IEEE Transactions on Power Systems, Vol. 3, No. 3, August 1988

DYNAMIC SECURITY ASSESSMENT PRACTICES IN NORTH AMERICA

Working Group on Dynamic Security Assessment,
Power System Engineering Committee
A. A. Fouad, Chairman

Abstract: This paper reviews the dynamic security assessment practices followed by some of the member utilities of the interconnected power network of North America. It contains a condensed version of the presentations made by seven panelists at two National Meetings of the Power Engineering Society. A cross-section of the industry practices are given: the issues involved, the concerns and problems encountered, the various measures and approaches to deal with these problems (e.g., by off-line studies or by on-line schemes), and the future plans when applicable.

The panel members are: F. Aboytes of Comision Federal de Electricidad of Mexico, V. F. Carvalho (and C. Graham) of Ontario Hydro, G. Cepero of Florida Power & Light Co., S. Corey of the New York Power Pool, K. Dhir of Middle South Services, R. Vierra of Pacific Gas & Electric Co. and A. Fouad of Iowa State University. P. Sauer of the University of Illinois chaired the panel.

INTRODUCTION

In North America the term power system security is used to mean "the ability of the bulk power electric system to withstand sudden disturbances such as electric short circuits or unanticipated loss of system components." This is the definition given by the North American Reliability Council (NERC) in its reliability reports and is accepted by the electric utility industry. In terms of the requirements for the proper planning and operation of the power system it means that following the occurrence of a sudden disturbance, the power system will: i) "survive" the ensuing transient and move into an acceptable steady-state condition, and ii) in this new steady-state condition all power system components are operating within established limits.

In the last two decades the electric utilities in North America have become increasingly concerned with security analysis to ensure that, for a defined set of contingencies, the above two requirements are met. However, the analysis required to meet the first requirement (i.e., surviving the transient) is transient analysis, which has recently become more complex to perform. This complexity has risen because of the increased system size, greater dependence on controls, more interconnections, and the operation of the interconnected system with greater interdependence among its member systems, heavier transmission loadings, and the concentration of the generation among few large units at light load.

The second requirement is met, however, by steady-state analysis. Techniques are now available to perform this type of analysis quickly and reliably. The state-of-the-art has advanced to the point where "security packages" are now available at Energy Management Centers, which analyze numerous contingencies using up to the minute data.

It is becoming an accepted terminology to call the latter analysis "Static Security Assessment." The former analysis, i.e., the transient analysis to determine whether the system survives the transition, is the subject dealt with in "Dynamic Security Assessment." It is the subject discussed in this paper.

The framework for assessment of a power system's ability to withstand contingencies and arrive at acceptable steady-state operating conditions is typically as follows: off-line studies are performed for different initial operating conditions and system configurations, for a prescribed sequence of events or contingencies. From these studies, "safe" operating levels are arrived at for a variety of system conditions. These are often given in terms of a critical system operating parameter such as: the loading of a certain power plant, the power flow at critical transmission interface, the voltage at a given bus, and so on.

Even with the relatively simple framework described above, the situation is considerably complicated by two main factors:

1. The diversity of conditions existing in the North American power networks regarding: size, load density, strength of transmission, strength of interconnections, etc. This diversity is reflected in the type of contingencies to be studied, and the type of transient phenomena to be analyzed; hence, in the dynamic security practices and concerns. For example, the phenomena to be analyzed range from the response of the system to small disturbances to extended transient stability, and from voltage and VAR problems to frequency transients

2. The power networks are operating closer to their "limits" due to heavier transmission loadings, increased power transfers, etc. Dynamic security is of primary concern in some systems, especially those with stability-limited operating constraints. In addition, the security of one power system often strongly depends upon the operating state of its neighbors.

The above factors have brought dynamic security into sharp focus lately. To be sure the industry is adequately coping with what is becoming a burdensome task: to maintain system security at all times. At the same time, will the ever changing conditions of modern power networks and the tools of analysis now available to the analyst make it possible for the industry to cope in the future? and could these tools of analysis be improved? these questions are at the heart of the issues addressed by the Working Group on Dynamic Security Assessment. To meet its objectives, the Working Group is attempting to identify the key issues involved, provide forums to discuss and clarify these issues, and encourage development of techniques to deal with them.

Current Industry Practices

To help address the issues outlined above, it is felt that a review of a sample of the current industry practices in the area of dynamic security assessment is in order. Panel sessions in recent National Meetings of the Power Engineering

87 SM 471-6 A paper recommended and approved by the IEEE Power System Engineering Committee of the IEEE Power Engineering Society for presentation at the IEEE/PES 1987 Summer Meeting, San Francisco, California, July 12 - 17, 1987. Manuscript submitted February 24, 1987; made available for printing April 24, 1987.

Society were organized along these lines. Future sessions will be planned to deal with issues identified as needing attention by the industry.

In our effort to have a common framework for dealing with the issues, the organizers* of the panel sessions on "Current Industry Practices" requested of the panelists to address the following questions in their presentations.

1. Identify the dynamic security concerns in their control area which affect the ability of their system to withstand a defined set of contingencies, and to survive the transition to an acceptable steady-state condition. The transition time was identified as up to 15 seconds to 5 minutes. The panelists were also asked to identify: a) what constitutes normal steady-state conditions, and b) conditions which affect their system's dynamic security.
2. Indicate how their system's response is currently affected. For example:
   a. identify parameters used to provide assessment,
   b. whether response is manual or automatic, and
   c. efforts made to address the concerns on an inter-control area basis.
3. Suggest how the responses described above be improved (given sufficient resources).

The panelists' presentations are summarized below.

DYNAMIC SECURITY ASSESSMENT IN CFE INTERCONNECTED SYSTEM

F. Aboytes

Centro Nacional de Control de Energia

(National Energy Control Center)

Introduction

This presentation summarizes the dynamic security problems and the corresponding analyses that are performed at CFE's National Control Center (NCC). CFE is the national electric utility in Mexico in charge of planning, constructing, and operating all the electric facilities in the country. It covers most of the Mexican territory, almost 2 million square Km. It should be pointed out that from the hydro plants in the southeast to the northwest part of the system there are more than 3,000 Km. Bulk transmission system is formed by 400 KV lines in the south and 230 KV lines in the north.

Main characteristics of the CFE interconnected system are summarized in Figure 1. It is a typical longitudinal system with remote generation centers and concentrated load areas that are dispersed in a very large geographical extension. As a result, the system is weakly interconnected and it is affected substantially by real and reactive power changes. Additionally, common problems faced in its operation require the analysis of dynamic phenomena.

One of the main objectives of the CFE control center is the implementation of security measures that keep the system operation through a sequence of secure states.

In the security analysis it is important to evaluate the effect of contingencies to determine operating limits, and also to design preventive operating strategies.

