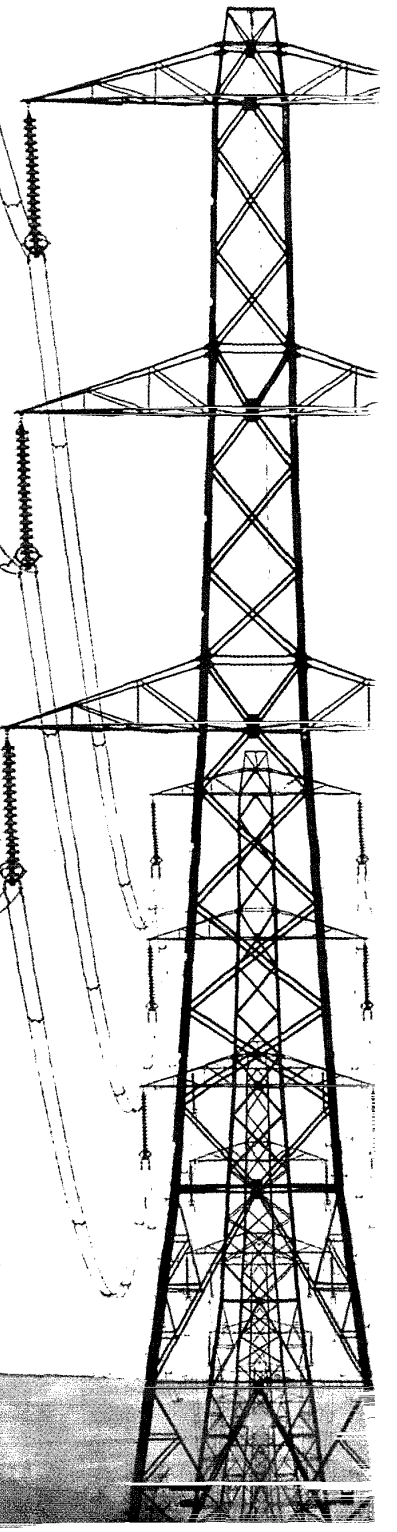
Power system security



Incidents on the electricity transmission system have a low probability but a high impact. All phenomena that have this characteristic are difficult to analyse. When a major problem has not happened for a long time, there is a natural tendency to wonder if the security measures are not too strict.

by Daniel S. Kirschen

According to the latest OFGEM report on the performance of the transmission and distribution systems in Great Britain,[1] each customer was without supply for an average of 86 minutes. Problems due to the transmission system or the generating plants accounted for only about 1 % of this unavailability. At first glance, we could therefore conclude that the performance of the transmission system is so good that we need not devote too much effort and resources to making sure that the level of security does not deteriorate. Such a conclusion, however, would be completely erroneous.

To convince ourselves of the importance of remaining vigilant about the security of the transmission system, let us consider the following scenario. Imagine that around 8:30 am on a cold Wednesday morning, an unpredictable failure compounded by plain bad luck causes the collapse of the entire power system of Great Britain. Millions of commuters are stuck in enormous traffic jams or left stranded on the rail network. Those who manage to get to work are sent home because the offices are dark and the factories are silent.

Meanwhile at the national control centre and at stations and substations around the country, engineers are working diligently to restore the power system to its normal state. The task they face is huge and complex. All the power plants have been shut down by their protection system during the collapse and need to be resynchronised. Restarting a thermal plant requires a substantial amount of power that must be brought in from the small number of plants that have black-start capability. In addition, the transmission network does not behave as it usually does because very little load and very few plants are connected. Because large overvoltages and wild frequency fluctuations could damage the equipment or cause disastrous setbacks in the restoration process, the operators work very cautiously.

If everything works according to plan, all consumers could be reconnected within 8-10 hours. On the other hand, since the system is mostly thermal and since there is no hands-on experience with a full-scale black-start restoration in Great Britain, the potential for delays and mishaps is substantial. It is therefore possible that some consumers may have to wait almost a whole day before normal service resumes.

