KEMA experience you can trust EXPERT PUBLISHED ARTICLE

Published in:
Electricity Journal
October 2004

http://www.electricity-online.com/journal.html

Reliability @ Risk[SM]

A New Paradigm for Assessing Reliability

Ralph Masiello, John Spare, Al Roark, and Sam Brattini

The Problem

The power industry has relied on the same reliability concepts since 1967, including Loss of Load Probability, Component Based Failure Analysis (especially in nuclear power), N-1 (or N-2) Maximum Credible Contingency Analysis, and Generation Reserve Requirements [1] [2]. These concepts generally involve the use of statistical engineering models for planning purposes and deterministic single (or double) failure avoidance rules for operations.

Recently, blackout events have been occurring in many countries and on a more frequent basis than traditional analysis would lead us to expect [3]. The industry needs a new methodology that explains this trend and helps us to better understand overall reliability. The August 14, 2003 blackout in the USA and other blackouts demonstrate that the reliability problem is complex and that the industry requires more information and more sophisticated approaches capable of dealing with the uncertainties in predictive modeling. Furthermore, the industry needs a metric to estimate the probability distribution function (pdf) of bulk power load interruptions that incorporates all conceivable contributing factors and produces estimates that track recently observed events. The industry also needs an approach that can be used to estimate the quantitative impact on reliability of hypothetical investments or expenditures not only in copper, iron and porcelain but also in communications, control, people, and processes. If such a reliability pdf could be dynamically adjusted in near real time to events and operating conditions, it would give a "dashboard" operational indication of the reliability of the power system at a moment in time. This dashboard index could also become a useful metric for tracking operational performance against goals.

Multiple failures have been more likely than the traditional "maximum credible" contingency mind set has anticipated. Contrary to the dictums of normal theory, the first failure somehow makes successive failures more likely to happen. Post mortem analyses indicate that the first set of problems set the stage for successive difficulties [3].

Failures of control and protection systems are often contributing factors – factors not traditionally considered in reliability analyses. Human error, including inaction or inappropriate action by the system operator and the failure of market participants or external suppliers to behave as needed, is a new, potent contributing factor.

These non-traditional reliability issues are not amenable to modeling in a traditional, component-based engineering model. The power industry needs to look to other disciplines for approaches to assessing reliability today.

Requirements for a New Approach

Instead of more detailed, complex engineering models, our industry needs a simpler modeling approach that is capable of being used operationally, while articulating how reliability is grossly affected by several major interdependent influences. What is required is a more sophisticated approach that reflects the many non-traditional compounding factors and one that will react dynamically to changing operational conditions.

Another requirement for measuring reliability is to acknowledge that not all failure modes have been identified or can even be modeled, and that not all statistics around event occurrences are known or observed. This new methodology could be adjusted and calibrated to align its results with real world observations, similar to the way in which parameters of volatility and kertosis in financial risk metrics are estimated based on observed market data. This preferred approach would provide information that is useful to operations in real time, moving from "Safe/Not Safe" to "How Safe" as the question to answer. It would also allow investments in Information Technology, communications and control, and people and procedures to be weighed against investments in copper and iron for new facilities or equipment. Most importantly, it would provide a mechanism for weighing reliability measures that impact markets against the market costs imposed.

The "old" and a "new" way of looking at the problem, together with some relevant technologies and methodologies that are applicable to aspects of the problem are summarized in Exhibit 1. This paper will explore how some of these methodologies can be applied to transmission reliability and some of the lessons that they can provide even with simple applications.

Exhibit 1: "Old" vs. "New" Approach to Viewing a Problem

Old	New	*New Disciplines*
Deterministic	Stochastic	*Probabilistic Contingency Analysis*
Binary Safe/Not	Gray	*Fuzzy Set Theory*
Static World	Dynamic	*Non-Stationary Stochastics*
Exact Model	Unknown and Erroneous	*Fuzzy Logic*
Predictable Conditions	Random Behavior	*Risk Management*
Perfect Operations	Failures	*Operational Risk*
Centralized Operations	Distributed/Market Operations	
Quasi steady state	Extreme Conditions	*Extreme Value Theory*
Known Disturbances	Unknown	
LOLP – Reliability	Reliability – Cost Tradeoffs	*Econometrics, Portfolio Optimization*
Separation of Forecast and Optimization	Integrated	*Real Options / Portfolio Optimization*

Reliability @ Risk (R@R) a New Paradigm

All sorts of things are neither modeled in typical reliability analyses nor capable of being modeled accurately in enough detail to affect transmission reliability. However, without accounting for them, results are too optimistic.

The financial world deals with similar issues to the power industry, specifically that the real world is too complex and events are often unknown to model with a high degree of fidelity. The answer is to use simpler models and calibrate them to observed data at appropriate intervals.

The financial world arrives at Value @ Risk (V@R) [4] as a measure of risk, defined as a function of a given set of obligations and the uncertainties that exist in the world. The authors offer an analogy -

Reliability @ Risk (R@R) - to use as a measure of risk over future time that can be updated as conditions change. Once a V@R or R@R is calculated, it can be used in decision making and in comparing alternatives.

The R@R model is a new way of looking at and measuring reliability that incorporates concepts from the financial services industry and the power industry.

The financial world is familiar with the concept of operational risk. Financial institutions use this concept to quantify risks due to failures of operational systems, people, or other factors not dealt with in market price, credit, and similar financial issues. Operational risk deals with the problem that major operational failures are rare and no one institution will have a set of observed incidents to use in developing predictive statistics.

In the power failure analysis world, the successive evolution of a system through different states due to random occurrences of component failures and models of recovery times (MTTR) is the normal form of analysis. A system is more or less exposed to unavailability due to failures based on how many failures have occurred and what the typical recovery times have been in the repair process.

R@R constructs a simple model of a reliability "state" of the power system based on easily understood and accepted concepts stemming from the traditional "N-1" contingency model. The power system is modeled as making transitions from one reliability state to another following a Markov Process. The transition rates in the Markov Processes used in the R@R model are dynamic based on real time conditions of the power system, associated control systems, ongoing maintenance activities, and other factors as they occur.

The R@R model provides for:

- A calculation of probability that the system will move to an unacceptable failure state within any particular operational time horizon, as well as a simple characterization of the current state that is operationally useful. This failure probability becomes a useful operational index in itself.

- Simplicity in providing for failure modes reflecting operator failures to correct reliability vulnerabilities or other non-transmission failure to perform events.