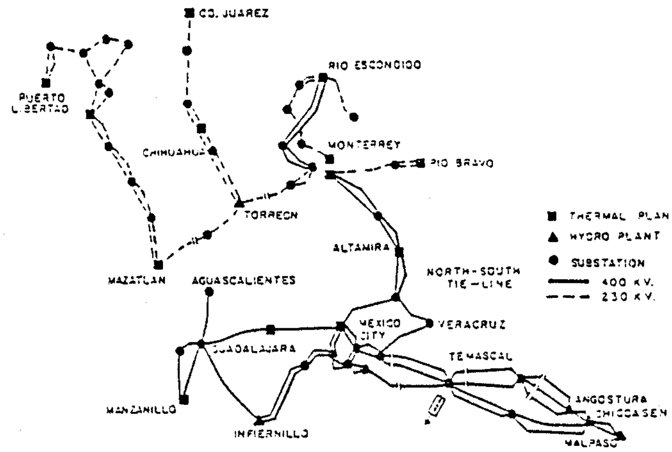


Figure 1. Mexican Bulk Transmission System

Operating criteria in the CFE interconnected system are based on a first contingency security standard. That is, the most critical single contingency in the system should not create emergency conditions or a partial collapse. However, the applications of this security standard in our system can lead to the trade off security versus economy. This is the case of remote generation sites, linked through not fully redundant transmission systems. If security conditions are applied, generation levels must be reduced and economic operation is substantially affected. In these cases, CFE has considered the use of supplementary control actions to improve the economic operation of the system and, at the same time, control actions are available to protect the system against a system collapse.

Typical Operating Problems in the CFE System

1. Faults in highly loaded transmission system linking remote generation centers. In the cases transient instability is a major concern.
2. Loss of voltage control devices that can lead to a voltage collapse or voltage instability.
3. Given the structure of the system, the operation in electrical islands is also very important. In these cases the generation-load imbalance will determine the frequency behavior in every island.

   For all these problems, preventive actions must be taken as there will be no time to implement corrective measures once critical contingencies have occurred.

1. **Stability**

Figure 2 is a schematic configuration of electrical areas in the system; in the north, single 230 KV lines are used as tie lines. North-South interconnection is through 2 - 400 KV lines.

In recent years supplementary control has been used to improve the utilization transmission facilities and energy resources. They are implemented in several areas of the system and require systematic analyses to evaluate their performance under different operating conditions.

Potential transient stability problems have been detected in several areas of the system, in many cases instability may occur in less than a second, therefore appropriate preventive measures have to be taken to eliminate the risk of instability. Generator dropping has been used in four areas to increase transmission limits, the scheme is based on predefined strategies to trip generators, should transmission outages occur.

---
* A. DiCaprio of the PJM interconnection, V. F. Carvalho of Ontario Hydro, A. Fouad of Iowa State University, J. Raine of Florida Power & Light Co., and P. Sauer of the University of Illinois.

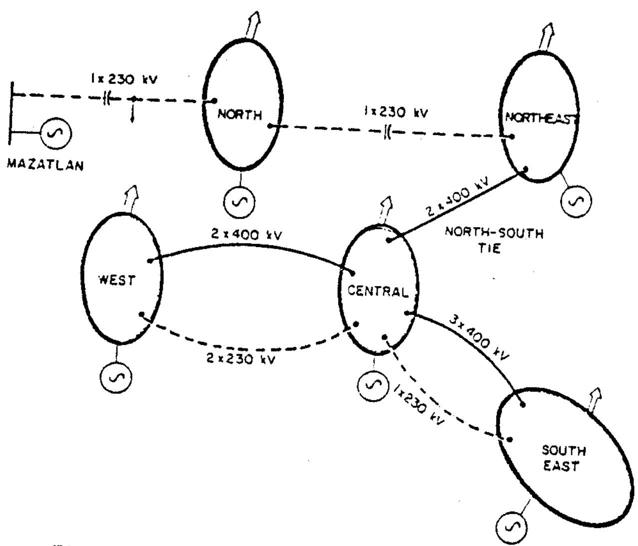


Figure 2. Schematic Diagram of CFE Areas

One of the applications of this scheme is in the southeast area, where 16 hydro units in three plants, with total capacity of 3,500 MW, are linked to the main load center in Mexico City through a 400 KV transmission system. We have several series compensated lines and a ± 300 MVAR static var compensator installed in this area of the system.

As the power flow exceeds a prespecified value, that depends on the configuration, the generation tripping scheme is activated by the operator in the Area Control Center. If by any reason, faults, manual tripping, etc., transmission lines are disconnected, an order is sent to trip certain units via power line carrier communication channels. The average time delay of this operation is eight cycles. The selection of units to be tripped will depend on the configuration of the system and the operating conditions. The transfer limits upon which the scheme is activated has to be continuously assessed as it varies substantially according to system configuration.

2. **Voltage**

Voltage control is an important problem in the operation of the system. Problems become critical under contingencies that produce large reactive power changes.

Six static var compensators of different types are installed in the system to obtain an appropriate voltage profile, but more important to provide a distributed reactive power system reserve for contingencies.

In the northeast area we have examples of transient stability and voltage control problems. Here a continuous supervision and assessment of generation levels in Rio Escondido power plant is required. This plant has 3 x 300 MW units and in the near future a fourth unit will be in service. An Automatic Generation Tripping Scheme (AGTS) has been implemented in this plant. Extreme conditions can be detected under maximum and minimum loading conditions. In the latter case voltage control becomes a problem as voltages at intermediate nodes are very sensitive to the number of units connected and the configuration of the transmission system.

Similar cases are detected in the west area, here the Manzanillo power plant has 4 x 300 MW units whose output is delivered through 2 x 400 KV lines. Each of these lines is equipped with single pole switching schemes, and also an automatic generation tripping scheme is available should a three pole tripping of the 400 KV lines occur. This area is also characterized by lack of voltage support in important load centers. Hence a continuous supervision and assessment of reactive power allocation is required to anticipate the effect of contingencies.

At the Infiernillo substation an automatic bus splitting scheme is implemented that prevents that all the generation from two hydro plants (1300 MW) could be left through a single 320 MW, 400 KV line under the outage of a 400 KV double circuit. This is an example of the control measures taken in system operation, through technical studies, to improve system performance and security.

Other important supplementary control implemented is the automatic load disconnection scheme. It is applied in the north area to control the power flows in the interconnection lines. It should be recalled that this area is connected through single 230 KV lines to the northeast and northwest areas. Hence the electric and inertial response of these areas is transmitted through very weak links. This is a fast acting shedding scheme (0.3-0.4 second) that tries to avoid stability problems and it operates based on the power flow of certain transmission lines. Assessment of activation limits is required as operating conditions change and when new generating units and transmission lines become operational.

3. **Islanding**

As a result of system structure, the operation in electrical island outages should be evaluated continuously. For these cases an adequate underfrequency load shedding scheme is essential to control the frequency decline in islands with generation deficits.

In our system very high frequency rates of decay can be observed in importing areas (2-3 Hz/sec). Under these conditions, a very close supervision of the scheme should be performed in system operations to anticipate its performance under different configurations. In some cases a coordination is necessary with voltage control strategies to improve system performance.

