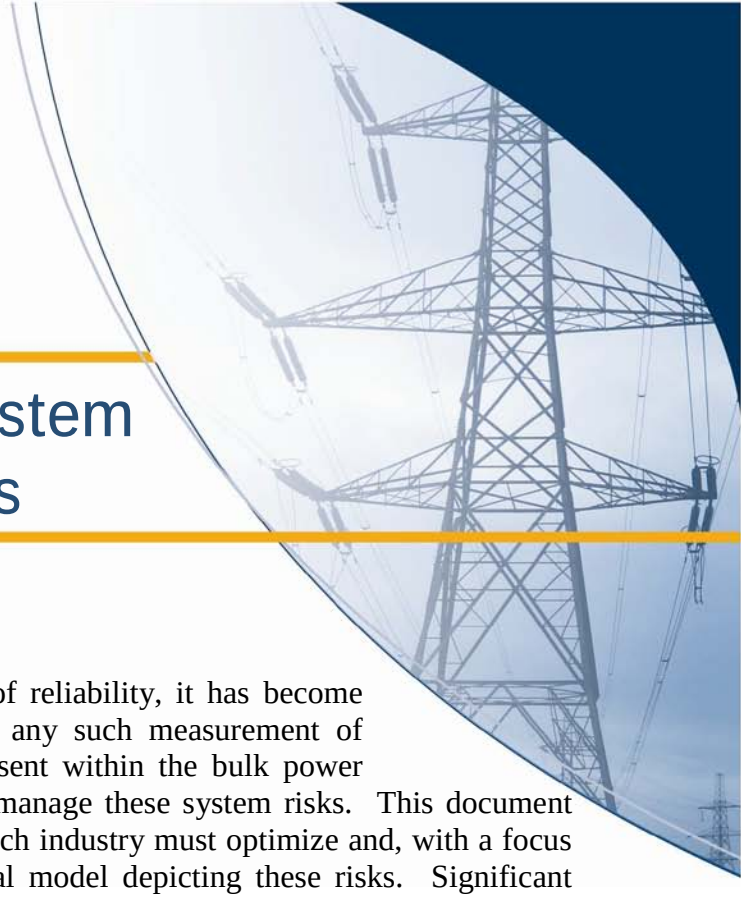
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION



Integrated Bulk Power System Risk Assessment Concepts

Executive Summary

In developing methods to measure acceptable levels of reliability, it has become clear to the Reliability Metrics Working Group that any such measurement of reliability must include consideration of the risks present within the bulk power system in order for us to appropriately prioritize and manage these system risks. This document identifies several categories of system risks against which industry must optimize and, with a focus on the subcategory of risk events, details a conceptual model depicting these risks. Significant efforts have been undertaken to determine and quantify the impacts of various historical events for which metrics may exist; this quantification helps to establish the foundation for measuring system performance and for considering risk mitigation prioritization. With this model it is expected that the industry will be better positioned to establish methods for quantifying the various risks within the system, prioritizing each of those risks and developing methods to optimize impacts against costs. This work relies heavily upon risk assessment methodologies.

Risk assessment is an essential tool for achieving the alignment between organizations, people and technology in quantifying inherent risks, identifying where potential high risks exist, and evaluating where the most significant lowering of risks can be achieved. Being learning organizations, the Electric Reliability Organization (ERO) along with the Regional Entities and the Registered Entities can use these tools to focus on the areas of highest risk to reliability and provide a sound basis for developing results-based standards and compliance programs. Risk assessment also serves to engage all stakeholders in a dialogue about specific risk factors, and helps direct a strategic plan for risk reduction and early detection. This document is intended to establish a method for measuring inherent system risks, evaluating risk events and integrate and complement initiatives currently under way, such as standard development, root cause analysis, events analysis, metrics and prioritization. Furthermore, this work does not purport to supersede other industry forums or mechanisms which evaluate priorities or establish policy.

The concept and framework proposed in this whitepaper provide a basic guide for the stakeholders to follow and make informed decisions, identify trends to lower overall system risk, and communicate the effectiveness of reliability programs.

