POWER SYSTEM SECURITY

Power system security is the ability to maintain the flow of electricity from the generators to the customers, especially under disturbed conditions. Since disturbances can be small or large, localized or widespread, the planning and design of the power system must achieve a certain level of security. To secure the system against more severe disturbances obviously requires more expensive designs; hence, the design criteria are chosen to meet an appropriate level of security. In the more developed countries, the customer is often willing to pay more for minimizing the interruption of power, whereas in the less developed countries the scarcity of capital and other factors keep the level of power system security lower.

It should be noted that after 9/11 the term 'power system security' has often been used to mean security against terrorist attacks on the power system, and the term 'power system reliability' has been sometimes used to mean the above ability of the system to withstand disturbances. In this section we continue to use the terminology of 'power system security' in the traditional manner. Of course, a system designed to be more secure (or reliable) can also withstand terrorist attacks better.

The measures of power system security are amount, duration, and frequency of customer outages. Outages can thus be represented in probabilistic terms (e.g.,*X* hours per year, or 99.9% reliable). Thus, the terms *reliability* and *security* have been used interchangeably for power systems, although *reliability* is more often used to refer to the probabilistic measures while *security* refers to the ability of the system to withstand particular equipment outages without loss of service.

Obviously, one way to withstand equipment outages is to have redundant equipment. Providing redundancy in generators, especially when the economies of scale favor fewer and larger units, is an expensive proposition. It is cheaper to have neighboring utilities provide backup in case of generator outages, and this led to widespread interconnection of the transmission systems in North America and Western Europe starting in the 1930s. This transmission network, often called the power grid, also must have redundant lines to provide alternate paths in case of transmission outages.

Although the inherent reliability of such large interconnections is very high, one major drawback is that the rare disturbance can affect larger geographic areas. This became vividly apparent for the first time in 1965, when the Northeastern United States suffered a massive blackout. Since then, computerized analytical tools have enhanced the planning and design of these large power networks. Moreover, an overlay of computers and communications on the power networks has allowed more secure operation and control but large area disturbances continue to occur, albeit rarely, with the biggest blackouts each affecting more than 50 million people happening in North America and Europe in 2003.

These engineering tools to enhance the security of the power system are the subjects of the following sections. First, security assessment is discussed as applied to generation, transmission, and distribution; also, the applications are separated into planning, operations planning, and operating functions. Second, the techniques and methods used in these tools are discussed in some detail.

SECURITY ASSESSMENT

The security of a power system must be assessed to guarantee a particular level of performance. This is true following any modification to the structure of the power system or to the operational condition. Providing redundant generation to enhance security requires assessment tools different from when providing redundant transmission paths. Thus, in this section security assessment is looked at in two different ways: One is a hierarchical look at generation, transmission, and distribution security; the other is a view of security for the planning, operations planning, and operational time horizons.

This approach to security assessment has been developed over the last three decades, when the power companies have had a vertically integrated structure. As restructuring of the electric power industry takes place, security assessment must be adjusted. Since the physical structure of the generation-transmission-distribution grid will not change, the security of the system will be assessed as in the past. However, the responsibility for maintaining security will change, and so the planning and operational decisions may be somewhat different.

Hierarchical View

Enough generation must be available at all times to meet the load demand. Thus, generator units must be managed in such a way that planned outages of units, as well as forced outages, should not result in a shortage of generation. The installed generation capacity obviously has to be greater than the maximum demand, and it has to meet specific security criteria.

If a generator is forced out, the remaining generators on line must have enough excess capacity to make up for the loss. This excess capacity is called *spinning reserve.* In addition, there must be some generation capacity that could be brought on line rapidly, say within 10 to 15 min. This is known as *ready reserve.* All systems have criteria for maintaining spinning and ready reserves for secure operation.

Since the probabilities of forced unit outages are well known from historical data, it is possible to calculate the probability of generation being less than the load demand. This *loss of load probability* is kept within certain criteria (e.g., 1 day in 10 years) by planning for enough capacity and number of units.

Still, it is not enough just to ensure that generation availability is higher than the load demand. This power has to be transmitted to the loads without overloading the transmission lines and while maintaining voltages within a certain band of the nominal level, typically 5%. Moreover, the system should be able to continue operating in this way even after the outage of a transmission line or generator. The transmission lines have to be connected in a network so that the outage of a particular line leaves adequate parallel paths between the generators and the loads.

A common criterion for operational security is this ability of the system to withstand the outage of any one piece of equipment. The difficulty with this criterion is that checking the effects of an outage on the transmission system requires a significant amount of computation. Thus, assessing the security of the transmission system, although significantly enhanced by the use of digital computers, remains an analytically demanding problem.

The distribution system, unlike the transmission system, is largely radial, and there is usually only one electrical path from the feeding substation to a load. Thus, an outage of any section of a distribution line is bound to disrupt supply to some load(s). Better security in the distribution system can be provided by the ability to sectionalize the distribution feeders with switches that can be turned off and on to provide alternate paths to feed the loads. Since the main goal here is to minimize the time of load disruption, the ability to handle trouble calls and dispatch crews rapidly also affects security.

