1990

Expert systems for security trend analysis of transient-voltage-limited power systems

S. Venkataraman
Iowa State University

Order Number 9100504

Expert systems for security trend analysis of transient-voltage-limited power systems

Venkataraman, S., Ph.D.

Iowa State University, 1990

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

Expert systems for security trend analysis of transient-voltage-limited power systems

by

S. Venkataraman

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: Computer Engineering

Approved:

Signature was redacted for privacy.

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

Members of the Committee:

Signature was redacted for privacy.

Iowa State University
Ames, Iowa
1990

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ACKNOWLEDGEMENTS

I would like to thank my major professors, Dr. A. A. Fouad and Dr. J. A. Davis for their invaluable guidance and encouragement throughout this work. Their professional enthusiasm motivated me to overcome the occasional difficulties during my research. The technical discussions with my major professors helped me develop my analytical skills. I am thankful to Dr. Fouad for providing financial support during my Ph.D. program and arranging my visits to important conferences connected to my research. I am grateful to the Electrical and Computer Engineering department for arranging visits to Northern States Power Company for data collection.

I would like to thank my committee members, Dr. A. V. Pohm, Dr. V. Vittal, Dr. G. M. Prabhu and Dr. E. Johnston for their contribution to my research. I would like to acknowledge Dr. J. Lamont's help on development of user interface of the expert system.

I am thankful to the Northern States Company (NSP) for supplying all the data for the development of the expert system. I would like to thank Mr. D. C. Don, Mr. Benedict G. Deutsch, Mr. Michael D. McMullen, Mr. Steve Larson and the power system operators of NSP for their help in building the knowledge base for the expert system.

The fellow graduate students in the power program at Iowa State University

provided a good research environment and made my work enjoyable. I want to thank my parents for their blessings and support. My special thanks to my wife Geetha, who helped me prepare this dissertation and provided moral support throughout the graduate program.

CHAPTER 1. INTRODUCTION

Power System Reliability

There is an increasing need for electrical energy in North America and also in the rest of the world. Modern society has become very dependent upon a reliable supply of electricity and the electric utility companies encompass this expectation in their planning and decision making. The North American Electric Reliability Council (NERC) defines *reliability* in a bulk power electric system as the degree to which the performance of the elements of that system results in power being delivered to customers within accepted standards and in the amount desired [1]. Bulk power electric system reliability can be addressed by considering two basic and functional aspects viz., *adequacy* and *security.*

Adequacy is defined as the ability of the bulk power system to supply the aggregate electric power and energy requirements of the customers at all times, taking into account scheduled and unscheduled outages of system components [1]. The bulk power system can build new sources of electrical energy to match the demand for energy. Electric utilities have a strongly interconnected power system network. They are connected to the neighboring utilities by tie-lines so that power can be transferred from utilities having excess power to the utilities requiring additional power. Thus, the import and export of electrical power among utilities may be used to meet

the demand for power. In an interconnected power system however, interdependence among member systems may impact system reliability. The reliability of the power network of an electric utility in a strongly connected power system depends on its system conditions, the system conditions of the neighboring utilities, and the connecting network. The utility may be affected by a remote utility even if both are not directly connected by a tie-line.

Power System Security

Power system security is currently one of the most important concerns in the electric utility industry. Power system security can be defined as the ability of the bulk power electric system to withstand a predetermined set of disturbances (sometimes referred to as contingencies). A *disturbance* may be defined as a sudden change to the system operating conditions or parameters. This change may take place as a result of a short circuit or a loss of one or more system component such as generators, loads, transmission lines, transformers, etc. [1]. If a power system is not secure, a situation may result where cascading outages occur, leading to a large-scale interruption (known as blackout).

During a blackout, a large area loses its supply of electrical energy, resulting in monetary losses for the electric utility and the customers in the entire area. The utility supplying electric power also incurs losses to equipment and the blackout may extend to neighboring utilities. To avoid cascading outages, electric utilities try to ensure that their power system is secure enough to withstand credible disturbances.

Dynamic System Security Assessment

Security assessment is the evaluation of available data to estimate the relative robustness (security level) of the system in its present state. Security of power systems can be broadly classified into dynamic and static security. Dynamic security of a power system deals with the power system in transition, following a disturbance, from an initial operating state to another steady-state condition. The objective of dynamic system security assessment (DSSA) is to ensure that the power system will survive any "relevant" disturbances. When power systems are heavily loaded, they become more vulnerable to disturbances. Thus, dynamic system security assessment is becoming increasingly important.

The electric utilities control the operation of their power systems within the guidelines provided by their respective reliability councils. The North American reliability councils are Mid-Continent Area Power Pool (MAPP), East Central Area Reliability Coordination Agreement (ECAR), Electric Reliability Council of Texas (ERCOT), Mid-Atlantic Area Council (MACC), Mid-America Interpool Network (MAIN), Northeast Power Coordinating Council (NPCC), Southeastern Electric Reliability Council (SERC), Southwest Power Pool (SPP), and Western Systems Coordinating Council (WSCC).

Usually, electric utilities are advised by the reliability councils to maintain the power system so that it is secure for the worst-case disturbance in the worst-case power system configuration. For a stability-limited power system, the power system is considered secure for a given system configuration if it remains stable for the disturbances specified by the reliability criteria. Thus, for a stability-limited power system, the security assessment involves stability analysis for different system configurations

and for different disturbances.

There is a large number of possible disturbances based on the loss of different system components. Even if we consider only single contingencies, the number of possible disturbances are as many as the number of system components. For multiple contingencies, this number is much larger. More over, because the power system's configuration keeps changing, all the different configurations must be considered for security assessment. Considering the combinations of different system components in operation, to determine possible system configurations will constitute 2^N different power system configurations, where N is the total number of system components. For a moderately sized system, the number of different system configurations could be on the order of a million. All of these configurations may not be of interest, but the set of network configurations studied for DSSA is a large subset of possible configurations. If one considers only the controllable parameters, the power system can have possible configurations equal to the number of controllable parameters multiplied by the allowable range of values for these parameters, which is an extremely large number. The minimum number of case studies required for DSSA is shown in Figure 1.1. Thus, we have to study transient stability for a large number of cases as described above, analyze the output data from all these case studies and organize them for further processing.

Each of the above mentioned cases is a transient stability study, which may be done by either time simulation techniques or by direct methods of transient stability analysis such as the transient energy function (TEF) method. When time simulation studies are used, the power system is represented by a set of differential and algebraic equations. The critical parameters such as bus voltages, generator angles, etc., are

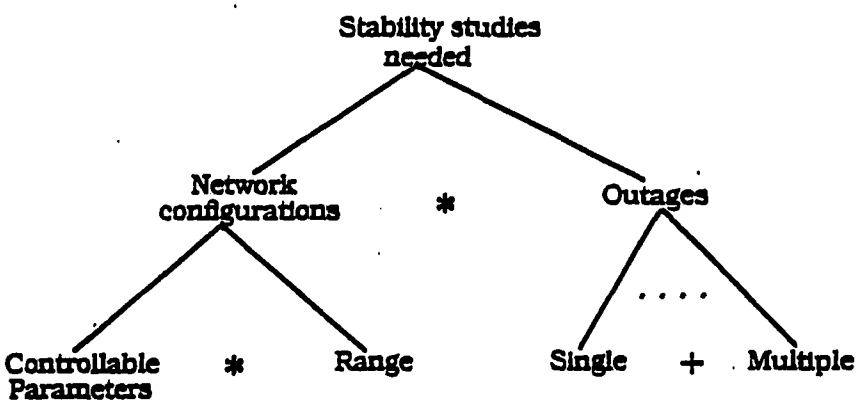

Figure 1.1: Transient stability studies for security analysis

solved for as a function of time and their values are monitored. The critical parameters should lie within the specified limits, during the transient. This method takes a long time for computation and gives only a "Yes" or "No" answer for stability. We need an assessment which can give a qualitative stability assessment of the power system for a given fault. This information may be used to reduce the number of case studies for DSSA. The TEF method, which is described in the next section, has this ability.

Transient Energy Function Method

The TEF method [2], computes the transient stability of the power system using direct methods based on Lyapunov's theory. This method of direct stability analysis involves calculating the post-disturbance equilibrium points of the system [2]. The equilibrium points of interest for transient stability analysis are the stable equilibrium point, θ^s, and the controlling (relevant) unstable equilibrium point (UEP), θ^u. For a multi-machine power system, the transient energy (V) is made up of two components: potential energy (PE) and kinetic energy (KE). The system transient energy, V, is evaluated with respect to the post-disturbance equilibrium conditions. Its critical value V_{cr}, is given by the value of potential energy at the controlling UEP V^u, for the particular disturbance under investigation.

The first swing stability assessment of the system is made by computing the difference between the value of V_{cl} at the end of the disturbance and V^u. Stability is maintained if $V_{cl} < V^u$, or if the energy margin $\Delta V > 0$, where$\Delta V = V^u - V_{cl}$; the converse is also true. The normalized energy margin provides a qualitative measure of the degree of system stability.

The TEF method represents a potentially powerful tool for helping power system operators [3, 4]. It has the ability to express the degree of system stability in terms of a quantified index (normalized energy margin). It also has the flexibility to obtain analytical sensitivity information, for the simulated contingencies, on how the energy margin is affected by varying system parameters and conditions. In addition, the method can give information on corrective and predictive actions needed to maintain security. These capabilities make the TEF method suited for dynamic security assessment.

Need for Trend Analysis

In general, electric utilities have a parameter which they uses as a measure of how secure the power system is during day-to-day operation. For stability-limited systems, such security indices used by different utilities can be tied to the normalized energy margin discussed in the previous section. To maintain safe operation, it is essential to compute and keep the security index within predetermined limits. To determine that the power system will be secure during a period in the future, it is necessary to know both the current level of security and how that level is affected by varying system conditions and external factors. Thus, it is important to study how this security index varies as time progresses. This study is known as the *trend analysis* of the security of a power system.

Trend analysis depends on the trend of the parameters which affect the security index. If the trend of the security index is known in advance, the vulnerability of the power system can be computed. Thus, the vulnerability of the system is a function of both current security index and its trend. If the vulnerability is known in advance,

the operator could take appropriate control actions to maintain the security of the power system. The control actions may be to change the values of some parameters, which affect the power system security. Thus, the security trend analysis gives the operator additional time for executing their control actions. With sufficient time, the operators can execute an economical operation of the power system and also ensure the system security.

To analyze the trend of power system security, the sensitivity analysis of the TEF method is needed. As mentioned before, there are various system conditions which may have an effect on the security index. Sensitivity analysis of the TEF method gives an insight as to how different parameters affect the security in different power system configurations. It gives a qualitative assessment that can be used as the additional intelligent information for making decisions. This extra dimension will reduce the number of stability studies for DSSA and for determining the trend.

