1992

A framework for power system security and vulnerability assessment

Qin Zhou
Iowa State University

U·M·I

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

Order Number 9311548

A framework for power system security and vulnerability assessment

Zhou, Qin, Ph.D.

Iowa State University, 1992

U·M·I
300 N. Zeeb Rd.
Ann Arbor, MI 48106

A framework for power system security and vulnerability assessment

by

Qin Zhou

A Dissertation Submitted to the
Graduate Faculty in Partial Fulfillment of the
Requirements for the Degree of
DOCTOR OF PHILOSOPHY

Department: Electrical Engineering and Computer Engineering
Major: Electrical Engineering (Electric Power Systems)

Approved:

Signature was redacted for privacy.

In Charge of Major Work

Signature was redacted for privacy.

For the Major Department

Signature was redacted for privacy.

For the Graduate College

Iowa State University
Ames, Iowa

1992

Dedicated to

my mother and my father:

De-Xin Chen

Rong-Guang Zhou

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ACKNOWLEDGEMENTS

I would like to thank my major professor, Dr. A. A. Fouad for his invaluable guidance and encouragement throughout this research work. I deeply appreciate his fatherly advice. The technical discussions with my major professor helped me develop my analytical skills. I am also thankful to Dr. Fouad for providing financial support during my Ph.D. program.

I am thankful to Dr. V. Vittal and Dr. J. Davidson for their contribution to my research. I would also like to thank the other members of my committee: Dr. J. Lamont, Dr. E. Johnston, and Dr. M. H. Khammash.

This research was sponsored by National Science Foundation and the Electric Power Research Center at Iowa State University. I appreciate their financial support.

I am thankful to Mr. Vamsi Chadalavada for his assistance in using the sensitivity program. My fellow graduate students in the power program at Iowa State University provided a good research environment and made my work enjoyable.

My special thanks to my father Rong-Guang Zhou, who provided moral support throughout the graduate program.

1. INTRODUCTION

In modern society, the electric utilities must supply the customers with reliable electricity at nearly constant voltage and frequency without interruption of service [1]. Thus the power system security is currently one of the most important concerns in the electric utility industry.

1.1 Power System Security

The security of a bulk power supply is defined as: "the ability of the bulk power system to withstand sudden disturbances such as electric short circuits or unanticipated loss of system components" [2].

Based on the above definition of power system security, the system must be able to meet the load demand in the presence of sudden disturbances. It is also necessary that enough reserve generation and transmission capacities are available to take up the changes in loading caused by the disturbance, and that the control devices are able to return the system to normal operation after the disturbance. Such "robustness" of the system relative to the credible disturbances is at the heart of power system security.

The current situation in most of the power systems in North America is that the continued rise in power demand has reduced the overcapacity of generation of a few years ago to minimal level. Problems with construction of new generation facilities means that the electric utility industry may soon have much reduced reserve capacity. On the other hand almost every electric utility has experienced the difficulties of getting new transmission facilities approved and built, resulting in heavier loading of existing transmission network. Therefore, the power system is operating closer to its operating limit than it was before, and this means that power system security is a growing concern.

The basic requirement of power system security is that, following the occurrence of a sudden disturbance, the system can "survive" the ensuing transient and move into an acceptable steady-state condition. In this new steady-state condition all power system components must be operating within established limits. Thus there are two major security problems encountered [3].

1. Static security

It deals with whether all power system components are operating within established limits. If there are changes in the network, they are assumed to have taken place and the new steady-state operating condition have been reached.

The method used for static security analysis is steady-state analysis, and the static security includes two components:

a. Thermal:

   That is the loading of the power system element does not exceed the thermal rating.

b. Voltage:

   The voltage at a given bus is within specified limits.

2. Dynamic security

It deals with the power system in transition, following a disturbance, from an initial operating state to another acceptable steady-state condition. Therefore, it is often a stability concern.

Dynamic system performance models and tools are used for dynamic security analysis. For a stability-limited system, two problems are usually encountered in this analysis:

a. Small disturbance stability:

   It means that there is no state variable or system parameter which increases indefinitely when the power system is subjected to a small disturbance.

b. Large disturbance stability:

   Means that if the power system is subjected to a large disturbance, it can "survive" the ensuing transient and reach an acceptable steady-state operating condition.

1.2 Power System Security Assessment

Security assessment is concerned with the evaluation of available data to estimate the present security level of the system. An earlier working procedure for static security assessment is presented in [4-6], in which the security of the power system is tested with respect to a set of contingencies. The operating state of system is said to be secure if no disturbance in the next contingency set would bring about an emergency operating condition, and insecure otherwise. Therefore, security assessment starts with the selection of a set of next contingencies, and then the evaluation of the system's response to these contingencies. If a contingency caused any violation of system operating constraints, security control actions may be employed to steer the system away from insecurity.

In modern system operation, power systems in North America are planned and operated in cascading outages prevention mode in accordance with the reliability criteria set by their respective reliability councils. These criteria specify the type of disturbances which the power system should withstand. Therefore, the security assessment process should involve the analysis of many possible disturbance scenarios which involve outage of credible single or multiple contingencies as anticipated by the operations planning engineers. Therefore, it is very important to use faster and more efficient techniques in the assessment of system security. By doing this more contingency data and results can be processed and consequently, more accurate and less conservative operating decisions can be made.

A brief review of the state-of-the-art of security assessment is as follows:

1. Static security:

The methods and theories for contingency selection, external network modeling, contingency evaluation and security optimization etc. are available. The on-line application of static security assessment and control has been implemented in the last decade in modern energy control centers, called energy management systems (EMS) [7].

2. Dynamic security:

Currently the framework of dynamic security assessment used in North America is typically as follows:[8]

a. Off-line studies are performed for different initial operating conditions and system configurations, for a prescribed sequence of events or contingencies.

b. From these studies, "safe" operating levels are arrived at for a variety of system conditions.

c. These are often given in terms of limits for the critical system operating parameters.

d. The system is operated such that the critical parameters are within those limits.

1.3 The Need for a New Framework for Assessment of Dynamic Security

As previously mentioned, today's power systems are operated closer to their limits because of the heavier transmission loadings, increased economic interchanges, etc. This has brought dynamic security assessment into sharp focus lately, especially for those power systems which are stability-limited. There are two issues which need to be resolved for this analysis;

1. For a stability-limited system off-line studies must be conducted well in advance of the actual operating conditions. It has become very difficult to provide the operating limits for all possible situations that might be encountered. Therefore, dynamic security analysis must be conducted much closer to real time than is now possible.

2. The framework for power system dynamic security assessment should be able to analyze both the current status of security and its trend with changing system operating parameters, such as changes caused by disturbances, load variations, external changes(e.g., weather) etc.. Therefore it is important to study how this security status varies as time progresses.

It is generally recognized that the tools of stability analysis presently used in off-line studies, and the current framework for dynamic security assessment are not capable of meeting the needs outlined above. The interest, therefore, has focused on new tools of analysis, which have the potential of meeting the above needs; and a new framework for assessing power system dynamic security.

Regarding the tools of stability analysis, current research work is focused on the transient energy function (TEF) method that determines transient stability without solving the system dynamic equations [9]. This method has the potential for conducting stability analysis, to determine transient stability limits, faster than existing tools. It is also capable of providing information on the degree of stability and instability, and can give information on the sensitivity of the energy margin to changes in system parameters or operating conditions. This method has been developed to the point that tests on large-scale systems have been successfully conducted.

The new framework for dynamic security assessment is presented through the concept of system vulnerability, which is the focus of the research presented in this dissertation.

One thing that should be kept in mind is the increasing need for dynamic security analysis. This is because of the power system's increased size, interconnection between systems, more new control devices and heavier loading of the transmission network make the operators encounter more complex situations. Recent research, as well as recent IEEE forums identified the need for a new framework for security trend analysis. The operators need to know, not only that the system is secure at the present time, but also wish to know what may happen in the future, i.e., how the system security is affected by changes in system conditions and what kind of remedial action can be applied. These industry demands for security analysis are the motivation of our research work. The requirements for this new dynamic security assessment framework should include:

1. For a given system, dynamic security analysis should deal with both the level of the indicator(s) of dynamic security and their trend with changing system conditions.
2. This framework should be available for on-line security assessment.
3. It should be able to provide fast , accurate and reliable assessment.

The above are incorporated in the concept of system vulnerability, which is the focus of the research presented in this dissertation.

1.4 Concept of System Vulnerability

Power system vulnerability is a new concept used to assess the power system dynamic security. It measures the rate of deterioration in system security. This concept includes two indicators of system security: 1) the level of security, and 2) how that level is changing with changing system conditions or parameters. The concept was first suggested in the EPRI report No. EL-6796 [10]. At about the same time an IEEE forum [11] on power system security assessment came out with the conclusion that "Security Index should deal with changes in actual system parameters or conditions. It should help the system operator detect the "softness" in his system."

The following graphs are used for illustrating the idea of vulnerability. When the transient energy function is used as the tool for security analysis, the energy margin ΔV will indicate the level of security.

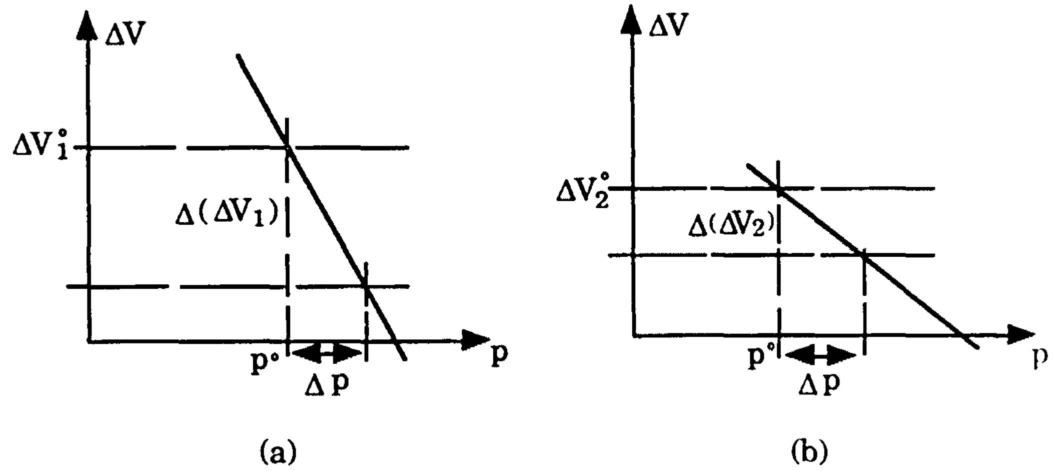

Figure 1.1 Energy Margin Sensitivities - System Vulnerability

From Figures 1.1 a and b it is clear that, for the same original operating condition the value of a critical parameter p is p^0; regime #1 appears to be more secure than regime #2 since $\Delta V_1^0 > \Delta V_2^0$. However, for the same amount of change in the parameter p, which is Δp, regime #1 is more vulnerable to the changes in p because of the high sensitivity of the energy margin. Figure 1.1 indicates that $\Delta(\Delta V_1)$ is much larger than $\Delta(\Delta V_2)$. Therefore the system vulnerability should include both the levels of ΔV and its sensitivity $\partial \Delta V / \partial p$.

1.5 Scope of This Research Work

The scope of this research work includes the following:

1. Use the transient energy function(TEF) method to develop a framework for system vulnerability. The new framework can indicate both the present security level using the energy margin ΔV, and the trend of security status due to the possible variation of a system operating parameter p using the energy margin sensitivity $\partial \Delta V / \partial p$. Therefore, this framework can identify the weakest point in the system, and how the changes of the parameter will cause the system to become vulnerable.
2. Establish thresholds for acceptable levels of ΔV and $\partial \Delta V / \partial p$; and relate these thresholds to stability limits of critical system parameters.
3. Develop a procedure for security and vulnerability assessment.
4. Apply artificial neural networks(ANNs) in TEF method for fast pattern recognition and classification of security status for on-line analysis.

TEF is a very powerful method for evaluating system security and it is easy to apply the sensitivity technique in this method. The detailed analysis of TEF and its sensitivity technique are introduced in Chapter 2. The framework and procedure for vulnerability assessment are introduced in Chapter 3, and applied to a test system in Chapter 4.

The reason of applying ANNs technique in dynamic security assessment is that it has been successfully used for classification of complex systems. We can predict that a TEF-ANN method which could improve on-line security and vulnerability assessment would be welcome in a power system control center. The basic theory and the application of ANNs are discussed in Chapter 5.

From dynamic security point of view there are several critical parameters which may be of concern such as plant generation, system configuration, transmission interface power flow, etc.. In this research work, we first consider the variation of plant generation to build our security and vulnerability framework. The same idea could be extended to cover the effect of other parameters on system dynamic security.

2. TOOLS FOR SECURITY AND VULNERABILITY ANALYSIS FOR A STABILITY-LIMITED POWER SYSTEM

There are basically two methods for power system transient stability analysis: the time domain simulation method and the transient energy function method. Therefore, a stability-limited power system will depend on one or both of these methods for security and vulnerability analysis. The following is a review of those two methods.

2.1 Time Domain Simulation Method

Time domain simulation is the conventional, and standard, method for transient stability analysis. Transient stability studies are intended to determine if the system will remain in synchronism following major disturbances such as transmission system faults, sudden large load changes, loss of generating units, or switching of a loaded line. In all stability studies, the objective is to determine whether or not the machines being perturbed return to acceptable steady-state operation. In this time domain simulation method, nonlinear differential and algebraic equations are used for modelling the power system, and these nonlinear equations are solved by iterative step-by-step procedures to evaluate the system stability for a variety of operating conditions, system configurations etc.. From these calculations, transient stability limits are computed [12].

The advantage of this method is that we can obtain the profile of different variables as the time progresses. Thus, we can obtain a lot of information from these variables. In addition, it has no modelling limitations.

The disadvantages of this method are: first the speed of calculation is slow because it needs step by step integration. Second, this method can only tell us whether the system is stable or not, but can not give qualitative information on the degree of stability. In order to compute the stability limit for a given contingency we must run the program several times. Thus, it is very time consuming. Another disadvantage of this method is that it can not give the information on sensitivity to system parameters.

On the basis of above analysis, this method is not considered suitable for on-line dynamic security analysis and the contingency ranking.

2.2 Transient Energy Function Method (TEF Method)

2.2.1 Introduction

Since 1980 research work on the TEF method has made considerable progress. This method is based on the Lyapunov's theory. It evaluates the power system stability problem from a system energy point of view. The principal idea of this method is based on the following concept. If the rate of change of the energy E(x) of an isolated physical system is negative for every possible state $\underline{x}$ except for a single equilibrium state $\underline{x}_e$, then the energy will continually decrease until it finally assumes its minimum value $E(\underline{x}_e)$. In 1892 Lyapunov showed that certain other functions could be used instead of energy to determine stability of the equilibrium point. The above concept was developed into a precise mathematical tool by Lyapunov, that is the Lyapunov's second method [13]. The basic concept of this method can be explained by the the following example.