Recommendations

1. NERC should embrace the use of risk assessment to identify trends in addition to lessons learned in order to improve bulk power system reliability.
2. Risk-informed prioritizations should be used to support standards development.
3. The risk to bulk power system reliability should be assessed annually as risk factors are time and configuration dependent.
4. As trend evaluations increase the knowledge of risks to the bulk power system, data required to support additional assessment should be gathered. Further, NERC's event analysis activities may be requested to develop root-cause analysis.
5. Risk Assessment should be incorporated into NERC's annual *Long-Term Reliability Assessment* since it provides an important vehicle to communicate the status of bulk power system reliability.
6. NERC should continue to coordinate and communicate with other working groups (e.g. EAWG, RMWG, DSR-SDT, etc.)

1. Background

With modern technology and higher reliability requirements, virtually every complex system in the world, such as communication, financial computing and bulk electric systems benefit from integrated risk assessment. NERC's traditional definition of "reliability" consists of two fundamental concepts – adequacy and operating reliability:

> ***Adequacy***[1] is the ability of the electric system to supply the aggregate electric power and energy requirements of the electricity consumers at all times, taking into account scheduled and reasonably expected unscheduled outages of system components.
>
> ***Operating reliability***[2] is the ability of the electric system to withstand sudden disturbances such as electric short circuits or unanticipated loss of system components.

This definition was recently further refined with the identification of specific characteristics that define an Adequate Level of Reliability (ALR):[3]

1. The System is controlled to stay within acceptable limits during normal conditions;
2. The System performs acceptably after credible Contingencies;
3. The System limits the impact and scope of instability and cascading outages when they occur;

---

[1] Definition of Adequacy is available at http://www.nerc.com/docs/standards/rs/Glossary_of_Terms_2010April20.pdf.

[2] NERC had used the term "security" until September 2001 when security became synonymous with homeland protection in general and critical infrastructure protection in particular. To remedy the increasing confusion over what we meant by security, NERC replaced that term with "operating reliability." Operating reliability is not a definition in the NERC Glossary of Terms but instead is a reliability concept that predates the ERO.

[3] Details of the ALR definitions are available at http://www.nerc.com/docs/pc/Definition-of-ALR-approved-at-Dec-07-OC-PC-mtgs.pdf.

4. The System's Facilities are protected from unacceptable damage by operating them within Facility Ratings;
5. The System's integrity can be restored promptly if it is lost; and
6. The System has the ability to supply the aggregate electric power and energy requirements of the electricity consumers at all times, taking into account scheduled and reasonably expected unscheduled outages of system components.

Recent technological (i.e. intelligent electronic devices) and regulatory (i.e. ERO or NERC) changes provide an opportunity and need to enhance the current risk management practices. For example, the use of new information technologies (e.g. internet, open communication protocols, etc.) can lead to interdependencies and complexities that create new vulnerabilities and risks. These advancements represent new risks to reliability that must be managed, and do not lend themselves to the traditional, avoidance of risk approach historically used due to complexities and less known consequences. Therefore, NERC proposes to develop a set of risk management tools in this whitepaper, including a risk-informed approach for identifying and classifying the severity of risk events. The development of the tools and risk-informed severity scales are aimed to support:

1) ***Standard Development*:** risk assessment can be used to prioritize standard development and identify suitable results-based performance measures.
2) ***Compliance:*** supports the prioritization of monitoring and enforcement program based on risk to the bulk power system reliability.
3) ***Lessons Learned:*** a continuous process of learning from events and reliability indicators to ensure desired performance is realized.

2. Identification of a Risk Model

The scope for the Reliability Metrics Working Group (RMWG)[4] includes a task to develop a risk-based approach that would have the benefit of providing consistency in the area of quantifying the severity of events.

Within the NERC, currently there is no accepted scale to measure the impact of events on bulk power system reliability. Additionally, there are no definitions or criteria that identify the characteristics of an event. There are a number of NERC groups that are ranking specific events based on attributes such as the number of MW affected, the systems that mis-operated, root-cause determination or the potential consequences of the identified mis-operations.[5]

It is useful to consider the definition for Disturbance[6]:

i. An unplanned event that produces an abnormal system condition.
ii. Any perturbation to the electric system.
iii. The unexpected change in ACE (Area Control Error) that is caused by the sudden failure of generation or interruption of load.

