An Overview of Risk Based Security Assessment

James D. McCalley, Sr. Mem. *jdm@iastate.edu*
Vijay Vittal, Fellow *vvittal@iastate.edu*
Iowa State University
Ames, Iowa

Nicholas Abi-Samra, Sr. Mem. *nabisamr@epri.com*
Electric Power Research Institute
Palo Alto, California

Abstract: We describe weaknesses in using deterministic methods for performing security assessment for bulk transmission systems. We also present motivation for using probabilistic risk and provide fundamental relations for making the associated calculations. The benefits and applications of using a risk index for security assessment are discussed, and an illustration is provided for line overload security assessment in the operational context.

Keywords: transmission, security assessment, probabilistic risk, overload, voltage security, dynamic security.

1 Introduction

Identifying various alternatives to problems and choosing from among them, so as to make decisions "now" for an uncertain future, is a challenging task for today's technologically evolved society. Information management, uncertainty handling, and decision making are mature sciences in many spheres, among which are nuclear power, the actuarial industry, financial markets, process control, and the aerospace industry. Many people refer to it as decision analysis. A central feature of this science is the ability to quantify and manage *risk*. In this paper, we advocate use of probabilistic risk for assessing security in bulk electric power systems, and we provide a framework for this that satisfies both operations and planning needs.

Power system reliability, once mainly the domain of planning and operating engineers within the utility, now must involve a diverse group of people. These people represent the interests and needs of transmission owners, system operators, energy sellers, large industrial customers and other end users, regulators, reliability councils, security centers, manufacturers, marketers, scheduling coordinators, and power exchange personnel. In parallel with the increase in the diversity of participants, the conditions under which power systems are operated have also become more diverse. Transmission loading patterns differ from those for which they were originally planned, and the ability to monitor and control them has increased in complexity. High uncertainty is a characterizing feature of this complexity, and the ability to obtain, manage, and use large amounts of information has become the primary means of handling the uncertainty.

Reliability is at the heart of the discussion about changes in industry structure - restructuring - and concern for it has been a primary reason why changes have not proceeded more rapidly. These concerns have been well founded, as significant deterioration in reliability levels could have social and economic consequences that directly counter benefits of decreased energy costs brought about by competition.

Within the network, an individual disturbance resulting in a cost consequence may occur for a number of reasons at any time. The disturbance may result in overload, voltage collapse, or transient instability, drawing the prevailing system to an uncontrollable cascading situation leading to widespread power outages. To maintain system reliability under uncertainty, studies are performed to aid in operating and planning decisions. The current practice uses deterministic methods with significant safety margins to cover "all" the possible unknown uncertainties. This means that power engineers propose a strong system and then operate it with large security margins. Though investment and operational costs are relatively high, this has resulted in a corresponding high reliability level in most power systems.

The power system, however, has shifted from a regulated system to a competitive, uncertain market environment. This has led engineers to face more pressure, from economic imperatives in the marketplace, to operate power systems with lower security margins. To operate the system closer to the traditional deterministic limits, or even beyond them, more refined methods for power system security assessment are needed that account for the probabilistic nature of uncertain variables in the decision-making environment. This paper motivates and describes an assessment framework that does this called *Risk Based Security Assessment* (RBSA). The overview provided here is of the specific framework developed by the authors; we do not attempt to survey other approaches that have been reported in the literature.

2 Security Assessment

We begin by focusing our discussion of "reliability" on the more narrow term "security." This term reflects the part of reliability that pertains to study and prevention of undesirable consequences following unforeseen outages, and it identifies the area to which we will apply RBSA.

Security has been considered one aspect of reliability, with the other one being adequacy. Generally accepted definitions of security and adequacy are given by the North American Reliability Council (NERC) Planning Standards [1]: *Security* is the ability of the electric systems to withstand sudden disturbances such as electric short circuits or unanticipated loss of system elements. *Adequacy* is the ability of the electric systems to supply the aggregate electrical demand and energy requirements of customers at all times, taking into account scheduled and reasonably expected unscheduled outage of system elements.