Need for Artificial Intelligence Methods

There is a large number of transient stability studies conducted to obtain the operating limits for a transient stability-limited power system. The results from such studies form a large knowledge base which needs to be organized and presented to the operator in a concise form for making decisions. Power system operators will have to consider company policies on economic operations and other contractual obligations to customers. Sometimes they operate based on their earlier experience in power system operation and control. The above information/knowledge is in the form of heuristic rules which are not easily coded in an algorithmic procedure. These rules frequently change with company policies and power system conditions. Algorithmic

procedures usually need large software modifications for such changes, which is time consuming and is not economical. As an alternative, artificial intelligence (AI) methods are suitable for such a rule-based approach and they require little effort in terms of software changes for rule modifications.

AI methods are suggested for use in power system security analysis for the following reasons [5]:

- The organization and manipulation of a large knowledge base is done more efficiently than algorithmic methods. Operations such as selecting relevant data from the knowledge base, searching a large knowledge base, and updating the knowledge base are executed faster in AI based methods.

- AI methods are naturally suited for *learning*. Learning can be broadly defined as collection, correction and updating of knowledge as new experience is gained.

- Knowledge available in the form of heuristic rules can more easily be coded and modified using AI methods than using algorithmic methods.

There are various techniques used in AI, such as neural networks, pattern recognition and expert systems. *Neural networks* are a large interconnection of nodes, similar to neuron cells of human brain. Each of these nodes consist of a processor of limited computing capability, but they are interconnected and the knowledge is stored in the interconnection network [6]. A large and relevant database is required to make the system learn before system input can be processed. Neural networks are difficult to implement and they are very domain-specific. They are not flexible for modifications and they may not always converge to the required result. *Pattern*

recognition also has implementation problems. The collection of knowledge is from past statistics/results and the learning process is not continuous.

All the above methods are more suited for "Yes" or "No" type answers, or require special programming and compromises to achieve both quantitative and qualitative answers. These methods are not economical because both hardware and software costs are incurred. Some of the above methods are less flexible for modifications and may prove expensive. On the other hand, *expert systems* are software based, flexible and economical. They are well suited for the DSSA problem.

Thesis Organization

The next chapter gives introduction to expert system applications and briefly describes some of the power system applications relevant to the project. It also gives information regarding hardware and software requirements for expert systems. Design details for building an expert system for power system security analysis are described in the third chapter. It contains an application of the technique for a transient-voltage-limited power system. The last chapter has the conclusions of the project and some suggestions for future work.

CHAPTER 2. USE OF EXPERT SYSTEMS FOR POWER SYSTEM APPLICATIONS

Expert Systems

Among the various techniques in AI, the knowledge-based expert system has been the most successful technique for practical implementation. In the simplest form, an *expert system* is one that handles real world problems using a computer to reach the same conclusions as would a human expert faced with a comparable problem [7]. An expert system is defined as a program that will perform at the level of a human expert within a specific and limited task domain [7].

In power system security analysis, the results from off-line stability studies form a large knowledge base; by consulting and manipulating this knowledge base the security of the power system is determined. The available knowledge on the load trends and weather are used to determine the trend of the system security. The knowledge base needs to be organized for easy reference, which can be done using expert system techniques. Furthermore, the power system operator's experience can be incorporated in the form of heuristic rules efficiently using expert system techniques. The potential of expert system techniques is evident from research in the field, since several computationally-intensive problems that were thought to be untractable problems have been solved using these techniques. Expert systems are gaining acceptance

in greater numbers in almost every area of human endeavor.

Sample Applications

Expert system techniques have been used for various power system applications since 1960. Practical implementations have been documented in areas such as alarm processing [8, 9], reactive power and voltage control [10, 11], power system trouble analysis [12], unit commitment [13], load forecast [13], isolation of line section faults [14], contingency screening [15], restoration and loss reduction of distribution systems [16], etc. These applications are interrelated and are used with existing Energy Management System (EMS) Software. The expert system for power system security analysis developed in this project uses key concepts from contingency screening, load forecasting and reactive voltage power and voltage control. The following sections briefly describe expert systems in these areas and some of the key concepts common to expert systems for security trend analysis.

Intelligent Alarm Processing

When a disturbance occurs, power system operators are usually flooded with numerous alarm messages. Based on their importance, some alarm messages can be ignored since they are redundant. Usually, the operators use a combination of extensive analysis and some reasoning, i.e., heuristic rules based on their experience to decipher the exact condition of the power system from the alarm messages. It is important that this process be expedited so that the operator can cope with the situation and execute control actions promptly.

An intelligent alarm processor [8] is an expert system dedicated to continuous

analysis of the alarm messages and reports the resultant system conditions instead of simply listing the alarm messages. The knowledge and experience of the operators in analyzing the alarms is incorporated into the expert system, which gives it the ability to present concise and relevant information regarding the system conditions. Expert systems for alarm processing have been built by Northern States Power Company, Consolidated Edison Company, and some European power companies. The key concept common to these expert systems is capturing the operator's experience and available knowledge on the alarm messages.

Reactive Power and Voltage Control

In this area, expert systems are used to detect voltage violations and other voltage-related problems. After a fault is detected, the expert systems arrive at a control scheme to correct the voltage problems [10]. To improve the voltage of a specific bus, operators use empirical rules and carry out a set of control actions, including:

- removal or insertion of shunt capacitors
- adjusting tap-changers in transformers
- controlling some generator voltages
- adjusting synchronous condensers.

In a normal operating situations, the operators rely on their experience and knowledge of the power system to design and execute the necessary combination of control actions. However, in an emergency situation, the power system operators will have

to make quick decisions to produce the right set of control actions. Expert systems can aid the operators by quickly producing a prioritized list of possible control actions that the operator can choose from. Expert systems for reactive power and voltage control have a knowledge base containing information about critical bus locations and the corresponding set of control actions to adjust their voltages, based on the system configuration. The output of the expert system is a list of control actions which even an inexperienced operator can follow. In the on-line mode, expert systems in this area take their input values from the Supervisory Control and Data Aquisition System (SCADA) and the existing EMS. The expert system for power system security described in this dissertation, uses control actions similar to the control actions used by expert systems for voltage control.

Isolation of Line Section Faults

During faults, automatic switches installed in electric utility systems between power circuit breakers in a transmission line are used to isolate the faulted section. Often, the operation of the automatic switches does not completely isolate the fault. Sometimes, a larger section of the power system than is necessary to isolate the fault loses supply of electrical energy when the fault is cleared. System operators then use their judgement and experience to decide on an economic way to isolate the fault. Electric utilities give preference in supplying electrical energy to customers bound by contracts and other critical customers, even if it is not economical. System operators apply reasoning and heuristic rules based on their experience to determine a set of actions which will isolate the minimum fault section.

Expert system prototypes are available for isolation of line section faults, which

have in their knowledge base the reasoning and the heuristic rules used by the operators [14]. This helps in maximizing the area of power availability. Rules are developed to take care of the critical customers and supply them with electrical energy. The knowledge aquisition scheme used by the expert systems in this area involves interaction with power system operators, engineers and planners. A similar procedure is used for developing the expert system for security trend analysis.

Load Forecast and Unit Commitment

Software packages are available for load forecasting, which use previous loading trend, weather forecast, and current power system conditions to determine the current loading load for a given day. Unit commitment packages use the result of a load forecasting program, economy factors, and some company policies to find level of generation required to meet the loading trend. Due to changing company policies, economy issues, parameters affecting the load forecast, etc., these software packages are modified frequently. If algorithmic programs are used, it will be difficult and time consuming to incorporate those changes. Load forecasting cannot be modeled precisely in mathematical form as it involves external weather factors such as temperature, humidity, illumination, wind speed, continuous cold front, continuous warm front, rain, snow, storms, etc.

The expert systems in this area use the standard information, as well as other heuristic rules specific to the power system and some probability factors [13]. They have a large knowledge base consisting of load trend information, weather data, sensitivities of the weather parameters on the load trend, etc. The heuristic rules are normally used for economic reasons, company policies and contracts with customers

and neighboring utilities. The rules are used to capture the experience and knowledge of the power system operator on load trends. The expert system for security trend analysis described in this dissertation computes the loading trend using a similar procedure.

Computing Environments for Expert Systems

The computing environment of the expert systems built so far have many similarities. The main components of expert systems are the user interface, the knowledge base and the inference engine. These components of expert systems can be designed in different formats, depending on the hardware and software requirements of the applications.

Hardware Requirements

There are two main options to consider in choosing computer system hardware for an expert system. The expert system may either be developed as a stand-alone dedicated computer, or integrated into the computer system currently used by the power utility company. The important factors considered in choosing a computer system for supporting expert system applications in the power area are:

- If the expert system runs on a separate computer system, it should be capable of communicating with the existing computer systems. This is essential as the expert system has to collect and transfer data from the computer systems already in use at power utilities. It is often very difficult to provide the necessary communication facilities.

- The computer system should support efficient search facilities for accessing the knowledge base. It also should support rule selection strategies for selecting the relevant rule from a conflict set.

- The computer system should have a large memory to accommodate the knowledge base. Availability of interactive environment and some graphic support are needed for efficient user interface.

As mentioned before, the expert system can be a part of the Energy Management System. In this type of implementation, the access to data for the expert system is easily available, but the computing effort required by the expert system may reduce the efficiency of the energy management system. Hardware cost is usually low for extra memory but software cost can be high. It will be ideal to incorporate the expert system in the dispatcher training simulator as it has access to all the power system data and yet will not reduce the speed performance of the existing energy management software [17].

If the expert system is built in a separate computer system, the on-line data is made available through communication links. The communication complexity involved in providing knowledge and data from the host system, may reduce the speed performance of the expert system. This will be offset by the performance improvement due to the available special facilities for the expert system. When a separate computer system is provided, it will not reduce the efficiency of the energy management system in the host computer. Moreover, software issues will be less stringent during the development stages of the expert system as additional supports specific to expert systems are available. Modifications to the expert system, during testing

stage will not affect the host computer performance. In this dissertation, the expert system is developed in a stand alone computer environment.

Software Requirements

Languages: A wide spectrum of computer languages are used in building expert systems. Some of the popular languages used are Lisp, PROLOG, c, FORTRAN and Pascal. Lisp has been used for expert system application for more than twenty-five years because it allows easy manipulation of data at a symbolic, abstract level. PROLOG is useful for logic programming and has both backward chaining and forward chaining rule-based programming capability. FORTRAN is popular as most power system application software is written in this language and very often expert systems require interfacing to the available software. The programming languages Pascal and c support structured programming. The c language is a general purpose programming language and it combines the elements of high-level languages with the functionalism of an assembly level language. The c language matches the capabilities of different computers and is highly portable. Many expert system shells are written in c and the language has capabilities to invoke software written in other programming languages. An advanced version, C++ has object oriented programming capabilities suitable for expert system applications. In this project the expert system is designed using the c language to achieve programming convenience and portability.

Shells: In most expert systems, the rules are evaluated sequentially in the absence of a specific rule selection control strategy. This does not give any flexibility in adding rules or knowledge. Some expert systems have a special environment or a shell such as

ART, KEE, OPS5, OPS83, PCPLUS, etc., which provide additional control strategies for rule selection. In this environment, a rule is chosen from a conflict set, (containing rules whose conditions are satisfied) using a predetermined control strategy. This gives the flexibility in adding rules when new knowledge is acquired. The additional rules will be considered along with the existing ones. Standard shells are not used in the expert system developed for this dissertation as they are not easily portable. Moreover, standard shells are not cost-effective and have limited user interface. In the security trend analysis expert system, rule selection is built into the code.