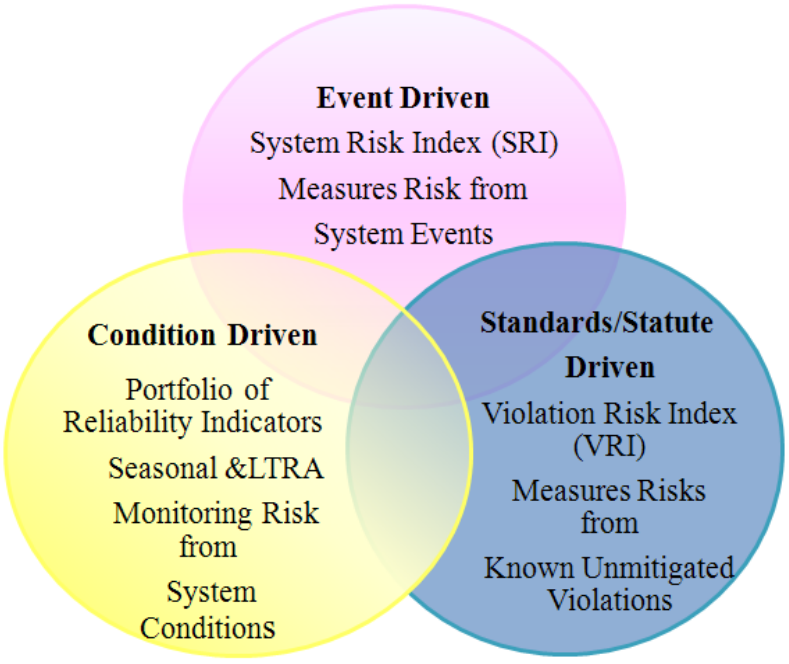
[4] The RMWG scope can be viewed at http://www.nerc.com/filez/rmwg.html.
[5] The draft of NERC's event categories is available at http://www.nerc.com/docs/pc/Item%206.l_-_Draft%20Event%20Categories%20and%20Levels%20of%20Analysis%2005042010.pdf.
[6] The NERC's Glossary of Terms is available at http://www.nerc.com/docs/standards/rs/Glossary_of_Terms_2010April20.pdf.

In fulfillment of its scope, the RMWG will develop an integrated risk ranking process, where a foundational risk model must be developed to establish a method for measuring, managing, and mitigating risk. The beginning for this work is to identify risks within the bulk power system environment. The measurement and relative ranking of the risks will be validated using historical event data.

One approach to develop a measurement for risk is to construct tightly engineered metrics based upon decision tree criteria. However, this approach is more applicable for systems in a relatively well contained environment, notably where probabilities of a variety of components and the relationships of dependent and independent variables leading to measurable events are well known. The bulk power system exists in an environment where such an approach is not viable as it is subject to significant external effects, while, at the same time comprised of a wide variety of inputs, uses and components. Certain historic experiences may be known, and may be used to calculate event probabilities for risk events; however, the vast majority of event probabilities or occurrence rates are unknown.

NERC is developing a portfolio of risk information to quantify bulk power system reliability, including condition-driven reliability indicators,[7] standards/statute-driven violation risk measures,[8] and event-driven risk indices,[9] illustrated in Figure 1. This model attempts to capture the "universe of risk" to the bulk power system for which risk measurement methods for the "Event-Driven Risk" are developed.

Figure 1 – Conceptual Risk Model for Bulk Power System



[7] The details of reliability indicators are available at http://www.nerc.com/docs/pc/rmwg/RMWG_Metric_Report-09-08-09.pdf.
[8] Detailed standards/statute-driven risk measure proposals are available at http://www.nerc.com/filez/pmtf.html.
[9] Details on NERC's TADS, GADS and Event Analysis Databases are available at http://www.nerc.com.