In this paper, we address the manner in which *the potential* for outage events influences operating and planning decisions. We heavily use the label "security," interpreting the term as the ability of the system to withstand sudden disturbances in terms of three types of problems that can result from these disturbances: circuit overload (lines and transformers), voltage problems (low voltages and collapse), and dynamic problems (early swing transient instability and oscillatory instability). We include these problems under the same umbrella because our intent is to develop an assessment

0-7803-5569-5/99/$10.00 © 1999 IEEE

framework to encompass all of them. In this paper, further references to "security" refer to this conceptualization.

2.1 Security States

One notion of security "states" was proposed in [2]. Here, it was considered that the power system always resides in one of four states: normal, alert, emergency, or restorative, where the emergency state could be extreme, temporary, or controlled. These states are distinguished based on system response to one of a defined, limited set of contingencies. These concepts were recently evolved in [3].

The importance of the four security states is that they provide a conceptual basis for making security-related decisions. This basis rests on the assumption that any normal state is acceptable and any other state is unacceptable. Traditionally, security-related decisions in both operations and planning have been made with the criterion being that the power system should remain in the normal state at all times. Although conceptually appealing, application of this criterion must confront a serious problem: there does not exist a quantitative method to measure security level and therefore distinguish between the states. As a consequence, rough rules of thumb are used in the decision process, and resulting boundaries between the various regions of the stable state, where problems are only potential, do not represent the same risk. Most importantly, lack of a security level index disguises the fact *that there is no fundamental difference between the normal state and the alert state*: in both states, unexpected events may cause undesirable consequences. The only difference is that the likelihood and/or severity of the undesirable consequences change, i.e., the states differ only in terms of the risk corresponding to the operating conditions and configuration, and we need a measurable index to reflect this. This perception is similar to the one taken in [4], where it was recognized that the system is *always* insecure, and it is just a matter of the *degree* of the insecurity.

2.2 Time Frames for Security-Related Decisions

There are generally three different time frames for security-related decisions. In operations, the decision-maker is the operator, the decision is how to constrain the economic operation of the power system in order to maintain the normal state, and the basis for the decision are operating rules. In operational planning, the decision-maker is the analyst[1], the decision is what the operating rules should be, and the basis for the decision is reliability criteria specifying minimum operating requirements, which defines acceptable performance for the credible contingencies. In facility planning, the decision-maker is the analyst, the decision is how to reinforce the transmission system, and the basis for the decision is reliability criteria for system design, which generally adheres to the same disturbance-performance criteria specified by minimum operating requirements.

We believe that the conceptual development of RBSA presented in this paper is applicable to all three time frames. It represents a particularly significant development for operations and operations planning, since probabilistic approaches, until now, have remained mainly in the domain of the facility planner. Yet, operators have been calling for its application for quite some time, as illustrated by the following remarks that were made in 1988 by an experienced and respected operating engineer:

"Operators, in making decisions about what corrective actions are going to be taken, need to know the probability of occurrence, and then determine whether or not we want to take some steps that may be very undesirable.....If we agree, in the coming hour, to make a certain transaction that we know is going to increase the loading on certain facilities, is that going to have a significant effect on the security of the system? This is something we are thinking about. This is in my way of thinking a system parameter: a transmission system, a cross-state transfer, a loading or something like that, that if we go that next hundred megawatts, is that going to make a significant difference in the system security? If so, it's not worth the economics. If on the other hand, for a relatively small increase in the probability that the security is going to increase, then it may be worth it. And we're into dollars and cents. 'What is the value of taking that next step?' and then 'What is the cost of having a major disturbance occur?' " [5].