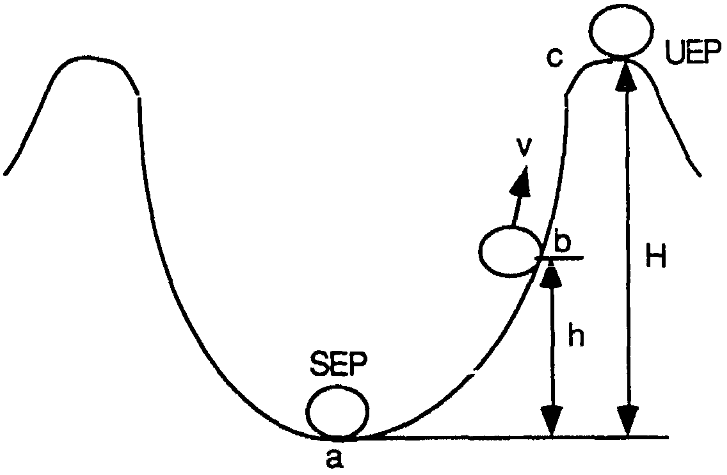

Figure 2.1 An Example of System Stability

In Figure 2.1 originally the ball is in the stable equilibrium position which is represented by the stable equilibrium point (SEP) a. The ball is disturbed by a sudden sharp push, forcing it to move. At some point the ball is in the position b with the velocity v. If the mass of the ball is m then the kinetic energy is

$$V_k = \frac{1}{2} mv^2$$

and the potential energy is

$$V_p = mgh$$

therefore the total energy is $V = V_k + V_p$, that is

$$V = \frac{1}{2} mv^2 + mgh$$

When the ball is in the position c with v = 0, the potential energy is mgH. We define this point c to be the unstable equilibrium point (UEP) and the corresponding potential energy is the critical energy. That is

$$V_{cr} = mgH$$

which is also the maximum potential energy for the ball. It is clear that if the the disturbance is large enough such that $V > V_{cr}$, the ball will go over the point c and can not go back to point a, which means the system is unstable. If $V < V_{cr}$ then the ball will go back toward the SEP and the system is stable. If there is damping (e.g., due to friction), the ball will eventually settle at the SEP.

2.2.2 The transient energy function [9]

There are two key points in applying the TEF method to a power system. The first one is finding the transient energy tending to separate one or more generators from the rest of the system. The second one is calculating a critical value of the transient energy against which transient stability assessment is made. This critical energy is the potential energy at the controlling UEP, for the particular disturbance under investigation. The UEP is a solution of the steady-state system equation with certain generators' angles generally greater than $\pi/2$, we call these generators advanced or critical machines. The potential energy at the UEP represents the power network's ability to "absorb" all the transient energy at the end of the disturbance. It is not an easy task to find the controlling UEP because for a n generator system there are 2^{n-1} -1 UEPs. Different UEPs have different advanced machines, thus different UEPs have different potential energies and only one of them can give the correct critical energy. This UEP is the so-called controlling UEP. Recent research work [9] has shown that the controlling UEP is in the direction of the disturbed system trajectory; its identity depends on both the disturbance itself and the post-disturbance network. Therefore the determination of the controlling UEP is among the key steps in stability assessment.

The mathematical statement of the controlling UEP is that: if x_e is the point where the unstable system trajectory crosses the stability boundary, then the controlling UEP is the UEP that x_e lies on its stable manifold. Determination of the controlling UEP involves: 1). identification of the severely disturbed generators, i.e., the critical generators, and 2). solving for the specific equilibrium point in which the angles of the critical generators are greater than 90°. Two procedures are used in determining the critical generators in the controlling UEP [9]: the MOD procedure, and the exit point method.

The MOD procedure is applied to a set of candidate UEPs in the direction of the system trajectory. The controlling UEP is that with the lowest normalized potential energy margin at the instance the disturbance is removed. In the exit point method two steps are involved: (1) the first potential energy maximum on the faulted system trajectory, called the exit point, is determined, and (2) from the exit point the associated gradient system is integrated until its minimum is found.

The controlling UEP is solved for at a point on the Potential Energy Boundary Surface (PEBS) near the desired UEP. In the MOD procedure, the UEP solution is started at the so-called ray point [9]. In the exit point method, the UEP solution is started at the minimum gradient point.

The advantages of the TEF method can be characterized by its ability to: (1) give qualitative measurement of the degree of system stability, (2) identify the critical generators which are severely affected by the disturbance, (3) be adapted for sensitivity analysis, and (4) achieve faster computation of stability limits. Thus it is a powerful method for fast security assessment and can be used for on-line security assessment or as a screening tool for off-line analysis.

2.2.3 The mathematical model

For the classical power system model the equations of motion of the synchronous generators, written with respect to an arbitrary synchronous frame, are given by

$$M_i\dot{\omega}_i = P_i - P_{ei}$$

$$\dot{\delta}_i = \omega_i \quad i=1,2,\ldots,n \qquad (2.1)$$

where n is the number of generators.

$$P_{ei} = \sum_{\substack{i=1 \\ j\neq i}}^{n} \left[C_{ij}(\sin(\delta_i - \delta_j) + D_{ij}(\cos(\delta_i - \delta_j)\right]$$

$$P_i = P_{mi} - E_i^2 G_{ii}$$

$$C_{ij} = E_i E_j B_{ij} \qquad D_{ij} = E_i E_j G_{ij}$$

and, for the i-th generator,

P_{mi} the mechanical input power

G_{ij} the real part of ij-th element of internal node reduced bus admittance matrix

B_{ij} the imaginary part of ij-th element of internal node reduced bus admittance matrix

E_i the machine's internal constant voltage source behind transient reactance

M_i the inertia constant of i-th machine

ω_i, δ_i generator speed and angle respectively.

Transformation of equation (2.1) into the center of inertia (COI) coordinates is done by defining the position of the center of inertia by the equations

$$\delta_0 = \frac{1}{M_T} \sum_{i=1}^{n} M_i \delta_i$$

$$\dot{\delta}_0 = \frac{1}{M_T} \sum_{i=1}^{n} M_i \dot{\delta}_i \qquad (2.2)$$

where

$$M_T = \sum_{i=1}^{n} M_i$$

The COI motion is defined by the equations

$$M_T\dot{\omega}_0 = \sum_{i=1}^{n} (P_i - P_{ei})$$

$$= \sum_{i=1}^{n} P_i - 2\sum_{i=1}^{n-1} \sum_{j=i+1}^{n} D_{ij}\cos\delta_{ij} \equiv P_{COI} \tag{2.3}$$

$$\dot{\delta}_0 = \omega_0 \qquad i=1,2,\ldots,n$$

We define the generators' angles and speeds relative to the COI by

$$\theta_i = \delta_i - \delta_0 \qquad \tilde{\omega}_i = \dot{\delta}_i - \dot{\delta}_0 \qquad i=1,2,\ldots,n$$

The system equations of motion become

$$M_i\dot{\tilde{\omega}}_i = P_i - P_{ei} - \frac{M_i}{M_T} P_{COI}$$

$$\dot{\theta}_i = \tilde{\omega}_i \quad i=1,2,\ldots,n \tag{2.4}$$

The transient energy function V is defined for the post-disturbance system. It can be derived from the n acceleration equations in the COI frame of reference as shown in equation (2.4). It is given as follows

$$V = \frac{1}{2}\sum_{i=1}^{n} M_i\tilde{\omega}_i^2 - \sum_{i=1}^{n} P_i(\theta_i - \theta_i^s) - \sum_{i=1}^{n-1}\sum_{j=i+1}^{n}\left[C_{ij}(\cos\theta_{ij} - \cos\theta_{ij}^s) - \int_{\theta_i^s+\theta_j^s}^{\theta_i+\theta_j} D_{ij}\cos\theta_{ij}\,d(\theta_i+\theta_j)\right] \tag{2.5}$$

The physical meaning of each term of the transient energy function can be interpreted as follows:

The first term is the total change in kinetic energy of all generators relative to the COI. Which is

$$\frac{1}{2}\sum_{i=1}^{n} M_i\tilde{\omega}_i^2$$

The remaining parts of the energy function are the total change of the potential energy, it consists of three parts:

- $$-\sum_{i=1}^{n} P_i(\theta_i - \theta_i^s)$$

is the change in position energy of all rotors relative to the COI.

- $$C_{ij}(\cos\theta_{ij} - \cos\theta_{ij}^s)$$

is the change in the stored magnetic energy of branch ij.

- $\int_{\theta_i^s+\theta_j^s}^{\theta_i+\theta_j} D_{ij}\cos\theta_{ij} d(\theta_i+\theta_j)$

is the change in the dissipation energy of branch ij. An approximation of this term is used to avoid calculating the actual system trajectory. It is defined as

$$I_{ij} \equiv \int_{\theta_i^s+\theta_j^s}^{\theta_i+\theta_j} D_{ij}\cos\theta_{ij} d(\theta_i+\theta_j)$$

where

$$I_{ij} = D_{ij}\frac{\theta_i+\theta_j-\theta_i^s-\theta_j^s}{\theta_{ij}-\theta_{ij}^s}(\sin\theta_{ij}-\sin\theta_{ij}^s)$$

Using the COI framework to derive the energy function the result will be more accurate. This is because it eliminates the energy components contributing to the motion of COI and not affecting the stability of the system.

It was also found that not all the transient kinetic energy contributes to the separation of the critical generators from the rest of the system. The corrected kinetic energy is that of two equivalent groups of generators: the critical group and the rest of the generators. It is given by

$$V_{KE\,|corr} = \frac{1}{2} M_{eq}(\tilde{\omega}_{eq})^2 \qquad (2.6)$$

where

$$M_{eq} = M_{cr}{*}M_{sys}/(M_{cr} + M_{sys})$$

$$\tilde{\omega}_{eq} = \tilde{\omega}_{cr} - \tilde{\omega}_{sys}$$

cr ; index set of critical generators

sys ; index set of non-critical generators

Therefore the first term in (2.5) should be replaced by (2.6).

2.2.4 Transient stability assessment

Transient stability assessment using the TEF method is made by computing the energy margin ΔV given by

$$\Delta V = V_{cr} - V_{cl}$$

where V_{cl} is the value of V at fault clearing, and V_{cr} is the potential energy at the controlling unstable equilibrium point (UEP). Thus, the energy margin is given as follows:

$$\Delta V = -\frac{1}{2}M_{eq}(\tilde{\omega}_{eq}^{d})^2 - \sum_{i=1}^{n} P_i(\theta_i^u - \theta_i^{cl}) - \sum_{i=1}^{n-1}\sum_{j=i+1}^{n}\left[C_{ij}(\cos\theta_{ij}^u - \cos\theta_{ij}^{cl}) - I_{ij}\Big|_{\theta^{cl}}^{\theta^u}\right] \quad (2.7)$$

where

$$I_{ij}\Big|_{\theta^{cl}}^{\theta^{u}} = D_{ij}\frac{\theta_i^u+\theta_j^u-\theta_i^{cl}-\theta_j^d}{\theta_{ij}^u-\theta_{ij}^d}(\sin\theta_{ij}^u-\sin\theta_{ij}^{cl})$$

θ_i^{cl} the clearing angle of i-th machine rotor in COI reference frame

θ_i^u the controlling UEP angle of i-th machine rotor in COI reference frame

Thus the transient stability (or instability) is determined by whether ΔV is great or less than zero. $\Delta V > 0$ means the system is stable for the given contingency while $\Delta V \leq 0$ means system is unstable.

2.3 Sensitivity Analysis of the Transient Energy Function Method

There have been various research efforts on the application of sensitivity analysis based on the TEF method. The researchers who made significant contribution in this area are Sauer, El-kady , Fouad, Vittal , and Pai etc. [14], [15], [16],[17], [18], [19]. Taking the changing parameter to be the generation and using the first order sensitivity technique, the variation of energy margin caused from generation changes can be approximated as

$$\Delta(\Delta V) \cong \sum_{k=1}^{N} \frac{\partial \Delta V}{\partial P_{mk}} \Delta P_{mk} \qquad (2.8)$$

The energy margin is a function of the clearing angles, clearing speeds, UEP angles, and the voltages behind transient reactance. Thus, the sensitivity of the energy margin with respect to the generation shift at the k-th machine is given by the partial derivative of ΔV with respect to P_{mk}. Differentiating equation (2.7) by using the chain rule of differentiation, we get

$$\frac{\partial \Delta V}{\partial P_{mk}} = -M_{eq}\tilde{\omega}_{eq}^{d}\dot{u}_{eq,k}^{d} - (\theta_k^{u}-\theta_k^{cl}) - \sum_{i=1}^{n} P_i(u_{ik}^{u}-u_{ik}^{d})$$

$$+\sum_{i=1}^{n-1}\sum_{j=i+1}^{n} C_{ij}\left[\sin\theta_{ij}^{u}(u_{ik}^{u}-u_{jk}^{u}) - \sin\theta_{ij}^{cl}(u_{ik}^{d}-u_{jk}^{d})\right]$$

$$+\sum_{i=1}^{n-1}\sum_{j=i+1}^{n} D_{ij}(\sin\theta_{ij}^{u} - \sin\theta_{ij}^{cl})[\frac{(u_{ik}^{u}+u_{jk}^{u}-u_{ik}^{d}-u_{jk}^{d})}{\theta_{ij}^{u}-\theta_{ij}^{d}}$$

$$-\frac{(u_{ik}^{u}-u_{jk}^{u}-u_{ik}^{d}+u_{jk}^{d})(\theta_i^{u}+\theta_j^{u}-\theta_i^{cl}-\theta_j^{cl})}{(\theta_{ij}^{u}-\theta_{ij}^{cl})^2}]$$

$$+2\sum_{i=1}^{n}\frac{\partial E_i}{\partial P_{mk}} E_i\, G_{ii}(\theta_{ij}^{u}-\theta_{ij}^{cl})$$

$$+\sum_{i=1}^{n-1}\sum_{j=i+1}^{n}\frac{(\theta_i^{u}+\theta_j^{u}-\theta_i^{cl}-\theta_j^{cl})}{\theta_{ij}^{u}-\theta_{ij}^{d}} D_{ij}[\cos\theta_{ij}^{u}(u_{ik}^{u}-u_{jk}^{u}) - \cos\theta_{ij}^{cl}(u_{ik}^{d}-u_{jk}^{d})]$$

$$-\sum_{i=}^{n-1}\sum_{j=i+1}^{n}(\frac{\partial E_i}{\partial P_{mk}}E_j + \frac{\partial E_j}{\partial P_{mk}}E_i)B_{ij}(\cos\theta_{ij}^{u} - \cos\theta_{ij}^{cl})$$

$$+\sum_{i=}^{n-1}\sum_{j=i+1}^{n}[(\frac{\partial E_i}{\partial P_{mk}}E_j + \frac{\partial E_j}{\partial P_{mk}}E_i)G_{ij}\frac{(\theta_i^{u}+\theta_j^{u}-\theta_i^{cl}-\theta_j^{cl})}{\theta_{ij}^{u}-\theta_{ij}^{d}}(\sin\theta_{ij}^{u} - \text{sins}\theta_{ij}^{cl})] \tag{2.9}$$

where

$$\dot{u}^{d}_{eq,k} = \dot{u}^{d}_{cr,k} - \dot{u}^{d}_{sys,k}$$

$$\dot{u}^{d}_{cr,k} = \frac{1}{M_{cr}} \sum_{i \in cr} M_i \dot{u}^{d}_{ik}$$

$$\dot{u}^{d}_{sys,k} = - \frac{1}{M_T - M_{cr}} \sum_{i \in cr} M_i \dot{u}^{d}_{ik}$$

the variables introduced in the above equations are defined as follows

Clearing angle sensitivity coefficient

$$u^{d}_{ik} = \frac{\partial \theta^{d}_{i}}{\partial P_{mk}}$$

UEP angle sensitivity coefficient

$$u^{u}_{ik} = \frac{\partial \theta^{u}_{i}}{\partial P_{mk}}$$

Clearing speed sensitivity coefficient

$$\dot{u}^{d}_{ik} = \frac{d}{dt} \frac{\partial \theta^{d}_{i}}{\partial P_{mk}}$$

2.4 Using TEF Method for Security and Vulnerability Analysis

Because of the continued developments, the TEF method is now capable of providing accurate and reliable stability assessment. Therefore, in a stability-limited power system we use TEF method as the tool for security and vulnerability analysis. When the TEF method is used for this study the energy margin ΔV will be the indicator of the security status. Therefore $\Delta V > 0$ means that the system is stable for the given contingency while $\Delta V \leq 0$ means that the system is unstable.