Temporal View

Planning of the power system—that is, the decision to add new generation, transmission, or distribution—must consider security criteria. Similarly, the operation of the power system, during which new equipment cannot be added but existing equipment can be switched in and out and controlled, must be affected according to security criteria. In the United States and Canada, the security criteria for planning and operation have been set by the North American Electric Reliability Council (NERC) for the last three decades. After the 2003 blackout the responsibility for maintaining reliability is being shifted to the Federal Energy Regulatory Commission (FERC) with NERC transitioning to be their implementation arm under the name Electric Reliability Organization (ERO).

The planning horizon is usually upward of one year as it is not normally possible to design and install major equipment in less than that time. The operations horizon is anything less than one year, but most of the decisions are made for about one week. Moreover, the decisions made for the next day and beyond are often referred to as operations planning, whereas operations involve real-time decisions.

Planning for adequate generation, as mentioned earlier, uses a probabilistic load prediction and plans sufficient generation to ensure that the loss of load probability will be under a certain level. Transmission planning, on the other hand, uses worst-case scenario simulations to ensure that the system will be able to withstand outages under some defined worst condition. Because the modeling of transmission is complex, probabilistic measures for transmission reliability, although desirable, remain difficult to calculate.

In the operations horizon, probabilistic measures are less meaningful as the anticipated loads can be predicted with more certainty, say over a span of several days. Thus, generation is scheduled with the security criteria for adequate spinning and ready reserve to withstand generator outages. Transmission security for operations planning is ensured, in the same way as in planning, by simulating the worst-case scenarios according to some standard procedures.

In real-time operations, generation is automatically dispatched to meet load. Thus, if adequate spinning and ready reserves are available, load should always be met provided that sufficient transmission capacity. There are two functions that must be performed here: One is the continuous adjustment of the generation to match exactly the total load that is varying, and the other is checking that adequate reserves are always available that can respond to the changing load as well as to a loss of a generation unit. The first is known as *load following* or *regulation* and is performed with one or more feedback control mechanisms. The second, known as *reserve monitoring,* is accomplished by the control center computers, which monitor the availability of generation.

Ensuring transmission security in real time requires significant on-line computation of contingency scenarios. It should be pointed out here that the availability of more on-line analysis, attributed to increasing use of computers and communication, results in more efficient use of the power system; that is, the system can be operated closer to its limits because these limits can be calculated on line. Without such tools, limits set off line have to be more conservative to ensure security.

Responsibility in a Restructured System

As long as the utilities are vertically integrated, maintaining security within one company's geographic area is its responsibility. Since most utilities are interconnected, the security criteria have to be jointly agreed upon, and planning and operations of neighboring companies must be coordinated.

The power industry is being restructured, but the power system, at least for the foreseeable future, will continue to have the same physical structure. Thus, the security of the system must be assessed and maintained in the same way as before. However, the responsibility for maintaining security must be assigned to a particular organization with the appropriate authority to do so. In the new structure, it appears that the generation companies will be deregulated while the transmission and distribution companies will continue to be regulated. The distribution companies will have distinct geographic boundaries within which they will own the "wires," and so the responsibility for maintaining security of these distinct distribution systems is obviously going to rest on the distribution companies.

The transmission network is often made up of lines of different ownership, and under the new structure, generators of different ownership will connect to the nodes of this network. To ensure operational security, one entity must be made responsible, and the transmission grid operator is the obvious choice. In countries where utilities were government owned, as in England or Chile, the transmission grid has been assigned to one entity for both ownership and operation. In the United States, where ownership of transmission is in multiple private hands, regions have been encouraged to form *independent system operators* (*ISO*), which can then be responsible for the secure operation of each regional transmission network.

To ensure secure operation, the transmission grid operator must have some control of the generators. That is, when security limits are exceeded, the only way to ensure security may be to modify the generation pattern, in which case the operator must have authority to do so. Thus, the generation companies can have complete operational independence only until a security limit is reached, a condition often referred to as transmission congestion. All transactions of power between generation companies and their customers must be under continuous scrutiny of the operator to maintain security. This must be done in both the operations planning (i.e., day ahead) mode as well as in real time. The opening of the market for the buying and selling of electric energy is already creating large trading floors, and even a secondary market for options, but most of these trades are made for the long term without much concern for the security of the system. However, the actual transactions of energy must be subject to the security constraints of the power system at that time, and any imbalance will have to be made up on the day-ahead or the real-time spot market, in which prices can be expected to be volatile if unexpected security constraints are encountered.

Ensuring security in the long run—that is, planning enough generation and transmission addition—may also become more complicated. Since the generation companies no longer have a legal obligation to serve, appropriate generation addition is not always guaranteed. It is assumed that the financial incentive will rise enough to encourage adequate generation availability.

SECURITY ASSESSMENT TECHNIQUES

Planning Techniques

Long-term planning focuses on the installation of adequate generation and transmission facilities to meet anticipated load growth. It may take several years from initial decision to installation for new plants or transmission lines. Thus, load projections, based on anticipated economic and population growth and generation availability are needed for several years into the future. These longer-term forecasts are subject to a significant amount of error and must be addressed by statistical approaches.