User Interface

The most important part of any expert system is its user interface. The expert system should provide a comfortable interface for the user. If we use an expert system with standard shells, then the interface will be limited to the facilities provided by that shell. This project uses no such standard shell and provides an interface suitable to the power system operator's needs for graphic support and an interactive environment.

- Graphical Support: Whenever a trend analysis is made, it is convenient if the raw data is accompanied by a graphical representation. This helps processing of data efficiently.

- Interactive Environment: The designed expert system can be used by the power system operators as a study tool as they can change values of different parameters and analyze their effect. This is made possible by providing an interactive environment with screen control programming. A scheme for continuous and non-interactive operation is also suggested.

The expert system for security trend analysis was developed in the language c on an AT&T 3B2/1000 (UNIX system V), a SUN SPARC I station (UNIX, SUNOS 4.0), and an IBM PC (MS-DOS).

CHAPTER 3. PROJECT DESCRIPTION

Project Objectives

The objective of this dissertation is to investigate the use of expert system technology for power system security trend analysis and to demonstrate the associated knowledge base structure and other development aspects of expert system applications. The expert system designed will provide a valuable demonstration of potential application of the technique in the area of dynamic system security assessment using the TEF method results. The results should also contribute to establishing the proper framework for more general development and implementation of expert systems in various phases of Energy Management Systems of a stability-limited power network [3, 4].

Approach Followed

When the TEF method is used for power system transient stability assessment, the normalized transient energy margin ΔV gives a quantitative as well as a qualitative assessment of the degree of stability (or instability). Thus, the manner in which ΔV is affected by the changes in the key operating parameters can be used for assessment of power system security.

Use of ΔV to assess system security is illustrated in Figure 3.1 and Figure 3.2 [3,

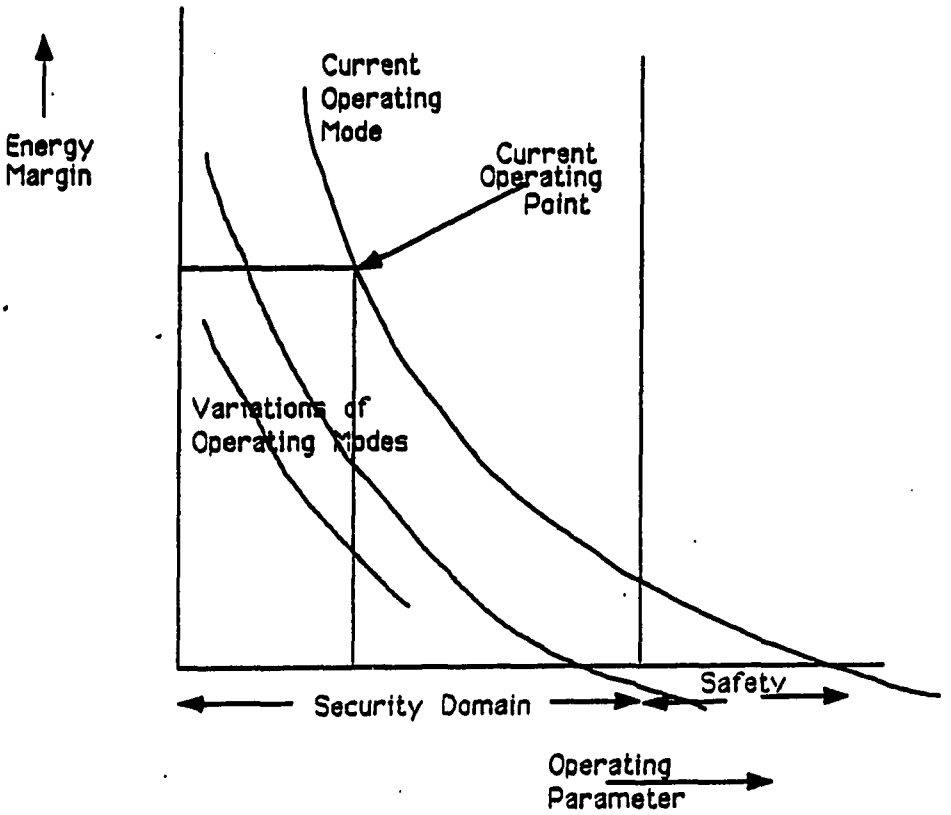

Figure 3.1: Sensitivity analysis with a single parameter

4]. Figure 3.1 shows the variation of ΔV with respect to one critical parameter; in this case the power flow on a key transmission interface (one of the operating parameters of a power system affecting security). When the operating mode changes, the variations of ΔV with respect the interface flow also changes as indicated by the dotted lines in the Figure 3.1. The security domain for the current operating mode in Figure 3.1 is based on a safety cushion predefined by the company policy.

Figure 3.2 shows the security domain as a function of two such operating parameters which influence security. The operating point is chosen so that it is within the security domain for both the operating parameters. When more operating parameters are considered, the problem of finding a security domain satisfying security constraints for all parameters becomes more complex.

Moreover, the variations of ΔV for an operating parameter may be different for different operating regimes. An operating regime may be secure for some modes of operation (for example, current operating mode) but vulnerable with respect to some future operating condition. Figure 3.3 shows two operating regimes which are presumed to be equally secure (i.e., initially both have equal ΔV). Regime 1 may represent current operating mode and regime 2 may represent operating conditions after changes to other operating parameters (e.g., power flows, generation availability, weather concerns, loading, etc.). In regime 2, the value of ΔV is more sensitive to changes in values of the operating parameter than in regime 1 as shown in Figure 3.3. In other words, the sensitivity of the operating parameter on ΔV is higher for regime 2 than regime 1. This rate of change of security is used as a measure of the vulnerability [3, 4]. Thus, the vulnerability of a power system is computed by analyzing the trend of the system security index ΔV. System security is often

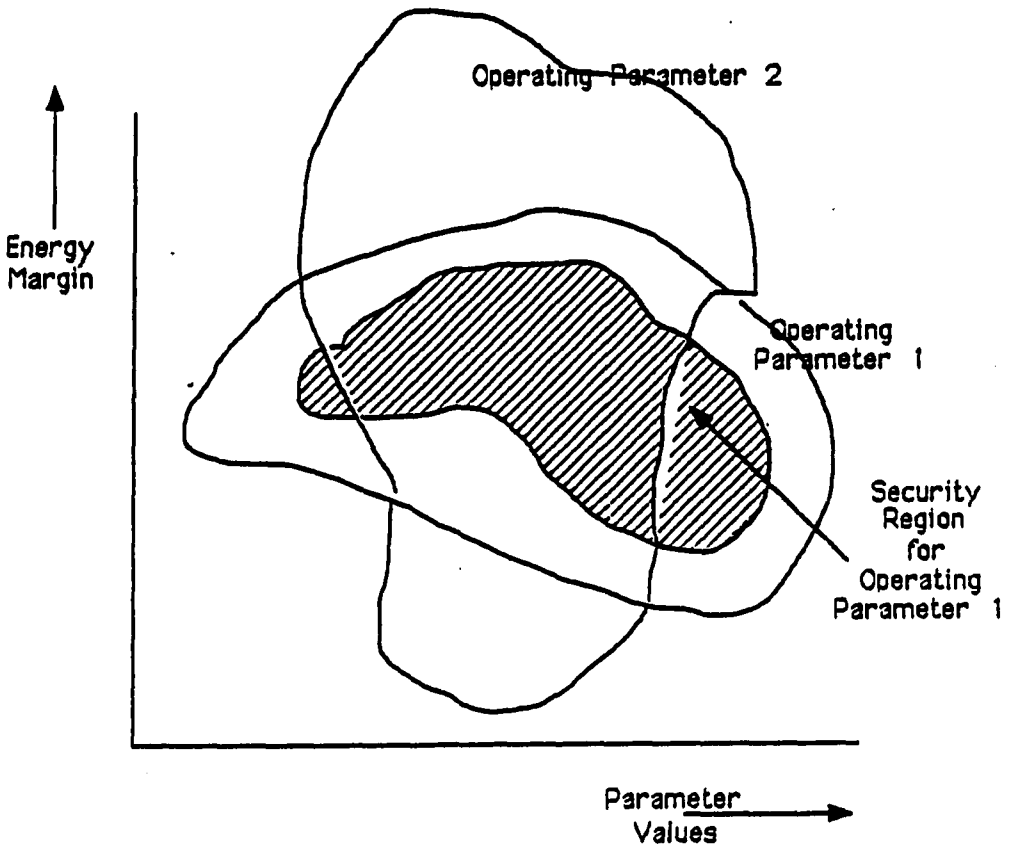

Figure 3.2: Sensitivity analysis with two parameters

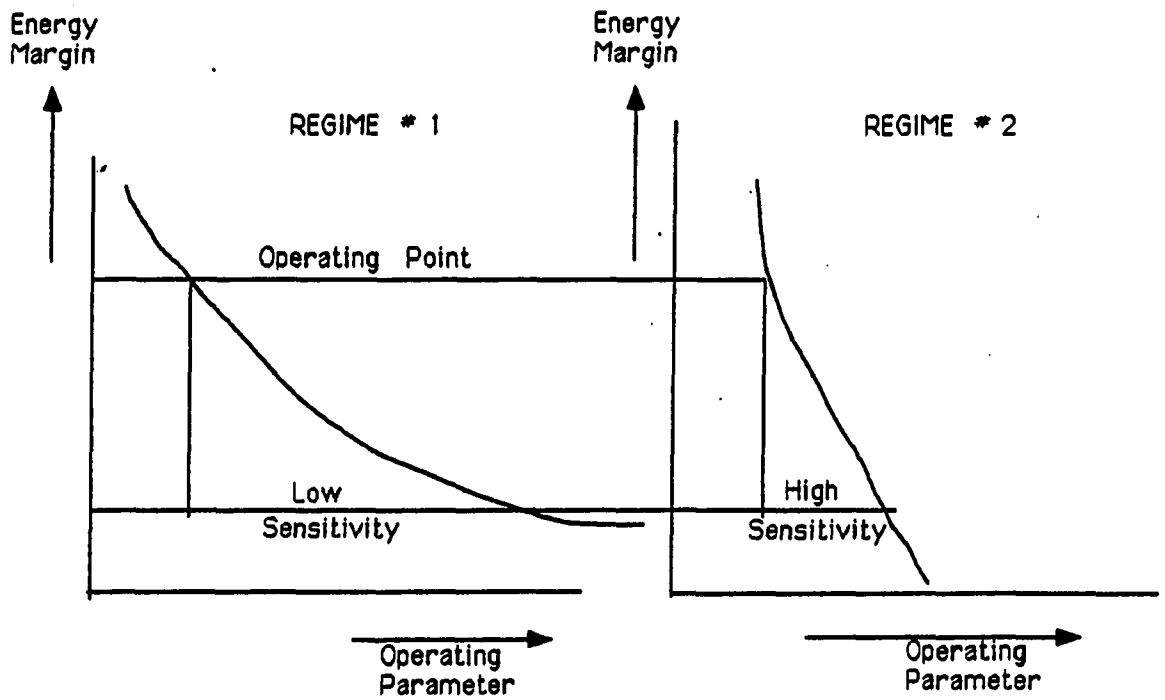

Figure 3.3: Sensitivity and system vulnerability

related to (or measured by) the following criteria:

- Degree of system strength, as indicated by the critical energy V_{cr}
- Severity of a disturbance, as indicated by the energy at fault clearing V_{cl}
- Probability of that disturbance.