The bottom line is simple and stark. A single blackout could easily cause the equivalent of 10-20 years' worth of 'normal' unavailability in one day. In monetary terms, the cost would be even higher. The cost to users of supply interruptions is normally calculated by multiplying the energy not served by a factor called the 'value of lost load' (VOLL), which is determined using customer surveys.[2] This approach does not fully represent the massive disruptions caused by a large-scale blackout. To get a rough idea of the numbers involved, consider that there would be virtually no economic activity for one day and that a substantial part of the next day would be devoted to cleaning up and restarting business and industrial processes. The economic cost of a one-day blackout could amount to about 0·5 % of GDP. In addition, social costs might include deaths and injuries attributable to the lack of electricity supply as well as the consequences of the acts of vandalism and civil disturbances that might arise.

If this scenario seems far-fetched, consider Table 1, which lists some of the major blackouts that have affected power systems industrialised magnitude see be

Secruity in the end depends on the way a power system is operated

completely, even in a system such as Britain's, which has never suffered a complete blackout since it was interconnected.

This impressive record is not due simply to the number of transmission lines that are in service or the total capacity of the reactive support equipment that have been installed. Just like a bicycle can be ridden safely and a lorry can be driven recklessly, what counts in the end is the way a power system is operated. In the remainder of this article we will take the perspective of system operators who are in charge of a power system whose structure and components they cannot change. If operators push this system too hard, in other words if they make it carry more power than it can handle, it may collapse either totally or partially. On the other hand, if they are too cautious, they will not deliver the full economic benefits of electrical energy. Somewhere between these two extremes, there must be an optimum.

Outage mechanisms

In a system that consists of tens of thousands of components, the failure of a single component is not a rare event. This is particularly true if some of these components (such as the transmission lines) are exposed to inclement weather conditions and others (such as the generating plants) are subjected to repeated changes in operating temperature. Under normal conditions, the failure of a single element of a power system does not have wider repercussions. The faulted or failed component is taken out of service and the system continues to operate normally while the failed component is repaired or replaced. Occasionally, however, one of these random and unavoidable failures triggers a sequence of events that leads to a partial or total collapse of the power system. Before discussing how to measure and maintain the security of a power system, it is useful to review the various mechanisms that could cause load disconnections.

Table 1 Some of the large disturbances that have affected the power systems of industrialised countries (part of the information was obtained from Reference 3)

country or region	year	loss of demand
New England	1965	100 %
New York City	1977	100 %
France	1978	75 %
Greece	1983	100 %
Sweden	1983	63 %
Netherlands	1984	100 %
Portugal	1985	100 %
United Kingdom	1986	16 %
Tokyo	1987	21 %
Belgium	1990	78 %
Spain	1993	15 %
Israel	1995	70 %
western USA	1996	4750 MW

Frequency collapse

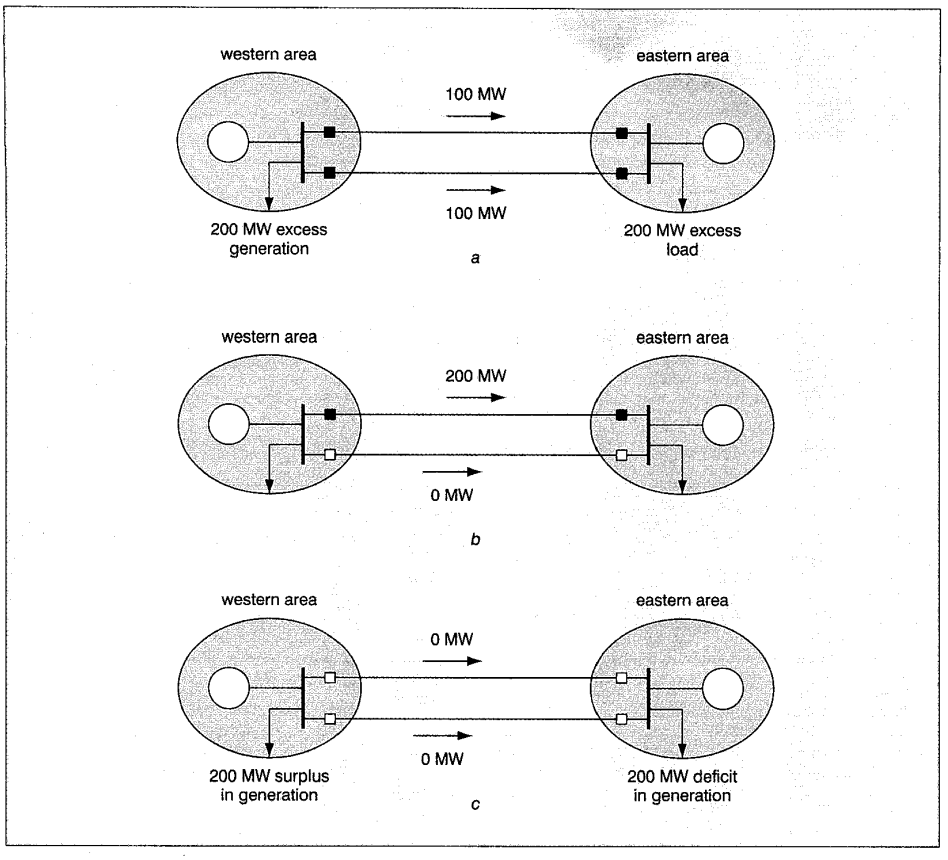
If a large and fully loaded generating plant is suddenly disconnected from the rest of the power system, the amount of power produced no longer matches the load. This deficit draws down the kinetic energy stored in the rotating machines connected to the system. As the rotational speed of these machines decreases, the frequency of the system drops. If the load/generation balance is not restored quickly enough, the frequency may drop to the level where the protection relays of some generators disconnect them from the system to protect these valuable assets from damage. These disconnections exacerbate the deficit of generation and the possibility of collapse.

