%
	6.063	3.653	9236	C3 < A6	90%
	12.584	6.488	2002	C3 < A6	90%
A7-C4	0.616	2.645	25000	C4 ~ A7	53%
	-5.226	3.044	22713	A7 < C4	90%
	-13.106	7.518	4657	A7 < C4	90%
A8-C4	6.247	3.776	12117	C4 < A8	90%
	-1.412	2.985	25000	C4 ~ A8	29%
	3.253	2.82	25000	-	-
A9-C4	13.816	8.374	2019	C4 < A9	90%
	0.641	2.989	25000	C4 ~ A9	47%
	4.734	2.875	24550	C4 < A9	90%

In Table 4.3, the first column shows the comparison that were carried out; the second shows the estimated difference between the EENS of the reference case and the EENS of the new case; the third shows the standard deviation of this estimate; the fourth shows the number of Monte Carlo trials, the fifth shows the conclusion that can be

drawn from this test and the last column shows the degree of confidence that can be attached to this conclusion. Table 4.4 shows the results obtained with scale B.

Table 4.4: The measured stress levels of new cases on scale B of 24-bus IEEE Reliability Test System

Test	**$\Delta eens$**	**$\Delta\sigma_{eens}$**	**Trials**	**Conclusion**	**Confidence**
B1-C1	-0.744	0.365	2612	B1 < C1	90%
	-1.136	0.351	5448	B1 < C1	90%
	-1.464	0.507	3675	B1 < C1	90%
B2-C1	4.4	2.416	4396	C1 < B2	90%
	5.046	2.708	5448	C1 < B2	90%
	3.173	1.858	7058	C1 < B2	90%
B1-C2	-4.55	2.498	2602	B1 < C2	90%
	-8.634	3.683	3420	B1 < C2	90%
	-10.061	5.14	2125	B1 < C2	90%
B2-C2	-0.509	0.461	25000	B2 ~ C2	92.85%
	-0.72	0.466	25000	B2 ~ C2	89.86%
	-0.512	0.449	25000	B2 ~ C2	93.08%
B3-C2	3.928	2.252	17215	C2 < B3	90%
	16.223	8.136	3420	C2 < B3	90%
	4.109	2.264	15360	C2 < B3	90%
B4-C3	-13.500	8.169	2511	B4 < C3	90%
	-4.718	2.769	15375	B4 < C3	90%
	-3.862	2.341	19904	B4 < C3	90%
B5-C3	-11.888	6.843	3615	B5 < C3	90%
	-1.713	2.146	25000	B5 ~ C3	28.67%
	0.010	2.132	25000	B5 ~C3	77.07%
B6-C3	2.419	2.28	25000	C3 ~ B6	2.92%
	7.089	4.298	6700	C3 < B6	90%
	13.149	7.878	2344	C3 < B6	90%
B7-C4	-6.538	3.782	15910	B7 < C4	90%
	8.251	4.963	4975	C4 < B7	90%
	-0.302	2.764	25000	B7 ~ C4	57.72%
B8-C4	-2.079	2.984	25000	C4 ~ B8	11.29%
	9.074	5.469	4536	C4 < B8	90%
	8.184	4.929	6752	C4 < B8	90%
B9-C4	12.647	7.652	2868	C4 < B9	90%
	10.416	6.142	4020	C4 < B9	90%
	9.362	5.645	5767	C4 < B9	90%

These results suggest that there is a trade-off to be made between the resolution of the scale used for the probabilistic indicator of stress and the confidence that can be attached to the estimates based on that scale.

4.6.2 1085-bus Model of the NGT (UK) System

Figures 4.7(a) and 4.7(b) show the calibrated indicators of system stress of the 1085-bus model of the NGT (UK) system using the first (i.e., scale A) and second calibration techniques (i.e., scale B) respectively.

Figures 4.7(c) and 4.7(d) show the stress levels of new cases measured using the scales A and B respectively.

The indicator's span has been divided into two regions. The first region extends up to 2MWh of EENS along the calibrated scale where the resolutions are slightly unequal, and the second region, which starts from 2MWh of EENS level along the calibrated scale, has a uniform resolution of 2MWh. The first region was created to measure the stress levels of average day events. Since the system stress with respect to the variables that use to calibrate the indicator of stress is highly non-linear at the lower end of the scale it is difficult to obtain a uniform resolution throughout the scale. This is the reason for defining two resolution levels of stress platforms along the calibrated scales.

The indicator of stress is calibrated for the feasible load limit with only the available generation. The span of the scale could not be extended further as the information supplied by the state estimator output does not show generators that are not committed.

It is also very important to re-calibrate the indicator of stress if the system is connected with new busses, new generating plants, new transmission lines, new transformers, and new compensating devices. This is because the Correlated Sampling applies the same set of contingencies to both networks (i.e., comparing networks). Both networks should therefore have the same configuration although the components states can be different.

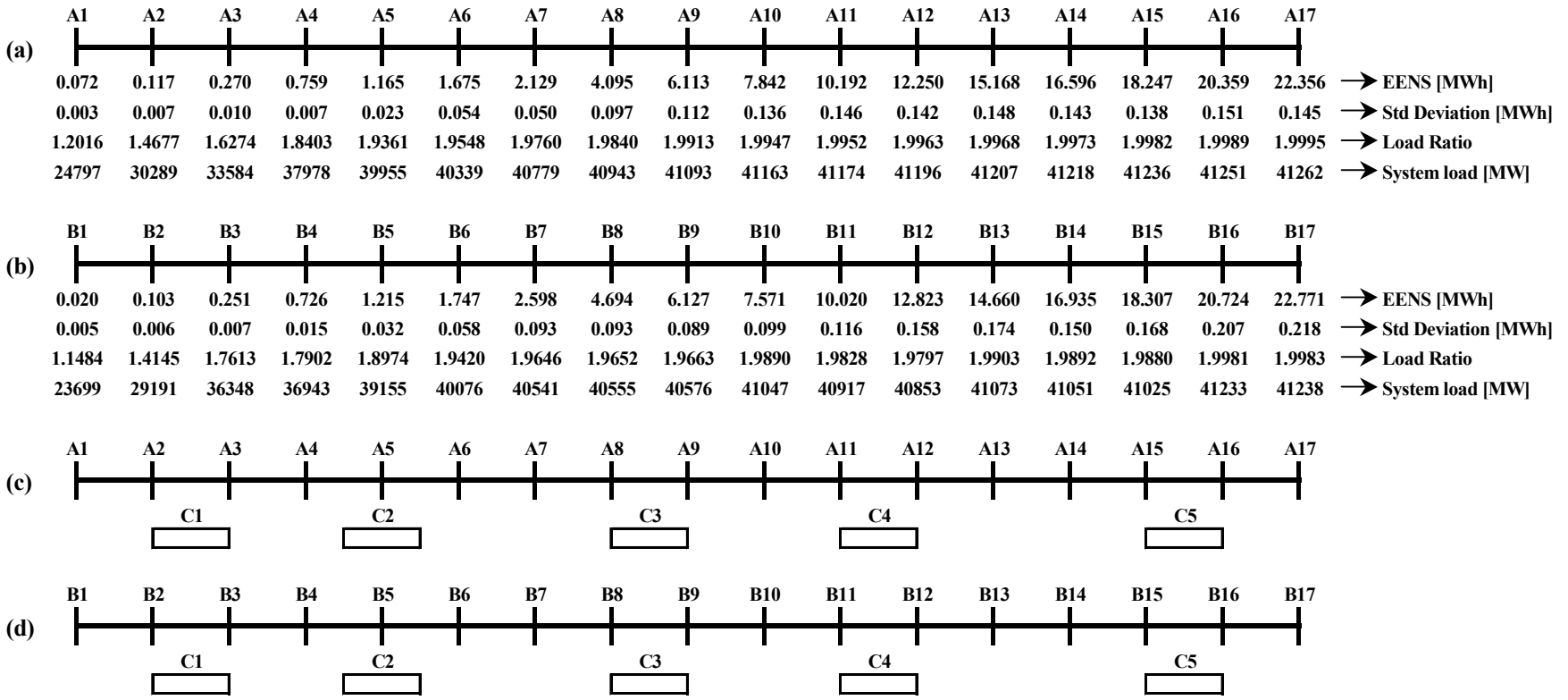

Figure 4.7: Calibrated indicators of stress of the 1085-bus model of the NGT (UK) system and measured stress levels of the new cases. Figure 4.7(a) shows the indicator of stress calibrated using the first calibration technique (scale A). Figure 4.7(b) shows the indicator of stress calibrated using the second calibration technique (scale B). Figure 4.7(c) shows the stress levels of new cases measured using scale A. Figure 4.7(d) shows the stress levels of new cases measured using scale B.

The indicator of stress that is shown in Figure 4.7(b) (i.e., scale B) is also calibrated to achieve similar resolutions and similar absolute values of EENS as in the scale A. This enables compare both calibration techniques. When comparing both calibration techniques in terms of CPU time, the second calibration technique used about 10% more CPU time than the first calibration technique. This is because the simulated random contingencies in the reference cases, in some occasions, lead to infeasible system operation resulting in larger load disconnections. With respect to the first calibration technique, as an average, it takes about 1 to 2 hours to simulate a reference case for absolute values and 30 to 40 minutes for measuring the stress of a new case. Lower resolution in a calibrated scale can lower the CPU time demand when comparing new cases. This is because a lower resolution in a scale increases the difference between stress levels of consecutive reference cases, which on the other hand increases the confidence limit that is used to identify whether a new case is centred over a reference case with the degree of confidence γ. In this test the half of the resolution, which is the confidence limit in this test is used to determine the degree of confidence of the conclusion and the details about this test is given in section 4.4.7. This enables to reduce the required number of trials for a conclusion or in other words achieves a relatively faster convergence due to lengthen confident interval.

According to Figure 4.7(c) (i.e., with respect to scale A) it can be concluded with 90% certainty that the system stress of the, first new case C1 is between the stress level of reference cases A2 and A3; the second new case C2 has a stress level similar to the level of the reference case A5; the stress of the third new case C3 is between the stress level of reference cases A8 and A9; the stress of the fourth new case C4 is between the stress levels of the reference cases A11 and A12; and the fifth new case C5 is between reference cases A15 and A16. Table 4.5 shows more details about these conclusions.

Table 4.5: The measured stress levels of new cases on scale A of 1085-bus model of the NGT (UK) system.

Case	$\Delta eens$	$\Delta\sigma_{eens}$	Trials to converge	Conclusion	Confidence
C1-A3	-0.022	0.013	3165	C1 < A3	90%
C2-A5	-0.005	0.003	2000	C2 ~A5	90.223%
C3-A8	2.544	1.54	5383	C3 > A8	90%
C3-A9	-5.513	3.33	2000	C3 < A9	90%
C4-A11	1.836	1.092	16104	C4 >A11	90%
C4-A12	-3.339	1.988	3196	C4 < A12	90%
C5-A15	4.411	2.639	2828	C5 > A15	90%
C5-A16	-6.558	3.610	2000	C5 < A16	90%

There are negligible differences in absolute values in scale B as fine-tuning of the indicator of stress for exact values through both calibrating techniques is difficult due to the random nature of the outages. According to Figures 4.7(c) and 4.7(d) the conclusions obtained with the indicator of stress calibrated using the first calibration technique were not affected even when the indicator of stress was calibrated through the second calibration technique. With respect to the scale B (i.e., Figure 4.7(d)), it can be concluded with 90% certainty that the stress of the first new case C1 is between reference cases B2 and B3. The third new case C3 is between reference cases B8 and B9. The fourth new case C4 is between reference cases B11 and B12. Finally, the fifth new case C5 is between reference cases B15 and B16. The stress of the second new case C2 is similar to the stress level of the reference case B5. This conclusion carries a 95.88% of certainty. Table 4.6 gives more details about these conclusions.

Table 4.6: The measured stress levels of new cases on scale B of 1085-bus model of the NGT (UK) system.

Case	$\Delta eens$	$\Delta\sigma_{eens}$	Trials to converge	Conclusion	Confidence
C1-B3	-0.150	0.089	19246	C1<B3	90%
C2-B5	-0.055	0.033	2000	C2~B5	95.88%
C3-B8	2.019	1.149	7799	C3>B8	90%
C3-B9	-1.885	1.145	5394	C3<B9	90%
C4-B11	7.386	4.368	2059	C4>B11	90%
C4-B12	-4.242	2.505	5484	C4<B12	90%
C5-B15	2.567	1.558	9858	C5>B15	90%
C5-B16	-4.660	2.749	3293	C5<B16	90%

This similarity of measurements in the calibrated scale allows flexibility in choosing a technique for calibrating and testing. Calibrating the indicator of stress with a lower level of resolution may indicate same level of stress for average day events as well as events that are slightly more stressed than average day events. Therefore choosing the resolution of the indicator of stress is a key issue when calibrating the indicator of stress.

4.7 How to Use in Power System Operation?

Proposed indicator of stress is network specific. It should be benchmarked into specific stress zones, for example normal, alert and emergency. These three zones can be defined based on the system operators' experience or off-line calculation of EENS using a Monte Carlo simulation from a set of selected new cases. Once benchmarked the three stress zones, the system stress at a particular operating condition should be located within one of these three stress zones. The stress level of the current operating condition can be identified by correlating current operating condition with reference cases using correlated sampling.

If the measured stress level of the current operating condition is in emergency zone, the operator should do something immediately. The operator can test actions aimed at reducing the stress by using the same indicator of stress. In this way, the operator has the information to decide the best remedy to lower the stress.

The indicator of stress is proposed for power system operational use although it could also be used for power system planning. When used for operations, the current state estimator output is correlated with the reference cases. When used for planning, possible-operating conditions that simulate operating plans and abnormal operating conditions are correlated with reference cases to identify the system stress of these new cases.

4.8 Benefits of the Indicator of System Stress

There are cases, where a system is classified as 'N-1' secure by conventional security assessment tools, but happens to be very stressed. On the other hand, there are cases where the system is classified as 'N-1' insecure but is only lightly stressed. Such a situation is illustrated in the following example based on the 24-bus IEEE Reliability Test System that is shown in Figure 4.4. There are two new cases. The first case (Cx) has a load ratio of 1.5 where the lines L2, L18, L21, L25, and L32 are disconnected. In the second case (Cy), lines L3, L4, L22, L25, L30, L32, L34, L36, L38, and reactor at bus 6 are disconnected. 100MW of load connected at bus 6 was shifted to bus 8 (50MW) and bus 10 (50MW). 80MW from bus 1 and 90MW from bus 3 are also shifted to bus 5 (50MW), bus 7(20MW) and bus 15 (100MW). Then the load ratio is set to 1.79. In this example the failure rate of L26 is set to 10.0 as the outage of L25 heavily stresses L26. According to the contingency analysis, the first case (Cx) is 'N-1' insecure as thermal and voltage limit violations exist for 'N-1' contingency and the second case (Cy) is 'N-1' secure, as no violations exist for any 'N-1' contingency. Figure 4.5a shows the calibrated indicator of stress for this test system using the first calibration technique. Figure 4.8 shows the measured stress levels of cases Cx and Cy on this scale. Table 4.7 shows more detailed conclusions of these measurements.

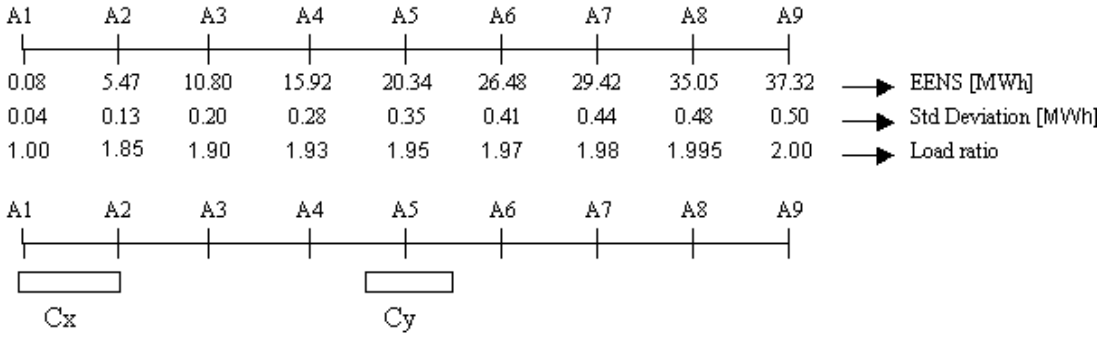

Figure 4.8: Calibrated indicator of stress for 24-bus IEEE Reliability Test System and measured stress levels of cases Cx and Cy.

Table 4.7: Conclusions of the cases Cx and Cy.

Test	ΔEENS	σ	Trials	Conclusion	Confidence
A1-Cx	-2.729	1.407	7720	A1<Cx	90%
A2-Cx	3.435	1.5	4435	A2>Cx	90%
A5-Cy	0.053	1.673	5461	A5~Cy	90.518

According to stress measurements that are shown in Figure 4.8 and Table 4.7, although the case Cx is 'N-1' insecure it has a lower level of stress (stress level less than case A2 but more than case A1 with a 90% degree of confidence) and case Cy is 'N-1' secure but very stressed (stress level similar to case A5 with a more than 90% degree of confidence). Cases such as Cy could have devastating consequences because the operators may be unaware of the actual level of stress in the system.

Therefore, the ability of identification of such operating conditions is a particular advantage of proposed indicator of stress in operators' perspectives.

The indicator of stress can be used to signal the operator on the current level of stress and additionally it can be used to identify the suitability of the remedial action to relieve the system of stressing. Existing power system tools are less informative on indicating how close the current operating state to a more problematic state. Proposed indicator provides quantitative indication of system security.

4.9 Summary

A novel probabilistic indicator of system stress is proposed in this chapter. The indicator is calibrated with two alternative calibrating methods to investigate the performance. The first calibrating technique uses system load to vary the levels of system stress in a network. The second technique takes some system components out of service, up-rates and de-rates plants, and then adjust system load to create a set of cases that have the same levels of stress as in the first calibrating technique. The system active and reactive loads are adjusted proportionally. Monte Carlo simulation is used for estimating the metric of indicator for absolute values. With large power systems the Monte Carlo simulation requires techniques to reduce artificially the variance of the

estimate. Stratified sampling with stratification of the shed load is introduced to reduce the variance of the estimate effectively. Correlated sampling is used for comparing the reference cases to determine their position in the scale and to measure the stress levels of new cases on the calibrated indicator. The ranking of the calibrated indicator is also tested for the robustness.

A new stopping rule is introduced for Monte Carlo simulation and is referred as fixed standard deviation criterion. Fixed standard deviation criterion applies in parallel with the standard stopping rules. The fixed standard deviation criterion is very useful for estimating ENS of healthy cases through the Monte Carlo simulation, as these cases are very rarely vulnerable to load disconnections.

Three statistical tests are also introduced to measure the stress levels of new cases. The first rule examines whether a new case is more stressed than a reference case, the second test examines whether a new case is less stressed than a reference case and the third test examines whether a new case has the same stress level as a reference case.

Indicators of stress were developed for the 24-bus IEEE Reliability Test System and the 1085-bus model of the NGT (UK) system. Their validity was tested by creating a set of new cases that represent a set of operating conditions in a power system. The proposed indicator of stress measures the system stress quantitatively rather than qualitatively or binarily as conventional security assessment programs do.

4.10 References

[1] M. Rios, D. S. Kirschen, D. Jayaweera, D. P. Nedic, and R. N. Allan, "Value of Security: Modelling Time-Dependent Phenomena and Weather Conditions," *IEEE Transactions on Power Systems*, vol. 17, pp. 543-548, 2002.

[2] G. J. Anders, *Probabilistic Concepts in Electric Power Systems,* New York: John Wiley, 1990.

[3] D. S. Kirschen, K. R. W. Bell, D. P. Nedic, D. Jayaweera, and R. Allan, "Computing the Value of Security," presented at IEE PSMC, London, 2002.

[4] M. Rios, D. Kirschen, and R. Allan, "Computation of the Value of Security: Final Report - Volume II," University of Manchester Institute of Science and Technology, Manchester, UK, November 1999.

[5] W. G. Cochran, *Sampling Techniques*, 3rd Edition ed. USA: John Wiley and Sons, Inc., 1977.

[6] C. Grigg, P. Wong, P. Albrecht, R. Allan, M. Bhavaraju, R. Billinton, Q. Chen, C. Fong, S. Haddad, S. Kuruganty, W. Li, R. Mukerji, D. Patton, N. Rau, D. Rappen, A. Schneider, M. Shahidehpour, and C. Singh, "The IEEE Reliability Test System - 1996," *IEEE Transactions on Power Systems*, vol. 14, pp. 1010-1020, 1999.

[7] V. Barnett, *Elements of Sampling Theory*, 1st ed. London: The English University Press Ltd., 1974.

[8] D. S. Kirschen, D. Jayaweera, D. Nedic, and R. N. Allan, "Probabilistic Indicator of System Stress," presented at 7th International Conference on Probabilistic Methods Applied to Power Systems, Naples, Italy, 2002.