Most of the CFE underfrequency load shedding scheme is based on solid state underfrequency relays with a definite operating time of 6 cycles. Also 50% of the load is included in the load shedding scheme, this fact has to be considered, especially under light load conditions when load shedding could result in very high voltages, with risk of unit tripping by underexcitation. As an example to show the operation of the scheme, on July 27, 1983 as a result of a fault in a 400 KV line and a relay missoperation, several islands were formed, the largest island had a generation deficit of 1800 MW. A minimum value of 58.35 Hz was observed. After the operation of four shedding steps the frequency returned to a value very close to 60 Hz. More than 1200 MW were disconnected in less than a second.

4. **Computing Facilities**

I will now give an overall idea of the computing facilities and programs available to analyze and solve these problems.

All the dynamic security assessment is performed off-line on a PRIME 550 Computer with 1.5 megabytes of main memory.

This computer is dedicated to evaluate the security of the entire system. It is used at the National Control Center in Mexico City and at eight Regional Control Centers around the country.

An overview of the functions that are considered necessary in the security analyses is presented in Figure 3.

The models for electromagnetic transient and dynamic equivalents are still in the phase of development or testing. It is important to point out that at the NCC all the information of the interconnected system is available through the data links with the computers at six Regional Control Centers.

In all the dynamic studies a predisturbance condition is necessary as a starting point, this is obtained from a steady state simulator that is also implemented in this computer. This simulator is also used to perform load flow calculations and sensitivity analysis.

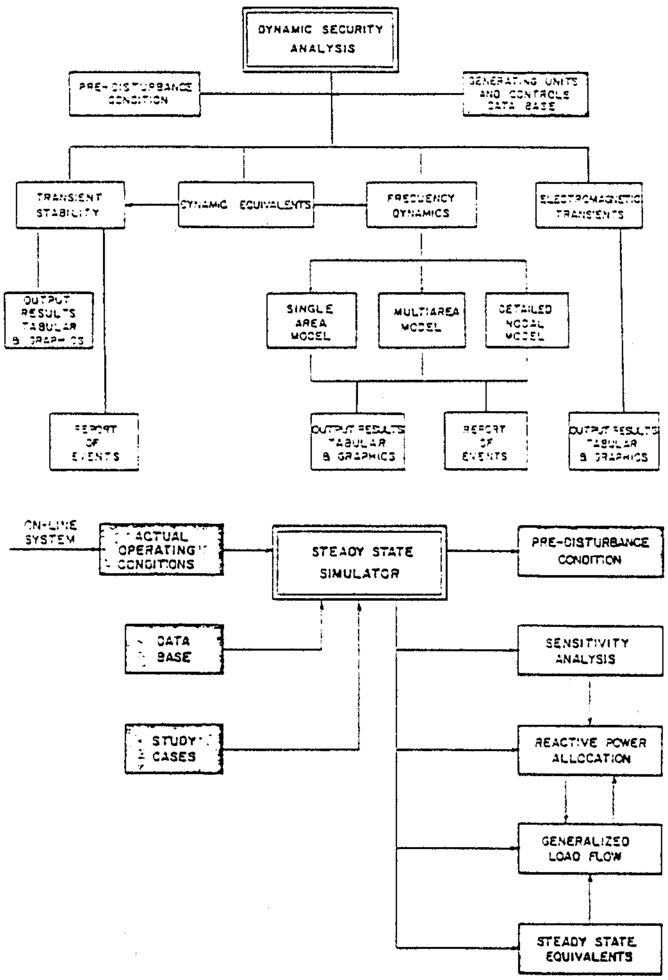


Figure 3. Security Analysis Functions

Load flow calculation and sensitivity analysis could be performed and the corresponding files are stored with basic information for the predisturbance condition.

5. **Future Plans**

At present we do not have a direct link between the on-line computerized system and the steady state simulator, but we expect to have it in the future.

We believe that there is still much to be done to improve the security of our system, but practical solutions have to be implemented combining security and economic factors.

We are interested and are studying possible ways of implementing automatic segregation schemes to protect the system under very critical events.

Also consideration has been given to load shedding based on information of power flows, voltages, frequency, or a combination of variables.

Effort has also been concentrated on analyzing and selecting variables to be used for an automatic activation of supplementary controls that could take care of expected and unexpected contingencies.

Tuning of models and adjustment of parameters are essential in dynamic security studies, they could be improved through the systematic use of dynamic information from the system under disturbances. Tests have been conducted to obtain appropriate recordings of dynamic data.

Although it is not a common problem, low frequency sustained oscillations have been detected several times, as these oscillations depend on system configuration and operating conditions, there is a growing interest in assessing the damping of these oscillations, especially when most of new generating units are equipped with fast excitation systems and power system stabilizers.

The operation of the CFE system and of the many longitudinal systems face complex operating problems; most of them related to the dynamic behavior of power systems. This requires that the operating personnel must exercise continuously their preventive attitude to reduce the risk and effects of contingencies. This is a task to be performed all the time; based on the knowledge of the system, considering the supplementary controls available and trying to optimize the usage of resources. In this decision-making process interactive computer models play an important role.

Although computers and expert systems are evolving rapidly, we believe that in this type of system it is essential, and most important, to improve the technical background of system operators, dispatchers, and system analysts, so that they can better analyze and solve the challenging problems faced in the operation of longitudinal power systems.

DYNAMIC SECURITY ASSESSMENT

AT ONTARIO HYDRO

V. F. Carvalho

Power System Operations Division

1. **Dynamic Security Concerns**

The operation of Ontario's Power System is constrained by stability problems arising from the transfer of power over long distances and by weakness in the overall transmission caused by severe delays in obtaining routes for new 500 kV transmission lines. High reliability standards set by the company and by the Regional Council (NPCC), combined with stability problems, have resulted in difficulties in managing the stability of the power system in real-time. Various techniques have been developed for Ontario Hydro's System Control Centre in order to manage the stability problems as outlined in this presentation.

The basic philosophy of operation is that the system should always be operated to observe company and pool contingency criteria.

Steps including interruption of Firm load are taken to ensure that transmission limits are observed in System Operation. Following recognized contingencies in the NORMAL state:

a) The system should be stable (survive the transition).

b) Damping should be good (Damping ratio should be > .01).

c) Line loadings should be below the 15-minute limited time rating.

d) Voltage drop (at the 230 kV/115 kV level) should not exceed 10% for double element contingencies and 5% for single element contingencies.

Repreparation for the next event (the transition from the Alert State back to the Normal State) should be as follows:

a) Repreparation should commence as soon as possible.

b) Should not exceed about 15 minutes during adverse weather.

c) Should not exceed about 30 minutes otherwise.

Dynamic Security Assessment should be updated in 30 seconds to one minute in order to allow as much time as possible for decision and action time.

2. Types of Stability Problems

The instability phenomena encountered are three basic types: 1) Plant Mode, 2) Interarea Mode, and 3) Voltage Instability. The Plant Mode of instability and voltage instability arise for two reasons: firstly, delay of incorporation facilities, and secondly, during major transmission outages. The interarea mode occurs because of insufficient transmission capacity between major subsystems of the Eastern Interconnection. These types of instability are mitigated by Discrete Control Schemes which further complicate the security assessment problem.

