



Integrated Security Analysis

Final Project Report

Power Systems Engineering Research Center

*A National Science Foundation
Industry/University Cooperative Research Center
since 1996*





Power Systems Engineering Research Center

Integrated Security Analysis

Final Report

**Kevin Tomsovic, Project Leader
Washington State University**

**Project Team Members
Anjan Bose, Washington State University
Peter Sauer, University of Illinois**

**Student Members
Jie Tong, Washington State University
Adisorn Sittithumwat, Washington State University**

PSERC Publication 03-06

May 2003

Information about this Project

For information about this project contact:

Kevin Tomsovic
Professor School of Electrical Engineering and Computer Science
Washington State University
P.O. Box 642752
Pullman, WA 99164
Phone: 509-335-8260
Fax: 509-335-3818
Email: tomsovic@eecs.wsu.edu

Power Systems Engineering Research Center

This is a project report from the Power Systems Engineering Research Center (PSERC). PSERC is a multi-university Center conducting research on challenges facing a restructuring electric power industry and educating the next generation of power engineers. More information about PSERC can be found at the Center's website: <http://www.pserc.wisc.edu>.

For additional information, contact:

Power Systems Engineering Research Center
Cornell University
428 Phillips Hall
Ithaca, New York 14853
Phone: 607-255-5601
Fax: 607-255-8871

Notice Concerning Copyright Material

PSERC members are given permission to copy without fee all or part of this publication if appropriate attribution is given to this document as the source material. This report is available for downloading from the PSERC website.

Acknowledgements

The work described in this report was sponsored by the Power Systems Engineering Research Center (PSERC). We express our appreciation for the support provided by PSERC's industrial members and by the National Science Foundation under grant NSF EEC-9813407 received under the Industry/University Cooperative Research Center program.

Thanks are also given to the following individuals who contributed to this project:

Prahba Kundur	PowerTech Labs	Industry advisor
Kip Morrison	PowerTech Labs	Industry advisor
Robert Stuart	Pacific Gas and Electric	Industry advisor
Ben Williams	Pacific Gas and Electric	Industry advisor

Executive Summary

In today's power marketplace, the ability to accurately and quickly determine system security limits has become increasingly important. Over the past several decades, research has resulted in significant advances in analytical techniques needed for quantifying system security limits. At the same time, the phenomenal growth in computational speeds of modern computers has brought on-line security analysis closer to practical use.

Despite these great strides, system operators continue making limited use of new system analysis tools. Operators tend to follow relatively fixed sets of procedures and pre-calculated system limits. One of the factors hindering operator adoption of new sophisticated security techniques is their limited understanding of the underlying analysis methods on which the new tools are based. Another barrier to adoption is the natural preference to use older, well-understood and tested tools given the critical responsibilities operators have for maintaining security.

There is a need for a comprehensive security analysis framework that operators can use. This project explored the issues associated with developing such a framework and implemented an approach that integrates techniques that make extensive use of off-line studies. In doing so, the project has contributed to the understanding of integrated security analysis in a number of ways.

- A comprehensive framework was developed for on-line estimation of security margins, calculated based on current operating practices.
- The framework includes families of estimators, each specialized for specific system limits and the appropriate security criteria (i.e., static, dynamic or voltage). The estimators can be combined to provide an overall assessment of system operating conditions.
- A system of estimators was implemented and tested on a modified New England 39 bus system.
- Based on the insights from the New England system, a more sophisticated set of estimators were implemented and tested on a 6500 bus model of the Western Area system. The focus of this study was the California-Oregon inertia transfer limits.
- A number of software tools were developed to help automate the process of evaluating security margins in off-line studies.

The results show that very accurate on-line estimation of security margins is possible for large systems. The main limitation of the implemented approach resides in the ability of time-consuming off-line studies to accurately model system dynamics. Directions for further development were proposed.

Table of Contents

1	Introduction	1
2	Background	4
2.1	Operations Planning and Reliability Policies.....	5
2.1.1	Dynamic Security	6
2.1.2	Voltage Security.....	8
2.1.3	Remarks.....	9
2.2	WSSC Reliability Criteria.....	10
2.2.1	Performance Levels.....	10
2.2.2	WSSC Voltage Stability Criteria	14
2.3	Estimation of Stability Margins	14
3	Operations Issues.....	16
3.1	Combined Security Analysis Concepts	16
3.2	Operator Surveys.....	18
4	Proposed Methodology	19
4.1	Overall Security Framework	19
4.2	Generation of Training Data	21
4.3	Estimator Design.....	22
4.3.1	Feature Selection and Processing.....	23
4.3.2	Network Structure, Hidden Layers and Voting Schemes	24
4.3.3	Splitting Training Data for Estimation and Validation	24
5	Numerical Results	25
5.1	Studies on IEEE 39 Bus System	25
5.1.1	System and Case Study Description.....	25
5.1.2	Analysis.....	25
5.2	Studies on WSCC System Model.....	33
5.2.1	System and Case Study Description.....	33
5.2.2	Analysis.....	35
6	Conclusions and Future Studies	42
6.1	Significant Contributions	43
6.2	Recommended Further Developments	43
7	References	45
8	Description of Study Data and Developed Software	47
9	Project Publications and Presentations.....	48

1 Introduction

In today's power marketplace, the ability to accurately and quickly determine system security limits has become increasingly important. Over the past several decades, research has resulted in significant advances in analytical techniques needed for quantifying system security limits. At the same time, the phenomenal growth in computational speeds of modern computers has brought on-line security analysis closer to practical use.

Despite these great strides, system operators continue making limited use of new system analysis tools. Operators tend to follow relatively fixed sets of procedures and pre-calculated system limits. One of the factors hindering operator adoption of new sophisticated security techniques is their limited understanding of the underlying analysis methods on which the new tools are based. Another barrier to adoption is the natural preference to use older, well-understood and tested tools given the critical responsibilities operators have for maintaining security.

There is a need for a comprehensive security analysis framework that operators can use. This project explored these issues and implemented an approach that integrates techniques that make extensive use of off-line studies.

In current practice, operational planners employ detailed power system studies to find the maximum allowable loadings in particular areas and the associated transfers across key interfaces. Reliability standards require that the system withstand any credible contingency and maintain a security margin to allow operators time to respond. Under this approach, system ratings tend to be conservative because the off-line security studies used to establish the ratings are based on unusually stressed conditions. In addition, the studies are incomplete because not all combinations of loadings and equipment out-of-service are analyzed. Furthermore, even though the off-line studies are conservative, the limits are increasingly of questionable value since energy trades may easily result in loading conditions inconsistent with the off-line studies.

Most operators have advanced applications at their disposal for assessing static security limits. They can also receive engineering support for detailed studies with the advanced applications, given sufficient time. Even so, they tend not to systematically use these applications.

This project investigated possibilities for the integration of existing tools for static, dynamic, voltage and steady-state stability security assessment into a comprehensive and integrated security analysis framework. This investigation included the examination of efficient mechanisms for determining security results and conveying those results most effectively to assist system operators. The fundamental approach described in this report is a system of estimators based on specific security criteria with the lowest margin estimate used to determine the system security margin. A set of such estimators is

implemented for a small test system as well as for a larger more practical system, the Western Systems Coordinating Council (WSCC). While the developed method only employs a few selected analysis techniques (i.e., time-domain simulation and static voltage margin computations), the approach is generic and can efficiently incorporate any security approach – numerical or analytic. This framework promises greater effectiveness for off-line and on-line computations, and for improved support of system operations.

The main research thrusts of this project were to:

- Investigate an overall strategy for the integration of existing security assessment tools.
- Investigate the overlap and possible duplication of effort in the various tools.
- Investigate intelligent system approaches to the integration strategy.
- Investigate mechanisms for improving security assessment efficiency and mechanisms for supporting operators and operational planners.
- Develop realistic test cases and a prototype program for testing the integrated security analysis strategy.
- Evaluate the developed system performance.
- Document the framework and prototype program performance.

In a previous PSERC project [1], it was shown that a system of estimators based on Neural Networks could accurately and quickly estimate security margins for on-line application. That work considered only static voltage security and recommended “... *(investigating) other security criteria that may be less amenable to interpolation.*” The approach in that project leads naturally to the more general framework proposed in this project. This framework is based on more sophisticated modeling and time-domain simulations.

In recent years there have been several database or pattern matching methods introduced for finding security limits (e.g., [2,3]). The essential idea is to select a set of representative features (such as line flows, loads, and generator limits) and then train an estimator (typically an Artificial Neural Network or ANN) on simulation data to estimate the security margin. The estimator is expected to interpolate or generalize to similar unstudied cases.

The problem with much of this previous work is that researchers have focused on generic power system models that ignore the practical difficulties in determining these limits and the specifics of reliability criteria for a particular system. Our earlier work has shown that accurate estimates can be obtained for voltage security on practical systems (in this case, the WSCC system [4]) only by developing very narrowly focused estimators. For example, different ANNs can be trained based on certain major equipment outages and security criteria. In this project, this framework is extended to other security considerations. A hierarchical design is developed that combines margin estimators for

different security criteria and operating conditions. A voting mechanism is introduced that combines individual estimates. Each estimator is designed using statistical criteria that ensure optimal performance [5].

The project has contributed to the understanding of integrated security analysis in a number of ways.

- A comprehensive framework was developed for on-line estimation of security margins, calculated based on current operating practices.
- The framework incorporates families of estimators, each specialized for specific system limits and the appropriate security criteria (i.e., static, dynamic or voltage). The estimators can be combined to provide an overall assessment of system operating conditions.
- A system of estimators was implemented and tested on a modified New England 39 bus system.
- Based on the insights from the New England system, a more sophisticated set of estimators were implemented and tested on a 6500 bus model of the Western Area system. The focus of this study was the California-Oregon intertie transfer limits.
- A number of software tools were developed to help automate the process of evaluating security margins in off-line studies.

The results show that very accurate on-line estimation of security margins is possible for large systems. The main limitation of the implemented approach resides in the ability of time-consuming off-line studies to accurately model system dynamics. Directions for further development were proposed.

2 Background

Power system security is the ability of a system to withstand sudden disturbances with minimum disruption to quality of service. Examples of such disturbances are electric short circuits, change of transmission system configurations due to faults, loss of system components, line-switching actions, and sudden load increases. For proper planning and operation, having a secure system means that after a disturbance occurs, the power system (1) will survive the ensuing transient and move into an acceptable steady-state condition, and (2) in this new steady-state condition, all components will operate within established limits [6]. The analysis used for the first requirement is transient analysis or Dynamic Security Assessment (DSA). The analysis for the second condition is static security assessment (SSA). In addition, voltage support has become an increasing concern so a third analysis is voltage security assessment (VSA), although this analysis often overlaps with SSA and DSA.

Typically, SSA is performed first, followed by DSA. SSA evaluates the post-contingent steady state of the system, neglecting the transient behavior and any other time-dependent variations. For on-line SSA, modern computational speeds allow load flow studies of a large number of contingencies in near real-time. Such software is a standard component of energy management systems (EMS), although this software usually does not directly compute security margins but simply evaluates static limits. Several other techniques are now available to quickly and reliably perform SSA; however, they are not widely used in practice.

DSA evaluates the time-dependent transition from the pre-contingent to the post-contingent state, determining the stability of the system for both small and large disturbances. Two dynamics problems, transient stability and voltage collapse, should be considered when performing a dynamic security study. Transient stability assessment is the major concern in DSA for multi-machine power systems analyzing whether a fault on the system, or loss of a large generator can give rise to large electromechanical oscillations between generating units leading to a loss of synchronism in the system.

On-line DSA methods are still not fully operational, with some approaches currently being tested and evaluated. Research on on-line DSA has generally focused on using fast methods to quickly determine system stability, including both time-domain simulation for transient stability indices and various energy function methods. This is in sharp contrast to the comprehensive, detailed and time-consuming studies employed in operational planning. Conventional techniques for dynamic security analyses require excessive computational time. Therefore, these are generally undesirable for on-line purposes.

VSA has been based primarily on static or pseudo-dynamic methods, with some useful on-line tools available. The voltage stability problem is generally associated with the increased loading of long transmission lines and insufficient local reactive power supply. An initial gradual voltage drop, followed by a rapidly accelerating decline or collapse,

characterizes these types of phenomena. The time interval of the slow voltage decay phase typically is between 1 to 10 minutes, which is often allows time for the operator to exercise corrective action.

2.1 Operations Planning and Reliability Policies

System security depends on the cooperation of different interconnected entities to coordinate operation of the system. The primary method to ensure this coordination in practice is to establish precise guidelines for the allowable effects neighboring systems may have on each other. These guidelines are based on both field experience and extensive operational studies. Different performance levels are used, depending on the type of disturbance. For example, under WSCC guidelines, allowable post-transient voltage deviation is 5% for a single generator outage and 10% for the outage of two generators. Thus, each reliability criteria depends on the type of disturbance. The disturbance should not violate constraints on:

- loading within emergency equipment ratings,
- transient voltage dip both in percentage deviation and in time duration,
- minimum transient frequency,
- post transient voltage deviation, and
- positive damping (i.e., stability).

Operation planners generally address these criteria through detailed time domain simulation studies for different loading conditions and for all major contingencies. In addition, there may be further requirements on running system studies. In the WSCC, this includes using either the P-V method (MW margin) or V-Q method (MVar margin) to determine an adequate voltage security margin. System operators, to a greater or lesser degree depending on the utility, tend to rely heavily on the limits identified by operational planners and make relatively limited use of the on-line security tools.

Generally speaking, each operational planning study must look at static, dynamic and voltage security concerns. For a given loading condition and the status of any significant equipment out-of-service, response to all credible and major contingencies is investigated. The loading, or other key system parameter (KSP), is varied to determine the proximity, or margin, to a security problem. For example, in VSA, P-V and/or V-Q curves [6] are employed using the distance to the nose as the margin. The allowable margins and associated reliability criteria are based on the regional council guidelines [7]. Margins for each scenario can be determined and documented in look-up tables or nomograms. Nomograms graphically depict the system limits for some KSP given a few scenarios, such as scenarios involving equipment outages or large transfers. The operator will then base the real time decisions on this information.

