Project Title: Security Assessment of Power Systems

Project No: 8-21-654

Principal Investigator: Dr. A. S. Deba

Sponsor: U. S. Dept. of the Interior

Agreement Period: From 1/23/75 Until 7/22/75

Type Agreement: P. O. Mo. A1590 (Fixed Price)

Amount: 9,713

Reports Required: Interim Progress; Final Report

Sponsor Contact Person(s):
Mr. Richard Mariscal
Chief, Branch of Supply
U. S. Department of the Interior
Office of the Secretary
18th & E Streets, N.W.
Washington, D.C. 20240

Assigned to: Electrical Engineering

COPIES TO:
Principal Investigator
Library
School Director
Rich Electronic Computer Center
Dean of the College
Photographic Laboratory
Director, Research Administration
Director, Financial Affairs (2)
Director, Security-Reports-Property Office
Patent Coordinator
Project File
Other

RA-3 (6-71)
RESEARCH PROJECT TERMINATION

Date: October 22, 1975

Project Title: Security Assessment of Power Systems

Project No: E-21-654

Principal Investigator: Dr. A. S. Deba

Sponsor: U. S. Dept. of the Interior

Effective Termination Date: 8/22/75

Clearance of Accounting Charges: all charges have cleared

Grant/Contract Closeout Actions Remaining: NONE

Assigned to: ELECTRICAL ENGINEERING

COPIES TO:
- Principal Investigator
- School Director
- Dean of the College
- Director of Research Administration
- Associate Controller (2)
- Security-Reports-Property Office
- Patent and Inventions Coordinator
- Library, Technical Reports Section
- Rich Electronic Computer Center
- Photographic Laboratory
- Terminated Project File No. E-21-654
- Other

RA-4 (5/70)
INTERIM PROGRESS REPORT
for project entitled
SECURITY ASSESSMENT OF POWER SYSTEM
by
A. S. Debs

The following developments took place in our effort to write a state-of-the-art report on security assessment.

1. Literature review and evaluation of papers in the following areas:
   (a) steady state contingency evaluation
   (b) Pattern recognition methods
   (c) Transient security assessment
   (d) Probabilistic security assessment

2. A questionnaire was mailed to 50 U.S. utilities on their efforts and projected plans in the area of security analysis and associated data base systems. Copy of the questionnaire is enclosed.
Part I: Methodology and Facilities

Company Name: 

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>On-line continuous or frequent steady-state contingency analysis using power flow program.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>On-line continuous or frequent steady-state contingency analysis using distribution factors.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>On-line contingency analysis program for occasional use, using power flow program.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>On-line contingency analysis program for occasional use, using distribution factors.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td>Off-line power flow programs used for post-analysis of disturbances.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>On-line continuous or frequent analysis of contingencies involving transients.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>On-line interactive transient analysis program for dispatchers or operators.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Off-line transient analysis programs used for post-analysis of disturbances.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>Off-line transient analysis programs used in system planning.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Logging on automatic printout device.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Display on CRT output monitor.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>Reduction of results to form security indices.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

QUESTIONS

1. What is the primary cause of concern in operating your system? (List in order of priority)
   a) Transient Stability
   b) Over-loaded Transmission Lines
   c) Long-Term Dynamic Stability
   d) Other (specify)

2. Comments
SECURITY ASSESSMENT QUESTIONNAIRE

Part II: Data Base

1. Do you plan to use state estimation to provide the data base of security assessment?

   YES  NO

2. If "YES"

   a) What is the redundancy ratio = \frac{\text{#measurements}}{\text{#states}}?

   b) What type of algorithm will be used?

      AEP Lines Only
      BPA's Sequential State Estimator
      Weighted Least Squares using Sparsity Techniques
      Other (Specify)

   c) Will you use bad data rejection programs?

      YES  NO

   d) How often is the estimator run?

3. If "NO"

   a) Will your real-time measurements be sufficient to solve a load flow on-line?

      YES  NO

   b) Is excessively noisy data rejected?

      YES  NO

      How?

4. What type of information do you exchange with your neighboring utilities in real-time?

   YES  NO

   a) Tie Line Power Flows
   b) Status of High-Voltage Transmission Lines
   c) Status of Major Generating Units
   d) Spinning Reserve Margins
   e) Others (Specify)
ABSTRACT

A review of the state of the art in assessing the security of power system operations is provided. Emphasis is placed on the overall philosophy of preventive system operation, and the computational and data acquisition systems required for on-line monitoring and analysis of system security. Critical comparison of various approaches is provided. Recommendations for effective security assessment for a single company, as well as an interconnection are provided. Furthermore, industry practices and guidelines in the area of system security are presented and commented upon.

1. INTRODUCTION

1.1 Definition of System Security

A secure operating state of a power system is defined as that state which is invulnerable to unacceptable system conditions such as:

- cascading outages;
- system separation;
- wide-spread outages (blackouts);
- violation of emergency limits of line current;
- bus voltages, or system frequency; and
- loss of synchronization among generators.

Simply stated, the process of security assessment consists of judging if the system is in a secure operating state. No power system, however, is secure in the above sense. Catastrophic disturbances, simultaneous critical faults, or other improbable but possible occurrences can bring any utility system into any or all of these unacceptable system conditions. Economics and the reality of physical construction dictate that some attainable measure of security be supplied. This measure is usually in terms of the invulnerability of the system to single faults, single occurrences of loss of generation, or other credible contingencies.

It should be noted immediately that it is the security of the bulk power transmission that is being considered. Customer service interruptions at the distribution level are not included although they may occur if the bulk power transmission system fails.

1.2 Historical Background

Historically, the system planner always has considered the security of the system by providing comfortable margins of generating capacities, transmission line capabilities and tie-line interconnections. The planner, however, could not predict all possible system configurations and system demands. A system which is well planned under adequate engineering assumptions for secure operation will not be so necessarily under unpredicted conditions. The 1965 Northeast blackout and similar events showed clearly that a well-planned system is indeed vulnerable to possible disturbances and that this vulnerability can be catastrophic. Not only the planner but now the system operator is very much concerned about security and its assessment.

The first analysis of the problem of security was by Stienmetz(1) who studied the effect of disturbances on systems' stability. In 1926, Evans and Wagner(2) proposed some stability-enhancing schemes like the use of a ground-current relay to decrease prime mover input by governor control. And in 1930, Summers and McClure(3) proposed using a dynamic braking resistor for stability augmentation. Many works on related topics appeared since then. However, it was around 1968 when DiLiacco(6) formulated the new philosophy of secure operation. In essence, he decomposed system operation into three states: Normal; Emergency; and Restorative. In the Normal State all system equality and inequality constraints are satisfied. In the Emergency State some of the inequality constraints are violated (e.g., frequency drops, overloading of lines, etc.). Finally, in the Restorative State some of the equality constraints are not satisfied. (e.g., a load area is not serviced but the rest of the system is in the Normal State.) Refinements of these definitions were later obtained whereby the Normal State was decomposed into two states: Secure and Alert (or Insecure). A Secure Normal State is a Normal State whereby single system contingencies will not cause any transitions from the Normal State. In the Alert (or Insecure) Normal State a single system contingency can cause a transition to an Emergency State. A representative diagram of state transitions is shown in Figure 1.

![Figure 1. Schematic Diagram of System Operating States and Associated State Transitions Due to Disturbances and Control Action](image-url)
1.3 Applications of Security Assessment Methods

Analysis of system security is a primary function in three major applications: long-term planning; planning of operations; and minute-by-minute operation. Specific applications are listed as follows:

1. Long-Term Planning
- evaluation of generation capacity requirements
- evaluation of interconnected system power exchange capabilities
- evaluation of transmission system adequacy.

2. Planning of Operations
- determination of spinning reserve requirements in the unit commitment process
- scheduling of hourly generation as well as interchange scheduling among neighboring systems
- outage dispatching of transmission lines and transformers for maintenance and system operation.

3. On-Line Operation
- monitoring of the operating state of the system
- contingency evaluation
- prediction of the level or measure of system security in the near term
- providing inputs to security enhancement functions.

The primary concern of this report is on on-line operation since this is the area where most significant recent progress has taken place. The impact of this on long-term and operational planning, will however, be discussed.

1.4 General Problem Framework

Security assessment is part of an overall operating strategy to maintain the system in the Normal State as long as possible. Inputs to the security assessment process consist of:
- on-line telemetry data provided periodically every few seconds
- mathematical models of the system
- information on external interconnected systems
- system operating limits
- types and locations of possible disturbances
- security enhancement control strategies
- historical data
- uncertainties associated with measurements, mathematical models and predictions defined by means of probability distributions.