2.3 Deterministic Security Assessment

In deterministic security assessment, the decision is founded on the requirement that each outage event in a specified list, the contingency set, results in system performance that satisfies the chosen performance evaluation criteria. These assessments, typically involving large numbers of computer simulations, are defined by selecting a set of network configurations, a range of system operating conditions, a list of outage events, and the performance evaluation criteria. Study definition requires careful thought and insight because the number of possible network configurations, the range of operating conditions, and the number of conceivable outage events are each very large, and exhaustive study of all combinations of them is generally not reasonable. Consequently, an approach has evolved within the electric power industry to minimize study effort yet provide useful results. We call this approach the deterministic approach. This approach depends on the application of two criteria during study development:

Credibility: The network configuration, outage event, and operating conditions should be reasonably likely to occur.

Severity: The outage event, network configuration and operating condition on which the decision is based, should result in the most severe system performance, i.e., there should be no other credible combination of outage event, network configuration, and operating condition which results in more severe system performance.

The deterministic approach consists of 6 basic steps:

[1] Identifying operating rules, typically in the form of tables or graphs, has traditionally been the domain of the operational planner. There has been some progress recently in automating rule development. One notes that even here, the automation is in terms of identification of specific numerical levels characterizing the rules. However, the *nature* of the rule is still developed off-line. It will require some significant progression in the field of artificial intelligence before operational rule determination is fully automated and completely done on-line.

1. Select the time period (year, season) and loading conditions (peak, partial peak, off peak).
2. Select the network configuration. Unit commitment is selected based on typical unit availability for the chosen time period. The topologies selected are normally all circuits in service; here, credibility is emphasized over severity. Sometimes sensitivity studies are also performed for a few weakened topologies. Also, short-term operational studies are often performed with the explicit purpose of identifying limits for topologies expected to be encountered in the near future.
3. Select the contingency set. Normally this set consists of all "N-1" events, although some particularly credible "N-2" events may be included (e.g., two circuits on the same towers). This set may be shortened to only include events resulting in performance that is affected by operating conditions or facilities pertinent to the goals of the study.
4. Refine the operating conditions in terms of dispatch and voltage profile. Here, the analyst seeks conditions that reflect balance between credibility and severity with respect to the selected events.
5. Perform the simulations of the events and identify any that violate the performance evaluation criteria.
6. Identify solutions for any event resulting in violation of the performance criteria. These solutions may be of three types. *Operating guidelines* include guidelines on generation, transfer, or voltage levels and are developed for use by the operator to indicate operating conditions that lead to a violation. These guidelines are normally given in the form of limits on operating parameters, beyond which operation is unacceptable. *New Facilities* include circuit addition, circuit reconductoring, capacitor installation, bus reconfiguration, and transformer replacement. *Special protection schemes* (SPS) are special switching schemes activated by pre-specified events. Typical SPS includes generator rejection, load rejection, controlled separation or islanding, and shunt or series capacitor switching.

3 Why Change?

The deterministic approach has served the industry well; it has provided high reliability levels without requiring excessive study effort. Yet there has been a real and tangible price to pay for using this approach: solutions tend to be overly conservative, due to the emphasis of the most severe, credible event. Consequently, existing facilities are not fully utilized, from an operating perspective, and the system becomes overbuilt, from a planning perspective. This price was affordable as long as it could be spread among the pool of captured customers. Now, however, this pool is shrinking as the retail power market is being made more widely available and higher rates for any reason risks losing these customers to a less expensive supplier. As a consequence, utilities are less willing to invest in new facilities yet more willing to push transmission limits in order to take advantage of less expensive energy and lower production costs.

It is in this environment of frequent stressed system operation that the weaknesses of the deterministic approach become salient. One glaring weakness is that it is difficult to economically evaluate the security level. Therefore, it can be hard to integrate security into economic decision-making processes. More fundamental weaknesses are:

Occurrence frequency of events is not measured. For some problems such as overload and voltage security, measures of event severity do exist, e.g., over-current or under-voltage, and these measures are used within deterministic assessment to judge security level. Yet these measures do not account for event occurrence frequency. Application of the deterministic approach accepts the implicit assumption that all events in the contingency set occur with equal frequency. However, even if the contingency set includes only N-1 events, significant variation in occurrence frequency may exist.