Cascading thermal overloads

Consider the simple example shown on Fig. 1. Two identical 100 MVA transmission lines connect the western and eastern areas of a power system. If generation in the western area is much cheaper than in the eastern area, economics make it desirable to transmit power from west to east using the two transmission lines. Under normal conditions, each of these lines could carry up to 100 MW. However, if the system is operated in this fashion and one of the lines fails, the loading on the remaining line suddenly jumps to twice its thermal rating. This line is now severely overloaded and begins to sag. Within minutes its clearance drops below the safe level and a second fault occurs, severing the remaining tie between the two parts of the system. The eastern area of the system suffers from a generation deficit that might cause a frequency collapse.

Transient instability

The power transfer capacity of the transmission system decreases significantly during a fault. Some of the generating units will therefore be unable to inject into the system all the mechanical power supplied by their prime mover. This excess energy is transformed into kinetic energy and these generators accelerate. Once the fault is cleared, the transmission system recovers some of its transmission capacity. Under normal circumstances, the generators that have started accelerating slow



1 Simple example illustrating cascading thermal overloads: (*a*) Pre-fault conditions; (*b*) Post-fault conditions; and (*c*) Conditions after the thermal overload trip

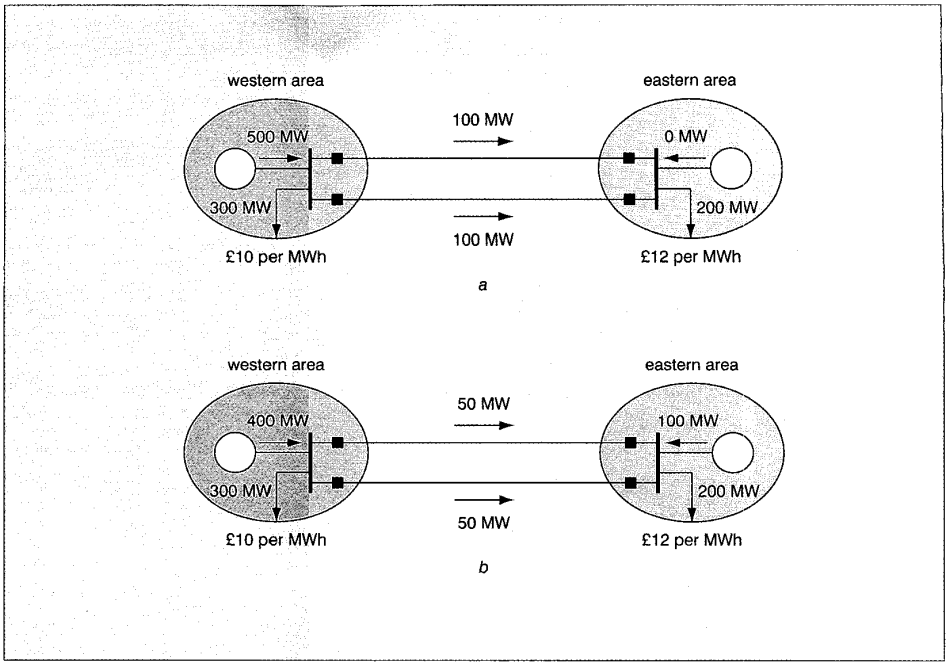
down and the system recovers a uniform frequency. On the other hand, if the system is heavily loaded, it may not be able to handle the power transfers required to decelerate the affected generators. The differences in voltage angle between different parts of the system may continue to increase. Various protection devices would then detect an abnormal situation and would act to safeguard the equipment. Groups of generators may be shut down or split from the rest of the system. Other parts of the system may be left with large generation deficits. The frequency in these islands would then quickly collapse.