- A reliability state framework that presents state probabilities that are observable and/or inferable from observable phenomena, and that are modeled or determined experimentally.

    - These state probabilities (for normal, insecure, and emergency conditions) are useful indicators that must be considered when the overall failure rate does not align with reality.

    - The framework is flexible and adaptable to different definitions or number of states. For instance, it can be adopted to the NERC reliability definitions and operating state definitions as used in the different NERC regions

    - State transition probabilities adjusted in real time as events and conditions change

How the R@R Model Works:

Operational Risk

Many enterprises and organizations, are subject to business risks that arise from human error, malignant human activity, IT system failure, and other "non-market" or "non engineering" risk. The more severe risks (in terms of dollar impacts) normally are too infrequent for any one enterprise to estimate them based on internally observed statistics.

The Basel Accords in the financial services industry provide that institutions of similar size and scope should examine the failures encountered globally by all entities in the group over a multi-year period and assess gross statistics of likely exposure using this broader set of data. Rules are then established on how these risks should be modeled and the quantity of reserves required against those risks. [5] R@R proposes a similar approach to modeling power reliability operational risk.

Failure Analysis and Markov Model

Failure analysis models usually are developed from component level system diagrams. A Markov model of system states and state transitions is constructed behind these failure analysis models and the stochastic behavior of the system can be simulated and analyzed.

The R@R approach does not address the component level, as this would necessitate very large models with fine degrees of detail. This level of detail is good for an engineering design but does not meet the objective of having a simple model we can use to develop operational views and metrics.

The R@R Reliability State Model

In 1967 DyLiacco proposed what has become a standard terminology and model for the operational security state of the system as shown in Exhibit 2: Secure, Insecure, Failed, and Restorative.

Exhibit 2: DyLiacco [14] Security State of the System Terminology

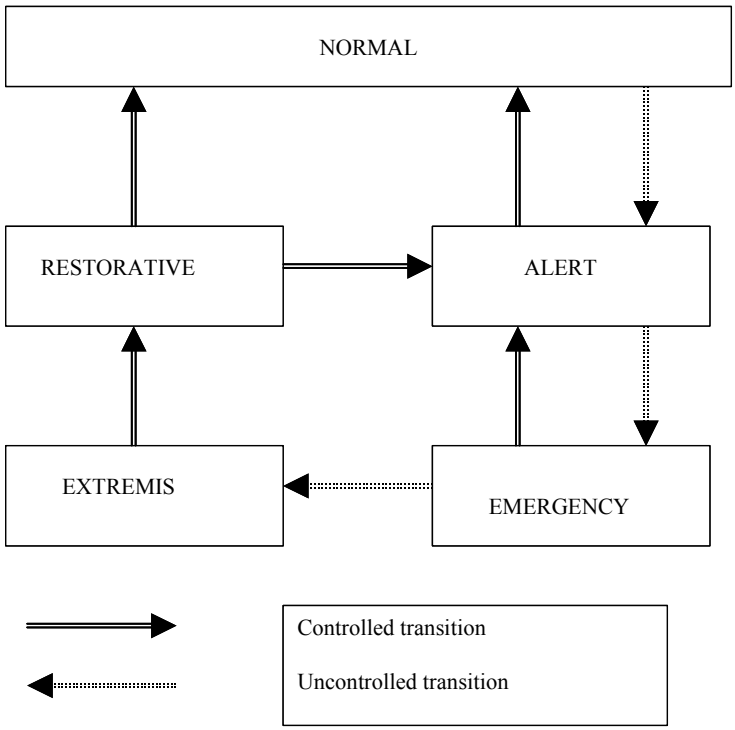


Exhibit 3: Reliability States in a Market Environment

Actual / Contingency	Operating within Normal Limits	Operating outside Normal Limits but Within Emergency Limits	Outside Emergency Limits	System Failure has occurred
Contingency is within Normal Limits	State IA Secure	Not Valid State	Not Valid State	Not Valid State
Contingency is outside Normal Limits but within Emergency Limits	State IB Secure	State IB Secure	Not Valid State	Not Valid State
Contingency is Outside Emergency Limits	State IIA Insecure	State IIB Insecure	State III Emergency	State IV Failure

As shown in Exhibit 3, the R@R Reliability State Model expands these terms to define six states of reliability that are formalized in terms of specific definition with respect to operating conditions:

- ***State I A "Secure"*** - The system is operating with all normal* operating limits and no N-1 Contingency analysis reveals a normal limit to be exceeded.

- ***State I B "Secure"*** - The system is operating within all normal operating limits but one or more contingencies will cause one or more normal operating limits to be exceeded. Also note that State IB can occur if the system is both operating outside Normal Limits and creates a contingency event that is outside of Normal Limits. No emergency* limits are exceeded.

- ***State II A "Insecure"*** - All normal limits are observed but one or more contingencies will cause one or more emergency limits to be exceeded.

- ***State II B "Insecure"*** - One or more normal limits are exceeded and one or more contingencies will cause one or more emergency limits to be exceeded.

- ***State III Emergency"*** - One or more emergency limits are exceeded and immediate dramatic action is required (disconnection of load, generation, or interconnection).

- ****State IV "Failed"*** - One or more emergency limits are exceeded and system failure has occurred (meaning involuntary disconnection of load/ generation/ interconnection).

* **Definitions**

"Normal" limit is the threshold under which equipment or system parameters can be operated indefinitely.

"Emergency" limit is the threshold under which equipment or system parameters can be operated outside the normal limit for a defined period of time but must eventually return to the normal limit in that timeframe or create a failure to operate.

While different control areas, utilities, and reliability regions have different terminologies, it is feasible to adapt all variations to some version of this model.

Note that the “failed” states do not include a quantitative assessment of the severity of a failure - that is how much load, generation, or interconnection is affected. The R@R model can be extended to incorporate a quantitative measure as discussed later in this paper. At this point, the failed state has not been quantified other than to note that there is a significant unplanned loss of load at the bulk power or transmission level. Quantifying the extent of a failure in the R@R model is discussed below.