The outputs of the process provide a measure of system security. Definition of such a measure is, at present, controversial and dependent on certain philosophies to be elaborated upon later. These outputs, at any rate, are the basis of security enhancement strategies. (63)

A strong and mutual coupling exists between security assessment and security enhancement. Violation of a security limit requires preventive control action. However, the availability of an adequate corrective strategy means that the system is inherently more secure. All of this is done with strong regard of operator evaluation and action, and consequently, the design of effective on-line interactive systems.

The security assessment process itself consists of two primary functions:

1. Security Monitoring: this consists of the processing of incoming data, correlating it with available data in order to reliably determine the operating state of the system at present or in the near future.

2. Security Analysis: this consists of simulating the system under various contingency conditions in order to evaluate the measure of system security and provide inputs to enhancement strategies.

In either of the above functions updated mathematical models of the system are required. These models are classified as steady-state (static) and dynamic. And each class can be deterministic or stochastic. Furthermore, all modeling assumptions, whether in the static or dynamic cases, are of varying degrees of complexity depending on:
- computational requirements;
- on-line data requirements;
- data on model parameters;
- model reliability; and
- required solution accuracies.

System disturbances are classified into load and event disturbances. Load disturbances consist of small random fluctuations superimposed on slowly varying trend changes. Both the slow trends and the statistics of the small random disturbances can be predicted by forecasting methods (if the data is available). Event disturbances consist of:
- faults on transmission lines;
- cascading events due to protective relay action following severe overloads or violation of operating limits;
- generator outages due to loss of synchronism or malfunctions;
- sudden and large load changes.

Transmission line outages are generally due to weather (lightning or storms), improper relaying, operator errors or accidents (falling trees, airplanes, contact by construction equipment, etc.). Most such outages will affect single lines. However, multiple line outages may occur due to bus faults or accidents involving multiple line towers. Therefore they should not be disregarded entirely. Statistics on transmission line outages may or may not be available in a given utility. In general, however, higher voltage lines have smaller outage rates. Generator outage statistics are perhaps more understood with data available on most systems. In general, generator outages are more frequent with new units.

In Table I a summary is provided for the possible impact of various disturbance types on system security. It is clear from that table that maintaining the system in the Secure Normal State should be a highly desirable objective provided that the cost of so doing is not prohibitive.

1.5 Summary of Present Status

Present and projected efforts in the security assessment field consist, to our knowledge, in activities in the following areas:

The decomposition here is not unique since some utilities would use "Security Monitoring" to mean both of these primary functions. However, we are adopting these definitions to be consistent with Dyliacco. (63)
### TABLE I. Effect of Various Types of Disturbances on System Security

<table>
<thead>
<tr>
<th>Disturbance Type</th>
<th>Possible Outcomes</th>
<th>Impact on Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Faulted line which is cleared (3-phase and otherwise)</td>
<td>(a) Stable system with acceptable steady-state response</td>
<td>(a) Secure Normal State</td>
</tr>
<tr>
<td></td>
<td>(b) Loss of synchronism leading to generator tripping</td>
<td>(b) Generation-Load imbalance which may lead to an emergency if spinning reserves are not sufficient or to long-term dynamic instability.</td>
</tr>
<tr>
<td>2 Permanent line fault leading to line outage</td>
<td>(a) Stable system with acceptable steady-state response</td>
<td>(a) Secure Normal State</td>
</tr>
<tr>
<td></td>
<td>(b) Stable system with unacceptable steady-state response</td>
<td>(b) Steady-State emergency requiring corrective action. Otherwise cascading events will occur.</td>
</tr>
<tr>
<td></td>
<td>(c) Dynamic instability due to inadequate reserves</td>
<td>(c) Emergency State requiring emergency control</td>
</tr>
<tr>
<td>3 Generator Outage</td>
<td>(a) Stable system with acceptable steady-state response</td>
<td>(a) Secure Normal State</td>
</tr>
<tr>
<td></td>
<td>(b) Stable system with unacceptable steady-state response</td>
<td>(b) Same as 2(b)</td>
</tr>
<tr>
<td></td>
<td>(c) Dynamic instability due to inadequate reserves</td>
<td>(c) Emergency State requiring emergency control</td>
</tr>
</tbody>
</table>

a. Development of several computationally efficient steady-state contingency evaluation programs to test steady-state response to generator or line outages. Each program has its advantages and limitations and is strongly dependent on the type of data base used or proposed.

b. Development of feasible transient and long-term dynamic stability contingency evaluation algorithms which are based on different approaches. Some of these include:

- Use of Lyapunov's functions;
- Digital computer numerical integration;
- Hybrid computer on-line simulation.

c. Off-line computation of security functions by means of pattern recognition methods to be used in on-line operation.

d. Development of security indices based on contingency evaluation to aid the dispatcher to assess system security through interactive displays.

e. Development of probabilistic measures of security which are based on methods of reliability evaluation.

f. Development of optimum power flow programs with security constraints.

The remainder of this paper will discuss these topics from a critical point of view. Following that, a section is devoted to discussions and recommendations.

2. ANALYSIS OF PRESENT STATUS

2.1 Steady-State Security Assessment

In steady-state security assessment use is made of nonlinear power flow network models or, in some cases, linear steady-state current/voltage models. Analysis based on these models is natural since the Normal State is essentially in the steady-state and since most operating limits can be defined in terms of power flow, current and voltage quantities. Furthermore, these models are amenable to on-line computer analysis and are well understood by engineers.

In the discussion below emphasis will be placed on the following topics:

- Steady-state security monitoring;
- Steady-state contingency evaluation;
- Contingency evaluation modeling requirements.

2.1.1 Steady-State Security Monitoring

A. Data Base Systems

In steady-state security monitoring the objective is to determine, on a minute-by-minute basis, whether the system is in the Normal State or not. To do so, on-line data acquisition systems are required to various degrees of complexity. A minimal data acquisition system should provide information on the status of all major transmission and generation elements together with analog data on power flows, generation levels and inter-tie flows. The major transmission elements to be monitored should be determined in off-line studies during the planning phase. Such a minimal system should have the following capabilities:

- Drive operator displays to show major station single line diagrams, key flows on major lines, and generation levels; and
- Provide inputs for approximate contingency evaluation algorithms like the distribution factors algorithm.

An intermediate system will require an on-line ac power flow solution for the main grid network of a given utility. The trend at present is to do so by means of extensive data acquisition systems (Supervisory Control and Data Acquisition—SCADA), which provides status information on all lines, transformers and generators together with redundant measurements of power flows, voltages, loads and generation levels. The statistical techniques of Weighted Least Square estimation coupled with bad data rejection algorithms proved reliable, and hopefully accurate, on-line power flow solutions. The advantages of this over the minimal system are:

- All power flow outputs, measured or otherwise, are available to the display system.
- Furthermore, voltage and various quantities provide an added significant input.
- Contingency evaluation can be performed using ac methods provided adequate external network equivalents are available.
- Short-term bus load forecasting is possible. This provides a data base for predictive security analysis operational planning and possibly, on-line automatic control.
Figure 2. Major Functions Involving Control and Security of System Operation

- Improved economic dispatching through the availability of accurate load values and network configurations. Here an improved B-constant approach or an optimum power flow become possible.

A maximal system would consider the problem of interconnected system security. Here a coordination computer will act as a medium of data processing of vital data of interest to the interconnection as a whole. The individual pool members may have intermediate or minimal systems. The coordination computer will provide the following added advantages:

- Ability to perform contingency analysis on a company level or a pool-wide level with accurate knowledge of the status of the entire interconnection.
- Ability to evaluate emergency transfer capabilities on-line.
- Ability to perform pool economic dispatching.
- Improved emergency and security enhancement controls.

At present, most security monitoring systems are of the minimal or intermediate type (see Appendix B). However, some large interconnections perform, at least, the economic dispatching function on the pool level.

B. State Estimation

The role of state estimation is to provide a reliable and accurate estimate of bus voltage magnitudes and phase angles, real and reactive power flows, as well as, real and reactive bus power injections. This is achieved by overmeasuring the system with more measurements than are needed to solve a load flow problem. This redundancy enables a form of cross-checking among measurements to eliminate any gross measurement or system configuration errors. It also makes it possible to obtain power flow and injection estimates which are more accurate, on the average, than meter readings, provided that the network data is itself very accurate.

At present, there are a variety of state estimation programs with various characteristics. They are all based on the so-called static state estimation concept whereby a snapshot scan of the system provides all the information needed for computation. Furthermore, they all attempt to minimize the weighted least square errors between measured and estimated quantities.