When we are concerned with the system vulnerability the change of the security status with respect to a change in a system parameter p is also of interest. The tool for security trend analysis is the sensitivity of energy margin $\partial \Delta V/\partial p$. By using the sensitivity technique, we can determine which parameter has the significant influence on system security. It also provides a fast way to know the new system security status. The purpose of our research work is to incorporate the information of energy margin and the sensitivity of energy margin with changing system parameter to build a framework for system vulnerability assessment. The basic ideas and the procedure of this framework are discussed in Chapter 3.

3. FRAMEWORK AND PROCEDURE FOR SECURITY & VULNERABILITY ASSESSMENT

3.1 Basic Idea of this Framework

The proposed framework for assessing the system vulnerability includes two basic ideas:

1. The first idea in this framework is combining the energy margin ΔV and the sensitivity $\partial\Delta V/\partial p$ to evaluate the vulnerability status. A low value of ΔV with a high value of $\partial\Delta V/\partial p$ means that the system is vulnerable for changing the parameter p. Therefore, if we can divide ΔV and $\partial\Delta V/\partial p$ into high and low level classes, that is

$$\Delta V = \left\{ \begin{array}{l} \text{High level} \\ \text{Low level} \end{array} \right. \quad \text{, and} \qquad \frac{\partial \Delta V}{\partial p} = \left\{ \begin{array}{l} \text{High level} \\ \text{Low level} \end{array} \right.$$

then the system vulnerability can be determined from these levels. For example, if security assessment results in the following combination of ΔV and $\partial\Delta V/\partial p$:

ΔV= Low level

and

$$\frac{\partial \Delta V}{\partial p} = \text{High level}$$

then the system is vulnerable for this contingency. Therefore, the choice of the levels of the thresholds determines the system vulnerability. Within this framework, we must address the question of how to determine the thresholds which separate the high and low levels for ΔV and $\partial \Delta V/\partial p$.

2. The second idea is to correlate the levels of ΔV and $\partial \Delta V/\partial p$ with the stability limits of the critical system parameters. Since all the system parameters should be operated within their stability limits, the correlation of the levels of ΔV and $\partial \Delta V/\partial p$ with those limits is very important for evaluating the trend of security status.

3.2 Procedure of Security and Vulnerability Assessment

The procedure is illustrated for changes in generation P, and the following assumptions are made:

- Only three phase fault contingencies are considered.
- The mode of instability, i.e., the identity of the most disturbed generators, does not change when there is a generation shift.
- The total system generation is constant.
- The sensitivity of energy margin with respect to generation change are available[18].

We have emphasized that the key point in this framework is to find the thresholds which separate the high and lower levels for ΔV and $\partial \Delta V/\partial p$ and those thresholds should be connected with the stability limits of those critical system operating parameters. Therefore the procedure of security and vulnerability assessment will consist of two steps: the first one is finding the security domain of each system parameter, and the second one is determining the thresholds of ΔV and $\partial \Delta V/\partial p$ based on the security domains of those parameters.

In order to explain this procedure clearly we first assume that there are m contingencies but only the change in generation P is of concern, then the energy margin values corresponding to the original operating point P^o are:

$$\Delta V = \{\Delta V_1^o, \Delta V_2^o, \ldots, \Delta V_m^o)$$

We also assume that the sensitivity of energy margin has the linearized characteristics. Therefore we can obtain the following graph (Figure 3.1).

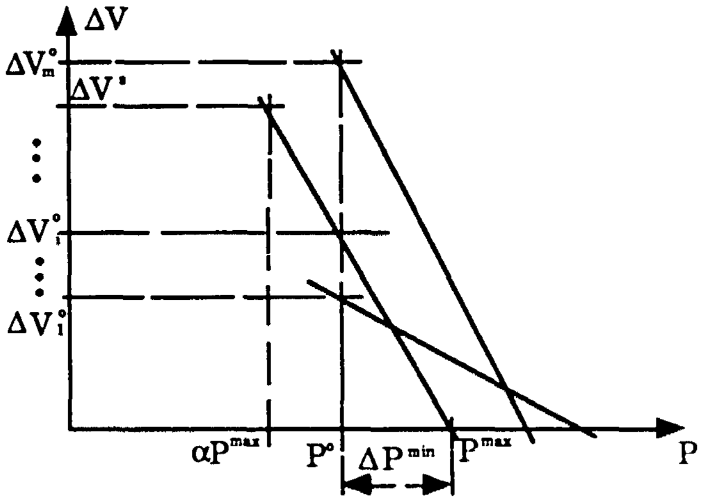

Figure 3.1 Energy Margin vs. Plant Generation

Figure 3.1 shows that at the initial operating point P^o the energy margin of those m fault locations are $\Delta V_1^o, \Delta V_2^o, \ldots, \Delta V_m^o$. It also shows that they have different sensitivity values, that is their slopes are different. If we increase P, all the energy margin values will decrease. The rate of change of the energy margin depends on their sensitivity values. Therefore by using the equation

$$\frac{\partial \Delta V_i}{\partial P}\Delta P+\Delta V_i^o=0$$

we can find the smallest increment of P, which is ΔP^{min}, that will cause a certain energy margin ΔV_i to first become zero (it should be kept in mind that the largest $\partial \Delta V_i/\partial P$ will not necessarily correspond to the ΔP^{min}). The stability limit of P will then be given by

$$P^{max}=P^o+\Delta P^{min}$$

Since in practical situations P can not be operated at point P^{max}, the security domain of P should be $P < \alpha P^{max}$, where α depends on the prevailing utility's policy, typically $0 < \alpha < 1$. Now, we can check whether P^o is greater or less than αP^{max}. If P^o is greater than αP^{max}, this means that the system is vulnerable to the change in this parameter P. Therefore, the energy margin value ΔV^s, which would be obtained if the initial power P^o is equal to αP^{max} (as shown in Fig. 3.1). The sensitivity value $\partial \Delta V_i/\partial P$ corresponding to the ΔV^s will be used to determine the thresholds of ΔV and $\partial \Delta V/\partial P$.

On the basis of the above analysis, if there are m contingencies and if the changes in the powers of n generators are of concern, then we have the following energy margin and sensitivity values:

$$\Delta V = (\Delta V_1^o, \Delta V_2^o, \ldots, \Delta V_m^o) \tag{3.1}$$

$$\left[\frac{\partial \Delta V}{\partial P}\right] = \begin{bmatrix} \frac{\partial \Delta V_1}{\partial P_1} & \frac{\partial \Delta V_2}{\partial P_1} & \cdots & \frac{\partial \Delta V_m}{\partial P_1} \\ & \vdots & & \\ \frac{\partial \Delta V_1}{\partial P_n} & \frac{\partial \Delta V_2}{\partial P_n} & \cdots & \frac{\partial \Delta V_m}{\partial P_n} \end{bmatrix} \tag{3.2}$$

and the operating point is

$$P^o = [P_1^o, P_2^o, \ldots P_n^o] \tag{3.3}$$

The procedure of the security and vulnerability assessment involves the following steps:

1. Finding the security domain for each generation change,
2. determining the thresholds of the energy margin and its sensitivity, and
3. for the selected set of contingencies classifying ΔV and $\partial \Delta V / \partial P$, and evaluating the system vulnerability situation.

Detailed procedure is explained in the following subsections.

3.2.1. Security domain for each parameter

Each row in the sensitivity matrix (3.2) corresponding to the sensitivity of the energy margins ΔV_i (i=1,...,m) with respect to the change in the power of the jth generator. Therefore, the procedure of defining the security domain is as follows:

a. For each row of (3.2), and using the equation

$$\frac{\partial \Delta V_i}{\partial P_j}\Delta P_j+\Delta V_i^o=0 \qquad i=1,2,...m \qquad (3.4)$$

ΔP_j^{min}, which is the smallest generation change ΔP_j which causes the new energy margin to become to zero, is calculated.

b. P_j^m, which is the stability limit of Pj, is calculated using

$$P_j^m=P_j^o+\Delta P_j^{min} \quad j=1,2,...n \qquad (3.5)$$

c. The security domain of Pj is defined as αP_j^m. Here α is chosen according to the established utility policy. Then αP_j^m is used to check the security of the original operating point in (3.3). If

$$P_j^o \geq \alpha P_j^m \quad , j=1,2,...n$$

then the corresponding jth generator is operating in the vulnerable domain.

3.2.2. Thresholds of energy margin and its sensitivity

The thresholds of ΔV and $\partial\Delta V/\partial P$ can now be defined as follows:

a. We check each P_j^o and pick up those P_j^o for which $P_j^o \geq \alpha P_j^m$. Assume there are k such values of P_j^o. Corresponding to each value of P_j^o there is a sensitivity value, which corresponds to $P_j^m = P_j^o + \Delta P_j^{min}$. That is:

$$\frac{\partial \Delta V_i}{\partial P_j} \Delta P_j^{min} + \Delta V_i^o = 0 \qquad (3.6)$$

b. For those k values of P_j^o with $P_j^o \geq \alpha P_j^m$, by using the sensitivity value defined in step a, we can calculate the energy margin ΔV_i^s which would be obtained if the initial power P_j^o is equal to αP_j^m. That is:

$$\frac{\partial \Delta V_i}{\partial P_j} (1-\alpha) P_j^m + \Delta V_i^s = 0 \qquad j=1,2,\ldots,n. \quad (3.7)$$

c. By repeating steps a and b for j=1,...,n, we can obtain those k values of $\partial\Delta V/\partial P$ and ΔV_i^s which correspond to those k generators with $P_j^o \geq \alpha P_j^m$, $k \leq n$.

d. The maximum of those k values of ΔV_i^s is taken as the ΔV threshold. That is:

$$S_{\Delta V} = \max\{\Delta V_{i1}^s, \Delta V_{i2}^s, \ldots, \Delta V_{ik}^s\} \qquad (3.8)$$

All values of ΔV lower than $S_{\Delta V}$ are considered low level.

The smallest magnitude of those k values of $\partial\Delta V/\partial P$ is taken as the sensitivity threshold. That is:

$$S_{\Delta V/\Delta P} = \min\left\{\left|\frac{\partial\Delta V_{i1}}{\partial P_{j1}}\right|,\left|\frac{\partial\Delta V_{i2}}{\partial P_{j2}}\right|,\ldots,\left|\frac{\partial\Delta V_{ik}}{\partial P_{jk}}\right|\right\} \tag{3.9}$$

All values of $\partial\Delta V/\partial P$ higher than $S_{\Delta V/\Delta P}$ are considered high level.

It is clear that by choosing the thresholds in this way it includes all the $P_j^o \geq \alpha P_j^m$ cases.

It should be mentioned here that for the threshold of energy margin sensitivity we need to consider the negative and positive sign sensitivities separately since they will make the security status move toward opposite directions. We will also find out in the next chapter that the negative sign sensitivity are mainly of concern from the system vulnerability point of view.

3.2.3 System vulnerability assessment

The thresholds obtained form (3.8) and (3.9) are used to divide the ΔV and $\partial\Delta V/\partial P$ values in equations (3.1) and (3.2) into high and low level categories. Then if for any contingency ΔV belongs to the low level class and the sensitivity values of some generators belong to the high level class, then we know that the system is vulnerable for this contingency if there are the generation shift at the corresponding generators.

The above analysis indicates that the system vulnerability is determined by incorporating the information of ΔV and $\partial\Delta V/\partial P$, and the levels of ΔV and

$\partial \Delta V/\partial P$ are correlated with the stability limits of the generation. The physical meaning is that a low ΔV value means for the corresponding contingency the system is close to its stability limit. If at the same time, the values of $\partial \Delta V/\partial P$ of some generators belong to the high level, the ΔV value will be greatly reduced if there are generation change at these machines. This means that the system will go toward its stability limit very quickly and will tend to become unstable. Therefore, the above procedure is a proper evaluation of both the system security status at the present operating condition and the trend of this security status by changing the system parameter.

In Chapter 4 we apply this framework to a test power system and evaluate its security status for different operating conditions.

4. APPLICATION TO A TEST SYSTEM

4.1 Test System Description

The test system used for this study is the IEEE 50-generator test system. This system is characterized by large blocks of generation delivered from power stations nos. A and B through 500 kv and 230 kv transmission networks [20]. Figure 4.1 is a one line diagram of the network in the area of power stations nos. A and B.

For this system its security and vulnerability status were evaluated for two system operating conditions: a base unstressed case and a stressed case.