Performance requirements are not uniform. Typical deterministic reliability criteria, for each contingency in the contingency set, might include: 0.8 pu minimum first swing bus voltage dip, thirty minute emergency ratings for transmission conductors based on two feet per second wind speed and 40 degrees C ambient temperature, 0.95 minimum post-contingency steady state voltage level, no out of step condition, and damped oscillations. Each performance requirement represents a threshold on economic impact, within which performance for credible contingencies must be maintained. However, there is no guarantee that the various performance requirements represent the same threshold. In some cases, one easily recognizes that they represent different economic impacts. For example, exceeding a conductor 30 minute emergency overload rating by 1% for 30 minutes is unacceptable, but there is almost zero economic impact. An out of step condition at a plant is equally unacceptable, yet the cost of replacing the energy source is high.

Non-limiting events are ignored. The deterministic approach bases decisions on the performance of the most restrictive event(s). Less restrictive events have no influence on the decision. Yet, they do contribute risk to the operating condition being considered and therefore are important when considering the acceptability of the operating condition. The problem is that the deterministic approach is unable to recognize the composite influence of more than one contingency as a function of operating condition. As a result, decisions are made that address only the effects of contingencies that are constraining the system[2].

Limiting the contingency set to N-1 contingencies, using simple, conservative performance requirements, and basing decisions on "worst-case" analysis are methods the industry has used to handle uncertainty in security assessment. These methods were *acceptable* under the earlier industry structure

---

2 For example, consider a stability limited generation plant that feeds its loads over two transmission circuits, one of which is higher impedance than the other. In the deterministic approach, the stability limit is decided by the most constraining of the two contingencies, likely loss of the lower impedance circuit. It may be that one circuit is so much weaker than the other that its outage does not result in instability at all. In this case, the stability limit is, and should be, driven by outage of only the strong circuit. On the other hand, suppose the two circuits are very nearly the same in impedance. In this case, outage of the weaker circuit does in fact cause instability, but at a slightly higher generation level than outage of the strong circuit. This is a higher risk situation than the first situation. Effectively, the frequency of the event "loss of synchronism," as a function of generation level, has increased.

because stressed operation occurred infrequently, and conservatism was embraced. These methods were perceived as *necessary* because of the difficulty in assessing uncertainty via performing increased computations or obtaining additional data. Today, transmission and generation owners are keen on fully utilizing equipment to maximize the return on their investment in these facilities. Further, over-conservatism in security assessment is subject to scrutiny by those incurring reduced profit margins resulting from associated transmission constraints. Simultaneously, computational speed has dramatically increased, and fast computers available today can effectively be used to probe a wider range of operating conditions and consequently reduce uncertainty. Finally, obtaining appropriate data, once thought to be a major hurdle in assessment of uncertainty, can be viewed as a decision-making problem itself, where one employs probabilistic decision paradigms for deciding whether to spend resources for gathering that data by comparing its worth to the cost of the necessary resources.

4 Risk-Based Security Assessment (RBSA)

Development of RBSA began in 1994 at Iowa State University. One contribution of this work is the development of an index that quantitatively captures the factors that determine security level: likelihood and severity of events. Other indices have been used in the past. Among these, deterministic methods have employed performance measures such as line current, voltage magnitudes, and stability margins. Yet these measures reflect severity but not likelihood. A well known probabilistic index is loss of load probability (LOLP), but it reflects likelihood but not severity. Other probabilistic indices, including expected unserved energy (EUE) and "system minutes," do capture likelihood and severity, but the measure of severity reflects only load interruption and not costs associated with equipment damage or lost opportunities from equipment unavailability. Also, most previously proposed probabilistic indices used rather crude rules based on fixed bus voltage and line current limits for identifying when load interruption occurs.