In Table II, the following state estimation methods are compared:

1. Sequential State Estimation (SSE) (87)
2. American Electric Power Method (AEP) (83)
3. AEP'S Method modified to include bus voltages and line currents (Modified AEP) (90)
4. Decoupled Weighted Least Squares (Decoupled WLS) (89)
5. Weighted Least Squares (WLS) (77)
6. Generalized Load Flow (GLF) (88)

In addition to that table, the following comments are made:

(a) All these methods except SSE use sparse matrix techniques;
(b) They are very competitive with one another in terms of computational speed;
(c) An exact comparison among them is difficult to obtain since different methods use different measurement systems;
(d) These comparisons are based on our experience with simulated tests. Our experience with actual system data indicate serious network modeling problems which degrade the accuracy of solutions. (122)

Several approaches to the detection and identification of gross measurement or modeling errors have been reported. However, there is no report on actual operating experience. (115-119)

2.1.2 Steady-State Contingency Evaluation Methods

A. Introductory Remarks

Research on steady-state contingency evaluation methods has yielded a wide spectrum of computational approaches whereby rational comparisons can be made on the basis of (a) computational speed, (b) computational storage requirements, and (c) solution accuracies. Various modeling assumptions are made for each approach. In each case, however, the interest is in predicting line loadings, and possibly, voltage and various levels in the network under consideration, following single or multiple line outages or single generator outages.

This comparison is primarily subjective based on the writers' experience and published literature.
In either case, a pre-outage "state" should be available (e.g., base-case load flow solution). For line outages, assumptions pertaining to the load flow problem are retained. And for generator outages, assumptions related to the redistribution of lost generation among the remaining generators are used.

Line outages produce a significant change in the network parameters of the problem. Assuming that the pre-outage case is given by

\[ f(x, p) = 0 \]  

where \( x \) is the vector of state variables (complex bus voltages) and \( p \) is the vector of network parameters, then the post outage case is given by

\[ f(x + \Delta x, p + \Delta p) = 0 \]

where \( \Delta p \) represents the change in \( p \) due to the outage and \( \Delta x \) is the resulting change in \( x \). Here \( f(.,.) \) corresponds to the system's power flow equations. Invariably, all contingency evaluation algorithms follow either (or a combination) of the following approaches:

(a) **Sensitivity Analysis**

Here one writes,

\[ f(x + \Delta x, p + \Delta p) = f(x, p) + (\frac{\partial f}{\partial x})_{|x,p} \Delta x + (\frac{\partial f}{\partial p})_{|x,p} \Delta p \]

and by implication, one writes:

\[ \Delta x = -(\frac{\partial f}{\partial x})_{|x,p}^{-1} (\frac{\partial f}{\partial p})_{|x,p} \Delta p \]  

(b) **Improved Sensitivity Analysis**

In this case, it is assumed that the \( \Delta p \) is not small. Hence, one writes:

\[ f(x + \Delta x, p + \Delta p) = f(x, p + \Delta p) + (\frac{\partial f}{\partial x})_{|x,p} \Delta x + (\Delta p)_{|x,p} \Delta x \]  

This leads to the solution:

\[ \Delta x = (\frac{\partial f}{\partial x})_{|x,p}^{-1} (\frac{\partial f}{\partial p})_{|x,p} \Delta p \]  

In each of the above approaches, simplifications (or approximations) are made regarding the load flow equations, \( f(.,.) \), the Jacobian matrix, \( \frac{\partial f}{\partial x} \), or both. In the ac methods this permits the use of additional iterations to improve solution accuracy.

The major factor which makes this approach computationally efficient is the so-called Matrix Inversion Lemma, which in equation form is stated as follows:

\[ (A + CD^T)^{-1} = A^{-1} - A^{-1}C(I_m + D^T A^{-1} C)^{-1} D^T A^{-1} \]  

where:

- \( A \) is an \( m \times m \) non-singular matrix
- \( C, D \) are \( m \times m \) matrices (normally \( m = 1 \), or \( m \ll n \))
- \( I_m \) is an \( m \times m \) identity matrix.

Thus, the problem of inverting \( (A + CD^T)^{-1} \) simplifies to that of inverting an \( m \times m \) matrix provided \( A^{-1} \) is available. In most cases, however, the triangular factors of \( A \) are used within a scheme of sparse matrix computation.

The solution of a generator outage case is computationally simple. Here, the post-outage power flow equations can be written as:

\[ f(x + \Delta x, p) = \Delta S \]

where \( \Delta S \) represents the change in net power injections due to the outage. \( \Delta x \) is obtained by means of one or more iterations of the type

\[ \Delta x = -(\frac{\partial f}{\partial x})_{|x,p}^{-1} \Delta f \]  

The difficulty, however, is in the evaluation of \( \Delta S \) itself. The following schemes provide certain possibilities:

(a) Redistribute lost generation among remaining generators by means of "participation factors" and iterate if slack generation turns out to be too excessive;

(b) Redistribute generation according to the economic dispatch criterion;

(c) Allow slack bus to absorb lost generation, or

(d) Redistribute lost generation among the remaining AGC generators according to their participation factors. If more MW capacity is needed than is available by AGC, exit from program: "System Insecure."

Thus, the main difficulty here is in adequately representing steady-state response following a generator outage without excessive data requirements.

### B. Comparison of Line Outage Methods

In the bibliography, we have tried to refer to most known outage methods. For purposes of comparison, however, six representative methods were selected. These are:

1. Distribution Factors Method (DF)
2. Exact DC Outage Analysis (EDC)
3. Z-Matrix Method (ZM) (159)
4. Stott's Decoupled Load Flow (SDLF) (167)
5. Modified AEP Suboptimal ALP + KV + Line Currents 3 or 4 or 5
6. WLS Optimal Mixed 6
7. GLF Suboptimal Mixed 4 or 5

---

**Table II. Comparison of Six State Estimation Methods**

<table>
<thead>
<tr>
<th>METHOD</th>
<th>ACCURACY</th>
<th>MEASUREMENT SYSTEM</th>
<th>COMPUTATIONAL SPEED RANKING</th>
<th>CORE STORAGE RANKING</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. SSE</td>
<td>Suboptimal</td>
<td>Mixed</td>
<td>1 or 2</td>
<td>1</td>
</tr>
<tr>
<td>2. AEP</td>
<td>Suboptimal</td>
<td>Line Power Flow Only</td>
<td>1 or 2</td>
<td>2</td>
</tr>
<tr>
<td>3. Modified AEP</td>
<td>Suboptimal</td>
<td>AEP + KV + Line Currents</td>
<td>3 or 4</td>
<td>3</td>
</tr>
<tr>
<td>4. Decoupled WLS</td>
<td>Optimal</td>
<td>Mixed</td>
<td>3 or 4 or 5</td>
<td>5</td>
</tr>
<tr>
<td>5. WLS</td>
<td>Optimal</td>
<td>Mixed</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>6. GLF</td>
<td>Suboptimal</td>
<td>Mixed</td>
<td>4 or 5</td>
<td>4</td>
</tr>
<tr>
<td>#</td>
<td>METHOD</td>
<td>MODEL</td>
<td>REPRESENTATION OF LINE i-j OUTAGE</td>
<td>CHANGE IN FLOW ON LINE k-l, OR, CHANGE IN STATE VARIABLES</td>
</tr>
<tr>
<td>----</td>
<td>-----------------------------</td>
<td>------------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>1</td>
<td>Distribution Factors (DF)</td>
<td>DC Load Flow</td>
<td>$A \rightarrow A - \frac{1}{X_{ij}} e_{ij} e_{ij}^T$</td>
<td>$\Delta T_{k-l} = \frac{1}{X_{ij}} e_{ij} e_{ij}^T A^{-1} e_{ij} T_{ij}$</td>
</tr>
<tr>
<td>2</td>
<td>Exact DC Outage Analysis (EDC)</td>
<td>DC Load Flow</td>
<td>$A \rightarrow A - \frac{1}{X_{ij}} e_{ij} e_{ij}^T$</td>
<td>$\Delta T_{k-l} = \frac{1}{X_{ij}} D e_{ij} e_{ij}^T A^{-1} e_{ij} T_{ij}$</td>
</tr>
<tr>
<td>3</td>
<td>Z-Matrix Method (ZM)</td>
<td>ZI = E with no load impedances and E initialized at base-case solution</td>
<td>$Z^{-1} \rightarrow Z^{-1} - \frac{1}{V_{ij}} e_{ij} e_{ij}^T$</td>
<td>$\Delta(E_k - E_l) = \frac{y_1}{1 - y_1} e_{ij} Z_{ij}$</td>
</tr>
<tr>
<td>4</td>
<td>Stott's Decoupled Low Flow (SDLF)</td>
<td>$\Delta P / \Delta V = B' A_0$</td>
<td>$B' \rightarrow B' - B' e_{ij} e_{ij}^T$</td>
<td>$\Delta P = \frac{(B')^{-1} e_{ij} e_{ij}^T}{B' - e_{ij} e_{ij}^T} \Delta V$</td>
</tr>
<tr>
<td>5</td>
<td>Iterative Linear Load Flow (ILLF)</td>
<td>$A_0 = P' + P''$</td>
<td>$A \rightarrow A = A_{ij} e_{ij} e_{ij}^T$</td>
<td>$\Delta P = \frac{A^{-1} e_{ij} e_{ij}^T (P' + P'')}{A_{ij} - e_{ij} e_{ij}^T}$</td>
</tr>
<tr>
<td>6</td>
<td>Sachdev-Ibrahim Method</td>
<td>Full AC Power Flow</td>
<td>Compensate for outage by injecting real and reactive powers at bus j and i. Denote compensation by $\begin{bmatrix} \Delta P \ \Delta Q \end{bmatrix}$</td>
<td>$\begin{bmatrix} \Delta P \ \Delta Q \end{bmatrix} = \left( \frac{\partial f}{\partial x, p} \right)^{-1} \begin{bmatrix} \Delta F \ \Delta G \end{bmatrix}$</td>
</tr>
</tbody>
</table>