3. Managing Dynamic Security Problems in Real Time

The basic problem in real-time management of the Dynamic Security problems is the definition of the boundaries of secure regimes and displaying these to the operator. However, algorithms are not available at the present state of the technology to enable the secure regimes to be adaptively computed in real time. The following procedure is followed at Ontario Hydro:

a) Operator Guides are provided for the "normal" system connectivity and for any one of "n" critical elements out of service (i.e., (n-1)).

b) For outages of critical elements exceeding the above, instructions are provided on demand by off-shift engineering staff.

c) All stability limits are monitored by a Pattern Matching software system and "proximity to limit" bars are displayed and out-of-limit conditions are alarmed to the operator (see Figure 4).

d) Discrete control schemes, such as generator rejection, are monitored and associated limits are automatically adjusted to account for the status of arming these schemes.

4. Intercontrol Area

The dynamic security assessment problem gets more complicated if more than one control area is involved in a common stability problem. As shown in Figure 5, operating limits may have to be reduced so that each system can be operated independently or special procedures need to be developed for coordination of real-time operation.

5. Future Requirements

Future requirements would require that the system described in Figure 6 be extended to be adaptive to changing system loading and connectivity. This system would process a list of contingencies (based on a discrete list or based on leveling the risk) and use algorithms (rather than off-line studies) to determine the secure regimes. A check would first be required to determine if any special operator guides were available for the specific information in case the algorithms provide approximate results.

Figure 4 USUAL ASSESSMENT TECHNIQUE AT ONTARIO HYDRO'S SYSTEM CONTROL CENTRE

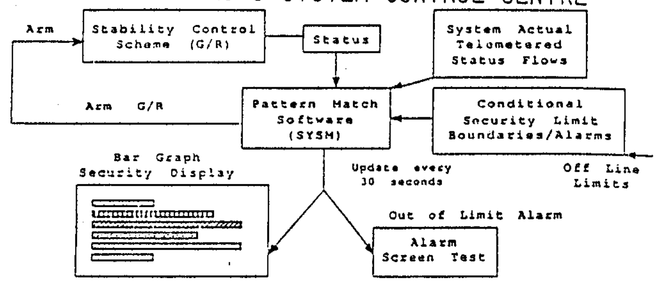


Figure 5 INTER-CONTROL AREA

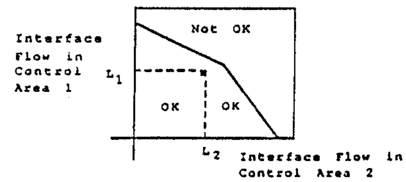
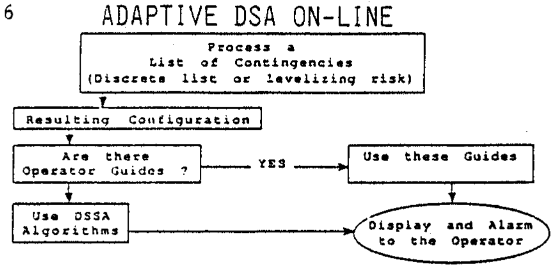


Figure 6 ADAPTIVE DSA ON-LINE



DYNAMIC SECURITY ASSESSMENT AT FLORIDA POWER & LIGHT CO.

Gus R. Cepero

System Planning Department

Background

Over the past five years, Florida Power & Light Co. (FPL) has added two major 500 kV interconnections with Georgia Power and extended its 500 kV system from the Florida-Georgia State Line to Southeast Florida.

Concurrently with the transmission expansion, FPL has increased coal-by-wire transfers from less than 100 MW in 1979 to a current level of 2000 MW from Southern and up to another 1000-1500 MW from other Florida utilities.

In 1985, FPL interchange purchases accounted for nearly 35% of the FPL energy mix. By contrast, just five years earlier, FPL purchases constituted much less than 5% of the energy mix.

The 500 kV expansion and the large increment in coal-by-wire purchases have caused profound changes in the behavior and protection requirements of the electrical system.

FPL operates the system with sufficient margins to withstand any single contingency without experiencing overloads or low voltages. Consequently, there are no transient, dynamic, or steady state security problems following single contingencies. Indeed, the 500 kV expansion has significantly improved the single contingency system performance because Florida-Southern separations, which were at one time common place for single contingencies, are no longer a risk. FPL has an on-line system security assessment capability (see presentation for characteristics of the system) which assists FPL operators in insuring the system satisfies this constraint.

FPL, however, is vulnerable to transient and dynamic* instability for double contingencies. Prior to the 500 kV expansion, the Florida systems had very weak interconnections with Southern and would readily separate from Southern for double contingencies and initiate underfrequency load shedding. The addition of the Florida-Southern 500 kV interconnections has significantly strengthened the interface and the tendency is for the systems to remain interconnected even for double contingencies. Therefore, FPL had to revise its strategy to cope with double contingencies.

FPL has implemented a family of remedial schemes (HIR exciters in 12 generating units and 600 MW of load set at 59.82 Hz. for ultra-fast shedding) aimed at stabilizing system behavior during the transient (0-10 seconds) period following a double contingency. The remainder of this discussion will concentrate on the measures which FPL has adopted to assess and control the dynamic (0-60 seconds) stability of the system, following double contingencies.

Dynamic Security Assessment

More specifically, FPL needs a dynamic security assessment and control system because the sudden loss of two or more large (> 600 MW) generating units, or of a 500 kV corridor, may result in severe reactive overloads and a voltage collapse (system separation) within 30 seconds unless automatic corrective action is taken.

The risk exists because of three basic reasons. First, the bulk transmission system is heavily loaded during normal conditions (normal - 100% of SIL; post-contingency - 150% of SIL); second, at times, up to 50% of the load is served with interchange power which means there are fewer local reactive generation sources to support the voltage following the contingency. And, finally, there is a limited number of transmission paths to deliver synchronizing power flows (two 500 kV and two 230 kV).

The reactive overload condition which results from a double contingency must be corrected in less than 30 seconds to avoid voltage collapse. The 30 second window is based on two factors:

- Units can tolerate reactive overload for approximately 30 seconds. Maximum excitation limiter (MEL) protection will reduce field voltage to rated levels normally after 30 seconds.
- Distribution voltage regulators will start boosting feeder voltages after approximately 30 seconds.

The need to act in less than 30 seconds was a controlling factor in defining and evaluating the alternatives to prevent the conditions described above. Specifically, this need effectively precluded any alternative which involved post-contingency human operator intervention. The alternatives considered were as follows:

- "Force" Early System Separation
- Restrict Imports
- Add Massive Reactive Compensation
- Develop a Fast (< 30 seconds), Limited (800 MW) Load Shedding System.

The last alternative was eventually selected because it offered the most favorable balance between cost and reliability.

The design requirements of the fast, load shedding system were as follows:

- Must key on system conditions rather than frequency decline.
- Must segregate between single and double contingencies.
- Must execute in < 30 secs. and preferably < 20 secs.
- Must be secured from false/mis-operations.

Alternative systems were investigated and the assessments for each alternative were made.