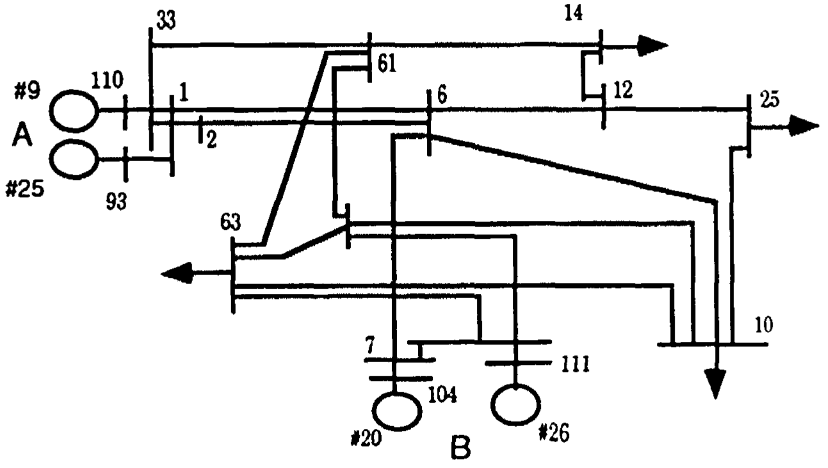

Figure 4.1 IEEE 50 Generator System - Power Stations A & B Area

The base case power flow is characterized by setting the generation at generators 9 and 25 to be 700 MW each, while the stressed case power flow is characterized by setting the generation at generators 9 and 25 to be 1300 MW each. The generation at station B is held at 4000 MW for both cases. In the following sections all the faults are three-phase faults and the fault clearing time is fixed at 0.108 second.

Nine fault buses were chosen to evaluate the system security status; they are buses numbered 7,6,12,1,2,10,25,61, and 63. The ΔV values corresponding to these nine faults and the $\partial \Delta V / \partial P$ values of the advanced generators are calculated for both base-case and stressed-case operating conditions. The detailed results of assessing the system vulnerability are shown in the following sections.

4.2 Base Case Security and Vulnerability Assessment

For the base case operating condition, the ΔV values corresponding to these nine contingencies and the $\partial \Delta V / \partial P$ values of 28 advanced generators are calculated using the EPRI program Direct version 3.0. The results are shown in Table 4.1.

Table 4.1 Energy Margin Values (base case)

Bus No.	7	6	12	1	2	10	25	61	63
ΔV	0.4599	2.2758	27.648	31.722	31.838	31.176	30.388	35.702	36.189

From Table 4.1 we know that the energy margin values are quite small for faults at buses 7 and 6, while the energy margin values for the rest of contingencies are quite large. This means the security status for faults at buses 7 and 6 are close to the stability limits.

For the disturbances investigated up to 28 generators may be considered severely disturbed. The sensitivity matrix for the 28 generators of interest are shown in Table 4.2. By analyzing the data in this table two things are observed. The first is that the negative sensitivity values are mainly of concern from the system vulnerability point of view because most of the elements have negative sign and many of them have significant magnitudes. This means that if we increase the generation at the corresponding machines the ΔV value will decrease rapidly. The second observation is that for faults at buses 7 and 6 only generators 20 and 26 have large negative sensitivities.

4.2.1 Security domain for the critical generators

Based on the procedure proposed in Chapter 3, the first step of vulnerability assessment is to define the security domain of the generation for each critical machine. Using the above data in Tables 4.1 and 4.2, the result of finding the security domain is shown in Table 4.3.

In Table 4.3 the first column is the critical machine numbers, and the second column is the initial generation P^o. The third column is the stability limits P^{max} of those critical generators as calculated by equations (3.4) and (3.5). The fourth column is the values of αP^{max} which are the security domain of those advanced machines. The fifth and sixth columns are the sensitivity values and ΔV^s values corresponding to equation (3.7); they will be used for

Table 4.2 Energy Margin Sensitivity Values (Base Case)

Gen\Bus	7	6	12	1	2	10	25	61	63
2	0.3142	0.2847	-1.7863	-1.7894	-1.7894	-1.7664	-1.7718	-1.8048	-1.8224
3	0.2936	0.2512	-1.3171	-1.2711	-1.2718	-1.2790	-1.2830	-1.2592	-1.2645
4	0.2942	0.2572	-1.3080	-1.2714	-1.2713	-1.2751	-1.2786	-1.2618	-1.2677
5	0.3400	0.3300	-1.7911	-1.7346	-1.7355	-1.7782	-1.8043	-1.7599	-1.7734
6	0.5050	0.4244	-2.5383	-2.5253	-2.5243	-2.4451	-2.4666	-2.4306	-2.4322
7	0.2031	0.1943	-0.8548	-0.8458	-0.8460	-0.8535	-0.8483	-0.8668	-0.8776
8	0.3692	0.2955	-2.0417	-1.9291	-1.9292	-1.9843	-2.0510	-1.9159	-1.9254
9	0.4064	0.4173	-1.8777	-1.9811	-1.9800	-1.8447	-1.8575	-1.9098	-1.9263
10	0.1577	0.1541	-0.6351	-0.6280	-0.6283	-0.6408	-0.6345	-0.6548	-0.6650
11	0.1183	0.1145	-0.3728	-0.3571	-0.3575	-0.3831	-0.3758	-0.3878	-0.3942
12	0.4406	0.3744	-2.0347	-1.9596	-1.9755	-1.9789	-2.0323	-1.9269	-1.9373
13	0.3209	0.2904	-1.8700	-1.8785	-1.8785	-1.8455	-1.8541	-1.8914	-1.9084
14	0.4541	0.3506	-2.6620	-2.6360	-2.6353	-2.5588	-2.5817	-2.5332	-2.5310
15	0.4032	0.3974	-2.0174	-2.1393	-2.1365	-1.9788	-1.9902	-2.0474	-2.0596
16	0.4445	0.3830	-2.1838	-2.1795	-2.1795	-2.1154	-2.1343	-2.1151	-2.1204
17	0.4056	0.2883	-2.1037	-2.0164	-2.0159	-2.0202	-2.0531	-1.9573	-1.9664
19	0.4450	0.4158	-2.0227	-2.0538	-2.0542	-1.9762	-1.9930	-2.0050	-2.0145
20	-3.0858	-2.9571	-2.2894	-2.2860	-2.2851	-2.2250	-2.2235	-2.2099	-2.2229
21	0.4673	0.4089	-2.2738	-2.2584	-2.2583	-2.2085	-2.2606	-2.1942	-2.2077
22	0.4535	0.3961	-2.2721	-2.2595	-2.2596	-2.2084	-2.2594	-2.1970	-2.2104
23	0.2556	0.2582	-1.6982	-1.6427	-1.6434	-1.7174	-1.7179	-1.7088	-1.7236
24	0.3106	0.3291	-1.4464	-1.4377	-1.4390	-1.4581	-1.4559	-1.4800	-1.4944
25	0.4063	0.4147	-1.8665	-1.9713	-1.9703	-1.8336	-1.8457	-1.9055	-1.9214
26	-1.653	-1.6420	-2.0318	-2.0313	-2.0307	-1.9741	-1.9781	-1.9982	-2.0134
27	0.4074	0.2969	-2.0745	-1.9953	-1.9953	-1.9945	-2.0272	-1.9398	-1.9497
33	0.2042	0.2045	-1.5651	-1.4932	-1.4941	-1.6101	-1.5931	-1.5953	-1.6103
34	0.3021	0.2871	-1.5492	-1.5392	-1.5393	-1.5487	-1.5487	-1.5738	-1.5867
35	0.3285	0.3044	-1.6569	-1.6594	-1.6595	-1.6417	-1.6490	-1.6789	-1.6950
49	0.0128	0.0133	0.1298	0.1343	0.1344	0.1242	0.1267	0.1280	0.1292

Table 4.3 Stability Limits and Security Domains of Each Parameter (Base Case)

Gen.No.	P^o	P^m	$\alpha*P^m$	$\partial\Delta V/\partial P$	ΔV^s	Bus No.
2	14.86000	30.33874	28.82180	-1.78636	2.70980	12
3	2.50000	23.49243	22.31781	-1.31717	1.54718	12
4	0.47000	21.60896	20.52851	-1.30804	1.41327	12
5	0.70000	16.13778	15.33089	-1.79110	1.44522	12
6	6.73000	17.62318	16.74202	-2.53834	2.23668	12
7	0.22000	32.56443	30.93620	-0.85488	1.39193	12
8	0.64000	14.18273	13.47359	-2.04173	1.44787	12
9	7.00000	21.72570	20.63942	-1.87771	2.03973	12
10	3.00000	46.53397	44.20727	-0.63515	1.47780	12
11	1.31000	75.46217	71.68906	-0.37289	1.40695	12
12	0.60000	14.18926	13.47979	-2.03474	1.44357	12
13	1.40000	16.18642	15.37710	-1.87000	1.51343	12
14	4.26000	14.64700	13.91465	-2.66204	1.94954	12
15	2.00000	15.70585	14.92056	-2.01743	1.58427	12
16	1.70000	14.36140	13.64333	-2.18385	1.56816	12
17	3.10000	16.24367	15.43149	-2.10372	1.70861	12
19	1.35000	15.01974	14.26875	-2.02276	1.51907	12
20	20.00000	20.14886	19.14141	-3.08580	3.10877	7
21	16.20000	28.36047	26.94245	-2.27381	3.22432	12
22	10.80000	22.96946	21.82099	-2.27213	2.60948	12
23	8.00000	24.28153	23.06746	-1.69828	2.06184	12
24	0.52000	19.63618	18.65437	-1.44645	1.42014	12
25	7.00000	21.81343	20.72276	-1.86659	2.03584	12
26	20.00000	20.27785	19.26396	-1.65320	1.67617	7
27	3.00000	16.32822	15.51181	-2.07459	1.69372	12
33	29.97000	47.63654	45.25471	-1.56514	3.72789	12
34	10.09000	27.93773	26.54085	-1.54925	2.16413	12
35	30.05000	46.73724	44.40038	-1.65699	3.87216	12

* $\alpha = 0.95$

calculating the thresholds of ΔV and $\partial \Delta V/\partial P$. The last column is the corresponding fault locations.

By carefully analyzing the data of the initial generation P^o, the stability limits P^{max} and the security domain αP^{max} in Table 4.3, it is found that only generators 20 and 26 are operating in the vulnerable domain, i.e.,

$$P_{20}^{o} \geq \alpha P_{20}^{max} \quad \text{and} \quad P_{26}^{o} \geq \alpha P_{26}^{max}$$

For the rest of generators their initial values of generation are much smaller than their stability limits.

4.2.2 Thresholds for ΔV and $\partial \Delta V/\partial P$

Our second step is to calculate the thresholds of ΔV and $\partial \Delta V/\partial P$ using equations (3.8) and (3.9). In the last subsection we know that only generators 20 and 26 are operating in the vulerability domain. Thus in Table 4.3 we check the ΔV^s values in the sixth column and the sensitivity values in the fifth column, which correspond to generators 20 and 26. It is found that the largest ΔV^s value is 3.1088 and the sensitivity value with smallest magnitude is -1.65320. Therefore the results are as follows:

margin threshold	sensitivity threshold
3.10880	-1.65320

4.2.3 Classification of levels of ΔV and $\partial \Delta V/\partial P$

The third step is using these two thresholds to classify the ΔV and $\partial \Delta V/\partial P$ into high and low level two categories. As shown in Tables 4.4 and 4.5.

Table 4.4 Energy Margin Status for Different Fault Locations (Base Case)

1=high 0=low

Fault Bus No.	7	6	12	1	2	10	25	61	63
ΔV status	0	0	1	1	1	1	1	1	1

Table 4.5 Sensitivity Status of Each Generator Corresponding to Different Fault Locations (Base Case)

1=high 0=low

gen.\bus	7	6	12	1	2	10	25	61	63
2	0	0	1	1	1	1	1	1	1
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	1	1	1	1	1	1	1
6	0	0	1	1	1	1	1	1	1
7	0	0	0	0	0	0	0	0	0
8	0	0	1	1	1	1	1	1	1
9	0	0	1	1	1	1	1	1	1
10	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0
12	0	0	1	1	1	1	1	1	1
13	0	0	1	1	1	1	1	1	1
14	0	0	1	1	1	1	1	1	1
15	0	0	1	1	1	1	1	1	1
16	0	0	1	1	1	1	1	1	1
17	0	0	1	1	1	1	1	1	1
19	0	0	1	1	1	1	1	1	1
20	1	1	1	1	1	1	1	1	1
21	0	0	1	1	1	1	1	1	1
22	0	0	1	1	1	1	1	1	1

Table 4.5 (continued)

23	0	0	1	0	0	1	1	1	1
24	0	0	0	0	0	0	0	0	0
25	0	0	1	1	1	1	1	1	1
26	1	0	1	1	1	1	1	1	1
27	0	0	1	1	1	1	1	1	1
33	0	0	0	0	0	0	0	0	0
34	0	0	0	0	0	0	0	0	0
35	0	0	1	1	1	0	0	1	1
49	0	0	0	0	0	0	0	0	0

4.2.4 System vulnerability status

The last step is to evaluate the system vulnerability status based on the ΔV and $\partial \Delta V/\partial P$ levels. Tables 4.4 and 4.5 show that the ΔV values for faults at buses 7 and 6 belong to lower level and the corresponding $\partial \Delta V/\partial P$ values of generators 20 and 26 belong to high level. Therefore, the final result of the system vulnerability assessment is:

```
system is vulnerable for the fault at following buses:
bus No.=  7
     generation increased at Gen. No.:  20
     generation increased at Gen. No.:  26
bus No.=  6
     generation increased at Gen. No.:  20
```

Thus, the system is vulnerable for faults at bus 7, and 6 if the generation is increased at either generator 20 or 26.

4.3 Stressed Case Security and Vulnerability Assessment

For the stressed case operating condition the ΔV values corresponding to those nine contingencies and the $\partial \Delta V / \partial P$ values of 29 advanced generators are calculated in Table 4.6.

It is shown in Table 4.6 that for a fault at Bus 6 the energy margin is negative, which means that the system is unstable for this contingency; therefore we only need to evaluate the system vulnerability status for the rest of contingencies.

Table 4.6 Energy Margin Values (Stressed Case)

Bus No.	7	6	12	1	2	10	25	61	63
ΔV	0.7088	-5.4769	5.166	6.340	6.569	8.921	8.123	13.481	13.822

The sensitivity values corresponding to these nine contingencies are shown in Table 4.7.

The procedure of system vulnerability assessment is similar to the base case operating condition. We first calculate the stability limit and define the security domain of the generation for each critical machine. Using the data in Tables 4.6 and 4.7 the result of finding the security domain is shown in Table 4.8.