Thus, the system security depends on the current system configuration and the expected disturbances. Often the power system operators are also interested in the trend of the system security, i.e., in-system vulnerability. System vulnerability is often related to the following criteria [3, 4]:

- Sensitivity of a security index to changes in one or more operating parameters. For example, if we consider an operating parameter "p," the sensitivity is given by: (ΔEnergy Margin / Δp).
- Next contingency environment. The system may survive a particular disturbance but may not be secure for the next possible single or double contingency.
- Difficulty of consequent restoration. A disturbance may have a relatively smaller impact on the security than other disturbances but is more difficult to deal with from the system restoration point of view.

Electric utilities use different security indices to suit their power system reliability requirements. The normalized energy margin ΔV, computed by the TEF method can be correlated to these security indices, and a corresponding correlation function can be developed. The sensitivity analysis procedures of the TEF method compute the sensitivities of the energy margin ΔV to changes in selected system parameters.

Thus, the effect of these parameters on the system security can be computed. These sensitivities can also be used to find the trend of the security index and compute the vulnerability of the power system. Thus, if the trend of the control parameters and the sensitivities are known the trend of the security index can be calculated. In addition, the trend of the control parameters can be used to keep the security index at a pre-determined safe value depending on the company policies and procedures.

The development of expert systems for trend analysis of the security index will be different for different electric utilities. The structure of the expert system will depend primarily on the choice of security index used by the respective electric utility. The operator requirements in DSSA which can be addressed by expert system techniques will be different and have to be identified. The following tasks are required for developing an expert system:

- Problem identification
- Collection of data and knowledge
- Design of the expert system components
- Verification and validation of the expert system's decisions
- Results and discussions.

In the next section, the above mentioned tasks are demonstrated by the design and implementation of a sample expert system for security trend analysis of a transient-voltage-limited power network.

Application to a Transient-Voltage-Limited Power Network

The expert system developed is based on conditions encountered in the Northern States Power Company (NSP), of Minneapolis, Minnesota, in the mid-1980s. The data used in this dissertation was obtained from a number of reports received from NSP by an IEEE Power Engineering Society working group [18, 19]. These reports explain the dynamic security assessment practices at NSP and how this electric utility derived operating security limits for transient voltage-limited conditions. The data collected from the reports and from the power system operators at NSP are intended to illustrate the procedure for deriving the operating security limits for a typical, yet hypothetical operating condition.

System Description

The 345 KV system of NSP is shown in Figure 3.4. A network of 115 KV lines located at the Twin Cities area transmits power through the three 345 KV lines. The power (MW) flows on key lines and generators (in large numbers) and important reactive power (MVAR) flows (in smaller numbers) are shown in Figure 3.4.

Generation and Tie Line Flows: A large amount of power is produced in the northwestern portion of the 345 KV loop. The total generation input into the northwest area is from Sherco power plant (2350 MW), Monticello power plant (600 MW) and C.U-D.C. line (1000 MW). Together they are called as the "West Side Generation" (WSG). On the East side of the Twin Cities 345 KV loop, there is a base loaded nuclear plant at Prairie Island capable of producing 1000 MW. King is another low operating cost, coal fired plant in the East side capable of producing 550 MW. There

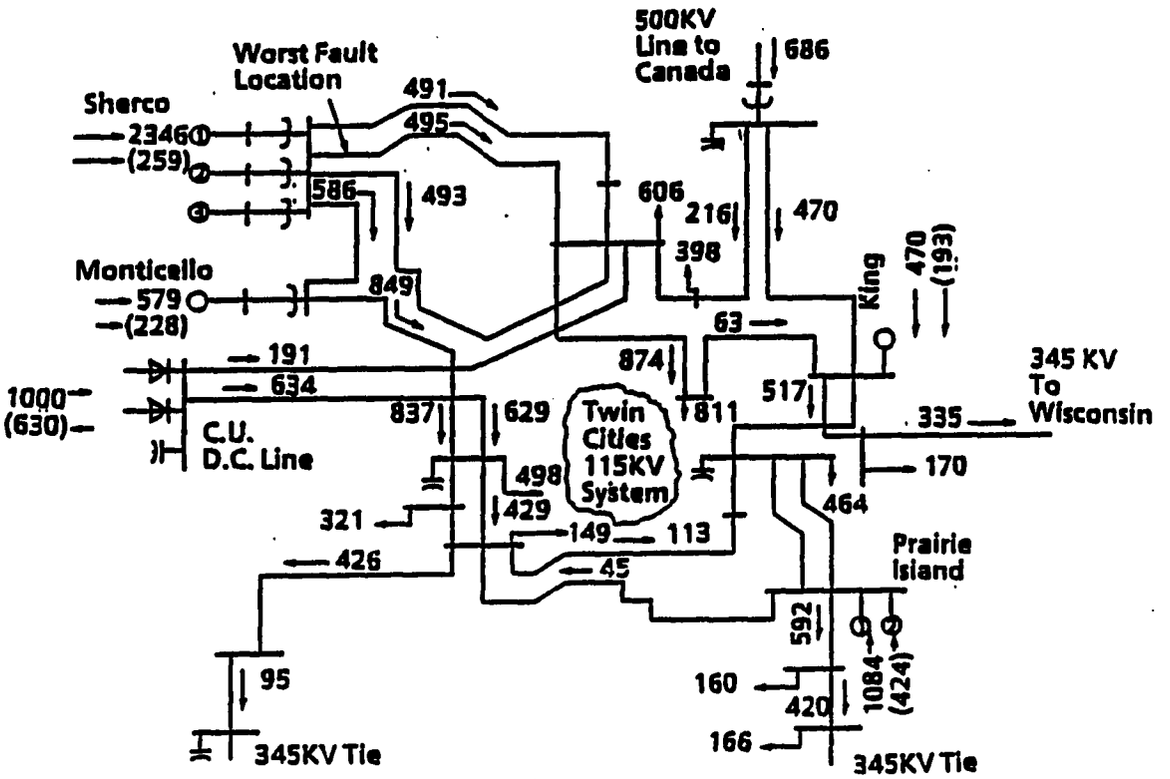

Figure 3.4: NSP Twin Cities 345 KV loop

are intermediate to high cost, oil-fired generating units located in the central Twin Cities 115 KV system. These central 115 KV and eastern 345 KV generating units are called "East Side Generation" (ESG). Inertia of the East side generating units has considerable influence on the transient stability characteristics of the system (higher inertia is beneficial).

There is a 500 KV tie line from Manitoba to the North of the 345 KV loop, with a capacity of 1000 MW flow. The power flow through this line also affects the system transient stability and will be referred to as the "Manitoba lineflow" (MAN). There are three 345 KV tie lines from the Twin Cities area, typically carrying 500-1500 MW of power. The power flow through these lines is called the "Twin Cities Export" (TCEX). Two of the 345 KV lines are located in the South and the third line delivers power to the East.

Problem Identification

Experience (supported by analysis) indicates that it is required to have a balance between the West side generation and East side generation, since the inertia of the East side generation is an important factor for maintaining stability. For certain disturbances, the transient voltage dip may be large enough to cause tripping of the Prairie Island power plant. This may lead to severe reactive power deficiency causing voltage collapse. Large economic generating plants are located in the West side, while the East side generators are smaller and some of them have higher cost of generation. The WSG, ESG, MAN, power flows on the tie lines, generation and line outage conditions and loading are some of the factors which influence the transient stability.

The major stability criteria are based on the bus voltage at the Prairie Island nuclear power plant. Following a disturbance, if the transient-voltage at this bus dips below 78% for a period of "one" second, the reactor coolant pump is set to trip and this in turn will trip the Prairie Island plant. Thus, 1000 MW of power, as well as the reactive power needed for voltage support will be lost suddenly. This would cause cascading outages which will result in a blackout.

It was found from experience that the stability problem is the greatest at 75% loading situations. The East side generators with high generation cost are shut off during such loading, thus creating an imbalance in the inertia. During high loading situations, all the available generators are switched on including the East side units, resulting in a better inertia balancing situation.

Security Index: The utility regularly conducts stability studies to avoid the transient-voltage stability problem previously described. At present, the security level of NSP is indicated by a parameter called the Twin Cities export margin (TCEM). The TCEM is calculated using the instantaneous values of control parameters viz.:

- West side generation (WSG).
- East side generation (ESG).
- Manitoba flow (MAN).
- Power import (IMP).
- Line outage.
- Generation outage.

The stability calculations conducted off-line computes the allowable export from Twin Cities for a base case system configuration and a given combination of line and generator outages. This information is stored in a stability table shown in Table 3.1. Each of the values shown in the table, is the Twin Cities export limit which corresponds to a combination of line and generation outage and is calculated by several time simulation stability studies. The number of stability studies will be reduced to two per entry when the TEF method with sensitivity techniques is used.

The final export limit is computed using the value from the stability table corresponding to the combination of line and generation outage condition and applying sensitivity factors to correct for the current values of the control parameters. To compute the security index TCEM, the actual Twin Cities export is subtracted from the export limit. TCEM gives a measure of how much additional export of power is allowable through the three 345 KV tie lines from the Twin Cities without experiencing stability problems.

At present, the power system operators at NSP refer to a display which computes the instantaneous value of the security index. They do not have an opportunity to study the effect of changes in the control parameter values on the TCEM. The operators are more concerned with knowing the trend of this security index, when the system conditions and the external conditions change. If the trend of the security index is known in advance they can adjust the control parameters taking into account both the economic and security constraints. Thus the problem to be solved consists of:

- Computing the security index, TCEM.
- Studying the effects of control parameters on TCEM.

Table 3.1: Stability table

Line Outage	Normal	Only one unit off			Two Units off line		
					SHC or MNN off and		
	Base Units On	SHC or MNN Off	PRI or ASK Off	RIV 8 Off	SHC or MNN Off	PRI or ASK Off	RIV 8 Off
INTACT	1050	1390	535	735	1390	980	1210
ASK-CNN	545	1000	340	545			
ASK-ECL	200	74	60	200			
ASK-RRK	430	1045	285	430			
ASK-TER	220	1055	210	220			
BLL-IVH	670	1150	535	670			
BLL-WLM	415	875	225	415			
BUl-CNC	-120	925	-290	-120			
BYN-ADM	315	660	190	315			
CNC-DKN	385	525	115	385			
CNC-KOL	380	1120	180	380			
CNC-TER	810	600					
DKN-PKL	-695	405	-830	-695			
ECL-ARP	445	830	360	445			
EDP-BLL	665	1145	465	665			
KOL-CHI	630	1205	465	630			
MNN-PKL	-320	645	-390	-320			
MNN-SHC	660	430	490	660			
PKL-BLL	665	1145	465	665			
PKL-EDP	660	1140	495	660			
PRI-BLL	600	1150	470	600			
PRI-BYN	125	555	10	125			
RRK-IVH	605	1120	470	605			
RRK-PRI1	670	1150	470	670			
RRK-PRI2	670	1150	470	670			
SHC-BUL	-585	865	-725	-585			
SHC-CNC1	-485	865	-655	-485			
SHC-CNC2	-485	865	-655	-485			
WLM-LAJ	470	970	395	470			

- Correcting or fine tuning the sensitivities used with sensitivity analysis of TEF.
- Computing the trend of the security index, given the trend of the control parameters.
- Suggesting the changes in values of control parameters, which will satisfy economy as well as security constraints.