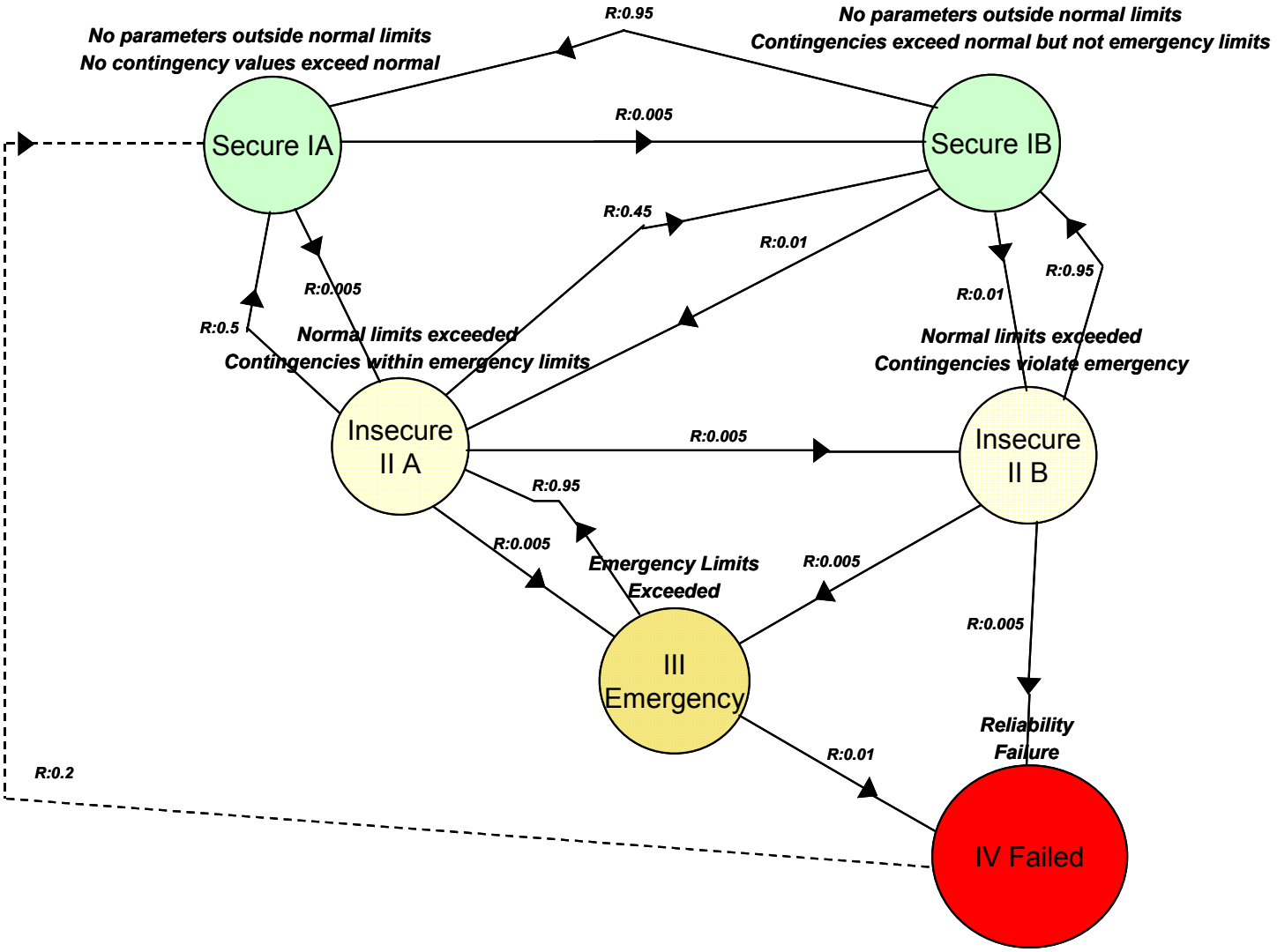
The six states and the transition probability (modeled as a Markov Process model) [6] are shown in Exhibit 3. Some transitions are not allowed because they are inconsistent with the model, for instance from Secure IA or IB directly to Emergency III or Failed IV.

Below, some of these paths are added as ways of allowing for “N-2” events that are modeled as successive events happening in rapid-fire order. Transitions between states are allowed in R@R that will either decrease or increase reliability. Successful operational action or fortuitous changes in condition over time, for instance, will cause a state transition from a less reliable state to a more reliable state. Assuming a set of numeric state transition probabilities, the probability of being in state IIA or IIB within any future time window can be computed as a function of factors affecting the probability of being in the current state.

One or more transitions from the “Failed”, “Emergency”, or “Insecure” states back to “Secure” states must exist. It is mathematically critical to have this restoration transition so that the Markov model is ”irreducible” - that is, it is possible to communicate from any state to any other via sufficient transitions. This enables us to compute the steady state or “stationary” state probabilities in a straightforward if tedious fashion via Monte Carlo simulation. If the system is not irreducible, multiple stationary probability distributions are possible. (In this case with infinite time sequences, there is zero probability of emerging from the failed state.)