Chapter 5

Comparison of Deterministic and Probabilistic Security Criteria

5.1 Introduction

The current practice within the electricity supply industry is to use deterministic methods to perform security studies. These deterministic methods determine the security margins that is needed to cover possible unpredictable contingencies. A real and tangible price must sometimes be paid for using this approach because the operating conditions that are deemed secure can be overly conservative because on the emphasis placed on the most severe, credible events. On the other hand, this approach occasionally ignores some dangerous combinations of contingencies because they are deemed not credible. In these situations, the price to be paid is an increased risk of blackout. Unfortunately, as recent events have demonstrated again, this increased risk occasionally translates in actual costs when a blackout occurs.

To operate a power system beyond the traditional deterministic security limits, more refined security assessment methods are needed. These methods should take into account the probabilistic nature of many uncertain events. Probabilistic approaches are widely regarded in academic circles as more rigorous than deterministic approaches.

This chapter explores deterministic and probabilistic security criteria through modified 24-bus IEEE Reliability Test System (1996). The outcomes of these approaches are integrated in chapter 6 for defining the adaptive deterministic security criteria.

Following sections of this chapter detail the network that is used for the deterministic and probabilistic security assessments, the distributed slack bus, calculation of deterministic security boundary, estimation of probabilistic cost of security considering

the weather effects and influences of system blackouts, and a comparison of the results of deterministic security boundary and probabilistic cost of security levels.

5.2 Network

Figure 5.1 shows the network that is used for calculating the deterministic security boundary and probabilistic cost of security. This is the same network as was used in [1] for the comparison of deterministic and probabilistic approaches.

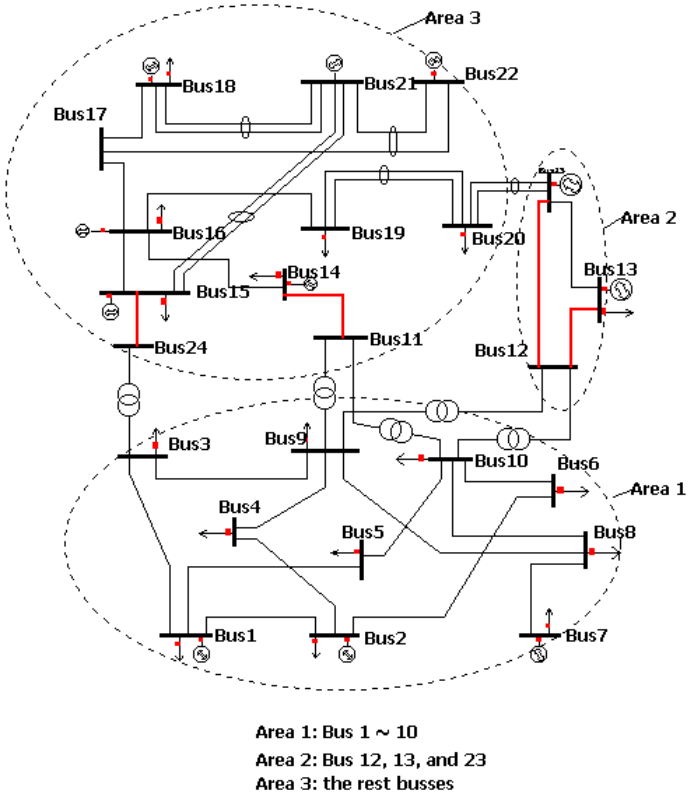

Figure 5.1: Modified 24-bus IEEE Reliability Test System (1996).

The network shown in Figure 5.1 is constructed by modifying the 24-bus IEEE Reliability Test System (1996) [2] to contrive a security constrained region as it can clearly demonstrate the benefits and differences between deterministic and probabilistic security criteria.

Following are the modifications that were performed on IEEE Reliability Test System (1996) to construct the network shown in Figure 5.1.

- Line from bus 11 to bus 13 is disconnected
- Set terminal voltages of the generators connected at bus 23 to 1.012p.u and bus 15 to 1.045p.u.
- Reactor connected at bus 6 is disconnected
- Shift 480 MW of load from busses 14, 15, 19, 20 to bus 13.
- Add generation capacity at busses 1 (100 MW unit), 7 (100 MW unit), 15 (100 MW unit, 155 MW unit), 13 (197 MW unit), 23 (2x155 MW unit)
- Change the outage rates of lines from bus 12 to bus 23, bus 13 to bus 23, and bus 11 to bus 14 to 0.11, 5, and 10 respectively
- Two new generators (which are not existing with the network in [1]) are also existing with the network shown in Figure 5.1.
    - The new generator connected at bus 13 has an installed capacity of 197 MW
    - The new generator connected at bus 23 has an installed capacity of 300 MW

5.3 Identification and Adjusting Study Parameters

Once determined the network it is necessary to identify the study parameters and ways of adjusting these parameters. Study parameters are the parameters that can be used to identify operational limits. Ways of adjusting the study parameters are called study criteria.

As shown in the Figure 5.1, the system is divided into three areas called Area-1, Area-2, and Area-3. The basic idea is that significant North-to-South transfers cause high flow through Area-2 and the interconnection between Area-1 and Area-3, which causes overload and voltage problems. Area-2 can alleviate the severity of these problems by shifting generation from bus 23 to bus 13. Thus the study parameters are the total 'North to South flow' and the 'Generation at bus 23'. The study parameters are varied according to the following criteria.

$$\Delta P_{23} = -\Delta P_{13} \tag{5.1}$$

$$\Delta p_{area3} = -\Delta p_{area1} \tag{5.2}$$

Where ΔP_{23} is the change in active power generation at bus 23, ΔP_{13} is the change in active power generation at bus 13, Δp_{area3} is the change in active power generation in Area-3, and Δp_{area1} is the change in active power generation in Area-1.

5.4 Distributed Slack Bus

The deterministic security boundary and the probabilistic cost of security are calculated using a distributed slack bus [3], as it is a more precise way of modelling a slack bus for real power systems.

The slack bus is conventionally used to provide a reference voltage angle and to pick up the system losses, which cannot be predicted prior to running the study. It could also be thought of compensating any difference between load and generation and in this way this is similar to a generator with governor control. The largest PV node on the system is often chosen as the slack bus.

In practice there will not be only one generator operating with governor control. The true behaviour of the system is represented by a 'distributed slack' where one bus is retained as providing a reference, but adjustments to active power generation due to differences between the total load (including the losses) and total generation are divided among a number of PV buses in proportion to the maximum generation at the bus since this can be taken to be proportional to the inertia of the machine(s).

Once the maximum mismatch becomes less than some pre-defined threshold, the difference between the reference bus active generation and its scheduled generation is distributed among the 'free governor' buses, changing the scheduled P setting at the start of the next iteration. Subsequent changes in reference bus active generation from one iteration to the next iteration are similarly distributed.

When load exceeds generation and this mismatch must be covered using the distributed slack, the output of the frequency responsive plants is first increased. Then, if this is not sufficient, pumped storage generation and other spinning reserves are used to increase

the slack generation. If this is still not sufficient, gas turbines are switched on. As a last resort load is shed from the worst mismatch zone. When generation exceeds load, the generation of frequency responsive plants is first lowered to their minimum. If this is not sufficient, gas turbines are stopped. If this is still not sufficient, expensive generation is reduced, proceeding backward from the merit order.

A distributed slack is very important when the system is islanded as the power flow has the option to choose new slack buses within each island. The difference between the reference bus active generation and its scheduled generation can then be distributed as described among the frequency responsive generators.

5.5 Benefits of Distributed Slack on Study Criteria

Study parameters are adjusted according to the criteria in Equations (5.1) and (5.2). When changing the generation pattern using the criteria in Equations (5.1) and (5.2), at some operating points the generation at the slack bus (i.e., bus 13 in Figure 5.1) is needed to switch off to compensate for the increased generation at bus 23 (Figure 5.1). Since the slack is distributed, the difference between the total load (including losses) and total generation can smoothly be distributed among the appropriate generating plants. On the other hand the criteria in Equations (5.1) and (5.2) uses all the PV buses for a change in generation pattern and the distributed slack minimise the changes in generation pattern, which therefore do not satisfy exactly the criterion in Equation (5.1).

5.6 Deterministic Security Assessment

The deterministic security assessment is performed to identify a secure region within the study parameters platform. Any operating condition within this region is deemed as secure, and outside the region is deemed as insecure. Following paragraphs describes the steps that are followed to identify the deterministic security boundary. The constraints in this study are the thermal and voltage limits.

In deterministic security assessment the first step (i.e., Step1) is constructing the base case according to the planned schedule. The details of constructing the base case are given in section 5.2. Following are the other steps that are performed to calculate the deterministic security boundary. Note that the implementations of the first four steps are given following their steps.

Step2: The contingency set is limited to N-1 contingencies anywhere in the system that might cause overload or voltage problems limiting the North-to-South transfer.

With the implementation of this step for the network shown in Figure 5.1 the following outages caused overload or voltage problems.

- Circuit outages from:
  bus 12 to bus 23; bus 13 to bus 23; bus 12 to bus 13; bus 15 to bus 24; bus 14 to bus 11; bus 20 to bus 23; bus 14 to bus 16; bus 12 to bus 9; bus12 to bus 10
- Generator outages of:
  350 MW unit at bus 23; 197 MW unit at bus 13; 400 MW unit at bus 21; 100 MW unit at bus 7

Step3: Identifies the parameter ranges.

With the implementation of this step for the network shown in Figure 5.1, the parameter ranges identified as:

- Generation at bus 23: 0 MW ~ 945 MW
- North to South flow (i.e., accumulated active power flow on lines from bus 15 to bus 24, bus 14 to bus 11, bus 23 to bus 12, bus 13 to bus 12): 478 MW ~ 1192 MW

Step4: Identify the limiting contingencies.

Performance evaluation criteria (i.e., the threshold limits that is used to identify security problems) of this study are set as:

- Post-contingency bus voltages should be at least 0.95 p.u.
- Pre-contingency circuit flow should not exceed the circuit's continuous rating
- Post contingency circuit flow should not exceed the circuit's emergency rating

Power flow study indicates that there are, within the study range, three violations of the performance evaluation criteria. They are:

- Post-contingency overload limit violation of line from bus 13 to bus 23 due to outage of line from bus 12 to bus 23
- Post-contingency over-load limit violation of line from bus 12 to bus 23 due to outage of line from bus 13 to bus23
- Post-contingency over-load limit violation of line from bus 14 to bus 16 due to outage of line from bus 15 to bus 24

Step5: Identify where these limiting contingencies first violate the study parameters within the study range.

Step6: Identify the security boundary in the space of the study parameters. A Nomogram can illustrate the deterministic security boundary, which is constrained by limiting contingencies.

Note that the Implementations of steps 5 and 6 are given in section 5.7.

5.7 Deterministic Security Boundary

Figure 5.2 shows the deterministic security boundary developed using the steps detailed in section 5.6 for the modified 24-bus IEEE Reliability Test System. Implementations of steps 5 and 6 can be observed from Figure 5.2. The operating region for the 'North to South flow' considered as from 500MW to 1100MW while for the 'Generation at bus 23' it extends from 300MW to 900MW.

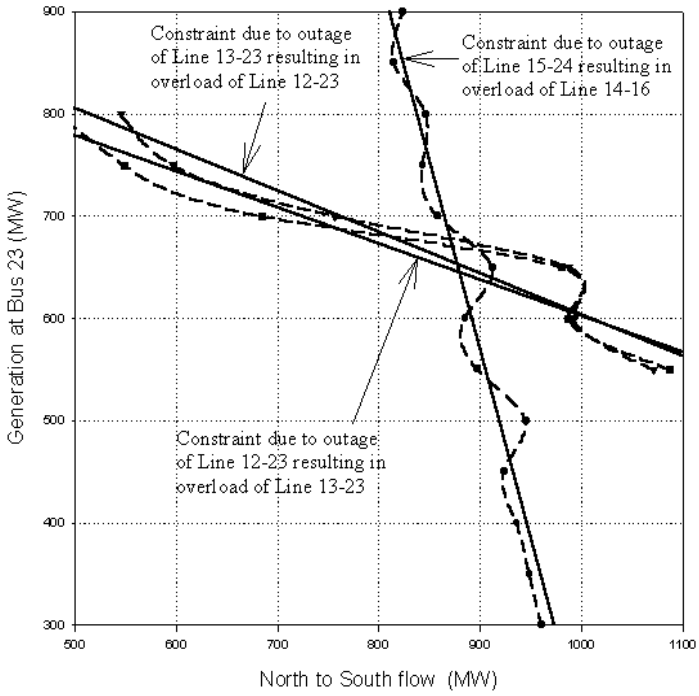

Figure 5.2: Deterministic security boundary for the modified 24-bus IEEE Reliability Test System.

In Figure 5.2, the dashed lines pass through the data points of the limiting contingencies that are obtained through the deterministic security assessment. The straight lines are the linear regression of these data points. The deterministic security boundary is determined by the linear regression defined by the outages of lines from bus 12 to bus 23 and bus 15 to bus 24. For the determination of the deterministic security boundary it is assumed that the system has a constant system load throughout the study period (i.e., 1 hour).

The deterministic security boundary shown in Figure 5.2 and the deterministic security boundary reported in [1] are compared. In general the agreement is good, but one limiting contingency which contribute to the deterministic security boundary in Figure 5.2 is different from the corresponding limiting contingency reported in [1]. Reference [1] shows that the limiting contingencies as the outages of lines connected from bus 13 to bus 23, bus 12 to bus 23 and bus 11 to bus 14 , and our analysis shows that deterministic security boundary is determined by the outages of lines connected from bus 12 to bus 23 and bus 15 to bus 24. However, this difference has not significantly

affected the boundary limits. According to our analysis the boundary associated with the line connected from bus 11 to bus 14 (This is the one of the contingencies that constrain the deterministic security boundary in [1]) operates beyond the operating limits of the boundary of the outage of line from bus 15 to bus 24. The reference [1] suggesting that the increase in generation at bus 23 is secure only up to 600MW when there is a 'North to South flow' of 500MW, but our analysis suggesting that if does an economic despatch the 'Generation at bus 23' is secure up to 775MW when there is a 'North to South flow' of 500MW.

5.8 Probabilistic Security Assessment

Steps 1 to 3 and 6 described in section 5.6 are also common with the Probabilistic Security Assessment. The cost of security in this probabilistic assessment is calculated using the Monte Carlo simulation.

Step 4: Divide the operating region with a suitable sized grid and construct base cases corresponding to each grid points in the operating region. These base cases are created using the network that is shown in Figure 5.1 (i.e., the case which is used to calculate deterministic security boundary). Each of these cases should also have the 'North to South flow' and 'Generation at bus 23' according to it's own grid point. For example the base case at the grid point ('North to South flow'=700MW, 'Generation at bus 23' = 600MW) has a 700MW of 'North to South flow' and 600MW of 'Generation at bus 23'.

Step5: Calculate the cost of security of all these cases and construct a contour plot, which reflects different levels of cost of security. Cost of security is calculated using the Value of Security Assessor (VaSA) program. Contour plot is established within the study parameter platform. The contour lines in the contour plot reflect the levels of cost of security.

Since each grid point has a value of cost of security a contour plot can be used to demonstrate them in a systematic form. Such a representation can be used to obtain a

comparative measure between deterministic security boundary and probabilistic cost of security levels.

5.9 Probabilistic Cost of Security

The probabilistic cost of security was estimated for the same network that is used in deterministic security assessment (i.e., 24-bus IEEE Reliability Test System shown in Figure 5.1). The Monte Carlo simulation was performed for a single sample with a 90% of degree of confidence and a 10% of confidence interval for a one-hour period. The minimum and maximum number of trials for the Monte Carlo simulations were set at 10,000 and 400,000 respectively. With the network shown in Figure 5.1, the average CPU time for processing a single trial in the Monte Carlo simulation takes 0.012 to 0.018 seconds (i.e., 2 to 3 minutes per 10,000 trials). In this study, the operating region (i.e., 'North to South flow' from 500MW to 1100MW and 'Generation at bus 23' from 300MW to 900MW) is divided using a 50MW grid.

Following sections describe the smoothing technique that was used for smoothing the values of cost of security, the influence of weather and system blackouts on cost of security, and a comparison between the results of deterministic security boundary and probabilistic cost of security levels. Influence of system blackouts on cost of security was investigated by considering the system blackouts for the estimation and by ignoring them.

Note that in following sections a 'raw value' is referred to a cost of security value obtained through the Monte Carlo simulation (i.e., before smoothing).

5.9.1 Smoothing

Representing the cost of security of each grid points using a contour plot does not precisely reflect the cost of security throughout the study range unless the size of the grids is very small. This is because the preciseness of a contour plot also depends on the number of data points. On the other hand, using the study criteria given in Equations

(5.1) and (5.2) it was impossible in a few occasions to create base cases that exactly match the co-ordinates of the grid points. For example it was impossible to get a 'North to South flow' of 950 MW and 'Generation at bus 23' of 750MW; the only possible 'North to South flow' is 945MW or 960MW and there is no 'North to South flow' in between 945MW and 960MW although this case achieves 'Generation at bus 23' of 750MW.

Developing base cases and calculating the costs of security for very small sized grid points require a very large amount of time. For example if the grid size is 10MWx10MW and if the feasible operating region is 600MW x 600MW in a two study parameter platform it is necessary to develop 3,600 base cases and to calculate the cost of security for all. Such a calculation can be simplified by choosing a coarser grid and then smoothing the costs of security values using a smoothing technique. The use of a smoothing technique also mitigates the problems of the cases that do not exactly match the study parameter values of grid points as smoothing is performed considering very small girds.

Therefore, the raw values of cost of security were smoothed with seven types of smoothers to choose the best smoother. A smoother is a mathematical function that transforms the relationship between a continuous variable and a response variable. These smoothers are: Loess, Negative-exponential, Bi-square, Inverse-distance, Running-average, Running-median, and Inverse-square[4]. Loess smoothing best reflects the raw values of cost of security after smoothing compared to the other smoothing techniques that were trued.

Loess is a locally weighted running line smoother. For each data point (X_0), Loess uses the k nearest neighbouring points. Each adjacent point in the neighbourhood is given a weight. The weight function in Loess smoothing is given by:

$$\begin{aligned} W(u) &= (1-u^3)^3 \qquad \text{for } 0 \le u < 1 \\ &= 0 \qquad\qquad\quad \text{otherwise} \end{aligned} \tag{5.3}$$

Where, $u = |X_0 - X_i| / D$, D is the distance from data point (X_0) to the furthest point in the neighbourhood, and X_i is the adjacent point in the neighbourhood.

The weight assigned to each data value in the window is determined by its normalised distance '*u*' from the smoothing location. Then the weighted linear least square is carried out in the neighbourhood of points. This smoother has options to use a linear regression or a polynomial regression.

In Loess smoothing the percentage of total raw values of cost of security that is used for smoothing is called sampling proportion. Investigations with Loess smoothing showed that smoothing the raw values of cost of security with more than 50% of sampling proportion and using a polynomial regression often results in negative values. To avoid smoothing towards negative values, all the raw values of cost of security were smoothed with a 20% of sampling proportion and using the linear regression. With this choice of parameters, the smoothed data closely follow the raw data.

In the rest of this chapter, all the values of the costs of security presented with contour plots are smoothed values using Loess smoothing technique.

5.9.2 Weather Conditions and Modelling Parameters

The cost of security is influenced by the weather conditions because these conditions affect the component failure rates. The Monte Carlo simulation can thus take the weather conditions into account when estimating the cost of security. Three weather conditions have been considered: fair, average and adverse weather. When the weather is fair, the probability of component failure due to weather-related incidents is very small. On the other hand, during adverse weather conditions, the component failure rates can be very high. Average weather reflects a theoretical weather condition, which lies between fair and adverse weather and where the failure rates is equal to the average value calculated over a year.

Details of the modelling of weather are given in Chapter 3 of this thesis. The proportion of failure during adverse weather conditions was computed using data collected in Canada during the period 1991-1995 [5]. According to [5], 67% of the permanent failures take place during adverse weather conditions at 300kV to 400kV for any type of

supporting structures. 72% of 110-149kV line failures occur in adverse weather. When modelling the adverse weather the proportion factor of failures is chosen as 70% throughout the network. When modelling the average weather the proportional factor of failures of Area-1 is chosen as 20% and Area-2 and Area-3 are chosen as 15% each. [6].

5.9.3 Cost of Security With Fair Weather and Considering System Blackouts

When considering system blackouts, the cost of security is estimated using the Monte Carlo simulation. The stratified sampling with shed load stratification is used to reduce the variance of the estimate. Figure 5.3 shows the smoothed values of probabilistic cost of security with fair weather effects considering the system blackouts. The method of estimating the cost of security is described in Chapter 3 of this thesis.