Voltage instability

In addition to the well-known active power balance, the steady-state operation of a power system requires a balance between the reactive power consumed and the reactive power produced. Under heavy load conditions, most of the reactive power is consumed as I^2X losses in the transmission lines and the transformers. The generators and the reactive compensation devices must supply these reactive losses. If the reactive power needed in a given area cannot be supplied by a local source, the voltage in this area will drop to make possible the import of reactive power from other sources. Under heavily loaded conditions, the sudden outage of a transmission line or of a generator may put the system in a state where it cannot supply the reactive power needed to maintain the voltage. As the system tries to supply more reactive power, the voltage drops, further increasing the need for reactive power. If the load consists in large part of induction motors (e.g. those used for air conditioning), such a voltage collapse may take only a few seconds. A collapse could also be driven by on-load tap-changing transformers trying to maintain the distribution voltage constant. In this case, the process may take up to 20 minutes, giving the operator at least a chance to take corrective actions.

Hidden failures

Modern power systems are equipped with a variety of protection devices designed to identify dangerous situations and isolate the affected equipment quickly. Most of the time these devices operate as expected and therefore help maintain the stability and security of the



2 Simple example illustrating the cost of re-dispatching for security purposes: (*a*) Economic dispatch: total cost = £5000; and (*b*) Secure dispatch: total cost = £5200

system. Occasionally however, in response to a disturbance in the system, the protection system malfunctions and disconnects a healthy piece of equipment in addition to the faulted one. Such a malfunction transforms what should be a routine fault clearing into a major incident because two components are disconnected rather than one. If this double disconnection occurs when the system is under stress, it can trigger a voltage collapse or a cascading thermal overload. Protection malfunctions are caused by hidden failures, i.e. defects in the protection system that remain hidden until they are exposed by a fault or other abnormal condition. A study[4] of significant disturbances reported to the North American Electric Reliability Council for the period from 1984 to 1991[5] indicates that the protection system was a contributing factor in almost 70% of all major disturbances.

Providing security

Since it is impossible to eliminate completely random faults and failures, measures must be taken to reduce the likelihood that disturbances degenerate into major incidents involving the disconnection of consumers. We will therefore define power system security as the ability of the system to withstand unexpected failures and continue operating without interruption of supply to the consumers. A power system can never be totally secure. It is always possible to devise a sequence of events that will lead to a total or partial collapse of the system. The probability of such a sequence of events may be very small but it will never be zero. At the other extreme, a power system operating on its stability limit has zero security because any deterioration in its condition (such as the outage of a component or a small increase in load) will result in the disconnection of at least some consumers.

There are various types of actions that the operator of a power system can take to improve the security of the system in its charge. These measures can be classified in terms of their cost and in terms of the time at which they are implemented.

Cost-based classification

As we concluded from the discussion of the mechanisms that lead to major incidents, the security of the system is reduced when active power transfers are high and when reactive support is insufficient. Actions that affect the provision and flow of reactive power have an almost negligible cost compared to actions involving active power because no energy needs to be consumed to produce Mvars. When an operator is concerned about a potential voltage problem, the first thing that he or she will do is thus to adjust the transformer taps or the voltage set-points of generators and

SVCs (static var compensators) to improve the voltage profile and increase the reactive reserve.