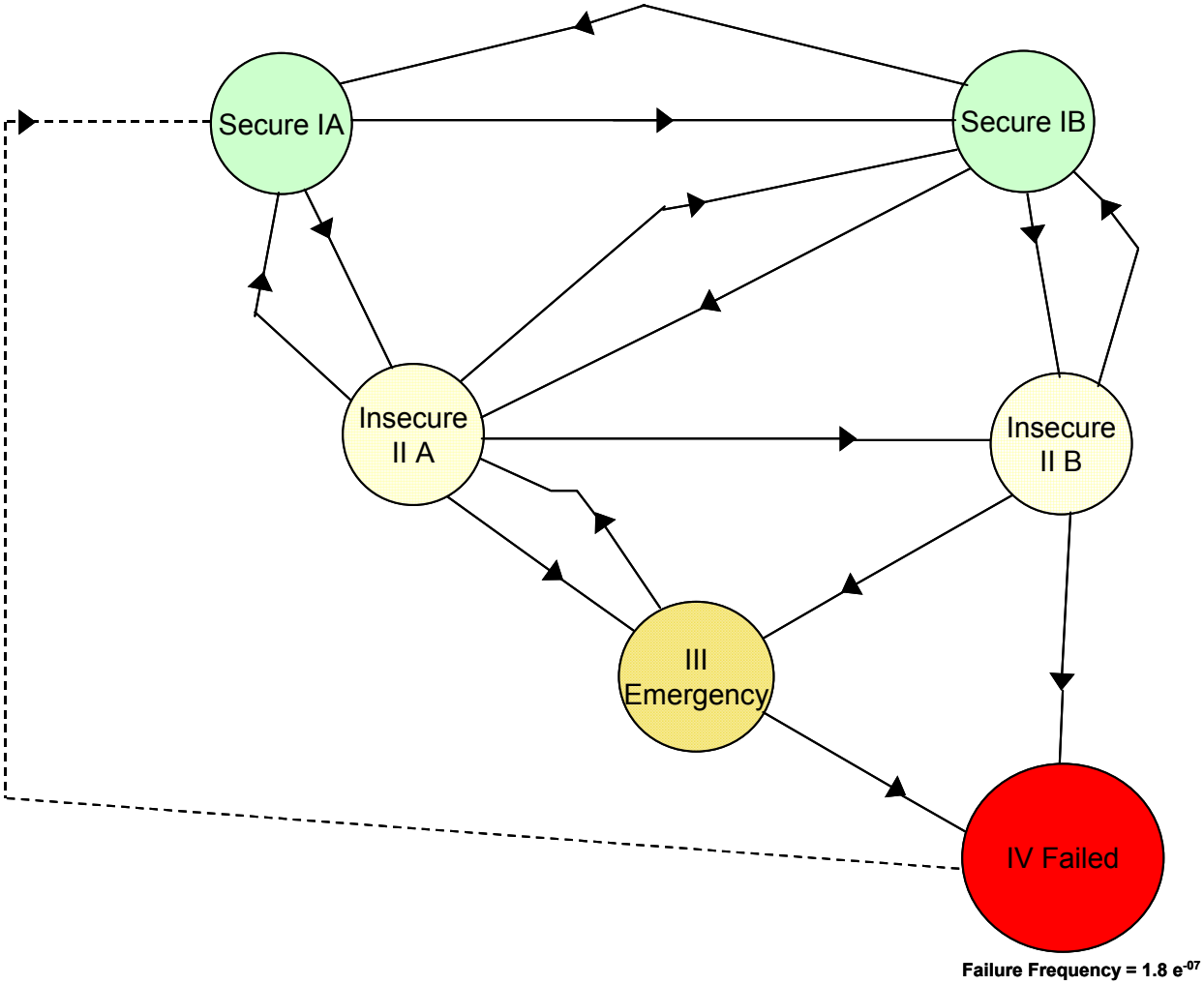
In Exhibit 4 we have assumed some logical transition probabilities: the “downhill” transitions of decreasing reliability due to contingency and loading events are put at 0.5 percent, corresponding to a contingent event occurring a little less than once a week. Further, the “restorative” transitions due to operational action are designated to be 0.95, meaning that 95 percent of the time operations will correct the problem within one hour. Anecdotally, these are conservative values in the experience of at least one large North American RTO (implying that contingent events happen once every two weeks and/or operator success rates are higher than 95 percent).

Exhibit 4: The Markov Process Model



These transition probabilities can then be used to simulate/analyze the system and determine the overall probabilities of a reliability failure within 10 years. These statistics are shown in Exhibit 5. The net result is that the system shows a failure frequency of 1.8 e^{-07}, i.e., a reliability failure once in 1600 years.

Exhibit 5: Example of Transition from "Failed" State back to "Secure" States with Final Failure Probability



However, even the most reliable grid operations have had localized outages more than once in 10 years. The simple model at this point is off by 2 or 3 orders of magnitude given "typical" event rates [3]. Additional reliability factors must bring the simple R@R model closer to observed behavior. The difficulty is to match observed statistics not to two decimal places but to an order of magnitude.

Factors Affecting State Transition Probabilities

Some contributing factors have the effect of increasing the probability of the "first" N-1 transmission or generation contingency. Familiar examples are weather and load dependencies – that is, high temperatures or severe storms that change probabilities of transitioning from state to state. Less familiar but arguably more important factors include activities such as maintenance activity. For example, the

presence of maintenance crews in an energized substation automatically increases the probability of an "event."

Some contributing factors will increase the probability of the "next" N-1 or even N-2 event. Occurrence of the first N-1 event should a priori increase the probability of the second event. Ann integrated cumulative loading effect increases the probability of a failure (i.e., transformer temperature and line sag) even if normal limits are not exceeded, as well as a rapid cumulative effect of limits being exceeded.

The effect of total load and load versus forecast can be included. Loads much greater than forecast inherently imply riskier conditions as conditions deviate from plan.

Some factors decrease the probability of successful "return" transitions. If a primary Energy Management Systems (EMS) is already down, if data communications have failed, or if an inexperienced operations crew is on duty, the probability that a successful recovery may not be achieved is increased. A failed primary EMS increases the possibility that operations could be without system visibility upon a back-up failure. This increases the probability that limit excursions would go unnoticed. Just as with transmission maintenance in a substation, software maintenance activity in an EMS or telecommunications maintenance activity temporarily increases the probability of a failure.

While truly unplanned transmission outages appear to occur at a rate of once every week or two, a delay in the completion of planned outage activity can also upset operating plans. Statistics on these delays from planned outage recovery may be different from the unplanned events as planned outages occur almost on a daily basis.

Additional factors that might be considered include whether restorative actions require the cooperation of market participants, the probabilities of successful unit start ups based on unit types, temperature, as well as similar types of operational concerns. As a factor in developing contingency probabilities the likelihood of protection system failures would need to be considered, as discussed further below.