Where past reliability indices were largely measures of the system's ability to incur or avoid failure, the RBSA risk index is a measure of the system's *exposure* to failure. Consequently, this risk index accounts for both likelihood and severity, and it uses a severity model that captures all cost-consequences, including load interruption, equipment damage, and opportunity costs due to equipment outage. The basic relation for computing risk is

$$Risk(\mathrm{Im} \mid X_t) = E(\mathrm{Im}(X_{t+1}) \mid X_t)$$
$$= \int_{X_{t+1}} \int_{E_i} \Pr(E_i, X_{t+1} \mid X_t) \times Risk(\mathrm{Im} \mid E_i, X_{t+1}) dE_i dX_{t+1} \qquad \text{(eq. 1)}$$

where Im denotes an impact or cost-consequence associated with load interruption, equipment damage, or opportunity cost due to equipment unavailability. Here the risk associated with the pre-contingency operating condition Xt (e.g., loading, dispatch, voltage profile) is given by the expected value of the monetary impact of the operating condition in the next time period $Xt+1$ (the next hour) given the current operating condition, i.e., $E(\mathrm{Im}(Xt+1)|Xt)$. This expectation is an integral of the product of probability of the *uncertain event*, defined by Ei (the contingency state) *and* $Xt+1$ (operating condition in the next time step) times its corresponding impact over the set of all possible events.

A distinctive feature of RBSA is that the impact of a specified contingency state Ei for a specified operating condition $Xt+1$ is considered to be uncertain, therefore we denote it as $Risk(\mathrm{Im}|Ei, Xt+1)$. (The set of contingency states $\{E_i, \forall\, i = 0, N\}$ includes the possibility that the current state remains the same, i.e., an outage does not occur.) The uncertainty associated with this impact depends on the nature of the impact. For line overload, the uncertainty is in the ambient temperature, wind speed and direction, and solar flux [8]. For transformer overload, it is in the ambient temperature and the transformers' loading cycle [9]. For voltage security, it is in the interruption voltage level of the loads at each bus [10]. For dynamic (angle) security, it is in the fault type and fault location of the outaged circuit corresponding to contingency state Ei [11,12]. In what follows, we briefly describe computation of $Risk(\mathrm{Im}|Ei, Xt+1)$ for line overload [8]. Similar computations for transformer overload, voltage security, and dynamic (angle) security can be found in references [9-13]. Two companion papers presented for this panel also describe computation of voltage security risk and dynamic (angle) security risk.

For overload analysis, specification of the contingency state and the operating condition enables solution of a power flow, resulting in specific values of current in every line. Therefore, given that the region of interest has NLINES and NBUSES, we evaluate $Risk(Im|Ei, Xt+1)$ according to

Acceptability of a line current level is determined by the amount of sag and the damage (loss of life) incurred by the

$$Risk(\mathrm{Im} \mid E_i, X_{t+1}) = \sum_{k=1}^{N_{LINES}} Risk(\mathrm{Im} \mid I_k) \qquad \text{(eq. 2)}$$

conductor. If we assign an economic impact with sag and loss of life [8,13], then the associated risk as

(eq. 3)

where the probability distribution for conductor temperature

$$Risk(\mathrm{Im} \mid I_k) = \int_{all\,\theta_k} \Pr(\theta \mid I_k) \times \left\{ \mathrm{Im}_{sag}(\theta) + \mathrm{Im}_{damage}(\theta) \right\} d\theta$$

$\Pr(\theta|\mathrm{Ik})$ is computed using the conductor thermal model and the statistics of the model inputs e.g., ambient temperature, wind speed and direction, and solar radiation.

We provide an illustration of this analysis on a modified IEEE Reliability Test System (RTS). We have chosen a scenario where 3 contingencies, each one a transmission line outage, result in line overload. Fig. 3 illustrates this system. Fig. 4 shows the risk plots from eq. 1. Since there are three lines that suffer overload risk, the plot shows 4 curves: one for each line and one for the total. The total overload risk is dominated by the risk of line 130-120, which makes the 130-120 risk curve not very visible. This is consistent with the fact that line 130-120 transfers most of the energy from the northern part of the system to the southern.