Definitions:

- $e_{ij}$: ith row, jth column
- $T_{ij}$: real flow on line i-j
- $Z$: nodal impedance matrix with no shunt terms and with shunt nodal voltages
- $E$: vector of nodal voltages at slack bus = 1+j1
5. Iterative Linear Load Flow (ILLF)\(^{(166)}\)
6. Sachdev-Ibrahim Method (SIM)\(^{(172)}\)

In Table III, a summary is provided regarding the numerical schemes involved. Methods 2-5 make use of the Matrix Inversion Lemma while Method 1 is strictly a sensitivity analysis method and Method 6 is a "compensation-type" method. Table IV provides a comparison of these methods from the computational, data requirements (type of security monitor), and output characteristics points of view. In comparing computational speed requirements two alternative regimes were assumed:

1. The inverses of matrices are stored as such. This is normally true for DF, EDC, and ZM methods.
2. Only triangular factors of matrices are stored. This is normally true for SDLF, ILLF, and SIM methods.

The argument for storing the inverses as such is that system operators can restrict the study system to those lines which tend to overload as well as those that cause the overload. The computational gain in speed is of the order of 100:1 over the regime of storing triangular factors only.

### 2.1.3 Contingency Evaluation Modeling Requirements

The minimal and intermediate forms of the security monitor provide information on the so-called internal system with little or no reference to the external system (part of which may belong to the utility under consideration). In order to perform contingency analysis, however, an equivalent representation of the external system is necessary.

The classical approach to static network equivalents consists of the following steps:

(a) Define as boundary buses those internal system buses which are connected to the external system.

(b) Eliminate all external system buses using the linear model of the nodal admittance matrix. This elimination creates an equivalent interconnection among the boundary buses which has the same form of a model admittance matrix.

(c) The original internal network plus the equivalent network form the basis for a power flow program. The boundary buses, here, retain their original classification as (P,V) or (P,Q) buses.

The main criticisms leveled against this classical approach are the following:

(a) The power flow problem is essentially nonlinear. Hence, a linear approach to equivalencing is, at best, an approximation. Experience has shown that very poor results are sometimes obtained.

(b) The external system may be very large (many thousands of buses) requiring considerable effort of data processing. Conceivably, a good portion of that system has no impact on the internal system.

(c) Boundary buses consist of a combination of the old boundary buses and all of the eliminated buses. There is no reason to believe that the old (P,V) or (P,Q) classification remains valid after the reduction.

(d) Certain utilities have large numbers of boundary buses. The equivalencing process will create large numbers of interconnections among these buses with each boundary bus connected to every other boundary bus. Computationally, the system matrices become highly non-sparse. This is detrimental to computational speed and storage requirements.

The advantages of this equivalencing approach are:

(a) Simplicity; and

(b) The retained system is always observable (by the security monitor). Hence, a base-case solution for contingency analysis will be available.

Researchers have tried to overcome some of the problems involved in the classical approach. Following is a discussion of some of the reported research:

(a) Approach of Ref. (184): In this approach the classical network reduction method is retained. However, prior to the reduction, a substantial portion of the external system is simply removed. The criterion here is that all flows to the removed system are positive. This maintains a net generation surplus in the retained part of the external system.
system. Portions of the external system are retained within the internal system representation in order to improve solution accuracy. The main drawbacks here are that the state estimator could be extended to a neighbor's utility. Furthermore, sparsity can still be sacrificed.

(b) Approach of Ref. (187): Studies on a particular system showed that boundary nodes are best represented as (P, V) nodes. This prompted the analysis of two alternatives. In the first, the equivalent system is solved with all boundary nodes classified as (P, V) nodes. And in the second, the external system is represented by the linear DC power flow model. In turn, this linear system, rather than the admittance matrix, is eliminated. The main difficulty here is that the (P, V) classification is system-dependent. Furthermore, sparsity still sacrificed if the boundary nodes are numerous.

(c) Approach of Ref. (186): The main concern here is the sparsity of the equivalent network. It is shown that by retaining a portion of the external nodes in the equivalent considerable savings in computer storage and execution times is possible. Obviously, this may require an extension of the domain of the state estimator.

Aside from the above discussion, a significant problem remains. In the minimal and intermediate security monitors very sketchy on-line information is available about the overall external network. A non-valid equivalent can provide very inaccurate information in contingency analysis. Some preliminary effort to overcome this difficulty has been reported in Ref. (188). Here the equivalent is identified as using on-line data from the internal system. However, there are no reported test results on these efforts. Efforts to achieve valid equivalents by means of adequate inter-utility data exchange, thus eliminating the need for identification, have not yet succeeded.

2.2 Transient and Dynamic Stability Security Assessment

2.2.1 Introduction

Transient stability assessment consists of determining if the system's oscillations following a short circuit fault will cause loss of synchronism among generators. The primary physical phenomenon involved here is that of inertial interaction among the generators as governed by the transmission network and bus loads. This phenomenon is of short duration (1-3 seconds) in general. For longer durations the dynamics of boilers, turbines and other power plant components cannot be ignored. Coupled with that is the control action of impedance and underfrequency load shedding relays. As a result, the effect of a fault-initiated disturbance may continue past the transient stability phase to the so-called long-term dynamic stability phase which can be of the order of 10-20 minutes or more. Serious blackouts that have occurred over the past 15-20 years were generally the result of long-term instability and sequences of cascading events. The events causing these blackouts are given in Ref. (238), and can be classified into the following:

(a) Faults on lines when other system components are out for maintenance;
(b) Loss of generation causing overloaded inerties;
(c) Operator initiated errors;
(d) Relay malfunction or inadequate relay settings.

Transient stability analysis is much easier to conduct than long-term dynamic stability analysis both in terms of modeling requirements and the duration of system response times. As will be shown below, this has serious implications in regard to data base requirements and on-line implementation. In the discussion below transient stability assessment is first considered with emphasis on numerical solution techniques and the problem of dynamic equivalents. Following that, approaches to long-term dynamic stability analysis are discussed.

2.2.2 Transient Security Assessment

A. System Modeling Requirements

Each generator is represented electrically as a constant voltage source behind transient reactance. Loads are represented as constant impedances or constant load currents which are determined from pre-fault load flow conditions. System dynamics are represented by the generator second-order torque equation assuming constant mechanical inputs. Mathematically one writes

\[ d^2 \delta_i \over dt^2 + \frac{d \delta_i}{dt} + D_i \delta_i = M_i \cdot P_M - P_E_i + P_{\delta i} \]

where

\[ i \] = ith generator index.

\[ M_i, D_i \] = generator inertia and damping constants, respectively

\[ P_M \] = constant mechanical input

\[ P_E_i, P_{\delta i} \] = electrical output

All electrical outputs and loads are represented by load-flow equations or linear voltage-current equations.

For this mode, pre-outage on-line data requirements consist of

(a) Voltage magnitudes and angles at all buses (state estimates)
(b) Status of all units
(c) Unit constants
(d) Network characteristics
(e) Fault type, duration and location.

Thus, an intermediate type security monitor will be adequate provided the external system is properly modeled by a dynamic equivalent.

Models of higher degree of complexity than the above are sometimes desired and used. This may include
- Excitation system model,
- Detailed generator electrical model,
- Governor control model, and
- Turbine models.

B. Stability Analysis

Two primary approaches are used in the literature to perform transient stability analysis: numerical integration and the use of Lyapunov's method. Practically, however, numerical integration is the only method used.
Several numerical integration approaches have been proposed and used. They generally fall under the categories of implicit or explicit methods. As in all integration schemes, the usual limiting factor is the smallest time constant of the system which is caused normally by synchronizing oscillations. The use of implicit predictor-corrector methods has generally allowed larger step-sizes while maintaining a high level of numerical stability. Normally, the transient stability program will alternate between an integration step and a load-flow solution to solve the network equations. Thus, sparse matrix methods can be quite effective and useful in this context.

Attempts to by-pass the limitations of synchronizing oscillations have been made in the Dynamic Energy Balance approach. Here, a modeling assumption is introduced - assuming coherency among tightly coupled generators. By implication, each coherent group is represented by a single inertial equation by neglecting all synchronizing oscillations within the group. This permits the use of longer integration step-sizes and the prediction of system conditions over periods of 20 seconds or so. The drawback of this approach is that coherent areas cannot be determined in advance always.