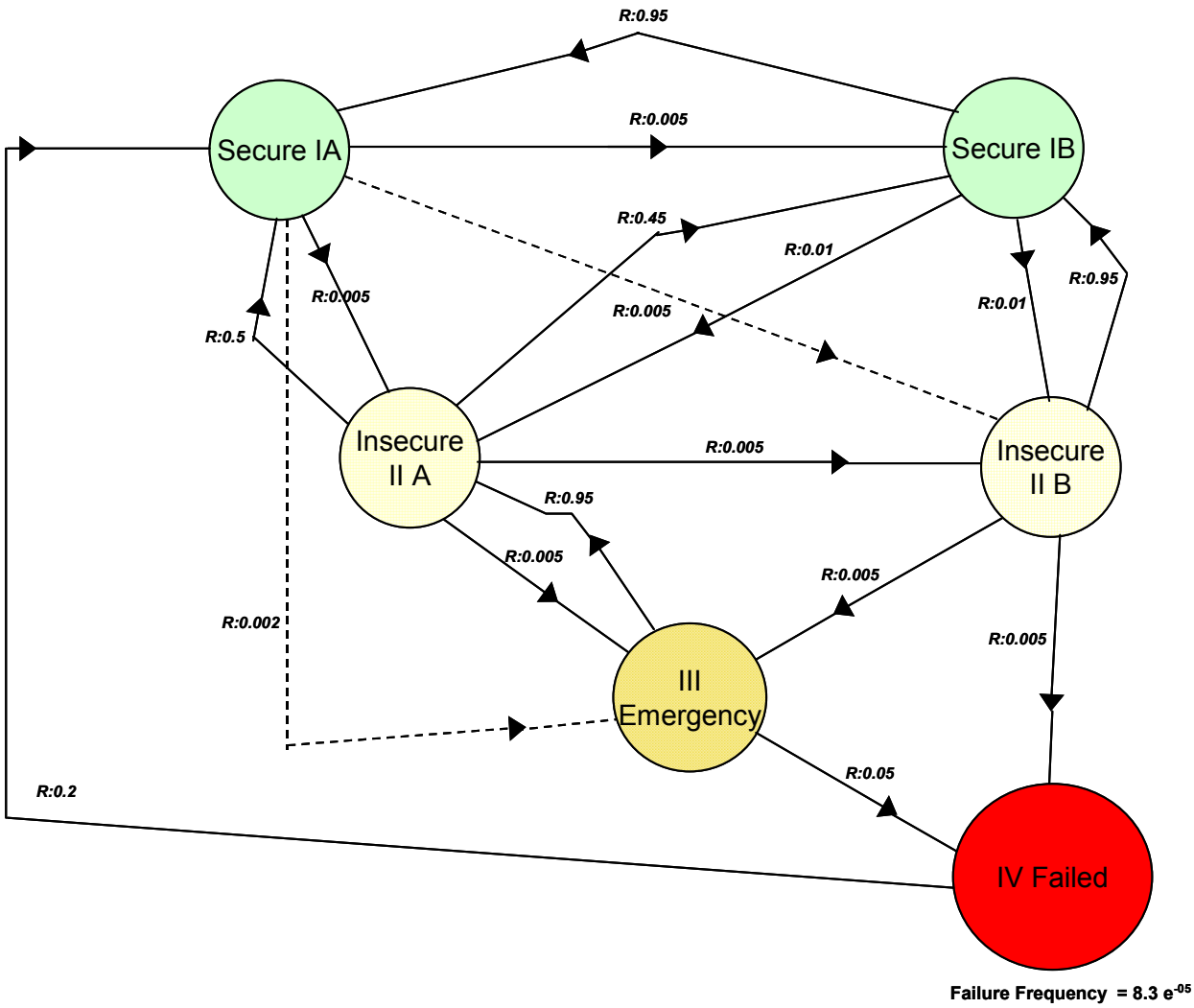
The overall impact of Standard Market Design (SMD) and Locational Marginal Price (LMP) based system operations may not be fully understood. The major advantage of SMD is articulated to be that reliability and market economics are handled in an integrated way. This is certainly correct, in so far as the analysis goes. [7]

However, an LMP-based system dispatch will always have some transmission paths loaded up to "normal" limits whenever congestion is present. On the one hand, "regional" oversight of this process by an ISO leads to an improved security dispatch process compared to a number of control areas performing localized security dispatch. On the other hand, in a pre-deregulation world many control areas would not normally engage in economy transactions right up to security limits. In fact, systems are often operated with transmission "slack" due to the lack of rigorous security dispatch programs.

On balance, the system is probably operated closer to reliability boundaries under an LMP paradigm. This leads to the observation that any errors in the LMP process due to seams issues, data errors, software errors, failure of participants to follow instructions all can add to the probability of a downhill state transition.

A version of the R@R model that produces failure probabilities more in line with the real world is shown in Exhibit 6. Here, additional transition paths representing failures in the security dispatch/contingency analysis process and increased likelihood of operational errors due to market participant failures, seams coordination issues, etc., have been factored in. The model produces a failure rate of 8.3 e^{-05} - or something between once in one and two years. This is probably realistic on a continental level but pessimistic on an ISO level. Fine-tuning the transition probabilities will result in rates representative of particular grid operations.

Exhibit 6: R@R Model Producing Failure Probabilities Closer to Real World Occurrences



A representative list of factors affecting transition probabilities and their order of magnitude impact is shown in Exhibit 7.

Exhibit 7: Factors Affecting Transition Probabilities

RT Limit Violations
N-1 Limit Violations
Weather
Scheduled Outages
Unscheduled Outages
Maintenance
Equipment Failures
EMS Problems
Labor Problems

Engineers may complain that this approach is imprecise and inaccurate. However, existing methodologies are already arguably shown to ignore the biggest causes of major outages. The purpose of R@R is NOT to precisely compute an alternative figure of merit to LOLP, for instance, that can be used in the same way that a detailed stochastic model is used to compute the value of a Congestion Permit Hedge[1]. Rather, R@R's purpose is to determine a gross measure of reliability that is sensitive to changing conditions and which reflects many factors not considered in engineering models.

If the only observed data available for use to "fit" the model is the failure rate, then there are too many degrees of freedom (the 17 transition probabilities) in even this simple model. In order to fit the model with intellectual integrity we need to

- Develop observations of the stationary probabilities of all the states in the model – an exercise which could readily be performed but for which published data is not available today and which in any case are not stationary due to all the operational factors identified above, and
- Reduce the degrees of freedom by parameterizing some of the transition probabilities – fixing their relationships to each other, for instance.
- Formally recognize that the transition probabilities are themselves unknown and time varying

Determining State Transition Probabilities

Rough estimates for the transition probabilities can be developed via a number of paths:

- **Using statistics that are already collected in transmission operations and planning, including:**

  - Probabilities for generator, line and transformer, and other outages
  - Probabilities for successful starts of generators (Combustion Turbines especially)
  - Statistics for various levels of operating reserves
  - MTTF and MTTR statistics for EMS systems and telecommunications

  These kinds of statistics can be used to build up transition probability contributions in aggregate from component-based analyses.

- **Inferring statistics from other observed data that may be available.** Statistics not directly observed today but where data is available include the probabilities of line and transformer outages based on existing severe weather conditions. In many systems, sufficient historical data also is kept to allow the derivation of such statistics. Other inferred statistics include probabilities of transmission outages given the local presence of maintenance activity, and probabilities of transformer failures based on short-term historical loading and ambient temperature conditions.

- **Conducting experiments, especially with regard to operator effectiveness.** A number of statistics can be experimentally observed. Many control areas – statistically less than 50 percent today but likely more in the future under new NERC guidelines - conduct operator simulator training. Statistics can be collected on how frequently operators fail to take appropriate corrective action against simulated emergency conditions and these can be used in modeling the "return" transitions.

