On-Line Power System Security Analysis

NEAL BALU, SENIOR MEMBER, IEEE, TIMOTHY BERTRAM, ASSOCIATE MEMBER, IEEE, ANJAN BOSE, FELLOW, IEEE, VLADIMIR BRANDWAJN, SENIOR MEMBER, IEEE, GERRY CAULEY, SENIOR MEMBER, IEEE, DAVID CURTICE, SENIOR MEMBER, IEEE, AZIZ FOUAD, FELLOW, IEEE, LESTER FINK, LIFE FELLOW, IEEE, MARK G. LAUBY, SENIOR MEMBER, IEEE, BRUCE F. WOLLENBERG, FELLOW, IEEE, AND JOSEPH N. WRUBEL, SENIOR MEMBER, IEEE

Invited Paper

A broad overview of on-line power system security analysis is provided, with the intent of identifying areas needing additional research and development. Current approaches to state estimation are reviewed and areas needing improvement, such as external system modeling, are discussed. On-line contingency selection has become practical, particularly for static security. Additional work is necessary to identify better indices of power system stress to be used in on-line screening filters for both static and dynamic security analysis.

Use of optimal power flow schemes to recommend optimal preventive and corrective strategies is presented on a conceptual level. Techniques must be further developed to provide more practical contingency action plans, which include real-world operating considerations and use a reasonably small number of control actions. Techniques must be developed for costing operating variables which are not easily quantified in dollars. Soft or flexible constraints and time variables must be included in the preventive and corrective strategy formulation.

Finally, the area of on-line transient and dynamic security analysis is presented. Methods are being investigated to speed up for on-line application existing analysis techniques currently used in an off-line planning mode. Transient energy function (direct) methods, expert systems and neural networks, fast approximate contingency screens, and parallel processing may also have significant roles in this area.

DEFINITIONS

Secure — (Dictionary) adj. Free from or not exposed to danger; safe.

Security — 1) freedom from danger, risk, etc.; safety. 2) Freedom from care, apprehension, or doubt; confidence. 3) Overconfidence

Security — (Power Systems) an instantaneous, time-varying condition reflecting the robustness of the system relative to imminent disturbances; the complement of the risk of disruption of unimpaired system performance.

Security Monitoring — The on-line measurement of system and environmental variables that affect system security; provides base case conditions for analysis of the effects of contingencies (security assessment).

Security Assessment — The evaluation of data, provided by security monitoring, to estimate the relative robustness (security level) of the system in its present state (i.e. determination of whether the system is in the Normal or Alert operating state).

Security Enhancement — Specific operations taken on-line to improve system robustness, ie. to raise the performance level of system security. Includes or is also referred to variously in the literature as security dispatch, security control, corrective rescheduling, preventive action, etc.

Manuscript received August 27, 1990; revised October 4, 1991.

N. J. Balu, G. Cauley, and M. G. Lauby are with the Electrical Systems Division, Electric Power Research Institute (EPRI), Palo Alto, CA 94304.

T. Bertram is with the Power System Security and Optimazation, Bertram, Inc., Seattle, WA 98103-0067.

A. Bose is with the Department of Electrical Engineering, Arizona State University, Tempe, AZ 85287.

V. Brandwajn is with Systems Control, ABB Power Automation, Palo Alto, CA 94304.

D. Curtice is at 542 Live Oak Lane, Redwood City, CA 94062.

A. Fouad is with the Department of Electrical Engineering, University of Iowa, Cooper Hall, Ames, IA 50011.

L. H. Fink is with the Energy & Control Consultants, Fairfax, VA 22033-3899.

B. F. Wollenberg is with the University of Minnesota, Minneapolis, MN 55455.

J. N. Wrubel is with System Reliability, Public Service Electric & Gas Company, Newark, NJ 07101.

IEEE Log Number 9106713.

0018–9219/92$03.00 © 1992 IEEE

Security Control In view of the accepted meaning of the term "control," it seems best to reserve this as an umbrella term comprising security monitoring, assessment and enhancement.

Emergency Control Control taken after one or more operating constraints have been violated in order to return the system to the normal (or at least to the alert) state. May include or be referred to as remedial action, determined in advance relative to one or more possible contingencies for which security enhancement is not feasible.

VAR Reactive volt-ampere, the unit of reactive power, corresponding to the active power unit, watts. VAR's by convention, are "supplied" by capa-citive loads and "consumed" by inductive loads but actually they are a measure of the flow of reactive power being interchanged between electrostatic and magnetic fields each cycle (60th of a second). The two must always be in balance and the balance is maintained by fluctuations in voltage levels; a low voltage indicates a local shortage of VAR's.

I. Introduction

A. What is Security?

Security is freedom from risk or danger. Power systems, however, can never be secure in this absolute sense. Accordingly, in a power system context, security can only be a qualified absence of risk, specifically of risk of disruption of continued system operation.

In practice, to avoid confusion, security has been defined in terms of how it is monitored or measured. Thus security has come to mean the ability of a system to withstand without serious consequences any one of a preselected list of "credible" disturbances ("contingencies"). Defined in this way, "security" becomes a sometimes misleading label based on an arbitrary classification procedure. More appropriately, one may think of insecurity as the level of risk at any point in time of disruption of a system's continued operation.

From a control perspective, the objective of power system operation is to keep the electrical flows and bus voltage magnitudes and angles within acceptable limits (in a viable region of the state space), despite changes in load or available resources. From this perspective, security may be defined as the probability of the system's operating point remaining in a viable state space, given the probabilities of changes in the system (contingencies) and its environment (weather, customer demands, etc.).

B. Why is Security an Issue?

There is one factor in the functioning of electric energy systems that is so basic as to be taken for granted, usually escaping the notice even of engineers from other fields. This basic factor is that operation of the collective power systems covering most of North America, as of those elsewhere, requires nearly strict synchronism in the rotational speed of many thousands of large interconnected generating units, even as they are controlled to continuously follow significant changes in customer demand. The rotational energy involved is considerable. The consequences of any cascading loss of synchronism among major system elements or subsystems can be catastrophic.

The design of equipment and of interconnected power systems that make possible such synchronized operation in an almost routine ongoing manner is an engineering achievement that is not generally appreciated by those who are not directly involved. Such operation requires, not just proper functioning of machine governors, but that operating demands on all equipment remain within physical capabilities, regardless of changes in customer demand or sudden disconnection of equipment from the system.

Obviously, because of the intimate role that electric energy plays in the national economy, secure and reliable operation of the nation's electric energy infrastructure is crucially important. It is the interconnection of systems, for reasons of economy and of improved availability of supplies across broader areas, that makes widespread disruptions possible. Without interconnection, small individual systems would be individually more at risk, but widespread disruptions would not be possible. We have passed the quarter-century anniversary of the 1965 northeast blackout, and the effects of any such event today could only be more severe. Although significant improvements have been made, such as load shedding schemes, the risk of cascading outages still exist.

The risk entailed in interconnected operation has been and is being aggravated by a variety of circumstances. The mid-seventies oil embargo, causing wide swings in the costs of fuels resulted in significant disruptions of the geographic patterns of generation relative to load. This has resulted in transmission of electric energy over longer distances in patterns other than those for which the transmission networks had been originally designed. At the same time, rising costs due to inflation and increasing environmental concerns inhibited any relief through further transmission construction. Therefore, transmission, as well as generation, must be operated closer to design limits, with smaller safety (security) margins and greater exposure to unsatisfactory results following disturbances. More recently, relaxation of energy regulation to permit sales of electric energy by independent power producers, together with increasing pressure for essentially uncontrolled access to the bulk power transmission network, threatens to erode further traditional levels of system security.

This current situation means that our understanding of the nature of and conditions for security must be explored and strengthened in order that the historic level of reliable electric energy supply in this country can be can be maintained under new, unprecedented conditions and requirements.

II. Background

A. Evolution of the Concept of Security

In the history of the electric utility industry, security as it is understood today is a relatively recent concept. Through the first two-thirds of this century, the system operator's major "security" concerns (although that term was not used) were to make sure that sufficient spinning reserve was on line to cover unforecasted load increases or potential loss of a generator and to check the potential effects of removing a line or other piece of equipment for maintenance. "Chasing VAR's around the system" to maintain a desirable voltage profile was his spare-time responsibility. During that period, security was subsumed under reliability, and was assured in the system planning process by providing a robust system that could ride out any "credible" disturbances without serious disruption. Perhaps the epitome of this approach was the midcentury American Electric Power (AEP) system, which, in 1974, rode out five simultaneous major tornadoes, losing 11 345-kV lines, one 500-kV line, two 765-kV lines, and three major switching stations, without interruption of service to customers [1]. This earlier approach is no longer economically feasible.

The problem of security as it pertains today emerged in the wake of the 1965 northeast blackout. Possibly the first mention in the literature of "security" in its present sense was in the *Proceedings of The Second Power System Computation Conference* in 1966 [2]. The most significant early paper, however, is that of DyLiacco on "adaptive reliability" [3]. In this paper, the concept of system operating states is defined. The problem of security monitoring, is introduced as that of monitoring, through contingency analysis, the conditional transition of the system into an emergency state.

The shift of focus in the concept of security from that of system robustness designed into the system at the planning stage, which is an element of reliability, to that of risk aversion, which is a matter operators must deal with in real time as a function of the system's environment, has led to some continuing ambiguity and even confusion of the roles of security assessment in the two environments. System planning is concerned with security as a factor on reliability. To the planner, security is an abstract concept in the sense that the planner is removed from the time-varying real world environment within which the system will ultimately function. When used in this sense, the term "security" refers to those aspects of reliability analysis that deal with the ability of the system, as it is expected to be constituted at some future point in time, to withstand unexpected losses of certain system components. For instance, the widely quoted NERC definition [4] defines reliability as comprising two components, adequacy and security. Adequacy is the ability to supply energy to satisfy load demand. Security is the ability to withstand sudden disturbances.

What is overlooked in such an approach is that even the most reliable of systems will inevitably experience periods of severe insecurity from the operators perspective. System operations is concerned with security as it is constituted at the moment, with a miscellaneous variety of elements out for maintenance, repair, etc., and exposed to environmental conditions that may be very different from the implicitly normal conditions considered in system planning. In operations, systems nearly always have less than their full complement of equipment in service. As a consequence, an operator must often improvise to improve security in ways that are outside the purview of planners.