Load growth rates of 4 to 5% were typical in the industrialized countries and fairly regular for much of the postwar period, which simplified the planners' responsibilities. In recent decades, load growth has slowed considerably, to around 2%, and is somewhat more difficult to forecast. Further, the expansion of facilities has been constrained by more heightened public concerns for environmental impact. This has meant increased emphasis on precise planning. The recent moves to deregulate are certain to provide yet greater emphasis on detailed planning studies, but in the completely different environment of competitive markets, by generation and transmission companies. Still, the level of precision that can be included in studies is inversely related to the time frame of interest. Longer-term planning studies must necessarily focus on statistical methods to analyze the adequacy of the proposed infrastructure for a variety of possible future scenarios.

Generation Planning. The required generating capacity in a power system depends on the availability of generating units and the load pattern. Generation must be available in sufficient quantity to account for unplanned or forced outages as well as normal maintenance of units. Generator availability is most commonly measured in terms of the unit *forced outage rate* (*FOR*), which is the expected fraction of time for a unit to be unavailable exclusive of scheduled outages.

The load pattern on a daily and seasonal basis also plays an important role, as the system must be able to supply the peak loads. These forecasted loads are usually modeled by arranging the daily loads in descending order over the study period, say a particular year into the future year. The resulting curve, known as the *load duration curve,* is shown on the left-hand side of Fig. 1. From this is obtained the load probability distribution, which can be combined with generation capacity statistics to calculate the probability that demand exceeds capacity on any given day. This is commonly called the *loss of load probability* (*LOLP*). A probabilistic load distribution curve, shown on the right-hand side of Fig. 1, is modified by the generator availability probability distributions to calculate the LOLP. The resulting shaded area is the expected unmet energy. The NERC established criterion for this unmet energy is less than 1 day in 10 years. New generator units must be planned if this criterion is not met.

The basic indices described previously are widely used, but they fail to provide insight into either the frequency or the duration of outages. Statistics on the expected time to repair generator outages and load duration are necessary to compute expected outage times. Transition rates between different generator conditions (i.e., normal, under repair, and so on) can be used to model the projected generation availability through Markov methods. This provides deeper understanding into the reliability particularly for specific load points in the system. For large systems, it is impractical to model all possible combinations of unit states and load patterns, so simplified load and outage models are employed.

The planning of generation will change completely as the buying and selling of generation is deregulated. The installation of new generation will be a function of the sales forecasts and contracts of generation companies rather than the forecasted load in a given area. The larger generation companies will, of course, need to do an analysis similar to that described here to ensure that they can reliably service their customers.

Transmission Planning. Sufficient generation capacity cannot alone guarantee load service. There must also be adequate transmission facilities to deliver the power. The transmission system is a complex interconnection of transmission lines, transformers, capacitors, and so on and is networked with multiple paths between generators and loads. This transmission equipment can carry currents of as much as several MA at voltage levels between 115 kV and 745 kV, but despite such high ratings, there are still strict limits to the loading of equipment. Analysis of the flows along the different paths during steady-state conditions is needed to ensure viable operation of equipment.

In addition, transmission systems in North America crisscross vast geographic areas, resulting in wide expo-

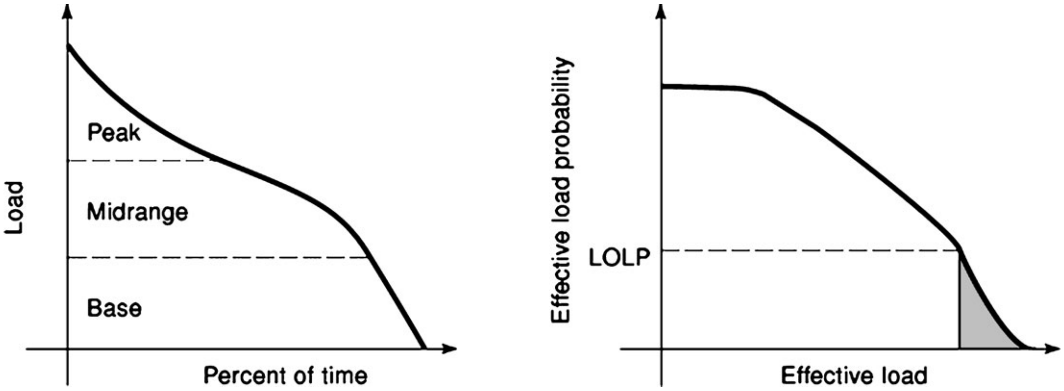

Figure 1. Loss of load probability calculation.

sure to a variety of harsh elements (mostly related to weather but also unusual phenomena, such as geomagnetic storms). Thus along with the normal load fluctuations, the system experiences disturbances and must be able to respond dynamically to the disturbance and settle into a satisfactory steady state. Engineers design the system so as to withstand numerous equipment outages. The so-called $(n - 1)$ criterion established by NERC/ERO requires systems to be planned and operated so as to withstand all single contingencies (e.g., one line de-energized, or one generator unit outage) for various worst-case scenarios, called base case studies. Regional reliability agreements establish these base case scenarios, which typically include one or more major outages, so the reliability criterion is, in practice, somewhat more conservative than a simple single outage.