In order to improve on the computational speed requirements of direct integration, Lyapunov's stability methods for power systems were developed. This involves the derivation of a scalar Lyapunov function $V(x)$, where $x$ is the dynamic state vector of the system's set of differential equations, which has the following properties:

- $V(0) = 0$, i.e., $x = 0$ is the equilibrium state
- $V(x) > 0$, $x \in \mathbb{R}$, $x \neq 0$
- $\frac{dV(x)}{dt} \leq 0$, $x \in \mathbb{R}$

where $\mathbb{R}$ is a region around the stable point $x = 0$, which is called the region of stability. It can be shown that if, due to a fault, $x \in \mathbb{R}$ (but $x \neq 0$) then $x \to 0$ as $t \to \infty$. In Ref. (221-234) various forms of the Lyapunov function were derived. The main difficulty here is that determination of the boundary of the stability region is very difficult numerically. In a recent paper (234) it is claimed that such a difficulty can be overcome. However, this remains to be demonstrated on a large-scale system.

The advantages of Lyapunov's method, once the above obstacle is cleared, are:

(a) It can determine quickly if a system is stable directly from the post-fault condition.

(b) It can provide a measure of the margin of stability for given fault conditions.

The drawbacks of the method are:

(a) It cannot predict instability. Thus it may produce too many false alarms.

(b) The Lyapunov function depends strongly on the dynamic model chosen. Any increase in modeling complexity may invalidate the approach. For example, it has been reported that the inclusion of network line conductances is detrimental to the method. In fairness, however, many Lyapunov functions have been obtained in which machine saliency and governor action are represented.

### C. Dynamic Equivalents

As in the steady-state case, an equivalent representation of the external system is necessary. A good dynamic equivalent should have the following properties:

- provide accurate and reliable post-fault predictions within the internal system;
- be computationally efficient;
- require minimal on-line information from the external system.

Methods of generating dynamic equivalents are grouped into two classes: those based on coherency and those based on linear modal analysis. The coherency methods are based on the empirical/heuristic assumption that generators tend to swing together. A coherent group can be represented by one equivalent generator or a group of generators which maintain among themselves constant rotor angle differences. On the other hand, modal analysis is a mathematical approach based on linearizing system's differential equations, performing eigenvalue analysis and discarding the irrelevant modes (e.g., those which damp very quickly).

Coherency based methods differ from one another in a variety of details like

- methodology of selecting coherent groups,
- methods of connecting the equivalent machine to the original machine nodes, and
- methods of equivalencing exciter, turbine, and governor dynamics.

Reference (259) contains a comprehensive discussion of several dynamic equivalencing methods and proposes an automated approach for that purpose. The only drawback of this approach is that the equivalent is a function of fault location. However, it has the advantage of predicting instabilities in the external system among the equivalent generators. And this is not the case with the modal approach.

The main conclusion about dynamic equivalents is that there are distinct advantages in an automated equivalencing approach for on-line as well as off-line studies. However, some problems related to dependency of the equivalent on fault location remain to be solved. Furthermore, validation of the results using actual system measurements has not been attempted yet.

#### 2.2.3 Long Term Dynamic Response Assessment

The objectives of this type of assessment are:

- Evaluation of dynamic reserve response characteristics including distribution of reserves and effect of fast starting units;
- Evaluation of emergency control strategies like load shedding by underfrequency relays, fast valving, dynamic braking, and others.

These objectives fall primarily under system planning, control system design, as well as post-disturbance analysis. However, the operating implications cannot be neglected. As reported in Ref. (238), most of the major system disturbances in the past several years occurred under abnormal system conditions. On-line dynamic response analysis, if feasible, can indicate to the operator the catastrophic risks involved with given contingencies. These risks are difficult to evaluate effectively by means of steady-state or transient analysis.

Two approaches to this problem have been investigated so far: the digital (238) and hybrid (220) computer approaches.
Advantages of the digital approach are:

- Detailed representation of power plant models, relay systems and control strategies is straightforward;
- Flexibility in changing system parameters or switching from one system to another;
- Relatively low cost of running programs on a general purpose computer.

Its disadvantage is in the computational time requirements which make the digital approach an off-line tool. The advantage of the hybrid approach obviously is computational speed which can be 100 times faster than real time of simulated process. The disadvantages are:

- Inflexibility in changing network and system parameters for on-line contingency analysis. However, serious attempts have been made to overcome this difficulty.(220)
- Complex modeling of the system can add appreciable investment costs in system hardware which may not be justified economically since the system will have to be dedicated for that purpose. However, a simple facility for transient analysis may be attractive.

In conclusion, both approaches may prove to be of significant value. The digital approach will continue to be indispensable in off-line analysis. And, with cost reduction breakthroughs in hybrid systems, on-line applications may yet result. In either case, however, model calibration and validation is still a major problem requiring a fair amount of investigative work.

2.3 Pattern Recognition Security Assessment

The main objective of pattern recognition security assessment is to reduce on-line data and computational requirements to a minimum. This is done at the expense of elaborate off-line computations. The original suggestion for using pattern recognition came from Dylicco(10) who proposed a deterministic as well as a stochastic approach to the problem. Further research as later reported in Ref.'s (283-289).

The classical methodology of pattern recognition consists of defining a pattern vector \( x \) whose components consist of all the significant variables of the system. This vector is evaluated at many representative operating conditions to generate what is termed the training set. Since many components of the pattern vector will be strongly correlated with one another, a process of dimensionality reduction is performed to identify significant and, hopefully, uncorrelated set of variable \( z_1, \ldots, z_m \) which are functions of the components of \( x \). Hopefully the vector \( z = (z_1, \ldots, z_m)^T \) is much smaller in dimension than \( x \). This process is called feature extraction. The final step is to determine a function \( S(z) \) such that

\[
S(z) = \begin{cases} 
0 & \text{for a secure } z \\
< 0 & \text{for an insecure } z 
\end{cases}
\]

This is called a security function. Several methods are available for generating \( S(z) \) based on the form \( S(z) \) is assumed to take. If \( S(z) \) is assumed to be linear in the linear programming or least-squares methods can be used. Nonlinear functions, like quadratic functions, or multiple functions can be used. Here least squares or optimal search methods have been successfully used. The main objective of these methods however, is to minimize the number of misclassifications especially when an insecure pattern is misclassified as secure. In Ref. (289) a bias term is added which yields false alarms but very few misclassified insecure patterns. Furthermore, different security functions can be developed for steady-state and transient security.

From reviewing the literature on the subject one obtains a mixed opinion. Several reported tests have shown successful results with a record of misclassification of the order of 1-10% depending on the complexity of \( S(z) \) and size of the training set. Results of failure have also been reported whereby it is argued that the computational effort to generate an adequate \( S(z) \) for a large system is impractical. (289)

From our point of view pattern recognition offers the following advantages:

- It can drastically reduce the requirements of on-line security analysis. All what is required is the computation of \( S(z) \) based on direct on-line measurements or state estimator outputs. This is particularly true in the case of transient security assessment where on-line computation is time consuming.
- The requirement that \( S(z) \geq 0 \), can be used as the security constraint in an on-line optimum power flow or for preventive as well as corrective control measures.
- The process of training can pinpoint weaknesses in the system that may pass unnoticed otherwise.

Disadvantages of the method are:

- Off-line computation may be too excessive
- \( S(z) \) may vary widely to system configuration. Any scheduled or unscheduled outages may require the use of a different \( S(z) \). This can add a considerable computational burden.
- Pattern recognition can be construed as a form of extrapolation from the training set to the actual operating state. Since insecurity will arise as a result of abnormal operating conditions this extrapolation may give poor results.

2.4 Measures of Security

2.4.1 Objectives and Types of Security Measures

Contingency evaluation provides the main working tool to answer the various "what if" questions posed automatically or by the operator. A measure of security is intended to summarize the information resulting from many contingency checks in a simple form to be used by the operator as a help guide for preventive control action.

In general two types of security measures have been proposed: deterministic and probabilistic. In the deterministic case listing of contingencies that may cause emergencies is provided to the operator, together with information on the security of each case. The operator will then decide what to do either through experienced judgement or by interrogating programs for corrective action. In the probabilistic case two approaches have been proposed:

(a) Security indices approach;
(b) Reliability analysis approach.

Discussion of these follows.
2.4.2 Security Indices

Ref. (263) contains a comprehensive analysis of the idea of security indices. It differentiates between steady-state and transient indices.

In the steady-state case consideration is given to the following indices:
- line and transformer MVA flow index
- bus voltage index
- generator reactive reserve index.