B. What is Security Assessment?

Security assessment is analysis performed to determine whether, and to what extent, a power system is "reasonably" safe from serious interference to its operation. Thus security assessment involves the evaluation of available data to estimate the relative robustness (security level) of the system in its present state or some near-term future state. The form that such assessment takes will be a function of what types of data are available and of what underlying formulation of the security problem has been adopted.

Two alternative approaches to the security assessment problem may be distinguished—direct and indirect. The direct approach attempts to estimate the likelihood of the system operating point entering the emergency state. The indirect approach tracks a variety of reserve margins relative to predetermined levels deemed adequate to maintain system robustness *vis-a-vis* preselected potential disturbances.

Direct security assessment requires calculating the probability that the power system state will move from the normal operation state to the emergency state, conditioned on its current state, projected load variations, and ambient conditions. A formalization of this approach has been presented by Blankenship and Fink [5]. An alternative direct approach, formulated in terms of estimates of the probability distribution of time to insecurity, has been developed by Wu *et al* [6], [7].

The common practice of assessing security by means of analysis of a fixed set of contingencies and classifying the system as insecure if any member of the set would result in transition to the emergency state, is a limiting form of direct assessment, because it implies a probability of one of the system's being in the emergency state conditioned on the occurrence of any of the defined contingencies.

An indirect method of security assessment can be formulated by defining a set of system "security" variables that should be maintained with predefined limits to provide adequate reserve margins. This was the method that was generally followed during mid-century, when operators primarily monitored their spinning reserve level. In today's environment, appropriate variables might include, in addition to MW reserves, equipment (line, transformer, etc.), emergency ratings or VAR reserves within defined regions, etc. The reserve margins that should be maintained for each of the security variables could be determined by offline studies for an appropriate variety of conditions with due consideration to the degree to which random events can change the security level of a system, for better or worse, in real time. Security assessment then would consist of tracking all such reserve margins relative to system conditions. An example of an element of such an approach is provided by Consolidated Edison Company's monitoring of their VAR reserves [8].

Because early concerns in security were with potential postcontingency line overloads and because line MW loadings can be studied effectively by means of a linear system network model, it was possible to study the effects of contingencies by means of linear participation or distribution factors [9]. Once derived for a given system configuration, they could be applied without further power flow analysis to determine post-contingency line loadings even, by superposition, for multiple contingencies. Such a computationally simple method of analysis made on-line contingency assessment practicable for "thermal security," where reactive flows were not of concern.

It is only in the recent past that postcontingency voltage behavior has become a prominent element in security assessment. Assessment of "voltage security" is not straightforward, not so much because of the computational burden as because voltage dynamics on stressed systems are not yet fully understood. There has been a great deal of discussion over the past several years as to whether voltage collapse is basically a steady state or a dynamic phenomena, i.e., whether or not it can be studied effectively by means of static load flow analysis. It is now becoming clear as a result of recent research that the behavior of a system undergoing voltage collapse cannot be completely explained on the basis of static analysis.

The current practice of security assessment via analysis of the potential effects of a predetermined set of credible disturbances not only narrows its range, but also ignores the pervasive effects of uncertainty. All security assessment operates with confidence limits, whether or not they are recognized and acknowledged [10]. It is prudent to get as good a handle as possible on these confidence limits. This requires that uncertainties be estimated as closely as possible, and that calculations be made accordingly. Incorporation of uncertainties would require some changes in present practice.

C. What are the Implications of Security?

Concern with system security as an operating problem is a consequence of recognizing that the globally robust power systems of the past are no longer economically or environmentally feasible. Requirements of active security control have been traded off against the costs of such robust systems. It is important to recognize that this trade-off may, but does not necessarily entail, a decrease in reliability. It does, however, entail an increase in the responsibilities of the system operator. Accordingly, it imposes responsibilities on system management for operator training and for development and provision of tools that will enable the operator to function effectively in his new environment and to fulfill his new responsibilities. Any failure in meeting requirements for operator training tools will necessarily result in decreased system security.

III. On-Line Security Analysis

A. Security Analysis

There are three basic elements of on-line security analysis and control, namely, monitoring, assessment and control. They are tied together in the following framework:

Step 1) *Security Monitoring:* Using real-time system measurements, identify whether the system is in the normal state or not. If the system is in an emergency state, go to step 4). If load has been lost, go to step 5).

Step 2) *Security Assessment:* If the system is in the normal state, determine whether the system is secure or insecure with respect to a set of next contingencies.

Step 3) *Security Enhancement:* If insecure, i.e., there is at least one contingency which can cause an emergency, determine what action should be taken to make the system secure through preventive actions.

Step 4) *Emergency Control:* Execute proper corrective action to bring the system back to the normal state following a contingency which causes the system to enter an emergency state. This is sometimes called remedial action.

Step 5) *Restorative Control:* Restore service to system loads.

Security analysis and control have been implemented through a number of software packages in modern energy control centers. The major components of on-line security analysis are shown in Fig. 1. The monitoring component starts with the real-time measurements of physical quantities such as line power flows, line current flows, power injections, and bus voltage magnitudes; as well as, the status of breakers and switches. The measurement data are telemetered from various locations to the control center computer. Bad measurement data are rejected by filtering the transmitted data through a simple check of their reasonability and consistency. The remaining data are first systematically processed to determine the system configuration (generator and transmission network connections) or network topology. Then the available data are further processed to obtain an estimate of the system state variables (bus voltage magnitudes and phase angles for normal steady-state). State estimation is a mathematical procedure for computing the "best" estimate of the state variables of the power system based on the available data, which are in general corrupted with errors. Prior to state estimation, one would like to know: 1) whether state estimation of the

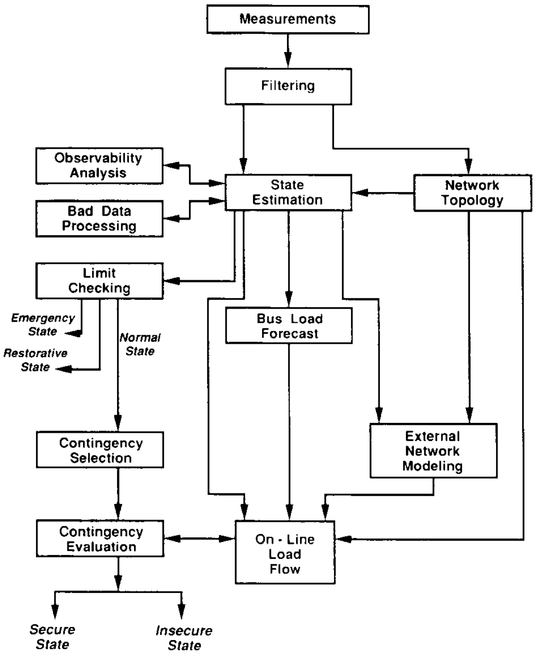

Fig. 1. Major components of on-line security analysis.

system is possible (enough of the network is observable); and 2) if not, for which part of the system state estimation is still possible. One would also like to know whether there is any bad data present, and if so, which data is bad and should be discarded. The observability analysis and bad data detection and identification are parts of the state estimation.

To assess whether a normal operating state is secure or not, a set of contingencies is needed. The contingency selection process employs a scheme to select a set of important and plausible disturbances. Security assessment currently involves primarily steady-state load flow analysis. Stability constraints are expressed in terms of the limits on line flows and bus voltages. Therefore, to assess the system response to contingencies, a contingency evaluation is carried out using the on-line load flows. The on-line load flow uses the actual load flow model of one's own system (from the state estimation solution) together with a system representation of the unmonitored network and neighboring systems, i.e., an external network model. Because the contingencies are future events, a bus load forecast is needed. Certain implementations of the state estimator render the external model observable by strategic placement of pseudo-measurements. Then the state estimate is performed on the entire model in one step.

B. State Estimation

There are three types of real-time measurements: 1) the analog measurements that include real and reactive power flows through transmission lines, real and reactive power injections (generation or demand at buses), and bus voltage magnitudes; 2) the logic measurements that consist of the status of switches, transformer LTC positions, and breakers, and 3) the pseudo-measurements that may include forecasted bus loads and generation. Analog and logic measurements are telemetered to the control center. Errors and noise may be contained in the data. The sources of data errors include: failures in measuring or telemetry equipment, errors in the measuring instrumentation, noise in the communication system, delays in the transmission of data, etc.

State estimation is a mathematical procedure for computing the best estimate of the state variables (bus voltages and angles) of the power system based on the noisy data. Once state variables are estimated, other quantities (e.g., line flows) can readily be obtained. The network topology module processes the logic measurements to determine the network configuration. The state estimator processes the set of analog measurements to determine the system state; it also uses data such as the network configuration supplied by the network topology, network parameters such as line impedances, and, perhaps, pseudo-measurements. The network parameters may introduce another source of error, as it is impractical to make extensive measurements of these parameters in the field. Often, manufacturers data and one line drawings are used to determine parameter values. Error reduction in state estimation measurements and model parameters is an area requiring further work.

C. Observability

As mentioned earlier, if the set of measurements is sufficient in number and well-distributed geographically, the state estimation will give an estimate of the system state (i.e., the state estimation equations are solvable). In this case we say the network is observable. Observability depends on the number of measurements available and their geographic distribution. Usually a system is designed to be observable for most operating conditions. Temporary unobservability may still occur due to unanticipated network topology changes or failures in the telecommunication systems. The following questions emerge naturally in connection with state estimation in system operation:

1) Are there enough real-time measurements to make state estimation possible?
2) If not, where should additional meters be placed so that state estimation is possible?
3) How are the states of these observable islands estimated?
4) How are additional pseudo-measurements to be included in the measurement set to make state estimation possible?
5) How can one guarantee that the inclusion of the additional pseudo-measurements will not contaminate the result of the state estimation?

The analysis which leads to answers to these questions is called observability analysis. It includes observability testing, identification of observable islands, and measurement placement. It should be performed prior to the state estimation.