Look-up tables have the obvious drawback of inflexibility and are prone to errors because operators must search for the relevant scenario in the tables. Nomograms, on the other hand, provide slightly greater flexibility as they depict trade-offs in operating conditions, such as between some loading condition and a transfer across a key interface. Still, nomograms fail to fully capture all the information contained in the off-line studies and lack the ability to manage situations that are more varied. This practical approach differs significantly from approaches described in much of the on-line security literature that focus on contingency screening and fast methods for calculating the security. In practice, security limits are tabulated off-line as described above.

2.1.1 Dynamic Security

In practice, the typical criteria for DSA include [8]:

- Inertial stability criteria. This mainly concerns the evolution of relative machine angles and frequencies.
- Voltage excursions (dip or rise) beyond specified threshold level and duration. This includes separate voltage excursion threshold/duration pairs for voltage dip and voltage rise, and maximum/minimum instantaneous excursion thresholds.
- Relay margin criteria. These are defined for pre-disturbance and post-disturbance conditions. If relay margin is violated for more than a maximum specified time after the disturbance, it is identified as insecure.
- Minimum damping criteria. For a designated list of contingencies, if the post-disturbance system exhibits oscillations, they must be positively damped (decreasing in amplitude).

Identifying the specific set of security constraints to be introduced for the dynamic security studies is based on experience, knowledge of the system, and judgment of the planning and operations engineers. Generally, the objective of DSA is to determine which contingencies may cause power system limit violations or system instability. The ultimate goal is to generate the operating guidelines for defining the areas of secure operation. Generating the operating guidelines includes selecting contingencies, performing a detailed stability study, and analyzing the results for violations. Research on new methods for DSA can be divided into three areas: simulation (numerical integration method, direct or Lyapunov methods, and probabilistic), heuristic (expert system), and database or pattern matching approaches. An overview of these methods is provided below.

Numerical Integration

The numerical integration algorithms are used to solve the set of first order differential equations that describes the dynamics of a system model [9]. The most widely used methods are Runge-Kutta predictor and predictor-corrector methods. Numerical integration provides exact solutions relating to the stability of the system, depending on

the detail of the models employed. This is the most widely applied approach in off-line environments, but is generally too computationally intensive for on-line application.

Direct/Lyapunov Methods

This approach is also referred to as the transient energy function (TEF) methods. The idea is to replace the numerical integration by stability criteria. The value of suitably designed Lyapunov function V is calculated at the instant of the last switching in the system and compared to a previously determined critical value V_{cr} . If V is smaller than V_{cr} , the post-fault transient process is stable [10].

In practice, there are still some unresolved problems and drawbacks of this approach.

- The efficiency of this method depends on simplification of the system variables.
- The integration of the fault-on system equations is needed to obtain the critical value for assessing stability.
- It is difficult to construct the appropriate Lyapunov function to reflect the internal characteristics of the system.
- The method is rigorous only when the operating point is within the estimated stability region.

Probabilistic Methods

With these methods, stability analysis is viewed as a probabilistic rather than a deterministic problem because the disturbance factors (type and location of the fault) and the condition of the system (loading and configuration) are probabilistic in nature. Therefore, this method attempts to determine the probability distributions for power system stability. It assesses the probability that the system remains stable should the specified disturbance occur. A large number of faults are considered at different locations and with different clearing schemes. In order to have statistically meaningful results, a large amount of computation time is required [11]. Therefore, this method is more appropriate for planning. Combined with pattern recognition techniques, it may be of value for on-line application.

Expert System Methods

In this approach, the expert knowledge is encoded in a rule-based program. An expert system is composed of two parts: a knowledge base and a set of inference rules. Typically, the expertise for the knowledge base is derived from operators with extensive experience on a particular system. Still, information obtained off-line from stability analyses could be used to supplement this knowledge. The primary advantage of this approach is that it reflects the actual operation of power systems, which is largely heuristic based on experience. The obvious drawback is that it has become increasingly difficult to understand the limits of systems under today's market conditions characterized by historically high volumes of transactions.

Database or Pattern Recognition Methods

The goal of these methods is to establish a functional relationship between the selected features and the location of system state relative to the boundary of the region of stability [12,13]. This method uses two stages to classify the system security: (1) feature extraction and (2) classification. The first stage includes off-line generation of a training set of stable and unstable operation states, and a space transformation process that reduces the high dimensionality of the initial system description. The second stage is the determination of the classifier function (decision rule) using a training set of labeled patterns. This function is used to classify the actual operating state for a given contingency. Typically, the classifier part of this approach is implemented using ANNs.

2.1.2 Voltage Security

Voltage stability margin is a measure of the available transfer capacity, net transfer capacity, or total transfer capacity. The margin is the difference (or a ratio) between operation and voltage collapse points based on the KSP (loading, line flow, etc.) and accounts for a pattern of load increase or generation loss. As a concept for system operators, margin is a straightforward and easily understood index, and as a result, widely accepted. There are a number of advantages of the stability margin as a collapse index.

- The margin is not based on a particular power system model and can be used with static or dynamic models independent of the details of the power system dynamics.
- It is an accurate index that takes full account of the power system non-linearity and device limits as loading is increased.
- Sensitivity analysis may be applied easily and quickly to study the effects of power system parameters and controls.
- The margin accounts for patterns of load increase.

The primary disadvantage is that it may oversimplify the view of the stability problem and therefore not account for the variety of ways in which instabilities can arise.

In theory, the computation of the stability margin should be performed for all contingencies. This would be an excessively time-consuming process but is generally not necessary in practice. Instead, the margin is determined based on the most critical contingency from a relatively short list of known severe contingencies. Key to the analysis is the degree of experience needed to identify a more manageable list of disturbances. Still, the precise computation of the margin is time-consuming, thus limiting application for on-line use.

The most common methods to estimate the proximity of the voltage collapse point are the minimum singular value, point of collapse method, continuation power flow, and optimization method. Some other methods are sensitivity analysis, second order performance index, the energy function method, and modal analysis.

The minimum singular value of the load-flow Jacobian matrix has been proposed as an index for quantifying proximity to the voltage collapse point [14]. It is an indicator easily available from normal load-flow calculations. The method is based on the analysis of a linear system. The singular value decomposition is applied to the linearized load-flow equations to analyze power system voltage stability. The analysis studies the influence of a small change in the active and reactive power injections to the change of angle and voltage. A Jacobian matrix is a linearisation at the operation point and the voltage stability problem is non-linear in nature. If the operation point is far away from the voltage collapse point, then the minimum singular value does not describe the state of the system accurately. Thus, the minimum singular value of a load flow Jacobian matrix is also sensitive to the limits on generator reactive power output, transformer tap settings and static var compensation devices.

The point of collapse method is a direct method [15]. It computes the voltage collapse point, the power demand, and corresponding state variables directly without computing intermediate load-flow solutions. The method is based on bifurcation theory and the singularity of the load-flow Jacobian matrix. In applying bifurcation theory to power systems, the power demand is often used as the slowly changing parameter. A voltage collapse point is found by changing the parameter in a specified direction.

The purpose of the continuation load-flow is to find a continuum of load-flow solutions for a given load/generation change scenario (or computation direction) [16]. It is capable of generating the full PV curve. The continuation load-flow finds the solution path of a set of load-flow equations that are reformulated to include a continuation parameter. This scalar equation represents phase conditions that guarantee the non-singularity of the set of equations. The method is based on prediction-correction techniques. Another direct computation method of voltage collapse point is the optimization method [17] With this approach, the voltage stability margin is maximized according to the load flow equations and power system constraints. Generally, the optimization is not global over the parameter space.

2.1.3 Remarks

Bridging the gap between the practical procedures employed to determine power system interface limits and the various proposed methods for on-line security requires consideration of a number of factors.

- Operational planning methods cannot identify all possible operating conditions that may arise and are generally too slow to repeat on-line when unstudied system conditions arise.
- Operators do not have full access to all the detailed assumptions that might have been used in an off-line study. Furthermore, they only have access to the

- conclusions of a study (i.e., the actual transfer limit and limiting outage) and not all the underlying case studies that might have been performed.
- Many of the proposed on-line security methods are fast methods to determine security but are not as effective at determining a practical operating limit, such as the transfer between systems.
 - The various proposed on-line security methods work well under certain conditions but will fail at other times in ways that may not be well understood.
 - Most of the on-line security methods do not base assessment on the detailed reliability requirements employed by the various regional councils.
 - Practical system security assessment always has a certain degree of system specific considerations that do not lend themselves to more formal analysis.
 - Most operators are not well versed in the computational techniques employed in security analysis and are hesitant to place confidence in “black box” approaches.

2.2 WSSC Reliability Criteria

This section provides a detailed discussion of the WSCC reliability criteria to establish the environment for operations. Continuity of service to loads is the primary objective of the reliability criteria. Preservation of interconnected operation during a disturbance is secondary to the primary requirement of preservation of service to loads. Although allowing for the possibility of failures, each system within the WSCC must strive to protect its customers against loss of service. The reliability criteria may be defined and measured in terms of the performance of a system under stress conditions. Prediction of performance requires extensive simulation because actual tests on existing systems are not practical.

2.2.1 Performance Levels

The reliability councils specify different performance levels based on the severity of a disturbance. The minimum allowable performance levels for interconnected bulk power systems range between having no appreciable adverse system effects to having substantial effects, perhaps involving load shedding and controlled islanding. The minimum level of performance that is acceptable under simulation tests is presented in Table 1, referred to as the “Disturbance-Performance Table.” This table defines the performance to be expected for a given class of initiating disturbances. A higher level of performance is required for disturbances that generally occur with a higher frequency or likelihood.

Types of elements lost due to various disturbances are listed in the Disturbance-Performance Table in descending order of frequency and increasing order of severity. Performance is specified as five discrete levels: A, B, C, D and E. Levels A through D do not permit any uncontrolled loss of generation, load, or uncontrolled separation of transmission facilities. For Level E disturbances, uncontrolled loss or separation may

occur. Within Level E, a number of extreme contingencies that are judged to be critical by the transmission planning entity are selected for evaluation. Initiating events must be viewed as being associated with a specified performance level.

The Disturbance-Performance Table portrays these ranges by giving several examples of disturbances considered under each category; however, it is not exhaustive. Only a limited number of all possible facility outages under each listed contingency are evaluated. The examples presented should provide a basis for estimating performance levels for disturbances that are not listed. When multiple elements are specified, they are assumed to be lost simultaneously. In cases where a prior outage exists on a system, system adjustments will be made to allow the system to meet the required performance specified for the next disturbance. As an example, the loss of a generator with a prior system condition of one generator out is not considered a simultaneous loss of two generators. The table applies equally to either of the following: (1) a system with all elements in service; or (2) a system with one element removed and system adjustments made following the outage.

The different levels are summarized here below with details given in Table 1 [7].

- Level A performance should produce no significant adverse effects outside of the system in which the disturbance occurs. This includes loss of load (firm or interruptible) or facility loadings that are outside emergency limits.
- Level B performance allows for some adverse effects that may occur outside of the system in which the disturbance occurs. For example, interruptible load shedding may occur, but there should be no loss of firm load. Facility loadings should remain within emergency limits.
- Level C performance allows substantial adverse effects outside of the system in which the disturbance occurs. Firm and interruptible load shedding may occur, but facility loadings should remain within emergency limits.
- Level D performance seeks only to prevent cascading and the subsequent blackout of islanded areas. Some additional adverse affects may occur, including firm and interruptible load shedding or sustained (but not growing) oscillations.
- Level E performance seeks only to evaluate risks and consequences. Additional adverse system impacts that may occur are substantial loss of customer demand and generation in a widespread area or areas. Portions or all of the interconnected systems may or may not achieve a new, stable operating point.

Table 1 WSCC Disturbance-Performance Table of Allowable Effects on Other Systems [7]

Performance Level	Disturbance: - No fault - 3-phase fault with normal clearing - Single line to ground fault with delayed clearing - DC Disturbance	Transient Voltage Dip Criteria	Minimum Transient Frequency	Post Transient Voltage Deviation	Loading Within Emergency Ratings	Damping
A	Generator One Circuit One Transformer DC Monopole	Max V Dip - 25% Max Duration of V Dip Exceeding 20% - 20 Cycles	59.6 Hz Duration of f Below 59.6 Hz – 6 cycles	5%	Yes	>0
B	Bus Section	Max V Dip - 30% Max Duration of V Dip Exceeding 20% - 20 Cycles	59.4 Hz Duration of f Below 59.4 Hz – 6 cycles	5%	Yes	>0
C	Two Generators Two Circuits DC Bipole	Max V Dip - 30% Max Duration of V Dip Exceeding 20% - 40 Cycles	59.0 Hz Duration of f Below 59.0 Hz – 6 cycles	10%	Yes	>0
D	Three or more circuits on common ROW			Cascading is not permitted		
E	Loss of multiple 500 kV or higher circuits (3 or more) that cross one another at 1 location Loss of 3 or more circuits that share a common linkage Loss of entire plant with 3 or more generating units Loss of entire substation Loss of multiple circuits, multiple generators, or circuits and generators that have no common mode of failure			Evaluate for risks and consequences		

Table 2 WSCC Voltage Stability Criteria [18]

Performance Level	Disturbance: - Fault or No Fault - DC Disturbance	MW Margin	MVAR Margin
A	Any element such as: One Generator One Circuit One Transformer One reactive Power Source One DC Monopole	$\geq 5\%$	Worst Case Scenario
B	Bus Section	$\geq 2.5\%$	50% of Margin Requirement in Level A
C	Any combination of two elements such as: A Line and a Generator A Line and a Reactive Power Source Two Generators Two Circuits Two Transformers Two Reactive Power Sources DC Bipole	$\geq 2.5\%$	50% of Margin Requirement in Level A
D	Any combination of three or more elements such as: Three or More Circuits on ROW Entire Substation Entire Plant Including Switchyard	> 0	> 0

2.2.2 WSCC Voltage Stability Criteria

It is well known that voltage magnitudes alone are poor indicators of voltage stability or security. Voltages can be near normal levels with generators, synchronous condensers, and SVCs near current-limiting levels, thus resulting in a possible voltage collapse. Therefore, it is prudent to specify a MVar margin or MW margin. In the WSCC, voltage stability criteria are expected to apply equally to studies of interfaces and load areas. Interfaces include major WSCC paths, tie lines with neighboring systems, and critical paths within a system. The WSCC voltage stability criteria are specified in terms of real and reactive power margins. The margin for *N-0* (base case) conditions must be greater than the margin for performance level A to allow for unforeseen increases in load or interface flows without remedial action schemes that would be activated during contingency conditions but not during normal conditions.