- **Developing models that provide some insight into how statistics might evolve.** There are also statistics that must be modeled without significant observations to support them. These include failures of market participants to follow instructed actions, and failure of protection systems due to incorrect settings versus component failure. Here it may be appropriate to consider that if secondary protection has been observed to act correctly within some time span, for example one to two years, it can be assumed that it will function correctly. If it has not been

[1] Congestion permits compensate the holder financially for day-ahead congestion.

observed to work then it is suspect. This has the effect of increasing particular contingency probabilities.

Even with the most diligent efforts to pursue all the possible ways of quantifying transition probabilities, the non-stationary nature of the model and the extent to which it is an extreme reduction of a very large, complex physical process will guarantee that the probabilities assigned to the various transitions will always have some uncertainty. Other engineering disciplines (robotics, telecommunications, web architectures and loading analysis, for example) deal with similarly complex and hard to observe phenomena and have had success with the application of Fuzzy Markov Processes.

Fuzzy Markov Processes

The Fuzzy Markov Process [8] [9] [10] explicitly contemplates that the state transition processes are themselves unknown members of fuzzy sets – which seems to perfectly fit the problem defined above. Under fuzzy probabilities, we "sort of" know the transition probabilities within some rough boundaries that are not sharp. The mathematics allows us to transform the fuzzy transition probabilities into fuzzy state probabilities, that is, to incorporate the uncertainty in the transition probabilities themselves into the pdf of the states. An exposition of the Fuzzy Markov Process is beyond the scope and space of this paper but three observations about the use of fuzzy logic relative to this problem can be made. First, working the examples is more difficult because readily available failure analysis software usually does not incorporate the methodology. Second, the fuzzy process is mathematically robust and not sensitive to small errors in the transition probabilities when there are order of magnitude differences among them as is the case in this problem and where classical Markov chains are sensitive to errors. Third and most important, the gross conclusions will be the same but incorporating a fuzziness to the state probabilities reflecting the uncertainties in the transition probabilities.

How Insecure Are We?

The R@R model is deliberately kept very simple for two reasons:

1. It is far easier to understand what it tells us about gross system reliability as influenced by all the operational and non-engineering factors we want to consider, and
2. It will be much easier to fit the model to the thin set of observations that we really have.

Much more detailed system models could be incorporated while still having tractable Markov process transition matrices to manipulate. In fact component failure analysis does precisely this in other disciplines. However, it is preferable that this level of detail and dimensionality be kept behind the scenes, as it were, being subsumed in the gross transition probabilities visible in the simple model. Better to be fuzzy about whether we are really insecure than to have angst over how insecure we are.

However, this philosophy is still unsatisfying in one important sense. Not all reliability failures are equal, and it would be highly desirable to be able to quantify the expected magnitude of a reliability failure. In other words, what is the pdf of MW of service lost due to a reliability failure? If we can generate this pdf then we have a true R@R measure analogous to V@R in the financial world. In order to do this we have to return to the engineering model of transmission contingency analysis.

Role of Probabilistic Contingency Analysis in R@R

Work has been performed over the years on probabilistic contingency analysis. However, emphasis waned, as with all reliability research, while intellectual capacity was devoted to "market" and deregulation issues.

The concept is simple: assign a probability of occurrence within the time window of interest to each independent single contingency and then look at the aggregate results of all contingencies. If we use contingency analysis to produce "safe or not safe" answers only, then we can get an aggregate probability of "safe" or "not safe" at the moment that the contingency analysis is performed.

This can be put in the context of the R@R model above and could be used to drive state transition probabilities. However, all the arguments as to why equipment failure statistics alone do not suffice to explain observed reliability failures still apply. If we accept that the calibration of the reliability model state transition probabilities creates, in effect, a scaling factor to the results of contingency analysis particular to each state then the probabilistic analysis can be used as a factor in driving state transition probabilities at a moment in time.

In the end the Markov model above always has contingency and other physical (load change, for instance) events on the transmission/generation system as the causes of state transitions. The various non-contingency factors affecting the transition probabilities are in the end affecting contingency and return probabilities. So we can use the lessons of the Markov model to determine the probability weightings or scalings to be used in a probabilistic contingency analysis.

An obvious advantage of this approach is that most large grid operators perform contingency analyses today. The computation of a probabilistic security index does not complicate the simulation/solution process at all and has minimal effect on the overall complexity and computational cost of the contingency solution.

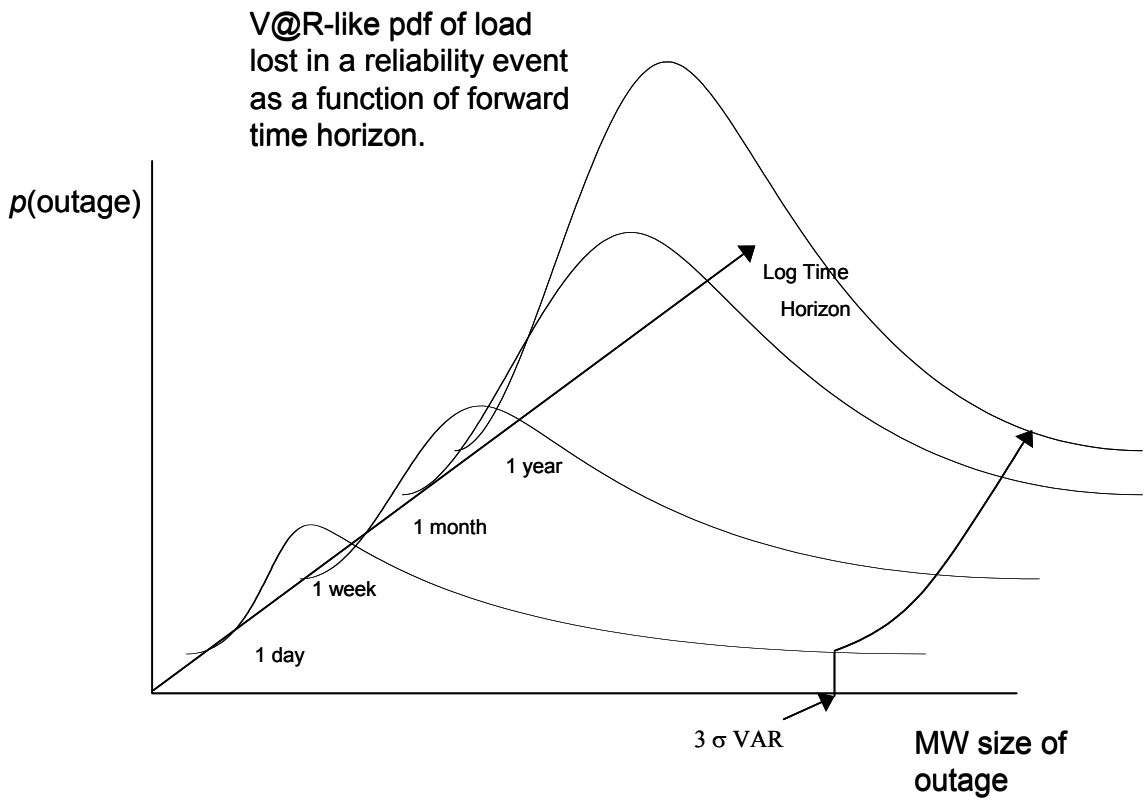
Extending R@R to a Metric of Quantitative Failure