D. Bad Data Detection and Identification

State estimation processes a given set of measurements to give the best estimate of the state of the system. It is formulated as a weighted least square error problem. Implicitly assumed in the formulation is that the errors are small. Occasionally, large errors or bad data do occur due to meter failure or other reasons. It is very important 1) to detect the presence of any such bad data; 2) to identify which measurements are bad; and 3) to remove all bad data so that they do not corrupt the result of state estimation. As a matter of fact, one of the major benefits of state estimation so far in practice has been the identification of bad data in the system.

Intuitively, if bad data or structural error is present, the residual (the Weighted Least Square error) will be large. This suggests a way of detecting bad data. Rigorous analysis using statistical techniques of hypothesis testing can be used to determine when the residual or the error is too large. Hypothesis testing using "normalized" residuals is found to be reliable for the detection of bad data. However, the larger error can also be caused by a switch indicating other than its true position. In this case, a valid analog reading is discarded.

E. Benefits of Implementing a State Estimator

Implementation of a state estimator is a difficult and time consuming process. However, once accomplished, the company or pool control center personnel have correctly established the following data:

- the correct impedance data for all modeled facilities;
- the correct fixed tap position for all transformers in the modeled network;
- the correct load tap changing information for all modeled Load Tap Changing (LTC) transformers;
- the correct polarity of all MW and MVAR flow meters.

The correct impedance data for all modeled facilities might seem to the casual observer to be information which should be readily available from the system planners of any given power system. However, experience has shown that between the time a facility is planned and placed in service, distances for transmission lines change due to right-of-way realignment, or the assumed conductor configuration is changed, or the conductor selected is not as assumed, etc. The net result is that the system planner's impedances may be up to 10% off from the as-built. The problem is that the system planners may not catch up to this discrepancy for years. While it may not be crucial to the planning function, a state estimator will recognize that the impedance data is inconsistent with the flow data and it will "grumble." The worst part of this problem is that it doesn't grumble in any language engineers understand. The state estimator generally assumes the metered data is wrong, not impedance data.

In the ongoing use of a fully implemented state estimator, bad meters are detected as they go bad. The implication is that if meters are corrected as they are detected to be bad, a high degree of confidence is established in the entire active meter set. This means that when an unusual event occurs on the power system, the active meter set can be believed before the power system security process has been rerun. This provides time savings to the system operators when they need it most.

F. External Network Modeling

Power systems are interconnected. An energy control center for a member system of the interconnection is responsible for the control of a part of the interconnected system. The control center receives telemetered data of real-time measurements. The monitored part of the power system covered by these measurements normally consists of one's own system; we call it the internal system. The system is connected to neighboring systems; we call that the external system. Any unmonitored portions of the internal system such as lower voltages networks or unmonitored substations, must also be incorporated in the "external" mode.

Using a state estimator, it is not necessary to know more about the external system for the purpose of determining the present situation of the internal system. To evaluate the consequence of various contingencies for security assessment, however, the response of the external system needs to be included. An external model may be constructed either on-line or off-line, or a combination of both. Because from the state estimation, we have the load flow solution of the internal system at the present time (we shall refer to this case without contingency as the base case), we require that the solution of the load flow model consisting of the internal system plus the external model for the base case be the same as the one obtained from the state estimation. This is accomplished by the so-called boundary matching as described in the following:

- From the state estimation, calculate the flows from the boundary buses into the internal system.
- Use the external model together with the complex voltages of the boundary buses from the state estimation to compute the flows from the external network into the boundary buses.
- For each boundary bus add power injections so that the flows into and out of the bus are balanced.

After boundary matching, the adjusted external model (the original external model plus the boundary injections) is attached to the internal system as the load flow model for evaluation of internal system response of contingencies.

During contingency analysis, the external system may be represented by an unreduced or a reduced load flow model, or a combination of both. A reduced load flow model of the external system is called an external equivalent.

One of the modeling decisions which must be made is where to eliminate or put into equivalent form portions of the underlying transmission or subtransmission system for which there is no direct telemetry. One rule of thumb in use is to eliminate the underlying network if its most direct through-path directly paralleling a modeled transmission path is ten times or more the impedance of the modeled path. Another consideration is whether or not the step-down transformers to the underlying system are to be monitored. If they are, the underlying system must be at least modeled as an equivalent path.

The issue of obtaining data for state estimation from neighboring systems is still a difficult one. One question that arises is how much of the neighboring systems need to be measured for satisfactory performance of the state estimator. Data exchange between utilities is often a difficult and sensitive issue.

IV. Contingency Analysis

A. *Definition of Contingency Analysis*

Contingency analysis is a software application run in an energy management system to give the operators an indication of what might happen to the power system in the event of an unplanned (or unscheduled) equipment outage. That is, the contingency analysis application allows the operator to ask "what if" questions such as: "What will be the state of the system if we have an outage on part of our major 500-kV transmission system?" The answer to this question might be that the system power flows and voltages will readjust and remain within acceptable operating limits, or the answer might be that severe overloads and undervoltages will occur such that the system's very survival is in question should the outage occur.

An overload itself can damage transmission and generation equipment if it is severe enough and if it persists long enough. However, virtually all equipment in a power system is protected against a fault with fast-acting relays. Therefore, an overload which persists long enough on a piece of transmission or generating equipment usually results in its being switched out once it fails. However, the outage of the second piece of equipment due to relay action often results in yet more readjustment of power flows and bus voltages that can in turn cause more overloads and cause further removals of equipment, etc. This can cause an uncontrollable cascading series of overloads and equipment removals resulting in shutting down a large part of the system.

The use of a contingency analysis application in an energy management system is predicated upon the idea that when forewarned, the operator can take some action before or after the event that will help the system avoid problems should an outage occur. As such, its economic justification comes from the electric utility's desire to avoid overloads that might directly damage equipment, or worse, might cause the system to lose a number of components due to relay action and then cause widespread power outages to customers.

Typical contingencies on a power system consist of outages such as loss of generating units or transmission components (transmission lines, transformers, substation buses, or pieces of switch gear). In addition, contingencies can result in short circuits on the system that persist until the affected equipment is removed by relay action. Contingencies can occur in the form of single equipment outages or in the form of multiple outages when taking relay actions into account. That is, relays may be set to automatically take out a number of components when one component is faulted and in this case the contingency definition itself must include all such components.

The causes of equipment removal and short circuits can be classified as internal or external. Internal causes arise from phenomena such as insulation breakdown, over temperature relay action or simply incorrect operation of relay devices. The external causes result from some environmental effects such as lightning, high winds and ice conditions or else are related to various nonweather related events such as vehicle or aircraft coming into contact with equipment, or even human or animal direct contact. All of these causes are treated as unscheduled, random events which the operators do not expect to occur, but for which the operators must be prepared.

The system planners who design the power system transmission and generation systems keep statistics on these events and use them in reliability evaluations of new designs to meet reliability criteria established by regional reliability councils within North America. To achieve reliability, planners add redundant circuits or adjust the design whenever possible to reduce the possibility of interruption to customer load due to an unscheduled event.

The fact that the power system is designed to account for outages does not mean power system operators can passively assume the system will withstand all such events. There is, as already pointed out, a great difference between the system planners design and the actual system the operations department must use to generate and deliver power. Construction can be delayed or denied by regulatory agencies, load patterns can shift in unforeseen ways or generator outages can necessitate purchasing power and transmitting it over long distances. The result is a situation wherein operators must play an active role in maintaining the system security.

The first step in this active role is to run a contingency analysis application program at frequent enough time intervals to guarantee that system conditions have not changed significantly from the last execution. The output of the contingency analysis is a series of warnings or alarms to the operators stating something like this:

ALARM: Loss of component XYZ will result
in an overload of X% on line ABC.

To achieve an accurate picture of the system's vulnerability to outage events several issues need to be addressed:

A) *System model:* Contingency analysis is carried out using a steady-state or power flow model of the power system. If stability is to be assessed as well, then additional information concerning the dynamic aspects of the system needs to be added (this is discussed later). Included in the considerations when building the model are what voltages to include (i.e., whether to include low voltage equipment or not) and what geographic extent the model is to encompass. The usual practice today is to include all voltages that have any possibility of connecting circuits in parallel with the high voltage system while leaving out those that are radial to it such as distribution networks. The geographical extent is harder to determine, but common practice is to model the system to the extent real-time measurement data is available to support the model.

B) *Contingency Definition:* Each contingency to be modeled must be specified separately. The simplest form of contingency definition is to name a single component. This implies that when the model of the system is set up, this contingency will be modeled by removing the single component specified. How the component outage is specified is also an important consideration. The component can be specified by name, such as a transmission line name, or more accurately, a list of circuit breakers can be specified as needing to be operated to correctly model the outage of the component. Contingencies that require more than one component to be taken out together must be defined as well. Here there is an advantage to the "list of breakers" method in that the list is simply expanded to include all breakers necessary to remove all relevant equipment.

C) *Double Contingencies:* A double contingency is defined as the overlapping occurrence of two independent contingent events. More precisely, one outside event causes an outage and while this outage is still in effect, a second totally independent event causes another piece of equipment to be taken out. The overlap of the two outages often causes overloads and undervoltages that would not occur if either happened separately. Therefore, many operating groups require that a contingency analysis program be able to handle double contingencies. That is, the programs must be able to take two independent contingencies and model them as if they had happened in an overlapping manner.

D) *Contingency List:* Usually contingency analysis programs are constructed to run off of a list of valid contingencies. Part of the technical difficulty involved in creating a contingency analysis program that functions usefully can be seen when such a list is compiled. To begin, the list might consist of all single component equipment outages including all transmission lines, transformers substation buses, and all generator units. For a large interconnected power system (for example one that would need several thousand electrical buses to model) just this list alone could result in over 5000 contingency events to be tested. Worst yet, if the operators wished to model double contingencies, the number becomes millions of possible events. Methods of selecting a limited set of priority contingencies are discussed later.

E) *Performance:* How fast should the contingency analysis application program execute? Generally, utility operators wish to have results from a contingency analysis program in the order of a few minutes up to fifteen minutes. Anything longer means that the analysis is running on a system model that was updated too long ago for the results to be reliable.