The mechanics, characteristics, and decision criteria of the system eventually implemented were developed.

FPL continues to evaluate alternatives to control dynamic system response following severe contingencies. We are investigating the cost and feasibility of transmission improvements to avoid any load shedding, even for double contingencies. However, even if these improvements are implemented, some version of the current fast acting load shedding system will likely remain operational as a "back-up."

SECURITY ASSESSMENT FOR SYSTEM OPERATION AT THE NEW YORK POWER POOL

Steven L. Corey

Introduction

Following the Northeast Blackout in 1965, the New York Power Pool (NYPP) was formed to improve the reliability of operation of the electric power system in New York State. The Pool consists of eight (8) member utilities that serve approximately 99% of the load in the state. The NYPP is directly connected to four neighboring systems: Ontario Hydro (OH), the New England Power Exchange (NEPEX), the Pennsylvania-New Jersey-Maryland interconnection (PJM) and Hydro Quebec (HQ). NYPP is a member of the Northeast Power Coordinating Council (NPCC).

NYPP, a summer peaking system, recently established a new record peak load of 23,006 MW. The bulk power transmission system consists primarily of 345 kV and 230 kV transmission, with one 765 kV tie-line that originates in the Hydro-Quebec system near Montreal, runs down to Massena in the northern part of New York State, and terminates in central New York near Utica.

Although the number of functions performed by the Pool has expanded over the years, its primary mission, the secure operation of the Bulk Power System, has never changed. In the past, security assessment for operations has concentrated on static security analysis, which will continue to be an important factor for some time. However, in recent years work has begun in the area of dynamic security assessment (DSA), which is beginning to have an impact on system operation.

* The author notes that the term "dynamic stability" is sometimes used in this paper instead of "steady-state stability" as recently recommended by a Task Force of the Power System Engineering Committee.

Security Assessment At NYPP

Both on-line and off-line computerized methods of security assessment have been used at NYPP since the early 1970's. Seasonal transfer limit studies were conducted using the off-line computer to determine the first-contingency real power thermal transfer limits for several transmission interfaces under peak load conditions. The on-line computer allowed the system dispatcher to monitor the actual power flows across the transfer interfaces against the transfer limits. The dispatcher also monitored line flows, bus voltages, and system frequency with respect to appropriate ratings, limits, and normal operating levels. The off-line computer programs were later improved to allow the thermal transfer limits to be evaluated on a daily basis. An on-line contingency evaluation program was implemented which used distribution factors to predict the transmission line flows that would result from unexpected single line or generator outages.

In 1977, the NYPP began to operate under Pool-wide Economic Dispatch and Automatic Generation Control. Security assessment was an integral part of the economic dispatch process. The system dispatcher ran security assessment programs that identified potential pre- and post-contingency transmission overloads, and provided recommendations in the form of generation shifts to relieve the overloads. These programs were somewhat cumbersome for the dispatcher to use.

After the blackout of New York City in July 1977, the NYPP continued to add to and improve its on-line security assessment programs. An on-line multiple contingency evaluation program was implemented which, again using distriubtion factors, can predict the steady-state transmission line flows that would result from the unexpected outage of up to ten transmission lines and/or generators. In 1981, the Pool replaced its classical economic dispatch program with the Security Constrained Dispatch (SCD) program which automatically factors pre- and post-contingency transmission constraints into the economic dispatch solution. This freed the system dispatcher of some of the burdens placed on him by the previous security assessment programs, and also improved the response to system security problems.

In the late 70's and early 80's, as oil prices went up and up and thermal transmission bottlenecks were removed, the power transfers across the transmission system increased dramatically. The emphasis of off-line studies shifted from thermal transfer capacity to voltage and transient stability concerns. An increasing number of incidents of unusual voltage decline caused the Pool to establish more restrictive voltage operating criteria. The Pool also began to observe transient stability related transfer limits on key transmission interfaces on the basis of off-line computer simulation analysis. The Operations Engineering Section was established at the Pool to perform short-term off-line security studies used to determine necessary operating limits to address voltage and transient stability concerns.

Present State Of DSA At NYPP

The NYPP Operating Committee has established the following security criteria for normal operation of the NYPP Bulk Power System. (Simplified)

1. Flows on transmission lines must be within normal ratings.
2. Predicted post-contingency flows on transmission lines must be within appropriate emergency ratings.
3. Bus voltages must be within pre-contingency high and low limits.
4. Bus voltages must be within post-contingency high and low limits following a contingency.
5. Transfer interface flows must be within transient stability transfer limits.

The pre- and post-contingency transmission criteria are addressed by the on-line contingency evaluation and Security Constrained Dispatch (SCD) programs mentioned earlier. Although the SCD program uses static security assessment techniques, the program runs on a nominal five minutes cycle and uses a five minute ahead load projection for security computations, thus attempting to recognize the short-term load trend of the system.

The post-contingency high and low voltage limits are normally $\pm 5\%$ of the nominal voltage level. (e.g. For a 345 kV bus the post-contingency high and low limits are 362 kV and 328 kV respectively.) However, the post-contingency high limits of many buses are more than 5% above nominal voltage. The post-contingency low limits were determined by experience and judgement.

The pre-contingency voltage limits are intended to be set such that the post-contingency limits would not be violated following the worst case criteria contingencies. Until recently these limits were determined on the basis of experience and judgment. In the last two years, however, some of the limits have been determined on the basis of off-line loadflow based voltage analysis. The analysis technique involves running several base case and contingency case load flows for various levels of transfer across an interface to determine the pre-contingency voltage level that corresponds to the point where the worst contingency case voltage falls below the post-contingency low limit, or rises above the post-contingency high limit.

The transient stability transfer limits are determined by running off-line time domain transient stability simulations for various transfer levels. Once the highest stable transfer level for an interface has been found, a 10% safety margin is applied to determine the operating limit. Machine angle swings, transfer interface flows, and transient bus voltage performance are key parameters that are evaluated in each transient stability test. Distance relay performance is also reviewed on critical parallel and underlying transmission facilities. For a run to be considered "stable" there can be no relay operations, the test must be stable for the "first-swing" and all parameters must exhibit positive damping in subsequent swings.

The on-line Security Assessment and Security Constrained Dispatch programs monitor the transfer flows across the transmission interfaces vs. the transient stability transfer limits, and will automatically shift generation if necessary to remain within the limits.

Although NYPP internal transmission or transfer constraints are normally handled automatically by the on-line security programs, the system dispatcher must take action when the transmission constraints involve tie-lines to neighboring systems, or when there is insufficient dispatchable generation in the Pool to relieve the constraints.

The voltage limits are monitored by the on-line computer. A warning is issued if the voltage at a bus approaches its pre-contingency high or low limit, and alarms are issued if the voltage exceeds the pre- or post-contingency limits. An Operating Policy provides the dispatcher with instructions and responsibilities for handling voltage problems, but the Pool and Member System dispatchers must determine the specific corrective actions to take.