The steady-state current flow through the network depends on the impedances of the transmission lines and the voltage level at different nodes (i.e., buses). While the network itself is generally linear, the load and generator characteristics are nonlinear, so determination of the flows through the network requires solution of nonlinear equations. The steady-state equations, known as the power flow or load flow equations, can be written for each bus i as

$$\begin{aligned} P_i &= V_i \sum_{j=1}^{n} V_j Y_{ij} \cos(\delta_i - \delta_j - \gamma_{ij}) \\ Q_i &= V_i \sum_{j=1}^{n} V_j Y_{ij} \sin(\delta_i - \delta_j - \gamma_{ij}) \end{aligned} \tag{1}$$

where P_i and Q_i are the real and reactive power injections, respectively, $V_\text{i}\angle\delta_\text{i}$ are the bus voltages (in polar coordinates), and $Y_\text{ij}\angle\gamma_\text{ij}$ are elements of the bus admittance matrix. Power flow studies normally specify real and reactive loads, generator real power outputs, and generator voltage levels. These equations can then be solved to determine the power flows and voltage levels throughout the transmission system. The most common solution method is based on the Newton–Raphson iteration or its derivatives. State-of-the-art commercial software can solve systems of tens of thousand buses within a few seconds on a desktop computer. Difficulties do arise in solving the power flow equations for unusual or highly stressed operating conditions resulting in either slow, or no, convergence to a solution.

If the solution to the power flow equations indicates that the steady-state currents and voltages are within equipment operating limits, then the transmission system has the nominal capacity to meet the demand. To satisfy the $(n - 1)$ criterion, repeated power flow studies are run for each significant outage under the base case scenario. Equipment limits are checked for each contingency solution. During the planning stage, these studies are based on projected peak demands and generally worst-case scenarios. These studies must consider the larger interconnected power system rather than just the local utility system, as the critical contingency or the necessary support may come from a neighboring system. If the $(n - 1)$ criterion is not met, transmission lines must be planned to ensure security.

In addition to the steady-state operation, the power system must survive dynamic events. During short circuits, the system is moved from its nominal operating point and will settle to a new operating point depending on the system dynamics. Because of the imbalance between the power input to the generator and the delivered electrical power arising from the disturbance, generators will deviate from synchronous speed, and the resulting frequency swing will cause power swings in the network. If these fluctuations are large, equipment limits may be breached and protective devices will disconnect equipment. Studies of such transient behavior primarily focus on the dynamics of generator units and their interaction with the network. Still, the load dynamics must be modeled accurately to study the system dynamics.

Models during the transient phase are governed by differential algebraic equations of the generic form

$$\begin{aligned} \dot{x} &= f(x, t) \\ y &= g(x) \end{aligned} \tag{2}$$

where $f(\cdot)$ represents the generator mechanical and electromagnetic dynamics and $g(\cdot)$ is the power flow equations. The dynamics can be highly nonlinear for large disturbances and so are analyzed by time domain numerical integration. The most commonly implemented approaches use both explicit integration, such as Euler or Runge–Kutta methods, or implicit methods, like trapezoidal integration. Typical studies focus on the first few seconds after a disturbance, when most instabilities occur; however, there are slower phenomena from seconds to several minutes that may develop into instabilities. Such instabilities may require not only new transmission but also new control and protection.

The preceding methodologies calculate the overall adequacy of the system but do not reflect problems at particular load points in the system. At the distribution level, the network is primarily radial with only secondary network redundancy, so there is a specific need to identify performance at different points in the system. Design for reliability in this case focuses on the ability to isolate faults by the protection system. Assessments at the distribution level are even more varied than the transmission level as both the number and type of customers takes on as much importance as the interrupted load. Distribution companies will assess performance in terms of outage duration, number of customer outages, types of interruptions (such as permanent or momentary), and the interrupted load.

It remains to be seen how transmission planning will be accomplished when the power industry is fully deregulated. It is expected that the transmission companies will remain regulated and the operation of the transmission within a particular region will be the responsibility of a neutral regulated party, who will ensure the security of the power system. What is not clear is whether there will be enough financial incentives in the generation market to build new transmission or whether regulations will be needed to force new transmission building under certain conditions. The cost of energy will certainly rise in an area where generation is in short supply, providing incentives to build new generating plants within the area or to build transmission lines to bring in excess capacity from a distant area. Since the return on transmission investment will probably be regulated while that on generation investment will be only subject to the market, the most advantageous regulations for the customer are still under discussion.