Table 2 lists the voltage stability criteria and the minimum margins for each disturbance level. Again, these apply equally to the system with all elements in service as well as the system with one element removed, and follow the general philosophy that a higher level of performance is required for disturbances generally having a higher frequency of occurrence. The system elements include any facility, such as a generator, transmission line, transformer, and reactive power source. The determination of credibility for contingencies is based on the definitions used in the WSCC Reliability Criteria [7]. The contingencies to be studied include the outage of any system elements that would impact the required margins. When multiple elements are specified, they are assumed to be lost simultaneously. In cases where a prior outage exists, system adjustments should be made to allow the system to meet the required performance specified for the next disturbance. As an example, the loss of a generator with a prior system condition of one generator out is not considered a simultaneous loss of two generators, as indicated above,. This is because the system should be re-dispatched or other corrective actions should be initiated following the outage of the first generator.

From Table 2, the performance level A margin requirement is 5%, decreasing by one-half for subsequent performance levels. The 5% quantity refers to the KSP for a given study. Thus, if the study considers a transfer across a key interface, then it is 5% of that flow that establishes the required margin. These numbers are subject to re-evaluation by the WSCC, but they are generally representative of current practices.

2.3 Estimation of Stability Margins

The previous discussion establishes the need for fast and accurate tools to evaluate security. For on-line application, a pattern matching or interpolation method rather than analytic approaches may be most appropriate. Among the alternative methods, artificial neural networks (ANNs) is the most promising [19] because ANNs have excellent

generalization capabilities, superior noise rejection, and fast execution (with most of the calculations occurring during the initial off-line training).

Over the past decade, a number of approaches using artificial neural networks have been proposed as alternative methods for DSA in power system operations. Sobajic and Pao proposed a technique using a multi-layered network to predict the critical clearing time (CCT) for a given system disturbance [20]. In their paper, the authors showed that the neural networks generalize to previously unencountered system topologies and load levels, and correctly estimate CCTs. In a follow-up paper, they presented a combined unsupervised and supervised learning algorithm to solve the same problem [21]. The input data were pre-processed using an unsupervised learning system to enhance the accuracy of the supervised learning algorithm.

El-Sharkawi et al exploited a multi-layer perceptron to predict the dynamic stability status of a power system [22]. A layered perceptron was trained to learn the mapping between system operating state, active and reactive power injections in some system buses and the corresponding dynamic security status. Kumar et al [23] discussed implementing a neural network for DSA in a large system, and proposed a hybrid expert system/neural network approach. The hybrid approach uses the knowledge of system operators in training neural networks. Mansour et al [24] proposed a neural network approach to provide contingency screening and ranking in dynamic security. The BC Hydro and Hydro-Quebec systems were used to test the network. Static and dynamic features were used as inputs, and the selected outputs were energy margin and maximum swing angle. In our previous work [4], an ANN was applied to estimate Q-V margins in the WSCC system.

The primary limitation of the above approaches has been their failure to fully employ the system specific studies used in practice. This project addresses that limitation by using the exact WSCC reliability criteria in the system security studies.

3 Operations Issues

Security analysis is done, to some degree, to support planning and operations functions. In the planning function, time is not critical and extensive security studies can be performed without the performance constraints of analyses done to support operations. However, in the planning function, the base case condition is not known with certainty. While there is some uncertainty associated with establishing the base case in operations analyses, there is generally much less uncertainty about topology and state values. The primary need for security analysis is critical in meeting operations functions. However, combined security analysis concepts discussed in this section are also valuable for planning functions.

3.1 Combined Security Analysis Concepts

This project's primary focus is on developing a method that can systematically combine the results of different types of security analysis into one comprehensive framework. One objective of this focus is to avoid overlap of repeated computational algorithms. This overlap can be avoided if capabilities or margins can be computed for classes of designs or conditions that are independent of time and of load distribution. An existing example of this independence, in a basic form, is the "St. Clair" curve [25] that addresses six basic factors limiting the capability of a transmission line: voltage level, stability, line current, net reactive loss, resistance loss, and actual temperature rise. When used to compute the permissible loading for lines of various lengths, the limiting factors can be compressed into a single curve giving line loadability in SIL (Surge Impedance Load) vs. line length, as shown in Fig. 1 below.

This original St. Clair curve was the motivation for an analytical formulation of line limits of higher voltages and longer lines [26]. The analytical model used a "pi" section for the transmission line, with sending-end and receiving-end equivalent lines and sources. This simple equivalent was then used to evaluate the loadability with the criteria of thermal rating, voltage drop, and steady-state stability margin (based on the angle across the system). This analytical model allows the reproduction of the existing St. Clair curves as well as their extension to other voltage levels, line lengths, and system parameters. The conclusion was that lines are thermally limited when they are less than 50 miles long. In addition, between 50 and 190 miles, the loading is limited due to the voltage drop across the line. Finally, for lines longer than 190 miles, the loading is limited due to the steady-state stability margin across the system. Caution in generalizing these conclusions was expressed in [27] because the reactive power supply capability was shown to be a critical parameter in allowing the stability margin portion of the St. Clair curves to be correct.

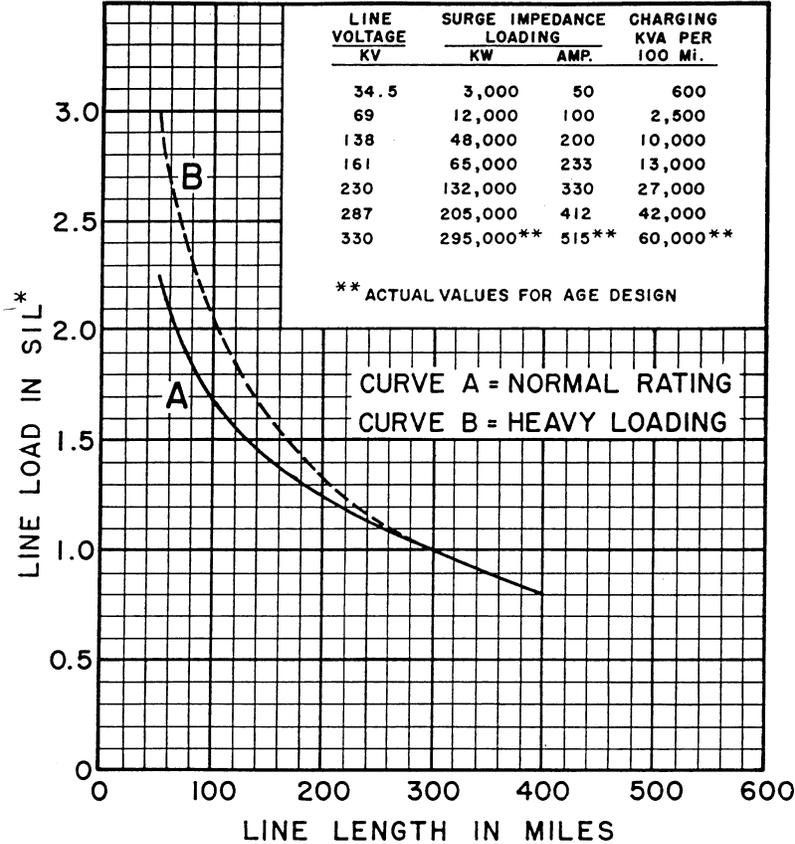


Fig. 1 St. Clair curve

Most recently, the difference between MVA and MW limits on lines was examined in relation to power transfer capabilities. Techniques to convert between these limits, and other issues associated with reactive power considerations, are described in detail in [28].

While knowing the constraints on lines and corridors is an important part of security analysis and dispatch, knowing how to change the constraints is also important. Translating individual constraints due to thermal, voltage, and stability limitations into a line flow (MW) limit hides the actual cause of the constraint. In addition, the line flow limit does not indicate how the constraints might be relaxed by operator actions, or by addition of new facilities or components. For example, if the true constraint is a voltage drop limit, the possible methods to increase the constraint might involve siting new reactive power sources, such as capacitors or reactive power devices. These remedial designs could indeed increase the line flow (MW) limit more directly and more economically than upgrading the line capacity through construction of parallel lines. Thus, the integration of security analysis tools must be done carefully and with the

understanding that all options should be considered to provide meaningful results for security enhancement.

An additional approach to integrating security analysis involves prioritizing the various security analysis tools and the phenomena that they are designed to capture. For example, it should not be necessary to perform steady-state analysis or voltage stability analysis to simply determine the stability of a post-contingency condition if time domain simulation is used to assess transient stability. As a matter of contingency screening, the integrated security analysis should use fast computational methods to determine insecure contingencies. In other words, if a contingency results in a simple-to-compute thermal overload, then there is no need to conduct the more difficult analyses of voltage or stability insecurities. This indicates that the integrated analysis should start with phenomena that are easy to compute, and then proceed to more difficult analysis only if all contingencies pass the simple tests.

3.2 Operator Surveys

This project included several surveys of operators and operation planning engineers. The purpose of the surveys was to identify existing tools that are in frequent use as well as to identify any tool-development needs that may exist in typical operations environments. In almost all cases, the actual security “calculations” performed in the operations environment focused on static security assessment only. All of the surveyed operators indicated that full AC load flow was the primary security analysis tool. Transient stability or voltage collapse issues were only evaluated when the full AC power flow indicated an unusual operating condition (such as questionable voltage profiles). When voltage collapse or transient stability problems were suspected, the analysis was transferred to operations planners for detailed analysis. Some operators were guided by seasonal nomograms that were cataloged according to primary corridor loadings or into “operator guidelines”. In several cases, operations personnel performed extensive time-domain simulations during day-ahead operations planning. In some cases this lack of dynamic security analysis activity was due to a lack of problems, or of interest in these phenomena. In other cases, it was due to a lack of efficient and integrated tools.

Of those operators that only performed static security analysis, there was an equal interest in finding voltage collapse and transient stability analysis tools. In many cases, the delay in finding these tools had to do with their low priority among other operational tasks, or high perceived overhead in getting the tools operational and maintaining new models. For those operators that were interested in future transient stability tools, there was a strongly expressed concern that these tools should require operators to process a minimal amount of information. In one case, the operators expressed a need for a program that would systematically examine possible fault current levels after contingencies or planned outages to ensure that the protection system fault duties were adequate. Additional details of these operator surveys will be documented in a report for the Integrated Security

Analysis project nearing completion by the Consortium for Electric Reliability Technology Solutions (CERTS, <http://certs.lbl.gov>).

4 Proposed Methodology

In this section, a framework is introduced to integrate the various security assessment methods outlined above and to take advantage of the benefits of using pattern matching approaches. Power system security assessment can be divided into two categories: classification and security limit determination. Classification includes determining whether the system is secure or insecure under all pre-specified contingencies. Classification does not indicate the distance from the base operating condition to the insecure conditions. Security limit determination, on the other hand, involves finding this distance. Safe operating levels based on various system conditions are given in terms of the KSP (e.g., loading of a certain power plant, the power flow at a critical transmission interface, and the voltage at a given bus).

The reliability standards require that the system be operated with sufficient margins to withstand any single contingency without experiencing overloads, low voltages, sustained oscillations or excessive frequency dip. For most utilities, the margin for each study case is used to produce a nomogram. Typically, the nomogram is a two-dimensional graph with the two axes corresponding to two critical parameters. All other critical parameters are set to selected values within a typical operating range.

In our framework, the power system security limit, in response to all predefined contingencies, is investigated for a given pre-contingency steady state of the system. The loading is varied to determine the security margin relative to each of the reliability criteria. The allowable margins and associated reliability criteria are those outlined in Section 2 based on WSCC guidelines for performance level A [7].

4.1 Overall Security Framework

The primary method to take better advantage of the off-line operational studies is to form a type of associative memory. In each study case, system conditions and the estimated security margin are recorded. There are several conclusions from our analyses using this approach.

- Simple linear regression models cannot accurately estimate security margins.
- Feedforward ANNs have the best understood design criteria and, for this type of estimation problem, display the most favorable performance.
- No single estimator appears to be workable across a variety of security indices or widely different network topologies regardless of the number of study cases.

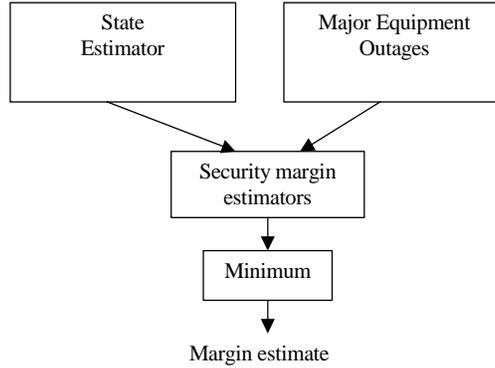


Fig. 2 Overall security margin estimation

- A family of smaller ANNs with different network parameters whose estimates are combined through a voting mechanism will perform better than a single large ANN.

As a result of our findings, we use several layers in the on-line estimation of security limits. At the highest level, the current state and major equipment outages are used to identify the appropriate set of margin estimators. This is depicted in Fig. 2. At this point in the development of the integrated security analysis framework, the minimum of all the estimated security margins is used because we have full confidence in the detailed models used to calculate the margins. However, a conceivable extension would be to allow for approximations, where the estimator is estimating a less precise margin. That approach is not investigated in this project to avoid ambiguities in the findings that may arise due to use of some particular index.

The set of estimators includes different estimators for different topologies. This does not imply a separate estimator for each outage scenario. For example, one estimator may represent (1) the base case, (2) a wide range of operating conditions, and (3) one or two major equipment outages. Another estimator could represent a similar set of operating conditions, except for different major equipment outages. This is in addition to the fact that the calculated margin is based on all chosen contingencies. As a result, each estimator could represent several nomograms. This is emphasized graphically in Fig. 3.

At the lowest level, a family of ANNs is used to estimate the security margin for a specific security criterion and operating condition. Fig. 4 shows the structure of an estimator for a given set of operating conditions and a specific security criterion.