DSA In The Future

It is obvious that we have only scratched the surface of the Dynamic Security Assessment issue. The following are just some of the concerns that should be addressed:

1. Off-line transient stability and voltage studies can only consider a relatively small number of "typical" or "worst case" operating conditions. These studies can not cover the full spectrum of system conditions that are encountered in actual operation.
2. More evidence of "dynamic oscillations" are being encountered in the transient stability studies and in actual operation. Current load models are not adequate to properly simulate the dynamic response of the system beyond about 10 seconds. Restrictions on the size of the system representation and the availability and reliability of data are common obstacles that inhibit adequate study of this phenomenon.
3. Although it appears that on-line implementation of direct energy methods of transient stability analysis may be feasible, this technique does not address the dynamic stability problem. Other on-line dynamic stability analysis techniques must be developed.
4. Once the dispatcher has been provided with the ability to determine that the system may be insecure or is moving toward insecurity in the dynamic security sense, he will also need to know what control actions may be taken to move the system to a more secure state. Ideally the boundaries between the secure and insecure state should be expressed in terms of parameters that the system dispatcher can recognize and control.
5. It is important to be able to quickly assess the state of the system following a large disturbance so that preparations can be made for the next possible contingency. Security assessment programs, both static and dynamic, need to be fast in order to minimize the time of exposure to the next contingency. These programs must also recognize that the system is probably still adjusting to the initial disturbance.
6. The voltage collapse phenomenon should be studied in greater detail to determine if the security criteria and associated operating limits currently in use are adequate and appropriate.
7. Many dynamic security problems are not confined to individual utility or control area boundaries. A lot more understanding, cooperation, and coordination on an inter-regional basis will be required to effectively deal with these problems.

A number of other concerns will need to be addressed, but the above represents some of the major concerns that will need to be addressed in order for DSA programs to be useful in system operations.

In conclusion, I would like to say that Dynamic Security Assessment is definitely needed since the power system is a dynamic system, and all system security problems are really dynamic in nature. DSA methods of analysis are currently being used in off-line studies to determine operating limits for system operation. Much more work is needed, however, to adequately address all the concerns and problems facing the modern system dispatcher.

DYNAMIC SECURITY ASSESSMENT AT MIDDLE SOUTH SERVICES, INC.

Kanwal J. Dhir

System Planning Department

General

The Middle South Utilities bulk power system is operated as a single control area by a System Operations Center located in Pine Bluff, Arkansas. The generating units are dispatched so as to minimize the total system production cost. This control area is further divided into several sub-areas.

The operating philosophy is that all line loadings and interface loadings are within predetermined first contingency limits. Voltage on the transmission facilities will not drop more than 5%. Enough spinning reserve is available so that loss of the single largest generating unit will not overload the interface.

D.S.A. Concerns

Middle South's dynamic security assessment concerns are mainly due to thermal problems caused by power transfers and reactive conditions. These concerns become more pronounced under light load conditions.

Procedure

The current assessment procedure is as follows:

a. **Off-Line**

- Off-line studies are made to determine loading limits on line(s), interface(s) and plant(s).
- These limits are derived for different system conditions, network conditions and equipment in and out of service.
- Operating guides are prepared and provided to the operating staff.

b. **Contingency Analysis**

Contingency analysis is based on monitoring of actual line loadings and interface loadings and voltages at major locations throughout the system. These are then compared to predetermined/preset limits and an alarm is sounded whenever these metered values exceed the precomputed limits. Generally, a safety margin is maintained between the alarm value(s) and the limiting conditions. This is to provide the operator enough time to monitor and/or initiate corrective action.

The response is usually manual. The operator will readjust the generation dispatch and initiate switching, if needed. Normal loading limits and voltages are used as guidelines. There is some automatic response, but it is reserved for serious operating conditions. With the ever changing operating conditions, it is impossible to pre-study all possible contingencies and provide operating guidelines. Thus what is needed is an on-line security assessment.

c. At the System Operations Center, the operator(s) run a contingency evaluation program every hour on a Real Time Dispatch based load flow. This program consists of 20 most critical contingencies, previously determined off-line. The evaluation consists of running a full load flow to determine line flows above a preset level, and low voltages. In addition, an Equal-Area Criteria stability evaluation is performed for each of the 20 contingencies.

d. The existing Middle South Operations Center is in the process of being upgraded to a state-of-the-art control center. When completed, it will have, among others, the capability for:

1. State Estimation
2. Contingency Evaluation
3. Transient Stability
4. Optimal Power Flow
5. Security Dipatch
6. Voltage Scheduler
7. Load Forecaster - with Weather Effects
8. Unit Commitment
9. Interchange Transactions Evaluator
10. Training Simulator

3. **Inter-control Area**

The dynamic security assessment of the inter-control area concerns are dealt primarily by direct communication between the various system operators. Also, increasingly an attempt is being made to exchange data on generation and transmission outages, coordinated maintenance scheduling, requested power flows, joint operating studies and also coordinated planning of facilities.

DYNAMIC SECURITY ASSESSMENT AT PGandE

R. Vierra

Power Control Department

Introduction

The PGandE Control Area encompasses 94,000 square miles in Northern and Central California from the Oregon-California border in the north to the Tehachapi Mountain range in Southern California. The primary backbone transmission for this large area consists of two 500 kV A.C. transmission lines that transfer power between the Northern and Southern boundaries of this vast area. This major transmission path is unique that it can be severely impacted by disturbances on other major transmission paths outside the area as well as those within the Company area. To analyze dynamic security assessment within the PGandE area, it then becomes necessary to become familiar with the bulk transmission systems both within and outside the PGandE control area.

WSCC Area

Four major National Electric Reliability Council (NERC) areas presently make up the Western Systems Coordinating Council (WSCC) region. These are divided into:

1. The Northwest Power Pool area
2. The Rocky Mountain Power area
3. The Arizona-New Mexico Power area
4. The California-Nevada Power area

A.C. transmission at 500 kV, 345 kV, 287 kV, and 230 kV as well as 850 kV and 1000 kV D.C. transfer large blocks of power between and within these major areas.

The WSCC area consisting of all four of these areas was formed in 1967 in order to "provide the reliable operation of the interconnected bulk power systems by the coordination of planning and operation of generating and interconnected transmission facilities." The Reliability Criteria of this council accepts "remedial actions" as a course that may be adopted amongst a number of systems. These are pre-planned actions (such as generator dropping) which take place in response to specific disturbances and which are used to avoid uncontrolled loss of firm load following a major disturbance. These disturbances may be for single or multiple contingencies. DSA within PGandE may therefore take place after single or multiple contingency disturbances have taken place on the interconnection and preprogrammed "remedial action" has taken place. It must also anticipate misoperation of preprogrammed stability schemes as another possible contingency.

Two of the major transmission arteries between the Northwest and California-Nevada areas, the 500 kV A.C. Pacific Interties and the 1000 kV D.C. Northwest-Southwest line, have major impacts on the reliability of the PGandE system. The 500 kV A.C. Pacific Intertie is capable of transferring 3200 MW of power approximately 2,000 circuit miles from the Pacific Northwest to California customers. The 1000 kV D.C. line likewise provides the same function transferring 2000 MW between the Pacific Northwest and Southern California. Disturbances associated with these transmission paths are primary contingencies that have to be considered in making DSA decisions.