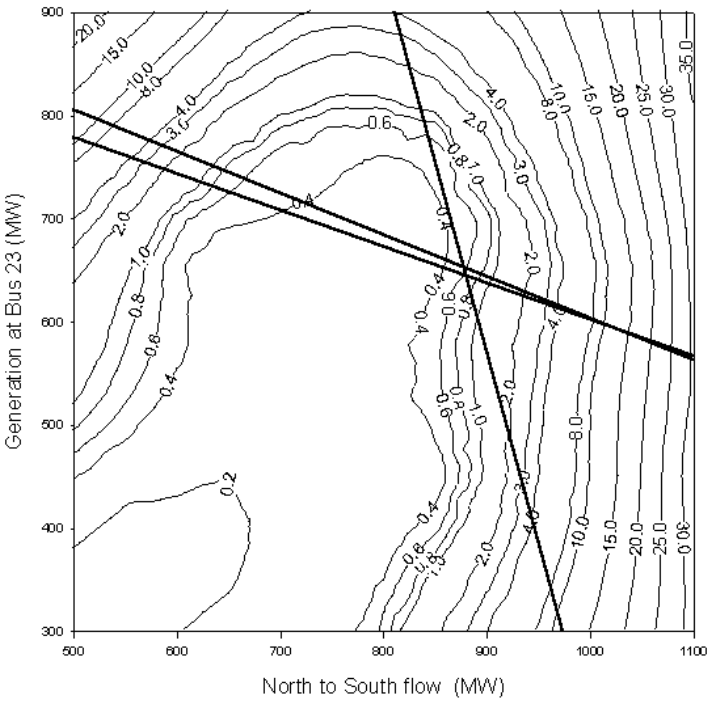

Figure 5.3: Probabilistic cost of security levels of modified 24-bus IEEE Reliability Test System for fair weather and considering system blackouts. The numbers along the contour lines indicate the cost of security (in thousands of pounds). This figure also shows the deterministic security boundary.

It can be observed from Figure 5.3 that the probabilistic cost of security is densely populated at the highest operating points, which are defined by the highest values of study parameters. Cost of security can be varied from £200 to £35,000 within the feasible limits of operation. In here the feasible limit is referred to the operating conditions beyond which power flow diverges. There is a region where the system can be operated compromising a cost of security of £200 to £400. Beyond this region the incremental cost of security tends to increase significantly.

The probabilistic method used in [1] is based on a resulting risk due to constraint violations, instead in our analysis it is the cost of security. Reference [1] change the generation pattern according to the criteria in Equations (5.1) and (5.2) where as our analysis adjust the generation pattern with respect to the criteria in Equations (5.1) and (5.2) together with an economic despatch. This is the reason why there is a difference between our results of probabilistic assessment and the results reported in [1].

Figure 5.4 shows the raw values of cost of security with fair weather effects considering system blackouts. When compared Figures 5.4 and 5.3, it can be seen that the smoothed values more close to the raw values.

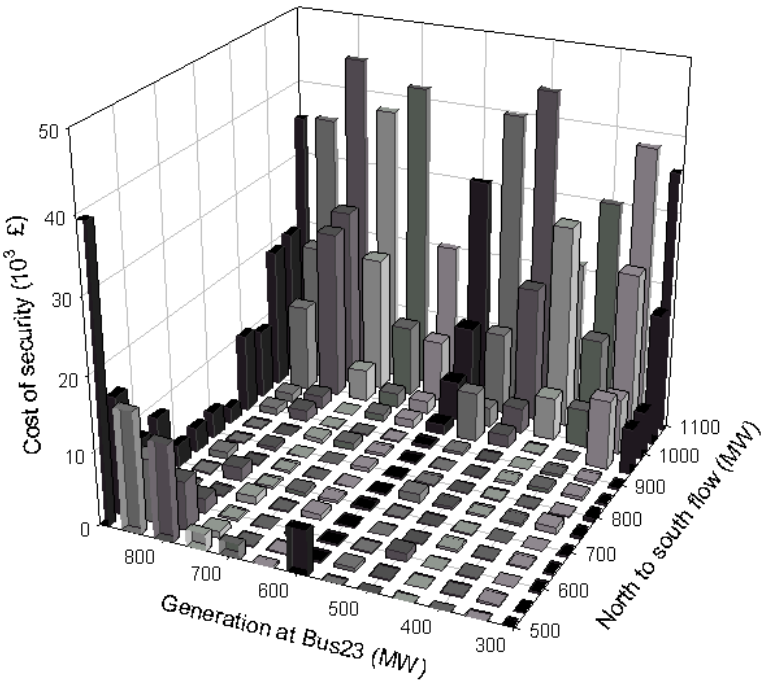

Figure 5.4: Raw values of the cost of security with fair weather effects when system blackouts are considered.

When the operating point moves from lower to higher 'North to South flow', because of a change in generation pattern, some of the plants in South (i.e., Area-1 in Figure 5.1) are switched off as the Northern generation is fully committed to supply the Southern demand. This is because the criterion in Equation (5.2) adjusts any change in generation in Area-1 with Area-3 and a reduction in generation at Area-1 causes occasionally requires the shut down of certain expensive plants, which also carries a significant amount of reactive power. Although the active power balance is maintained with respect to the criteria in Equations (5.1) and (5.2), these equations do not take into account reactive power control.

Increasing the 'North to South flow' reduces the reactive margin and increases the cost of security considerably at the highest levels of 'North to South flow' and the highest levels of 'Generation at bus 23'. Therefore under such operating conditions of the network, load disconnections are needed to get system back to normal operation. In addition, the plants in Area-1 & Area-3 do not have same generation capacity including the reserve to interchange the generation to follow the criterion in Equation (5.2). This imbalance also disturbs the change in generation pattern when the 'North to South flow' and 'Generation at bus 23' approach their boundary limits.

Figure 5.5 shows the number of system blackouts that are considered for the estimation of cost of security in Figure 5.4.

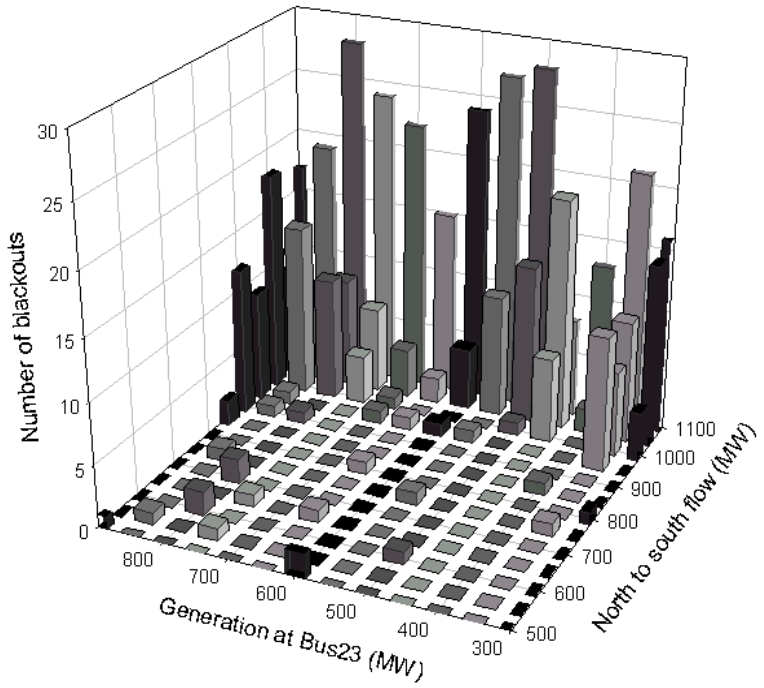

Figure 5.5: Number of system blackouts that are considered for the estimation of probabilistic cost of security in Figure 5.4.

It can be seen from Figure 5.5 that the insufficient reactive power control at the higher levels of 'North to South flow' triggers a large number of system blackouts. According to Figure 5.5, when the 'North to South flow' is highest, the cost of security is entirely dominated by system blackouts. Ignoring this effect distorts the estimate. The reason for larger number of system blackouts at these operating points is the lack of reactive reserve to compensate for the increase in reactive demand that results from line outages. When changing the generation pattern according to the criterion in Equation (5.1), the influence of system blackouts is not significant as this region experiences a small number of system blackouts. This is because this criterion is defined between the generators connected at two busses (i.e., bus 13 and bus 23 in Figure 5.1) and the imbalance between the reactive powers of the generators connected at these two busses can be compensated from the reserve in Area-3. Area-3 has the largest reserve and it can be controlled only by the criterion in Equation (5.2).

5.9.4 Cost of Security With Average Weather and Considering System Blackouts

Figure 5.6 shows the smoothed values of probabilistic cost of security with average weather conditions considering system blackouts. The average weather moderately affects the component failure rates and thus these effects are also incorporated into the probabilistic assessment.

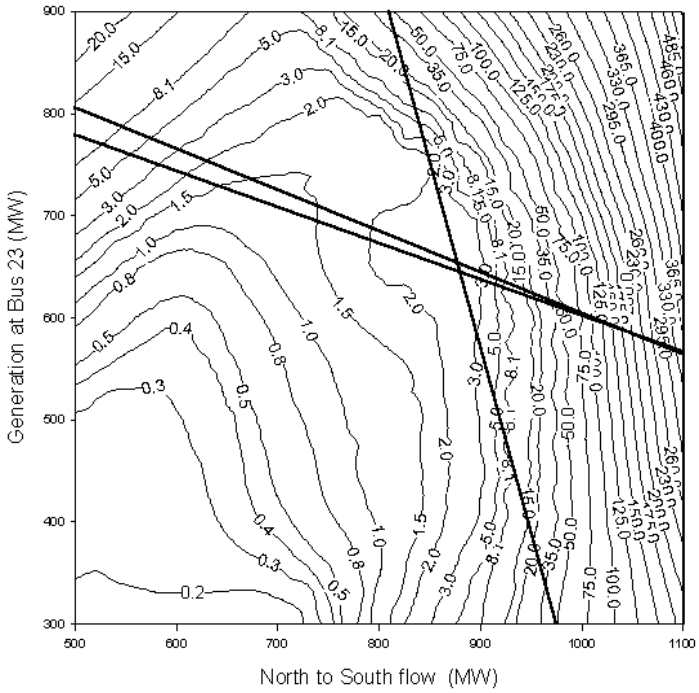

Figure 5.6: Probabilistic cost of security levels with average weather effects considering system blackouts. The numbers along the contour lines indicate the cost of security (in thousands of pounds). This figure also shows the deterministic security boundary.

Figure 5.7 shows the raw values of cost of security with average weather effects considering system blackouts. The scale of the cost of security in this figure is different from the scale in Figure 5.4. (Figure 5.4 shows the raw values of cost of security with fair weather condition considering system blackouts).

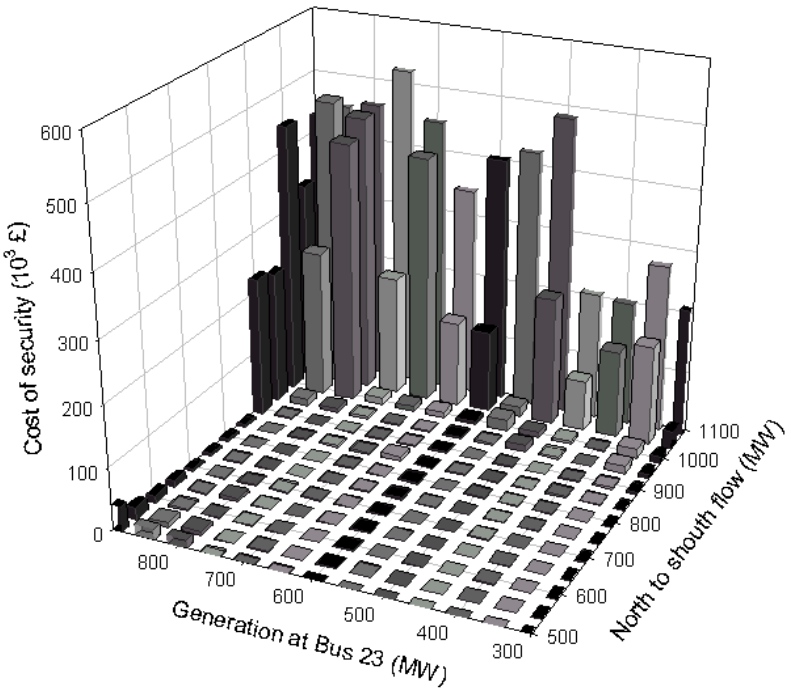

Figure 5.7: Raw values of cost of security with average weather effects considering system blackouts.

When compared Figures 5.4 and 5.7, it clearly signals that the system is very stressed when it is operated with the highest values of 'North to South flow'. Average weather effects magnify the level of stress in that region. However, rest of the region is not badly affected with the increased failures with average weather. This is because with lower operating points of 'North to South flow' although the line failure rates are increased moderately with the average weather effects, the local reactive reserve can fairly alleviate the voltage problems as in the fair weather effects.

Figure 5.8 shows the number of system blackouts experienced with average weather conditions. It is to be note that the scale used in Figure 5.8 for number of system blackouts is different from the scale used in Figure 5.5. (Figure 5.5 shows the number of system blackouts with fair weather effects).

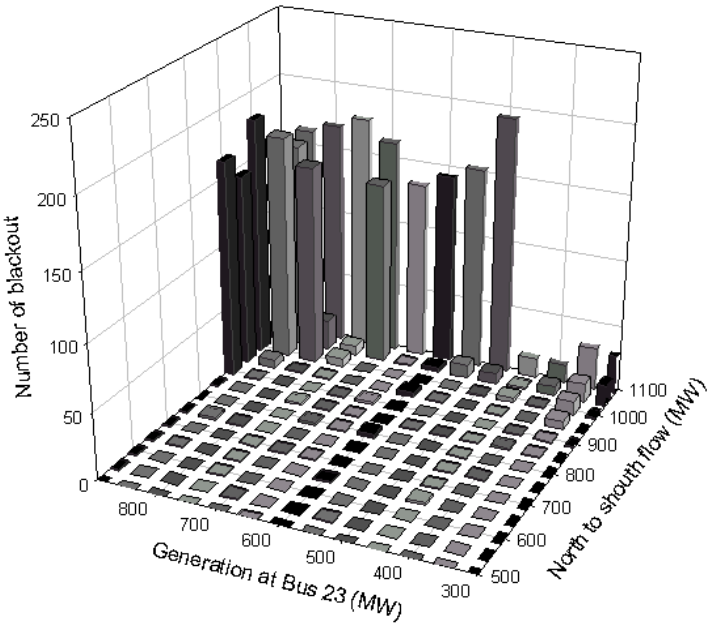

Figure 5.8: Number of system blackouts with average weather that are considered for the estimation of cost of security in Figure 5.7.

Figure 5.8 further evidences the high impacts due to system blackouts on cost of security at the highest operating points of 'North to South flow' and 'Generation at bus 23'. At these operating points system is very stressed and due to simultaneous outage of lines that are connected to the plants that have large reactive reserve causes to disconnect them from the system. Lack of sufficient reactive reserve to meet the system reactive demand causes voltage problems resulting a large number of system blackouts.

5.9.5 Cost of Security With Adverse Weather Effects Considering System Blackouts

Figure 5.9 shows the smoothed values of probabilistic cost of security with adverse weather effects considering system blackouts. Adverse weather severely affects the system security increasing the magnitude of cost of security significantly.

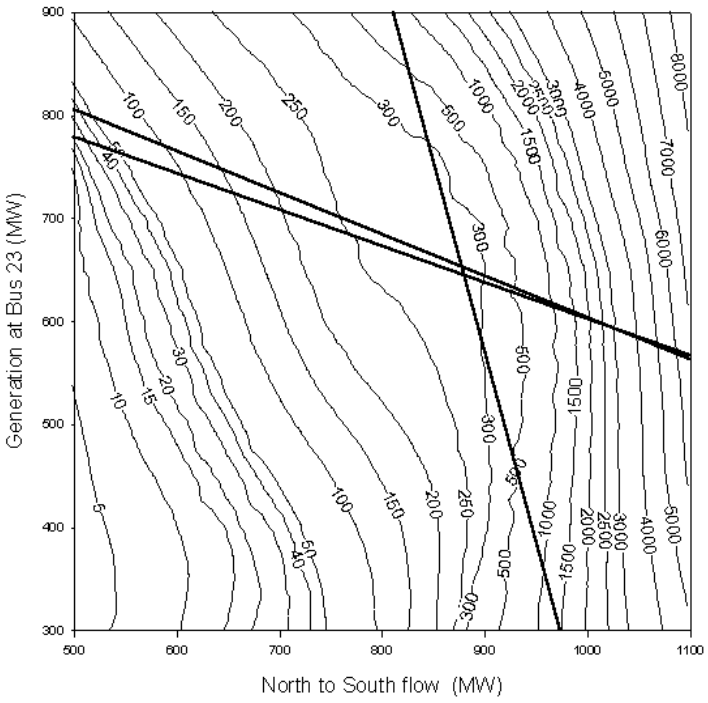

Figure 5.9: Probabilistic cost of security with adverse weather effects considering system blackouts. The numbers along the contour lines indicate the cost of security (in thousands of pounds). This figure also shows the deterministic security boundary.

Figure 5.10 shows the raw values of cost of security considering the system blackouts. Unlike fair and average weather, the system is heavily stressed with adverse weather conditions and picks up the cost of security even with the lower operating conditions in the power system. The cost of security scale in Figure 5.10 is different from the cost of security scale in Figures 5.4 and 5.7. (Figures 5.4 and 5.7 show the cost of security levels respectively for the fair and average weather effects)

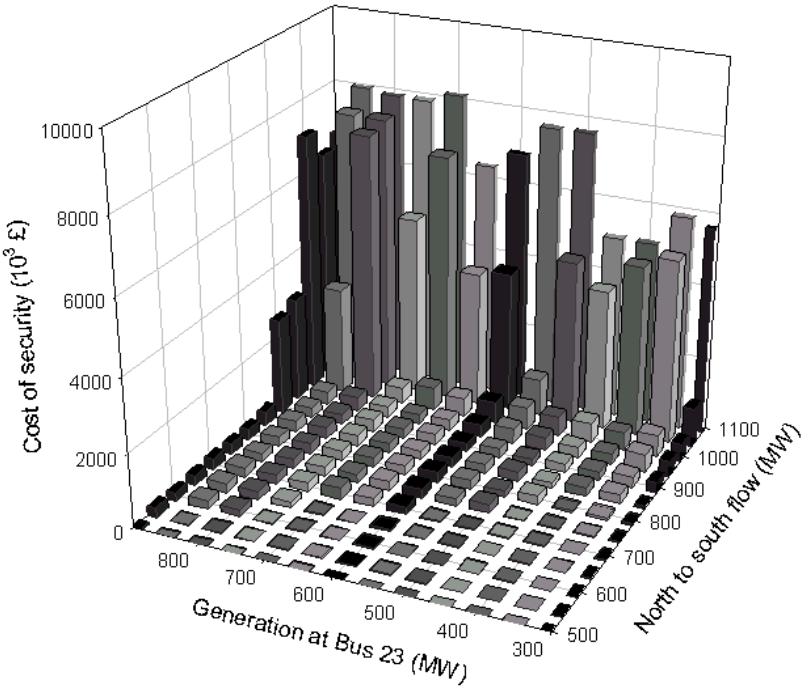

Figure 5.10: Raw cost of security with adverse weather effects considering system blackouts.

Figure 5.11 shows the number of system blackouts with adverse weather effects where the scale of number of system blackouts is different from the number of system blackouts with fair and average weather, which are shown in Figures 5.5 and 5.8. Since with the adverse weather effects the failures of components are significantly increased, there is a higher possibility to fail few components simultaneously. If few units, which have a major reactive control capability, are failed simultaneously a large amount of load disconnections are needed to get system back to normal. When the system operates at the highest operating points the number of system blackouts increases dramatically.

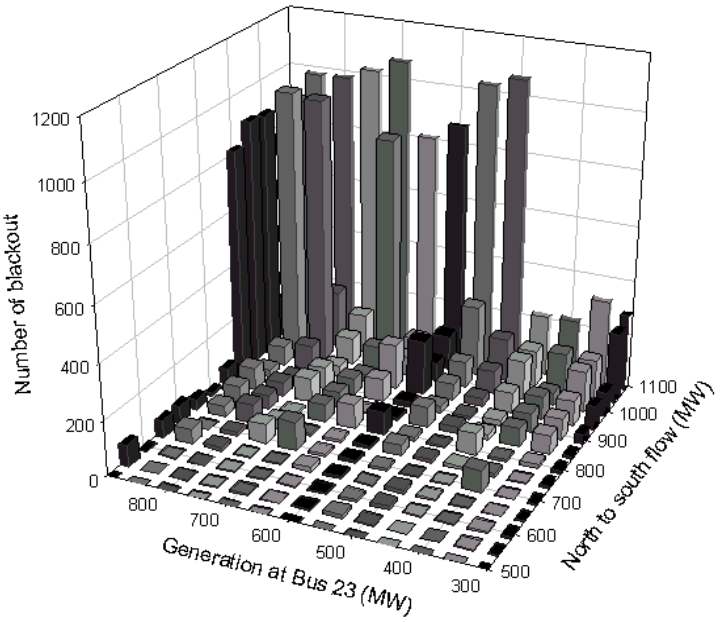

Figure 5.11: Number of system blackouts that are considered in the estimation of cost of security in Figure 5.10.

All these investigations considering the influences of weather conditions show that the weather conditions affect cost of security and estimation of cost of security should also account the weather effects for precise estimation of cost of security.