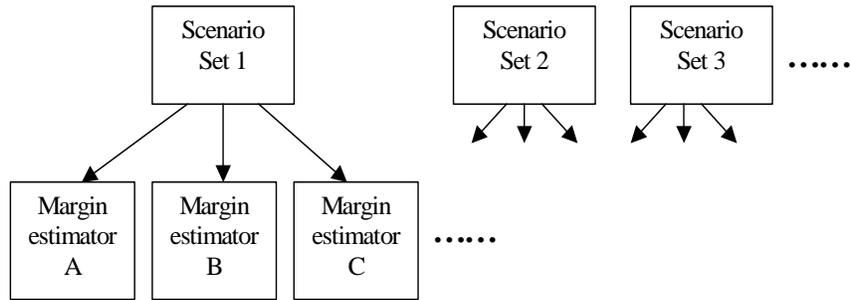


Fig. 3 Hierarchical structure of security margin estimators

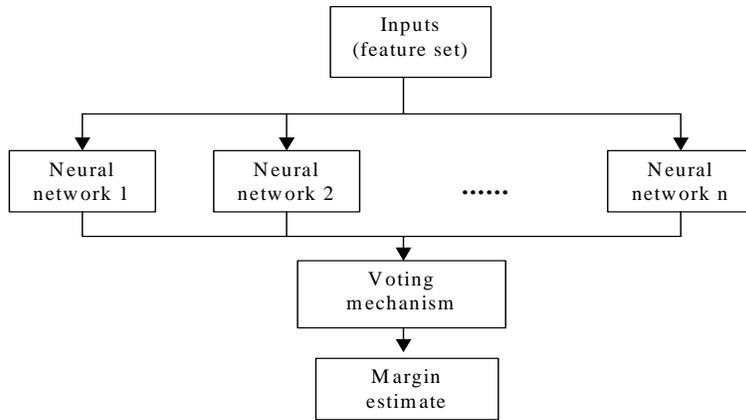


Fig. 4 Individual estimators with voting mechanism

4.2 Generation of Training Data

To determine the transient stability transfer limits or loading margins, a load flow must first be executed to insure that a given topology provides a satisfactory steady-state case. This steady-state case is then applied to initialize the network for the transient-stability simulation program. The program we use is the Extended Transient/Midterm Stability Program (ETMSP). When the simulation is completed, reliability criteria are applied to the extracted results from ETMSP. If the performance is adequate, then the loading is incremented and the load-flow software inputs are modified accordingly. This is repeated until the highest acceptable transfer level for an interface is found.

In general, to find the security limit, the process must be repeated for different contingency types and locations until the most constraining (i.e., lowest) transfer limit has been identified. It is impossible to pre-study all possible contingencies because the assessment processes are very time-consuming, and the analysis of every degraded topology is a problem of combinatorial dimensions.

For each of the system performance criteria identified in section 2.2, the limits of the power system operation are established. These limits may be total load in an area, interface transfer limit, or some other KSP. Starting from a base case, the set of relevant system variables is recorded and a full analysis of all major contingencies is performed. The KSP is incremented and the analysis repeated until the system limits are identified. Thus, for each performance criterion, there is a large set of studies that establish the operating limit and a correspondingly large set of variables describing the operating conditions.

There are three software packages used in the studies.

IPFLOW [29]

IPFLOW is interactive power flow software developed by EPRI. For the dynamics studies, it provides the initialization before any disturbances are considered.

VSTAB [30]

The VSTAB (Voltage STABILITY) program, developed by Ontario-Hydro with EPRI support, is a voltage stability assessment package for large complex power systems. It provides information on the proximity to and mechanisms of voltage instability. VSTAB uses a power flow (i.e., a steady state technique) for voltage “stability” analysis.

ETMSP [31]

The ETMSP (Extended Transient/Midterm Stability Program) package developed by Ontario-Hydro with EPRI support. It is used to analyze power system dynamics following disturbances.

4.3 Estimator Design

The simplest form of an estimator is a simple linear regression model. If we assume that the relationship between system variables and the margin can be modeled by a linear combination of first and second order terms, then we can write:

$$Y = \beta_0 + \beta_{11}X_1 + \beta_{12}X_1^2 \cdots + \beta_{1n}X_n + \beta_{n2}X_n^2 + \mathbf{e} = \mathbf{X}\boldsymbol{\beta} + \mathbf{e} \quad (1)$$

where Y is the observation (for us, the security margin) and X is the input feature set (e.g., line flows). The maximum likelihood (or unweighted least-squares) estimate of the parameters β is simply:

$$\hat{\beta} = (X^T X)^{-1} X^T Y \quad (2)$$

Of course, there are number of variations that can be introduced in this basic model. However, as will be seen, the non-linearities of the security analysis problem generally render the linear model approach problematic. The basic linear regression model is introduced to show the difficulty of simple interpolation. The estimators proposed in this work are feedforward ANNs based on the Levenberg-Marquardt and Bayesian Regulation algorithms [5]. Primary considerations in design of the neural network are outlined in the following section.

4.3.1 Feature Selection and Processing

Selected features should be based on engineering knowledge and statistical correlation between the selected features and the margins computed from security studies. Typically these features will be variables such as real and reactive power flow, reactive power reserve, and voltage levels. A large set of features can be selected and then carefully reduced based on correlation coefficients.

This stage is an extremely important pre-processing step, as selected features must properly characterize a variety of power system operating conditions. Generally, the dimension of the pattern vector is very large. Feature selection is the process of finding the most significant variables, eliminating redundancy, and reducing the dimension of the pattern vector. A number of different methods, most based on statistical approaches, are available for feature extraction (i.e., reducing the dimension of the input data vector). The parameters that may be applied to describe a system state are:

- voltage magnitude and phase angle at each system bus,
- active and reactive power of each bus load,
- active and reactive power flow of all the lines, and
- active and reactive power output of each generator plant.

The selection and extraction process involves engineering judgment and statistical analysis. The statistical analysis uses correlation coefficients and principal components analysis. The correlation coefficients between the selected features and the computed security margin are determined first. Subsequently, principal components analysis can be used. Principal component analysis (PCA), also called Karhunen-Loeve expansion, assesses the independence of the features in the selected feature set [5]. The PCA method determines the eigenvectors corresponding to the largest eigenvalues of the auto-correlation matrix of training vectors as its principal components. The reduced training

vectors are selected in the direction of the most dominant eigenvectors. In essence, an orthogonal set of features is sought to present to the estimator, improving both training time and accuracy. For example, for the P-V margin estimator for the WSCC system [4], the 106 system variables were reduced to 46 for training. The ANN is then trained with this new set of reduced vectors. This extraction closely relates to the performance of a neural network and computation time because the fewer the number of features, the fewer are the number of required samples.

4.3.2 Network Structure, Hidden Layers and Voting Schemes

Generally, multiple hidden layers improve the approximation process. Two hidden layers are needed when finding estimates for larger systems with more complicated non-linearities. The number of nodes in the hidden layers significantly impacts the performance. In the Bayesian framework of MacKay [32], the parameters are estimated using statistical techniques. Several ANNs with parameters near the calculated optima are trained. The estimates from these networks can be combined using a voting scheme. For example, one effective method is to disregard the lowest and largest margin estimates from such a set of networks and then average the remaining estimates.

4.3.3 Splitting Training Data for Estimation and Validation

A statistical theory of the overfitting phenomenon that may occur with ANNs is presented in [33]. If N is the size of the training set and W is the number of free parameters in the network, with $N < W$, the optimum split of the training data between estimation and validation subsets is given by

$$r_{opt} = 1 - \frac{\sqrt{2W - 1} - 1}{2(W - 1)} \quad (3)$$

where r_{opt} is the fraction to be used for training.

5 Numerical Results

This section presents detailed analysis of the proposed methodology applied to (1) a small test system, a modified IEEE 39 bus system, and (2) a large practical system, a model of around 6500 buses of the WSCC system.

5.1 Studies on IEEE 39 Bus System

5.1.1 System and Case Study Description

To illustrate the proposed approach, the New England 39 bus system was chosen. As shown in Fig. 5, the system is divided into two zones, one load center of only the load buses 17, 18, and 27, with three tie lines 3-18, 16-17, and 26-27. The other zone contains all other load and generation buses. The focus of study is on the power flow at the interface of this load center. The study applies only on the WSCC disturbance criteria for performance level A [7] considering only three phase faults with normal clearing.

The security margin is calculated by increasing the active power of the load center incrementally over the base case until there is a violation of the reliability criteria. The total system loading for the base case is 6150.5 MW and 1658.90 MVar. The flow across the interface of this load center is the parameter of interest. The entire data set consists of 983 samples, 20% for testing and 30% for validation. The training and testing data are obtained from transient stability studies using IPFLOW and ETMSP. Contingencies considered are three-phase faults on each line. For each load level, there are 31 cases, representing one base case and the 30 (n-1) contingencies.

5.1.2 Analysis

The first performance criteria considered is voltage stability as seen by the post-disturbance voltage response. The maximum voltage dip at any bus following a contingency cannot exceed 25% and a more than 20% dip cannot last for more than 20 cycles. The post-transient voltage dip should not exceed 5%. Finally, there must be positive damping. At times, these criteria will overlap with the dynamic security criteria.

Table 3 shows the statistics of the errors encountered using simple linear regression on first and second order terms of the reduced variable set. The average error is probably acceptable, but there are instances of large errors that would result in misclassification of the security. Fig. 6 plots the absolute and percentage errors for this linear estimator. The possibility of large errors for small margins can be seen. The designed ANN has a single hidden layer with 10 hidden nodes. There are 131 test cases of which 20% are used for testing. The overall performance is shown in Table 4. The results indicate very low percentage errors.

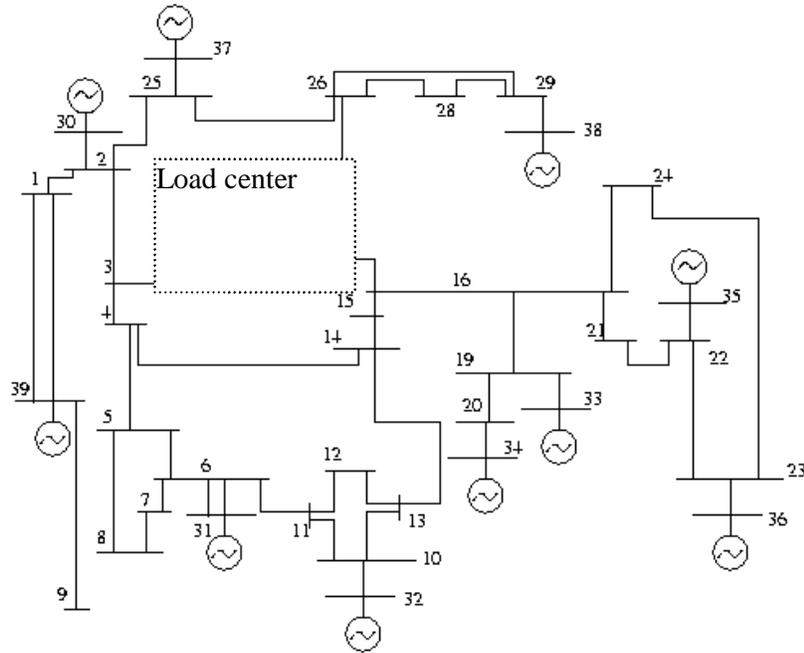


Fig. 5 New England 39 bus system

The second analysis is on estimation of the loading margin relative to transient frequency criteria (59.6 Hz – 6 cycles). The active and reactive power flows of all lines are used as the features to describe a system state. The ANN is trained using the data from the off-line operational studies. Initially, there are 96 total features (i.e., the active and reactive power flow of all the lines). These reduce to 31 features using principal components analysis. Statistical correlation coefficients were used to further reduce the dimension of the pattern vector to 11 elements. An ANN with 21 neurons in the single hidden layer was implemented using the Levenberg-Marquardt algorithm, and an ANN with 7 neurons of the single hidden layer was found to be adequate for Bayesian Regularization backpropagation. Since this is a rather small system, satisfactory performance is obtained using a simplified estimator of only one ANN.

The results, shown in Tables 4 and 5, indicate that more than sufficient accuracy is obtained using very small networks. The performance of the ANN using the Bayesian Regularization algorithm is more accurate than the Levenberg-Marquardt algorithm. Further, since the Bayesian algorithm has fewer hidden neurons, training using this algorithm is faster in computation time.

Table 3 Errors from linear regression of voltage security limits for 39 bus system

Max Error (MW/%)	Min Error (MW/%)	Mean Error (MW/%)	Standard Deviation (MW)	MSE (MW ²)
52.04/52.04	0.02 / 0.002	10.92/2.37	13.61	185.16

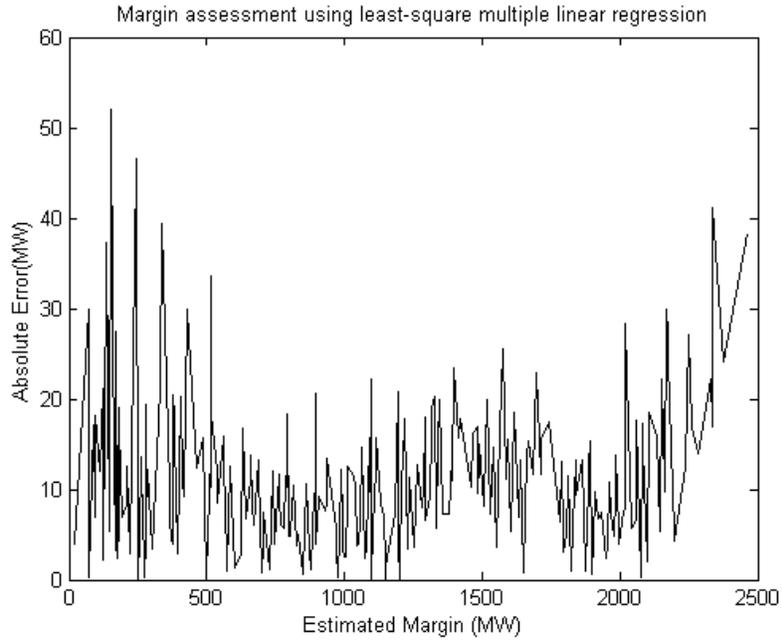
Table 4 Errors from ANN estimate of voltage security limits for 39 bus system

Max Error (MW/%)	Min Error (MW/%)	Mean Error (MW/%)	Standard Deviation (MW)	MSE (MW ²)
Levenberg-Marquardt				
2.95/2.50	0.0036/0.0005	0.63/0.15	0.73	0.72
Bayesian Regularization				
1.84/2.76	0.0011/0.0002	0.31/0.097	0.43	0.20