Unfortunately, these cost-free measures are often ineffective or insufficient to correct security problems. The operator is then forced to use the active power controls. The only one of these that is cost-free is the adjustment of taps on quad-boosting transformers. By introducing an artificial difference in voltage angle between its two terminals, a quad-boosting transformer provides a direct mean of controlling the flow of active power. By directing this power away from overloaded areas, the operator can improve the security of the system.

When these adjustments are not sufficient, the operator has to change the active power produced by the various generating plants connected to the system. If security were not an issue, the market for electrical energy would determine the output of these plants. This dispatch would thus reflect the competitiveness of each plant. If this economic dispatch is not secure enough, the system operator must modify it by intervening in the market. This intervention always involves buying energy from more expensive generators to replace energy from less expensive generators.

Let us revisit the example that we used to illustrate the consequences of cascade thermal overloading. Suppose, as shown in Fig. 2(*a*), that the price of energy produced in the western area is £10 per MWh, while the price of energy produced in the eastern area is £12 per MWh. Under these conditions, the most economic way to operate the system is to produce all the power from generation in the western area and to import 200 MW into the eastern area to cover the local load. As we saw above, this situation is not secure because a fault on one of the lines would lead to a cascading thermal overload and a blackout of the eastern area. The power transferred through the two lines must be reduced to a total of 100 MW by increasing the generation in the eastern area and reducing the production in the western area. This more secure, but more expensive, dispatch is illustrated in Fig. 2(*b*).

As our example shows, it is easy to see how redispatching active generation directly reduces the risk of cascading thermal overloads. Reducing the flow of active power also improves the security of a power system that might be vulnerable to transient or voltage instability. Given the characteristics of the system, it is possible to calculate the maximum amount of power that can be transferred without unduly endangering the security of the system. Sophisticated transient and voltage stability analysis programs have been developed in recent years to calculate these limits accurately.

Transmission lines and other transmission equipment are normally taken out of service only when they need to be maintained. Cancelling the maintenance on some equipment so it can be returned to service increases the transmission capacity of the system and therefore reduces the amount of generation that needs to be re-dispatched to maintain security. In the short run, delaying maintenance can therefore be a cost-free security action. Maintenance, however, cannot be postponed for ever without increasing the risk of failure. The schedule of equipment maintenance should be developed in such a way that the most critical equipment is taken out of service only when its unavailability does not impose a very costly, security-driven redispatching

We can therefore conclude that, notwithstanding the provision of reactive support and the intrinsic 'strength' of a power system, security considerations always impose a limit on the amount of power that can be transferred and often require a generation dispatch that is not the most economic one.

Timing-based classification

Security measures can also be divided into preventive, corrective and desperate actions. Preventive actions are intended to help the system ride through possible disturbances without immediate operator intervention. Since disturbances can occur at any time, preventive actions must be in effect at all times. Preventive measures that involve redispatching generation are thus very costly. It would be preferable to maintain the security of the system by reacting to unanticipated events. The cost of such corrective actions is much lower because they are implemented only when needed.

Going back to the example of Figs. 1 and 2 we see that, if it were possible to increase the generation in the eastern area to relieve the cascade overloading before it causes the second line to trip, we would not have to deviate from the economic dispatch. Even if the price of the energy provided by the generation in the

Security factors always impose a limit on the amount of power that can be transferred

There is a limit to what can be achieved with corrective actions

eastern area during the emergency were much higher, the overall cost would be lower because this cost would have to be paid only infrequently. There is unfortunately a limit to what can be achieved with corrective actions. The output of most generators cannot be increased fast enough to relieve an overloaded piece of equipment before it is damaged or tripped.

Conventional corrective actions have an even lower effectiveness when voltage or transient instability is a problem. Load shedding provides a much faster way to reduce the active power flow through a weakened corridor. If a network operator can enlist enough consumers by giving them sufficient financial incentives to agree to have their supply interrupted during emergencies, it might be able to significantly reduce the cost of preventive security measures. There are, however, practical limitations to the implementation of such schemes. First, the customers must be located in the right area. Second, the network operator must have a way to trigger these load sheddings without delay and must be confident that the load reduction will take place as expected in the event of an emergency. This is difficult if these corrective load sheddings involve more than a few large industrial customers.