Event-Driven Indicators – The Event-Driven approach provides a basis for prioritization of events based on bulk power system integrity, equipment performance, and/or engineering judgment. The event-driven severity-risk indicators can serve as a high value risk assessment tool to be used by stakeholders to investigate and evaluate disturbance history that can be useful in measuring the severity of these events. The relative ranking of events requires industry expertise, agreed-upon goals and engineering judgment. The final numerical ranking/scoring considers the NERC approved ALR[10] and existing NERC Standards.

Standards/Statute-Driven Indicators – The violation risk index measures improvement in compliance with Reliability Standards.[11] Each violation is associated with a predefined Violation Risk Factor (VRF) and an assessed Violation Severity Level (VSL). Based on these factors, known unmitigated violations of elevated risk factor requirements are weighted higher than lower risk factors. The index decreases if the compliance improvement is achieved over a trending period. Using information assembled through the industry, and starting the fourth quarter of 2008, the violation risk index indicated that risk to bulk power system reliability from known unmitigated violations of NERC Standards appears to have been reducing for five consecutive quarters. As of this time, the top five violations contributing the most risk to reliability are PRC-005, PER-002, EOP-005, FAC-003, and EOP-002.

Condition-Driven Indicators – Condition-driven indicators focus on a set of measurable system conditions to assess bulk power system reliability. These reliability indicators identify factors that positively or negatively impact reliability and are early predictors of the risk to reliability from events or unmitigated violations. A collection of these indicators measures how far reliability performance is from desired outcome, and if the performance is headed in the preferred direction.

The integrated model of event-driven, condition-driven and standards/statute-driven risk information can be constructed to show all possible logical relations between the three risk sets (disturbance events, at-risk conditions, and unreliable violations). Each risk set may, but does not need to overlap with the other two sets. The overlapping area or intersection represents common elements among all three sets. For example, if an Interconnection Reliability Operating Limit (IROL)[12] were exceeded for greater than the associated time (T_v), the event would be considered to be simultaneously a standards/statute-driven event, a condition-driven event and a risk event. Risk-informed decisions can be made from each of these perspectives to lower overall system risk, provide input to risk-informed standards development process, and communicate the effectiveness of reliability programs.

This whitepaper focuses on event-driven risks. Event-driven system risk indicators consider a wide variety of events and examine both the probability of an event and its possible consequences. By answering "what can go wrong, how likely it is, and what could the consequences be," better guidance is offered for the development of standards requirements and mitigation of compliance violations that are most important to the reliability of the bulk power system. Using this integrated

[10] Detailed definitions of ALR are available at http://www.nerc.com/docs/pc/Definition-of-ALR-approved-at-Dec-07-OC-PC-mtgs.pdf.
[11] Detailed standards/statute-driven indicators can be viewed at http://www.nerc.com/filez/pmtf.html.
[12] Details on operating within IROLs are available at http://www.nerc.com/files/IRO-009-1.pdf.

risk assessment approach, NERC will be in position to continuously monitor industry reliability performance to identify adverse trends and take prompt actions.

2.1 Basis for Results-Based Standards and Compliance Programs

NERC's reliability standards provide the foundation for industry to recognize and respond to reliability risk factors challenging the six ALR[13] characteristics and eight Reliability Principles[14] used to guide standards development. The industry uses these characteristics and Principles to measure their individual systems and define risk factors threatening its reliability. An effective approach for prioritizing NERC's Standards projects is to ensure those that can have the greatest ability to reduce the risk to bulk power system reliability are enacted.[15] In addition, stakeholders have recommended that NERC develop a more systematic process for prioritizing new Standards projects, focusing the development on those that will lead to the greatest improvement in reliability.[16] The risk assessment model proposed in this whitepaper can be used as a basis for results-based standards development and prioritization of new and/or existing Standards projects leading to the greatest improvement in reliability.

As the NERC Compliance Program enters its third year of operation with mandatory and enforceable reliability standards, the need for consistently measuring and reporting on compliance attributes and reliability improvements is ever increasing. The risk-informed standards/statute-driven indicators can be used to indicate relative risk levels to bulk power system reliability from known unmitigated violations of Reliability Standards. Further, by deploying risk assessment findings, risk reduction can be achieved to enhance efficiency and performance of NERC's Compliance Program.