Conceptually, the model has been developed to allow an operational computation of a probability of failure – useful in itself as an index. However, it is not likely to be useful in decision making without some quantitative measure of “how insecure” the system is – how can we quantify the magnitude of a probable failure.

This requires a quantitative assessment of the impact, in terms of potential load lost, of each potential chain of contingencies that lead to an emergency/failure condition. We have to say “potentially” lost as contingency analysis - either linear DC load flow or AC load flow based - will never actually get to which load is lost (buses/stations deenergized). Only dynamic or transient models claim to actually identify protective equipment actions and subsequent switching to deenergize parts of the grid. Arguably, these methods can be used, with great effort, to analyze what did happen after the fact once sequence of events data is available. However, they are less likely to be able to predict precisely “what will happen” for all the reasons discussed above of non-engineering risk.

If each contingency has an a priori probability of occurrence and an analyzed security index impact then we can develop a pdf of the post contingency security index from all the contingencies as approximated by the resulting index values bucketed into the quantitative failure buckets. In other words, we can compute an R@R that provides a pdf of “load at risk” for a specified future time period, very analogous to a V@R calculation (see Exhibit 8).

Exhibit 8: R@R



Mapping the security index to a magnitude of reliability failure is the most difficult aspect of the problem. The classic security index is a weighted sum of squares of post contingency values normalized to limits, and this does not directly map to MW interrupted. However, there are several possible ways to attack this problem.

We postulate that failures, which interrupt load, are a result of an imbalance among load, generation, and imports over a region of a network. Each region affected has to be dynamically determined as a result of post contingency loads computed in each case. Then the loads at risk for each case can be weighted by the contingency probabilities and summed to get a load at risk figure.

We can use DC load flow mathematics to compute distribution factors for post contingency flows as a result of line/generator outages and extend this to a linearized model for second and third contingency analysis over a wide number of cases. The industry is both familiar and comfortable with this methodology. For each final contingency state that causes overloads we can identify the cut set of branches determining a region and identify the magnitude of load at risk. [11] [12]

It is also possible to formulate an index of load at risk based on the post contingency voltages from an AC contingency analysis. This avoids the need for cut set analysis but requires AC solutions, which do not allow as straightforward a linearization.

R@R in Operations

The model can be used in operations to determine an index useful to compute and track over time. Like a stock market index, it will be useful primarily as a “change indicator” and can evolve to something used to drive dashboard style presentations of conditions.

R@R in Planning

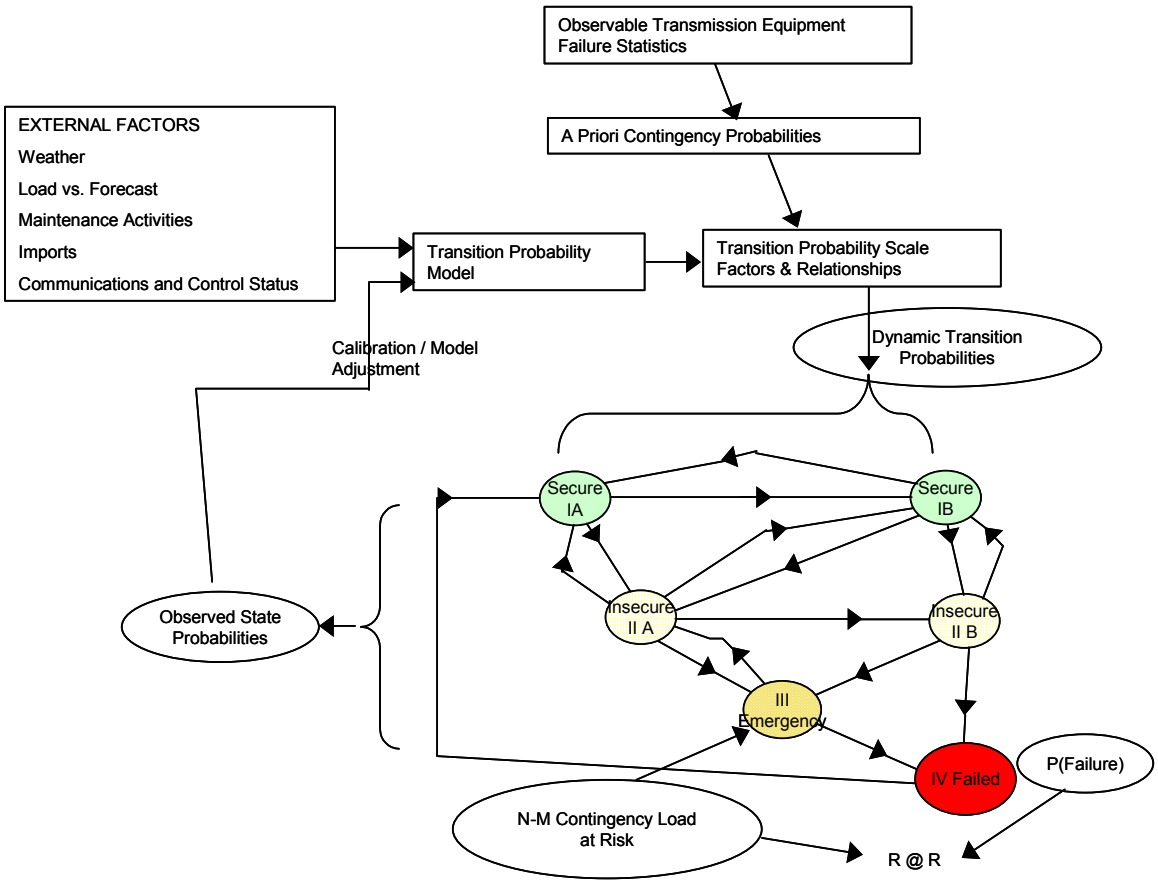
The Markov model can be used to create an "expected" R@R value over time, including risk as a function of load, seasons, and scheduled maintenance.