Corrective load sheddings should not be confused with the desperate actions that system operators have to resort to when preventive and corrective measures prove insufficient in the wake of a larger than expected disturbance. The goal of these desperate actions is to save the system by shedding significant amounts of load in critical areas. Such measures are taken in the hope of stopping the spread of the disturbance. Unlike the consumers who voluntarily agree to the interruptible contracts that underpin corrective load shedding, the victims of these desperate actions are usually not compensated.

Measuring security

The definition of security that we have used so far is purely qualitative. If we want to proceed further in our analysis, we must be able to measure security. This requires that we adopt either a gauge or a ruler. If we adopt a gauge, we will get a binary assessment of security. In other words, we will only be able to say whether our system is secure or not secure. On the other hand, if we develop a suitable ruler, we will have a continuous measure of the level of security in the system. Let us take a look at the principles, techniques, advantages and disadvantages of both approaches.

Binary security assessment

It is intuitively clear that single contingencies (i.e. losing a single piece of equipment because of a fault) are much more frequent than multiple contingencies. Binary security assessment takes this observation to the extreme. It postulates that the probability of two simultaneous independent faults or failures is so small that such events do not deserve to be considered. The set of credible contingencies therefore typically contains the outage of all network components (branches, generators and shunt elements) taken separately. In Britain, since most transmission corridors consist of two parallel circuits strung on the same towers, the simultaneous outage of both circuits due to a problem with one of the towers is considered credible.

This clear but artificial distinction between credible and non-credible outages makes possible a very simple form of security assessment. At any given time, to be considered secure, a power system must be able to withstand all of the credible contingencies. None of these contingencies should result in a thermal overload or the violation of a voltage or transient stability limit. If one or more of the credible contingencies would result in an unacceptable operating state, the system is deemed insecure. Preventive action must then be taken to change the system's condition in a direction such that no credible contingency causes a violation of the operating limits.

This approach to detecting possible security problems works only if the set of credible contingencies is clearly delineated. Enlarging the set to include less credible contingencies would lead to the detection of more and more 'problems' and require possibly contradicting adjustments to the state of the system. Binary security assessment thus provides unambiguous answers fairly quickly. On the other hand, it ignores the stochastic nature of the faults and failures that affect power systems. All credible contingencies are given the same weight, irrespective of the nature of the outaged component, its length and its exposure. At times, the security threshold that it enforces will be too strict because it treats all events as equally likely.

A considerable amount of money may therefore be spent on preventive actions that are required because a credible but unlikely

contingency would violate one of the security limits. For example, the probability of a fault on a short line in good weather conditions may be very low and it may not be worth protecting the system against its potential outage. On other occasions, the system may collapse because the security assessment did not consider the possibility of multiple outages caused by hidden failures.

Continuous security measurement

To remedy the limitations of binary security assessment, we need to put security analysis on a firmer theoretical footing. This means recognising that security analysis should be done on a probabilistic and not a deterministic basis. Rather than classifying a contingency as credible because it involves only one component and another as non-credible because it involves two, we should attach a probability to each contingency. Since we are not limiting ourselves to a moderately small set of contingencies, we can no longer assume that the system is secure unless a contingency results in conditions that violate the normal operating limits.

There will indeed always be combinations of outages that will force some load disconnection. Such contingencies may have very low probabilities but they exist and the system would thus always be considered insecure. We therefore need to define a ruler that will give us a continuous measure of the security of the system. This measure should combine the impact on the system of each contingency. To reflect the probabilistic nature of this approach, the impact of each contingency should be weighed by its probability.

But how do we measure the impact of a contingency on the system? When the concepts of power system security were developed in the 1960s, cascading thermal overloads were the primary concern of power system operators. In that context, it made sense to assess security on the basis of branch overloads because these overloads would ultimately cause the branch to trip. Nowadays, thermal overload is often less of a problem than voltage or transient instability. Extending the measure of security to include violations of voltage limits does not make sense because an under-voltage condition will not necessarily result in a voltage collapse. It seems more appropriate to measure the impact of a contingency by the actual damage that it produces, i.e. by the amount of load disconnection that it might cause. If we factor into our calculation the time required to restore the load following its disconnection, this index of security is similar to the Expected Energy Not Served (EENS) index that has been used by planning engineers for some years.