Operations Planning Techniques

While during the longer-term planning stages designers focus almost entirely on the peak demands, secure operation in the shorter term requires consideration of the specific load requirements. Loads are forecast for the day and week ahead on an hourly basis so that adequate generation can be scheduled to meet the demand and security requirements at the lowest cost. It is expensive to keep units on line, so some generators are shut down when their capacity is not needed. In practice, most systems consist of relatively inexpensive large units that operate base loaded all day. At peak demand times, more expensive "peaker" units may be started to fulfill the demands for short periods. In between, a variety of unit types may need to be cycled on and off. Figure 2 shows how such a pattern with the cycling units, illustrated by the dashed lines, meets the daily load cycle of the solid line. Obviously, an adequate number of units must be available to meet the load demand, and some longer-term scheduling of fuel, water, and maintenance is needed to ensure this.

The shorter-term scheduling of units to meet project loads is described in the next section. Once the units are scheduled, their effects on the transmission must be studied using power flow and transient stability programs to ensure secure operation. These studies are similar to the transmission planning studies mentioned previously except that the base cases are the worst loading scenarios projected for this shorter term, say one week. The usual ($n - 1$) criterion for withstanding single contingencies is often used to ensure security. After restructuring of the power industry, such studies to ensure security of the power system in the short term (i.e., day ahead) will be the responsibility of the independent system operator rather than the vertically integrated utility company.

Generation Scheduling. Generator units must be brought on line (referred to as the commitment) and the power outputs set (dispatched). The unit commitment problem determines the combination of on-line units that will minimize the cost of operation, which includes not only fuel costs but also fixed costs such as startup and shutdown, while meeting the specified demand and reserve requirements at each time step (usually an hour) of the study period. The constraints can be involved, allowing for different types of reserve (spinning and ready), fuel constraints, and ramping rates of the units. The costs can be written as

$$C = \sum_{t=1}^{m} \sum_{i=1}^{n} [C_e(P_i(t)) + C_f(U_i(t), U_i(t-1))] \tag{3}$$

where $C_e(P_i(t))$ is the fuel cost of energy production for unit i at time t and $C_f(U_i(t), U_i(t-1))$ is the fixed costs associated with a unit i with the unit on/off state represented by the binary variable $U_i(t)$. Fuel costs can be accurately modeled, as a quadratic function of power output or, as is often the case, by piecewise linear curves of the incremental cost. The study period for unit commitment is typically no more than one week.

Scheduling also includes a dispatch phase, which finds the specific generation outputs for each unit committed to meet the load most economically. This dispatch should satisfy the security constraints on the network flows. The optimal dispatch of the units under such constraints is referred to as security-constrained economic dispatch. If the voltage levels are considered as well, the formulation is referred to as *optimal power flow* to reflect the inclusion of the power flow equations. If in addition, security constraints are considered the calculations are referred to as a *security constrained optimal power flow*. Normally in the unit commitment phase, economic dispatch ignores the network constraints, which are later checked by power flow and stability studies; however, in some unit commitment programs a linearized load flow is used to perform a security-constrained economic dispatch. A full optimal power flow with or without security constraints, if performed at all, is left for hourly operations.

A simple way to commit units is simply to order units from least to most expensive. Such an approach, while simple, cannot guarantee optimality and leads generally to over commitment. For many, there were two fundamental methods for solving the unit commitment problem: dynamic programming and Lagrangrian relaxation. A full dynamic programming solution guarantees a global opti-

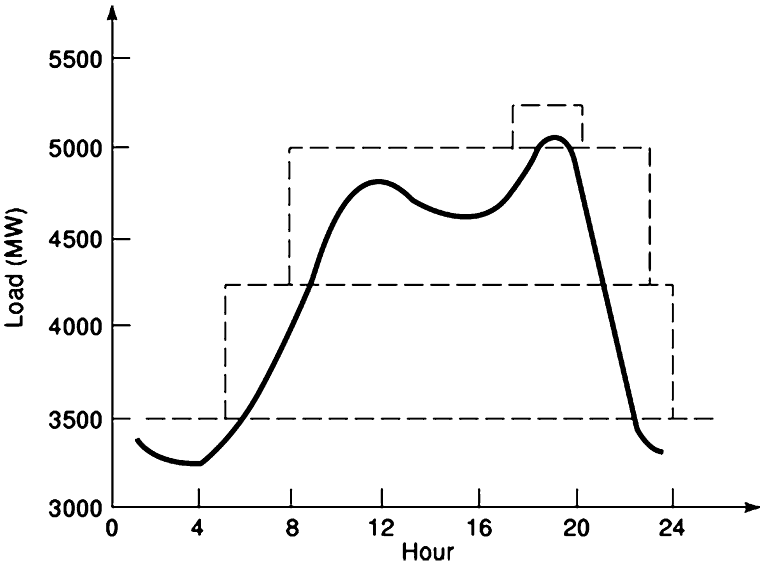

Figure 2. Unit commitment pattern.

mum but is extremely time consuming because the number of unit commitment patterns to consider dramatically increases with the number of units in a system, number of constraints, and length of the study period. Lagrangian approaches "relax" the unit coupling constraints, such as spinning reserve, allowing the problem to be solved one unit at a time by means of a single-unit dynamic program. Lagrangian relaxation methods are computationally efficient but cannot guarantee optimality. More recently, improvements in Mixed Integer Programming (MIP) algorithms have allowed this global optimization approach to become practical on large systems. The MIP approach is particularly attractive for electricity markets as the solution methodology is more transparent then the Lagrangian relaxation method, which provides assurance of fairness to market participants. Still, most utilities continue to rely on a combination of heuristics and these more systematic mathematical programming methods.