F) *Modeling Detail:* The detail desired by most utility operating engineers for a contingency case is usually the same as that used in a study power flow. That is, each contingency case requires a fully converged power flow that correctly models each generator's VAR limits and each tap adjusting transformer's control of voltage. Some utilities go so far as to include the modeling of controlled capacitors that regulate voltage.

B. Historical Methods of Contingency Analysis

Contingency analysis is difficult because of the conflict between the accuracy with which the power system is modeled and the speed required to model all the contingencies that the operator specifies. If the contingencies can be evaluated fast enough, then all cases specified on the contingency list are run periodically and alarms reported to the operators. This is possible if the calculation for each outage case can be performed very fast or else the number of contingencies to be run is very small.

With modern energy management systems the number of contingency cases to be solved is usually a few hundred to a few thousand cases. This coupled with the fact that the results are to be as accurate as if run with a full power flow program make the execution of a contingency analysis program within an acceptable time frame extremely difficult.

C. Selection of Contingencies to be Studied

If a power system network has serious reactive flow or voltage problems a full power flow solution must be used to solve for the resulting flows and voltages when an outage occurs. If the power system is large and the number of contingency cases is large the operators will not be able to get results soon enough.

One way to speed up the process of contingency analysis is to note that most outages do not cause overloads or undervoltages. Therefore, a significant speed increase could be obtained by simply studying only the important cases.

1) Fixed List: Many operators claim to know the outage cases that are important to their system and they can get along running them alone. In this way, they must choose the cases based on intuition and experience and then build a list of these cases for the contingency analysis program to use. This is acceptable to many operators but they are still left with the possibility that one of the cases they have assumed would be safe, may in fact present a problem because some of the operators assumptions used in making the list are no longer true.

2) Indirect Methods (Sensitivity Based Ranking Methods): Another way to use a reduced list of cases to be studied is to have a calculation that would indicate the possible bad cases and run it as often as the contingency analysis itself is run. Thus the list of cases is dynamically built and the cases that are included in the list may change as conditions on the power system change.

To do this requires a fast approximate evaluation to discover those outage cases that might indeed present a real problem and require further detailed evaluation by a full power flow.

The first attempt at solving this problem came in the form of a sensitivity method based on the concept of a network performance index. The idea is to calculate a scalar index that reflects the loading on the entire system.

The only other approaches to obtaining a global look at the power system network are those based on pattern recognition or neural networks. The base condition is passed into the neural network to see if the conditions are "close" to those studied before. If so, the case is then flagged. These methods suffer from the fact that training the pattern recognizer or neural network requires studying the power system in all possible combinations of network configuration, an impossible task. If this difficulty can be surmounted, such techniques may find a place in on-line system applications.

3) Comparison of Direct and Indirect Methods: In general, direct methods are more accurate and selective than the indirect ones at the expense of increased CPU requirements. Therefore, the challenge is to improve the efficiency of the direct methods without sacrificing their strengths.

There are multiple reasons for the increased CPU requirements of the direct methods. Some of them result from conceptual differences while others are purely computational in nature.

The direct methods assemble the appropriate severity indices using the individual monitored quantities (bus voltages, branch flows, reactive generation). This implies that these quantities have to be first calculated. In contrast, the indirect methods rely on explicit calculation of severity indices without evaluating the individual quantities. As a result, indirect methods usually are less CPU demanding.

The knowledge of the individual monitored quantities permits the calculation of severity indices of any desired complexity without significantly affecting the numerical performance of the direct methods.

The use of complex severity rankings (measures) and the knowledge of the individual monitored quantities, are the main reasons for the superior accuracy (selectivity) of the direct methods. Therefore, over the last few years, more attention is being paid to the direct methods. As a result, their efficiency and reliability have drastically improved.

4) Fast Contingency Screening Methods: One way of building a reduced list of contingencies is based upon the use of a fast solution (normally an approximate one) and ranking the contingencies according to its results. Direct contingency screening methods can be classified by the imbedded modeling assumptions. Two distinct classes of methods can be identified:

1) linear methods specifically designed to screen contingencies for possible real power (branch MW overload) problems;
2) nonlinear methods designed to detect both the real and reactive power problems (including voltage problems).

The best combination of numerical efficiency and adaptability to system topology changes was achieved with the introduction of the bounding methods [21], [22]. These methods determine the parts of the network in which branch MW flow limit violations may occur. A linear incremental solution is performed only for the selected system areas rather than for the entire network. The storage requirements of the bounding methods are very close to those for the factors of the system matrix and no elaborate off-line calculations are required. The accuracy of the bounding methods is only limited by the accuracy of the incremental linear power flow. No other approximations are introduced by the bounding process itself.

Over the last few years, the "efficient bounding method" [11], has been implemented in a number of energy management systems. In a practical implementation, the numerical efficiency of the bounding approach is enhanced by a judicious application of the "sparse vector methods" [12], [13].

The nonlinear methods are designed to screen the contingencies for reactive power and voltage problems. As a by-product, they can also screen for branch flow problems (both MW and MVA/AMP). This capability depends on the implementation details of different algorithms.

Over the years, a number of different trends has emerged. The most important of them is listed as follows:

1) attempts to localize the outage effects;
2) attempts to speed up the nonlinear solution of the entire system.

The "concentric relaxation" method of [14] can be seen as the earliest localization attempt. The main idea behind the method is to solve a small portion of the system in the vicinity of the contingency while treating the remainder of the network as an "infinite expanse." The area to be solved is concentrically expanded until the incremental voltage changes along the last solved tier of buses are not significantly affected by the inclusion of an additional tier of buses. As presented in [14], the method suffered from a number of weaknesses:

1) unreliable convergence, in terms of mismatches, of the Gauss–Seidel solution algorithm;
2) lack of consistent criteria for the selection of buses to be included in the small network;
3) need to solve a number of different systems of increasing size resulting from concentric expansion of the small network (relaxation).

Possibility of missing severe problems outside the selected solution pocket due to the use of the small cutoff network and the exclusion of the boundary buses from outage severity considerations.

A modification of the original approach used a fixed number of tiers for ac contingency screening [15]. Similar to the local dc screening, the modified local solution algorithm was specifically designed to supplement the voltage PI rankings [16]. The local ac screening approach suffers from weaknesses identical to its predecessor.

Different attempts have been made at improving the efficiency of the large system solution. They can be classified as follows:

1) attempts to speed up the solution by means of approximations and/or partial (incomplete) solutions[17]–[19].
2) attempts to speed up the solution by means of using network equivalents (reduced network representation)[20].

The use of a partial, incomplete solution became well established with the introduction of the "single iteration" approach [18]. The main idea behind the method is to take advantage of the speed and reasonably fast convergence of the Fast Decoupled Power Flow [21] by limiting the number of iterations to one. The approximate, first iteration solution can be used to check for major limit violations and the calculation of different contingency severity measures. Unfortunately, the original implementation checked only for limit violations and used a single severity index to classify contingencies. As a result, the method did not perform as well as it could.

The single iteration approach can be combined with other techniques like the use of the reduced network representations to improve numerical efficiency.

An alternative approach is based upon bounding of outage effects [22], [23]. Similar to the bounding in linear contingency screening, an attempt to perform a solution only in the stressed areas of the system is made. A set of bounding quantities is built to identify buses which can potentially have large reactive mismatches. The actual mismatches are then calculated and the forward solution is performed only for those with significant mismatches.

Following the backward substitution step, all bus voltages are known and it is possible to calculate a number of different severity indices. The complete bounding method [22] expanded the conventional set of limit violation severity indices by adding the severities of shifts from base case conditions. It was also suggested to process the different severity indices by a class of variables, e.g. bus voltage limit violations with the bus voltage shifts. In this way, a better measure of contingency affect is obtained and the selectivity of the algorithms improved.

5) Zero Mismatch Method: The zero mismatch (ZM) method [24] extends the application of localization ideas from contingency screening to full iterative simulation. Again, advantage is taken of the fact that most contingencies significantly affect only small portions (areas) of the system.

The localization of contingency effects can be clearly seen during analysis of the convergence pattern of different contingencies. It becomes clear quickly that significant mismatches occur only in very few areas of the system being modeled. There is a definite pattern of very small mismatches throughout the rest of the system model. This is particularly true for localizable contingencies, e.g., branch outages, bus section faults. Consequently, it should be possible to utilize this knowledge and significantly speed up the solution of such contingencies.

Even though significant differences can exist between different implementations, the following conceptual steps are common to all of them:

1) bound the outage effects for the first iteration using for example a version of the complete boundary;
2) determine the set of buses with significant mismatches resulting from angle and magnitude increments;
3) calculate mismatches and solve for new increments;
4) repeat the last two steps until convergence occurs.

The selection of buses with potentially significant mismatches can be performed in a number of ways. One possibility is to use the "approximate sparse vector methods" [13], especially the "skip backward by columns" techniques

The zero mismatch method is significantly different from the concentric relaxation approach. The main difference between the two methods is in the network representation. The zero mismatch method uses the complete network model while a small cutoff representation is used in the latter one. The accuracy of the network representation and the ability to expand the solution to any desired bus account for the high reliability of the zero mismatch approach.

Independent of the implementation details, the use of the zero mismatch concept produces results of acceptable accuracy. The zero mismatch concept can also be used to obtain base case solutions, i.e., regular power flow solutions.

V. Optimization of Preventive and Corrective Actions

We now turn our attention to the subject of identifying preventive actions for those contingencies which are found to cause overloads, voltage limit violations, or stability problems. Preventive action without optimization is a poorly defined problem. If a feasible solution exists to a given security control problem it is common for other feasible solutions to exist as well. When this is the case, one solution must be chosen from among the feasible candidates. If a feasible solution does not exist (which is also common), a solution must be chosen from the infeasible candidates. Security optimization is a broad term given to the problem of selecting the preferred solution from a set of (feasible or infeasible) candidate solutions. The Optimal Power Flow (OPF) is the name given to the computer application that performs security optimization within an Energy Management System.