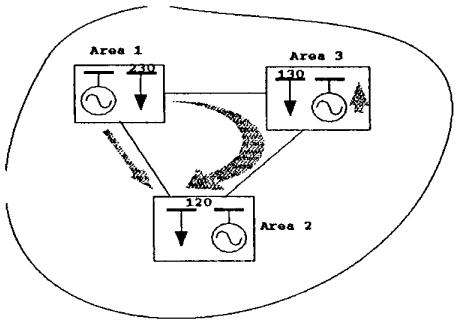

Fig. 3: Local Region of IEEE RTS

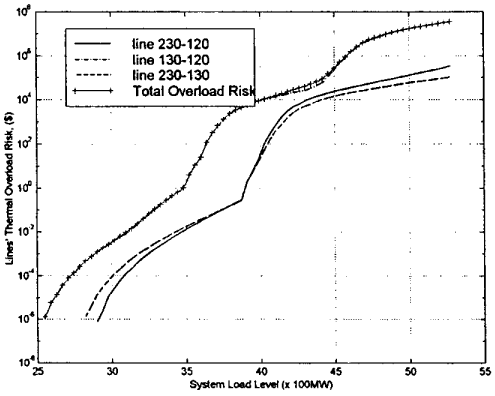

Fig. 4: Overload risk

5 Benefits of Using RBSA

Bridging economics and security: The risk calculated by eq. (1) has explicit economic meaning in that it represents the expected cost due to possible insecurity problems. It measures the economic consequence of an uncertainty weighted by its probability of occurrence. This property provides a direct bridge between power system economics and security, in that it is a means to explicitly include security in ordinary economic decision-making problems.

A leading indicator: The basic application of the risk index is to use available information to decide "now" in preparation for a condition that is minutes, hours, weeks, or years into the future. This ability is the basis for calling the risk index a leading indicator.

Risk as a Function of Operating Condition: Results of RBSA are provided so as to illustrate the functional dependence of risk on pre-contingency operating conditions that operators are able to monitor, understand, and control.

Risk is assignable: Because risk is computed for each security problem, each contingency, and each component, it is easy to identify components or conditions causing it and incurring it. Knowledge of component ownership therefore allows risk to be assigned to the appropriate entities.

Composite Risk: The risk computation reflects, for a local operating region or an entire system, the composite effect of all contingencies and all resulting security problems, including those associated with overload, voltage, and dynamic (angle) security. Therefore, it provides a measure of the overall security level of the region.

Cumulative Risk: If one provides a sequential trajectory of operating conditions through time [14], then risk can be calculated for each operating condition, and summation over all time instances provides a cumulative risk assessment over the specified time period. This cumulative risk assessment is useful for assessing the influence on security level of a particular facility plan.

Risk Preferences: RBSA provides the capability to manage security based on the decision maker(s) preference regarding risk exposure. Identification of preference is done in the context of decision analysis [15].

6 Applications of RBSA

In the decision contexts described in Section 2.2, the basic problem is to perform integrated assessment of the security level together with the cost or profit of accepting that security level. Below, we suggest a few typical situations where RBSA tools would enable this kind of assessment.

Operations: Because of the unique ability to compute composite risk, RBSA may be used to monitor regional and system security levels, providing significant information to operators in a compact index[3]. This enables more refined assessment of operational decisions involving economic-security tradeoffs. For example, in deciding whether to commit a unit to relieve a high transmission flow, the operator desires to weigh the risk associated with the flow against the cost of committing the unit. One also thinks of the security constrained economic dispatch (SCED), or more generally, the optimal power flow (OPF). Traditionally, SCED and OPF model hard security constraints. Yet, use of hard constraints sometimes results in high energy costs although the actual risk may be very low. An RBSA approach can combine production costs and risk in an objective function, eliminating the constraints, so as to identify an optimal security-economy balance. For auction-based dispatching, risk can be used as a "lever" to adjust the behavior of market participants via price incentives.