Collection of Knowledge

The operations planning group at NSP provided data from the results of off-line transient stability studies, and the information on the sensitivities of the control parameters which they use to compute the transient stability limits for other values of the parameters not shown in the Table 3.1. Power system operators at NSP, provided information regarding their security concerns, the different control actions they execute to keep the security index at safe level, their experience on the trend of total NSP loading, weather trend and information on economic constraints viz., customer contracts, cost of generation and import, etc.

It was found that the loading trend formed the basis for the trend of the control parameters which affect the security. Typical NSP loading for different week days in the month of January is shown in the Figure 3.5. The trend of the control parameters will be affected by the load fluctuations. The information on the previous year's total NSP loading, weather patterns, trend of control parameters, the stability results for selected line and generation outage situations etc., were available from the database maintained by NSP Control Center. Information on the control procedures used by operators was collected by observing them during regular operation and questioning

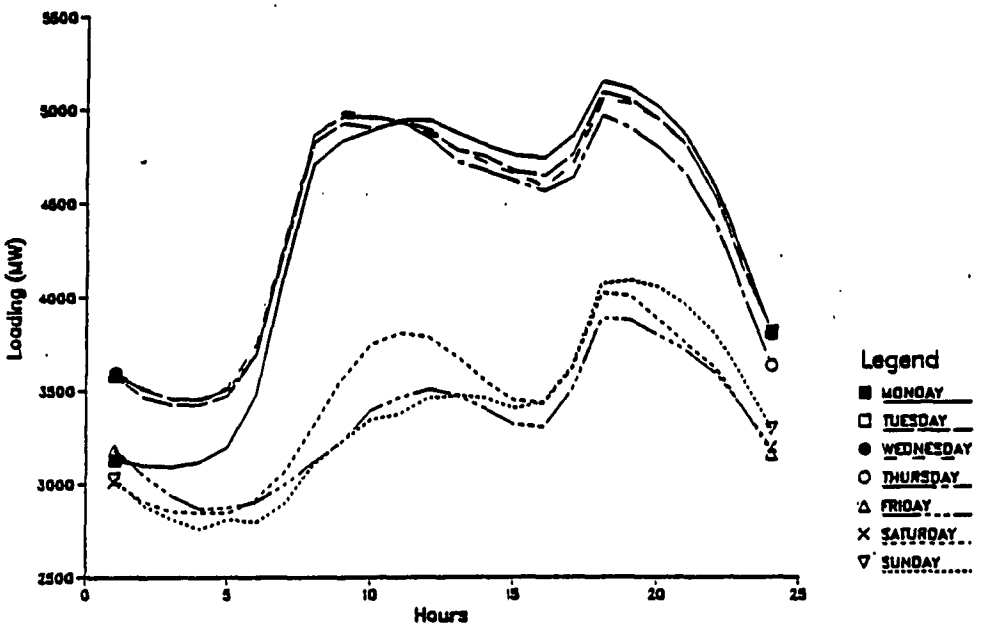

Figure 3.5: Loading trend

them about some hypothetical system configurations. The power system operators and the operations planning group of NSP expressed their requirements on the user interface component of the expert system. The NSP Control Center personnel helped at every stage to provide all the information needed to organize the knowledge base of the expert system.

Expert System Components

This section contains information on the components of an expert system and how they are designed for the NSP expert system. The three major components of any expert system are:

- User interface.
- Knowledge base.
- Inference engine.

User Interface: A user interface provides interactive facilities for the user to operate the expert system efficiently. An interactive system has both advantages and disadvantages. Interactive systems may reduce overall speed performance, can hide the big picture from the user and may demand more work from the user. At the same time, it provides the user with the ability to have control over the execution of the expert system by modifying working memory. During the design stage, it is difficult to decide what portion of the system should be interactive. Initially, interactive data transfer was employed for all inputs. During the testing and implementation stages, some of these interactive sessions were substituted with direct data transfer using files or other hardware-based communications. Parameters which can be measured

need not be entered interactively but if a change in the parameter is to be studied, then the user is provided with facilities to change the parameter value and analyze the effect. This is achieved by screen-oriented programming with cursor control facilities available in the standard graphics packages (e.g., UNIX curses software). The requirements of operators and the stability experts were considered to decide on the level of interaction so that the proposed system executes all the required tasks with minimum compromise on execution speed.

During an emergency situation, the power system operators usually have a lot of data to process and understand in a short time. If the output is not well organized, it will be more difficult for the power system operator to compare and comprehend different situations. Thus, graphical representation of the result is required for comparing different data. The projected parameter values are given in a tabular form on a hourly basis, similar to the displays used in the existing EMS software. With a stand-alone computing environment for the expert system, hardware with advanced graphic facilities could be chosen. The overhead of computing time due to graphics will not affect the host computer. In developing the cursor control schemes and graphic support portability of the software was given consideration. The expert system uses standard software packages [20] so the resultant software is portable in both mainframe and PC environment.

Knowledge base: The knowledge base for the expert system contains mostly the data collected from the previous experience. Every year, the utility measures the loading trend and the trend for the security index. These documented data are updated continuously whenever modifications to the data are necessary. In a continuous running

mode for the expert system, data are available for the previous one year period at any instant. In the initial design, the year was divided into four seasons and the days were classified as working day, holiday and special holiday. In the final implementation, each week day was treated separately. The previous year's data are considered along with the existing current trend corrected accordingly. Sensitivity factors are used to make the adjustments for the current trend (increased loading, low imports, heat wave, cold wave, etc.) in the final computed values. These factors are the values currently used by the forecasting division of NSP.

The sensitivity of the stability results to the changes in the parameters influencing the system security is stored in the working memory with the other sensitivity factors used in the calculation of the loading trend. Some of the sensitivities are obtained by off-line stability studies and some of them are computed by analyzing the power system from past experience. The second type of sensitivity often requires changes when the company policies change and are updated when necessary.

Heuristic Rules: The rules form the core of the expert system and along with the rule selection strategies as they provide the control for the execution of the expert system. For a good expert system, the rules should be flexible so that adding and deleting rules is easily done. The following are some of the rules for adjusting the control parameters, given the current values of the parameters, security level and the load trend. Each rule corresponds to a path in the decision tree shown in Figure 3.6. The expert system tries to match the system conditions to satisfy the conditions in the rules. Rules with conditions satisfied are put in a conflict set and one rule among the conflict set is chosen by the expert system for execution. In the NSP expert system

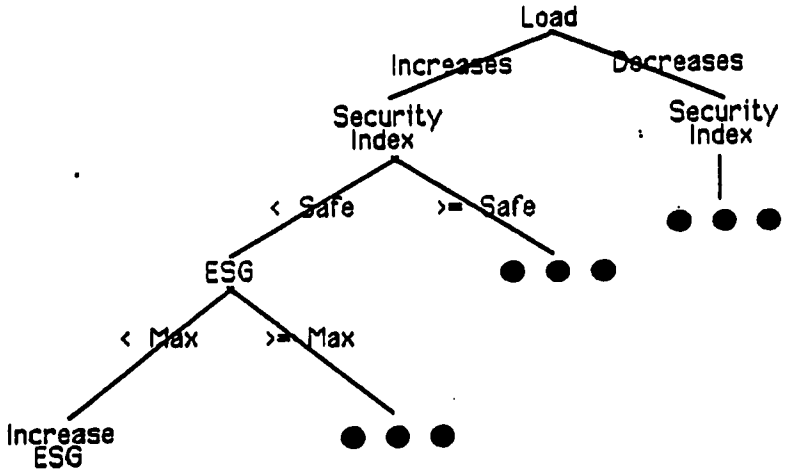

Figure 3.6: Decision tree for load fluctuations

system the rules are chosen from the conflict set and executed sequentially.

- *If* (Load increases) and (TCEM < safe level) and (ESG < Maximum ESG)
  - *then* Increase ESG.
- *If* (Load increases) and (TCEM < safe level) and (ESG ≥ Maximum ESG)
  - *then* Increase IMP.
- *If* (Load increases) and (TCEM < safe level) and (ESG ≥ Maximum ESG) and (MAN < Maximum MAN)
  - *then* Increase MAN.
- *If* (Load increases) and (TCEM ≥ safe level)
  - *then* Increase Sherco Generation along with ESG.
- *If* (Load increases) and (TCEM ≥ safe level) and (Sherco Generation ≥ Maximum Sherco)
  - *then* Increase MAN along with ESG.
- *If* (Load increases) and (TCEM ≥ safe level) and (Sherco Generation ≥ Maximum Sherco) and (MAN ≥ Maximum MAN)
  - *then* Increase IMP.
- *If* (Load decreases) and (TCEM < safe level) and (Sherco Generation > Minimum Sherco)
  - *then* Decrease Sherco Generation.
- *If* (Load decreases) and (TCEM < safe level) and (Sherco Generation ≤ Minimum Sherco)
  - *then* Decrease Import.
- *If* (Load decreases) and (TCEM ≥ safe level) and (ESG > Minimum ESG)
  - *then* Reduce ESG.

- *If* (Load decreases) and (TCEM $\geq$ safe level) and (ESG $\leq$ Minimum ESG) and (IMP > Minimum IMP)
  - *then* Decrease IMP.
- *If* (Load decreases) and (TCEM $\geq$ safe value) and (ESG $\leq$ Minimum ESG) and (IMP $\leq$ Minimum IMP)
  - *then* Decrease MAN and Sherco Generation.

In the above list of rules is a subset of a number of rules used for adjusting the control parameters. The minimum, maximum and safe values mentioned in the rules are variables which depend on the system conditions and are updated whenever they change. The *then* clauses of the above rules are procedures which suggest increase or decrease in the value of the control parameter taking into consideration the minimum or maximum permissible values, sensitivity factors and economy constraints. Typically, the rules will match existing system configuration and retrieve data (knowledge stored on the basis of previous experience) corresponding to the configurations. The result is corrected based on the forecast, and other current information using a set of sensitivities of the parameters. The control actions are selected by a similar set of rules as shown above and are executed by the *then* part of the rules. The rules select a set of optimum values for the controllable parameters taking into account the security constraints and some known economic constraints. This is used as a reference by the operators to decide on adjusting power generation and imports. The data, the rules and procedures for executing control actions form the knowledge base.

Inference engine: The intelligent part of the expert system having a problem solving ability is called the inference engine. Problem solving can be achieved by either forward chaining (bottom up) technique or by backward chaining (top down) technique.