A. The Role of Optimization in Security Control

As was mentioned earlier, it is common that a utility will have more than one control scheme to address a given security problem. It is also common that not all schemes will be equally preferred and thus having to choose the best or "optimal" control scheme is often an inescapable aspect of operating a power system securely. Moving controls to improve security can increase operating costs, increase duty on equipment, and can burden the dispatcher with additional tasks. It is desirable to find the control actions that represent the optimal balance between security, economy, and other operational considerations.

It is important to note that the utility's need is for an optimal solution that takes all operational aspects into consideration. At present, however, security optimization programs do not have the capability to incorporate all operational considerations into the solution. This current limitation does not prevent security optimization programs from being useful to utilities, since the operationally optimal solution may also not be known. In fact, these imperfect solutions can provide guidance and insight that would not be otherwise available to operations staff. Nonetheless, it is critical to keep in mind that the true goal of security optimization technology is to provide solutions that are optimal from an operational, rather than algorithmic perspective.

B. The Optimal Solution

The term "optimal" is the condition that exists when security, economy and other operational considerations are optimally balanced. For security optimization programs, the goal is to compute control actions that achieve this optimality condition. The program solution is called an "optimal solution" if the control actions achieve optimality.

A fundamental problem in security optimization is that of distinguishing the preferred of two possible solutions. Clearly, if a method can be found that chooses correctly between any given pair of candidate solutions, then the method is capable of finding the optimal solution out of the set of all possible solutions. There are two classes of methods for distinguishing between candidate solutions: one class relies on an objective function, the other class relies on rules.

1) The Objective Function: The objective function method is based on the premise that the user can assign a single numerical value to each possible solution, and the solution with the lowest value is the optimal solution. The objective function is this numerical assignment and can be visualized as a contour map superimposed on the solution space. Optimization methods that use an objective function typically exploit the analytical properties of the objective function, solving for control actions that represent the low point in the surface. The classical optimal power flow (OPF) is an example of an optimization method that uses an objective function.

In general, the objective function value is an explicit function of the controls and state variables, for all the networks in the problem.

The objective function is said to be separable if the cost for a given control (or state variable) remains constant as other controls (or state variables) change setting. The MW production cost is an example of a separable objective and the active power transmission loss is an example of a nonseparable objective.

There are many advantages to using an objective function method. Analytical expressions can be found to represent MW production costs and transmission losses, which are, at least from an economic view point, desirable quantities to minimize. The objective function has another important property: it imparts a value to every possible solution. Thus all candidate solutions can, in principle, be compared on the basis of their objective function value. Since the real-time power system state is continually changing, the objective function method assures, in principle, that the optimal solution of the moment can be recognized by virtue of its having the minimum value.

Typical objective functions used in OPF are expressions for the MW production costs or expressions for active (or reactive) power transmission losses. However, when the OPF is used to generate control strategies that are intended to keep the power system secure, it is typical for the objective function to be an expression of the MW production costs, augmented with fictitious control costs that represent other operational considerations. This is especially the case when security against contingencies is part of the problem definition. Thus when security-constrained OPF is implemented to support a utility's real-time operations, the objective function tends to be a device whose purpose is to guide the OPF to find the solution that is optimal from an operational perspective, rather than one which represents a quantity to be minimized. Examples of noneconomic operational considerations that a utility might put into its objective function are:

1) a preference for a small number of control actions;
2) a preference to keep a control away from its limit;
3) the relative preference or reluctance for preventive versus postcontingent action when treating contingencies;
4) a preference for tolerating small constraint violations rather than taking control action.

Perhaps the greatest shortcoming of the objective function method is that it is difficult (sometimes impossible) for the utility to provide an objective function that consistently reflects true production costs and other noneconomic operational considerations.

2) Rules: The expert system is a method that uses rules. A rule-based method is appropriate when the user can specify rules for choosing between candidate solutions easier than by modeling these choices via an objective function. Optimization methods that use rules typically search for a rule matching the problem that needs to be addressed. The rule indicates the decision (e.g., control action) that is appropriate to the situation. The principal shortcoming of a rule-based approach is that the rule base does not provide a continuous "fabric" over the solution space (as does the objective function). As a consequence, it can be difficult to derive guidance for the OPF from the rule base when the predefined situations do not exist in the present power system state.

Examples where rules might be used in security optimization appear in network switching and control prioritization. Typically, a network switching action affects "true" costs only in the change in losses caused by the switching. However, the network topology (and thus the integrity of the system) can be changed considerably and this latter issue can far outweigh the economics (represented by the change in losses) in the utility's view. Even if an objective function expression of the preference/reluctance for the switching could be provided, the action typically introduces large nonconvexities into the problem. Minimization methods to date are not well-equipped to handle this. By contrast, utilities are often equipped with operating guidelines that involve switching, and these can often be easily modeled in a rule-based method. In a similar fashion, rules can be used to admit controls in prioritized stages into the optimization, independent of their objective function costing. This approach would presumably be employed when the prioritization models the utility's operation better than an approach based on cost effectiveness (i.e., the objective function).

Rules can play another important role when the OPF is used in the real-time environment. As will be discussed later, the real-time OPF problem definition itself can be ill-defined and rules may be used to adapt the OPF problem definition to the current state of the power system.

C. Optimization Subject to Security Constraints

The conventional formulation of the OPF problem is one which minimizes an objective function subject to security constraints. In problem formulation, the constraints are often presented as "hard constraints," for which even small violations are not acceptable. We will discuss later the means by which OPF can be used to recognize "soft" constraints and allow for their violation in an optimal fashion.

The minimization formulation is useful as a conceptual approach to finding the optimal solution but it should be recognized that a purely analytical formulation may not always lead to solutions that are optimal from an operational perspective. For example, it may be necessary to incorporate rules into the minimization process to obtain solutions that are more in line with the utility's operating policies. For this reason, the above formulation should be regarded as a framework in which to understand and discuss security optimization problems, rather than as a fundamental representation of the problem itself [25].

1) Security Optimization for the Base Case State: Ignoring contingencies for the moment, let us consider the security optimization problem for the base case state. In this problem the power system is considered secure if there are no constraint violations in the base case state. This means that any control action required will be corrective action. The goal of the OPF is to find the corrective action that is optimal.

When the objective function is defined to be the MW production costs, the problem becomes the familiar active and reactive power constrained dispatch. When the objective function is defined to be the active power transmission losses, the problem becomes one of active power loss minimization.

2) Security Optimization for Base Case and Contingency States: Now let us consider the security optimization problem for the base case and contingency states. In this problem, the power system is considered secure if there are no constraint violations in the base case state, and all contingencies are manageable with post-contingent control action. In the general case, this means that base case control action will be a combination of corrective and preventive actions and that post-contingent control action will be provided in a set of contingency plans. The goal of the OPF is to find the set of base case control actions plus contingency plans that is optimal.

The presence of contingencies makes this a multiple network problem, comprised of the base case network and each contingency network. To obtain an optimal solution, these individual network problems must be formulated as a multiple network problem and solved in an integrated fashion. The need for the integrated solution is twofold: First, any base case control action will affect all contingency states. Second, the more a given contingency can be addressed with post-contingent control action, the less preventive action is needed for that contingency.

There are two special cases of this multiple network problem: the case of no preventive action and the case of no contingency plans. When a utility is not willing to take preventive action, then all contingencies must be addressed with post-contingent control action. From the utility's perspective, the extra security provided by preventive action is not worth the cost incurred. In this special case, the absence of base case control action decouples the multiple network problem into a single network problem for each contingency. When a utility is not willing to rely on post-contingent control action, then all contingencies must be addressed with preventive action. From this utility's perspective, the cost of the preventive action is preferred over the risk of having to take control action in the post-contingent state. In this special case, the absence of post-contingent control action means that the multiple network problem may be represented as the single network problem for the base case, augmented with post-contingent constraints.

In general, security optimization for base case and contingency states will involve base case corrective and preventive action, as well as contingency plans for post-contingent action. To guide the program to find the optimal solution, the utility must provide the objective function and rules that reflect operating policy. For example, if the utility prefers to address contingencies with post-contingent action rather than preventive action, then post-contingent controls may be modeled as having a lower cost in the objective function. Similarly, a preference for preventive action over contingency plans could be modeled by assigning the post-contingent controls a higher cost than the base case controls. Some contingencies are best addressed with post-contingent network switching. This can be modeled as a rule that for a given contingency, switching is to be considered before other post-contingency controls.

3) Soft Constraints: Another form of security optimization is one in which the security constraints are "soft" constraints that may be violated but at the cost of incurring a penalty. This is a more sophisticated method that allows a true security/economy trade-off. It has the disadvantage of requiring a modeling of the penalty function consistent with the objective function. When a feasible solution is not possible, this is perhaps the best way to guide the algorithm toward finding an "optimal infeasible" solution.

4) Security versus Economy: Typically, economy must be compromised for security. However, the trade-off can go the other way as well: security can be traded off for economy. This is especially true when considering the inconvenience to the dispatcher of implementing control actions for relatively small constraint violations. If the constraint violations are small enough, it may be preferable to tolerate them in return for not having to make the control moves. Many constraint limits are, after all, not truly rigid and can be relaxed to some extent. Thus in general, the security optimization problem is the determination of the proper balance of security and economy. When security and economy are treated on the same footing, it is necessary to have a measure of the relative value of a secure, expensive state relative to a less secure, but also less expensive state. This information is typically provided by the user in the objective function.

5) Infeasibility: A topic related to security/economy trade-off is the problem of infeasibility. For the utility, even if a secure state cannot be achieved, there is still a need for the least insecure operating point. For OPF, this means that when a feasible solution cannot be found, it is still important that OPF reach a solution, and that this solution be "optimal" in some sense, even though it is infeasible. This is especially appropriate for OPF problems that include contingencies in their definition. (For modern power systems, the situation of base case violations that cannot be corrected is less likely than that of contingencies that cannot be made manageable.)

Thus there is a need for the OPF program to be capable of obtaining the "optimal infeasible" solution. There are several approaches to this problem. Perhaps the best approach is one which allows the user to model the relative importance of specific violations, with this modeling then reflected in the OPF solution. This modeling may involve the objective function (i.e., penalty function) or rules, or both.