Operational Planning: Ratings of lines, transformers, and generators are often given for various conditions; for example, a transmission line typically has both a normal rating for continuous flow and a 15-30 minute emergency rating. Operators must also adhere to system limits on transmission flows and load levels, which can be complex functions of several operating parameters. These limits are driven by risk associated with normal conditions as well as with potential outage conditions. RBSA can be used in operational planning to quantify these risks and provide decision criteria for identifying these ratings and limits.

Facility Planning: System analysts studying future transmission and generation needs must select from

[3] A new project is underway that will implement this operational monitoring capability. This project, funded by EPRI with the Southern Company as host utility, involves the authors of this paper together with the Laurits R. Christensen Associates, Inc. Economics and Engineering Consulting, Madison WI, and Arun Phadke of Virginia Tech. Additional aspects of this project include integration of protection system reliability analysis and extension to analysis of high order contingencies and potential catastrophic events.

alternatives to solve perceived problems. This requires prediction of the conditions characterizing a distant future and consequently results in high inherent uncertainty, particularly with respect to outages and loading levels. RBSA provides tools for handling this uncertainty, quantifying long-term risk of a facility plan, and comparing this risk with the costs and benefits of the plan [13,16,17].

Design and Assessment of Special Protection Schemes: SPS are attractive today for increasing transmission capacity because of their low cost and installation time. Yet, SPS contributes significant risk because failures have high potential for catastrophic consequences because SPS is typically armed only under stressed conditions. RBSA can quantify this risk; in addition, SPS failure analysis used in RBSA can enhance SPS design standards [18].

Reliability Criteria: Some criteria used to judge acceptability of system performance is subjective. For example, many companies specify transient voltage dip performance requirements of 0.8pu, based on the perception that violation can cause interruption of some load types. Yet there exist little data characterizing load interruption as a function of voltage dip. Therefore, justification of related operating limits can be difficult. Agents that incur economic penalty as a result of being constrained off the system may press for justification of the violated performance requirement. RBSA can provide this justification; alternatively, it can provide the basis for performance requirement adjustment [13].

Data gathering by information valuation: Application of probability methods to characterize engineering systems requires data collection. The size and complexity of power systems makes this a formidable problem, and this has been reason in the past for abandoning probabilistic approaches altogether. The RBSA approach enables valuation of information before it is gathered in order to determine whether its value exceeds the cost of gathering it [13].

6 Conclusions

Use of probabilistic risk represents a natural evolution for security assessment procedures in that it quantifies the basic elements, probability and consequence, on which security assessment is based. The great advantage is that quantification of security level through probabilistic risk subsequently enables direct inclusion of security in mathematical decision tools. In addition, it provides that the notion of "reliability" can be posed in language and models understood by the energy marketer, the economist, and the financial engineer, all of who have been using risk for many years. Conversely, the power engineer will find that use of risk in security assessment provides a bridge between traditional power systems operations and planning procedures and the intricacies of financial markets. Although this is a wide open field with significant work yet to be done, we believe that this paper, together with those cited in the bibliography, provides a clear framework on which to begin.

References

[1] The North American Reliability Council, "NERC Planning Standards," approved by NERC Board of Trustees, September, 1997.

[2] L. Fink and K. Carlsen, "Operating Under Stress and Strain," *IEEE Spectrum*, Vol. 15, pp. 48-53, March, 1978.

[3] International Conference on Large High-Voltage Electric Systems (CIGRE), "Power System Security Assessment, A Position Paper," Final Report, CIGRE Task Force 38.03.12, June 30, 1997.

[4] L. Fink, "Security: Its Meaning and Objectives," *Proc. of the Workshop on Power System Security Assessment*, pp. 35-41, Ames, Iowa, April 27-29, 1988.

[5] J. Koehler, in remarks on [7], recorded in *Proceedings of the Workshop on Power System Security Assessment*, pp. 54-55, Ames, Iowa, April 27-29, 1988.