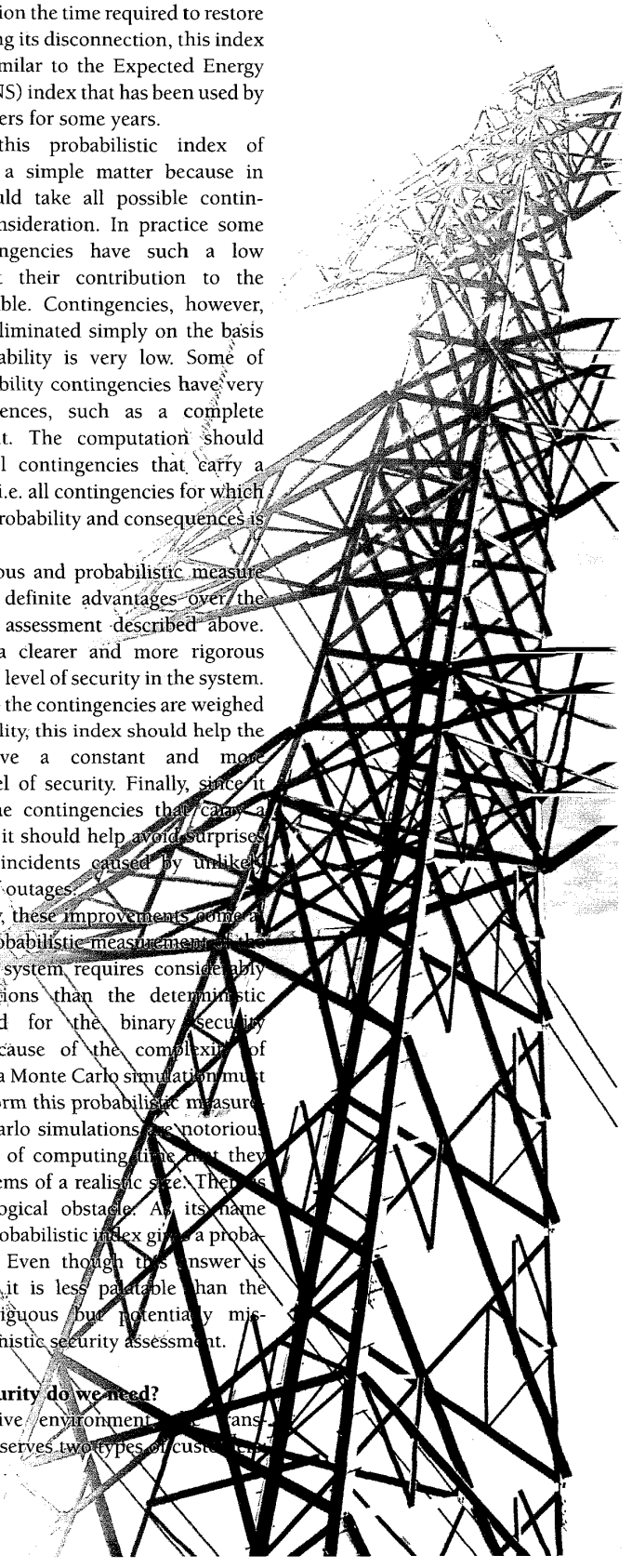
Calculating this probabilistic index of security is not a simple matter because in theory we should take all possible contingencies into consideration. In practice some of these contingencies have such a low probability that their contribution to the index is negligible. Contingencies, however, should not be eliminated simply on the basis that their probability is very low. Some of these low-probability contingencies have very severe consequences, such as a complete system blackout. The computation should thus include all contingencies that carry a significant risk, i.e. all contingencies for which the product of probability and consequences is not negligible.

This continuous and probabilistic measure of security has definite advantages over the binary security assessment described above. First, it gives a clearer and more rigorous indication of the level of security in the system. Second, since all the contingencies are weighed by their probability, this index should help the operator achieve a constant and more appropriate level of security. Finally, since it considers all the contingencies that carry a significant risk, it should help avoid surprises such as major incidents caused by unlikely combinations of outages.