D. The Time Variable

The power system state changes with time. Throughout the previous sections discussions of the network state (base case or contingency) have assumed the steady state condition. Thus all network states refer to the same (constant) frequency, and all transient effects due to switching and outages are assumed to have died out. Although bus voltages and branch flows are, in general, sinusoidal functions of time, only the amplitudes and phase relationships are necessary to describe the quiescent network state. Load, generation, and interchange schedules change slowly with time, but are treated as constant in the steady state approximation. Even though these time dependencies have been neglected there are still some vestiges of the time variable that need to be accounted for in the security optimization problem.

1) Time Restrictions on Violations and Controls: Perhaps the most important manifestation of the time variable is in the fact that constraint violations cannot be sustained indefinitely. Branch flow thermal limits typically have several levels of rating (normal, emergency, etc.), each with its maximum time of violation. (The higher the rating, the shorter the maximum time of violation.) Voltage limits have a similar rating structure and for some utilities, there is very little time to recover from a violation of an emergency voltage rating. Thus constraint violations need to be corrected within a specific amount of time. This applies to violations in contingency states as well as actual violations in the base case state. Base case violations, however, have the added seriousness of the elapsed time of violation: a constraint that has been in violation for a period of time has less time to be corrected than a constraint that has just gone into violation.

The limited amount of time to correct constraint violations is itself a security concern but it is further complicated by the fact that controls cannot move instantaneously. For some controls, the time required for movement is not trivial. Generator ramp rates can significantly restrict the speed with which active power is rerouted in the network. Delay times for switching capacitors and reactors and transformer tap changing mechanisms can preclude the immediate correction of serious voltage violations. The time-urgency of the violations and the time constraints on control movement can together determine the character of an OPF solution. If the violation is severe enough, slow controls that would otherwise be preferred may be rejected in favor of fast, less preferred controls. When the violation is in the contingency state, the time criticality may require the solution to chose preventive action even though a contingency plan for post-contingent corrective action might have been possible for a less severe violation.

2) Time in the Objective Function: For utilities that use OPF, it is common for the MW production costs to dominate the character of the objective function. Thus these OPF's seek a feasible solution that minimizes the cost per unit time of producing power. The point here is that the objective function involves the time variable to the extent that the OPF is minimizing a time rate of change. This is also the case when the OPF is used to minimize the cost of imported power or active power transmission losses.

Assume the production cost is expressed in dollars per hour. A dilemma arises from the fact that not all controls in the OPF can be "costs" in terms of dollars per hour. The start-up cost for a combustion turbine, for example, is expressed in dollars, not dollars per hour. The costing of reactive controls is even more problematic, since the reluctance to move these controls is not easily expressed in either dollars or dollars per hour. At present, OPF technology requires a single objective function, which means that all control costs must be expressed in the same units.

There are basically two approaches to this problem. One approach is to convert dollar per hour costs into dollar costs by specifying a time interval for which the optimization is to be valid. Thus control costs in dollars per hour multiplied by the time interval yield control costs in dollars, which now are in the same units as controls whose costs are "naturally" in dollars. This approach thus "integrates" the time variable out of the objective function completely. This may be appropriate when the OPF solution is intended for a well-defined (finite) period of time.

The other approach is to regard all fixed control costs (expressed in dollars) as occurring repeatedly in time and thus having a justified conversion into dollars per hour. For example, the expected number of times per year that a combustion turbine is started defines a cost per unit time for the start-up of the unit. Similarly, the reluctance to move reactive controls can be thought of as a reluctance over and above an acceptable amount of movement per year. This approach may be appropriate when the OPF is used to optimize over a relatively long period of time. A third approach is to simply adjust the objective function empirically so that the OPF provides acceptable solutions. This method can be regarded as an example of either of the first two approaches.

E. Using an Optimal Power Flow Program

OPF programs have been implemented in utility centers and are used both in the on-line environment and in off-line studies [25]–[27]. On-line and study mode uses of OPF are not the same and the characteristic features of each merits some discussion.

1) On-Line Optimal Power Flow: An OPF intended for on-line execution needs to be compatible with other aspects of the on-line environment. The power system state is, in general, changing through time, sometimes rapidly (or even abruptly), and at other times more slowly. The security status of the power system changes correspondingly. The users of the on-line OPF are the control center dispatchers, typically not familiar with OPF algorithms and having several concurrent activities demanding their attention (especially in times of emergency).

These aspects of the on-line environment produce special requirements for the on-line OPF. The solution speed of the program should be high enough so that the program completes before the power system has changed appreciably. Thus the on-line OPF should be fast enough to run several time per hour. The values of the algorithm's input parameters should be valid over a wide range of operating states, such that the program continues to function as the state of the system changes.

Other important requirements of on-line OPF are that it address the correct security optimization problem and that the solutions conform to utility operating policy.

2) Advisory Mode Versus Closed Loop Control: On-line OPF programs are implemented in either advisory or closed loop mode. In advisory mode, the control actions that constitute the OPF solution are presented as recommendations to the dispatcher. For closed loop OPF, the control actions are actually implemented in the power system, typically via the SCADA subsystem of the EMS [28].

The advisory mode is appropriate when the control actions need review by the dispatcher before their implementation. Closed loop control for security optimization is appropriate for those security optimization problems that are so well-defined that dispatcher review of the control actions is not necessary. An example of closed loop on-line OPF is the Constrained Economic Dispatch (CED) function. Here, the constraints of interest are the active power flows on transmission lines, and the controls of interest are the MW output of generators on automatic generation control (AGC). When the conventional Economic Dispatch would otherwise tend to overload the transmission lines in its effort to minimize production costs, the CED function supplies a correction to the controls to avoid the overloads.

At present, security optimization programs that include active and reactive power constraints and controls, in contingency states as well as in the base case, are implemented in an advisory mode. Thus the results of the on-line OPF are communicated to the dispatchers via EMS displays. Considering the typical demands on the dispatchers' time and attention in the control center, the user interface for on-line OPF needs to be designed such that the relevant information is communicated to the dispatchers "at-a-glance."

3) The Real-Time Security Optimization Problem Definition: As the power system state changes through time, the various aspects of the security optimization problem definition can change their relative importance. For example, a utility's concern for security against contingencies may be a function of how secure the base case is. If the base case state has serious constraint violations, the utility may prefer to concentrate on corrective action alone, ignoring the risk of contingencies. Also, the optimal balance of security and economy may depend on the current security state of the power system. During times of emergency, cost may play little or no role in determining the optimal control action. Thus the security optimization problem definition itself can be dynamic and sometimes ill-defined.

The real-time OPF problem definition is not necessarily ill-defined for all utilities. When the utility has a high level of confidence in the OPF problem definition, no provision needs to be made to adapt the definition to changing conditions. The best example of this is the OPF implemented for closed loop control. Here the utility is so certain of the validity of the OPF problem definition that the computed control actions are automatically implemented in the power system. To date, closed loop OPF implementations tend to be limited to simple active or reactive power subproblems and do not take contingencies into consideration.

For those cases where the real-time OPF problem definition is known to be ill-defined, some different implementation approaches can be taken to adapt the problem definition to changing conditions. One approach is to implement real-time OPF so that it solves several well-defined problems in a single run. The dispatcher is thus presented with multiple "views" into the real-time security optimization problem making the OPF a decision support tool in real time. One of these solutions might be restricted to the base case problem alone and another might include contingencies. One solution may only seek feasibility, another might seek optimality. The challenge with this approach is to design the man-machine interface so that the dispatcher can absorb the results of several OPF solutions quickly and easily.

Another approach to the problem of the ill-defined real-time OPF problem definition is to implement the program such that it can determine the appropriate problem definition from existing conditions in the power system. This approach involves implementing the real-time OPF with some level of artificial intelligence, perhaps a rule-based expert system. For example, the following rule might be used to determine whether contingencies are to be included in the OPF solution: "If constraint violations exist in the current base case state, ignore contingencies in the solution; otherwise include contingencies." Another rule might be used to select the post-contingent constraint limits to be enforced: "For the current base case state, if a given contingency would cause violations of an emergency rating, enforce the emergency rating in the contingency plan; otherwise, enforce the normal rating." The challenge with this approach is to provide the expert system with an adequate rule base and sufficient real-time data to ensure that the correct problem definition will be found.

VI. Dynamic Security Analysis

A. *What is Dynamic Security Analysis?*

The North American Electric Reliability Council defines security as "prevention of cascading outages when the bulk power supply is subjected to severe disturbances." To make certain that cascading outages will not occur the power system is planned and operated such that the following conditions in the bulk power supply are met at all times: 1) no equipment or transmission circuits are overloaded; b) no buses are outside the permissible voltage limits (usually within +5% of nominal); and c) when any of a specified set of disturbances occurs, acceptable steady-state conditions will result following the transient (i.e., instability will not occur).

Security analysis is conducted to make certain that the above conditions are satisfied. The first two conditions require only steady-state analysis; the third requires transient analysis (e.g., using a transient stability computer program). Recently it has been recognized that some of the voltage instability phenomena are dynamic in nature, and require new tools of analysis.

In general, security analysis deals with the power system's response to disturbances. In steady-state analysis the transition to a new operating condition is assumed to have taken place, and the analysis is aimed at ascertaining that operating constraints are met in this condition (thermal, voltage, etc.). In dynamic security analysis the transition itself is of interest, i.e., the analysis checks that the transition will lead to an acceptable operating condition. Examples of what can go wrong: loss of synchronism by some generators, transient voltage at a key bus (e.g., a nuclear plant or a sensitive load) falling below a certain level and operation of an out-of-step relay resulting in the opening of a heavily loaded tie-line.

At present, the computational capability of control centers has limited security analysis to steady state calculations. This means that the post-contingency steady-state conditions are calculated and limit checked for flow or voltage violations. It also means, however, that the dynamics of the system are ignored and whether the post-contingency state was reached without losing synchronism in any part of the system remains unknown. Thus instead of considering actual disturbances, the contingencies are defined in terms of outages of equipment and steady-state analysis is done for these outages. This assumes that the disturbance or fault did not cause any instability and the outage was caused by simple protective relaying. Usually, any loss of synchronism will cause additional outages thus making the present steady-state analysis of the post-contingency condition inadequate for unstable cases. Even if the post-contingency steady-state is guessed right the actual mode of instability is needed to determine any preventive remedial action. The need for dynamic analysis is obvious.