5.9.6 Cost of Security Ignoring System Blackouts

Naïve Monte Carlo simulation is capable of estimating the cost of security when the system blackouts are ignored. In this estimation the trials, which results system blackouts, are ignored from the estimation. Figure 5.12 shows cost of security levels when ignored system blackouts with the effects of fair weather. Figure 5.13 shows the raw values of cost of security corresponding to Figure 5.12

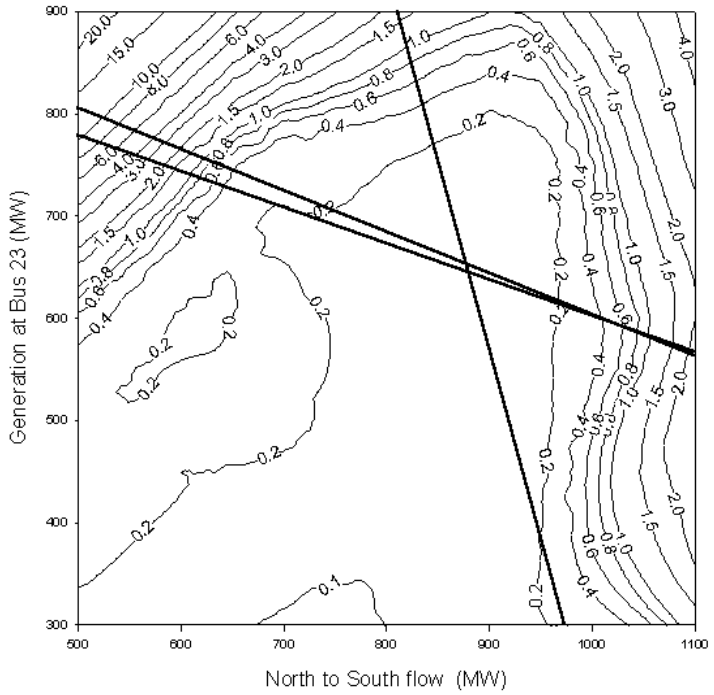

Figure 5.12: Cost of security levels with the fair weather effects when ignoring system blackouts. The numbers along the contour lines indicate the cost of security (in thousands of pounds). This figure also shows the deterministic security boundary.

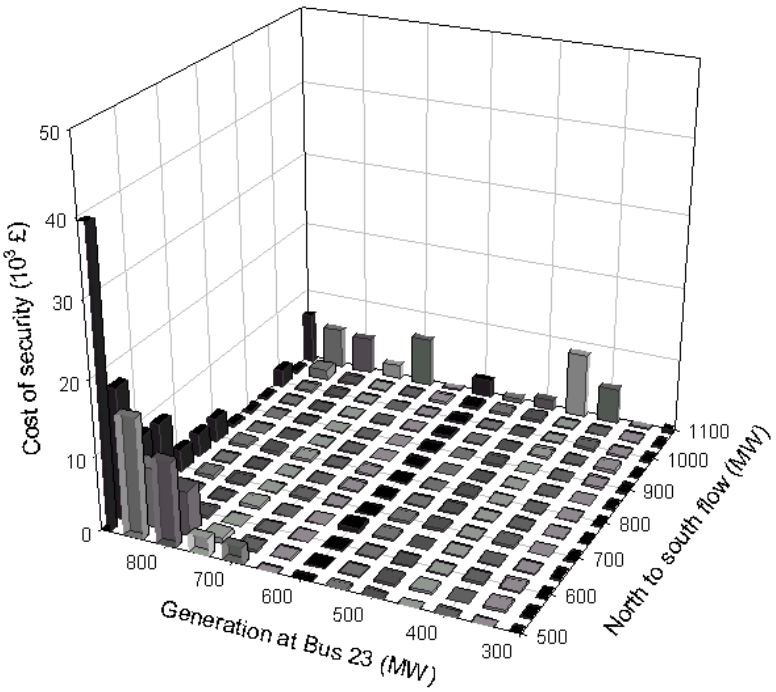

Figure 5.13: Raw values of the cost of security with fair weather effects when system blackouts are ignored.

When compared Figure 5.3 (which shows the cost of security when considered system blackouts) with the Figure 5.12, the ignorance of system blackouts have significantly affected the cost of security of the region that covered by the higher values of 'North to South flow'. This is because this is the region where the system experiences significantly large number of system blackouts and ignoring them results a relatively small cost of security. On the other hand, when the system operates keeping the 'North to South flow' lower and increasing the 'Generation at bus 23' has no major influences on cost of security although the estimation ignored system blackouts. This is because in this region a major cost of security is due to other events and experiencing system blackouts at this region is very small.

Figure 5.14 shows the cost of security levels ignoring system blackouts with the adverse weather effects.

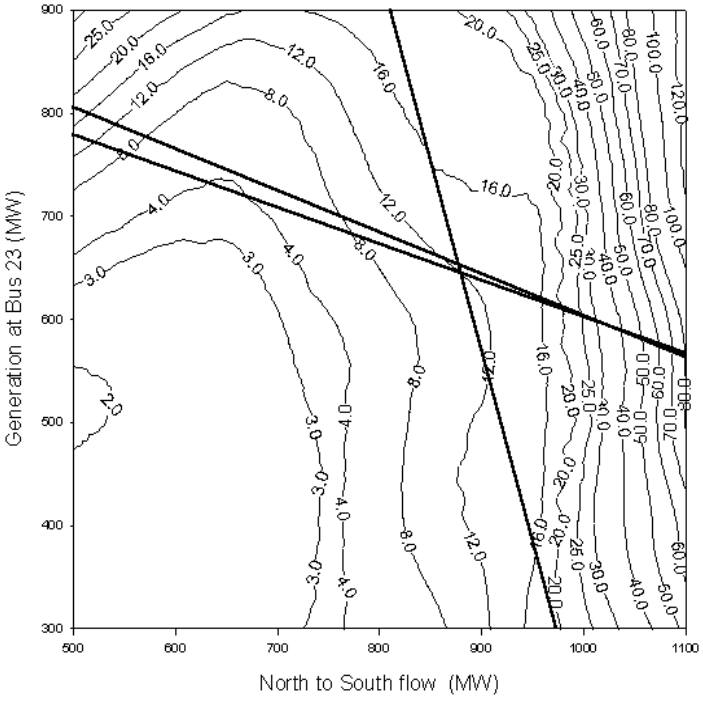

Figure 5.14: Probabilistic cost of security with adverse weather effects when ignored system blackouts. The numbers along the contour lines indicate the cost of security (in thousands of pounds).

When compared Figures 5.14 with Figure 5.9 it is obvious that the ignoring system blackouts with adverse weather effects significantly affects cost of security in a power system.

Figure 5.15 shows the raw values of cost of security when ignored system blackouts with the adverse weather effects.

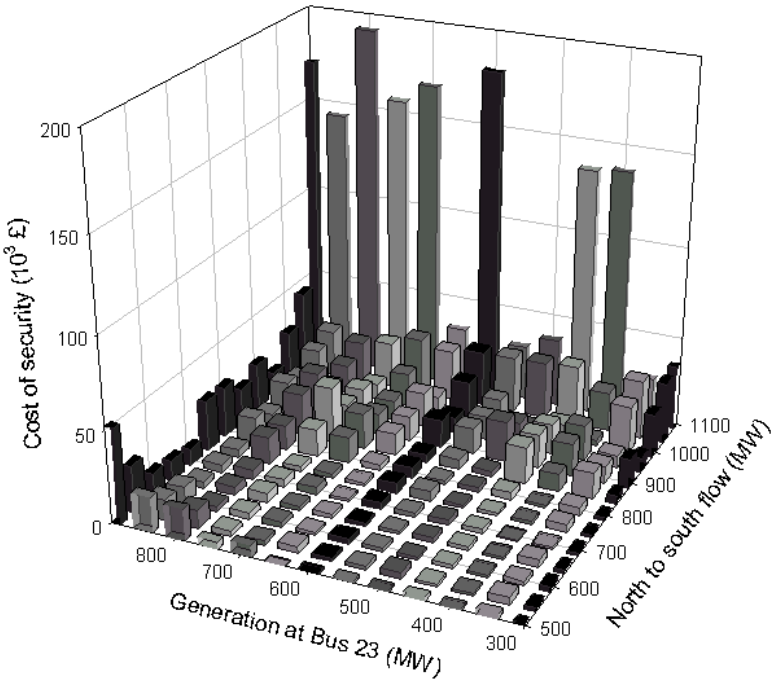

Figure 5.15: Raw cost of security with adverse weather effects when ignored system blackouts.

It can be seen from Figure 5.15 that load disconnections due to events other than system blackouts considerably increases with adverse weather effects.

These results suggest that it is very important to consider the influence of system blackouts for a precise estimation of cost of security and avoiding them devalue the value of security in a power system.

Extended investigations suggest that the influence of standard deviation on the cost of security is negligibly small when the convergence criteria of the Monte Carlo simulation have been satisfied.

5.10 Comparison between deterministic and probabilistic results

A deterministic security boundary does not provide information on how severe an operating point is within the insecure region or how secure an operating point is within the secure region. In other words it does not provide levels of security within a feasible operating region. The probabilistic method provides such an indication through the cost of security contour lines. Such indications are particularly important to identify the points where a small variation in operating conditions causes large variations in the cost of security.

The probabilistic approach provides significant information on the prevailing security level for a particular operating condition. According the Figure 5.3 with the fair weather effects and considering system blackouts the cost of security within the deterministic security boundary can be from £200 to £11,000. It is even possible to have a cost of security lower than £200 as there is also a small standard deviation associated with these estimates of the cost of security. Another observation from Figure 5.3 is that the deterministic boundary does not run along a single cost of security contour. Instead, the cost of security varies from £400 to £11,000 along this boundary. This emphasises the uncertainty about the cost of security along a traditional deterministic security boundary and the importance of probabilistic approaches when assessing power system security.

Beyond the deterministic security boundary in Figure 5.3, there is a region where the cost of security is less than £400. Beyond that, the cost of security increases continuously and considerably. If the system is operated at its maximum feasible capacity the cost of security rises up to £35,000.

According to Figure 5.6, average weather increases only moderately the cost of security. Under average weather, the cost of security ranges from £200 to £50,000 if the system operates within deterministic security boundary. Along the deterministic security boundary the cost of security varies from £1500 to £50,000. Operating at the maximum ‘North to South flow’ and ‘Generation at bus 23’ increases the cost of security up to £500,000.

According to Figure 5.9, with adverse weather, the cost of security can be anywhere from £5000 to £1.5 million within the deterministic security boundary. Along the deterministic security boundary the cost of security varies from £25,000 to £1.5 million. If the system is heavily stressed (i.e., when the system operates at the highest values of 'North to South flow' and 'Generation at bus 23') the cost of security can rise above £8 million.

These results suggest that the cost of security along the deterministic security boundary is not consistent and can vary significantly. Beyond the deterministic security boundary the incremental cost of security is significantly higher than within the deterministic boundary. Although the deterministic approach provides simple answers to questions about security, the confidence in these answers is not guaranteed. The probabilistic solutions provide more detailed solutions and make possible a quantification of the level of insecurity.

5.11 Summary

This chapter presents the deterministic and probabilistic security assessments. The deterministic assessment follows the steps described in [1]. On the other hand, the probabilistic assessment presented in this chapter is a novel methodology. Probabilistic assessment is based on the Monte Carlo simulation. In this simulation, the variance of the estimate is reduced using stratified sampling with shed load stratification. The Loess smoothing technique is used to smoothing the values of the cost of security and makes possible the development of contours showing the cost of security in graphical form.

A case study based the modified 24-bus IEEE Reliability Test System (1996), (the same network as was used in [1]) is performed. The influence of weather conditions on cost of security was investigated. These investigations considered fair, average, and adverse weather conditions. The significance of system blackouts in the cost of security was investigated by considering and ignoring system blackouts in the simulation. Results obtained through deterministic and probabilistic assessments are presented and discussed. The similarities and differences between the results presented in this chapter

and results reported in [1] are also highlighted and the reasons for the differences are given.

5.12 References

[1] J. McCalley, M. Bhavaraju, R. Billinton, A. Breipohl, H. Chao, J. Chen, J. Endrenyi, R. Fletcher, C. Grigg, G. Hamoud, R. Logan, A. P. Meliopoulos, N. Rau, M. Schilling, Y. Ychlumberger, A. Schneider, and C. Singh, "Comparison Between Deterministic and Probabilistic Study Methods in Security Assessment for Operations," *A task force organized by the IEEE PES Reliability, Risk, and Probability Applications Subcommittee*, 2001.

[2] C. Grigg, P. Wong, P. Albrecht, R. Allan, M. Bhavaraju, R. Billinton, Q. Chen, C. Fong, S. Haddad, S. Kuruganty, W. Li, R. Mukerji, D. Patton, N. Rau, D. Rappen, A. Schneider, M. Shahidehpour, and C. Singh, "The IEEE Reliability Test System - 1996," *IEEE Transactions on Power Systems*, vol. 14, pp. 1010-1020, 1999.

[3] K. Bell, "Computation of the Value of Security: Intermediate Project Report," University of Manchester Institute of Science and Technology, Manchester, UK, August 1998.

[4] Sigma-Plot, "Sigma Plot 8.0 - User's Guide," SPSS Inc., USA, 2002.

[5] C.E.A., "Forced Outage Performance of Transmission Equipment," Canadian Electricity Association, Canada, 1996.

[6] M. Rios, D. Kirschen, and R. Allan, "Computation of the Value of Security: Final Report - Volume II," University of Manchester Institute of Science and Technology, Manchester, UK, November 1999.

Chapter 6

Adaptive Deterministic Security Criteria

6.1 Introduction

Power system operators traditionally use deterministic security criteria such as 'N-1' or 'N-D' to assess security in a power system. These criteria are simple to implement and determine the level of security of a power system in a deterministic basis. However, they have major drawbacks. These drawbacks were reviewed in chapter 5 by applying both deterministic and probabilistic criteria to the modified 24-bus IEEE Reliability Test System (Figure 5.1 of chapter 5). The probabilistic security criteria are rigorous, computationally intensive and overcome the drawbacks of the deterministic security criteria.

However, power system operators are reluctant to adopt probabilistic approaches because in the high pressure, high responsibility environment of a control centre, operators do not want to be told that there is an X% probability that the system might collapse. They want straight answers to simple questions, such as: Do I need to do something? Is my plan of action acceptable? How much power can I let flow through this line?

These questions can be answered on the basis of the traditional deterministic security criteria. However, the resulting operating plans will, in some cases, be too conservative while under different conditions, it may subject the system to unacceptable risks. It has been argued that this criterion under certain conditions imposes unnecessary high constraint costs for both power producers and grid operators. The traditional deterministic security criteria do not consider economic aspects, and do not necessarily lead to the most cost effective operation. Furthermore they are not sensitive to varying outage probabilities for circuits exposed to changing weather conditions.

The level of risk can be fixed if the operating plans are evaluated and adjusted on a probabilistic basis. A purely probabilistic approach to security, as demonstrated during the first project on the Value of Security, is more rigorous. However, it is also difficult to implement and power system operators may find it difficult to accept because it is not easily integrated with the tools that operators use to design their plans (e.g. optimal power flow, unit commitment).

This chapter explores whether it is possible to develop adaptive deterministic security criteria (ADSC) that track more closely the probabilistic measures of security than the traditional 'N-1' or 'N-D' deterministic criteria. The ADSC consider the effects of outaged components on system security. However, the indication of security level in ADSC is also deterministic although it adapts itself to the operating conditions.

The first steps in the development of ADSC are the determination of the deterministic security boundary and the estimation of the cost of security for a range of operating conditions of the power system. These steps were presented in chapter 5. Therefore, this chapter explores ADSC using the deterministic and probabilistic results of chapter 5.

Three types of adaptive deterministic security boundaries (ADSBs) are explored in the following sections of this chapter. These types include single-line, rectangular and tri-line. At first, the reference contour plot is identified, and then for each ADSB, the reference ADSB is calculated.

Families of ADSB are calculated by separately adjusting the study parameters through the reference ADSB. The initial group of ADSB is calculated using the families of ADSB. The system ADSB is determined by constructing more groups of ADSB that distribute over the system feasible operating region.

The metric of the ADSB is the weighted-average cost of security as it can minimise the inconsistencies in the deterministic security boundary. Costs of energy of rectangular and tri-line system ADSBs are also presented. The chapter ends with a discussion of how this approach could be used in power system operation.

6.2 Mechanism of the Novel Security Assessment

ADSC use deterministic security boundary and the probabilistic cost of security to calculate the ADSB. As was demonstrated in the previous chapter, the cost of security along the deterministic security boundary is not consistent. The ADSC are designed to minimize this inconsistency. Therefore, the weighted average cost of security is introduced.

For calculating the weighted-average cost of security of a deterministic security boundary, the average cost of security is first calculated using Equation (6.1).

$$C_{av_j} = \frac{(C_i + C_{i+1})}{2} \tag{6.1}$$

Where C_i and C_{i+1} are the cost of security of consecutive cost of security contour lines that pass through the deterministic security boundary, C_{av_j} is the average cost of security along a piece of line segment in the deterministic security boundary that is bounded by these contour lines, i represents the cost of security contour line and j represents the piece of line segment. Figure 6.1 illustrates this idea.

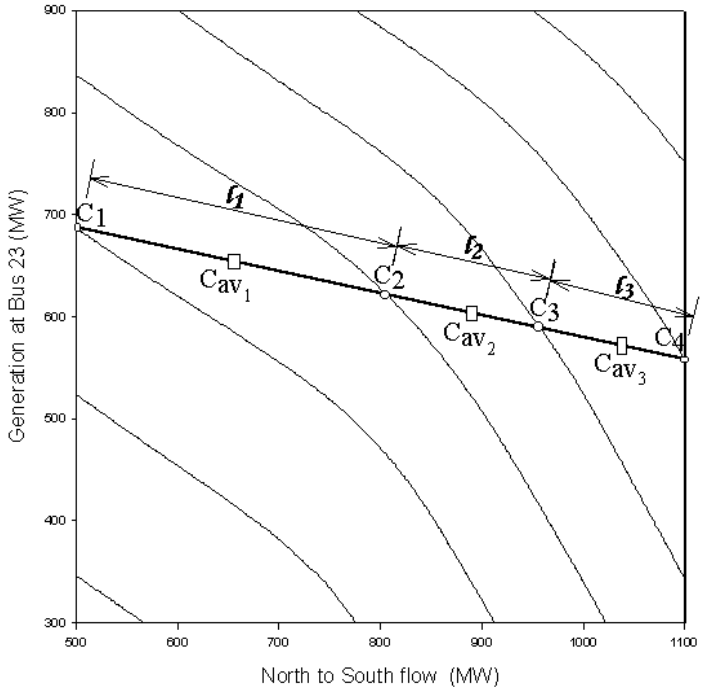

Figure 6.1: An example of average costs of security of consecutive contour lines.

In Figure 6.1, C_1, C_2, C_3, and C_4 represent the costs of security of consecutive contour lines. l_1, l_2, and l_3 represent the lengths of the pieces of line segments in the deterministic security boundary that are bounded by C_1 and C_2, C_2 and C_3, C_3 and C_4 respectively. C_{av1}, C_{av2}, and C_{av3} represent the average costs of security between C_1 and C_2, C_2 and C_3, and C_3 and C_4 respectively. For example the average cost of security between C_1 and C_2 (i.e., C_{av1}) is calculated by $((C_1+C_2)/2)$. This average cost of security (i.e., C_{av1}) belongs to the length of the line segment l_1.

Then the weighted-average cost of security (*Cwacs*) of the deterministic security boundary is calculated using Equation (6.2).

$$C_{wacs} = \frac{\sum_{j=1}^{n} C_{av_j} \times l_j}{\sum_{j=1}^{n} l_j} \tag{6.2}$$

Where l_j represents the length of the line segment along the deterministic security boundary and n represents the total number of line segments of the deterministic security boundary.

Once the inconsistency of cost of security along the deterministic security boundary is minimised with the weighted-average cost of security, a contour line that has the same value of weighted-average cost of security as the deterministic security boundary is identified. This contour line is considered as the reference contour plot for calculating the reference ADSB.

The reference contour plot can be represented by a single-line, rectangular, tri-line or more than three cascading lines. In this chapter, representations with up to three cascading lines are investigated. These representations are called ADSBs.

The reference ADSB should also have the same weighted-average cost of security as the deterministic security boundary. The weighted-average cost of security of the reference ADSB is also calculated using the same principle that is used for the calculation of

weighted-average cost of security of the deterministic security boundary using the Equations (6.1) and (6.2).

Figure 6.2 shows an example of the reference single-line representation.

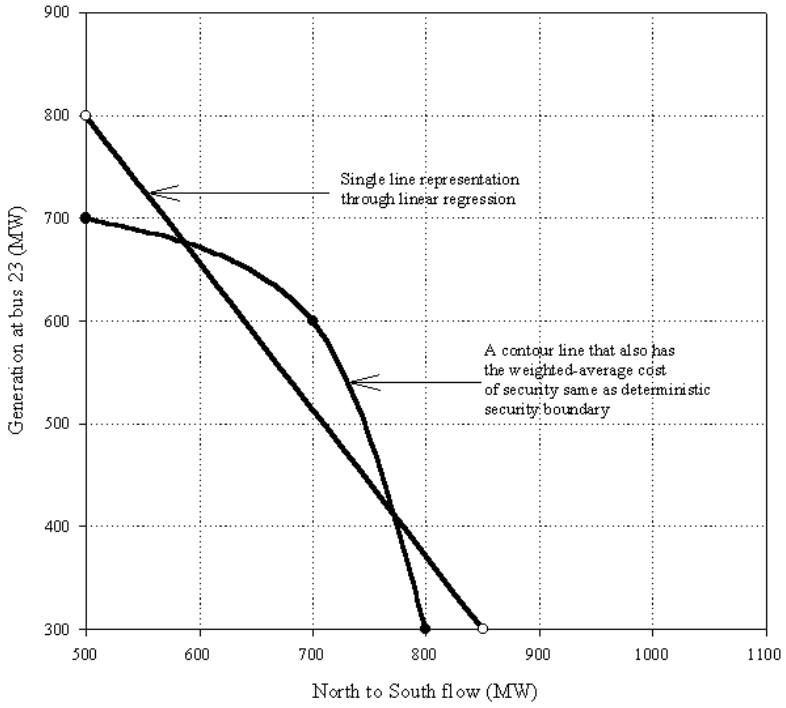

Figure 6.2: An example of the reference single-line representation. The figure also shows the reference contour plot.