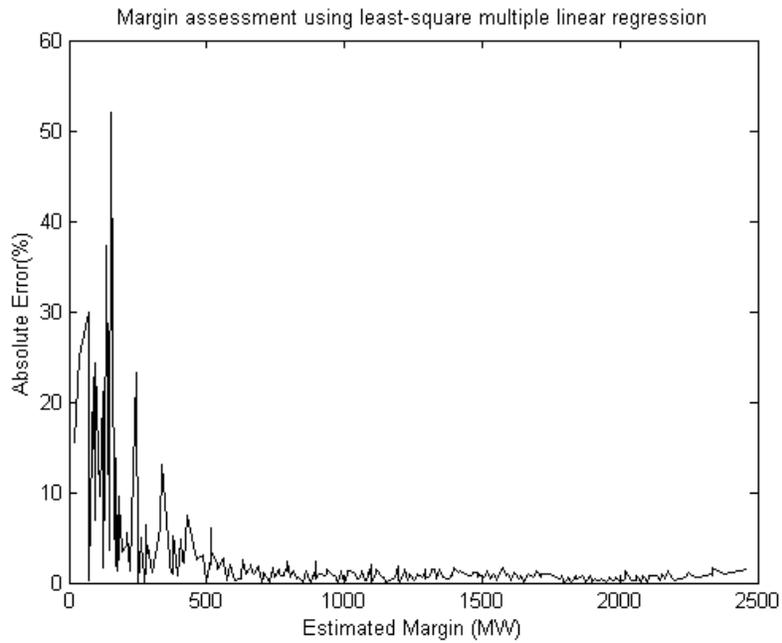
Table 5 Comparison of training routines on dynamic security estimator for 39 bus system

Max Error (MW/%)	Min Error (MW/%)	Mean Error (MW/ %)	Standard Deviation (MW)	MSE (MW ²)	Hidden neurons
Levenberg-Marquardt					
8.19/3.88	0.0024/0.0005%	0.49/0.15%	0.80	0.64	21
Bayesian Regularization					
1.07/1.90%	0.0014/0.0002%	0.15/0.11%	0.20	0.04	7

Figs. 7 and 8 show the plot the errors versus the magnitude of the voltage security margin. The errors are generally low where the margin tends to be large so there are no misclassifications of security. Figs. 9 and 10 show similar results for the dynamic security criteria. For the dynamic security, there is greater error near the lower margins, which could lead to misclassifications of security. However, the accuracy of the estimates for the voltage and dynamic security cases is more than adequate.

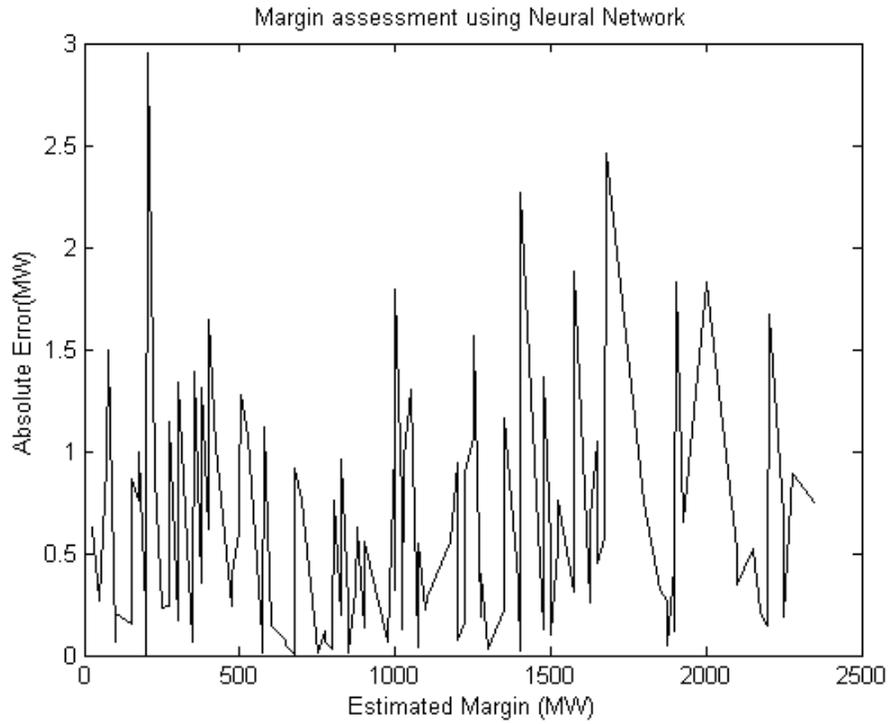


(a) MW error

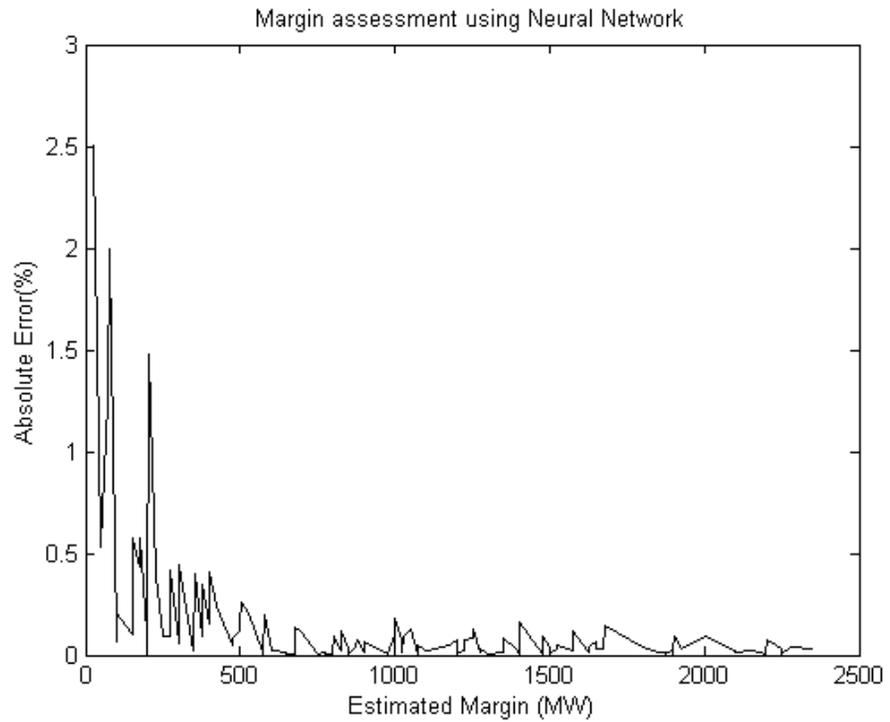


(b) % error

Fig. 6 Voltage security margin estimates using linear regression for the 39 bus system

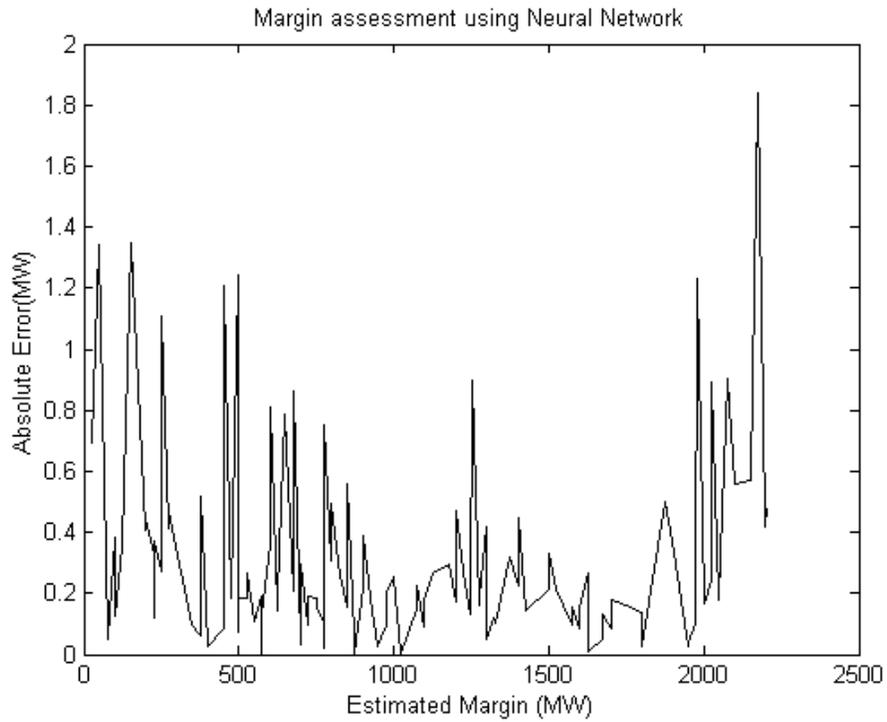


(a) MW error

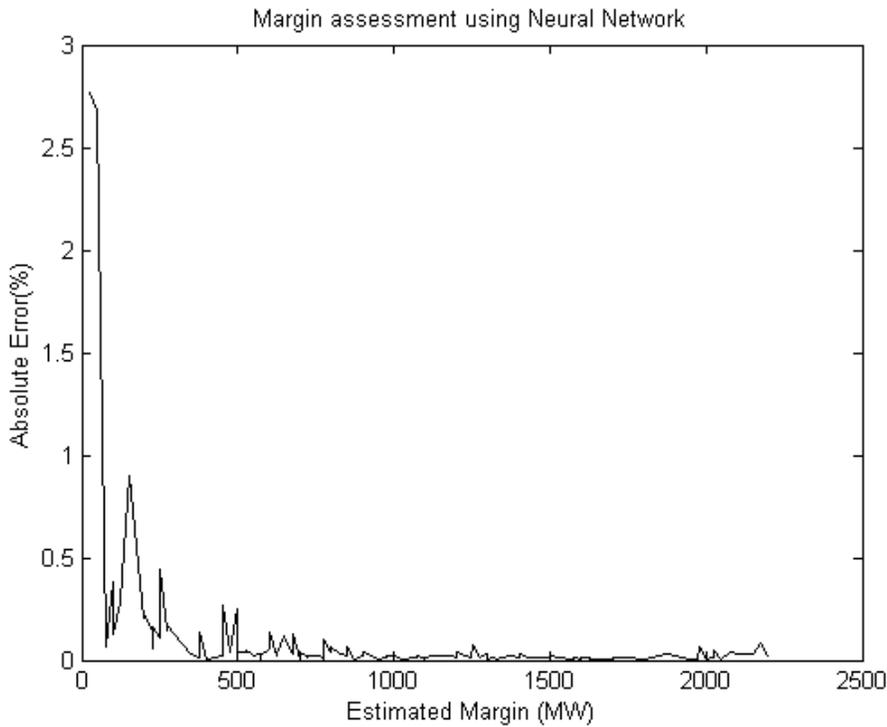


(b) % error

Fig. 7 Voltage security margin estimates using ANN with Levenberg-Marquardt training for the 39 bus system

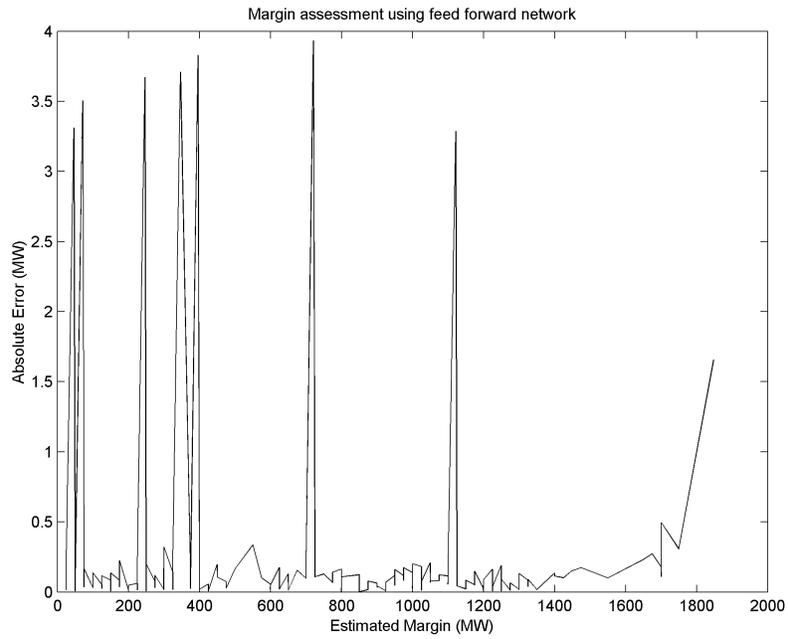


(a) MW error

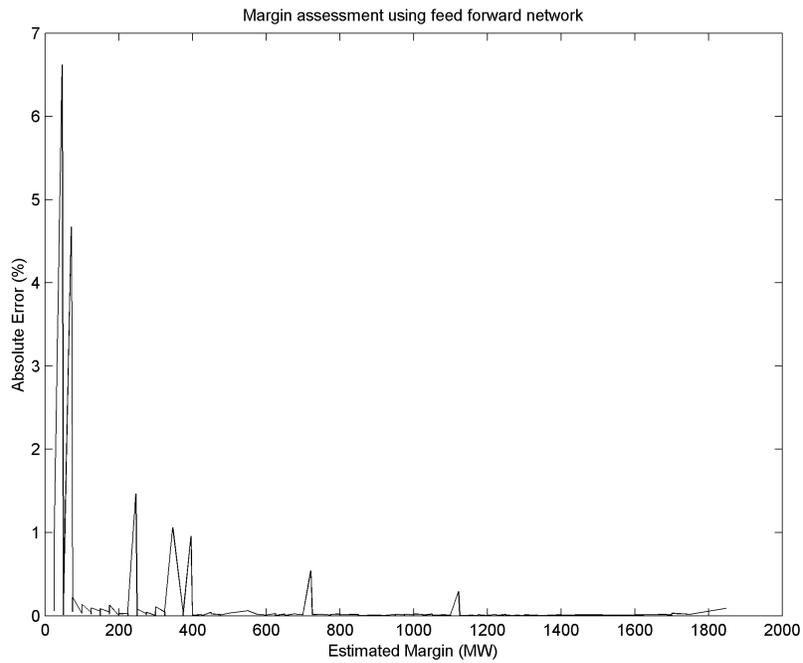


(b) % error

Fig. 8 Voltage security margin estimates using ANN with Bayesian Regularization training for the 39 bus system