It has become customary to define a list, albeit a large list, of equipment losses for present day static analysis. Such a list usually consists of all single outages and a careful choice of multiple outages. Ideally, these outages should be chosen according to their probability of occurrence but these probabilities are usually not known and even when some statistical data is available the probabilities are so small that comparisons are usually meaningless. The choice of single outages seems a reasonable one because they are likely to occur more often than multiple ones (for the same reason this is used as a planning criterion). The inclusion of some multiple outages is needed because certain outages are likely to occur together because of proximity (e.g., double lines on the same tower) or because of protection schemes (e.g., a generator may be relayed out when a line is outaged). The size of this list is usually several hundred and can be a couple of thousand.

For dynamic security analysis, contingencies are not considered only in terms of post-contingency conditions (i.e., outages) but in terms of the total disturbance. All faults can be represented as three phase faults, with or without impedances, and the list of contingencies is essentially a list of locations where this can occur. This is a significantly different way of looking at contingencies where the post-contingency outages are determined by the dynamics of the system including the protection system. Obviously, if all possible locations are considered, this list can be very large.

In steady-state security analysis, the handling of all of the hundreds of outages cases using power flow calculations has been found to be unnecessary. This is because the operator is usually interested in the worst possibilities rather than all possibilities, many of which do not pose any danger to the system. The usual scheme is to use some approximate but faster calculations to filter out these worst outages, which can then be analyzed by a power flow. This screening of several hundred outages to find the few tens of the worst ones has been the major breakthrough that made steady-state security analysis feasible. Usually this contingency screening is done for the very large list of single outages while the multiple outages are usually included in the short list for full power flow analysis. Today, the trend is to use several different filters (voltage filter versus line overload filter) for contingency screening. It is also necessary to develop fast filtering schemes for dynamic security analysis to find the few tens of worst disturbances for which detailed dynamic analysis will have to be done. The filters will of necessity be substantially different from those used for static security. The concept of severity indices remains valid, but new indices which indicate margin to instability must be developed.

From the viewpoint of the operator, static security analysis and dynamic security analysis are not two separate issues. The operator would like to know which disturbances on the system are the worst ones and what are the effects of these disturbances. The effects of most interest to the operator include the resulting outages and the limit violations in the post-contingency condition. In addition, it would be useful to know the mechanism that caused the outages, whether they were due to distance relay settings or loss of synchronism or other reasons. This latter information is particularly useful for preventive action.

The stability mechanism that causes the outages is referred to as the "mode of disturbance." A number of modes exist. A single generating unit may go out of synchronism on the first swing (cycle). A single unit may lose synchronism after several cycles, up to a few seconds. Relays may operate to cause transmission line outages. Finally, periodic oscillations may occur between large areas of load and/or generation. These oscillations may continue undamped to a point of loss of synchronism. All of these types of events are called modes of disturbances. Unfortunately, different analysis techniques may be necessary to satisfactorily assess the system for each mode of disturbance.

B. Need for Dynamic Security Analysis

As previously explained, the power network is planned to withstand the occurrence of certain disturbances. Security limits are then established and the power system is operated within these limits. In North America, NERC establishes the overall philosophy of planning and operating the power systems for reliability. The specific criteria which must be met, however, are established by the individual reliability councils. Each council sets the conditions under which the "strength" of its systems must be tested and the specific "criteria" it must meet. These are translated into the types of contingencies which the system must withstand for cascading outages not to occur.

The central issues in how power system security is dealt with in the North American Interconnections are: 1) how to determine the security limits under all possible conditions, and 2) how to ascertain that system security (based on these limits) is maintained at all times. The answer is conceptually very simple, yet it has become increasingly difficult to accomplish. All possible (and credible) conditions and scenarios are considered; analysis is performed on all of them to determine the security limits for these conditions given to the operating personnel in the form of "operating guides," establishing the "safe" regimes of operation. The key power system parameter or quantity is monitored (in real time) and compared with the available (usually precomputed) limit. If the monitored quantity is outside the limit, the situation is alerted or flagged for some corrective action.

Several trends in the North American electric utility industry have increased the need for on-line dynamic security analysis. Transmission lines bring large quantities of bulk power, in some cases, hundreds of miles from generating plants to population and industrial load centers. But increasingly, these same circuits are being used for other purposes as well: to permit sharing surplus generating capacity between adjacent utility systems, to ship large blocks of power from low-energy-cost areas to high-energy-cost areas, and to provide emergency reserves in the event of weather-related outages. Although such transfers have helped to keep electricity rates lower, they have also added greatly to the burden on transmission facilities and increased the reliance on control.

Economy energy transactions, reliance on external sources of capacity, and competition for transmission resources have all resulted in higher loading of the transmission system. It has also resulted in heavier loading of tie-lines which were originally built to improve reliability, and were not intended for normal use at heavy loading levels. This trend has increased interdependence among neighboring utilities. With greater emphasis on economy, there has been an increased use of large economic generating units. This has also affected reliability.

As a result of the trends mentioned above, systems are now operated much closer to security limits (thermal, voltage and stability). On some systems, transmission loadings are being operated at or near limits 24 hours a day. The implications of these trends are:

1) The industry trends have adversely affected system dynamic performance. A power network stressed by heavy loading has a substantially different response to disturbances from that of a nonstressed system. For example, while for a robust system the effect of a disturbance tends to be localized if no additional stimuli are introduced, the effect of a disturbance in a stressed power network may be felt far away; when they occur, system splits may take place away from the disturbance location; poor damping may lead to growing oscillations under small or large disturbances; and so on.
2) The potential size and effect of contingencies has increased dramatically. On the one hand, when a power system is operated closer to the limit, a rel-

atively small disturbance may cause a system upset. On the other hand, the largest size contingency is increasing (a contingency of 2600MW has already occurred on the eastern Interconnection). Thus to support operating functions many more scenarios must be anticipated and analyzed. In addition, bigger areas of the interconnected system may be affected by a disturbance.

3) Where adequate bulk power system facilities are not available, special controls are being employed to maintain system integrity. Overall, systems are more complex to analyze to ensure reliability and security.
4) Some scenarios encountered cannot be anticipated beforehand. Since they cannot be analyzed off-line, operating guides for these conditions may not be available, and the system operator may have to "improvise" to deal with them (and often does).

The present conditions in the North American interconnected system are such that thermal-limits and voltage limits are of concern to practically all the power systems. In addition, several areas are stability limited. It has become increasingly challenging to meet the NERC criteria for security. In addition, indications are that the conditions creating the present security-related problems will not improve in the future.

To come to grips with the industry trends and with the increased awareness of dynamic security, certain needs should be satisfied. These needs may require imaginative application of current tools; others may require new tools. Among the needs are:

1) Limit the number of conditions to be analyzed by moving the analysis closer to real-time.
2) Simplify computation of security limits by some new analytical means.
3) Explore moving toward "softer" limits, instead of hard limits to be strictly adhered to.
4) Give more emphasis to "trends" in security limits as system conditions change. This is actually how the system operator deals with security, yet it is not something that is usually quantified.

For on-line dynamic security analysis, what is given is a base case steady-state solution (the real time conditions as obtained from the state estimator and external model computation, or a study case as set up by the operator) and a list of fault locations. The effects of these faults have to be determined and, specifically, the expected outages have to be identified. This can be done by examining the dynamic behavior of the system. As stated before, some form of fast approximate screening is required such that the few tens of worst disturbances can be determined quickly.

Traditionally, for off-line studies, the dynamic behavior has been examined by a transient stability program. This program, in the very least, models the dynamic behavior of the machines together with their interconnection through the electrical network. Most production grade programs have elaborate models for the machines and their controls together with dynamic models of other components like loads, dc lines, static VAR compensators, etc. These models are simulated in time using some integration algorithm and the dynamic behavior of the system can be studied. If instability (loss of synchronism) is detected, the exact mode of instability (the separation boundary) can be identified. Many programs have relay models that can also pinpoint the outages caused by relay operation due to the dynamic behavior.

Obviously, the question for on-line analysis is that of the available time to do the analysis. That is, the analysis itself by a pure time domain simulation is known to be feasible but whether this analysis can be completed within the time frame needed in the control center environment is the real question.

The time taken for time domain analysis of power system dynamics depends on many factors. The most obvious one is the length of simulation or the time period for which the simulation needs to be done so that all the significant effects of the disturbance can be captured. Other factors include the size of the power system, and the size and type of the models used. Additional factors, like the severity of the disturbance and the solution algorithm used, also effects the computation time.

The determination of the vulnerability of the present system conditions to disturbances does not complete the picture because the solution to any existing problems must also be found. Quite often the post-contingency overloads and out-of limit voltage conditions are such that they can be corrected after the occurrence of the fault. Sometimes, and especially for unstable faults, the post-contingency condition is not at all desirable and preventive remedial action is needed. This usually means finding new limits for operating conditions or arming of special protective devices. Although remedial action is considered as a separate function from security analysis today, both are needed by operators of stability limited systems.

A number of approaches to the on-line dynamic stability analysis problem have been studied. To date, practical implementation for a large scale power system has not been feasible. More research is needed before an on-line dynamic security assessment capability is implemented. Presently, engineers perform a large number of studies off-line to establish operating guidelines, modified by judgement and experience. Conventional wisdom has it that computer capability will continue to make it more economically feasible to do on-line dynamic security assessment, DSA, providing the appropriate methods are developed.

The first obvious method for on-line DSA is to implement the off-line time domain techniques on faster, more powerful and cheaper computers. New workstations based on the RISC technology and the UNIX operating system hold some promise for realizing this vision. Equivalencing and localization techniques have been proposed as ways to speed up the time domain solutions. Also parallel and array processors show promise in accelerating portions of the time domain solution.

Direct methods of transient stability, e.g., the transient energy function method, have the potential of meeting some of the needs for DSA. They offer the possibility of doing stability studies in near real-time, provide a qualitative judgement on stability, and they are suitable for use in sensitivity assessments. Unfortunately, the TEF methods are limited to first swing analysis. An advantage, however, is that the TEF methods provide energy margins to indicate the margin to instability.