When forward chaining technique is used, the expert system reaches a goal starting from given input information. An expert system with backward chaining technique, starts with the overall goal, break down goals into simpler subgoals until the result is a collection of goals, each of which is either immediately attainable or at worst as simple as possible.

The expert system designed for the NSP problem has a mixture of both techniques. The main goals are solved by backward chaining, whereas the subgoals are solved using forward chaining. The duties of the inference engine may include the following [7]:

- recognizing immediately achievable goals.
- expanding goals (not immediately achievable) into simpler goals.
- taking necessary action to achieve primitive goals (for example, by querying the user or executing known procedures).
- breaking up solutions of subgoals to yield a solution to the main goal.
- maintaining a goal tree from which the explanation of the decision making process can be derived.
- facilitate learning process.

Since the NSP expert system does not use any standard expert system shell, the inference engine is built inside the code. The goal selection and control is achieved by organizing the rules and using priority factors. The expert system does not maintain a goal tree, but provides a comprehensive result display and facilities for the user to

correct the results and re-use the corrected result as the new data. The inference engine has both supervised and unsupervised learning.

Learning is provided by changes to knowledge base and some part of the inference engine itself such that the changes affect the long term performance of the expert system. In the case of unpredicted behavior, the expert system should be capable of informing the user and make or suggest some changes in the knowledge base. For example, checks are provided to detect wrong data and to warn the user regarding the allowable range of values for the parameters. The expert system operates when a goal or procedure is made active by the user. When there are active goals waiting for some parameter values, the expert system has prompts to the user indicating the non-availability of those parameters. This includes unsuccessful goals as a result of lack of data or insufficient rules. In either case if the user is informed, corrective actions can be taken, which constitutes the learning process in the expert system.

The proposed expert system, during continuous operating mode will develop the knowledge base and also will modify the existing data. This is easily done using the read/write constructs available in the programming language used. The input files can also be modified by writing into the file the required correction after predetermined check points. The rules are modified only on supervision, but the rules are made as exhaustive as possible to avoid frequent correction. The expert system is also capable of automatic or unsupervised learning. The current information on the trend is automatically updated. After the calculation of the loading trend, the expert system compares the calculated trend to the actual values and any deviation is corrected and updated in the knowledge base. The updating of the stability table by the TEF method and correction of the sensitivity parameters by the TEF sensi-

tivity analysis presently are done only off-line. In the future, the expert system can be designed to make the required control data file to execute specific case studies using TEF programs. This can be made to automatically calculate any stability or sensitivity information needed for new system configurations.

Verification

After the initial design, the expert system was tested with known data and checked for the results. The expert system calculated the security index correctly for all inputs similar to NSP procedure. When the control parameter values were changed, the expert system came up with the correct change in the security index. The control actions suggested by the expert system were checked with the NSP power system operators for correctness. The loading trend calculated by the expert system was checked with the operations planning engineers at NSP and their input was considered in the modifications implemented. The loading trends computed by the expert system were compared with the trends calculated by the operation planning group at NSP and both the trends matched closely. After calculating the loading trend, the user can correct the load for any hour or for a group of hours as required by the operation planning engineers. This facility was included after consultation with the forecast group at NSP control center.

The expert system was tested with a large number of system configurations, loading trends and starting security index values. In all the case studies, the expert system correctly found the trend for control parameters while bringing the security index close to a pre-determined security level. The results demonstrate the capability of the expert system to adjust the values of control parameters for the remaining

hours in a given day to bring the security index from different starting values to the predefined security level. The security constraints were given a priority for the above procedure. The NSP Control Center wanted an option to change the predicted values of the control parameters after computation, and this feature was added. The interactive schemes used in the expert system and the graphic representation of the results were aggreeable to the users at NSP control center.

Different procedures of the expert system are explained in the next chapter. The c programming language is used for the expert system and the software is available in both mainframe and PC environments. The PC-based software was taken to NSP control center and used for demonstration and verification.

CHAPTER 4. PROGRAMS DEVELOPED AND SAMPLE RESULTS

This chapter describes some of the programs used in the expert system developed for NSP, and discusses the results of some sample case studies. The block diagram of the expert system is shown in Figure 4.1. The user interacts with the expert system by selecting different system configurations and the expert system consults the knowledge base using the required rules. The expert system uses the results of the TEF method for updating the knowledge base. The user runs the main program which gives a menu for executing other programs. The control flow diagram of the important programs used in the expert system is shown in Figure 4.2.

Computer Programs Developed

Computer Program "Margin"

This program calculates the security index, TCEX, given the values of the control parameters. It takes default values for the critical parameters and allows the user to change values of one or more critical parameters. It uses the sensitivities to calculate the new TCEX and thus gives the user an opportunity to study the effect of different control parameters. If the TCEX is below the predefined minimum value, the procedure suggests a list of corrective actions to the user. The user can also set the security index and the operating parameter values and use this set of values as

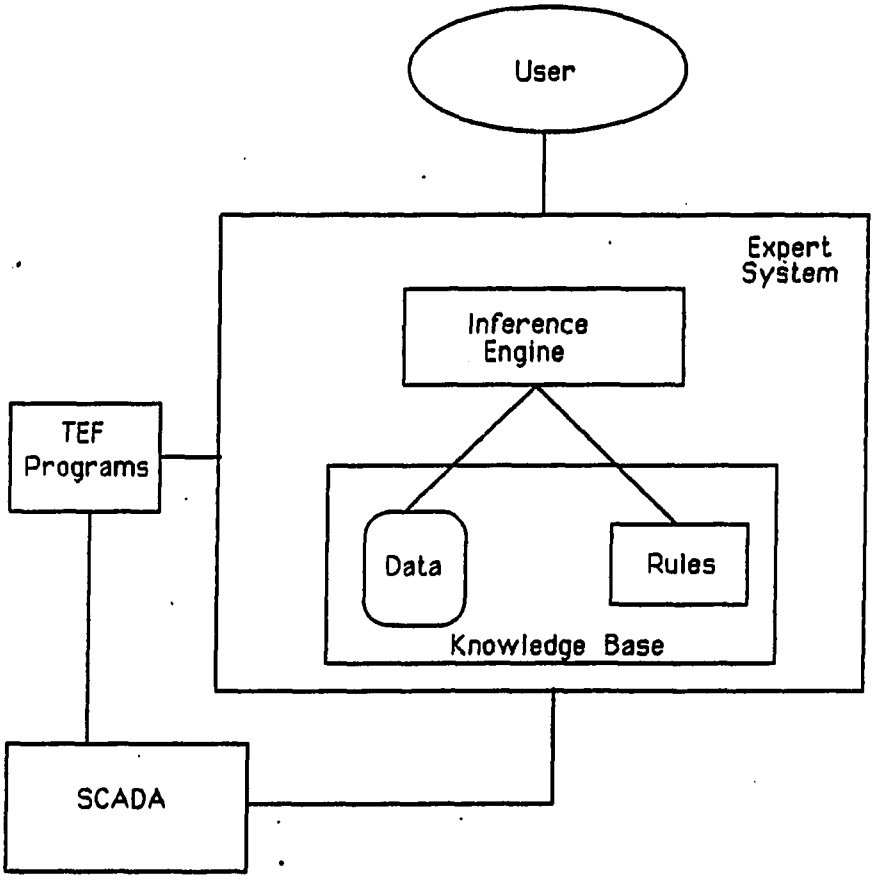

Figure 4.1: Block diagram of the expert system

input for studying the trend analysis.

Computer Program "Trend Analysis"

This program takes as input the stability table, previous loading trend, previous weather trend, sensitivities of weather parameters, sensitivities of control parameters, current system conditions, minimum and maximum values for different parameters, and current values of the control parameters. It uses the time information from the system clock as a default value, but the time values can be changed by the user for studying the trend analysis for other time values. The trend analysis program initially refers to the knowledge base for the previous trends of loading and weather for the given time input. The user can change the weather parameters, and can also add the necessary additional weather information such as a snow storm, a continuous heat/cold wave, and rain. The program then computes the corrected loading trend by adjusting the previous loading trend for changes in weather conditions, using sensitivity factors of weather parameters. At this stage, the user is given an option to correct the predicted loading trend for one particular hour or for a series of hours. The final load trend is obtained after the user's correction and is used as an input to find the trend of the control parameters and the security index.

The program uses heuristic rules in predicting an economical trend for the control parameters while meeting the security constraints. The program tries to bring the value of the security index to a value closer to a predefined optimum value. The user then has the option to correct the trend of any of the control parameters and the program adjusts the security index accordingly. The user can choose to run the margin program first to initialize the values of the control parameters and then

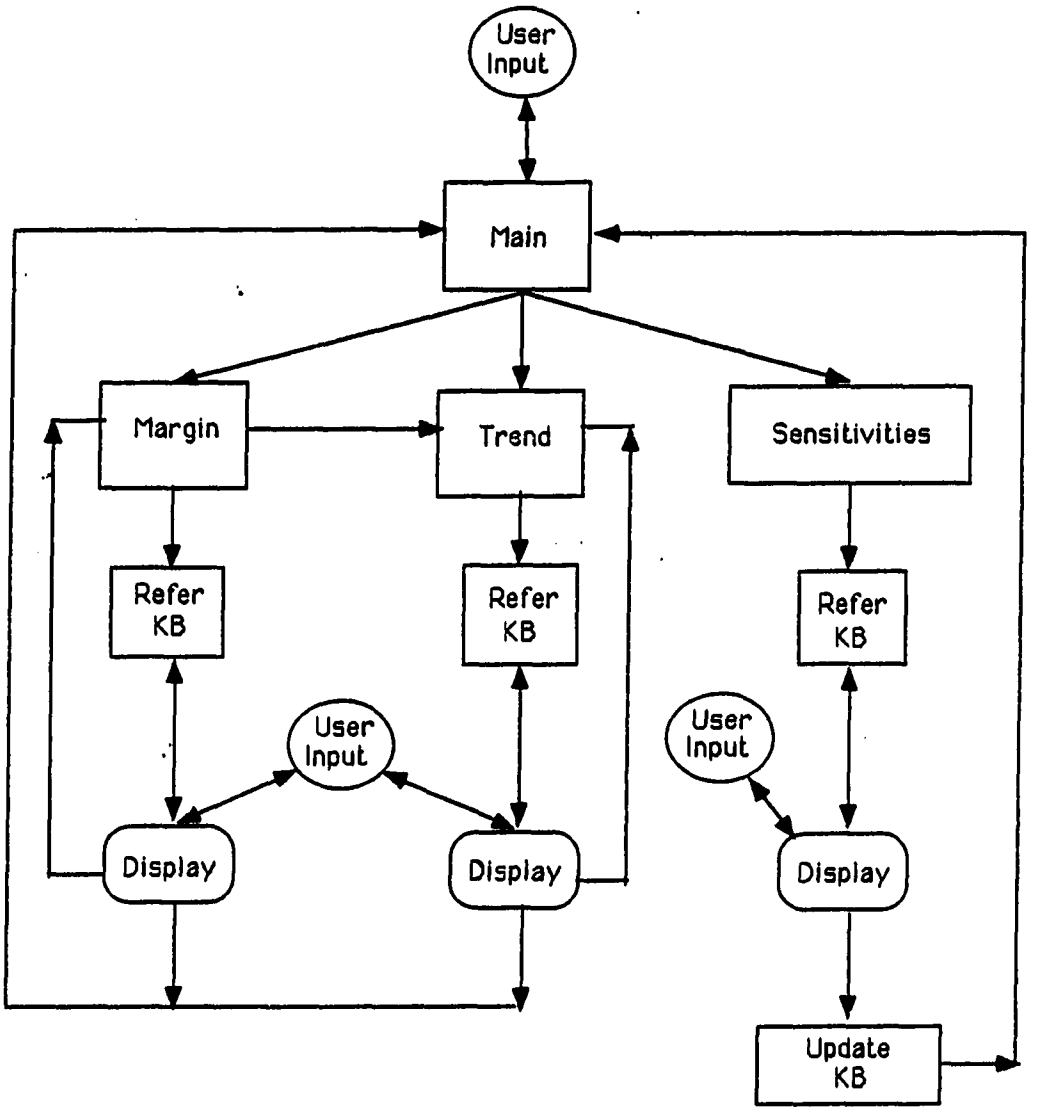

Figure 4.2: Control flow for the expert system

run the trend analysis program and thus will have the complete flexibility to study different scenarios.