Table 4.7 Energy Margin Sensitivity Values (Stressed Case)

Gen\Bus	7	6	12	1	2	10	25	61	63
1	-0.1451	-0.1496	-0.4924	-0.3842	-0.3861	-0.5445	-0.5306	-0.5329	-0.5402
2	-0.6404	-0.6788	-1.3310	-1.0314	-1.0408	-1.3754	-1.3662	-1.4127	-1.4441
3	-0.5519	-0.6266	-1.3483	-1.1336	-1.1371	-1.4026	-1.3842	-1.3483	-1.3604
4	-0.5489	-0.6162	-1.3389	-1.1307	-1.1344	-1.3978	-1.3786	-1.3484	-1.3611
5	-0.4337	-0.4536	-1.1284	-0.8594	-0.8675	-1.1815	-1.1590	-1.1794	-1.2014
6	-1.3853	-1.5054	-2.7978	-2.5206	-2.5292	-2.8589	-2.8287	-2.7541	-2.7761
7	-0.2986	-0.3181	-0.8474	-0.6982	-0.7008	-0.9176	-0.8971	-0.8997	-0.9103
8	-0.6802	-0.7759	-1.5945	-1.2709	-1.2793	-1.6299	-1.6369	-1.5755	-1.5987
9	-1.3774	-1.4386	-2.6593	-2.7363	-2.7337	-2.7412	-2.7003	-2.7022	-2.7310
10	-0.1914	-0.1933	-0.6032	-0.4859	-0.4884	-0.6666	-0.6492	-0.6578	-0.6669
11	-0.0608	-0.0638	-0.2515	-0.1855	-0.1944	-0.3000	-0.2859	-0.3032	-0.3141
12	-0.8964	-1.0111	-1.9361	-1.6410	-1.6495	-1.9751	-1.9777	-1.9046	-1.9291
13	-0.7161	-0.7556	-1.4422	-1.1331	-1.1429	-1.4888	-1.4775	-1.5251	-1.5558
14	-1.4937	-1.6310	-2.9437	-2.6527	-2.6607	-2.9964	-2.9643	-2.8813	-2.8990
15	-1.3702	-1.4296	-2.6449	-2.7143	-2.7121	-2.7265	-2.6863	-2.6940	-2.7190
16	-1.1768	-1.2831	-2.3931	-2.1469	-2.1547	-2.4554	-2.4301	-2.3821	-2.4039
17	-1.0408	-1.2045	-2.1685	-1.8283	-1.8370	-2.1911	-2.1873	-2.0942	-2.1210
19	-1.0959	-1.1697	-2.2217	-2.0182	-2.0260	-2.2991	-2.2735	-2.2555	-2.2804
20	-2.4344	-2.3980	-2.5022	-2.2030	-2.2117	-2.5577	-2.5105	-2.4745	-2.5051
21	-1.1650	-1.2657	-2.3515	-2.0738	-2.0833	-2.4090	-2.3947	-2.3410	-2.3699
22	-1.1707	-1.2696	-2.3527	-2.0771	-2.0864	-2.4109	-2.3969	-2.3461	-2.3753
23	-0.2364	-0.2084	-0.7488	-0.5052	-0.5123	-0.8031	-0.7730	-0.8313	-0.8513
24	-0.3054	-0.2468	-0.8417	-0.6391	-0.6465	-0.9053	-0.8650	-0.9397	-0.9616
25	-1.4125	-1.4666	-2.7115	-2.7825	-2.7804	-2.7962	-2.7554	-2.7645	-2.7911
26	-1.8181	-1.8374	-2.1009	-1.8151	-1.8236	-2.1465	-2.1137	-2.1162	-2.1494
27	-1.0262	-1.1825	-2.1379	-1.8067	-1.8154	-2.1629	-2.1592	-2.0744	-2.1011
33	-0.0991	-0.0932	-0.4108	-0.2113	-0.2164	-0.4495	-0.4298	-0.4943	-0.5103
34	-0.3205	-0.3382	-0.8499	-0.5843	-0.5920	-0.8903	-0.8815	-0.9354	-0.9574
35	-0.5136	-0.5453	-1.1498	-0.8656	-0.8746	-1.1922	-1.1852	-1.2332	-1.2619
49	0.0882	0.0910	0.1555	0.1398	0.1404	0.1602	0.1581	0.1566	0.1591

Table 4.8 Stability Limits and Security Domains of Each Parameter (Stressed Case)

Gen.No.	P^o	P^m	α*P^m	$\partial\Delta V/\partial P$	ΔV^s	Bus No.
1	0.51000	5.39322	5.12356	-0.14515	0.03914	7
2	14.86000	15.96679	15.16845	-0.64041	0.51126	7
3	2.50000	3.78417	3.59497	-0.55195	0.10443	7
4	0.47000	1.76110	1.67304	-0.54899	0.04834	7
5	0.70000	2.33408	2.21738	-0.43376	0.05062	7
6	6.73000	7.24164	6.87955	-1.38536	0.50161	7
7	0.22000	2.59335	2.46368	-0.29865	0.03873	7
8	0.64000	1.68192	1.59783	-0.68028	0.05721	7
9	13.00000	13.51456	12.83883	-1.37748	0.93080	7
10	3.00000	6.70324	6.36808	-0.19140	0.06415	7
11	1.31000	12.95449	12.30676	-0.06087	0.03943	7
12	0.60000	1.39067	1.32114	-0.89645	0.06233	7
13	1.40000	2.38968	2.27020	-0.71619	0.08557	7
14	4.26000	4.73453	4.49780	-1.49370	0.35360	7
15	2.00000	2.51730	2.39143	-1.37020	0.17246	7
16	1.70000	2.30231	2.18720	-1.17680	0.13547	7
17	3.10000	3.78101	3.59196	-1.04080	0.19676	7
19	1.35000	1.99677	1.89694	-1.09590	0.10941	7
20	20.00000	20.29116	19.27660	-2.43440	2.46984	7
21	16.20000	16.80841	15.96799	-1.16500	0.97909	7
22	10.80000	11.40545	10.83518	-1.17070	0.66762	7
23	8.00000	10.99729	10.44743	-0.23648	0.13003	7
24	0.52000	2.84074	2.69870	-0.30542	0.04338	7
25	13.00000	13.50181	12.82671	-1.41250	0.95357	7
26	20.00000	20.38986	19.37037	-1.81810	1.85354	7
27	3.00000	3.69070	3.50617	-1.02620	0.18937	7
33	29.97000	37.11804	35.26214	-0.09916	0.18403	7
34	10.09000	12.30113	11.68607	-0.32056	0.19716	7
35	30.05000	31.42998	29.85848	-0.51363	0.80717	7

* $\alpha = 0.95$

By comparing the data in the above table and the data in Table 4.3, which is the base case stability limit and security domain values, it is found that the big difference is that for the stressed case the stability limit P^{max} has been greatly reduced for almost all the machines. This means that for the stressed operating condition many more generators are operated closer to their stability limits. We can also find that in the base case only generators 20 and 26 are operated in the vulnerable domain while in the stressed case six machines are operating in the vulnerable domain. These are machines 9,20,21,25,26, and 35.

Our second step is to calculate the thresholds of ΔV and $\partial\Delta V/\partial P$ using the equations (3.8) and (3.9). We know that generators 9,20,21,25,26, and 35 are operating in the vulerability domain. Thus in Table 4.8 we check the ΔV^s values in the sixth column and the sensitivity values in the fifth column, which correspond to generators 9,20,21,25,26, and 35. It is found that the largest ΔV^s value is 2.46984 and the sensitivity value with smallest magnitude is -0.51363. Therefore, the results are as follows:

margin threshold	sensitivity threshold
2.46984	-0.51363

The next step is using these thresholds to divide the ΔV and $\partial\Delta V/\partial P$ in Tables 4.6 and 4.7 into high and low classes. It is shown as follows:

Table 4.9 Energy Margin Status for Different Fault Locations (Stressed Case)

1=high 0=low

Fault Bus No.	7	12	1	2	10	25	61	63
ΔV status	0	1	1	1	1	1	1	1

Table 4.10 Sensitivity Status of Each Generator Corresponding to Different Fault locations (Stressed Case)

1=high 0=low

gen.\bus	7	12	1	2	10	25	61	63
1	0	0	0	0	1	1	1	1
2	1	1	1	1	1	1	1	1
3	1	1	1	1	1	1	1	1
4	1	1	1	1	1	1	1	1
5	0	1	1	1	1	1	1	1
6	1	1	1	1	1	1	1	1
7	0	1	1	1	1	1	1	1
8	1	1	1	1	1	1	1	1
9	1	1	1	1	1	1	1	1
10	0	1	0	0	1	1	1	1
11	0	0	0	0	0	0	0	0
12	1	1	1	1	1	1	1	1
13	1	1	1	1	1	1	1	1
14	1	1	1	1	1	1	1	1
15	1	1	1	1	1	1	1	1
16	1	1	1	1	1	1	1	1
17	1	1	1	1	1	1	1	1
19	1	1	1	1	1	1	1	1
20	1	1	1	1	1	1	1	1
21	1	1	1	1	1	1	1	1
22	1	1	1	1	1	1	1	1
23	0	1	0	0	1	1	1	1
24	0	1	1	1	1	1	1	1
25	1	1	1	1	1	1	1	1
26	1	1	1	1	1	1	1	1
27	1	1	1	1	1	1	1	1
33	0	0	0	0	0	0	0	0
34	0	1	1	1	1	1	1	1
35	1	1	1	1	1	1	1	1
49	0	0	0	0	0	0	0	0

The last step is to evaluate the system vulnerability status based on the ΔV and $\partial\Delta V/\partial P$ levels. Tables 4.9 and 4.10 show that the ΔV value for fault at Bus 7 belongs to lower level and the corresponding $\partial\Delta V/\partial P$ values of generator 2,3,4,6,8,9,12-17,19-22,25-27,and 35, a total of 20 machines, belong to high level. Therefore, the final result of the system vulnerability assessment is as follows.

```
system is vulnerable for the fault at following buses:
bus No.=  7
     generation increased at Gen. No.:  2
     generation increased at Gen. No.:  3
     generation increased at Gen. No.:  4
     generation increased at Gen. No.:  6
     generation increased at Gen. No.:  8
     generation increased at Gen. No.:  9
     generation increased at Gen. No.:  12
     generation increased at Gen. No.:  13
     generation increased at Gen. No.:  14
     generation increased at Gen. No.:  15
     generation increased at Gen. No.:  16
     generation increased at Gen. No.:  17
     generation increased at Gen. No.:  19
     generation increased at Gen. No.:  20
     generation increased at Gen. No.:  21
     generation increased at Gen. No.:  22
     generation increased at Gen. No.:  25
     generation increased at Gen. No.:  26
     generation increased at Gen. No.:  27
     generation increased at Gen. No.:  35
```

Since the ΔV value for fault at bus 6 is negative, the system is insecure for this contingency. Thus, for the stressed case the system is insecure for a

fault at bus 6 and vulnerable for a fault at bus 7 if the generation is increased at any of generators nos. 2-4,6,8-9,12-17,19-22,25-27, and 35.

Comparing the results of system vulnerability assessment for the base case and the stressed case operating conditions it is clear that in the stressed case there are more machines operated close to their stability limits. From a system vulnerability point of view, the system is more vulnerable if there is generation shift occurring at any one of many more machines.

The above analysis shows the application of the framework for system security and vulnerability assessment to a test system. For two operating conditions of this test system this framework incorporated the information of ΔV and $\partial\Delta V/\partial P$ to evaluate the system vulnerability status. It indicates both the system security status at the present operating condition and the trend of this status caused by changing the generation. On the basis of this framework the artificial neural network is applied to the same test system for the system vulnerability classification. This is presented in Chapter 5.

5. APPLICATION OF NEURAL NETWORKS IN DYNAMIC SECURITY ASSESSMENT

5.1 Introduction

Artificial neural networks(ANNs) have been studied for many years in order to achieve human-like performance in the fields of speech and image recognition. An ANN can be defined as a highly connected array of nonlinear computational elements operating in parallel and arranged in patterns similar to biological neural nets. In general ANNs consist of three elements: (1) an organized topology of interconnected processing elements which constitutes the architecture of the neural network, (2) a method of encoding information which is basically the training or learning algorithm, and (3) a method of recalling information. Among those three components the architecture and the training method have significant influence on the performance of ANNs. Some basic concepts of ANNs are introduced as follows [21]:

- Processing elements

Processing elements (PEs), also called nodes or neurons, are the basic components of ANNs where most of the computing is done. Figure 5.1 is the

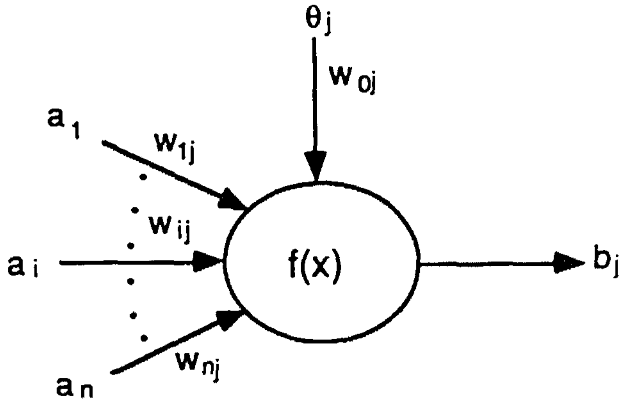

Figure 5.1 Processing Element of an ANN

configuration of a PE.

Figure 5.1 shows a schematic diagram of the jth PE. Here a_i is the ith input, and b_j is the output. Associated with each connected pair of PEs is an adjustable value w_{ij} called a weight. The input a_i, weight w_{ij} and the possible extra parameter θ_j are used to compute the output b_j by using the threshold function f(x). It is operated as

$$b_j = f\left(\sum_{i=1}^{n} a_i\, w_{ij} - w_{0j}\theta_j\right)$$

Where θ_j is considered to be an internal threshold value.

- Threshold functions

Threshold functions map a PE's input to the output. There are four commonly used threshold functions. They are linear, ramp, step and sigmoid functions. Among them the sigmoid function is widely used and its expression is

$$f(x) = (1 + e^{-x})^{-1}$$

- Architectures

ANNs' architectures are formed by connecting the PEs into layers and linking them with weighted interconnections. There are a variety of ANNs moaels and among them the six models mentioned in [22] are the most commonly used. They are hopfield net, hamming net, Carpenter/Grossberg classifier, perceptron, multi-layered perceptron, and Kohonen's self organizing feature maps.

- Learning

Learning or training is the most important concept of ANNs. It is defined to be any change in the value of the weight. There are different kinds of learning methods and all of them can be classified into two categories, supervised learning and unsupervised learning. Supervised learning is a process in which the desired output must be known. Unsupervised learning does not require knowledge of the output but relies only upon local information and internal control.

A brief summary of how an ANN works can be stated as follows:

After choosing an appropriate topology, an appropriate training method and appropriate input and output parameters, the ANN is trained by the selected sample data, or examples. If the training is good enough, the ANN should have the ability to properly classify data which has not been seen before and give the correct output. Thus, an ANN is taught by example, as opposed, for example, to an expert system, which is taught by rules.

The advantages of ANNs are characterized by parallel distributed processing, high computation rates, fault tolerance, and adaptive capacity. Distributed parallel processing and adaptive capacity make the ANNs very attractive. This is because the parallel processing allows the ANNs to deal with massive data in a very short period of time and the adaptive capacity allows the ANNs to classify complex nonlinear mapping between the input and the output.