If control areas determine an acceptable level of R@R then the impact of planned construction and the like (or maintenance for that matter) on R@R can become a metric in evaluating competing plans. Most significantly, this can be used to compare dissimilar types of initiatives aimed at improving reliability. For instance, the impact of an extensive operations coordination and training program within a region could be compared to specific transmission investment or load relief programs.

Summary

A process chart for the development of R@R is shown in Exhibit 9. We collect available statistics on reliability failures, infer additional statistics; experiment or model other statistics, and prepare a model that drives the transition probabilities in the state model.

Exhibit 9: Process Chart for Development of R@R



The state model is calibrated to achieve a probability of "failure" that is within range of observed history for the region/grid of interest and for a group of similar grids. This results in a set of contingency probabilities that are generally higher than we might otherwise anticipate to account for the various non-engineering failure factors.

The probabilistic contingency analyses (operationally) are performed to determine the amount of load at risk by each chain of contingencies that lead to failure. This yields a pdf of load at risk given a failure; the state model leads the pdf of a failure; the two together provide an R@R pdf as desired.

In the financial world, the concept of portfolio optimization is well known – how to optimize the risk/reward trade-offs inherent in investment decisions. The energy industry employs portfolio optimization to determine how to best hedge retail delivery portfolios or how to apportion investments in supply contracts and generation assets.

It has been difficult if not impossible to apply these methodologies to transmission planning for two reasons. First, there has not been a way to relate reliability to economics; that is, to make improved reliability fungible. So instead, the transmission planning analysis is driven by "requirements" or by the economics of congestion costs. Second, true measures of reliability have been hard to come by.

Furthermore, the "requirements" based analysis only addresses grid hardware investments; it does not allow the consideration of investments in IT, communications, and people in the process. Budget allocations between the two kinds of investment are at best made at a gut level, or more realistically, are left to the politics of grid charges, department budgeting, and the like.

The concept of an R@R measure will not solve the fungibility problem – the question of how much should the consumers pay for reliability (for a similar VAR based approach to this problem see [13]) - nor will it solve the problems of how to fund transmission investment.

However, it does provide a framework for balancing investments/expenses in non-transmission investments with grid investments. A very good set of questions can be posed as follows:

- What is the improvement in reliability obtained from an increase in grid charge driven by investments in IT and people?
- How will we know after the fact that we have obtained that proposed increase?
- How do we balance that investment/expense with money spent on copper, steel, porcelain, and maintenance?

An R@R methodology as laid out in this paper will go a long way to establishing a quantitative framework for answering these questions.

Ralph Masiello is Senior Vice President, Energy Systems Consulting with KEMA, Inc. A Fellow of the IEEE, he has over 20 years experience in Transmission and Distribution Operations and in control systems implementations at many of North America's largest utilities. Dr. Masiello can be reached at rmasiello@kemaconsulting.com.

John Spare is a Principal Consultant for T&D Consulting, KEMA, Inc. He has 31 years of experience in electric utility planning, engineering, and operations support including major projects in transmission and distribution reliability, reliability-centered maintenance, equipment condition monitoring, and asset management. Dr. Spare can be reached at jspare@kemaconsulting.com.

Alan Roark is Manager, Risk Assessment with KEMA, Inc. Mr. Roark has over 15 years experience in forecasting and risk management with various energy companies. Mr. Roark can be reached at aroark@kemaconsulting.com.

Sam Brattini is an Executive Consultant with KEMA, Inc. He has over 37 years of experience in the electric utility industry, including over 27 years of experience providing consulting services related to electric utility operational infrastructures. Mr. Brattini has managed major EMS planning and procurement projects for both domestic and international clients. Mr. Brattini can be reached at sbrattini@kemaconsulting.com.

References:

[1] Billinton, R. and R. Allan. “Reliability Evaluation of Power Systems”, (New York: Plenum Press, 1984).

[2] Ilic, M., J. Arce, Y. Yoon, and E. Fumagalli. “Assessing Reliability as the Electric Power Industry Restructures”, Electricity Journal, March 2001, page 55-67.

[3] U.S. - Canada Power System Outage Task Force. “Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations”, April 2004.

[4] Jorion, P. “Value at Risk: The New Benchmark for Managing Financial Risk”, (New York: McGraw-Hill, 1996).

[5] de Fontnouvelle, P., V. DeJesus-Rueff, J. Jordan, and E. Rosengren. “Using Loss Data to Quantify Operational Risk”, Federal Reserve Bank of Boston, April 2003.

[6] Haggstrom, O. “Finite Markov Chains and Algorithmic Applications”, (Cambridge: Cambridge University Press, 2002).

[7] Hogan, William W. "Successful Market Design ("SMD") and Failure Diagnosis: Blackouts and Lampposts in Regulating Electricity Markets." Center for Business and Government, October 2003.

[8] Buckley, J. and E. Eslami. “Fuzzy Markov Chains: Uncertain Probabilities”, Mathware and Soft Computing, 9 (2002), pages 33-41.

[9] Puyin, L. “Fuzzy-valued Markov Processes and their Properties”, Elsevier Science B.V., October 1997, pages 45-52.

[10] Zimmermann, H.J. “Fuzzy Set Theory and its Applications”, Kluwer Academic Publishers, 2nd Revised Edition, 1991.

[11] Brandwajn, V. “Complete Bounding Method for AC Contingency Screening”, Power Systems, IEEE Transactions on, Volume: 3, Issue 2, May 1988, pages 724-729.

[12] Brandwajn, V. “Efficient Bounding Method for Linear Contingency Analysis”, Power Systems, IEEE Transactions on, Volume: 3, Issue 1, February 1988, pages 38-43.

[13] Joy, C., J. Spare, and A. Roark. “Applying Financial Risk Controls for Power System Operation and Planning”, 8th International Conference on Probability Methods Applied to Power Systems, Ames Iowa, September 2004.

[14] Dy Liacco, T. E., "The Adaptive Reliability Control System," *IEEE Trans. on PAS*, vol. PAS-86, May 1967.