Computer Program "Sensitivity"

This program helps the user change the values of the sensitivity factors for control parameters and the sensitivity factors for external parameters such as weather. The sensitivity analysis program of the TEF method can be used to update the sensitivities of the security index to changes in the control parameters. At present, the user can manually correct and fine tune the different sensitivities in the study mode. The above stand alone programs use other procedures for reading current data, writing output for documentation and graphical displays, as shown in the Figure 4.2.

Sample Results

This section contains results from a set of case studies conducted using the expert system. Using the " Margin" program, the first two case studies show the results for different system conditions of the NSP system shown in Figure 3.4. In the remaining case studies, the results of the "Margin" program is used to create a set of initial conditions as an input for the "Trend Analysis" program.

Case Study 1 and 2

The "Margin" program is used to find the value of the security index for any given set of input values of the control parameters. In this section, two case studies are described to show how the NSP expert system computes the security index for different set of input values. For case study 1, the input values are:

```
Generator outage condition       = Normal.
Line outage condition            = Normal.
Sherco power plant generation    = 2000 MW.
Lineflow on Manitoba             = 200  MW.
Number of East Side units        = 6.
Twin Cities Export: Lakefield    = 100  MW.
Twin Cities Export: Byron        = 100  MW.
Twin Cities Export: Eau-Claire   = 100  MW.
```

Table 4.1: Results for case study 1

Export Limit from the Stability Table	=	1345 MW.
Increase in Export Margin due to Sherco	=	700 MW.
Reduction in Export Margin due to MAN	=	0 MW.
Increase in Export Margin due to ESG	=	300 MW.
Final Export Limit	=	2345 MW.
Actual Twin Cities Export	=	300 MW.
Twin Cities Export Margin (Security Index)	=	2045 MW.

Table 4.1 shows the results of the security index (TCEM) calculations for case study 1. The sensitivity values used in the calculations are supplied by the NSP. The optimum value for the security index is chosen to be zero (i.e., TCEM value of 0 MW or above is safe with reference to security constraints) for the case studies and results for case study 1 show a large value of security index. No corrective action is needed in this case study. The user can change the values of the control parameters and observe the effect of these changes.

For case study 2, the input values are chosen so that the security index is negative (i.e., the system conditions are not safe with reference to security constraints). Sherco

generation is increased to 2300 MW, Manitoba lineflow is increased to 600 MW, Twin City Export is increase to 1500 MW, and the number of East side generating units is reduced to one. The input values for the case study 2 are:

```
Generator outage condition      = Normal.
Line outage condition           = Normal.
Sherco power plant generation   = 2300 MW.
Lineflow on Manitoba            = 600  MW.
Number of East Side units       = 1.
Twin Cities Export: Lakefield   = 500  MW.
Twin Cities Export: Byron       = 500  MW.
Twin Cities Export: Eau-Claire  = 500  MW.
```

Table 4.2: Results for case study 2

Export Limit from the Stability Table	=	1345 MW.
Increase in Export Margin due to Sherco	=	0 MW.
Reduction in Export Margin due to MAN	=	345 MW.
Increase in Export Margin due to ESG	=	75 MW.
Final Export Limit	=	1075 MW.
Actual Twin Cities Export	=	1500 MW.
Twin Cities Export Margin (Security Index)	=	-425 MW.
NEGATIVE EXPORT MARGIN!!! Condition: Critical!		
Possible CORRECTIVE ACTIONS are:		
Increase ESG.		
Reduce WSG (Sherco).		
Reduce MAN.		
Reduce Twin Cities Export.		

Table 4.2 shows the results for case study 2. Since the security index (Twin Cities Export Margin) is negative, the expert system lists a set of corrective actions.

These corrective actions help the user adjust the values of the control parameters so that the value of the security index can be brought back to the safe level. The safe level for the security index can be modified by the user to make the expert system list warnings and corrective actions at the chosen safe level of the security index. The user can make changes in the values of one or more control parameters to bring the security index to the safe level. After the user makes these changes, the expert system recomputes the security index and displays the new results. Thus the user can operate interactively and study the effect of the changes he makes. The sensitivity information of different parameters are also given to the user along with the results.

Case Studies 3 and 4

These studies are conducted to illustrate how the expert system computes the trend of the control parameters. The input conditions for both the case studies are the same except the Twin City export. The value of Twin City export is used to get a difference in the value of security index for the case studies. For these cases the input values of the control parameters are:

```
Generator outage condition      = Normal.
Line outage condition           = DKN-PKL.
Sherco power plant generation   = 2000 MW.
Lineflow on Manitoba            = 200  MW.
Number of East Side units       = 4.
```

The total Twin Cities export for case study 3 is 300 MW whereas the the export value is 1500 MW for case study 4. The loading trend for both the case studies are

Table 4.3: Results for case study 3

Details of the Case Study:
Month = May, Day = Friday, Time = 10 A.M.
Current Temperature = 66 F.
Current Humidity = 50 %
Current Illumination = 4859 Foot Candles
Current Windspeed = 6 Miles per Hour
Current Loading = 4260 MW

Time	ExpMar	WSG	MAN	ESG	LOAD	IMPORT	Condition
10 A.M.	530	2060	200	300	4260	1014	
11 A.M.	476	2027	200	300	4373	1100	
12 noon	374	2078	200	300	4424	1100	
1 P.M.	329	2078	200	255	4379	1100	
2 P.M.	291	2097	200	255	4398	1100	
3 P.M.	282	2097	200	246	4389	1100	
4 P.M.	209	2097	200	173	4316	1100	
5 P.M.	89	2097	200	53	4196	1100	Alert!
6 P.M.	89	2097	200	53	4016	920	Alert!
7 P.M.	89	2097	200	53	3864	768	Alert!
8 P.M.	89	2097	200	53	3740	644	Alert!
9 P.M.	89	2097	200	53	3767	671	Alert!
10 P.M.	89	2097	200	53	3649	553	Alert!
11 P.M.	89	2097	200	53	3341	245	Alert!
0 A.M.	36	2097	200	0	2985	120	Alert!

chosen to be the same for comparison purposes by choosing the same set of weather conditions and the time factors. The results give the trend of the control parameters from a given hour until the end of the day.

Table 4.3 shows how the expert system adjusts the trends of the control parameters from the given starting values, to match the calculated loading trend and keep the security index closer to the optimum value. In case study 3, the starting value of the security index is high and hence its value is gradually reduced. In the predictive mode, the operators can observe the recommended trend for the control parameters and can correct any of the predicted values. The expert system recomputes the new values of the security index incorporating these corrections.

Table 4.4 shows how the trends are adjusted for the same loading trend if the starting value of the security index is negative. The expert system uses the rules given in Chapter 3 to compute the trend of the control parameters based on the loading trend. For example, the load increase at 11 A.M. is absorbed by WSG in case study 3 (when TCEM is positive) and is adjusted with ESG in case study 4 (when TCEM is negative).

The user can run case studies for different loading trends and different starting values of the security index and the control parameters. The "Margin" program helps the user initialize the input values of the control parameters and the trend analysis allows the user to choose different loading trends. After the computation of the trend of the control parameters, the user has the flexibility to change any of the values of the control parameters. The expert system will adjust the value of the security index accordingly.

Table 4.4: Results for case study 4

Details of the Case Study:
Month = May, Day = Friday, Time = 10 A.M.
Current Temperature = 66 F.
Current Humidity = 50 %
Current Illumination = 4859 Foot Candles
Current Windspeed = 6 Miles per Hour
Current Loading = 4260 MW

Time	ExpMar	WSG	MAN	ESG	LOAD	IMPORT	Condition
10 A.M.	-670	2000	200	300	4260	1014	Emergency!!
11 A.M.	-557	2000	200	413	4373	1014	Emergency!!
12 noon	-506	2000	200	464	4424	1014	Emergency!!
1 P.M.	-416	1955	200	464	4379	1014	Emergency!!
2 P.M.	-397	1955	200	483	4398	1014	Emergency!!
3 P.M.	-379	1946	200	483	4389	1014	Emergency!!
4 P.M.	-233	1873	200	483	4316	1014	Emergency!!
5 P.M.	7	1753	200	483	4196	1014	Alert!
6 P.M.	0	1753	200	476	4016	841	Alert!
7 P.M.	0	1753	200	476	3864	689	Alert!
8 P.M.	0	1753	200	476	3740	565	Alert!
9 P.M.	0	1753	200	476	3767	592	Alert!
10 P.M.	0	1753	200	476	3649	474	Alert!
11 P.M.	0	1753	200	476	3341	166	Alert!
0 A.M.	0	1753	200	476	2985	120	Alert!

In this chapter, we described the operation of the expert system for security trend analysis. Four case studies demonstrated how the expert system computes the security index for different system configurations, how it lists the control actions when the security index is below the safe value, and how the expert system computes the values for the control parameters to keep the security index near the safe value.

CHAPTER 5. SUMMARY AND CONCLUSIONS

In this dissertation, the design of the TEF-based expert systems for dynamic system security assessment is discussed. An effort was made to capture the thinking of the power system operators and understand their view of the power system security. The IEEE working group for security assessment introduced several new fundamental concepts in DSSA. Among them is the system operator's concern with how the security level changes with the changes in system conditions and the trend of the operating parameters which affect the system security index [18, 19]. The results of the surveys and the discussions with the power system operators were analyzed and integrated into an expert system framework. The project also develops the basic ideas associated with the structured knowledge base. The fundamental concepts and the basic requirements for a dynamic system security assessment expert system have been investigated for a stability-limited power network. The computerized procedure uses the stability results from the TEF method as input to the knowledge base of the expert system developed. It is now believed that the development of a general, large-scale implementation of the TEF-based expert system is achievable, and is beneficial in providing additional capabilities to the Energy Management Systems.

To demonstrate these results, a practical implementation of the TEF-based expert system was developed for the Northern States Power Company. Initially, data

were collected from NSP, which included the NSP system specifications, the stability and security criterion, the company policies, the existing heuristic methods for evaluating the system security, and other relevant data. The data thus collected were organized forming the knowledge base and the heuristic rules were organized to form the rule base for the expert system.