Since the neural network computing is still an immature area, till now there has been no theoretical method to find the optimal architecture for a particular system. It also has some additional disadvantages such as: long training time, and sometimes the training procedure may not find the global optimal solution.

In recent years ANNs have been proposed as an alternative method for solving certain difficult problems in power systems where the conventional techniques have not achieved the desired speed, accuracy or efficiency. These ANN applications in power systems can be divided into three areas [23].

1. Regression
   - Load forecasting
   - Machine modelling
   - Transient stability

- Contingency screening
- Harmonic evaluation

2. Combinatorial optimization
   - Topological observability
   - Capacitor control

3. Classification
   - Harmonic load identification
   - Alarm processing
   - Static security assessment

From the above introduction we know that ANNs have been proposed for solving many power system problems. As for the power system dynamic security assessment, using ANN for power system dynamic security and vulnerability assessment is still a new research topic. Thus it is an important component of this research work.

The reason of applying ANN technique in dynamic security assessment is that it has been successfully used for classification of complex systems [24],[25]. We can predict that a TEF-ANN method which could help the on-line security and vulnerability assessment would be welcome in a power system control center.

5.2 The Neural Network Model

5.2.1 Layered perceptron

There are a variety of ANN models, among those models the layered perceptron is receiving the most attention as a viable candidate for application to power systems. The advantages of layered perceptron are: [21],[23]

1. It is suited to pattern matching that require a two-class response.
2. It has the ability to learn significantly nonlinear relationships.
3. The test results show that it has better performance in terms of classification or regression accuracy than other ANN models for the application in power systems.

The following is a basic multi-layered perceptron model: (Figure 5.2)

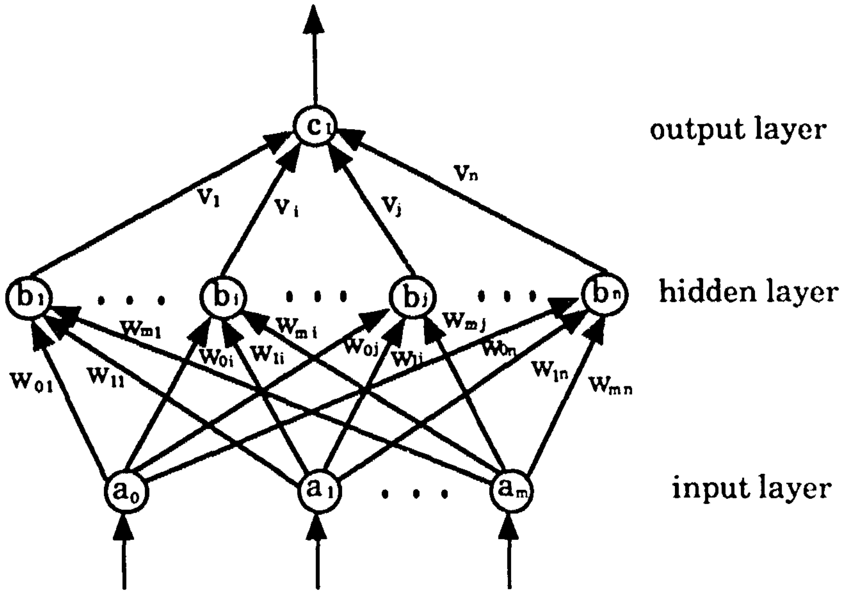

Figure 5.2 Multi-layered Perceptron

Layered perceptron is trained by numerical data. It operates in two modes: training and test. In the training mode, a set of representative training data is used to adjust the weights of the neural network. Once these weights have been determined, the neural network is said to be trained. In the test mode, the trained neural network is stimulated by test data. Usually the training and test data are different sets. The response of the layered perceptron should then be representative of the data by which it was trained.

5.2.2 Back-propagation algorithm

There is a variety of training algorithms available for the neural networks. The back-propagation algorithm is the most popular one used for the layered perceptron. It is a variation of steepest decent method for finding the minimum of a function. The basic idea is to use the sensitivity of the error with respect to the weight to modify the weight. If the multi-layered perceptron has L layers then for a weight $w_{ij}(\ell)$ in the ℓth layer, $\ell=1,2,\ldots,L$, this idea can be written as

$$w_{ij}(\ell) \Leftarrow w_{ij}(\ell) - \eta \frac{\partial E}{\partial w_{ij}(\ell)} \qquad (5.1)$$

where η is the step size. If there are M training data pairs then E is the total error, that is

$$E = \Sigma_{m=1}^{M} E^{m}$$

and E^{m} is the mean square error corresponding to the mth training data pair, that is

$$E^m = \frac{1}{2} \Sigma_{i=1}^{N_L} (t_i^m - r_i^m)^2$$

where t_i^m is the desired output and r_i^m is the computed output of the ith node in the output layer.

In its fundamental form, error back propagation modifies the weights in the following procedure: the adjustment to the weights is first made for the first input-output training data pair. A second step is made in response to the second training data pair, etc. In each step, all of the weights in the network are adjusted by using equation (5.1). When all of the training data has been used, the cycle is again repeated starting from the first training data pair. This process is repeated until an acceptably low error results.

The mathematical model of back-propagation is illustrated on the basis of the chain rule of partial derivatives. We can write the derivative term in (5.1) as

$$\frac{\partial E^m}{\partial w_{ij}(\ell)} = \frac{\partial E^m}{\partial s_i(\ell)} \frac{\partial s_i(\ell)}{\partial \sigma_i(\ell)} \frac{\partial \sigma_i(\ell)}{\partial w_{ij}(\ell)} \qquad (5.2)$$

where $s_i(\ell)$ is the output of ith node in ℓth layer and $\sigma_i(\ell)$ is the sum of the inputs to the ith node in the ℓth layer. That is

$$s_i(\ell) = f(\sigma_i(\ell))$$

and f(x) should be the sigmoid function. Define

$$\delta_i(l) = \frac{\partial E^m}{\partial s_i(l)}$$

We can show that we can get the following [23]

$$\frac{\partial E^m}{\partial w_{ij}(l)} = \delta_i(l)[\, s_i(l)(1- s_i(l))]s_j(l - 1) \qquad (5.3)$$

now the unknown value is $\delta_i(l)$ value. If the layered perceptron has L layers, then for l=L we have

$$\delta_i(L) = \frac{\partial E^m}{\partial s_i(L)}$$

$$= r_i^m - t_i^m \qquad (5.4)$$

It is simply the difference between the desired output and the computed output of the neural network. For $1 \leq l \leq$ L-1, we have

$$\delta_i(l) = \sum_{j=1}^{N_{l+1}} \delta_j(l + 1)[\, s_j(l+1)(1- s_j(l+ 1))]w_{ij}(l+1) \qquad (5.5)$$

From (5.4) and (5.5) we can see that δ_i(L -1) can be evaluated from δ_i(L), the value of δ_i(L -2) can be determined by δ_i(L -1) and onward, all the way to the input. Thus the error at the output is back propagated in order to adjust the weights using equation (5.1).

5.3 The Selected Neural Network Model

5.3.1 Layered perceptron and back-propagation algorithm

On the basis of the above analysis in section 5.2, the multi-layered perceptron was selected as the ANN model for the power system vulnerability classification. The back-propagation algorithm was used for training the layered perceptron. This layered perceptron has one input layer, one output layer and a number of hidden layers. There is only one node or neuron in the output layer, since for the system vulnerability classification the neural network works as a classifier. It categorizes the output into two categories: vulnerable or not vulnerable. The numbers of nodes in the input layer depends on how many variables are used as the input values and this will be discussed in the following subsection. As for the numbers of hidden layers and the nodes in each hidden layer they depend on the studied system condition, the size of training set and the nonlinear relation between the inputs and the output data of the training set. It has been shown that two hidden layers can classify any arbitrary decision region [22]. But we still need to determine the numbers of nodes in each hidden layer and this is one of the major tasks in training the neural network.

Until now we have selected the architecture of neural network and the training algorithm. The remaining job is choosing the appropriate input variables.

5.3.2 Input of neural network

An appropriate set of input variables should include those parameters which have significant impact on the power system vulnerability status. In Chapter 3 the ΔV and $\partial\Delta V/\partial P$ values are used in the new framework for evaluating the system vulnerability. Thus the input variables of neural network must have a strong relation to ΔV and $\partial\Delta V/\partial P$. Based on our study [26] the UEP angles θ^u are viable candidates to replace $\partial\Delta V/\partial P$ as the input of the neural network. (Other candidate input signals to the ANN are sensitivity values that can be easily computed, e.g., $\partial\theta^u/\partial P$.) The correlation between $\partial\Delta V/\partial P$ values and UEP angles can be explained by the UEP angles and sensitivity values in the following tables.

Tables 5.1 and 5.2 are the UEP angle matrix and sensitivity value matrix for the stressed case operating condition. Comparing these two matrices we do find that the sensitivity value has a strong relation to the UEP angle, especially for the advanced machines. For an advanced machine the UEP angle is equal to or greater than 90 degrees (1.57 radians). The physical meaning of an advanced machine is that this generator is severely disturbed and tends to lose the synchronism before other less disturbed generators. Tables 5.1 and 5.2 show that advanced machines their sensitivity values that are negative and have significant magnitudes. Thus, the negative sensitivity values are of primary concern. The generation increase at those advanced machines will cause the system to have severe stability problems.

On the basis of the above analysis the UEP angles are used instead of the sensitivity coefficients as the input of the neural network. At the same time we kept ΔV as another input of the neural network. The advantage of using UEP

Table 5.1 UEP Angles (radian) (Stressed Case)

Station A Generation = 2600 MW

Gen.\Bus	7	6	12	1	2	10	25	61	63
1	1.383	1.382	1.831	1.751	1.746	1.866	1.860	1.835	1.828
2	1.912	1.912	2.243	2.115	2.120	2.253	2.254	2.246	2.247
3	1.876	1.875	2.286	2.224	2.223	2.311	2.307	2.288	2.285
4	1.878	1.877	2.290	2.228	2.227	2.316	2.312	2.292	2.290
5	1.787	1.787	2.209	2.099	2.104	2.233	2.216	2.215	2.216
6	2.388	2.387	2.759	2.717	2.719	2.776	2.775	2.755	2.755
7	1.744	1.744	2.191	2.116	2.112	2.223	2.218	2.195	2.189
8	1.909	1.909	2.315	2.220	2.223	2.335	2.321	2.319	2.320
9	2.377	2.376	2.762	2.834	2.832	2.766	2.763	2.747	2.747
10	1.554	1.554	2.007	1.927	1.921	2.042	2.036	2.011	2.004
11	1.483	1.482	1.935	1.841	1.825	1.978	1.970	1.939	1.923
12	2.055	2.054	2.431	2.362	2.365	2.446	2.434	2.430	2.431
13	2.016	2.016	2.332	2.211	2.215	2.341	2.342	2.335	2.336
14	2.478	2.478	2.841	2.800	2.802	2.855	2.854	2.836	2.836
15	2.358	2.358	2.737	2.799	2.798	2.742	2.739	2.724	2.725
16	2.213	2.212	2.585	2.538	2.540	2.602	2.601	2.584	2.584
17	2.115	2.115	2.476	2.410	2.413	2.484	2.484	2.473	2.474
18	0.920	0.920	0.981	0.962	0.963	0.982	0.982	0.918	0.918
19	2.148	2.148	2.522	2.474	2.476	2.541	2.538	2.522	2.522
20	3.051	3.051	2.859	2.787	2.790	2.862	2.861	2.846	2.846
21	2.246	2.246	2.610	2.551	2.554	2.623	2.613	2.608	2.608
22	2.248	2.248	2.613	2.553	2.556	2.626	2.615	2.611	2.611
23	1.551	1.550	2.015	1.863	1.868	2.045	2.027	2.025	2.027
24	1.570	1.569	1.996	1.882	1.886	2.020	2.003	2.003	2.003
25	2.410	2.410	2.787	2.851	2.849	2.792	2.789	2.774	2.774
26	2.724	2.723	2.708	2.630	2.633	2.712	2.712	2.700	2.700
27	2.105	2.105	2.466	2.400	2.403	2.474	2.474	2.463	2.464
28	-0.049	-0.049	-0.064	-0.061	-0.062	-0.065	-0.064	-0.074	-0.074
29	0.098	0.098	0.100	0.098	0.098	0.099	0.100	0.077	0.077
30	0.271	0.271	0.288	0.282	0.282	0.287	0.288	0.252	0.252
31	0.152	0.152	0.160	0.157	0.157	0.159	0.160	0.133	0.133
32	-0.519	-0.519	-0.507	-0.502	-0.502	-0.510	-0.509	-0.506	-0.506
33	1.086	1.085	1.591	1.391	1.397	1.626	1.609	1.604	1.606
34	1.487	1.487	1.893	1.727	1.733	1.912	1.908	1.901	1.902
35	1.701	1.700	2.055	1.917	1.922	2.067	2.066	2.059	2.060
36	-0.013	-0.013	0.059	0.042	0.043	0.060	0.059	0.064	0.064
37	-0.457	-0.457	-0.452	-0.449	-0.449	-0.454	-0.453	-0.452	-0.452
38	-0.090	-0.090	-0.089	-0.087	-0.087	-0.090	-0.089	-0.090	-0.090
39	0.451	0.451	0.503	0.486	0.486	0.505	0.504	0.501	0.501
40	-0.198	-0.198	-0.232	-0.225	-0.225	-0.233	-0.233	-0.230	-0.230
41	0.505	0.505	0.477	0.483	0.483	0.476	0.477	0.479	0.479
42	0.055	0.055	0.019	0.027	0.026	0.018	0.019	0.021	0.021
43	-1.662	-1.662	-1.762	-1.741	-1.742	-1.764	-1.764	-1.744	-1.744
44	-0.662	-0.662	-0.722	-0.710	-0.710	-0.724	-0.723	-0.715	-0.715
45	0.063	0.063	0.053	0.055	0.055	0.053	0.053	0.049	0.049
46	0.188	0.188	0.191	0.189	0.189	0.190	0.190	0.178	0.178
47	0.090	0.090	0.079	0.082	0.082	0.078	0.079	0.078	0.078
48	0.103	0.103	0.062	0.070	0.070	0.060	0.061	0.064	0.064
49	-0.318	-0.318	-0.365	-0.356	-0.356	-0.367	-0.366	-0.361	-0.361
50	-0.060	-0.060	-0.084	-0.079	-0.079	-0.085	-0.084	-0.087	-0.087