For each index type an index function \( f(x) \) is defined on a component by component basis. This function assumes the value of 1.0 when the corresponding component is operated within safe limits. It assumes monotonically decreasing values from 1.0 to zero as the range of component operation varies from the safe to the unacceptable limit. Beyond the unacceptable limit this function is zero. The form of this function between the safe and unacceptable limits is cubic, quadratic and linear for line, bus voltage and reactive reserves indices respectively. For each steady-state contingency \( k \) the following index is computed

\[
\bar{I}_k = \frac{\sum w_{ik} f(x_{ik})}{\sum w_{ik}}
\]

where \( i \) ranges over all relevant components (e.g., lines and transformers, or bus voltages, etc.) and \( w_{ik} \) are weighting factor (e.g., line power flows for the line index). Finally for each index one computes

\[
\bar{I} = \frac{M \sum \sigma_k \bar{I}_k}{M \sum \sigma_k}
\]

where \( k \) ranges over all contingencies and \( \sigma_k \) is the probability of occurrence of that contingency.

Interpretation of the above approach based on judgement by its authors is summarized as follows:
- Choice of soft rather than hard constraints can account, at least heuristically, for the fact that violation of steady-state limits can be tolerated for a short time period which is normally of the order of a few minutes.
- The security index \( f \) although evaluated using certain probabilities, is not in itself the probability of system insecurity. It is only an index whose absolute value is dependent on system size.
- As a result of the above remark, the index becomes a starting point for more detailed analysis whereby the worst cases of limit violations are displayed to the operator.

In the case of transient security assessment reduction of the information in the form of an index is even more desirable than the steady-state case. The operator simply cannot cope with large numbers of swing curves. Again in Ref. (263) two types of transient security indices are proposed:
(a) Maximum angle separation index;
(b) Apparent impedance index.

The maximum angle index is given by

\[
\bar{\theta}_k = \max_{i,j} \max_{t} \theta_{ijk}(t)
\]

where \( \theta_{ijk}(t) \) is the angular separation between generation \( i \) and \( j \) at time \( t \) due to fault \( k \).

Obviously, if \( \theta_k \geq 180^\circ \) instability would occur. Normally \( \theta_k \) is limited to a certain maximum which depends on the system (\( \theta_{\text{max}} = 180^\circ - 200^\circ \)). A contingency swing factor \( \sigma_k \) is defined such that

\[
\begin{align*}
1 & \quad \text{if } \theta_k \to 0 \\
0 & \quad \text{if } \theta_k \to \theta_{\text{max}}
\end{align*}
\]

Subsequently, a composite transient stability index is defined considering all contingencies.

In the apparent impedance index, one evaluates

\[
Z_{ij}^* = \left( \frac{V_i}{I_{ij}^*} \right)^2 + \left( \frac{V_j}{I_{ij}^*} \right)^2
\]

which is the apparent impedance "seen" by relay at terminal \( i \) of line \( i-j \). A more appropriate quantity is

\[
Z_{ij}^* = \frac{Z_{ij}}{z_{ij}}
\]

Loss of synchronism will occur whenever \( Z_{ij}^* \) would cross the line segment [0,1]. Based on this, a contingency swing factor \( \sigma_k \) for the \( k \)th contingency can be defined:

\[
\begin{align*}
\sigma_k & \to 0 \quad \text{as } d_k \to 0 \\
\sigma_k & \to 1 \quad \text{as } d_k \to \infty
\end{align*}
\]

where \( d_k \) is the distance of \( Z_{ij}^* \) from the segment [0,1].

2.4.3 Reliability Analysis Approach

Application of reliability analysis methods to on-line security assessment was originally attempted in the evaluation of spinning reserve requirements as a function of the near-time future. System contingencies consisted of load forecasts and their uncertainties as well as generator outages described by outage probabilities. A risk function is defined as the probability of insufficient generating capacity and is illustrated in Fig. 3. In this figure it is assumed that at \( t = 0 \), the risk is zero. As \( t \) increases, the load increases causing smaller reserve margins and a non-zero probability of insufficient reserves. At \( t = t_R \), a reserve unit is added and obviously this decreases the risk instantaneously as shown. The decision to add the reserve unit at \( t_R \)
depends on exceeding the minimum risk level R. This level is decided upon by operational experience. Further elaborations upon this approach considers the inclusion of standby generators of different start-up response times. Start-up failures are included in a Markov-type model to represent more accurately the various risk probabilities. A key formula which is developed here is a security function defined by

$$S(t) = \sum_i P_i(t) Q_i(t)$$

where $P_i(t)$ is the probability that the system is in state $i$ at time $t$ and $Q_i(t)$ is the probability that state $i$ constitutes a breach of system security.

This idea of a security function is used in Ref. (341) in conjunction with on-line system security optimization. In that reference the following function is defined

$$S(g) = \sum_k \sum_{i,j} P[k, i, j] P[k, j]$$

The availability of the system is given by

$$a = 1 - S(g)$$

In the evaluation of $S(g)$ load uncertainty for the next instant is accounted for by means of normally distributed random vectors with appropriate means and standard deviations. An acceptable availability limit $a$ is established. And this becomes the basis for preventive or corrective action via security-constrained optimization.

2.5 Security-Constrained Optimization

Security constrained optimization consists of solving the problem of the allocation of generation subject to

(a) power flow constraints - equalities
(b) operating constraints - inequalities, and
(c) security constraints - inequalities.

While minimizing a performance criterion which is usually, but not necessarily, the cost of generation. Historically, an approximate form of the equality constraints has been (and is still being) used in conjunction with Economy Dispatch with a loss formula.

The availability of on-line state estimation now permits the use of load-flow equations directly as equality constraints. Furthermore, efficient security analysis programs permit the computation of security constraints either in the form of operating limit violations following a contingency or in the form of security functions.

Table V provides a summary comparison of a sample of security constrained optimization methods. A few remarks are in order regarding this table:

(a) Method No. (3) makes a distinction between a "global" and a "local" system security. In the global case all security constraints are satisfied. In the local case, allowance is provided for short-term (15 min) violations of line loading limits since the thermal limit is not reached instantaneously.

(b) Method No. (4) discusses the important topic of security constrained operational planning by incorporating the unit commitment problem into the formulation.

(c) Method No. (5) provides a novel approach based on reliability analysis and the "inconvenience level" associated with power outages.

(d) Method No. (6) emphasizes the point that when the system becomes vulnerable, the economic criterion may have to be ignored and replaced by a strictly security criterion.

In one respect security constrained optimization is an attempt to replace the operator as much as possible, by maintaining the system in the Secure Normal State as long as possible. It thus combines security assessment and enhancement. However, this is still costly from the computational viewpoint.

3. CRITICAL ASSESSMENT AND RECOMMENDATIONS

In our opinion, the main considerations in further progress in the security assessment process are:

(a) methodologies to reduce computational requirements;
(b) cost of insecurity, or the risk involved in insecure operation;
(c) accuracy and reliability of the analysis effort;
(d) role of the operator;
(e) interconnected system security assessment.

The remaining part of this section is devoted to brief discussions of these items.
3.1 Methodologies to Reduce Computational Requirements

As has been shown earlier, considerable effort has been, and continues to be spent on developing very efficient digital algorithms (and hybrid systems) to reduce the time required for contingency analysis. In spite of this, a complete security assessment process based on frequent steady-state and transient contingency analysis is either impossible or impractical with present systems. Various possibilities to overcome this are suggested:

(a) **Predictive security assessment**
   With the aid of bus load forecasting, one can perform the following function:
   \[ C_I = \sum_i P_i G_i \]
   where \( C_I \) is defined as the cost of insecurity, \( P_i \) is the probability of the ith outage, and \( G_i \) is the cost associated with the outcome of that outage. The cost associated with the outage of the outage will depend on any of the following factors:
   - Availability of post-outage corrective control measures--for thermal limit violations a minimum time of a few minutes is available for correction. For transient stability cases, measures such as dynamic breaking, fast valving and capacitor switching may also be available. In such cases the cost associated with limit violations may be quite small.
   - Possibility of cascading events. Here dynamic stability may be involved requiring, at least, a gross estimate of the resulting effects. Modeling of load-shedding logic may be of value in this case. At any rate, the cost associated with the limit violation will be very high.

(b) **Pre-screening computation**
   Fast and approximate algorithms can resolve the issue for many contingencies that are trivially secure. The more accurate algorithms will, consequently, be called upon less frequently. For example, the distribution factors method can be used to pre-screen contingencies for the more accurate ac methods. Similarly, steady-state analysis can pre-screen cases for transient analysis by considering steady-state stability limits. This will require an analysis of how much information can be derived from various types of analysis. And this can be the basis for a sequential pre-screening process.

(c) **Stochastic power flow analysis**
   Stochastic power flows can be put to good use in determining measures of uncertainty, and consequently, the probability of insecurity. This has been achieved in Ref. (339) in computing a probabilistic measure of security. The use of stochastic load flows is pertinent in conjunction with predictive analysis both for next hour or next day forecasting.