The expert system, which was written in the c language, was tested for known system configurations in a main-frame environment. Knowledge and rules were added or modified during this testing stage after consulting with the operation planning group at NSP. The expert system contained graphic support with concise displays and a simple tabulated form for results so that the user can make quick decisions. The expert system was designed to be portable and was easily moved from a SUN SPARC1 to an IBM compatible PC for testing at the NSP control center with current data. The portable version of the expert system has 4000 lines of code with 200 rules and 5000 data elements. The source code and the data consume 200K bytes of memory, and the executable file occupies another 160K bytes.

The major contributions of this project are:

- A successful attempt is made for DSSA using the results of the direct methods of stability analysis for determining the system security.
- The analytical results are combined with the power system operator's experience in the form of an expert system.
- In the NSP expert system, the security of the power system at any particular time and for different system configurations can be computed using the off-line stability results.

- The trend of the security index can be computed if the trend of the controlling parameters are known.
- The expert system can compute an economical trend for the control parameters for a given system configuration and a given loading trend.
- The expert system also demonstrates the need for integrating all the power system applications as it uses the results of load forecasting procedure and the off-line stability programs. In an online mode, the expert system can use the automatic generation control programs for executing the control actions.
- The NSP system operators, and engineers from the operations planning group have accepted the expert system as a study tool for security assessment and trend analysis.

When the NSP expert system is used in a continuous mode, it will take the current data directly from Supervisory Control and Data Aquisition (SCADA) system and compute the trend details automatically. The expert system will compute the trends and update the knowledge base at the beginning of every hour monitored by the system clock. The expert system will still be available as a study tool for the users.

Suggestions for Future Research

Based on the experience in the present investigation, the following developments are suggested for expert systems in power system security analysis. The expert system should be integrated into the existing EMS software. This can be done by initially using the dispatcher training simulator as a medium for integration. In this way it will

have access to the online data from SCADA and will not affect the performance of the EMS. The learning procedures in the expert system have to be fully automatic. At present, updating the loading trend is automatic, whereas other learning capabilities are supervised.

An interface with the sensitivity analysis program of the TEF method can be used for making automatic modifications to the sensitivities of the control parameters. An interface with the SCADA can help to modify the permissible limits for the current values of the operating parameters. The current stability table uses results of only single line outage situations. The TEF method can be used to provide the results for multiple line outage situations.

At present, the expert system uses sequential order for rule selection. When the number of rules increase, other control strategies for rule selection can be implemented using special shell environments for the expert system.

The expert system can be developed in a parallel processing environment where each of the processor can handle a different subtask and the data can be shared between them using either shared memory techniques or message passing techniques. In the parallel processing environment, transient stability analysis for a larger number of system configurations can be computed.

Application of TEF-based expert system techniques for power system security analysis is a continuing research effort and some of the above suggestions are being developed.

BIBLIOGRAPHY

[1] A. Bose, C. Concordia, R. D. Dunlop, A. A. Fouad, P. Kundur and R. P. Schultz. "Proposed Terms & Definitions for Power System Stability." *IEEE Transactions on Power Systems* PAS-101 (1982): 1894-1898.

[2] A. A. Fouad and Vijay Vittal. "Power System Transient Stability Analysis using the Transient Energy Function Method." Department of Electrical Engineering and Computer Engineering, Iowa State University, 1989.

[3] M. A. El-Kady, A. A. Fouad, C. C. Liu and S. Venkataraman. "Use of Expert Systems in Dynamic Security Assessment of Power Systems." Presented at the 10th Power System Computation Conference, Graz, Austria, August, 1990.

[4] M. A. El-Kady, A. A. Fouad and C. C. Liu. "Knowledge-Based System for Direct Stability Analysis." *EPRI Report* No. EI-6796, March 1990.

[5] N. J. Nilsson. "Principles of Artificial Intelligence." PaloAlto, California: Tioga Publishing Company, 1980.

[6] M. A. El-Sharkawi. "Tutorial session on Expert Systems and Artificial Neural Networks." Second Symposium on Expert Systems Application to Power Systems, Seattle, Washington, 1989.

[7] Lee Brownston, Robert Farrell, Elaine Kant and Nancy Martin. "Programming Expert Systems in OPS5." Reading: Addison Wesley Publishing Company, Inc., Jan. 1986.

[8] Bruce F. Wollenberg. "Feasibility Study for an Energy Management System Intelligent Alarm Processor." *IEEE Transactions on Power Systems* PWRS-1, No. 2 (May 1986): 241-246.

[9] Daniel S. Kirschen, Bruce F. Wollenberg, Guillermo D. Irisarri, Jeffery J. Bann and Bradley N. Miller. "Controlling Power Systems During Emergencies: The Role of Expert Systems." *IEEE Computer Applications in Power* 2, No. 2 April 1989: 41-45.

[10] Chen-Ching Liu and Kevin Tomsovic. "An Expert System Assisting Decision-Making of Reactive Power and Voltage Control." *IEEE Transactions on Power Systems* PWRS-1, No. 3 (August 1986): 195-201.

[11] E. D. Tweed. "Knowledge Based System: Voltage and Var Dispatch." *EPRI Report* EL-6489 Project 2944-2, October 1989.

[12] Sarosh N. Talukdar, Eleri Cardozo, Ted Perry. "The Operator's Assistant–An Intelligent, Expandable Program for Power System trouble Analysis." *IEEE Transactions on Power Systems* PWRS-1, No. 3 (August 1986): 182-187.

[13] Young-Il Park and Jong-Keun Park. "An Expert system for short term Load Forecasting by Fuzzy Decision." Second Symposium on Expert Systems Application to Power Systems, July 17-20, 1989.

[14] Kevin Tomsovic, Chen-Ching Liu, Paul Ackerman and Steve Pope. "An Expert System as a Dispatchers' Aid for the Isolation of Line Section Faults." *IEEE Transactions on Power Delivery* PWRD-1, No. 2 (July 1986): 1-8.

[15] Lars-Ola-Osterlund. "Contingency Selection using Object Oriented Programming and Heuristic Rules." Second Symposium on Expert Systems Application to Power Systems, July 17-20, 1989.

[16] Chen-Ching Liu, Seung Jae Lee and S. S. Venkata. "An Expert System Operational Aid for Restoration and Loss Reduction of Distribution Systems." *IEEE Transactions on Power Systems* PWRS-2, No. 3 (1987): 315-321.

[17] Ming Chen, M. J. Damborg and T. M. Athay. "Full Integration of an Expert System into an Energy Management System using a Dispatcher Training Simulator." Second Symposium on Expert System Applications to Power Systems, July 17-20, 1989.

[18] IEEE Working Group for Dynamic Security Assessment. "Minutes of the July 27, 1987 meeting of the Dynamic Security Assessment Working Group." Power System Engineering Committee of the Power System Engineering Society, IEEE.

[19] Jim Larson and A. A. Fouad. "Transient Stability Assessment & Operator Guide at Northern States Power Company." Correspondence between NSP representative and IEEE Working Group Chairman, Electrical Engineering and Computer Engineering Department, Iowa State University, Ames, Iowa, 1985-1988.

[20] Oliver Jones. "Introduction to the X Window System." Englewood Cliffs, New Jersey: Prentice Hall, 1989.

[21] C. C. Liu, K. Tomsovic and S. Zhang. "Efficiency of Expert Systems as On-line Operating Aids." PSCC Conference at Lisbon, 1987.

[22] M. Daneshdoost and S. S. Vijay. "An Expert System for Security Enhancement of Power Systems using Prolog in a Microcomputer Environment." *IEEE Transactions on Power Systems* PWRS-2, No. 2 (1987): 315-321.

[23] L. Wehenkel, Th. Van Cutsem and M. Ribbens-Pavella. "An Artificial Intelligence Framework for on-line Transient Stability Assessment of Power Systems." IEEE Summer Meeting, 1988. Paper No. 88 SM 699-1.

[24] J. A. Findlay, V. F. Carvalho, G. A. Maria and C. E. Graham. "State of the Art and Key Issues in Power System Security Assessment." Proceedings of the Workshop on Power System Security Assessment, April 27-29, 1988.

[25] Guy L. Steele Jr. "Common LISP: The Language" Hanover, Massachusetts: Digital Press, 1984.

[26] Yoh-Han Pao and Se-Young Oh. "A Rule-Based Approach to Electric Power Systems Security Assessment." *IEEE Transactions on Power Systems* No. 1 (1981): 490-492.

APPENDIX DEFINITIONS OF KEY TERMS

Power System: A network of one or more electrical generating units, loads, and/or power transmission lines, including the associated equipments electrically or mechanically connected to the network. A combination of generation resources and transmission facilities operated under common management or supervision to supply load.

Tie Line: A transmission line connecting two power systems.

Operating Parameters: Physical quantities, which can be measured or calculated, that can be used to describe the operating conditions of a power system.

Disturbance in a Power System: A disturbance in a power system is a sudden change or a sequence of changes in one or more of the operating parameters of the power system. In a small disturbance the equations that describe the dynamics of the power system may be linearized for the purpose of analysis, whereas this is not possible in case of a large disturbance.

Stability: A power system is stable for a particular steady-state operating condition and for a particular disturbance if, following that disturbance, the power system reaches an acceptable steady-state operating condition.

Security: 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 unantici-

pated loss of system components.

Security Assessment: Security assessment is the evaluation of available data to estimate the relative robustness (security level) of the system in its present state.

Dynamic Security: Dynamic security deals with security threats to the power system in transition, following a disturbance. Dynamic security involves security problems of the power system during transients, i.e., from the initial operating state to another steady-state condition.

Vulnerability: Vulnerability is the rate of change of the security level of a power system due to variations in the control parameters or the external conditions such as weather.

Artificial Intelligence: It is the study of methods for solving tasks that require "human-like" intelligence. The goal of artificial intelligence is to develop computer systems that in some way "think" or solve problems in a way that would be considered intelligent if done by humans.

Expert Systems: An expert system is a program which has high quality specific knowledge for solving limited problems (domain specific). Expert systems handle real world problems using computers to reach the same results, as would a human expert, if faced with a comparable problem.

Inference Engine: Inference engine is a part of an expert system with problem solving paradigms. It uses the forward chaining and/or backward chaining methods for problem solving.

Forward and Backward Chaining: Forward chaining methods start with a set of initial conditions and reach the desired goal similar to bottom-up strategy and hence used for synthesis. Backward chaining methods start with a goal situation, decompose

this goal to sub-goals and continue this process until all the sub-goals are solvable. This approach is similar to the top-down strategy and is often used for analysis.

Knowledge Base: It is a collection of data specific to the domain. In most of the literature, the set of rules for interpreting the data are also included in the knowledge base.

Learning: The ability of an artificial intelligence method to make changes to the knowledge base and some part of the inference engine (based on experience) such that the changes have a long-term effect on the performance of the method.

Heuristic Rules: Techniques used by human experts for solving problems based on their experience and knowledge rather than results based on analytical or algorithmic procedures.

Shell: Shells are special environments for the use of expert systems with built in inference engine.