In a single-line ADSB, the values of the study parameters corresponding to the reference contour plot are linearly regressed using the least square error technique. The resulting regressed line, in some occasions, does not have the same weighted-average cost of security as the deterministic security boundary. In such occasions, the regressed line can be adjusted in parallel to obtain the weighted-average cost of security same as the deterministic security boundary. The regressed line calculated in this way is the reference single-line ADSB for calculating the families of the single-line ADSB.

Figures 6.3 shows an example of the reference for the rectangular representation.

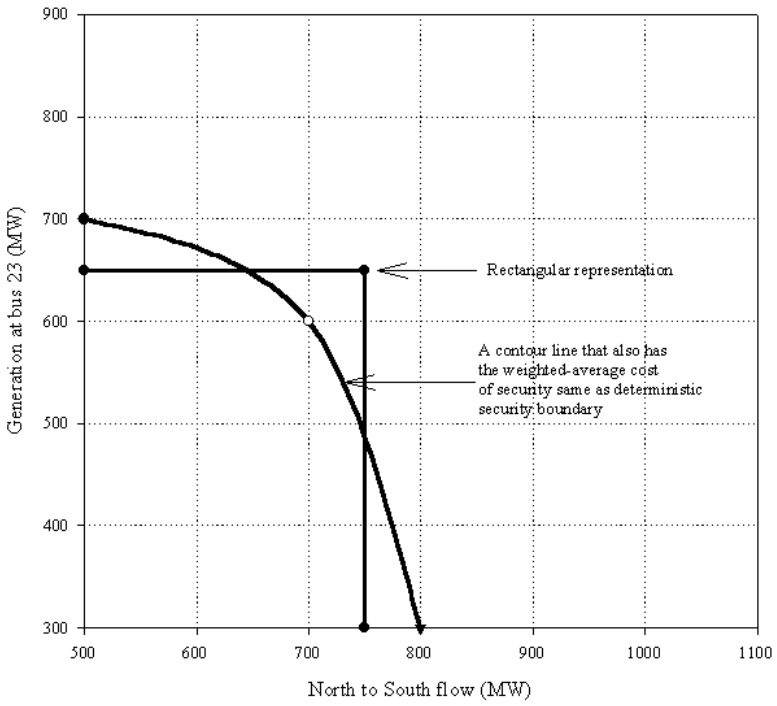

Figure 6.3: An example of the reference rectangular representation. The figure also shows the reference contour plot.

In a rectangular ADSB, the rectangular path should begin as close as possible to the reference contour plot and should closely pass through the relatively higher cost of security region that is associated with the reference contour plot. This is because such a beginning can extend the reference rectangular ADSB for higher number of members in a family (i.e., boundaries in a family of rectangular ADSB) within the feasible operating region than it begins with the other way round. Relatively higher cost of security region can be identified by observing the neighbouring cost of security along the reference contour plot.

Once the first line of the reference rectangular ADSB is drawn through the relatively higher cost of security region, the other line, which is perpendicular to the first line, is calculated to achieve the same weighted-average cost of security as the deterministic security boundary. The resulting rectangular ADSB is the reference rectangular ADSB.

Figures 6.4 shows an example of the reference tri-line representation.

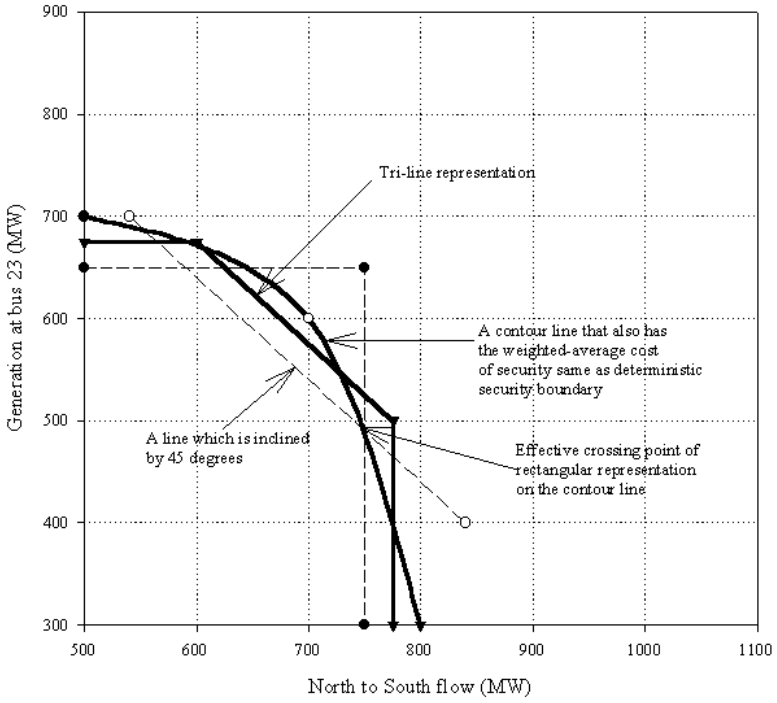

Figure 6.4: An example of the reference for the tri-line representation. The figure also shows the reference contour plot. The dashed lines show where the reference rectangular representation is cut off to form the tri-line representation.

To form the reference tri-line ADSB, the reference rectangular ADSB is cut off with a line to eliminate the portion of the reference rectangular ADSB that goes beyond the reference contour plot.

There is a strict rule when establishing the inclined line of reference tri-line ADSB. This is because the study parameters of the inclined line of reference tri-line ADSB cannot be adjusted one study parameter at a time and in same proportion to meet the adjusted inclined lines at a common point if the angle of the inclined line is not 45 degrees.

Figure 6.5 shows an example of such a situation where the dashed lines show the adjusting 'Generation at bus 23' and continuous lines show the adjusting 'North to South flow'. Both these study parameters are adjusted in same proportion (e.g. 50MW each).

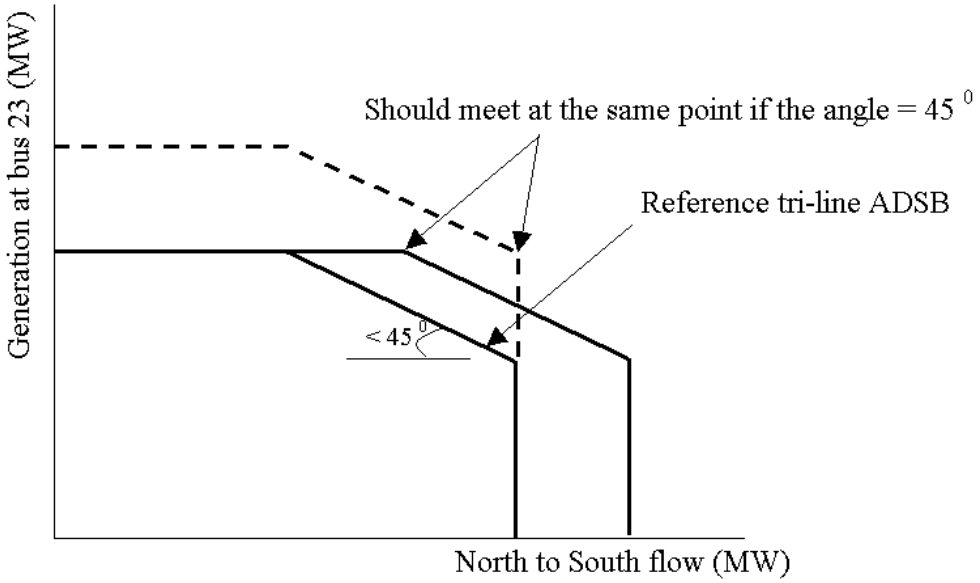

Figure 6.5: An example of reference tri-line ADSB of which the angle of the inclined line is less than 45 degrees.

Therefore, the line that is used to cut off a portion of the reference rectangular ADSB should have an angle of 45 degrees and should pass through the most suitable crossing point between the reference rectangular ADSB and the reference contour plot. The point where the 45 degrees line can eliminate most of the portion of the reference rectangular ADSB that goes beyond the reference contour plot is considered as the most suitable crossing point. The resulting tri-line ADSB is uniformly magnified to achieve the same weighted-average cost of security as the deterministic security boundary. This form of ADSB is considered as the reference tri-line ADSB.

The references of each type of ADSBs are used for the calculation of the families of each ADSB. Families of the each type of ADSBs are calculated by separately considering each study parameter.

To determine the initial group of ADSB in a representation, at first one family of ADSB is calculated only adjusting one study parameter. Then another family of ADSB is calculated adjusting the other study parameter. Next both families are combined together to form the group of ADSB. For example, at first calculates one family of ADSB by only adjusting the 'North to South flow'. Then another family of ADSB is

calculated by only adjusting 'Generation at bus 23'. Next, both of these families are combined together to form the group of ADSB.

More groups of ADSB can be constructed by moving the lines in the reference ADSB at the same time and then adjusting the study parameters separately. This set of groups of ADSB is calculated to distribute them over the system feasible operating region. Therefore, this set of groups of ADSB is called system ADSB of the corresponding representation.

These steps described in this section are illustrated with a case study.

6.3 Case Study

The determination of an ADSB begins with the calculation of deterministic security boundary and the estimation of probabilistic cost of security in a power system. The mechanism proposed in section 6.2 is applied to the modified 24-bus IEEE Reliability Test System that is shown in Figure 5.1 of chapter 5.

Average weather conditions are considered for the calculation of ADSB because the consideration of adverse weather conditions result in optimistic levels of security when considering real weather conditions. On the other hand, fair weather conditions result in pessimistic levels of security. In reality a combination of fair to adverse weather conditions arises. Such optimistic and pessimistic levels of security occur because, as shown in chapter 5, the fair weather conditions results in a low cost of security compared to the average weather conditions. Adverse weather conditions result in extremely high cost of security compared to the average weather conditions. However, the mechanism of section 6.2 could be used to calculate the ADSB considering fair and adverse weather conditions.

6.3.1 Identification of Reference Contour Plot

Figure 5.6 of chapter 5 shows the deterministic security boundary and the probabilistic cost of security of the modified 24-bus IEEE Reliability Test System considering the average weather conditions and system blackouts.

In Figure 5.6 of chapter 5, the contour lines show the probabilistic cost of security. The straight lines in Figure 5.6 are the deterministic security boundary. The weighted-average cost of security of the deterministic security boundary is £8100. Figure 5.6 also shows the contour line that also has a £8100 cost of security. This contour line is called the reference contour plot for calculating the reference for each type of ADSBs.

6.3.2 Single-line ADSB

6.3.2.1 Calculation of Reference for the Single-line ADSB

The reference contour plot is linearly regressed to calculate the reference single-line ADSB. The reference single-line ADSB that has an £8100 weighted-average cost of security is parallel to this regressed line.

Figure 6.6 shows the reference single-line ADSB.

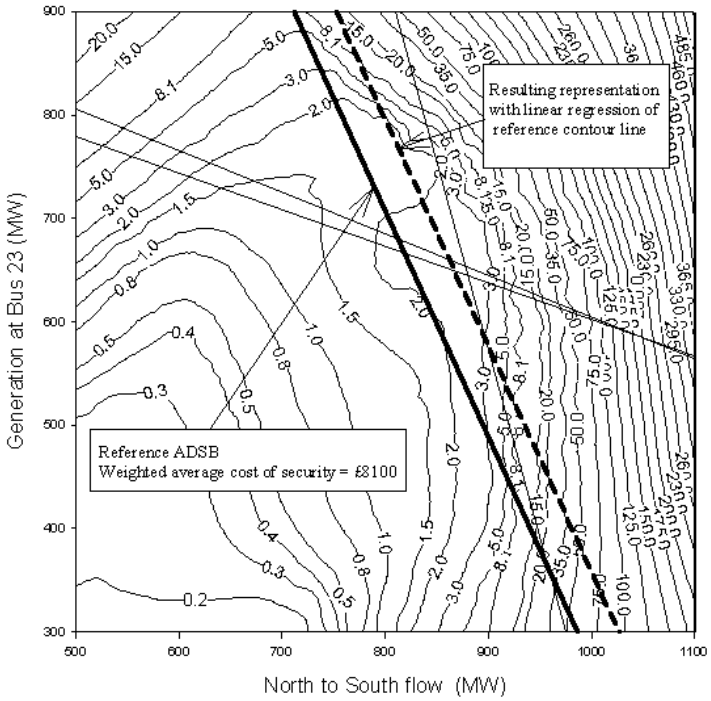

Figure 6.6: Reference single-line ADSB.

6.3.2.2 Calculation of Initial Group of the Single-line ADSB

The first step to calculate the initial group of the single-line ADSB is the calculation of families of single-line ADSB. Families of single-line ADSB are calculated by adjusting the study parameters in 50MW steps forward and backward from the reference single-line ADSB. At first the 'North to South flow' is adjusted in 50MW steps forward and backward from the reference single-line ADSB while the 'Generation at bus 23' is left unchanged. Figure 6.7 shows the resulting boundaries and these boundaries are considered as one family of single-line ADSB. A boundary in a family is called a member of that family.

The 'Generation at bus 23' is then adjusted forward and backward in 50 MW steps from the reference single-line ADSB, while the 'North to South flow' is left unchanged. Figure 6.8 shows the resulting boundaries and these boundaries are considered as another family of single-line ADSB. Figures 6.9 and 6.10 show respectively the weighted-average cost of security and the incremental cost of security of the families of single-line ADSB of Figures 6.7 and 6.8.

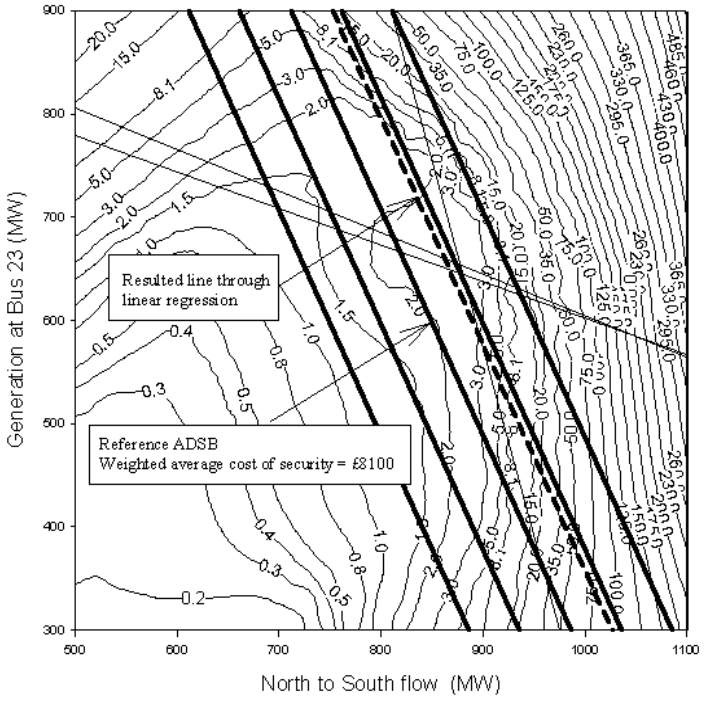

Figure 6.7: Family of single-line ADSB obtained by adjusting the 'North to South flow' in 50MW steps. The 'Generation at bus 23' is left unchanged.

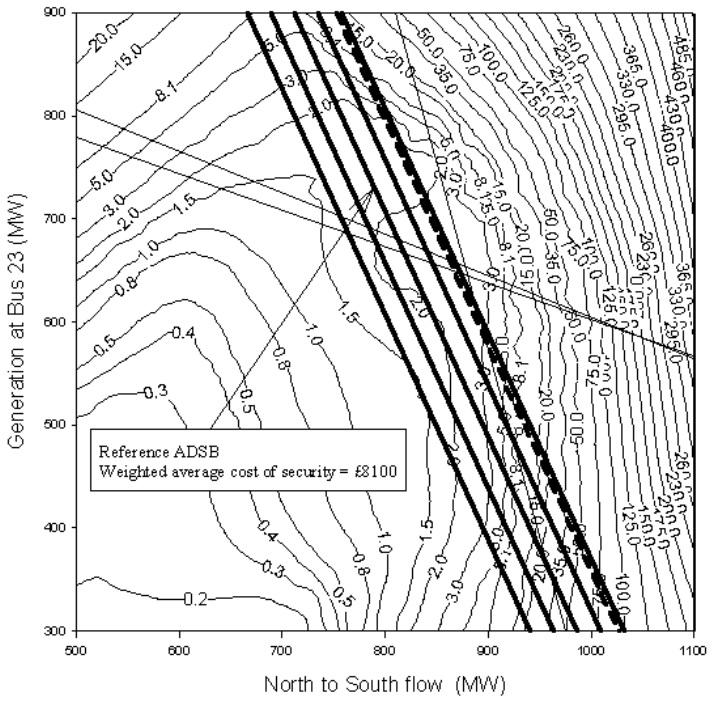

Figure 6.8: Family of single-line ADSB obtained by adjusting the 'Generation at bus 23' in 50MW steps. The 'North to South flow' is left unchanged.

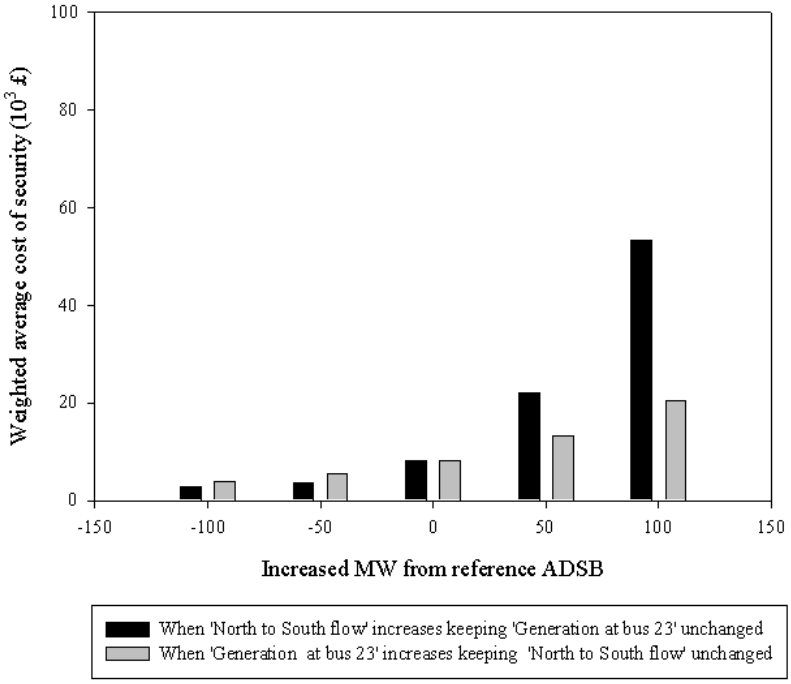

Figure 6.9: Weighted-average cost of security of the families of single-line ADSB. An increase of zero MW represents the reference single-line ADSB.

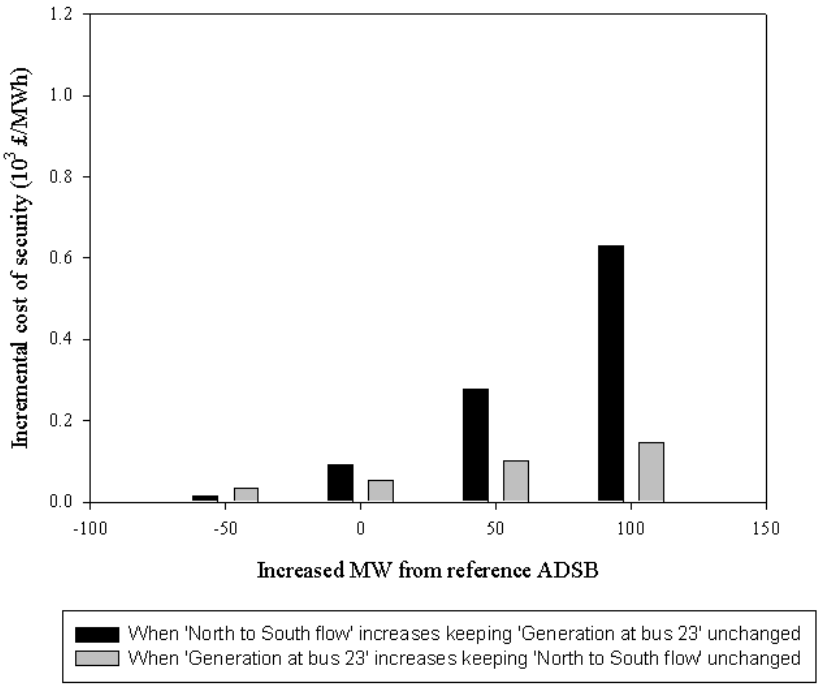

Figure 6.10: Incremental costs of security of the families of single-line ADSB. An increase of zero MW represents the reference single-line ADSB.