3.2 Cost of Insecurity

Reliability analysis can be put to good use in predicting the probability of system interruptions, given a computational methodology. This has been successfully applied in generation capacity planning whereby an acceptable risk of insufficient generation is assumed. This risk is based on accepted reliability standards and economic considerations.

The cost of an outage causing a blackout can be measured in terms of:
- lost energy serviced;
- inconvenience and possible danger to the public;
- embarrassment by utilities;
- security of the blackout; and
- frequency of occurrence.

If quantifiable, such factors can be introduced in computing the cost of insecurity. For example, one can express such cost as:
   \[ C_I = \sum_i P_i G_i \]
TABLE VI. Analysis of Errors Arising in the Security Assessment Effort

<table>
<thead>
<tr>
<th>Quantity and/or Item</th>
<th>Error Estimates</th>
<th>Improvement Method(s)</th>
<th>Status of Improvement Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>On-Line Measurement</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(a) Normal Errors</td>
<td>5-2% of Scale</td>
<td>Measurement Redundancy with State Estimation and Bad Data Rejection</td>
<td>Adequate</td>
</tr>
<tr>
<td>(b) Bad Data</td>
<td>Unknown</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Topology</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(a) Internal System</td>
<td>Small</td>
<td>Model Correction Logic</td>
<td>Experimental</td>
</tr>
<tr>
<td>(b) External System</td>
<td>Large</td>
<td>(a) On-Line Information Exchange (b) Model Correction by Internal System</td>
<td>Inadequate</td>
</tr>
<tr>
<td>Network Parameters</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(a) Internal System</td>
<td>5-10% of Value</td>
<td>(a) Parameter Estimation (b) Manual Adjustments</td>
<td>Adequate</td>
</tr>
<tr>
<td>(b) External System</td>
<td>5-10% of Value</td>
<td>Parameter Estimation</td>
<td>Experimental</td>
</tr>
<tr>
<td>Dynamic Models</td>
<td>Considerable</td>
<td>(a) Individual Component Modeling (b) Parameter Estimation</td>
<td>Adequate</td>
</tr>
<tr>
<td>Static Equivalents</td>
<td>Medium-Large</td>
<td>(a) Engineering Judgement (b) New Models (c) Parameter Estimation</td>
<td>(a) Adequate for Planning (b) Experimental and System Dependent (c) Experimental</td>
</tr>
<tr>
<td>Dynamic Equivalents</td>
<td>Large</td>
<td>(a) Heuristic-Automated (b) Parameter Estimation</td>
<td>Experimental</td>
</tr>
<tr>
<td>Bus-Load Forecasting (1-24 hours)</td>
<td>1-5%</td>
<td>Different Statistical Methods and Good Weather Forecasts</td>
<td>Experimental</td>
</tr>
</tbody>
</table>

The methodology of parameter estimation is a strong contender in providing statistically validated models for on-line use.

The methodology of stochastic load flow is significant in providing a quick summary of system statistical errors. This makes possible an effective use of bus load forecasting in predictive security analysis.

Engineering ingenuity is still indispensable in providing new approaches and in interpreting results.

3.4 Role of the Operator

The advantages of the operator over automated software systems are:

- He relies on a global perception of events in interpreting results;
- He can take into consideration peculiar situations not originally programmed;
- He can be trained to assess the impact of a given contingency;
- He can override the computer when the results are unreasonable.

Obviously his main disadvantage (or limitations) are:

- Slow reaction time;
- Judgement is dependent on training and intelligence of particular operators;

- Knowledge of software capabilities and limitations is operator-dependent.

Table VII provides a summary comparison of the overall relative roles of the operator vis-a-vis the software system. In essence, we see the operator as being in the position to interrogate and then judge the system. The interrogation and judgement can take the following forms:

(a) Simple--contingency checking and listing of limit violations for "critical" contingencies;
(b) Interpretive--assess dollar (or other) costs of a preventive control measure;
(c) Objective seeking--input performance indices for optimization programs and then interpret results;
(d) Assess credibility--override software recommendations.

3.5 Interconnected System Security Assessment

This is a topic of increased significance due to the fact that the causes of insecurity can originate outside the study system. Topics of particular interest here are:

(a) Availability and distribution of reserves (spinning and otherwise) in the interconnection;
(b) Power transfer capabilities on the inerties during the following emergencies;
In our opinion, an adequate data base for interconnected system security is required. It should be based on on-line information exchange. Guidelines for secure operation should be established especially when security and economy of operation are in conflict with one another.

TABLE VII. Comparison of Operator vs. Software Roles in Security Assessment

<table>
<thead>
<tr>
<th>Function</th>
<th>Operator's Role</th>
<th>Software Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contingency List Selection</td>
<td>Generate or Augment List</td>
<td>Generate List Based on Operations Planning</td>
</tr>
<tr>
<td>Probability of Contingency</td>
<td>Modify on Basis of System and Weather Conditions</td>
<td>Compute on Basis of Historical Data</td>
</tr>
<tr>
<td>Cost of Insecurity for Given Contingency</td>
<td>Interpret Simulation Result</td>
<td>Identify Possibilities</td>
</tr>
<tr>
<td>Impact of Contingency on System</td>
<td>Determine if Further Analysis is Required, e.g., Transient or Dynamic</td>
<td>Summarize Simulation Results in Adequate Form</td>
</tr>
<tr>
<td>Need for Corrective/Preventive Action</td>
<td>Recommend Corrective/Preventive Control</td>
<td>Compute Necessary Controls</td>
</tr>
</tbody>
</table>
Recommendations of the Federal Power Commission and of NAPSIC

The Northeast blackout of November 9-10, 1965, brought the utility systems of the country to the realization that a degree of vulnerability did exist, and that something should be done about the situation. The Federal Power Commission (FPC) began its study, and in July 1967 released its report on that subject. NAPSIC, the North American Power Systems Interconnection Committee--only three years old at the time of the blackout--also began a new series of studies, and upgraded its Operating Guides to provide more emphatic protection of bulk power system security.

Most of the 34 Recommendations of the F.P.C. have been translated into action by the utility systems and power pool organizations in North America. The recommendations stress coordination at the regional level for both planning and operation and for research into the remaining difficult problems; strengthening existing transmission systems and planning future expansions to be secure against contingencies; providing secure standby power for generating units and their auxiliaries; upgrading relay protective schemes, communications networks and display and recording equipment; making more effective use of computers; upgrading the training of operating personnel; making greater use of preventive maintenance and inter-utility reporting of troubles; and preparing for national defense emergencies.

Several of the recommendations relate to security enhancement through controls such as load shedding and generator isolation; and one, No. 17, directly addresses the subject of security assessment. It reads as follows: "Control Centers should be provided with a means for rapid checks on stable and safe capacity limits of system elements. The necessity for isolating a line or substation or dropping a generating unit, either in an emergency or for planned maintenance, can result in major shifts in network power flows. Rapid security checks to determine that various elements will be operated under safe limits under such modified conditions are essential to prevent unsafe loading. Rapid security checks are now feasible through the use of digital computers."

This recommendation for on-line contingency analysis is being followed by a number of utilities, as reported in the body of this paper, and research into improved security monitoring is currently very active.

NAPSIC's Operating Guides, like the F.P.C.'s recommendations, stress operating procedures for proper and safe operation, and for inter-utility coordination. The individual items are much more detailed than those of the F.P.C.

Operating Guide No. 21, approved in January, 1974 discusses the subject of security monitoring. The Guide recommends making off-line studies to determine potential problem areas, and making pre-planned solutions available to dispatchers. It recommends monitoring and display equipment to call attention to dangerous situations, and suggests the exchange of vital operating data between utilities. Voltage should be monitored and voltage schedules centrally coordinated. More specifically, the Guide recommends that "Transmission line monitoring should include a means of evaluating the effect of loss of transmission or the loss of generation or loss of both transmission and generation. Scheduled outages of facilities should be taken into account in the monitoring scheme."

APPENDIX B

State of the Art of Security Assessment in the Utility Industry

In this appendix we report the results of a questionnaire which was mailed to some 60 utilities in the U.S. and abroad, on the question of security assessment. Following is an interpretation of our findings.

A. Responses from 8 Large (>10 GW) Utilities in the United States and Canada

-- None has implemented to satisfaction an on-line, continuous or frequent steady-state contingency analysis program using power flow. However, two such utilities have implemented this program "with problems."
-- Only two are using distribution factors for contingency analysis.
-- Three are using power flow programs for off-line analysis of actual disturbances.
-- None has any present plans for an on-line transient security monitor, with or without interactive features.
-- Three are using transient analysis programs for off-line analysis of disturbances.
-- All are using transient analysis programs in the system planning process.
-- Seven are using automatic printout device for logging. One plans to add this capability in the near future.
-- Five now use input/output CRT display stations, and two others plan to do so in the near future.
-- Only one has implemented a form of security indices, and that one is experiencing problems.
-- There is a strong tendency to use a primary control computer for on-line monitoring and display functions, and to use a corporate computer for off-line studies.
-- Seven plan to utilize a state estimator and a bad data rejection program. The measurement redundancy ratios are from 1.5 to 2.9.
-- All have on-line tie-line power flow data, and half of this group have some on-line telemetering of some high-voltage line status, major generating unit status and spinning reserve in neighboring systems.