A further complication for scheduling considers fuel, or water in the case of hydroelectric plants, constraints. Many utilities enter into fuel contracts that determine the amount of fuel to be consumed over some time period. Scheduling over weeks or months attempts to utilize the available fuel as efficiently as possible. Similarly, hydro resources are necessarily limited and the scheduling of hydro-thermal systems requires scheduling over time to use the available water efficiently. In practice, every hydro system is different and governed by a complex set of multiple uses, including flood control, irrigation, navigation, fish migration, and so on. Schedulers seek to maintain specified reservoir levels and achieve the most effective use of the water resource. In either the fuel- or water-constrained case, studies over these longer periods do not normally model demand requirements on an hourly basis but rather schedule on a weekly basis months in advance.

Short-term generation scheduling has changed drastically under industry deregulation. The market is only aware of the bid prices, which may not be related to costs, uses these to minimize the market price, with typically the highest accepted bid setting the market-clearing price. Still, this optimizing procedure has similarities to that described above. Moreover, generation companies, particularly those with many units, will continue to have cost minimization as an objective.

Real-Time Operations

Secure operation of the power system in real time requires assessment of potentially rapidly changing system conditions. As conditions develop throughout the day, forecasted loads may be in error and unexpected equipment outages may occur. On the one hand, there is insufficient time to repeat the off-line planning studies, so those approaches must be simplified to allow approximate solutions that can be found rapidly. On the other hand, voltage and power flows can be measured and generator availability is generally known. Thus, the number of base case scenarios that must be considered is limited. As a result, statistical approaches are rarely employed; instead the focus is on finding critical contingencies. Real-time operation also depends to a great extent on operators, who, through experience, can quickly identify deteriorating conditions and steer the system away from vulnerable conditions.

Load Following. Although adequate generation capacity is scheduled to meet hourly load forecasts, the load fluctuates throughout the hour, indeed second to second, and the generated power must follow the changing demand. Any generation and load imbalance due to increasing load causes kinetic energy to be released (or absorbed for a load decrease) from generator rotating masses into the network. As this kinetic energy is released (or absorbed), the generators will decelerate (or accelerate). Rather than measuring each load and adjusting generators accordingly, which would be exceedingly difficult, turbine governors respond to these speed or frequency deviations and increase or decrease power output as appropriate. In general, governors in an area are adjusted to precise response characteristics governed by the expression

$$\Delta P = -\frac{1}{R}\Delta f \tag{4}$$

where Δf is the frequency deviation, R is a regulation constant, and ΔP is the change in mechanical power output of the turbine. This automatic governor action is the primary control that continuously corrects generation output to balance the changing loads.

The frequency deviations that control the governors are essentially constant throughout the interconnected system, so there is no direct way to determine the location of the load change from the frequency. As such, all generators react to the frequency deviation, which leads to unscheduled flows on the area tie lines. To maintain the tie schedules, power flow between areas is metered and governors on select units receive a centrally coordinated control signal. These secondary control signals, referred to *as automatic generation control* (*AGC*), are sent out to the generators every few seconds and add a tie line error component to Eq. (4) that ensures that each area meets its own load obligations. Less frequently, the governor set points will be adjusted so as to maintain the economic dispatch.

This continual matching of generation with the real-time load, known variously as *load-generation balancing, load following, regulation*, or *load frequency control*, is a necessary part of maintaining security of the system. However, it is not clear whose responsibility it will be when the vertically integrated utilities disappear. Obviously, the generation companies will have to provide this load following, and it is clear that they will have to be separately reimbursed for this ancillary service. The independent system operator, as the entity concerned with system security, is the obvious one to be responsible for obtaining this service from the generating companies and then exercising it by sending the control signals to the generators. However, in some cases, individual customers have been given the right to acquire this service directly from a generation company, the implementation of which will require a significant increase in real-time measurements and communication.

Reserves Checking. As the operating conditions change in real time, the prescheduled security constraints must be verified. Adequate generation reserves must be available to survive the most severe outages of generator units. Since new generation must be brought on within a limited amount of time, the reserves, in addition to sufficient quantity, must be sufficiently fast to be useful. For example, large units with slow ramp rates may not be effective as a reserve in an emergency situation. As determined by NERC, only the power that can be made available within 10 min can be considered as ready reserve. This may consist of the already synchronized spinning reserve plus any generation, like combustion turbines, that can be brought on line very quickly. The reserves are calculated in the control center by the generation monitoring programs, and operators are alerted to any shortages that develop. In addition, operators closely monitor the developing load conditions throughout the day to anticipate additional generator units that may need to be brought on line to maintain adequate reserves.