According to Figure 6.9, adjusting the 'North to South flow' or the 'Generation at bus 23' results in similar weighted-average cost of security up to the reference single-line ADSB. In figure 6.9, the reference single-line ADSB corresponds to zero increase in MW. Beyond the reference single-line ADSB, adjusting the 'North to South flow' result in higher weighted-average costs of security than adjusting the 'Generation at bus 23'. From Figure 6.10 it can be observed that the incremental cost of security increases significantly beyond the reference single-line ADSB for an increase in 'North to South flow'. This is because these are the areas where the cost of security increases rapidly for small changes in flows.

The initial group of the single-line ADSB is determined by combining the families in Figures 6.7 and 6.8.

6.3.3 Rectangular ADSB

6.3.3.1 Calculation of Reference for the Rectangular ADSB

Figure 6.11 shows the reference for the rectangular ADSB calculated using the methodology proposed in section 6.2.

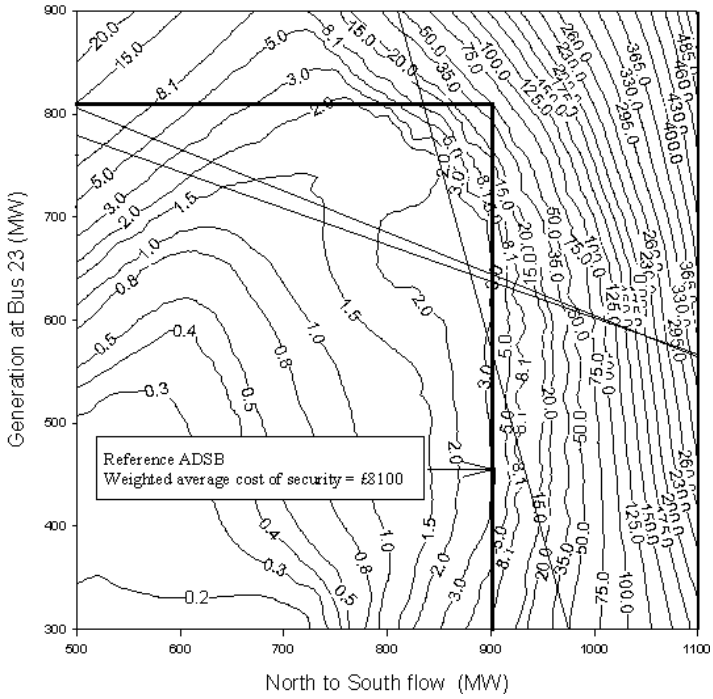

Figure 6.11: Reference rectangular ADSB.

In Figure 6.11 the region where the reference contour plot touches the 'North to South flow' axis has a higher cost of security than the region close to the 'Generation at bus 23' axis. Therefore, the first line of the reference rectangular ADSB begins from the 'North to South flow' axis. The second line is selected to give a weighted-average cost of security of £8100. The combination of these two lines is the reference for the rectangular ADSB.

6.3.3.2 Calculation of the Initial Group for the Rectangular ADSB

As in the single line ADSB, the first step to calculate the initial group of the rectangular ADSB is the calculation of families of rectangular ADSB. Families of rectangular ADSB are constructed using the same method as with the families of single-line ADSB. Figure 6.12 shows the family of rectangular ADSB for 50MW adjustments in the 'North to South flow' from the reference rectangular ADSB with the 'Generation at bus 23' unchanged. Figure 6.13 shows the family of rectangular ADSB obtained by adjusting the 'Generation at bus 23' in 50MW steps from the reference rectangular ADSB while the 'North to South flow' remains unchanged.

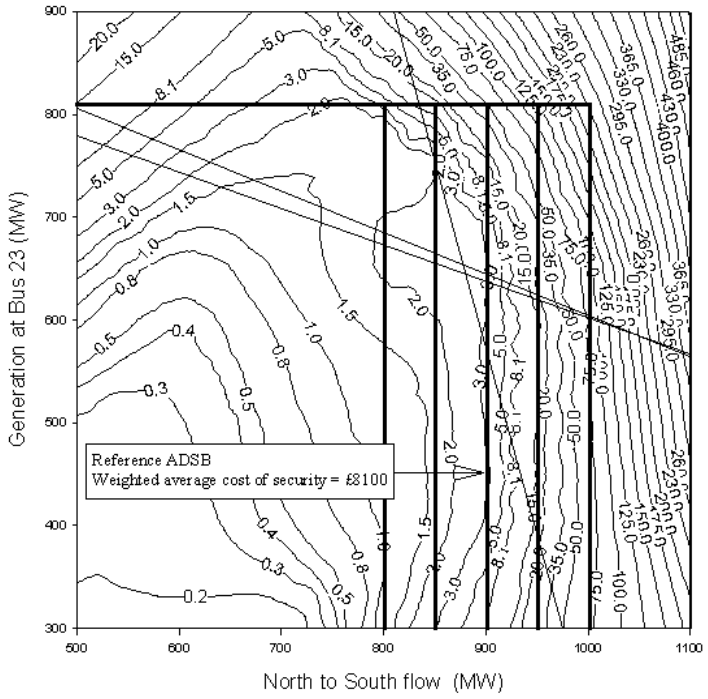

Figure 6.12: Family of rectangular ADSB obtained by adjusting the 'North to South flow' in 50MW steps. The 'Generation at bus 23' is left unchanged.

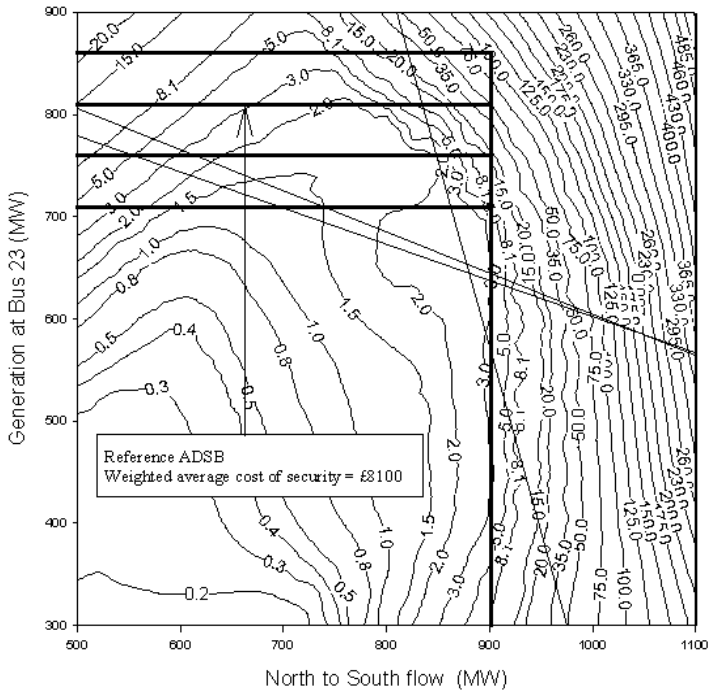

Figure 6.13: Family of rectangular ADSB obtained by adjusting the 'Generation at bus 23' in 50MW steps. The 'North-to-South flow' is left unchanged.

Figures 6.14 and 6.15 respectively show the weighted-average cost of security and the incremental cost of security of the rectangular ADSB that is shown in Figures 6.12 and 6.13. According to Figure 6.14, adjusting either the 'North to South flow' or the 'Generation at bus 23' within the reference rectangular ADSB results in a similar level of weighted-average cost of security. It can be observed from Figure 6.15 that the incremental cost of security increases significantly beyond the reference rectangular ADSB for an increase in 'North to South flow'.

The initial group of the rectangular ADSB is determined by combining the families of rectangular ADSB in Figures 6.12 and 6.13.

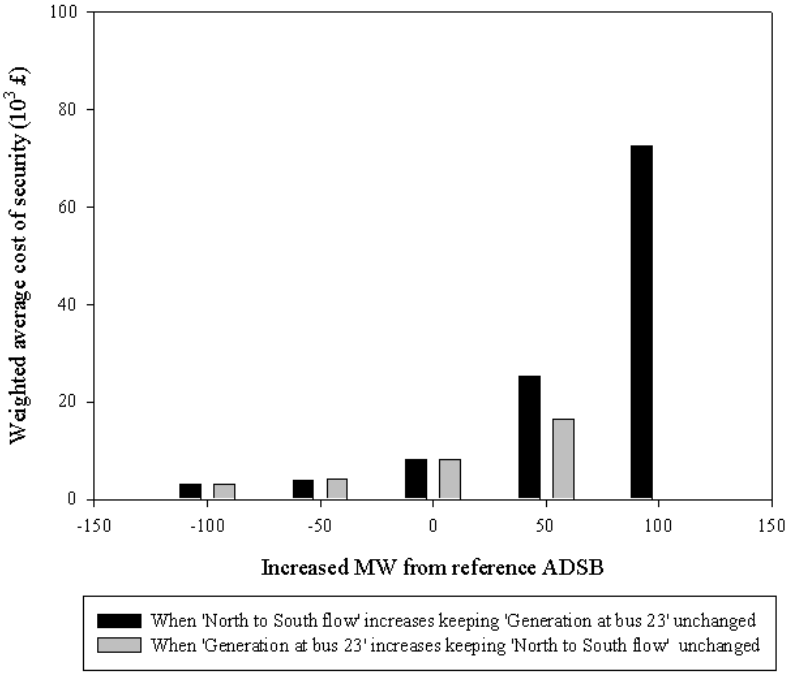

Figure 6.14: Weighted-average cost of security of the families of rectangular ADSB. An increase of zero MW represents the reference rectangular ADSB.

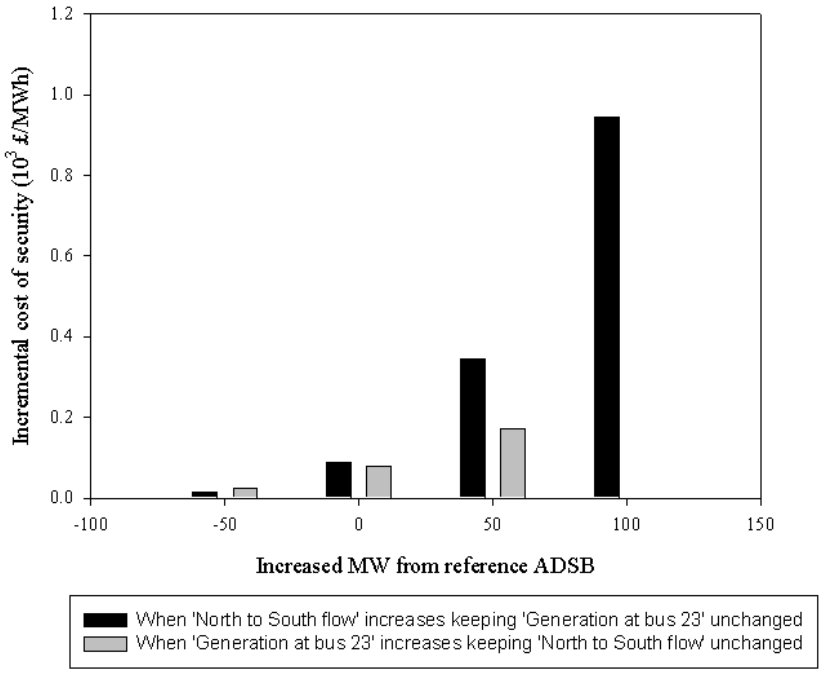

Figure 6.15: Incremental cost of security of the families of rectangular ADSB. An increase of zero MW represents the reference rectangular ADSB.

6.3.4 Tri-line ADSB

6.3.4.1 Calculation of Reference for the Tri-line ADSB

Figure 6.16 shows the reference tri-line ADSB. It can be seen from Figure 6.16 that the reference rectangular ADSB crosses the reference contour plot at two points. A line, which has an angle of 45 degrees, is drawn through one of these two points to remove the portion of the reference rectangular ADSB that goes beyond the reference contour plot. The point, which can remove the most of the portion of reference rectangular ADSB that goes beyond the reference contour plot is considered as the most suitable point to draw this line because this enables to construct more members in a family.

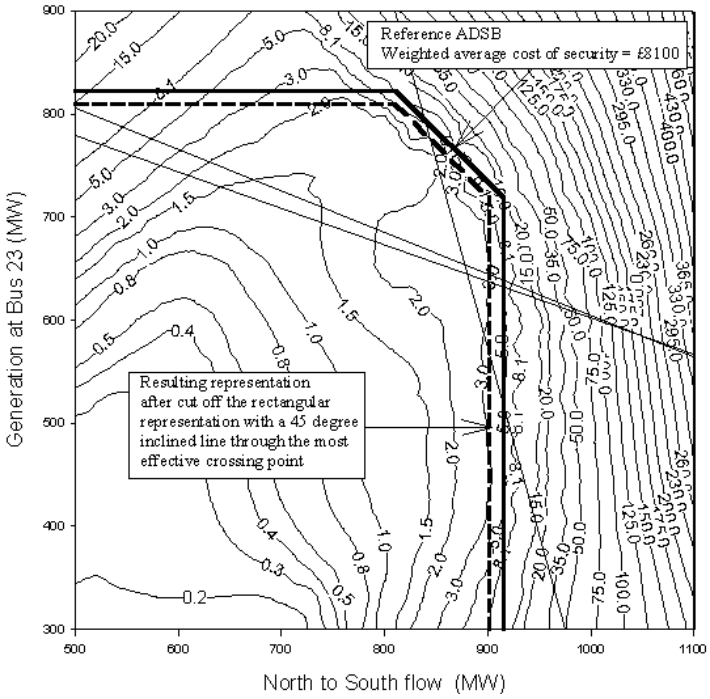

Figure 6.16: Reference tri-line ADSB.

With such a removal, the weighted-average cost of security reduces lower than £8100 at this stage of tri-line ADSB. It is needed to exist the weighted- average cost of security of the reference tri-line ADSB as £8100 because the weighted-average cost of security of the deterministic security boundary is £8100. This is achieved by uniformly enlarging the resulting tri-line ADSB until having a £8100 of weighted-average cost of security. Once achieved the £8100 of weighted-average cost of security, the resulting representation is called the reference tri-line ADSB.

6.3.4.2 Calculation of Initial Group of the Tri-line ADSB

As in the single line ADSB, the first step to calculate the initial group of the tri-line ADSB is the calculation of families of tri-line ADSB. Families of tri-line ADSB are constructed using the same method as used for the single-line ADSB. Figure 6.17 shows the reference tri-line ADSB and one family of the tri-line ADSB that is constructed by adjusting the 'North to South flow' forward and backward in 50MW steps from the reference while keeping the 'Generation at bus 23' unchanged. Figure 6.18 shows another family of tri-line ADSB obtained by adjusting the 'Generation at bus 23'

forward and backward in 50MW steps from the reference while keeping the 'North to South flow' unchanged. Figures 6.19 and 6.20 respectively show the weighted-average cost of security and incremental cost of security for the families of tri-line ADSB shown in Figures 6.17 and 6.18.

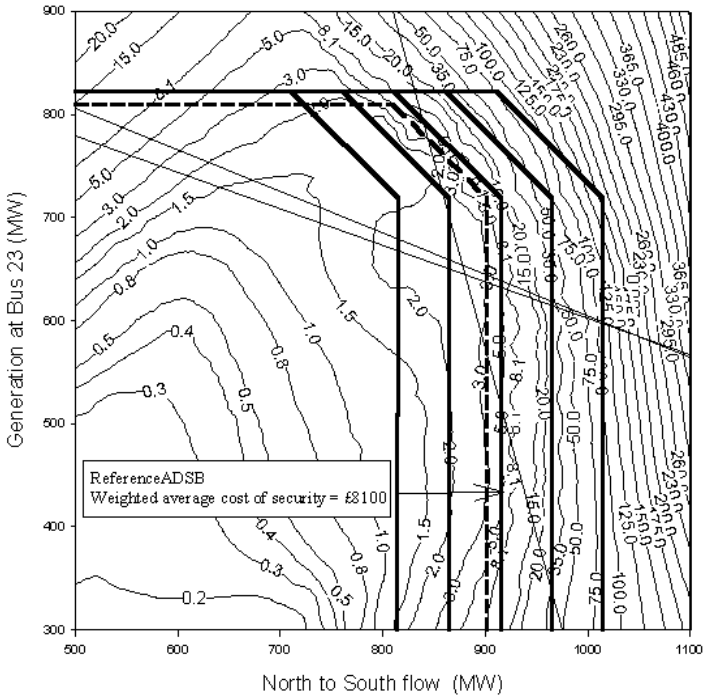

Figure 6.17: Family of tri-line ADSB obtained by adjusting the 'North to South flow' in 50MW steps. The 'Generation at bus 23' is left unchanged.

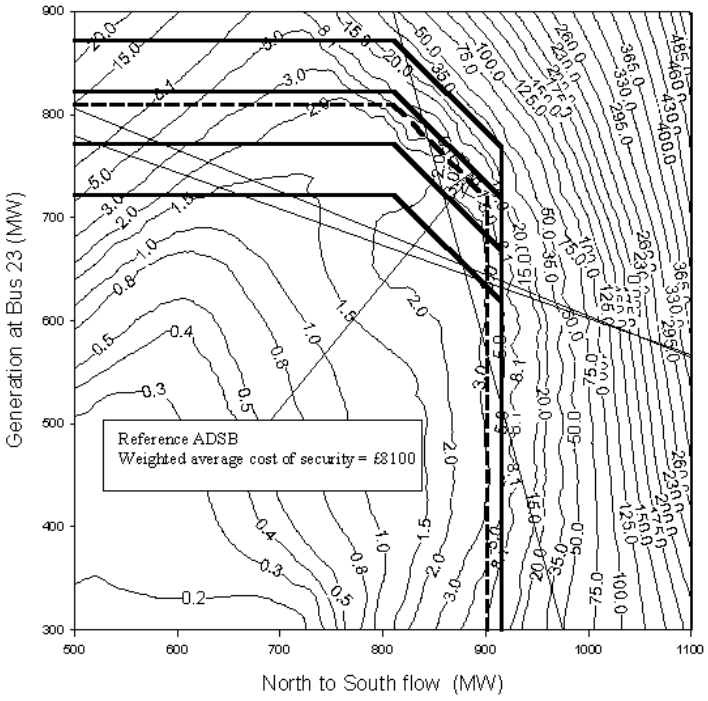

Figure 6.18: Family of tri-line ADSB obtained by adjusting the 'Generation at bus 23' in 50MW steps. The 'North to South flow' is left unchanged.

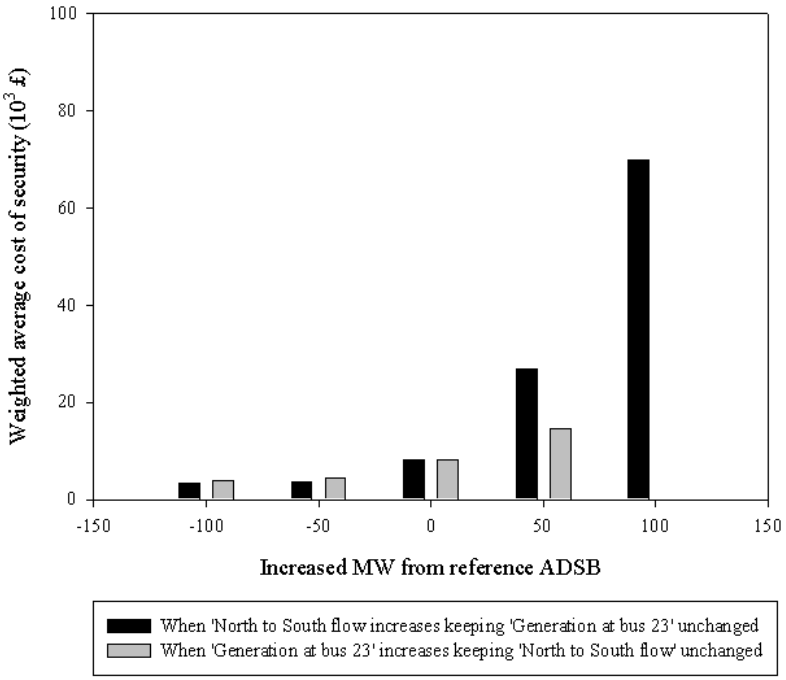

Figure 6.19: Weighted-average cost of security of the families of tri-line ADSB. An increase of zero MW represents the reference tri-line ADSB.