B. Responses from 28 Medium-Sized Utilities in the United States and Canada

-- Only two have implemented an on-line continuous or frequent steady-state contingency analysis program using power flow.
-- Three are now using similar programs but with distribution factors.
-- 18 use off-line power flows for post-analysis of disturbances.
-- Only one has attempted on-line analysis of contingencies involving transients. That one is satisfied with the program as implemented.
C. Responses from 6 Utilities (Medium-Sized and Very Large) in Europe and Japan

- Eight utilize off-line transient analysis programs for post-analysis of disturbances.
- Eleven use an automatic printout device for logging, and five more plan to do so in the near future.
- Only 8 use CRT input/output stations for display, with only 4 having near-future plans for such use.
- Three of these utilities have implemented to their satisfaction some form of security indices, and one plans to do so in the near future.
- In this group there is a more general mix of using corporate, standby control and primary control computers for on-line monitoring and display, and of corporate, special-purpose and secondary control computers for off-line functions.
- Not all of the respondents answered the questions about telemetered on-line data quantities. Of those who did, about 3/4 reported having on-line tie-line power flow data, while about half said they did have on-line information about some high-voltage line status, generator unit status and spinning reserve in neighboring systems.

D. Summary Evaluation of Utility Responses

- Power flow programs are well developed and widely used for off-line studies, but problems are revealed when attempts are made to use them for on-line contingency analysis. The major obstacles probably are inadequate information about neighboring systems, and inadequate methods of producing static reductions of external networks. These obstacles combine to produce highly inaccurate results when the conditions in either the external or the internal network is drastically changed, as it is in contingency analysis.
- Transient analysis programs also are well developed and are widely used for system planning studies even though their weaknesses are well known to most users. Only one utility reported successful use of an on-line transient contingency analysis program. It is safe to state that this usage is outside the present state of the art.
- The use of distribution factors is rare, but the utilities which do use them are "satisfied." The state of the art in simulation has far surpassed these distribution factors, but perhaps their usefulness is inadequately appreciated. They provide "ball-park" results at low computational cost.
- Security indices are well within the state of the art, conceptually, but their usefulness is not yet proven.
- State estimation has passed beyond the early R&D stage and some of the early myths about it have been dispelled. Still, only a few installations report much success. The concept is still in the vanguard of power system control technology.
- Some data rejection schemes and data-protective systems are row well developed and are used by any who have provided the economic justification.
- Of the utilities planning to use state estimation in the near future, most prefer the method of weighted least squares, possibly because it is the easiest to understand.
- Telemetering of information from the system's borders and beyond is well within the state of the art (both analog and digital). However, economic and other considerations inhibit the adequate development of inter-utility on-line data exchange systems.

For large systems, the major problems of operating the high-voltage grid are dynamic and transient stability. For medium-sized systems, the overwhelmingly most important problem is that of overloads. Other problems reported for this question were:

- System security
- Voltage and var balance
- Area Control
- Subsynchronous resonance
- Loss of customer loads
- Inadequate spinning reserve
- Short circuit levels
- Economics
REFERENCES

System Security - General Works


41. Final Report, EEI Project RP90-6, "Methods of Bulk Power System Security Assessment (Prob. Approach)" prepared by Electric Power Institute, Texas A&M University, College Station, Texas.


53. S. Narita and M. Hamann "Multicomputer control of voltage and reactive power in large-scale power pools," in Proc. 4th PSCC (Grenoble, France, 1972) Paper 2.3/1.


Steady-State Security Analysis

A. Contingency Evaluation and Load Flow Analysis


B. Interchange Capacity Calculations


C. Steady-State Equivalents


Transient and Dynamic Security Analysis


Transients and Dynamic Security Analysis

A. General Works on Transient Stability/Security


B. Numerical Methods


Measures of Security

A. Security Indices


263. Reference Number 40 above.


B. Probabilistic Security Measures


300. A. M. Sasson, "Combined Use of the Powell and
Fletcher-Powell Nonlinear Programming Methods

301. J. Peschon, et. al., "A Generalized Approach for
Determining Optimal Solutions to Problems Invol-
volved Technology and Security," System Control
Inc., Palo Alto, Calif., Final Report for Edison
Electric Institute, July 1970.

302. C. M. Shen and M. A. Laughton, "Power System
Load Scheduling with Security Constraints Using

303. J. F. Aldrich, J. F. Leuer, and H. H. Happ,
"Multi-area Dispatch," in Proc. 7th PICA Conf.

304. S. W. Andersen, R. T. Jenkins, and D. S. Joy,
"Short-Term Generation Schedule Optimization--A
Dynamic Programming Approach," Presented at IEEE
Paper 71 CP 598-MR.

305. N. V. Arvanitidis and J. Roel, "The Use of
Objective Functions in Real Power Dispatching," IEEE

Dispatch," in Proc. 7th PICA Conf. (Boston, Mass.,

"A Technique for Optimizing Real and Reactive

308. J. D. Guy, "Security Constrained Unit Commitment"

309. P. B. Henser and B. J. Cory, "Solution of the
Minimum Loss and Economic Dispatch Problems In-
cluding Real and Imaginary Transformer Tap Ratio"
in Proc. 7th PICA Conf. (Boston, Mass., 1971),
pp. 228-233.

310. F. L. Jaimies, and A. H. El Abiad, "Optimization
by a Sequence of Equality Constrained Problems--
its Application to Optimal Power Flow," in Proc.
7th PICA Conf. (Boston, Mass., 1971), pp. 219-
227.

311. J. C. Kaltenbach and L. P. Hajdu, "Optimal Cor-
rective Rescheduling for Power System Security," IEEE
Trans. Power App. &. Syst., Vol. PAS-90,

312. J. Peschon, D. W. Bree, and L. P. Hajdu, "Optimal
Solutions Involving System Security," in Proc.
7th PICA Conf. (Boston, Mass., 1971), pp. 210-
218.

313. W. O. Stadlin, "Economic Allocation of Regula-
ting Margin," IEEE Power App. Syst., Vol. PAS-

314. T. Adielson, "Determination of an Optimal Power
Flow By Iterative Suboptimizations," in Proc.

315. D. Arzamastev, P. Bartolomey, and A. Lipes,
"Statistical Gradient Method and Accelerated
Load Flow Calculation for Economic Load Schedu-
ling," in Proc. 4th PSCC (Grenoble, France, 1972).
Paper 2.1/7.

316. B. J. Cory and P. B. Henser, "Economic Dispatch
With Security Using Non-Linear Programming," in
2.1/5.

317. H. Daniels and M. S. Chen, "An Optimization
Technique and Security Calculations for Dispar-

318. J. C. Dodu, P. Martin, A. Merlin, and J. Pouget,
"An Optimal Formulation and Solution of Short-
Range Operating Problems for a Power System
With Flow Constraints," IEEE Trans. PAS-91,

319. C. H. Jollissaint, N. V. Arvanitidis, and D. G.
Luenberger, "Decomposition of Real and Reactive
Power Flows: A Method Suited for On-Line Ap-

320. O. P. Malik and A. S. A. Farag, "Optimization
of Power System Reliability Under Cost Con-
straint," IEEE Winter Power Meeting, New York,

321. J. Peschon, H. W. Dommel, W. Powell , and D. W.
Bree, Jr., "Optimum Power Flow for Systems with
Area Interchange Controls," IEEE Trans. Power
1972.

322. R. N. Mishra and V. R. Sastry, "Application of
Memory Gradient Method to Economic Load Dispa-

323. Y. Sekine and J. Kawakami, "Optimal Line Dis-
patching of Transmission Lines and Transformers,
" in Proc. 4th PSCC (Grenoble, France, 1972).
Paper 2.1/3.

324. R. L. Sullivan, "Minimum Pollution Dispatching,
presented at IEEE PES Summer Meeting, San
Francisco, Calif., 1972. Paper C72 438-0.

325. J. Peschon, D. W. Bree, and L. P. Hajdu, "Optimal
Solutions Involving System Security," in Proc.
7th PICA Conf. (Boston, Mass., 1971), pp. 210-
218.

326. W. O. Stadlin, "Economic Allocation of Regula-
ting Margin," IEEE Power App. Syst., Vol. PAS-

327. T. Adielson, "Determination of an Optimal Power
Flow by Iterative Suboptimizations," in Proc.


Security Enhancement