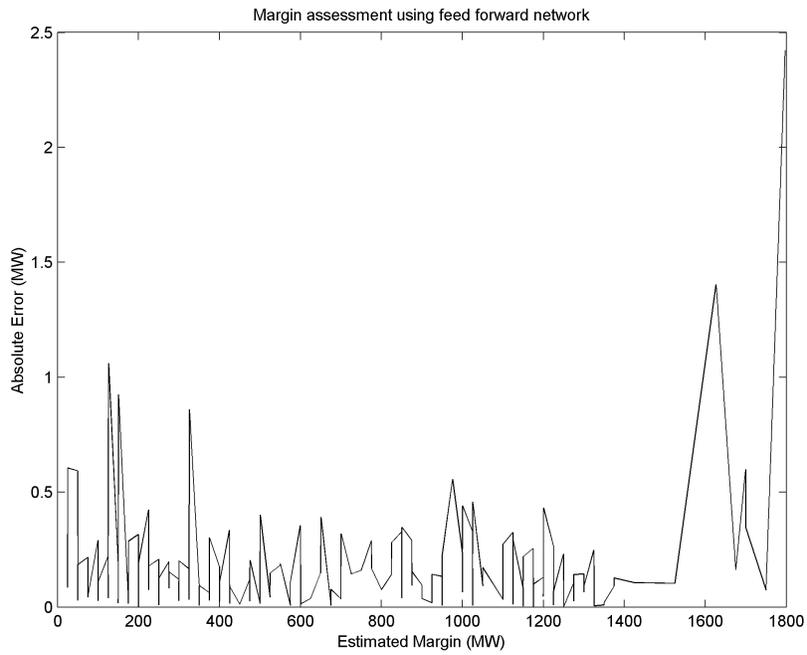


(a) MW error

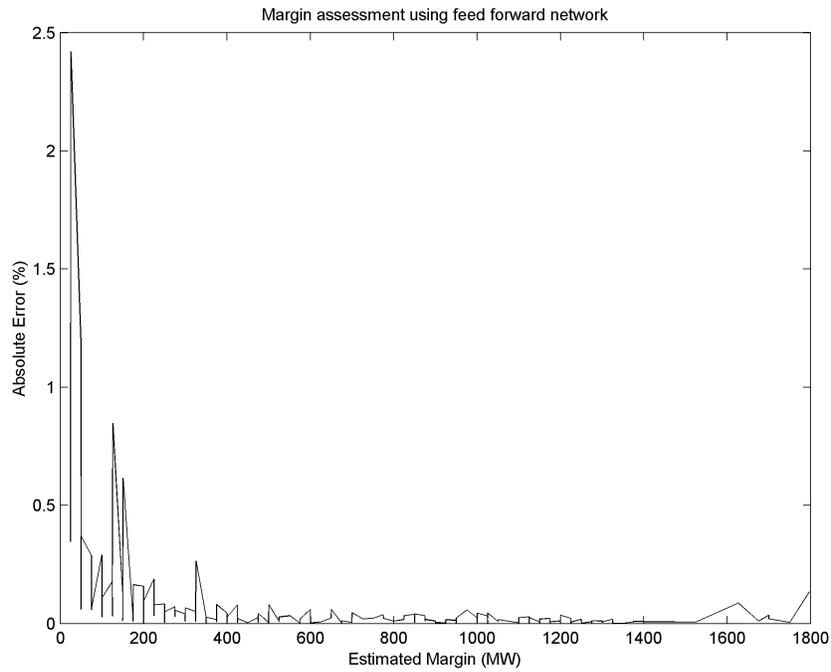


(b) % error

Fig. 9 Dynamic security margin estimates using ANN with Levenberg-Marquardt for the 39 bus system



(a) MW error



(b) % error

Fig. 10 Dynamic security margin estimates using ANN with Bayesian Regularization training for the 39 bus system

The combination of PCA and statistical correlation greatly reduced the number of needed features. This implicitly assumes that the training truly captures salient characteristics of these features. Furthermore, data or training sets must be representative of the different states of the power system since ANNs are designed for interpolation rather than extrapolation.

5.2 Studies on WSCC System Model

The proposed methodology was successfully applied to estimate the transfer limits on the WSCC system using a static method, P-V curves, to determine voltage security limits [4]. In this section, application of the full performance level A criteria is examined.

5.2.1 System and Case Study Description

The Western Interconnection encompasses a vast area of nearly 1.8 million square miles. The Western Interconnection is defined as the Western Systems Coordinating Council (WSCC) region, which is the largest and most diverse of the ten regional reliability councils of the North American Electric Reliability Council (NERC). It encompasses all or part of fourteen western states, two Canadian provinces, and portions of northern Mexico. It has characteristics that are distinct from the other three North American Interconnections. The WSCC divides into four geographic subregions: California, Northwest, Arizona/New Mexico/Southern Nevada, and Rocky Mountain. About sixty percent of the WSCC load is located in the coastal regions. A significant portion of the generation that serves these load centers is located inland, so transmission over long distances is needed. As a result, significant portions of the WSCC network are stability limited. Fig. 11 shows the major transmission paths of the WSCC system. The primary interface of interest in this study is the California-Oregon Intertie (COI). The COI consists of the two Malin-Round Mt. 500kV transmission lines (referred to as the Pacific AC Intertie) and the Captain Jack-Olinda 500kV line (referred to as the COTP).

To find the COI margin, generation in the Northwest area is scaled up while increasing loads in the California region. The minimum step size is 25 MW. For static voltage stability, VSTAB is employed. To find the margin for dynamic voltage stability and DSA, ETMSP version 5.0 is used. Software has been written to automate the process of evaluating the output of these simulation runs.

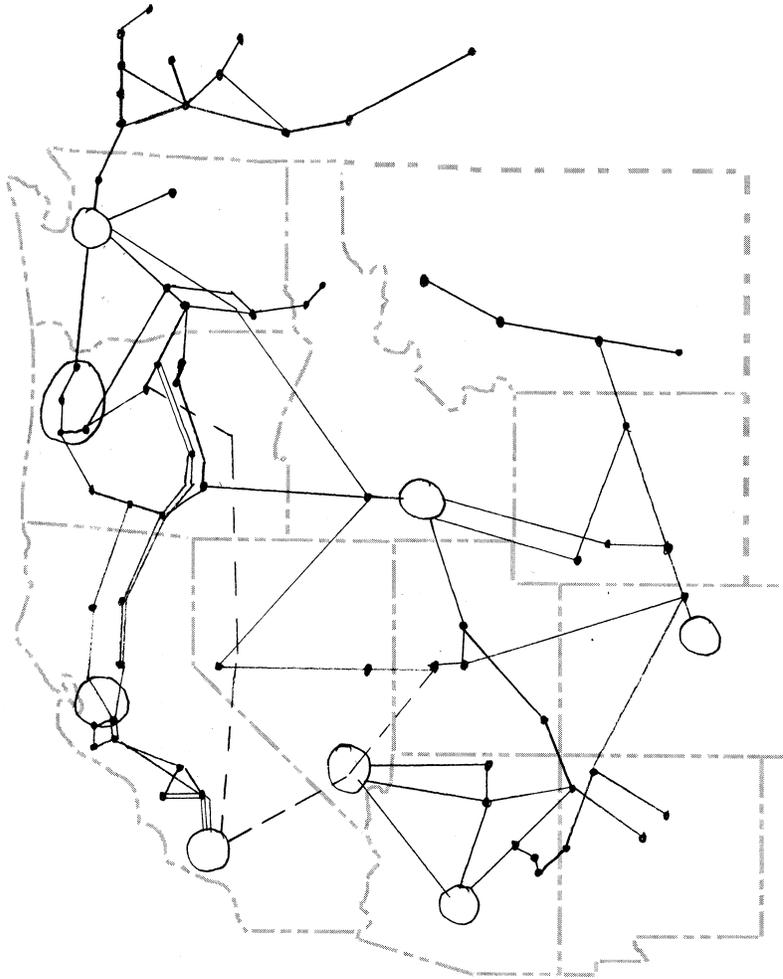


Fig. 11 Existing WSCC major transmission lines and load centers

For the static margin, every 500kV line outage is studied. While for the dynamic margin, a three-phase fault on each 500kV line is studied. The fault duration is 0.15 second (9 cycles), which is longer than the normal clearing time. However, this duration facilitates our analysis. The system is simulated for 50 seconds following the fault. After the fault is cleared, the dynamic voltage reliability criteria for the 500kV buses are checked for any violation. If there is a violation, the system is considered dynamic unstable. The base case COI flow is 3400MW. A three-phase fault on each 500 KV line is considered. Eighty-four contingencies were selected for the studies. The 168 total features (i.e., the active and reactive power flow of all the lines) were reduced to 55 features using principal components analysis. Then, statistical correlation coefficients were used to reduce the dimension of the pattern vector to 17 elements.

Due to inconsistencies in the available data, different system models were used to evaluate static and dynamic security. The specific base case and study system used were:

Dynamics: 1998 Spring 6500 bus system

Base case COI flow: Actual 4600MW (COI flow is reduced to 3700MW in the voltage simulation studies and 3400 MW in transient stability studies for convenience of study and comparison)

Static voltage stability margin: 1995 Spring 4000 bus system

Base case COI flow: 3700MW

5.2.2 Analysis

We begin by considering the voltage criteria. Table 6 shows the statistics of the errors encountered using simple linear regression on first and second order terms of the reduced variable set. In this case, both the average error and the maximum error are not acceptable, with a large number of instances that would result in misclassification. Fig. 12 plots the absolute and percentage errors for this estimator and shows how several large errors occur for the low margin cases. The overall performance of the ANN approach for the voltage criteria is shown in Table 7, again using two training methods; however, a voting scheme for three networks of different dimensions is used to improve accuracy. These results are plotted in Figs. 13 and 14. The errors in the estimates are extremely low and, therefore, should not lead to any misclassifications of security. Either of the two training approaches would be adequate, but Bayesian Regularization gives slightly superior results. This clearly establishes the effectiveness of this type of estimation.

Summary statistics are shown in Table 8. Figs. 15 and 16 show the relationship between margin and estimate error. The ANNs using Bayesian Regularization and Levenberg-Marquardt algorithm have similar performance with the Bayesian approach again showing slightly better performance. While most of the estimates are accurate, the low margin cases have larger errors. This is particularly troublesome because those are the cases where higher accuracy is most needed.

There are a number of issues arising from these results.

- 1) Data generation: In this study, there is a problem with generating a sufficiently large population of dynamically insecure states for the WSCC system. The fault-on period has been extended to find such cases. Still, only 84 insecure cases were found and these were poorly distributed. In the pattern matching approaches used in this project, data quality is the most important factor affecting performance.
- 2) ANN design: Another important issue is the choice of parameters as the input to the ANN. Our approach is to employ a voting scheme of networks with different

network parameters. At this point, the limited data prevents this from providing significant improvement in performance.

Our on-going studies are focused on improving the routines for generation of the training set. The first step will be to consider heuristics and generic search algorithms to help find interesting cases. The current approach is essentially a random generation of a large numbers of studies that does not provide a systematic approach to finding insecure operating points. This approach may include biasing techniques to emphasize unusual cases that provide more information on system limits. Pattern matching approach works well in interpolation but cannot extrapolate to the find limits. It is important to guide the data generation to capture the breadth of the operating range.

Table 6 Errors from linear regression of voltage security limits for the WSCC bus system

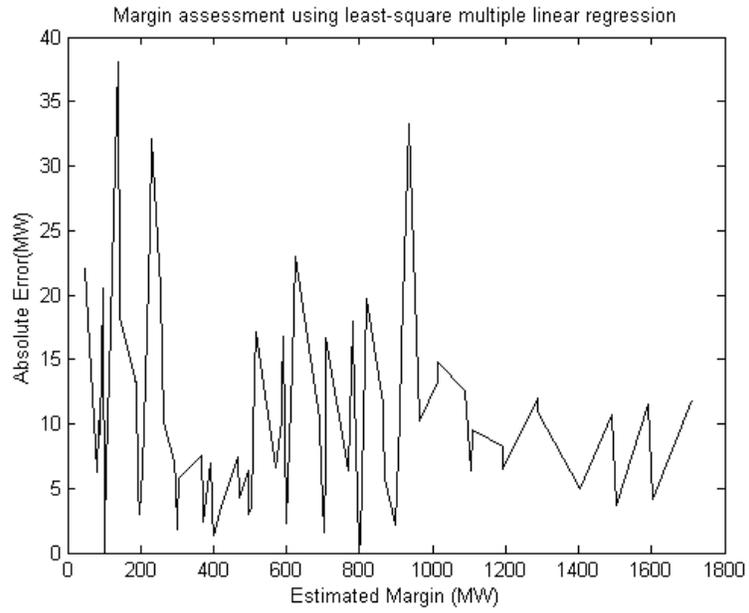
Max Error (MW/%)	Min Error (MW/%)	Mean Error (MW/%)	Standard Deviation (MW)	MSE (MW ²)
38.1/88.4%	0.11/0.027%	9.60/3.33%	11.60	138.70

Table 7 Errors from ANN estimate of voltage security limits for the WSCC bus system

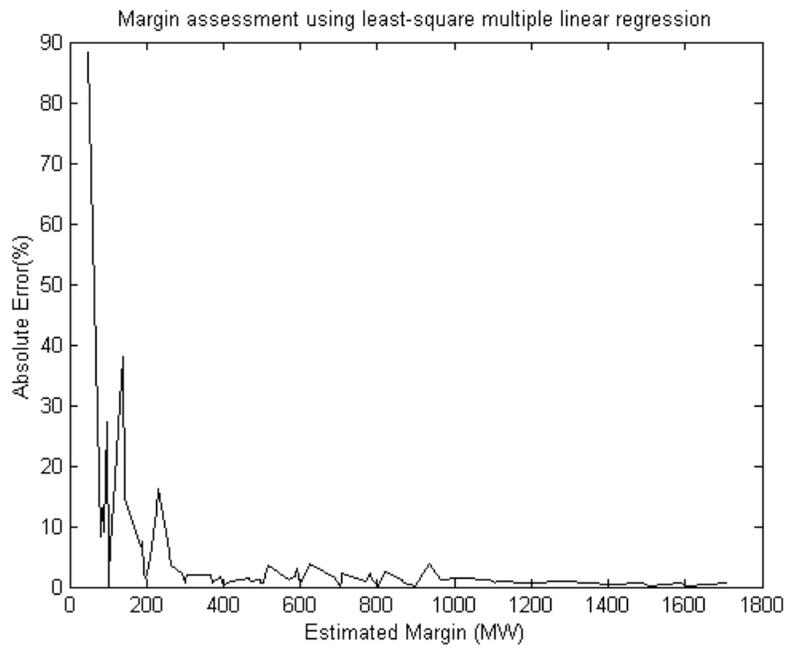
Max Error (MW/%)	Min Error (MW/%)	Mean Error (MW/%)	Standard Deviation (MW)	MSE (MW ²)
Levenberg-Marquardt				
31.72/6.86	0.046/0.0046	4.58/0.92	7.94	64.14
Bayesian Regularization				
12.64/3.48	0.024/0.0027	1.84/0.39	3.30	10.80