Table 5.2 **Energy Margin Sensitivity**

Station A Generation = 2600 MW

Gen.\Bus	7	6	12	1	2	10	25	61	63
1	−0.145	−0.149	−0.492	−0.384	0.386	−0.544	−0.530	−0.532	−0.540
2	−0.640	−0.678	−1.331	−1.031	−1.040	−1.375	−1.366	−1.412	−1.444
3	−0.551	−0.626	−1.348	−1.133	−1.137	−1.402	−1.384	−1.348	−1.360
4	−0.548	−0.453	−1.128	−0.859	−0.867	−1.181	−1.159	−1.179	−1.201
5	−0.612	−0.635	−1.823	−1.890	−1.896	−1.923	−1.990	−1.877	−1.888
6	−1.385	−1.505	−2.797	−2.520	−2.529	−2.858	−2.828	−2.754	−2.776
7	−0.298	−0.318	−0.847	−0.698	−0.700	−0.917	−0.897	−0.899	−0.910
8	−0.680	−0.775	−1.594	−1.270	−1.279	−1.629	−1.636	−1.575	−1.598
9	−1.377	−1.438	−2.659	−2.736	−2.733	−2.741	−2.700	−2.702	−2.731
10	−0.191	−0.193	−0.603	−0.485	−0.488	−0.666	−0.649	−0.657	−0.666
11	−0.060	−0.063	−0.251	−0.185	−0.194	−0.300	−0.285	−0.303	−0.314
12	−0.896	−1.011	−1.936	−1.641	−1.649	−1.975	−1.977	−1.904	−1.929
13	−0.716	−0.755	−1.442	−1.133	−1.142	−1.488	−1.477	−1.525	−1.555
14	−1.493	−1.631	−2.943	−2.652	−2.660	−2.996	−2.964	−2.881	−2.899
15	−1.370	−1.429	−2.644	−2.714	−2.712	−2.726	−2.686	−2.694	−2.719
16	−1.176	−1.283	−2.393	−2.146	−2.154	−2.455	−2.430	−2.382	−2.407
17	−1.040	−1.204	−2.168	−1.828	−1.837	−2.191	−2.187	−2.094	−2.121
18	0.225	0.222	0.426	0.391	0.393	0.439	0.430	0.422	0.416
19	−1.095	−1.169	−2.221	−2.018	−2.026	−2.299	−2.273	−2.255	−2.280
20	−2.434	−2.398	−2.502	−2.203	−2.211	−2.557	−2.510	−2.474	−2.505
21	−1.165	−1.265	−2.351	−2.073	−2.083	−2.409	−2.394	−2.341	−2.369
22	−1.170	−1.269	−2.352	−2.077	−2.086	−2.410	−2.396	−2.346	−2.375
23	−0.236	−0.208	−0.748	−0.505	−0.512	−0.803	−0.773	−0.831	−0.851
24	−0.305	−0.246	−0.841	−0.639	−0.646	−0.905	−0.865	−0.939	−0.961
25	−1.412	−1.466	−2.711	−2.782	−2.780	−2.796	−2.755	−2.764	−2.791
26	−1.818	−1.837	−2.100	−1.815	−1.823	−2.146	−2.113	−2.116	−2.149
27	−1.026	−1.182	−2.137	−1.806	−1.815	−2.162	−2.159	−2.074	−2.101
28	0.133	0.135	0.236	0.214	0.215	0.243	0.240	0.234	0.238
29	0.186	0.187	0.331	0.382	0.383	0.431	0.424	0.408	0.419
30	0.187	0.190	0.340	0.375	0.370	0.407	0.421	0.398	0.399
31	0.199	0.200	0.355	0.323	0.324	0.365	0.360	0.346	0.352
32	0.014	0.021	0.024	0.017	0.017	0.027	0.026	0.042	0.042
33	−0.099	−0.093	−0.410	−0.211	−0.216	−0.449	−0.429	−0.494	−0.510
34	−0.320	−0.338	−0.849	−0.584	−0.592	−0.890	−0.881	−0.935	−0.957
35	−0.513	−0.545	−1.149	−0.865	−0.874	−1.192	−1.185	−1.233	−1.261
36	−0.013	−0.004	−0.066	−0.042	−0.045	−0.070	−0.067	−0.043	−0.045
37	0.030	0.035	0.052	0.046	0.046	0.058	0.057	0.067	0.067
38	0.053	0.057	0.098	0.086	0.086	0.102	0.101	0.107	0.107
39	0.004	0.005	0.011	0.018	0.017	0.018	0.012	0.010	0.008
40	0.085	0.088	0.151	0.135	0.136	0.156	0.154	0.153	0.155
41	0.126	0.131	0.225	0.203	0.204	0.232	0.228	0.225	0.229
42	0.109	0.113	0.195	0.175	0.176	0.200	0.198	0.195	0.198
43	−0.021	−0.020	−0.061	−0.054	−0.055	−0.064	−0.063	−0.055	−0.056
44	0.069	0.071	0.121	0.108	0.109	0.124	0.123	0.122	0.124
45	0.092	0.095	0.167	0.150	0.151	0.173	0.170	0.170	0.172
46	0.120	0.121	0.222	0.200	0.201	0.229	0.226	0.220	0.223
47	0.078	0.082	0.142	0.127	0.127	0.147	0.145	0.148	0.149
48	0.108	0.112	0.192	0.173	0.173	0.198	0.195	0.193	0.196
49	0.088	0.091	0.155	0.139	0.140	0.160	0.158	0.156	0.159
50	0.106	0.109	0.189	0.170	0.171	0.194	0.192	0.189	0.192

angles as the input is that when we use the ANN for on-line security and vulnerability analysis, the system could consist of hundreds of generators and the contingencies of concern may also be a large number. Therefore, we are confronted with a lot of data. If the sensitivity $\partial \Delta V/\partial P$ is used as the input of neural network we have to calculate the $\partial \Delta V/\partial P$. Since the calculation of $\partial \Delta V/\partial P$ is so computationally intensive and time consuming, it may cause the on-line vulnerability analysis to be nearly impossible. By using the UEP angles as the input to the neural network, we do not need to calculate $\partial \Delta V/\partial P$ but depend on an ANN to find the complex relation between inputs and the output. Therefore, we can greatly reduce the computation burden by nearly 50%, and achieve faster on-line performance.

5.4 Results of Training the ANN

Using the same test system shown in Chapter 4, the above neural network was trained to classify the power system vulnerability status for three operating conditions. The first one was the base case operating condition, the second one was the stressed case operating condition. As we have mentioned in Chapter 4 the base case power flow is characterized by setting the generation at power station A to be 1400 MW, while the stressed case power flow is characterized by setting the generation at power station to be 2600 MW. The generation at station B is held at 4000 MW for both cases. The third one was a large operating region, it is obtained by increasing the generation at power station A from 1400 MW to 2600 MW. The increment is 200 MW per step.

Therefore, we have seven different operating points in this region from 1400 MW to 2600 MW.

For the system vulnerability classification the neural network works as a classifier. Therefore, the training set includes the following data:

1. desired output: system vulnerability status
   1 = vulnerable 0 = not vulnerable
2. inputs: a. ΔV value
   b. UEP angles

It should be emphasized that each training pair consists of one desired output and the corresponding inputs. The corresponding desired output or the vulnerability status for the selected contingency is evaluated by using the procedure of system vulnerability assessment proposed in Chapter 3. That is for a given contingency we can obtain the corresponding ΔV and $\partial \Delta V/\partial P$ values, by using the procedure of system vulnerability assessment proposed in Chapter 3 if the system is vulnerable, the desired output for this training stage pair will be 1, otherwise the desired output is 0. After the training stage, the ANN will classify the system vulnerability status based on this framework for system vulnerability assessment. In other words, we let the ANN develop a knowledge of system vulnerability classification from this framework through these training examples and then use the knowledge to classify the vulnerability status of other contingencies it had not seen before. It should be remembered, however, that in the training process the ANN accomplishes the additional task of finding the complex relationship between the θ^u inputs and the output results based on $\partial \Delta V/\partial P$ information.

Based on these training data, the multi-layered perceptron is trained for the system vulnerability classification by using the computer package NeuralWorks Professional II [27],[28].

5.4.1. Base case ANN training

For the base case condition, the neural network configuration includes one input layer, one hidden layer with two nodes and one output layer with only one node. For the nodes in input layer there are 28 advanced machines of concern. Thus, the inputs of neural network would be 29 UEP angles corresponding to these 28 advanced machines and 1 reference machine and plus one ΔV value. Therefore, there is a total of 30 nodes in the input layer.

Based on the results in Chapter 4 section 2 we know that in this operating condition the system is vulnerable for faults at Bus 7, and 6. Thus the desired output is 1 for faults at these two buses and 0 for the rest of fault buses. There are nine training pairs in the training set since there are nine contingencies of concern.

The training procedure is that the neural network picks up any training pair from the training set in a random order to learn. We can choose different training times for this training. Training times refer to how many times the neural network will pick up a training pair from the training set to learn. After training is finished, the same training set is used as the test set and input the data to this trained neural network. This is to check the results of system vulnerability classification of this layered perceptron for these nine contingencies. The results of training for the different training times are as listed in Table 5.3.

Table 5.3 Base Case Training Results vs. Training Times

	desired output	computed output	fault bus No.
a.	training times N=40		
	1.0	0.604214	7
	1.0	0.600523	6
	0.0	0.104742	12
	0.0	0.103040	1
	0.0	0.103020	2
	0.0	0.103084	10
	0.0	0.103274	25
	0.0	0.102697	61
	0.0	0.102684	63
	0.0	0.107041	33
b.	training times N=180		
	1.0	0.860502	7
	1.0	0.859243	6
	0.0	0.046341	12
	0.0	0.046147	1
	0.0	0.046145	2
	0.0	0.046151	10
	0.0	0.046168	25
	0.0	0.046124	61
	0.0	0.046123	63
	0.0	0.047050	33
c.	training times N=400		
	1.0	0.942520	7
	1.0	0.940745	6
	0.0	0.028891	12

Table 5.3 (continued)

0.0	0.028816	1
0.0	0.028814	2
0.0	0.028829	10
0.0	0.028833	25
0.0	0.028770	61
0.0	0.028765	63
0.0	0.028716	33

In Table 5.3 the first column is the desired outputs. They are obtained by using the procedure of system vulnerability assessment proposed in Chapter 3. The second column is the actual results of system vulnerability classification by the neural network. The third column is the corresponding contingency. Therefore the error between the desired output and the computed output will tell us the quality of training. If the training is perfect, the actual computed output would be either 0.0 or 1.0. However, according to reference [28], with the back-propagation training algorithm, an output less than 0.2 is usually considered 0.0. Likewise an output about 0.8 is considered 1.0. The above results show that when the training times are 180, the ANN gives the correct system vulnerability classification. As we further increase the training times, we get even better training results .

5.4.2 Stressed case ANN training

For this stressed case, the neural network configuration includes one input layer, one hidden layer with two nodes and one output layer with only one node. As for the nodes in the input layer, the difference is that in this case there are 29 advanced machines of concern. Thus, the inputs of neural network would be 30 UEP angles for these 29 advanced machines and 1 reference machine and plus one ΔV value. Therefore, the total nodes in the input layer is 31.

For this operating condition according to the results in Chapter 4 section 3 we know that the system is unstable for fault at bus 6 and vulnerable for fault at bus 7. Thus the desired output is 1 for faults at these two buses and 0 for the rest of fault buses. As with the base case, there are nine training pairs in the training set since there are nine contingencies of concern. The result of training the ANN is shown as follows and the training times are 180.

Table 5.4 shows that the ANN correctly classified the system vulnerability status for this stressed operating condition.

Table 5.4 Stressed Case Training Result

training times N=180

desired output	computed output	fault bus No.
1.0	0.864544	7
1.0	0.888366	6
0.0	0.070913	12
0.0	0.060058	1
0.0	0.059237	2
0.0	0.055472	10
0.0	0.056235	25
0.0	0.054391	61
0.0	0.054380	63

5.4.3 ANN training for a large operating region

In this operating region we collect the training data by increasing the output of the power station A from 1400 MW to 2600 MW. The increment is 200 MW per step. Therefore we have seven different operating points within this region from 1400 MW to 2600 MW. The selected contingencies are the same as those for the base case and the stressed case operating conditions. There are nine fault locations. As in Chapter 4, for each operating condition the ΔV and $\partial\Delta V/\partial P$ values are calculated for these nine faults. Then the system vulnerability status is evaluated for each contingency and each operating condition based on the framework proposed in Chapter 3. There are nine contingencies and seven operating conditions, thus we have a total of 63 pairs of training data. Table 5.5 is the system vulnerability status matrix, which is the desired output of ANN, for these nine contingencies with different operating conditions within this operating region. The values were obtained by using the procedure of system vulnerability assessment developed in Chapter 3.

Table 5.5 System Vulnerability Status Matrix

Pm\Bus No.	7	6	12	1	2	10	25	61	63
1400 mw	1	1	0	0	0	0	0	0	0
1600 mw	0	1	0	0	0	0	0	0	0
1800 mw	0	1	0	0	0	0	0	0	0
2000 mw	0	1	0	0	0	0	0	0	0
2200 mw	0	1	0	0	0	0	0	0	0
2400 mw	1	1	0	0	0	0	0	0	0
2600 mw	1	1	0	0	0	0	0	0	0

1= VULNERABLE 0= NOT VULNERABLE

In Table 5.5 the first column is the total generation at power station A, and the rest of columns are the system vulnerability status or the desired output of ANN for the corresponding contingency under various operating conditions.

It is generally recognized that if the size of training set is getting larger then the configuration of neural network will be more complicated. This means that there will be more hidden layers and more nodes in each hidden layer. It has been mentioned at the beginning of this chapter that there is no theoretical method to find the optimal architecture for a particular system. We therefore find the best configuration by trial and error. For this operating region after several tests the selected neural network configuration includes one input layer, two hidden layers with six nodes in the first hidden layer and two nodes in the second hidden layer, and one output layer with only one node. For this test, the same set of data is used for training and for testing the ANN network. The number of training times N=1000. The results are shown in Table 5.6.