DSA Decisions

Let us therefore briefly analyze some DSA decisions that are presently made on the PGandE System.

A. **Double Contingency Loss of Both 500 kV A.C. Lines (Malin-Tesla)**

1. Immediate Automatic Action (outside the PGandE Area)
   a. Area islanding
   b. Northwest generator dropping
   c. Application of the 1400 MW braking resistor
   d. Glenn Canyon generator tripping
2. Immediate Automatic Action (within the PGandE Area)
   a. Sense and send Intertie separation signal
   b. Trip 500 kV tie breakers
   c. Underfrequency load shedding
   d. 500/230 kV separation
   e. Selective pump tripping
3. DSA Actions to Return System to Normal
   a. Transfer AGC to "Suspend" conditions (5-10 sec.)
   b. Zero northwest interchange schedules (1 min.)
   c. Return AGC to "Auto" condition (1 min.)
   d. Trip reactors and close capacitors as necessary for voltage control (1-5 min.)
   e. Increase generation to restore frequency to 60 Hz (1-10 min.)
   f. Shed additional load manually if necessary to attain 60 Hz (5-10 min.)
   g. Reestablish 500 kV A.C. ties (5-10 min.)
   h. Close 500/230 kV breakers (5-10 min.)
   i. Reestablish schedules (10-30 min.)

B. **Loss of Single 500 kV A.C. Line (Malin-Tesla)**

1. Immediate Automatic Action (outside the PGandE Area)
   a. Northwest generator dropping
   b. Application of the 1400 MW braking resistor
   c. Suspend AGC control in Northwest area
2. Immediate Automatic Action (within the PGandE Area)
   a. Sense and send "Single Line Outage" signal
   b. Trip selective Feather River Hydro generation for line loss south of Table Mountain
3. **DSA Actions to Return System to Normal**

   Establish new scheduling capability. These have been preestablished based on the next possible contingency and may have a thermal or stability limit. The worst contingency could be loss of the 1000 kV D.C. Intertie after loss of a single 500 kV A.C. line. Some typical limits import limits under these conditions are:

Line	Thermal	Stability
Malin-Round Mtn.	1671	2000
Round Mtn.-Table Mtn.	1443	2000
Table Mtn.-Tesla	2666	2100
Table Mtn.-Vaca	2666	2100
Vaca-Tesla	1475	2400

The lowest value either thermal or stability restricted will then be used. Values are further adjusted depending on major generation changes such as Diablo Canyon Nuclear Unit 1 and/or 2 (1100 MW each), the Helms Pump Storage Facility (1200 MW total) or the Rancho Seco Nuclear Unit (850 MW).

C. **Loss of a Single Pole on the 1000 kV D.C. Line**

1. Immediate Automatic Action (outside the PGandE Area)
   a. Insert high speed capacitors at Bakeover and Fort Rock
   b. Selective tripping of Northwest Industrial load
2. Immediate Automatic Action (within the PGandE Area)

   None at present
3. DSA Action to Return System to Normal
   a. Reduce D.C. schedule by 1/2 (4 sec.-1 min.)
   b. Trip reactors and close capacitors as necessary for voltage control (4 sec.-10 min.)
   c. Increase generation for loss of the D.C. schedule (4 sec.-10 min.)

D. **Loss of 2 Poles on the 1000 kV D.C. Line**

1. Immediate Automatic Action (outside the PGandE Area)
   a. Insert high speed capacitors at Bakeover and Fort Rock
   b. Selective generator tripping (the amount depends on the A.C. flow and the D.C. power level)
   c. Selective tripping of Northwest Industrial load
2. Immediate Automatic Action (within the PGandE Area)

   None
3. DSA Action to Return the System to Normal
   a. Immediately reduce the schedule to 1/2 (4 sec.-1 min.)
   b. After 5 min., reduce the schedule to zero (4-6 min.)
   c. Increase generation for loss of D.C. schedule (4 sec.-10 min.)
   d. Trip reactors and close capacitors as necessary for voltage control (4 sec.-10 min.)

All DSA decisions are presently based on off-line studies performed by Operations and Planning Engineers. Normally, these are conducted seasonally for a pre-set of anticipated contingencies. This approach inherently does introduce inaccuracies in the results obtained since it does not depict actual conditions but "worst case" conditions with the system stressed. The number of contingencies are numerous but only a small portion of the single and multiple contingencies can be investigated.

Future plans call for on-line load flow and stability analysis of possible contingencies. Since our major contingencies are "outside the area," on-line analysis does introduce problems in obtaining an accurate data base for the whole WSCC area. Data exchange between systems will become mandatory as more emphasis is placed on dynamic security analysis to anticipate possible contingencies.

CONCLUSIONS

A brief review of the dynamic security assessment practices and concerns for six power systems in North America have been given. The power networks differ in: size, configuration, and geographical location. The operating practices would be expected to reflect all these factors. Yet, examination of these security practices reveals that the following factors are common to all or most of them:

1. Power System Security is of concern to the system operator (as well as to the system planner).
2. Complex operating problems exist in many North American power systems which are related to dynamic power system behavior.
3. Among the causes of the increased concern with security is the heavy loading of the transmission network (heavy power transfers, inadequate transmission circuits, etc.)
4. Dynamic problems of concern are both stability related and due to voltage collapse/reactive power support.
5. For most systems, it appears that the information provided by off-line studies are not adequate to cover all operation conditions encountered.
6. The need for improved dynamic analysis capability has been repeatedly expressed.
7. For some systems, there is concern for identifying control action to move the system toward secure regimes of operation.

The above concerns may strain the capabilities of existing tools of analysis. Furthermore, they may require more versatile approaches to assessment of the power system security at or near real time.

Discussion

C. Concordia (Consulting Engineer, Venice, FL): I should like first to emphasize that this paper is an excellent summary of the presentations made at the panel session on dynamic security assessment. Thus most of my comments concern the panelists rather than the summarizer.

First, as a general comment, although the session was billed as concerning security *assessment*, a great number of the presentations were devoted to describing how the panelists cope with emergencies (or incidents). This is, of course, of great interest, and in fact I noted that at the New Orleans session. Many, if not most, of the questions were on the details of how to cope, rather than on assessment. Thus attention was diverted from assessment. (In defense of the panelists, it must be noted that questions 2b and 3 of the questions to be addressed concern coping and not assessment per se). Some more detailed comments are

1) In the introduction, first paragraph, it is stated that a requirement for security is that following a disturbance the system will operate within "established limits." Perhaps it should be pointed out that these limits are not necessarily the normal limits.

2) In the third paragraph, mention is made of security packages now available for static security assessment. This brings to mind the even older practice of using simply fixed (or perhaps only manually varied) limits of loading, voltage, etc., but with these limits established not by rules-of-thumb but by previous off-line studies, including transient-stability studies. Is this then static security assessment, dynamic security assessment, or neither?

3) To be more specific about my first general comment, I should like to except from that comment the presentations by Ontario Hydro and NYPP, which kept very well to the subject of assessment.