Table 8 Comparison of training routines on dynamic security estimator for the WSCC bus system

Max Error (MW/%)	Min Error (MW/%)	Mean Error (MW/ %)	Standard Deviation (MW)	MSE (MW ²)	Hidden neurons
Levenberg-Marquardt					
73.61/53.34	0.014/0.0029	11.28/4.07%	16.68	278.76	30
Bayesian Regularization					
95.77/85.50	0.005/0.0006	8.78/4.34	18.30	333.45	24

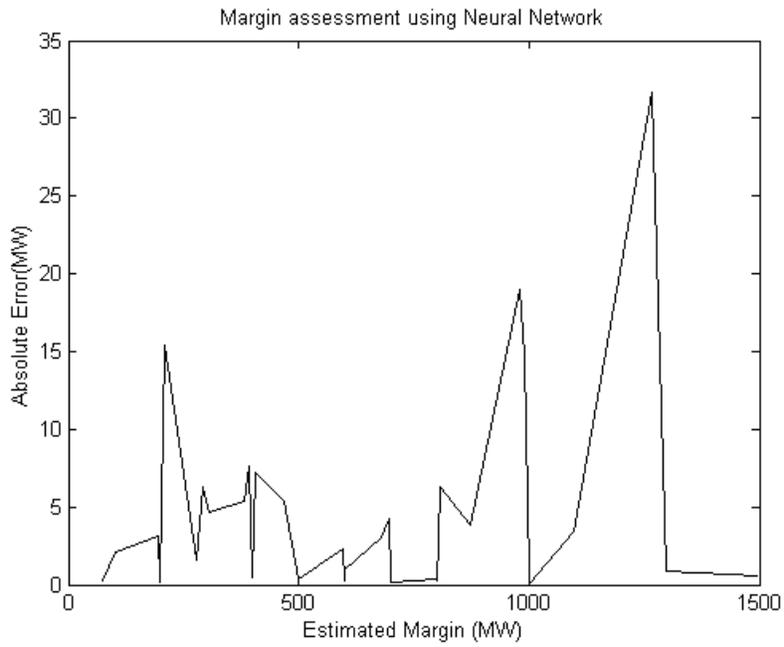


(a) MW error

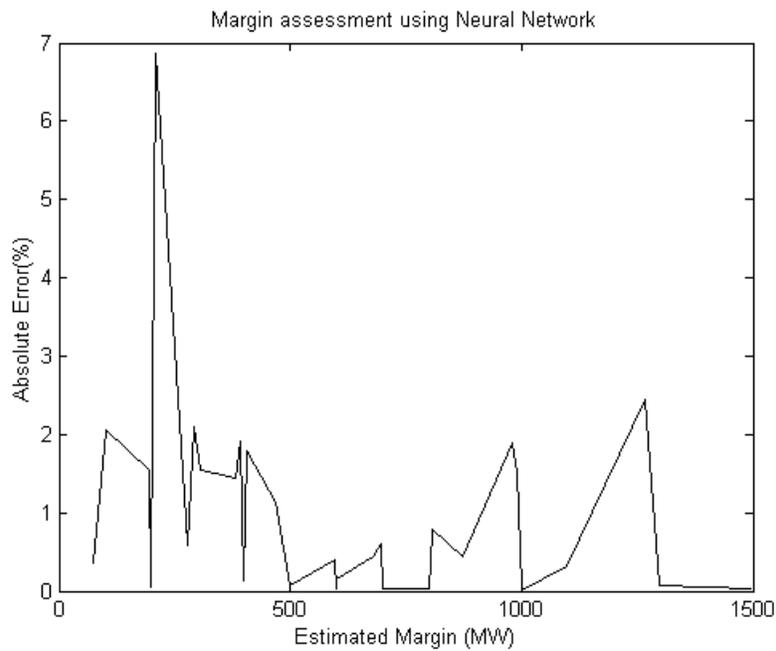


(b) % error

Fig. 12 Voltage security margin estimates using linear regression for the WSCC system

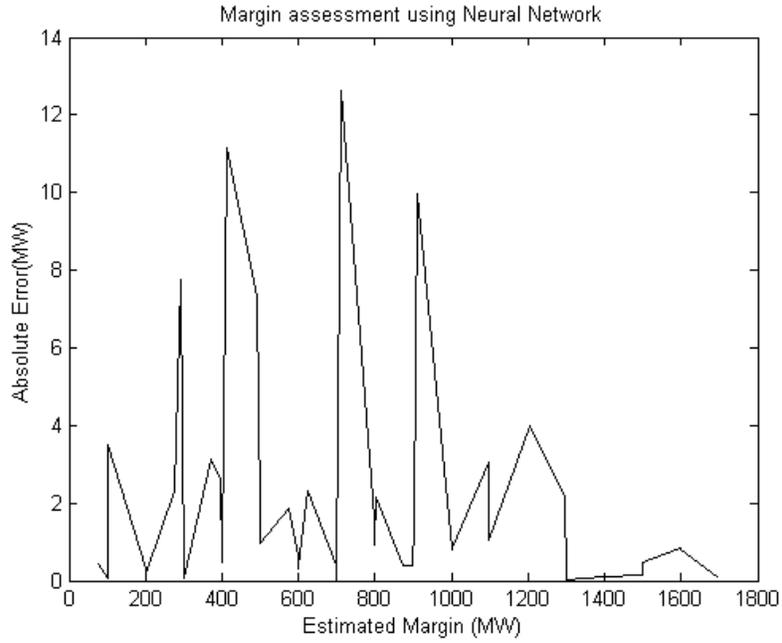


(a) MW error

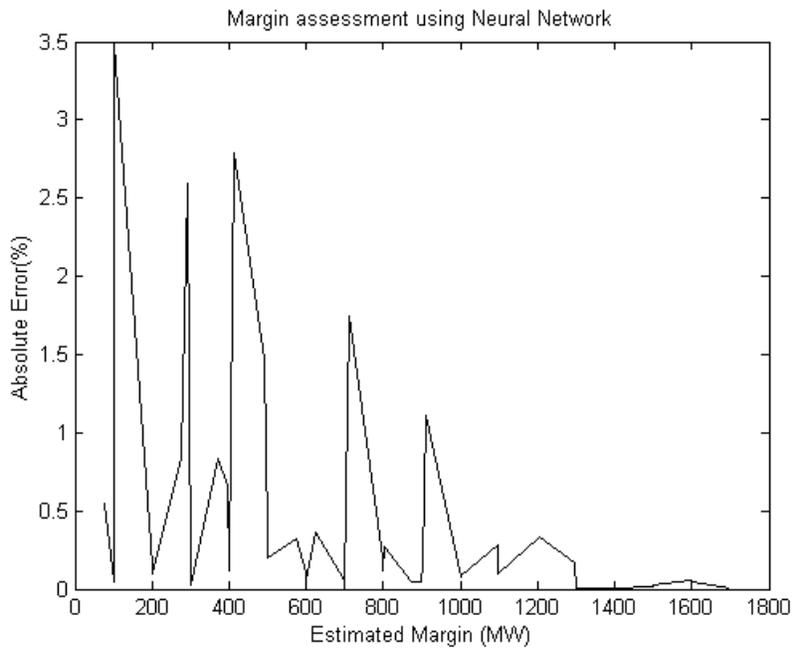


(b) % error

Fig. 13 Voltage security margin estimates using ANN with Levenberg-Marquardt training for the WSCC system

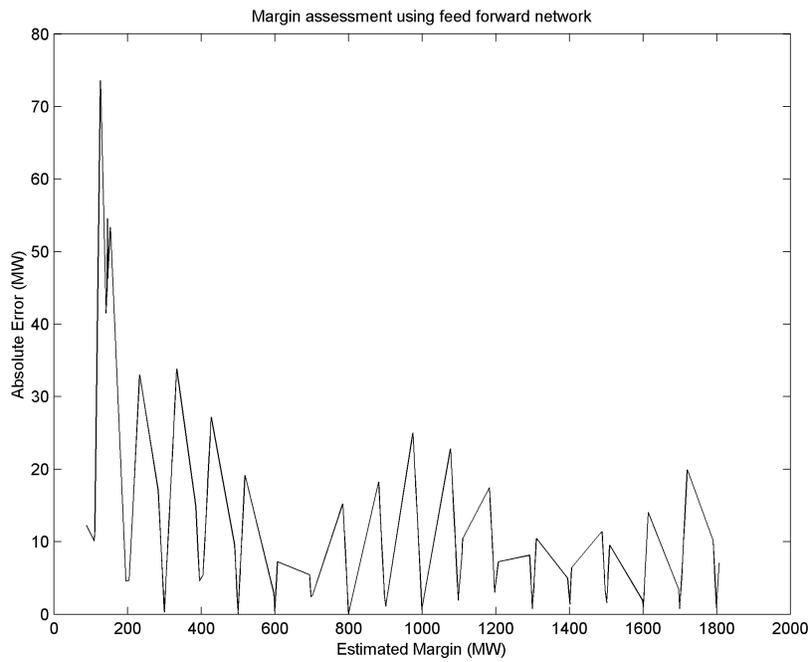


(a) MW error

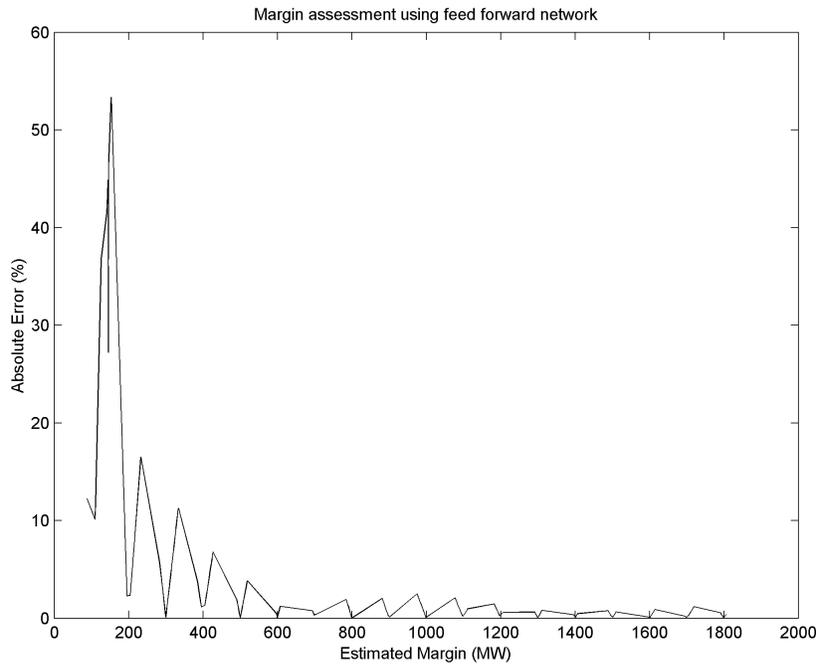


(b) % error

Fig. 14 Voltage security margin estimates using ANN with Bayesian Regularization training for the WSCC system

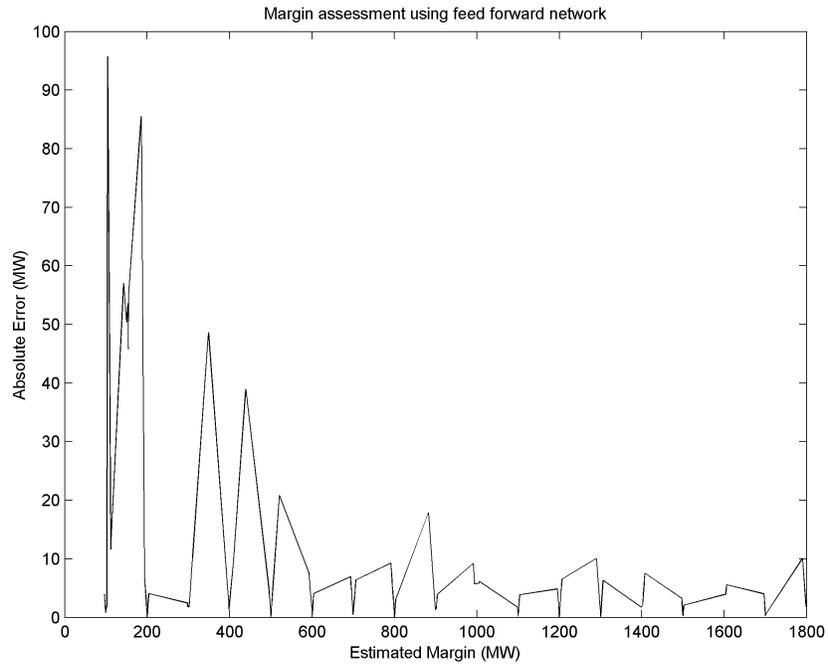


(a) MW error

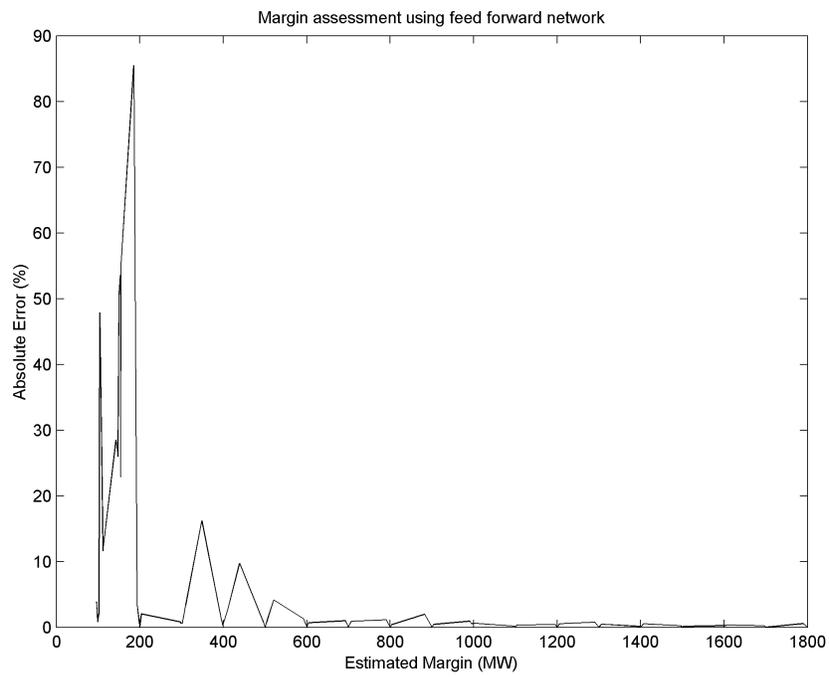


(b) % error

Fig. 15 Dynamic security margin estimates using ANN with Levenberg-Marquardt training for the WSCC system



(a) MW error



(b) % error

Fig. 16 Dynamic security margin estimates using Bayesian Regularization training for the WSCC system

6 Conclusions and Future Studies

This study developed and analyzed an integrated framework employing ANNs to estimate on-line security. The primary advantage of the approach is in:

- making full use of the numerous detailed off-line studies performed during operations planning,
- providing a simple intuitive assessment of security for operators, and
- allowing for any security index that may be of use for a particular system, including system specific indices.