Table 5.6 Training Results for a Large Operation Region

Training Times N=1000

Generation	Desired output	Computed output	Fault bus No.
1400 MW	1.0	0.773662	7
	1.0	0.874138	6
	0.0	0.010753	12
	0.0	0.010753	1
	0.0	0.010753	2
	0.0	0.010753	10

Table 5.6 (continued)

	0.0	0.010753	25
	0.0	0.010753	61
	0.0	0.010753	63
1600 MW	0.0	0.032605	7
	1.0	0.874137	6
	0.0	0.010753	12
	0.0	0.010753	1
	0.0	0.010753	2
	0.0	0.010753	10
	0.0	0.010753	25
	0.0	0.010753	61
	0.0	0.010753	63
1800 MW	0.0	0.023989	7
	1.0	0.874091	6
	0.0	0.010753	12
	0.0	0.010753	1
	0.0	0.010753	2
	0.0	0.010753	10
	0.0	0.010753	25
	0.0	0.010753	61
	0.0	0.010753	63
2000 MW	0.0	0.024542	7
	1.0	0.874131	6
	0.0	0.010753	12
	0.0	0.010753	1
	0.0	0.010753	2
	0.0	0.010753	10
	0.0	0.010753	25

Table 5.6 (continued)

	0.0	0.010753	61
	0.0	0.010753	63
2200 MW	0.0	0.090642	7
	1.0	0.874138	6
	0.0	0.010835	12
	0.0	0.010754	1
	0.0	0.010754	2
	0.0	0.010753	10
	0.0	0.010754	25
	0.0	0.010753	61
	0.0	0.010753	63
2400 MW	1.0	0.868662	7
	1.0	0.874138	6
	0.0	0.023517	12
	0.0	0.017382	1
	0.0	0.015791	2
	0.0	0.010863	10
	0.0	0.011434	25
	0.0	0.010753	61
	0.0	0.010753	63
2600 MW	1.0	0.874094	7
	1.0	0.874138	6
	0.0	0.031959	12
	0.0	0.024061	1
	0.0	0.023949	2
	0.0	0.023558	10
	0.0	0.023773	25
	0.0	0.010773	61
	0.0	0.010762	63

It is to be noted that in the training of the neural network an output less than 0.2 is usually considered 0.0. Likewise an output about 0.8 is considered 1.0. Thus, the above results show that the only error is for fault at Bus 7 when the generation at power station A is 1400 MW, in which the computed output is 0.773662. It is slightly away from the required value 0.8 indicating that the classification lies close to the border between two classes. However, the overall training is successful.

We now increase the training times by making the training times N=12000. A sample of the ANN results for four operating conditions and nine fault locations are shown in Table 5.7. The results for the remaining operating conditions are similar to those shown in Table 5.6.

The results in Tables 5.7 show that the ANN can give the correct classification for the training data when the training times is large enough.

Table 5.7 Training Result for a Large Operating Region
Training Times N=12000

Generation	Desired output	Computed output	Fault bus No.
1400 MW	1.0	0.859290	7
	1.0	0.987397	6
	0.0	0.020224	12
	0.0	0.020224	1
	0.0	0.020224	2
	0.0	0.020224	10
	0.0	0.020224	25
	0.0	0.020224	61
	0.0	0.020224	63
1800 MW	0.0	0.020224	7
	1.0	0.986061	6

Table 5.7 (continued)

	0.0	0.020224	12
	0.0	0.020224	1
	0.0	0.020224	2
	0.0	0.020224	10
	0.0	0.020224	25
	0.0	0.020224	61
	0.0	0.020224	63
2200 MW	0.0	0.028948	7
	1.0	0.987397	6
	0.0	0.020224	12
	0.0	0.020224	1
	0.0	0.020224	2
	0.0	0.020224	10
	0.0	0.020224	25
	0.0	0.020224	61
	0.0	0.020224	63
2600 MW	1.0	0.986034	7
	1.0	0.987397	6
	0.0	0.020255	12
	0.0	0.020224	1
	0.0	0.020224	2
	0.0	0.020224	10
	0.0	0.020224	25
	0.0	0.020224	61
	0.0	0.020224	63

5.4.4 ANN training by using different training and test data

In section 5.4.3 the 63 data pairs are used to train the ANN as well as to test it, i.e., it is also used as the inputs to check the ANN outputs. By comparing the ANN outputs with the desired outputs shown in Table 5.7 we get a completely correct system vulnerability classification.

It should be kept in mind that usually the training and test data are different sets. If the training is good enough, the ANN should have the ability to properly classify the test data which has not been seen before and give the correct outputs.

On the basis of above analysis, the above 63 training data pairs are divided into two sets.

a. training set:

It includes the data corresponding to the operating points (generation at power station A)

1400 MW

1600 MW

2000 MW

2200 MW

2600 MW

This data represents five operating conditions and nine contingencies. Thus there are total of 45 training data pairs.

b. test set:

It includes the data corresponding to the operating points

1800 MW

2400 MW

Thus there are 18 test data pairs.

The above two sets of data are used to train and test the ANN. Two cases are considered.

Case 1 Same data is used to train the ANN and as the inputs to check the training. The result is shown in Table 5.8.

Noting that in the training of the neural network an output of less than 0.2 is considered 0.0, and output equal to or greater than 0.8 is considered 1.0, the results in Table 5.8 show that the ANN output correctly predicts the system vulnerability for those 45 cases.

Case 2 After using the training set to train the ANN, the test set was used as the input to check if proper classification is obtained. The result is shown in Table 5.9.

The results in Tables 5.9 show that the ANN can give the correct classification for the test data which has not been seen before.

The above training and testing results indicate that the training of the neural network has been successful for a variety of operating conditions and disturbances for the IEEE 50-generator test system. We can conclude, therefore, that the multi-layered perceptron can successfully classify system vulnerability. As we have mentioned at the beginning of this chapter, the ANNs have advantages such as parallel distributed processing, high computation rates, fault tolerance, and adaptive capacity. Thus, it could be a potential tool for on-line power system dynamic security assessment application.

Table 5.8 Training Result for a Large Operating Region

(recall the training set)

Training Times N=12000

Generation	Desired output	Computed output	Fault bus No.
1400 MW	1.0	0.977602	7
	1.0	0.985038	6
	0.0	0.003377	12
	0.0	0.003377	1
	0.0	0.003377	2
	0.0	0.003377	10
	0.0	0.003377	25
	0.0	0.003377	61
	0.0	0.003377	63
1600 MW	0.0	0.007784	7
	1.0	0.985038	6
	0.0	0.003377	12
	0.0	0.003377	1
	0.0	0.003377	2
	0.0	0.003377	10
	0.0	0.003377	25
	0.0	0.003377	61
	0.0	0.003377	63
2000 MW	0.0	0.006081	7
	1.0	0.985038	6
	0.0	0.003377	12
	0.0	0.003377	1
	0.0	0.003377	2
	0.0	0.003377	10
	0.0	0.003377	25

Table 5.8 (continued)

	0.0	0.003377	61
	0.0	0.003377	63
2200 MW	0.0	0.011101	7
	1.0	0.985038	6
	0.0	0.003388	12
	0.0	0.003377	1
	0.0	0.003377	2
	0.0	0.003377	10
	0.0	0.003377	25
	0.0	0.003377	61
	0.0	0.003377	63
2600 MW	1.0	0.985037	7
	1.0	0.985038	6
	0.0	0.006941	12
	0.0	0.005901	1
	0.0	0.005876	2
	0.0	0.005812	10
	0.0	0.005839	25
	0.0	0.003378	61
	0.0	0.003377	63

Table 5.9 Training Result for a Large Operating Region (recall the test set)

Training Times N=12000

Generation	Desired output	Computed output	Fault bus No.
1800 MW	0.0	0.005920	7
	1.0	0.985037	6
	0.0	0.003377	12
	0.0	0.003377	1
	0.0	0.003377	2
	0.0	0.003377	10
	0.0	0.003377	25
	0.0	0.003377	61
	0.0	0.003377	63
2400 MW	1.0	0.984615	7
	1.0	0.985038	6
	0.0	0.005805	12
	0.0	0.004968	1
	0.0	0.004797	2
	0.0	0.003394	10
	0.0	0.003623	25
	0.0	0.003377	61
	0.0	0.003377	63

6. CONCLUSIONS

In this dissertation the need for a new framework for assessment of power system dynamic security, which includes the trend of security status, is discussed. Therefore, the system vulnerability is introduced as a new concept for assessing the system dynamic security. The transient energy function method of transient stability assessment is used as the tool of analysis to implement this new framework for system dynamic security and vulnerability assessment.

The major contributions of this research work can be summarized as follows:

1. A new framework for power system security and vulnerability assessment was developed based on the TEF method. The new framework indicates both the present security level using the energy margin ΔV, and the trend of security status due to the possible variation of a system operating parameter p using the energy margin sensitivity $\partial \Delta V / \partial p$. Therefore, this framework can identify weak points in the system, and how the changes of the parameter may cause the system to become vulnerable to contingencies.

2. Within this framework, the concept of system vulnerability is addressed. The indices of vulnerability are determined by establishing the thresholds for acceptable levels of ΔV and $\partial \Delta V/\partial p$; and relating these thresholds to stability limits of critical system parameters.

3. The procedure for system security and vulnerability assessment was implemented for changes in plant generation P. This procedure is simple and can be easily adopted for on-line system vulnerability assessment.

4. The artificial neural networks technique was used for power system security and vulnerability classification. A multi-layered perceptron model was selected and the back-propagation algorithm was used for training the neural network.

5. The correlation between the energy margin sensitivity with respect to the plant generation and the UEP angles were investigated and the UEP angles were used instead of the energy margin sensitivity values as the input to the ANN to achieve fast on-line performance.

6. The procedure for vulnerability assessment was demonstrated by a validation study on the IEEE 50-generator system. Data for an unstressed system condition as well as a stressed system condition (ΔV and $\partial \Delta V/\partial P$) were given. The corresponding generation limits were computed and the acceptable thresholds for the security indicator S_W

and its sensitivity indicator $S_{\Delta V/\Delta P}$ were presented. System vulnerability was assessed for these operating conditions.

7. The artificial neural network model was applied to this IEEE 50-generator system. It gives correct system vulnerability classification for a variety of operating conditions and disturbances including previously unseen data. We can conclude, therefore, that the multi-layered perceptron can successfully classify system vulnerability and could be a potential tool for on-line system dynamic security assessment application.

The suggestions for the future work are as following:

1. From dynamic security point of view, there are several critical parameters which may be of concern such as plant generation, system configuration, transmission interface power flow, etc.. In this research work we considered only the variation of plant generation to build our security and vulnerability framework. Therefore, the next step would be to extend the same idea to cover the effect of other parameters, as well as the combination of parameters, on system dynamic security.

2. When this new framework for power system security and vulnerability assessment is applied, and if the system is vulnerable for some given contingencies, the system operators need to know what kinds of control action should be applied in order to relieve a potentially vulnerable

situation. Thus, investigation of the necessary control actions for the vulnerable system condition would also be an important research topic.

BIBLIOGRAPHY

[1] Anderson, P. M., and Fouad, A. A., Power system Control and Stability , Vol. I, Ames, Iowa, Iowa State University Press, 1977.

[2] Fouad, A. A., F. Aboytes, G. Cepero, S. Corey, K. Dhir, and R. Vierra, "Dynamic Security Assessment Practices in North America," IEEE Trans. on PWRS, vol. 3, pp 1310-1321, Aug. 1988.

[3] Fouad, A. A., Pai, M. A., and Schlueter, R., "Security Assessment," presented at NSF Workshop On University Research For Electric Power System Engineering, Tempe, Arizona, April, 1987.

[4] DyLiacco, T. E., "The Adaptive Reliability Control System," IEEE Trans. Power App. Syst., Vol. PAS-86, pp. 517-531, May 1967

[5] DyLiacco, T. E., "Real-time Computer Control of Power System," Proceedings of the IEEE , Vol. 62, pp. 884-891, July 1974

[6] DyLiacco, T. E., "System Security: The Computer's Role," IEEE Spectrum, Vol. 15, pp. 43-50, June 1978

[7] Wu, Felix F., "Analysis Techniques for Power System Security Assessment and Optimization: Research Needs and Emerging Tools," Proceedings of the Workshop on Power System Security Assessment, Iowa State University, 1988.

[8] Fouad, A. A., "Research Issues in Computer Analysis of Power systems: Industrial Perspectives on Dynamic Security Assessment," Class note, Iowa State University, Fall Semester, 1991

[9] Fouad, A. A. ,and Vittal, V., Power System Transient Stability Analysis Using The Transient Energy Function Method. Prentice Hall, Englewood Cliffs, New Jersey, 1992

[10] El-Kady, M. A., Fouad, A. A. , and Liu, C. C., Knowledge-Based System for Direct Stability Analysis, EPRI Report No. EL-6796, 1990.

[11] Minutes of the Meetings of the Working Group on Dynamic Security Assessment", July, 1988 - July, 1990, Power System Engineering Committee, Power Engineering Society, IEEE.

[12] William D. Stevenson, Jr., Elements of power system analysis, McGraw-Hill Book Company, New York, 1982.

[13] Khalil, Hassan K., Nonlinear Systems, Macmillan Publishing Company, New York, 1992.

[14] Sauer, P. A., Demaree K. D., and Pai, M. A. "Stability Limited Load Supply and Interchange Capability." IEEE Trans. PAS-102 Nov. 1983 3/637-3/643.

[15] El-Kady, M. A., Tang, C. K., Carvalho, V. F., Fouad, A. A., and Vittal, V. "Dynamic Security Assessment Utilizing the Transient Energy Function Method." Proceedings of 1985 PICA Conference, San Francisco, California, May 1985, pp.132-139.

[16] Vittal, V., Fouad, A. A., and Kundur, P. "Determination of Transient Stability-Constrained Plant Generation Limits." Proceedings of IFAC

Symposium on Automation and Instrumentation of Power Plant, Bangalore, India, Dec. 1986, pp A-8-1 through A-8-5.

[17] Pai, M.A. et al. "Direct Method of Stability Analysis in Dynamic Security Assessment." Paper No. 1.1/A4, IFAC World Congress, Budapest, July 1984.

[18] Hwang, C., Sensitivity analysis of the transient energy function method, Ph.D. dissertation, Iowa State University, 1989.

[19] Vittal, V., Zhou, E. Z., Hwang, C., Fouad, A. A. "Derivation of Stability Limits using Analytic Sensitivity of the Transient Energy Margin." IEEE Trans. on PWRS, vol. 4, pp 1363-1372, Nov. 1989.

[20] Vittal, V., "Transient Stability Test Systems for Direct Stability Methods," IEEE Committee Report, IEEE Transaction on PAS, pp.37-42, Feb. 1992

[21] Simpson, P. K., Artificial Neural Systems, Pergamon Press, New York, 1990.

[22] Lippmann, R. P., "An Introduction To Computing With Neural Nets," IEEE ASSP Magazine, pp 4-22, April, 1987.

[23] El-Sharkawi, M. A., etc., "Neural Networks and Their Application to Power Engineering," Control and Dynamic Systems, Vol. 41, Academic Press, New York, 1991.

[24] Ostojic, D. R., Heydt, G. T., "Transient Stability Assessment By Pattern Recognition In The Frequency Domain", IEEE/PES 1990 Winter Meeting.

[25] Sobajic, D. J., and Pao, Y. H., "Artificial Neural-Net Based Dynamic Security Assessment For Electric Power Systems," IEEE/PES 1988 Winter Meeting.

[26] Zhou, Q., "Sensitivity and UEP analysis of the Transient Energy Function Method," First Midwest Electro-Technology Conference, Iowa State University, Ames, Iowa, April 10-11, 1992. pp 3-7

[27] NeuralWorks Professional II: Neural Computing, NeuralWare, Inc, Pittsburgh, Pennsylvania, 1989

[28] NeuralWorks Professional II: User's Guide, NeuralWare, Inc, Pittsburgh, Pennsylvania, 1989