4) The MSU presentation seemed to me to be about *static* security assessment with no mention of *dynamic* security assessment.

As a final remark on the subject of system security, it is very depressing to observe, not only here, but also in many other papers nowadays, the casual way in which load shedding is used. We used to regard the objective of corrective means to be saving the load. Load shedding was only used as a last resort, when the frequency fell. Now it is often being used on low voltage (where it is sometimes inappropriate) and on certain switching operations, that might result in islanding or low voltage, as well. The need for such signals arises from an inadequate transmission network, and unfortunately, with the increasing difficulties of installing new generating equipment, power systems are becoming more and more dependent on interarea transfers. Connections must be made, not to improve reliability, but to import power and energy from afar, often with some *decrease* in reliability as compared to local generation.

Manuscript received July 23, 1987.

James A. Larson (Northern States Power Co., Minneapolis, MN): The Operational Planning department at Northern States Power has the duty to provide the system operators with graphs that clearly show the safe operating limits to be followed. We have found it impossible to do enough off-line simulations to provide stability guides for all possible operating conditions. Six (or more) major system condition variables affect our transient stability. Because six variables are being considered, it is clearly impossible to study in detail all possible combinations off-line in advance. (And if we did, the control center would be stacked floor-to-ceiling with guides). But we must still be prepared with guides for the unexpected operating situations which frequently come up, such as the sudden tripping of a 345-kV line. When that happens, we clearly cannot then do dozens of full-detailed stability simulations for that situation. By the time we have completed the simulations and produced a guide, the line would be back in service.

Therefore, we are looking for methods that will help us do stability simulations quickly, and to wring the most information possible out of a limited amount of stability simulations. To do the latter, we are investigating the use of regression equations to describe stability limits. We hope to learn in more detail how the authors deal with sudden unexpected operating conditions.

To more clearly illustrate the nature of our stability assessment problem, Fig. 1 is an example of one of our operating guides. For 1) the current major lines out, 2) amount of East Side capacity on line, and 3) var operation mode, this graph shows the stable/unstable operating regions as a function of 4), West Side generation, 5) Twin Cities Exports, and 6) dc line flow.

Such a graphical aid is needed in order for our system operator to know when the system is operating near or in an unstable operating region (if subjected to a severe fault), and to determine what action must be taken to get back to, or stay in a stable operating region. These guides indicate where we are headed as the day progresses, for example, as the load and generation increases, or if it is all right to take a certain EHV line out.

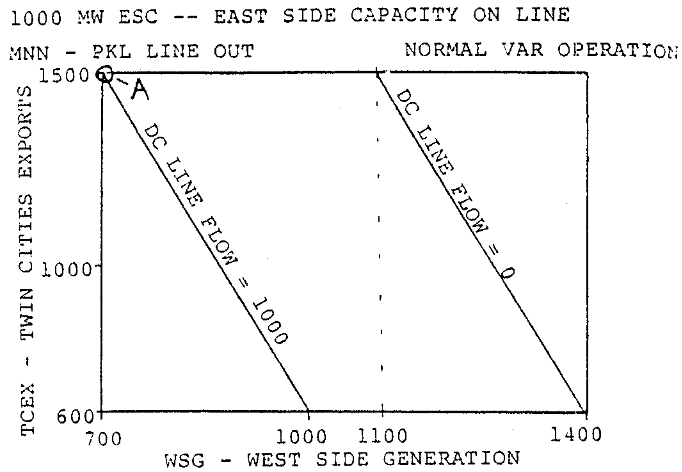


Fig. 1. Operating guide—threshold of stability limits for 1000 MW ESC. WSG = 1300 + 0.3 ESC − 0.4 DC − 0.333 TCEX.

The *ideal* solution to assessing stability is a very fast stability master program running on our energy management system (EMS) computer. Here it would run a worst-fault(s) stability simulation(s) on the real-time model. If the real system is found to be near or beyond safe stability limits, it would then vary modeled system conditions. It would run stability simulations on these different conditions in order to produce operating guides. And a special security dispatch program would find the most economic way to get within, or stay within, the operating limits.

Any fast stability software must accurately calculate system voltages and certain other critical system parameters such as the impedance seen by a relay. Specifically, on our system, the critical transient performance parameter is the Prairie Island nuclear plant voltage. Also, such software must be able to simulate a voltage collapse. We feel a voltage collapse occurs before angular stability is lost on our system.

As for our near-term realistic plan for assessing stability, we know of no stability program, fast or slow, that runs on our EMS Cyber computer. Therefore we occasionally plan to transfer the real-time model from the EMS to the PRIME computer, where our stability program resides.

We plan to produce operating guides by a regression process. As the first step to producing guides, we expect to do off-line stability simulations on a wide range of modeled system conditions. The results of these stability simulations will be used to produce regression equations. These equations describe threshold of stability limits as a function of variables that significantly impact stability. I think of the regression equation as describing the *sensitivity* of stability to these variables. Graphical operating guides would then be produced from this regression equation. The Offset and other terms of the regression equation can be adjusted by one, a few, or several stability simulations made on the real-time model. The regression equations and operating guides would then match current system conditions much more closely than equations and guides produced strictly from off-line studies.

Our EMS will monitor generation and interchange parameters that are important to stability. These parameters will automatically and periodically be plugged into the regression equation. A measure of how close we are to instability will then be calculated from this equation and parameters, and displayed. An alarm will be generated if the system is close to instability.

A more detailed discussion of using regression equations in stability is available on request. Note that using regression equations to describe a system variable as a function of other variables is not new. Stone and Webster and NSP have successfully used regression equations, based on multiple load flow runs, to describe losses as a function of load and Twin Cities exports.

Manuscript received July 29, 1987.

A. A. Fouad: On behalf of the Working Group and the panelists, I would like to thank the discussers for their comments.

Mr. Concordia's remarks about the differences between coping with emergencies and assessment of their impact are very interesting. As is often the case, Mr. Concordia's remarks will help clarify the issues related to dynamic security assessment and will be helpful to the Working Group in dealing with them. I wish also to add that if, in reviewing the industry's security practices, adequate differentiation between coping and assessment is sometimes overlooked, it is significant in itself.

In response to some of Mr. Concordia's specific comments, I wish to point out that established limits are not necessarily the normal limits, and that the terms static and dynamic security are used to refer to whether they deal with steady-state or dynamic system performance. The readers, as well as the Working Group members, will find Mr. Concordia's views on load shedding very interesting and enlightening.

Mr. Larson's discussion gives an excellent illustration of the type of problems which have increased the industry's awareness of dynamic security assessment, and of the need for new tools to deal with it. All too often we hear that current or conventional tools to obtain secure operating regimes may no longer be adequate to provide the answers needed in the desired time frame. The discusser's information on Northern States Power Co.'s proposed regression procedure is much appreciated. Many engineers in operations planning are facing similar operating decisions with stability-limited operating constraints. They will look to NSP's experience with this procedure with considerable interest.

Again, I wish to thank the discusser for their valuable comments.

Manuscript received September 8, 1987.