Unfortunately, these improvements come at a price. This probabilistic measurement of the security of the system requires considerably more computations than the deterministic procedure used for the binary security assessment. Because of the complexity of power systems, a Monte Carlo simulation must be used to perform this probabilistic measurement. Monte Carlo simulations are notorious for the amount of computing time that they require for systems of a realistic size. There is also a psychological obstacle. As its name indicates, the probabilistic index gives a probabilistic answer. Even though this answer is more rigorous, it is less palatable than the simple, unambiguous but potentially misleading deterministic security assessment.

How much security do we need?

In a competitive environment, a transmission system serves two types of customer:



Secruity is at least 100 times more valuable to consumers than it is to generators

the generators that inject power into the system and the consumers that extract it. It is in the interest of both types of users that the transmission system be able to withstand disruptions. If a generator is disconnected because of an incident in the transmission system, it loses the revenue from the sale of electricity. Using data from the Electricity Pool of England and Wales for 2000, this loss would be about £24 per MWh. The net loss will usually be much smaller because the generator does not incur the fuel costs for the duration of the disconnection. By comparison, the official estimate of the average loss to the consumers (i.e. VOLL) is of the order of £2800 per MWh. On average, security is thus at least 100 times more valuable to consumers than it is to generators.

This average clearly masks a wide variety of valuations. The cost of an interruption on an industrial process is considerably higher than the monetary equivalent of the nuisance caused to residential consumers. While it would be economically desirable if those who put a higher value on the continuity of supply paid more for security, this is not currently feasible. Incidents in the transmission system affect fairly large areas. Given the current state of the technology, it is not possible during a system collapse to isolate or treat differently a class of consumers that may be spread across the network. A higher degree of security therefore cannot be delivered to consumers who might be ready to pay for it.

Security is thus a system issue and the appropriate level of security must be determined on a system-wide rather than an individual customer basis. The regulator, acting on behalf of all consumers, has to decide what this level should be. To reach this decision, the cost of security must be balanced against the benefits it provides. Security should be increased up to the point where the incremental cost of security is equal to the incremental value it delivers. In other words, an additional £1 spent on security should save at least £1 in outage costs. The incremental cost of security is simply the difference in cost between a more secure and a less secure dispatch. Computing the incremental value of security is considerably more complex. Since security is provided to prevent outages, its value is equal to the cost of the avoided outages. Incidents in a power system being stochastic events, the best we can obtain is an expected value of the cost of avoided outages.

We can use this cost/benefit approach to evaluate different security criteria. However, as discussed above, these fixed criteria do not provide an optimal level of security under all circumstances. Ideally, this cost/benefit analysis should be performed close to real time, when the operating state of the power system and the weather conditions can be predicted with more accuracy. It might then be possible to decide which operating plan is likely to have the lowest total cost, where the total cost is defined as the operating cost plus the expected cost of outages.

Conclusions

Incidents on the transmission system have a low probability but a high impact. All phenomena that have this characteristic are difficult to analyse. When a major problem has not happened for a long time, there is a natural tendency to wonder if the security measures are not too strict. This article has tried to clarify the concepts and principles that must be understood if this question is to be answered rationally.

The behaviour of power systems is complex, particularly when they operate under abnormal conditions. Analysis tools have become much more sophisticated over the last few years and the enormous improvements in computing speed make possible the consideration of a much larger number of possible scenarios. There is, however, a considerable amount of work that remains to be done before we will be able to handle properly the stochastic nature of major incidents.

References

1 OFGEM: Report on Distribution and Transmission Performance 2000/2001, January 2002
2 KARIUKI, K. K., and ALLAN, R.N.: 'Evaluation of reliability worth and value of lost load', *IEE Proc.—Gener. Transm. Distrib.*, March 1996, **143**, (2)
3 KNIGHT, U. G.: 'Power systems in emergencies' (John Wiley & Sons, Chichester, UK, 2001)
4 TAMRONGLAK, S., HOROWITZ, S. H., PHADKE, A. G., and THORP, J. S.: 'Anatomy of power system blackouts: preventive relaying strategies', *IEEE Transactions on Power Delivery*, April 1996, **11**, (2), pp. 708-715
5 North American Electric Reliability Council: 'Disturbances analysis working group database', http://www.nerc.com/dawg/

Dr. Daniel Kirschen is with the Department of Electrical Engineering & Electronics, UMIST, PO Box 88, Manchester M60 1QD, UK, e-mail: D.Kirschen@umist.ac.uk