Prediction and generalization capabilities of these ANNs provide a flexible mapping of input attributes to the single-valued space of the security margin. Because ANNs have high computation rates, they are an excellent tool for on-line application. This conclusion holds particularly when either data requirements and/or the computational burden have rendered other approaches impractical for implementation.

The results obtained from the 39 bus system show that our integrated approach was able to predict the security margin with a high degree of accuracy for the complete security assessment problem. In our previous work, we showed that this methodology works for the static security assessment of large practical systems. This project subsequently demonstrates the feasibility of obtaining similar estimates for dynamic security assessment. While the 39 bus results appeared promising, the difficulty in implementing these approaches is in large system applications. While some additional analysis is needed, the full complex models used for the WSCC system establish that the approach is practical.

Perhaps the main concern with our approach is the added burden it places on operational planning. These off-line simulation studies are extremely time-consuming. This has been addressed somewhat in our approach by automating the process of applying reliability criteria to the simulation results. Experienced operational planners are far more efficient in their use of simulation tools because of their choice of studies; however, that approach can mislead operators dealing with unusual loading conditions. Finally, the method we propose can only be as good or complete as the off-line analyses. If models are incorrect, or if highly unusual load patterns arise, the estimates will be suspect. Finally, as was seen for transient stability of the WSCC, if the number of informative cases (i.e., unstable cases) are small and poorly distributed, then poor estimates will occur.

6.1 Significant Contributions

This project produced a number of contributions to the development dynamic security analysis techniques.

- A comprehensive framework was developed for on-line estimation of security margins, calculated based on current operating practices.
- The framework proposed families of estimators, each specialized for specific system limits and the appropriate security criteria (i.e., static, dynamic or voltage). The estimators can be combined to provide an overall assessment of system operating conditions.
- A system of estimators was implemented and tested on a modified New England 39 bus system.
- Based on the insights from the New England system, a more sophisticated set of estimators was implemented and tested on an 6500 bus model of the Western Area system. The focus of this study was the California-Oregon Intertie transfer limits.
- A number of software tools were developed to help automate the process of evaluating security margins in off-line studies.

The results show that very accurate on-line estimation of security margins is possible for large systems. The main limitation of the implemented approach resides in the ability of time-consuming off-line studies to accurately model system dynamics.

6.2 Recommended Further Developments

A number of efforts are needed to develop this integrated security analysis approach into a workable and efficient dynamic security assessment tool for large systems.

1. Improved generation of study data: Currently, the studies are essentially exhaustive. While some planning and operator experience is implicitly included due to the chosen reliability criteria, greater inclusion of such experience could reduce the needed computation time. For example, many security problems only arise under specific operating conditions. Such insight could be used to reduce the number of study cases. The analysis of the system response has been automated to a certain extent, but there are peculiarities that require case-by-case analysis. These can be quite time-consuming to address individually.
2. Use of alternative indices: This study employed the most detailed models available and used time domain analysis. The motivation was to avoid controversy that may be associated with the value of approximating some less than precise index. There are certainly many useful techniques, most notably energy function methods and transient

stability indices, that could be considered. The value of our proposed approach lies in improved computationally efficiency for on-line application.

3. Improved estimators: While the performance of the developed estimator appears more than adequate for most applications, a number of improvements could be made, including:
 - a. Dynamically updating the estimators based on the current operating conditions or new studies
 - b. Exploring select sets of features that work across different operating situations, thus simplifying estimator design
 - c. Grouping of data to identify similar operating conditions to possibly reduce the number of required estimators.
4. Suggested corrective action: The estimators could be used to identify generation adjustments or other corrective actions to increase security margins. In fact, they could be easily employed to form a security constrained Optimal Power Flow.
5. Improved operator interface: In this project, we did not investigate closely operator issues associated with the use of the selected estimators. For example, because the estimates are computed essentially instantaneously, an operator could easily use the estimators to quickly verify that a remedial action does not lead to other security violations.

7 References

- [1] *Automated Operating Procedures for Transfer Limits*, Final Report, PSerc Publication 01-05, May 2001.
- [2] A.A. El-Keib and X. Ma, "Application of Artificial Neural Networks in Voltage Stability Assessment," *IEEE Transactions on Power System*, Vol. 10, No.4, Nov. 1995, pp. 1890-1896.
- [3] S. Chauhan and M.P. Dava, "Kohonen Neural Network Classifier for Voltage Collapse Margin Estimation," *Electric Machines and Power Systems*, Vol. 25, No. 6, July 1997, pp. 607-619.
- [4] L. Chen, K. Tomsovic, A. Bose and R. Stuart, "Estimating Reactive Margin for Determining Transfer Limits," accepted for *IEEE Transactions on Power Systems*.
- [5] S. Haykin, *Neural Networks, a Comprehensive Foundation*, 2nd Edition, Prentice Hall, 1999, New Jersey.
- [6] C. W. Taylor, *Power System Voltage Stability*, McGraw-Hill, 1994, New York.
- [7] Western Systems Coordinating Council, *Reliability Criteria*, Aug. 2000.
- [8] IEEE Committee Report, "Dynamic Security Assessment Practices in North America," *IEEE Transactions on Power Systems*, Vol. 3, No. 3, August 1988, pp. 1310-1321.
- [9] H. W. Dommel and N. Sato, "Fast Transient Stability Solutions," *IEEE Transactions on Power Apparatus and Systems*, Vol. 91, July/August 1972, pp. 1643-1650.
- [10] M. Ribbens-Pavella and F. J. Evans, "Direct Methods for Studying Dynamics of Large-Scale Electric Power Systems – A survey," *Automatica*, Vol. 21, No. 1, 1985, pp. 1-21.
- [11] A. D. Patton, "Assessment of the Security of Operating Electric Power System using Probability Methods," *Proceedings of IEEE*, Vol. 62, No. 7, July 1974.
- [12] H. Hakim, "Application of Pattern Recognition in Transient Security Assessment," *Journals of Electrical Machines and Power Systems*, Vol. 20, 1992, pp. 1-15.
- [13] L. Wehenkel, *Automatic Learning Techniques in Power Systems*, Kluwer Academic Publishers, MA, 1998.
- [14] A. Tiranuchit and R. J. Thomas, "A Posturing Strategy Against Voltage Instabilities in Electric Power Systems", *IEEE Transactions on Power Systems*, Vol. 3, No. 1, February 1998, pp.87-93.
- [15] C. A. Canizares, F. L. Alvarado, C. L. DeMarco, I. Dobson and W. F. Long, "Point of Collapse Method Applied to AC/DC Power Systems", *IEEE Transactions on Power Systems*, Vol. 7, No. 2, May 1992, pp. 673-683.
- [16] T. Van Cutsem and C. Vournas, *Voltage Stability of Electric Power Systems*, Kluwer Academic Publishes, Boston, 1998.
- [17] W. Rosehart, C. Canizares and V. Quintana, "Optimal power flow incorporating voltage collapse constraints," *Proceedings of the 1999 IEEE PES Summer Meeting*, July 1999, Vol. 2, pp. 820-825.
- [18] Western Systems Coordinating Council, *Voltage Stability Criteria, Undervoltage Load Shedding Strategy, and Reactive Power Reserve Monitoring Methodology*, May 1998.

- [19] M. Moechtar, T. C. Cheng, and L. Hu, "Transient Stability of Power System – A Survey," *WESCON Conference Record Proceedings of 1995*, San Francisco, California, Nov. 7-9, 1995, pp. 166-171.
- [20] D. Sobajic, and Y. Pao, "Artificial Neural Net Based Dynamic Security Assessment for Electric Power Systems," *IEEE Transactions on Power Systems*, Vol. 4, No. 1, February 1989, pp. 220-228.
- [21] Y. Pao, and D. J. Sobajic, "Combined Use of Unsupervised and Supervised Learning for Dynamic Security Assessment," *IEEE Transactions on Power Systems*, Vol. 7, No. 2, February 1989, pp. 878-884.
- [22] M. A. El-Sharkawi, R. J. II Marks, M. E. Aggoune, D. C. Park, M. J. Damborg, and L. E. Atlas, "Dynamic Security Assessment of Power Systems Using Back Error Propagation Artificial Neuron Networks," *Proceedings of the 2nd Symposium on Expert System Applications to Power Systems*, Seattle, WA, July 1989.
- [23] R. Kumar, A. Ipahchi, V. Brandwajan, M. A. El-Sharkawi, and G. Cauley, "Neuron Networks for Dynamic Security Assessment of Large Scale Power Systems: Requirements Overview," *Proceedings of 1st International Forum on Applications of Neuron Networks to Power Systems*, Seattle, WA, July 1991, pp. 65-71.
- [24] Y. Mansour, A. Y. Chang, J. Tamby, E. Vaahedi, B. R. Corns, and M. A. El-Sharkawi, "Large Scale Dynamic Security Screening and Ranking Using Neuron Networks," *IEEE Transactions on Power Systems*, Vol. 12, No. 2, May 1997, pp. 954-960.
- [25] H. P. St. Clair, "Practical Concepts in Capability and Performance of Transmission Lines", *AIEE Transactions*, Vol. 72, 1953, pp. 1152-1157.
- [26] R. D. Dunlop, R. Gutman, and P. P. Marachenko, "Analytical Development of Loadability Characteristics for EHV and UHV Transmission Lines", *IEEE Transactions on Power Apparatus and Systems*, Vol, PAS-98, No. 2, March/April 1979, pp. 606-617.
- [27] T. W. Kay, P. W. Sauer, R. D. Shultz, and R. A. Smith, "EHV and UHV Line Loadability Dependence on VAR Supply Capability", *IEEE Transactions on Power Apparatus and Systems*, Vol. PAS-101, No. 9, September, 1982, pp. 3568-3575.
- [28] S. Grijalva and P. W. Sauer, "Reactive Power Considerations in Linear ATC Computation", *Decision Support Systems, The International Journal*, North-Holland, Elsevier, Vol. 30, 2001, pp. 327-340.
- [29] *Interactive Power Flow User's Manual*, EPRI TR-103643-V2, prepared by Ontario Hydro, October 1994.
- [30] *VSTAB Version 4.0 User's Manual*, prepared by Ontario Hydro.
- [31] *ETMSP Version 5.0 User's Manual*, prepared by Ontario Hydro.
- [32] D.J.C. MacKay, "Bayesian Interpolation," *Neural Computation*, Vol. 4, No. 3, 1992, pp. 415-447.
- [33] S. Amari, N. Murata, K.-R. Muller, M. Finke, and H. Yang, "Statistical Theory of Overtraining - Is Cross-validation Asymptotically Effective?" *Advances in Neural Information Processing Systems*, Vol. 8, Cambridge, MA: MIT Press, 1996, pp. 176-182.

8 Description of Study Data and Developed Software

This section summarizes the software developed and example data generated for this study.

System study data:

Modeling: ETMSP dynamic models data, disturbance descriptions, output descriptions (for modified 39 bus and WSCC 4000 and 6500 bus models).

Results: Power flow solutions for all study cases, calculated security margins for all indices and study cases (for modified 39 bus and WSCC 4000 and 6500 bus models). These results are stored in Matlab data files.

Margin calculation:

Contingency List: Several files and routines are needed for generating the complete list of contingencies for the system under study and varying the system load and generation pattern.

Output analysis: The ETMSP output is read into Matlab where it is analyzed for conformance with WSCC criteria. Each case is represented by a set of representative features, including real and reactive power flows on all major transmission lines. These results are stored in a database.

Estimator design:

Data analysis: Routines for computation of correlation coefficients and principal component analysis.

Estimator: Routines for training a neural net using Levenberg-Marquardt and Bayesian Regularization backpropagation and the resulting estimators for the system studies.

9 Project Publications and Presentations

Publications:

L. Chen, K. Tomsovic, A. Bose and R. Stuart, "Estimating Power Transfer Margins for Voltage Security," accepted subject to revision for *IEEE Transactions on Systems*.

A. Sittithumwat and K. Tomsovic, "Dynamic Security Margin Estimation using Artificial Neural Networks," *Proceedings of the 2002 IEEE PES Summer Meeting*, July 2002, Chicago.

K. Tomsovic, A. Sittithumwat and J. Tong, "On-line Estimation of Power System Security Limits," *Proceedings of the Bulk Power System Dynamics and Control V*, August 26-31, 2001, Onomichi, Japan.

Presentations:

Dynamic Security Margin Estimation using Artificial Neural Networks, *Bulk Power System Dynamics and Control V*, August 26-31, 2001, Onomichi, Japan.

Use of Planning Studies to Estimate Security Margins in Real-Time *PSerc Seminar*, Sept. 11, 2001. On-line: <http://www.pserc.wisc.edu/ecow/get/generalinf/presentati/psercsemin1>