[6] Western Systems Coordinating Council Reliability Criteria, March 1997.

[7] M. Beshir, "Probabilistic Based Reliability Criteria," presentation to the IEEE Task Force on Probabilistic Aspects of Reliability Criteria, IEEE 1998 Summer Meeting, July, 1998, San Diego, CA.

[8] H. Wan, J. McCalley, and V. Vittal, "Increasing Thermal Rating by Risk Analysis," to appear in *IEEE Trans. on Pwr Sys.*

[9] W. Fu, J. McCalley, V. Vittal, "Risk-Based Assessment of Transformer Thermal Loading Capability," *Proc. of the 30th North American Power Symposium,"* Cleveland,OH., Oct. 1998, pg. 118-123.

[10] H. Wan, J. McCalley, V. Vittal, "Risk-Based Voltage Security," under review, *IEEE Trans. on Pwr Sys.*

[11] J. McCalley., A. Fouad,, V. Vittal., A. Irizarry-Rivera,, B. Agrawal, R. Farmer, "A Risk-based security index for determining operating limits in stability-limited electric power systems" *IEEE Trans. on Pwr. Sys.*, Vol. 12, No. 3, Aug. 1997.

[12] V. Van Acker, J. McCalley, V. Vittal, "Risk-Based Transient Instability," *Proc. of the 30th N. American Power Symposium,"* Cleveland,OH., Oct. 1998.

[13] J. McCalley and V. Vittal, "Risk Based Security Assessment," final report for EPRI Project WO8604-01, Electric Power Research Institute.

[14] International Conference on Large High-Voltage Electric Systems (CIGRE), "Sequential Probabilistic Methods for Power System Operation and Planning,"CIGRE Task Force 38.03.13, *Electra,* No. 179, Aug., 1998.

[15] H. Wan, J. McCalley, V. Vittal, "Decision Making Under Risk," *Proc. of the 30th N. American Power Symposium,"* Cleveland,OH., Oct. 1998.

[16] Youjie Dai, James D. McCalley, V.Vittal, "Simplification, expansion, and exhancement of direct interior point algorithm for power system maximum loadability," to appear in *the Proc. of the 1999 Power Industry Computer Applicaions* (PICA).

[17] Youjie Dai, James D. McCalley, V.Vittal, "Annual risk assessment for system thermal overload", *Proc. of the American Pwr Conference*, April 1998.

[18] J. McCalley and W. Fu, "Reliability of Special Protection Schemes," to appear in *IEEE Trans. on Pwr Sys.*

Biographies

James D. McCalley is an associate professor of electrical engineering at Iowa State University, where he has been employed since 1992. He received his PhD from Georgia Tech. He was employed by Pacific Gas & Electric Company as a transmission planning engineer from 1986 to 1990. He is a registered professional engineer in California, and an IEEE senior member.

Vijay Vittal is professor of electrical and computer engineering at Iowa State University. He received his PhD from Iowa State University. He is recipient of the 1985 Presidential Young Investigator Award and an IEEE Fellow.

Nicholas Abi-Samra has a Bachelor of Engineering degree from the American University of Beirut, Masters of Science in Electrical Power Engineering from the University of Missouri. From 1977 to 1997, he was with Westinghouse Electric Corporation where he held positions of increasing responsibilities from engineering to management. He joined EPRI in August 1997. Currently he is Manager, Systems Planning, Grid Operations and Planning. He is also responsible for a number of strategic Science & Technology long-term projects. He is a Senior Member of the IEEE.

ACKNOWLEDGMENTS: Funding for this work came from the EPRI Contract WO8604-01, and the National Science Foundation, Grant ECS9502790. The authors also acknowledge the contributions of graduate students previously or presently involved in this work, including A. Irizarry-Rivera, Hua Wan, Weihui Fu, Vincent Van Acker, Sanyi Zhao, and Yougie Dai.