Artificial intelligence or expert systems have proven to be appropriate solutions to other power system operations problems, and there is speculation that these technologies will play a major role in DSA. Based on the success of applying expert systems to other operating problems, it is likely that research will be done to have expert systems handle the behavior of protection systems, predict the final state of the power system, interpret analytical results and provide English communication with the dispatcher, contingency selection and other aspects of the on-line dynamic security assessment capability. It may be that artificial intelligence techniques serve as the framework holding together a number of different analytical programs. The AI portion may provide a role much like the planning operations engineer.

Eigenvalue and related methods, and frequency response methods are used as part of off-line studies, for example, using frequency response method to design power system stabilities, but are not currently thought of as part of an on-line DSA.

Pattern recognition methods have the general capability to identify specific attributes of system behavior. They have had some problems with handling singularities. New techniques, such as chaos theory may help to solve this problem.

Probabilistic methods have the advantage of providing a measure of the likelihood of a stability problem. Their application in dynamic security assessment appears to be in the areas of contingency screening and in quantifying the probability of the next state of the system.

References

[1] G. D. Friedlander, "The other electric company," *IEEE Spectrum*, vol. 11 no. 6, pp. 48–54, 1974.

[2] H. D. Limmer, "Security application of on-line digital computers," in *Proc. Second PSCC*, Stockholm, Sweden, July 1966.

[3] T. E. DyLiacco, "The adaptive reliability control system," *IEEE Trans. Parallel Dist. Syst.* vol. PAS-86, pp. 517–31, 1967, (presented at the 1966 summer power meeting).

[4] *Reliability Concepts in Bulk Power Electric Systems*, North American Electric Reliability Council, 1985.

[5] G. L. Blankenship and L. H. Fink, "Statistical characterizations of power system stability and security," in *Proc. 2nd Lawrence Symp. Systems and Decision Sciences*, Berkeley, CA, Oct. 1978, pp. 62–70.

[6] F. F. Wu, Y-K. Tsai, and Y-X. Yu, "Probabilistic steady-state and dynamic security assessment," *IEEE Trans. Power Syst.*, vol. PWRS-3, pp. 1-9, 1988. (originally presented at the 1983 Winter Power Meeting.)

[7] F. F. Wu and Y-K. Tsai, "Probabilistic dynamic security assessment of power systems: Part I-basic model," *IEEE Trans. Circuits Syst.*, no. 3, pp. 148–159, 1983.

[8] J. Feinstein, J. Tscherne, and M. Koenig, "Reactive load and reserve calculation in real time computer control system," in *IEEE/PES Proc. PICA*, 1987, pp. 121–27.

[9] W. S. Ku and P. Van Olinda, "Security and voltage applications of the public service dispatch computer," in *Proc. IEEE/PES PICA*, 1969, pp. 201–207.

[10] L. H. Fink, "Security: Its meanings and objectives," in *Proc. workshop on power system security assessment,* Ames, IA, Apr. 1988, pp. 35–41.

[11] V. Brandwajn, "Efficient bounding method for linear contingency analysis," *IEEE Trans. Power Syst.*, vol. PWRS-3, pp. 38–43, Feb. 1988.

[12] W. F. Tinney, V. Brandwajn, and S. M. Chan, "Sparse vector methods," *IEEE Trans. Power App. Syst.*, vol. PAS-104, pp. 295–301, Feb. 1985.

[13] R. Bacher, G. C. Ejebe, and W. F. Tinney, "Approximate sparse vector techniques for power network solutions," presented at the 16th Power Industry Computer Applications (PICA) Conf., Seattle, WA, May 1–5, 1989.

[14] J. Zaborsky, K. W. Whang, and K. Prasad, "Fast contingency evaluation using concentric relaxation," *IEEE Trans. Power App. Syst.*, vol. PAS-99, pp. 28–36, Jan./Feb. 1980.

[15] M. G. Lauby, T. A. Mikolinnas, and N. D. Reppen, "Contingency selection of branch outages causing voltage problems," *IEEE Trans. Power App. Syst.*, vol. PAS-102, pp. 3899–3904, Dec. 1983.

[16] EPRI RP1530-1, "Transmission system reliability methods," Report EL-2526, vols. 1–2, July 1982.

[17] N. M. Peterson, W. F. Tinney, and D. W. Bree, "Iterative linear AC power flow solution for fast approximate outage studies," *IEEE Trans. Power App. Syst.*, vol. PAS-91, pp. 2048–2053, Sept./Oct. 1972,

[18] F. Albuyeh, A. Bose, and B. Heath, "Reactive power considerations in automatic contingency selection," *IEEE Trans. Power App. Syst.*, vol. PAS-101, pp. 107–112, Jan. 1982.

[19] K. Nara *et al.*, "On-line contingency selection for voltage security analysis," IEEE Trans. Power App. Syst., vol. PAS-104, pp. 847–856, Apr. 1985.

[20] W. F. Tinney and J. M. Bright, "Adaptive reductions for power flow equivalents," *IEEE Trans. Power App. Syst.*, vol. PWRS-2, pp. 351–360, May 1987.

[21] B. Stott and O. Alsac, "Fast decoupled load flow," *IEEE Trans. Power App. Syst.*, vol. PAS-93, pp. 859–869, May/June 1974.

[22] V. Brandwajn and M. G. Lauby, "Complete bounding method for AC contingency screening," *IEEE Trans. Power Syst.*, vol. PWRS-4, pp. 724–729, May 1989.

[23] Y. Chen and A. Bose, "Adaptive pre-filter for the voltage contingency selection function," paper presented at IEEE PES Winter Power Meeting, New York, NY, Jan. 29-Feb. 3, 1989.

[24] R. Bacher and W. F. Tinney, "Faster local power flow solutions: The zero mismatch approach," *IEEE Trans. Power Syst.*, vol. 4, pp. 1345–1354, Nov. 1989.

[25] ——, "Techniques for power network solutions," presented at the 16th Power Industry Computer Applications (PICA) Conf., Seattle, WA, May 1–5, 1989.

[26] "Security enhancement system final report," EPRI Final Report for Project RP1712.

[27] J. N. Wrubel, P. Van Olinda, B. F. Wollenberg, and G. W. Woodzell, "Installation and start up of an on-line state estimator," *IEEE Trans. Power Syst.*, vol. PWRS-100, pp. 4591–4596, Nov. 1981.

[28] IEEE Current Operating Problems Working Group Report, "Online load flows from a system operator's viewpoint," *IEEE Trans. Power Syst.*, vol. PWRS-102, pp. 1818–1822, June 1983.

[29] B.Stott, J. L. Marino, "Linear Programming for Power System Security Applications",*IEEE Trans. Power Syst.*, vol. PAS-98, pp. 837–848, May 1979.

[30] Utility Expands Storm Monitoring; *Electrical World*, Feb. 15, 1980.

[31] R. E. Orville, R. B. Pyle, and R. W. Henderson, "The East Coast Lightning Detection Network," *IEEE Trans. Power Syst.*, vol. PWRS-1, pp. 243–46, 1986.

[32] T. J. Bertram, K. D. Demaree, and L. C. Dangelmaier, "An integrated package for real-time security enhancement," presented at the IEEE/PES 1989 PICA Conf., Seattle, WA, May 1–5, 1989.

[33] R. Bacher and H. P. Van Meeteren, "Real-time optimal power flow in automatic generation control," *IEEE Transactions Power Syst.*

[34] B. Stott, O. Alsac, and A. Monticelli, "Security analysis and optimization," *Proc. IEEE*, vol. 75, pp. 1623–1644, Dec. 1987.

[35] D. I. Sun, B. Ashley, B. Brewer, A. Hughes, and W. F. Tinney, "Optimal power flow by Newton approach," *IEEE Trans. Power Syst.*, vol. PAS-103, pp. 2864–2880, Oct. 1984.

[36] A. Monticelli, M. V. F. Pereira, and S. Granville, "Security constrained optimal power flow with post-contingency rescheduling," *IEEE Trans. Power Syst.*, vol. PWRS-2, pp. 175–182, Feb. 1987.

[37] M. K. Enns, J. J. Quada, and B. Sackett, "Fast linear contingency analysis," *IEEE Trans. Power Syst.*, vol. PAS-101, pp. 783–791, Apr. 1982.

[38] M. G. Lauby, "Evaluation of a local DC load flow screening method for branch contingency selection of overloads," *IEEE Trans. Power Syst.*, vol. PWRS-3, pp. 923–928, Aug. 1988.

[39] T. A. Mikolinnas and B. F. Wollenberg, "An advanced contingency selection algorithm," *IEEE Trans. Power Syst.*, vol. PWRS-100, pp. 608–617, Feb. 1981.

[40] F. D. Galiana, "Bound estimates of severity of line outages in power system analysis and ranking," *IEEE Trans. Power Syst.*, vol. PWRS-103, pp. 2612–2622, Sept. 1984.

[41] V. Brandwajn and M. G. Lauby, "Critical review of branch contingency selection methods," IFAC Symp. Power Systems and Power Plant Control, Seoul, Korea, Aug. 22–24, 1989.

Neal Balu (Senior Member, IEEE), photograph and biography not available at the time of publication.

Timothy Bertram (Associate Member, IEEE), photograph and biography not available at the time of publication.

Anjan Bose (Fellow, IEEE), photograph and biography not available at the time of publication.

Vladimir Brandwajn (Senior Member, IEEE), photograph and biography not available at the time of publication.

Gerry Cauley (Senior Member, IEEE), photograph and biography not available at the time of publication.

David Curtice (Senior Member, IEEE), photograph and biography not available at the time of publication.

Aziz Fouad (Fellow, IEEE), photograph and biography not available at the time of publication.

Lester Fink (Life Fellow, IEEE), photograph and biography not available at the time of publication.

Mark G. Lauby (Senior Member, IEEE), photograph and biography not available at the time of publication.

Bruce F. Wollenberg (Fellow, IEEE), photograph and biography not available at the time of publication.

Joseph N. Wrubel (Senior Member, IEEE), photograph and biography not available at the time of publication.