Static Security Assessment. Maintaining security of the power system at all times is the main responsibility of the operator. The long-term planning provides adequate reliability. The short-term operations planning ensures that there is enough generation and transmission capacity in the system to meet the projected conditions for the next day or week. In real-time, the control center computers automatically send out signals to the generators to follow load and also monitor for adequate reserves in case a generating unit is suddenly lost. The static security assessment program ensures that the loss of any equipment—a generating unit, a transformer, a transmission line, and so on—does not result in voltages beyond their operating limits and transmission lines beyond their loading limits.

The calculations needed for the static security assessment are exactly the same as described in the transmission planning section, where all possible single contingencies are studied by solving the power flow equations for each contingency on the base case. In real-time, the same contingency cases have to be studied, but for the real-time conditions. To do this a power flow solution that accurately portrays the real-time conditions must be obtained. This is done by using the real-time data measurements from the power system to obtain the best estimate of the system state variables, which are the bus voltages. To do this *state estimation* of bus voltages with reasonable accuracy requires the acquisition of real-time measurements with adequate redundancy. Many control centers are set up to do this state estimation every few minutes. Thus, a power flow solution, updated every few minutes, of the real-time conditions of the power system is then available in the control center to the operator.

The real-time conditions very seldom mirror any of the base cases that were actually studied off line. The off-line studies usually construct worst-case scenarios to develop operational guidelines, and by their nature they tend to be conservative. Thus, the operational limits obtained from off-line studies are often too restrictive or, in the case when the real-time conditions stray into totally unstudied areas, irrelevant. Thus the availability of a power flow solution of the real-time conditions makes it possible for the operator to obtain more realistic operational guidance. This can be done manually by the operator studying the effects of equipment outages one at a time, a procedure very useful if the operator is contemplating some switching operations and could check the aftereffects on the computer before actually doing them.

The main use, however, of the real-time power flow solution is the automatic assessment of the static security of the system. The computer automatically studies hundreds of possible contingencies that could happen on the power system and determines how well the system can withstand them. This is tantamount to running hundreds of power flow solutions and then checking for line loading or voltage violations to alert the operator, and it has to be done within a few minutes for the information to be useful. This is a computational burden in terms of both the number of power flow solutions and the data sifting needed for checking violations. Thus, much of the development of static security assessment tools in the last two decades has concentrated on making this computation more efficient.

Instead of finding full power flow solutions for all hundreds of contingencies, more approximate but fast solutions are obtained to determine which contingencies pose the biggest hazards. This calculation is known as *contingency screening.* Most of the time, for well-planned systems, single contingencies should not cause any limit violations, and the main purpose of the contingency screening is to isolate the very few problem cases from the hundreds of nonthreatening contingencies. In addition to running fast approximate solutions, the screening must evaluate these solutions by a severity index to determine which contingencies are the worst. These severity indices must reflect line overloads and voltage violations such that the contingencies can be ranked according to their severity. Once this is done, only the worst contingencies are further studied with accurate power flow solutions, and the resulting overloads and undervoltages are reported to the operator as alerting messages.

The static security assessment program is thus designed to alert the operator if a particular contingency would cause the system to violate operational limits. The operator, if so alerted, must then decide whether to take *preventive action* right away so that this contingency does not pose a problem or to take no action at present but be ready to take *corrective action* if the contingency does occur. In most cases of overloading or undervoltages, the operator usually has several minutes to take corrective action, and so the latter course is most often taken. This approach saves the operator from making expensive changes in the operating condition since contingency most likely will never occur. However, in some regions the operator must ensure no violations for single contingencies, and in that case the more expensive but secure preventive action must be taken whenever any contingency study detects limit violations.

Dynamic Security Assessment. The static security assessment checks for limit violations after outages but it assumes that the system reaches steady state after these outages occur. Since outages are usually the result of an accidental short-circuit, which causes the protective systems to isolate the short-circuited elements, the power system may experience significant excursions in the voltages and power flows during this disturbance. If the disturbance is severe enough, these swings may actually cause generators to become unstable (lose synchronism), in which case there would be widespread outages instead of the single outage expected.

The dynamic security assessment identifies those short circuits or contingencies that cause instabilities. For a properly planned system, no contingencies should make the system unstable if operated within its limits. However, as noted before, in real-time operation the power system does end up in conditions that were not anticipated when the planning was done. Thus, it is important to check whether contingencies can make the system unstable. The problem is that the stability calculations (described in the transmission planning section) are even more time consuming than the power flow calculations, and the on-line checking of stability for hundreds of possible contingencies is a daunting task.

Still, with the price-performance ratio of computers falling continually, dynamic security assessment has become a reality. Techniques learned from running static security assessment as well as new algorithms have been very useful in developing the dynamic security assessment tools. The concept of contingency screening to isolate quickly the worst contingencies also holds for dynamic security: Most of the contingencies will be stable, and the task is to isolate the few that are not.