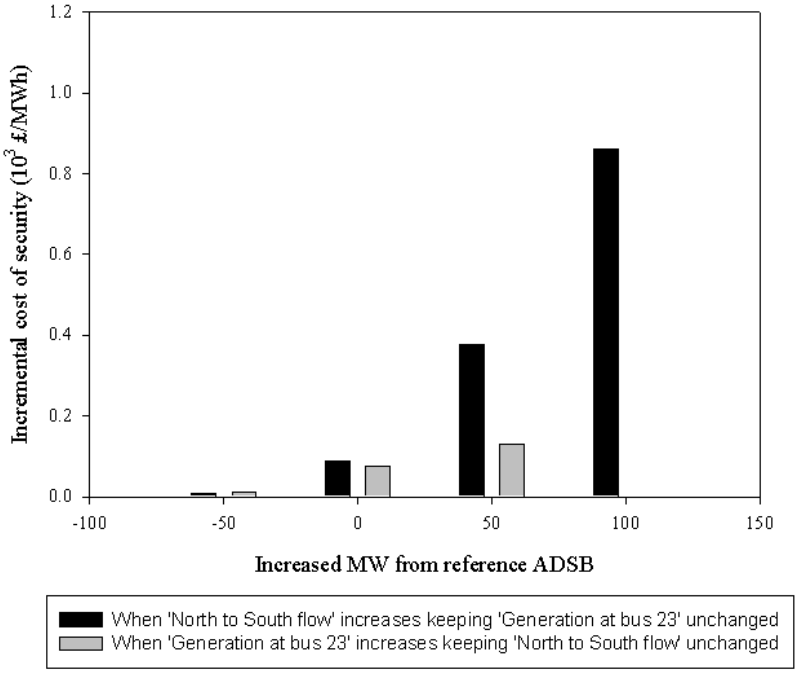

Figure 6.20: Incremental cost of security for the families of tri-line ADSB. An increase of zero MW represents the reference tri-line ADSB.

As in the previous types of ADSBs, the weighted-average cost of security beyond the reference tri-line ADSB increases significantly for an increase in 'North to South flow'.

The initial group of the tri-line ADSB is determined by combining the families of tri-line ADSB in Figures 6.17 and 6.18.

6.3.5 Calculation of System ADSB

The calculation of system ADSB is focused through rectangular and tri-line ADSBs as these two ADSBs better fit the reference contour plot than a single-line ADSB.

6.3.5.1 Rectangular System ADSB

In this step the rectangular system ADSB is calculated by moving the lines in the reference rectangular ADSB at the same time and then adjusting the study parameters separately. In other words more groups of ADSB are constructed to distribute them over

the system feasible operating region. This set of groups of ADSB is called rectangular system ADSB. Figure 6.21 shows the rectangular system ADSB.

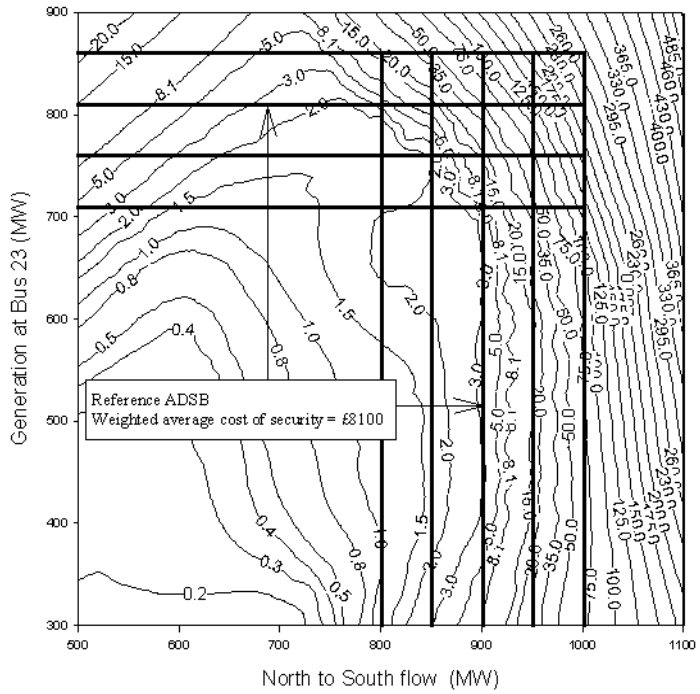

Figure 6.21: Rectangular system ADSB.

Figure 6.22 shows the weighted-average cost of security for the rectangular adaptive boundaries shown in Figure 6.21. Figure 6.22 confirms that the weighted-average costs of security increase with the 'Generation at bus 23' and the 'North to South flow'. In addition, the weighted-average cost of security of sets of rectangular ADSB also follows the same fashion as the smoothed values of cost of security (Smoothed values of costs of security are shown in Figure 5.6 of chapter 5).

Figure 6.23 shows the incremental cost of security of the rectangular ADSB for the adjustment of 'North to South flow'. Figure 6.24 shows the incremental cost of security of rectangular ADSB for the adjustment of 'Generation at bus 23'.

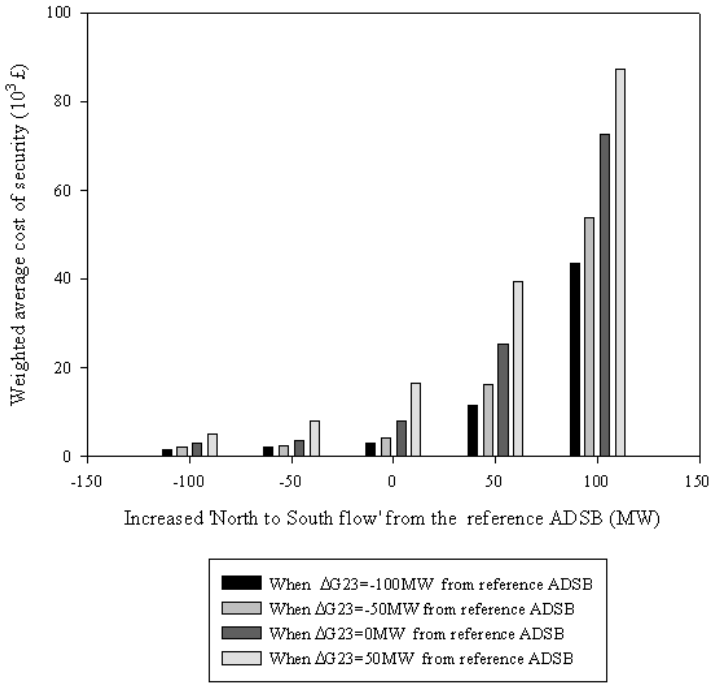

Figure 6.22: Weighted-average cost of security of sets of rectangular ADSB.

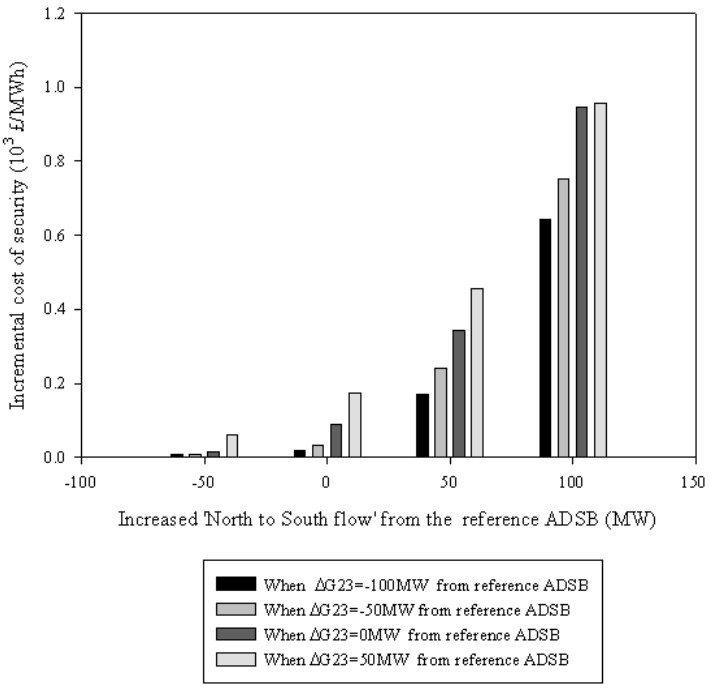

Figure 6.23: Incremental cost of security for the sets of rectangular ADSB for the adjustment of 'North to South flow'.

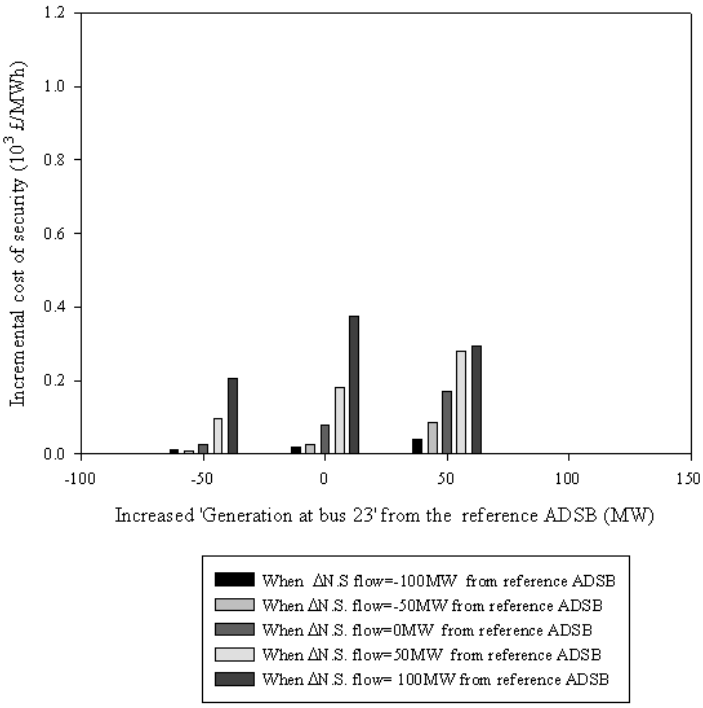

Figure 6.24: Incremental cost of security for the sets of rectangular ADSB for the adjustment of 'Generation at bus 23'.

6.3.5.2 Tri-line System ADSB

Figure 6.25 shows the tri-line system ADSB. The calculation of these boundaries follows the same method used for calculating the rectangular system ADSB from the initial group of the rectangular ADSB.

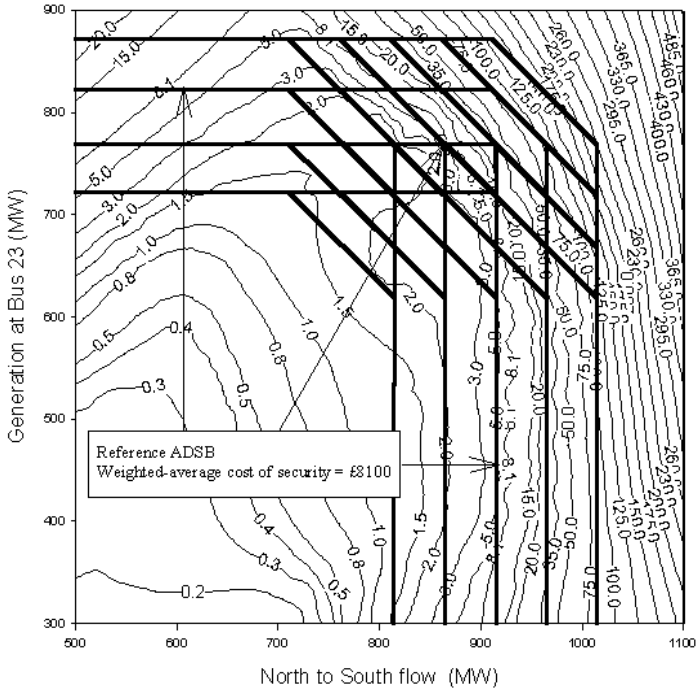

Figure 6.25: Tri-line system ADSB.

Figure 6.26 shows the weighted-average cost of security for the tri-line ADSB. Sets are defined with a specified 'Generation at bus 23' and adjusted 'North to South flow'. Comparing Figure 6.26 with Figure 6.22 shows that there is close similarity in weighted-average cost of security distribution of tri-line ADSB and rectangular ADSB. Both type of ADSBs also observe a similar uniformity. This is because for the tri-line ADSB, although the portion of the reference rectangular ADSB that goes beyond the reference contour plot is removed, when the resulting tri-line type ADSB is magnified, the tri-line types of the ADSB also have similar weighted-average costs as the rectangular ADSB.

Figure 6.27 shows the incremental cost of security for the tri-line ADSB for the adjustment of 'North to South flow'. Figure 6.28 shows the incremental cost of security for the tri-line ADSB for the adjustment of 'Generation at bus 23'.

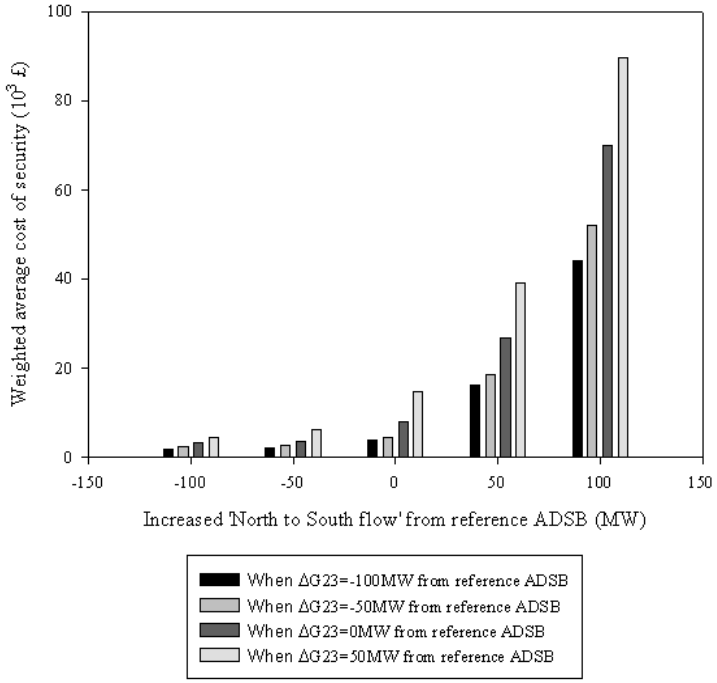

Figure 6.26: Weighted-average cost of security for the tri-line ADSB that are shown in Figure 6.25.

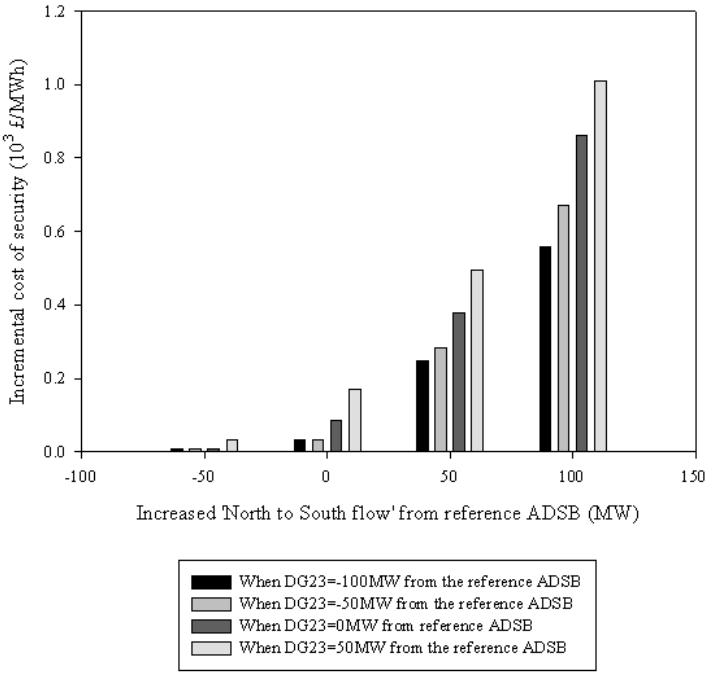

Figure 6.27: Incremental cost of security for the tri-line ADSB for the adjustment of 'North to South flow'. Weighted average costs of security corresponding to these sets are shown in Figure 6.26.

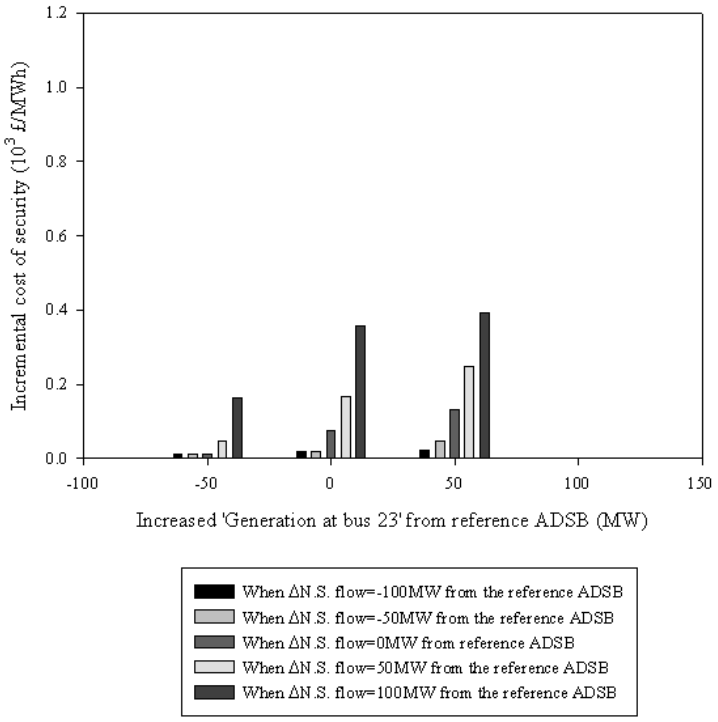

Figure 6.28: Incremental cost of security for the tri-line ADSB for the adjustment of 'Generation at bus 23'. Weighted average costs of security corresponding to these sets are shown in Figure 6.26.

From these investigations, it is obvious that the rectangular ADSB has the similar properties as of the tri-line ADSB. Single-line ADSB can also be used to calculate the ADSB. However, this type of ADSB does not fit well with the reference contour plot.

6.4 Cost of Energy and ADSB

ADSB reflects the cost of security in the power system. It is also vital to combine this information with the cost of energy along the ADSB, because this information is useful for the decision making process in power system operation. Figures 6.29 and 6.30 respectively show the rectangular system ADSB and tri-line system ADSB together with contours of constant cost of energy. The numbers along the contour lines indicate the cost of energy (in thousands of pounds).

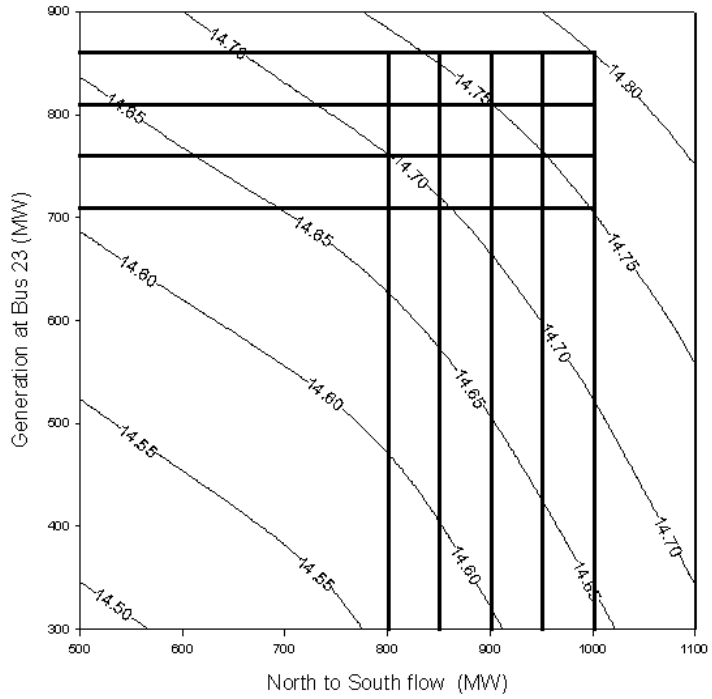

Figure 6.29: The cost of energy levels and the rectangular system ADSB. (Corresponding costs of security levels are shown in Figure 6.21).

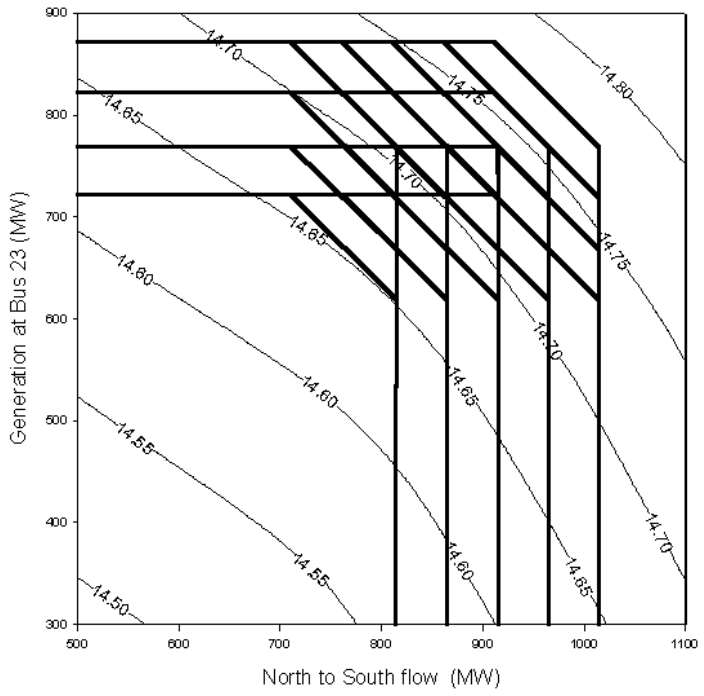

Figure 6.30: The costs of energy levels and the tri-line system ADSB. (The corresponding costs of security levels are shown in Figure 6.25).