Contingency screening requires a quick approximate method to determine the stability of the system. The traditional, and accurate, method is the time domain solution integrated over a long enough time period that allows the trajectories to portray stable or unstable behavior. The approximate methods developed so far calculate the time domain solution for only a short time, usually just beyond fault clearing, and then project the stable or unstable behavior from these trajectories by other calculations. The various techniques use transient energy and their margins, the equal area criterion, different coherency measures, and signal energy. These measures also provide the stability indices that can be used to rank the contingencies to determine the worst cases. Once the worst cases are determined, the traditional time domain solution can be used to determine accurately the stability of the system.

The techniques mentioned here work well for systems that are vulnerable to instabilities caused by the lack of synchronizing power. These instabilities occur quickly, within a second or so, and can be detected by a smaller amount of calculations. Several experimental programs are now operating in various parts of the world, and commercial packages for control centers are now available. Instabilities occurring after several oscillations because of negative damping, like those in the western United States, are difficult to detect without detailed and longer simulation or by modal analysis. For these kinds of systems, on-line dynamic security assessment is still not available, and conservative operating limits calculated off line are the only answer.

In those rare cases where the dynamic security assessment detects instabilities, the operator, once alerted, needs to take preventive action. This is because once the contingency occurs, the onset of instability is very rapid and there is no possibility of the operator taking manual corrective action after the fact. In some cases, the operator may be able to arm special protection devices to shed load or generation that ensures stability. More commonly, the preventive action available to the operator is modification of the generating pattern. Since this invariably increases the cost of operation, researchers are trying to find methods to calculate quickly the minimum changes required to maintain stability for a particular contingency. Often, the simplest way to do this is by recalculating the power flow limits on a particular transmission corridor.

Voltage Stability Assessment. A different case of instability is when the voltage becomes unstable, known as *voltage collapse.* Unlike the generator shaft instability mentioned previously, which is caused by an imbalance in real power in the system, the voltage collapse is caused by the imbalance of reactive power in an area of the system. Voltage instability can occur very slowly, and so the same techniques used in dynamic security analysis do not work well in detecting voltage collapse. Thus, voltage security analysis requires separate programs.

The main off-line tool used to study voltage collapse is the continuation power flow, which uses a special technique to obtain convergence of the power flow solution near voltage collapse conditions. This provides a method to determine the limits for avoiding voltage collapse. Proposals to use this same technique on line have been made, but actual implementation in the control center is not common. In addition, it has been recognized that the static and dynamic security assessment tools also provide much information about the voltage behavior of the real-time system under contingencies, and this should be used to predict voltage collapse. For example, the static security assessment does calculate the voltages for each contingency, and voltages that are particularly low may indicate that the system is near the voltage collapse limit. If the power flow does not converge for a contingency, it may be an indication of voltage collapse and should be studied by the continuation power flow.

CONCLUSION

Maintaining the security of the power system requires adequate planning and proper operational procedures. The 1965 blackout of the Northeastern United States and Canada brought about methods for ensuring security, and similar methods have been adopted by all countries whose economies have become more dependent on the reliable supply of electricity. These methods, as described in this article, have worked well for vertically integrated utilities that were responsible for generating, transmitting, and distributing electricity to customers.

As the structure of the electric supply industry around the world is changed to foster more competition, such change must be accomplished without compromising security of supply to the customers. Thus, the methods developed over time must be adapted to the new structure. This has been recognized in all the countries that are changing the rules that regulate the power industry, and the responsibility to maintain overall system security is being largely assigned to the entity in charge of operating the transmission grid (while the reliability of supply to the individual customer will remain with the distribution company or the retail supplier). However, the authority of the transmission grid operator, especially over the generating companies and electricity traders, is evolving over time and the ability of the operator to maintain security will be affected by this authority.

BIBLIOGRAPHY

1. R. Billinton and R. Allan, *Reliability Evaluation of Power Systems*, Pitman Publishing, London, 1984.
2. C. B. Lankford, J. D. McCalley and N. K. Saini, Bibliography on transmission access issues, *IEEE Transactions on Power Systems*, pp. 30–40, Feb. 1996.
3. P. Kundur, *Power System Stability and Control*, McGraw-Hill, New York, 1994.
4. A. Wood and B. Wollenberg, *Power Generation Operation and Control*, John Wiley and Sons, New York, 1984.
5. V. Brandwajn, A. B. R. Kumar, A. Ipakchi, A. Bose and S. D. Kuo, Severity Indices for Contingency Screening in Dynamic Security Assessment, *IEEE Transactions in Power Systems.*, vol. 12, No. 3, pp. 1136–1142, August 1997.
6. C. A. Castro, A. Bose, E. Handschin and W. Hoffman, Comparison of Different Screening Techniques for the Contingency Selection Function, *International Journal of Electrical Power & Energy Systems*, vol. 18, No. 7, pp. 425–430, October 1996.
7. N. J. Balu, T. Bertram, A. Bose, V. Brandwajn, G. Cauley, D. Curtice, A. Fouad, L. Fink, M. G. Lauby, B. F. Wollenberg and J. N. Wrubel, On-line Power System Security Analysis, Invited Paper, *Proceedings of the IEEE*, vol. 80, No. 2, pp. 262–280, February 1992.

ANJAN BOSE
KEVIN TOMSOVIC
Washington State University,
Pullman, WA