One particular feature of the cost of energy is that it does not vary significantly throughout the feasible operating region. The minor deviations in cost of energy levels are due to the outages of generating plants. Outages of generating plants reduce the plants that actively supply energy. Thus, fewer units in operation reduce the cost of energy.

6.5 Discussion

Novel security criteria are proposed in this chapter to assess the power system security. These criteria are called adaptive deterministic security criteria and they calculate ADSB.

These criteria at first calculate the deterministic security boundary and then the probabilistic costs of security levels. Cost of security is estimated using the Monte Carlo simulation. A weighted-average cost of security is used to minimise the inconsistency of the cost of security along the deterministic security boundary.

Three ADSBs are proposed to calculate and to identify the best ADSB. They are single-line, rectangular and tri-line. Separate investigations were performed for each of these types of the ADSBs. The calculation of the ADSB using the results of deterministic security boundary and the probabilistic cost of security has three main processes. The first process identifies the reference contour plot and calculates the reference ADSB. The second process extends the reference ADSB to calculate the families of the ADSB and combines them to form the initial group of ADSB. The third process calculates the system ADSB by calculating more groups of ADSB to distribute them over the system feasible operating region. The methodology of the adaptive deterministic security criteria was applied to the modified 24-bus IEEE Reliability Test System.

ADSB can be used to justify the cost of security for a particular operating condition. They also signal the incremental cost of security of such an operation. The incremental costs of security of the ADSB can be used to test the operational plans optimally.

6.6 How to Use in Power System Operation?

Figure 6.31 shows the rectangular system ADSB calculated for the modified 24-bus IEEE Reliability System, where inter boundary adjustments are in 50MW steps. The weighted-average costs of security corresponding to this figure are given in Figure 6.22 and the incremental costs of security are given in Figures 6.23 and 6.24.

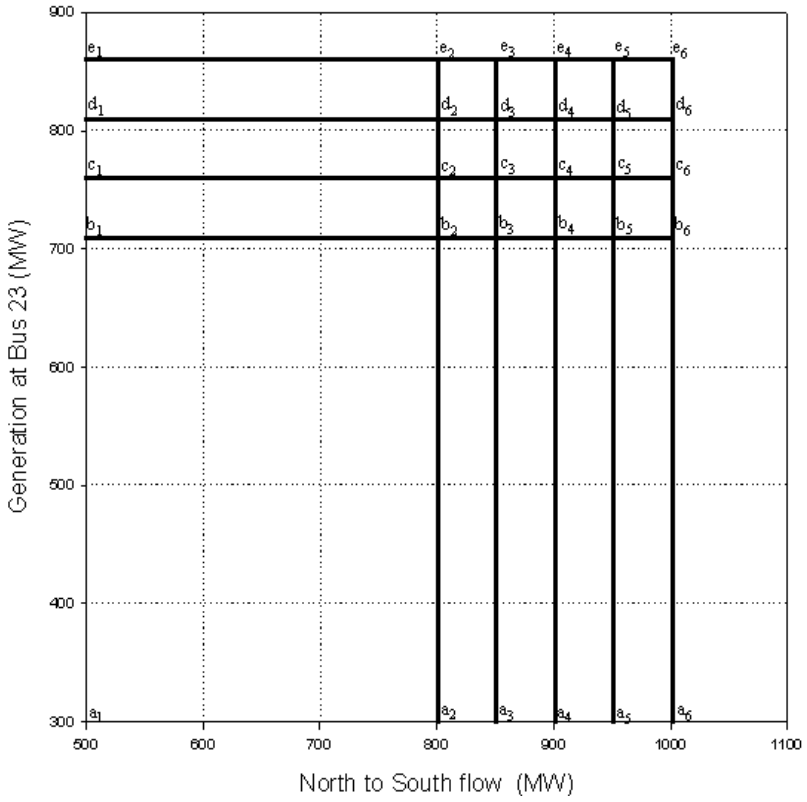

Figure 6.31: Rectangular system ADSB calculated for the modified 24-bus IEEE Reliability Test System.

For example if the system operates within $a_1a_2b_2b_1$ boundary the weighted-average cost of security for this operation would be £1656. If the system needs to be operated beyond the $a_1a_2b_2b_1$ boundary then there are three options.

The first option is to increase the 'North to South flow'. A 50MW increment from $a_1a_2b_2b_1$ (i.e., $a_2a_3b_3b_2$ region) results in a weighted-average cost of security of £2063 and an incremental cost of security of 8 £/MWh; Increasing the flow beyond 50MW but

up to 100MW (i.e., $a_3a_4b_4b_3$ region) results in a weighted average cost of security of £2969 and an incremental cost of security of 18 £/MWh; Increasing it beyond 100MW but up to 150MW (i.e., $a_4a_5b_5b_4$ region) results in a weighted average cost of security of £11431 and an incremental cost of security of 169 £/MWh; Increasing it beyond 150MW but up 200MW (i.e., $a_5a_6b_6b_5$ region) result a weighted average cost of security of £43626 and an incremental cost of security of £644/MWh.

The second option is to increase the 'Generation at bus 23'. For example up to 50MW from $a_1a_2b_2b_1$ (i.e., $b_1b_2c_2c_1$ region) results in a weighted average cost of security of £2176 and incremental cost of security of 10 £/MWh; beyond 50 MW but up to 100MW (i.e., $c_1c_2d_2d_1$ region) results in a weighted average cost of security of £3026 and incremental cost of security of 17 £/MWh; beyond 100MW but up to 150MW (i.e., $d_1d_2e_2e_1$ region) results in a weighted average cost of security of £5080 and incremental cost of security of £41/MWh.

In the third option, both study parameters are adjusted simultaneously. For example both the 'North to South flow' and the 'Generation at bus 23' can be increased by up to 50MW from the $a_1a_2b_2b_1$ boundary to the $a_2a_3c_3c_1b_1b_2$ region, which results in a weighted average cost of security of £2536 or else the study parameters can be adjusted in different proportions such as the 'North to South flow' of up to 100MW and the 'Generation at bus 23' up to 50MW from $a_1a_2b_2b_1$ to $a_3a_4c_4c_1b_1b_3$ region, which results in a weighted-average cost of security of £4211.

In this way, the operator can test their operational plans to minimise the cost of security. The ADSB can also be used as a metric in a security/economy trade-off situation. Such tools are particularly useful in the current competition in the electricity industry as the systems are more stressed and more vulnerable to outages than in the past. In that context security tools should be capable of more than the 'N-1' or 'N-D' security criteria.

Chapter 7

Conclusions and Recommendations for Further Research

7.1 Conclusions

7.1.1 General

Power systems are always vulnerable to disturbances. These disturbances are unpredictable and some of them are unavoidable. Current practice uses a considerable safety margin to protect power systems against credible but unpredictable contingencies. Traditional security assessment does not consider the possibility of cascading tripping of lines or sympathetic tripping. Such events can cause catastrophic damages to power systems and can have severe financial and social impacts.

Traditional security assessment classifies the system as secure or insecure. There is no gradation between these two states. In other words, it does not give to the operators a quantitative measure of the level of security in a power system. Such security indications also carry risks if the system operates close to or beyond the deterministic security limits, as happens more and more frequently because of the deregulation of the electricity industry. Such practice can invite disastrous consequences for the power system, including partial or total system blackouts. This highlights the importance of tools that can measure system security quantitatively.

In a power system, since contingencies are random in nature, they can only be analysed rigorously using probabilistic techniques. Probabilistic analysis can be performed with state enumeration or Monte Carlo simulation. With larger power systems, the state enumeration approach is infeasible because of its complexity. Monte Carlo simulation is the most attractive in this context and easy to implement. Correlated Sampling is very

attractive when comparing scenarios faster because it converges faster than naïve Monte Carlo simulation. Typically, correlated sampling is 5-10 times faster than naïve Monte Carlo simulation.

The Probabilistic Indicator of System Stress described in this thesis provides such a quantitative measure of system security. The details of the design, calibration and testing of this indicator are given in Chapter 4. The conclusions that can be drawn from Chapter 4 are given in section 7.1.2 of this Chapter. The proposed indicator of stress is a novel technique and operators would have to be trained in its use.

Chapter 5 compares the deterministic and probabilistic security criteria. The conclusions that can be drawn from chapter 5 are given in section 7.1.3.

Although probabilistic approaches are capable of indicating system security comprehensively and rigorously, operators may not be comfortable with using this type of analysis because of the complexity associated with applying this type of decision making process in a busy operating centre. They need simple and robust deterministic answers. To fill this gap Adaptive Deterministic Security Criteria are proposed in Chapter 6. The conclusions that can be drawn from Chapter 6 are given in section 7.1.4 of this Chapter. These criteria combine the deterministic security criteria with a probabilistic measure of the cost of security. The decisions can be made with simple and robust rules as in deterministic security criteria. It makes the decision-making process easier and provides some knowledge of the economical benefits of the decisions made. More importantly, it can minimise the hidden risks associated with operating conditions.

7.1.2 Probabilistic Indicator of System Stress

A novel technique is proposed for measuring the level of security or the level of stress in a power system. This technique is designed to be used in an operational environment. It performs a probabilistic rather than a deterministic analysis to indicate the system stress on a continuous scale. This indicator of stress was tested on the 24-bus IEEE Reliability Test System and on a 1085-bus model of the NGT (UK) System, which is

based on a snapshot from NGT's state estimator. Calibrated indicators for both systems complied with the design requirements.

The ranking of the reference cases in the indicator of stress remains robust for any system conditions. This has been proved by investigating the ranking for increased failure rates. This further verifies the suitability of the indicator for power system operations, and particularly highlights the suitability even with severe weather conditions.

The maximum and minimum limits in the scale of indicator of stress are decided by the highest and lowest load levels in the base case for which the system can be operated. Infeasibilities are identified by the divergence of the power flow. Two different calibration techniques were tested. The first calibration technique progressively increases the system demand to increase the system stress and creates a set of reference cases that spans the entire scale of the indicator of stress. The second technique take some components out of service, up-rates and de-rates some plants and then adjust the system load to create another set of reference cases. These new cases have comparable levels of stress as the cases produced by the first calibration technique. Measured stress levels of new cases, which simulate real time power system operating conditions, indicate that both techniques calibrate the indicator of stress with similar accuracy. The indicator of stress is thus not affected by the way it is calibrated. A drawback of the second calibration technique is that it requires a slightly higher CPU time than the first calibration technique. Building the reference cases in the second calibration technique is almost more complicated than in the first calibration technique.

Monte Carlo simulation and extended stratified sampling play a vital role when calibrating or re-calibrating the indicator of stress for large real networks. This is because in large networks complete system collapses dominate the convergence of Monte Carlo simulation. A variance reduction technique is thus required to ensure convergence.

In extended stratified sampling the disconnected loads are used as the stratification variable. Then number of strata that would reduce the variance of the estimate and maintain the precision of the estimate is determined. Strata are allocated without emptying any stratum. In this allocation, one stratum is allocated with the trials that do not disconnect any load, and another stratum is allocated with the trials, which experience larger load disconnections such as partial blackouts (system blackouts are ignored when designing an indicator of stress for 1085-bus model of the NGT (UK) system). Remaining strata are allocated with other trials according to the amount of load disconnection.

A new convergence criterion is proposed for the Monte Carlo simulation and is referred to as the fixed standard deviation criterion. This fixed standard deviation criterion functions in parallel with the criterion that has to be satisfied to meet the degree of confidence for the confidence limit of the estimation. Such a combination is useful when estimating the energy not served of the healthiest cases with the Monte Carlo simulation.

Three statistical tests are also proposed for determining where a new case should be placed on the calibrated scale of system stress. The first test determines whether a new case is more stressed than a reference case, the second test determines whether a new case is less stressed than a reference case and the third test determines whether a new case has about the same stress level as a reference case. When comparing new cases with the reference cases of the calibrated indicator of stress if any of these tests is satisfied with the certainty of the comparison then the comparison stops as it reached a conclusion.

The resolution of the calibrated scale determines how much time is required to estimate the placement of new cases on the scale. A higher resolution requires a larger the number of correlated sampling trials. The choice of resolution is thus a key issue when calibrating the indicator of stress. In the operational time frame processing time should indeed be as small as possible.

Since the proposed indicator of stress is system-dependent, calibration has to be performed for each power system. If there are major expansions or reinforcement in the network, re-calibration of the indicator of stress may be necessary.

One of the major advantages of the proposed indicator of stress over the contingency analysis tools is its ability to highlight cases that are highly stressed but satisfy the deterministic security criteria. Timely identification of such operating conditions could avoid blackouts of devastating consequences.

Measuring the stress against simultaneous outages makes the measurements realistic. A continuous indication of stress level could be used by power system operators to decide if the current level of stress justifies taking preventive actions aimed at improving the security of the system. It is often said that power systems are being operated much closer to their limit than in the past. Since this index of stress takes into account all the factors that are relevant in system operations, it could be used to provide a quantitative verification of this statement.

7.1.3 Comparison of Deterministic and Probabilistic Security Criteria

The deterministic security boundary is determined by the limiting contingencies. The region where none of the limiting contingencies causes a violation of operating constraints defines the region where the power system can be safely operated according to the deterministic security criteria. Operating the system beyond these boundaries is considered unacceptable because credible contingencies could cause violations of operating limits.

A probabilistic measure of system security can be determined based on a calculation of the cost of security. This measure can be obtained at each point of a grid spanning the feasible operating region of a power system. Each grid point corresponds to a base case for the Monte Carlo simulation, which is used to estimate the costs of security.

The Monte Carlo simulation uses stratified sampling with shed load stratification to reduce the variance of the estimate and accelerate convergence. In this study, one stratum is allocated with the trials that do not disconnect any load and another stratum is allocated with the trials, which experience system blackouts. Remaining strata are allocated with other trials according to the amount of load disconnection.

Contour plots are used to highlight how the cost of security varies with the operating conditions.

Extended investigations suggest that the influence of standard deviation on the cost of security is negligibly small when the convergence criteria of the Monte Carlo simulation have been satisfied.

Comparison of probabilistic cost of security levels and deterministic security boundary shows that the cost of security along the deterministic security boundary is not consistent.

7.1.4 Adaptive Deterministic Security Criteria

Adaptive deterministic security criteria (ADSC) integrate deterministic security boundary and the probabilistic cost of security through the weighted-average cost of security. Three robust and simple types of the adaptive deterministic security boundaries (ADSBs) are proposed for investigating the ADSC. These include single-line, rectangular and tri-line. Rectangular and tri-line ADSBs are most similar in weighted-average cost of security as well as incremental cost of security at the respective boundaries. The tri-line ADSB takes slightly more time than rectangular ADSB to calculate the system ADSB and the inclined line in the tri-line ADSB must be 45 degrees.

The rectangular and tri-line ADSBs provide more precise adaptive deterministic security boundaries compared to the single-line ADSB as they can fit well with the reference contour plot. The single-line ADSB does not fit well with the reference

contour plot compared to rectangular and tri-line ADSB. Further, the angle of a single-line ADSB should be 45, 90, 135 or 180 degrees. Maintaining such an angle and performing linear regression of the reference contour plot may be difficult. Therefore, these investigations suggest that the rectangular ADSB is the best form of ADSB among the types that were investigated.

The following steps should be followed to determine the ADSB for a system with two study parameters:

- Calculate the deterministic security boundary
- Divide the feasible operating region with a suitably sized grid
- Estimate the cost of security at each point of the grid
- Smooth the values of cost of security
- Represent the cost of security as a contour plot
- Calculate the weighted-average cost of security of the deterministic security boundary
- Identify the reference contour plot
- Calculate the reference rectangular ADSB using the reference contour plot
- Calculate the families of rectangular ADSB using reference rectangular ADSB
- Determine the initial group of the rectangular ADSB using families of rectangular ADSB
- Determine the rectangular system ADSB by constructing more groups of the rectangular ADSB, which distribute over the system feasible operating region
- Calculate the weighted-average cost of security and incremental cost of security of each rectangular ADSB

Any operating point within the feasible operating region is bounded by an adaptive deterministic security boundary. This enables the operators to justify the cost of security at a particular operating condition and the feasibility of such operation. The adaptive deterministic boundaries are simpler and more robust than the probabilistic cost of security. Unlike the traditional deterministic security boundary, the ADSB indicates system security even beyond the ‘N-1’ or ‘N-D’ deterministic security criteria. Such ADSBs are particularly important in the current climate of competition in the electricity

industry because it makes it possible to balance security levels and economical benefits when operating the system beyond the traditional security limits.

7.1.5 Use of the Proposed Tools in Power System Operation

The probabilistic indicator of system stress provides a global measure of system security. It can be used in the first place to measure the system security quantitatively. It could be applied in parallel with existing security tools. Such an arrangement provides a wider basis for the operators' decisions.

The ADSB could be used to identify operating conditions that are economically justifiable on the basis of the cost of security. The ADSB provides a deterministic solution in a probabilistic framework. On the other hand, the indicator of system stress provides a purely probabilistic solution.

7.2 Validation of Probabilistic Indicator of System Stress

The probabilistic indicator of system stress was calibrated and tested on the 24-bus IEEE Reliability Test System and on a model of the NGT (UK) system. It is required to validate the proposed indicator of stress of the model of NGT (UK) system. Testing the indicator calibrated on the NGT (UK) system model with actual operating scenarios would further validate its usefulness. It would also help determine the levels of stress into normal, alert and emergency ranges.

7.3 Calculation of ADSB for a Model of the NGT (UK) System

Adaptive deterministic security criteria are defined and ADSB is calculated for the modified 24-bus IEEE Reliability Test System (1996). The results of these investigations suggest that defining ADSC is possible and it can capture the system security more accurately than the traditional deterministic security criteria. Therefore, it is suggested to calculate the ADSB for a model of the NGT (UK) system.

7.4 Recommendations for Further Research

7.4.1 Probabilistic Indicator of System Stress

The criticism that reviewers of the paper submitted to IEEE Transactions on Power Systems made of the indicator of system stress is that it does not help the operator decide what needs to be done if the indicator of stress suggests that there is a problem. Therefore, further work of the indicator of system stress will focus on determining the areas where most of the problems occur. This could be done by identifying the regions where most of the load is shed during the Monte Carlo simulation.

7.4.2 Adaptive Deterministic Security Criteria

ADSB were calculated considering two study parameters. It is vital to calculate ADSB with three study parameters because the operation of a power system often cannot be reduced to two parameters.

With three study parameters (for example, the generation level, the flow level, system load), the deterministic security boundary would have to be represented in three dimensions and the deterministic security boundary would be a two-dimensional surface. This surface can be calculated by adjusting the study parameters with suitable study criteria. In such a development the following issues are to be addressed.

- Choosing the study parameters
- Choosing suitable study criteria
- Calculating deterministic security surface
- Integrating deterministic security surface with the cost of security levels

Calculating ADSB for three study parameters would obviously be much more complex than with two parameters when integrating the deterministic security surface with the cost of security.

These difficulties can be mitigated by separately calculating the deterministic security boundary and the cost of security considering two parameters at a time. Once calculated three sets of two-dimensional deterministic security boundary, the cost of security levels corresponding to each set can be integrated with the respective deterministic security boundary to calculate three sets of ADSBs as demonstrated in chapter 6.

Then three-dimensional ADSB can be calculated by averaging the weighted-average cost of security of each two-dimensional ADSB. In this approach, the three-dimensional ADSB would be surfaces.

Therefore, it is recommended to extend the calculation of the ADSB considering three study parameters.

7.4.3 Value of Security Assessor

VaSA can be used to define security-classified zones in a power system according to the levels of insecurity. The levels of insecurity are determined on the basis of the cost of security.

At first each bus in a power system is considers as located in separate unit zones. For example if there are *n* busses in a power system then there will be *n* unit zones. Then, the cost of security for the outage of each bus is separately estimated using VaSA. This is because outage of a bus results in the maximum cost of security that can occur for outage of any number of components that are connected to this bus. If disconnecting a bus results in infeasible operation (i.e., divergence of the power flow) then the cost of security of such an operating condition can be valued at the cost of security of a system blackout.

Next, the costs of security of each bus outage are classified into set of groups. For example group one can be allocated with the busses that have the lowest cost of security (i.e. the lowest insecurity level in the power system). In this way, all the busses in the

system are allocated to a particular group according to their cost of security. These groups are considered as security-classified zones.

In this approach, the loads disconnection due to Monte Carlo simulation can be used to identify the maximum number of affected zones for an insecurity problem in a particular unit zone.

This approach can be extended to explore the possibility of classifying the level of insecurity according to the group maximum cost of security and the maximum number of affected zones for an insecurity problem in a group. To estimate the maximum cost of security in a group, the cost of security must be estimated by disconnecting buses one by one until the maximum cost of security in that zone is reached.

Such security-classified zones and the information on possible affected zones would be useful to identify where new facilities should be built to enhance the overall level of security. It would also help identify the possible number of zones that may be affected by outages in a particular zone.

Therefore, it is recommended to apply VaSA to the definition of security-classified zones in a power system.