3. Examples of Risk Models

Risk models refer to the use of quantitative or statistical methods to determine the aggregate risk based on a portfolio of individual risk factors. One of the fundamental statistical methods used widely among many industry sectors is regression analysis. Other techniques include Value-at-Risk (VaR), Historical Simulation (HS), Extreme Value Theory (EVT) or Scenario Analysis to assess a portfolio of risk categories. Formal risk modeling is also required by the various institution regulators, including the Federal Aviation Administration, the Nuclear Regulatory Commission, and the Food and Drug Administration. Many firms use risk modeling to help guide a strategic plan for risk reduction and early detection.

Datasets supporting risk analyses can be classified as time-series data, cross-sectional data, or multidimensional data. Time-series datasets contain observations over time; for example,

[13] http://www.nerc.com/docs/pc/Definition-of-ALR-approved-at-Dec-07-OC-PC-mtgs.pdf
[14] Details of the Reliability Principles are available at http://www.nerc.com/files/Reliability_Principles.pdf.
[15] As of April 2010, more than 120 NERC Standards have been approved by NERC's Board of Trustees, covering planning and operating performance, frequency and voltage performance, reliability information, emergency preparation, communications and control, personnel, wide-area view, and security. Between 2007 and 2009, NERC received a total of 33 standard authorization requests (SARs), 42 standards interpretation requests, and 61 standards improvement suggestions.
[16] Three-Year Electric Reliability Organization Performance Assessment Report http://www.nerc.com/files/NERC%203-year%20Assessment_report_COMPLETE_FINAL7-20-09.pdf

transmission outages over several years. Cross-sectional datasets contain observations at a single point in time; for example, many individuals' disturbance events in a given year. Multidimensional data contain both time-series and cross-sectional observations.

4. Conceptual Model for Managing Event-Driven Risk

Historically, risk has been managed by bulk power system planners by setting thresholds and safety margins so as to avoid "unacceptable" risk, where acceptability levels are typically determined by industry experience. For example, probabilistic models have been used by industry to build systems with sufficient generating capacity so that it would fail to meet demand no more than one day in ten years. Similarly, power system operation is governed to a large extent by the "N-1 security criterion" which requires that the system, as a whole, can sustain failure of any one element (e.g. generator, transmission line, transformer etc.).[17] Conceptually, these approaches represent an avoidance of risk, by use of deterministic criteria, rather than the management of risk, by use of probabilities of events with specific known severities.

Managing risk is a single continuous process that, if implemented consistently among bulk power system owners and operators, can be used to recognize and act upon the risk to the bulk power system from undesired potential performance shortfalls. The objective of managing risks is to decrease the probability of events that reduce bulk power system reliability. The recognition of acting upon reliability risks should evolve the industry towards a single continuous process. In the graph below, Figure 2, the red line depicts the events ranging from minor outages to very high-impact extreme events. There are events that occur with high frequency, but are quite small in terms of customer impact, as depicted in the blue line. Many bulk power system events have generally no impact (and may be considered off-normal events[18] or "operated as designed" type events) due, potentially in part, to the redundancy built in the bulk power system or other mitigating operations. Additionally important in Figure 2 is a line marked "Reporting Threshold", which is conceptually a level below which the severity does not even warrant external reporting because the impact is low (or outside the jurisdiction of the regulatory framework) or the system has operated as designed (also resulting in limited impact).

Events of greater severity can be studied[19] along with the identification of overall trends as a way to manage risks associated with these events. The result would be to move the curve downward and to the right, reducing the severity and frequency of high-impact events, or eliminating them. The efficient processing of this information, to create a comprehensive rational and effective risk-mitigating and learning environment, is the challenge faced by system owners/operators, Regional Entities and NERC.

[17] Oren, S., "Risk Management vs. Risk Avoidance in Power Systems Planning and Operation," IEEE-PES, 2007, http://www.ieor.berkeley.edu/~oren/pubs/II.B.10.pdf

[18] More on off-normal events are available at the NERC RoP Section 808 and can be viewed at http://www.nerc.com/files/NERC_Rules_of_Procedure_EFFECTIVE_20100205.pdf.

[19] For this purpose NERC has created a categorization system to help filter those events which warrant more attention for learning purposes. See NERC website at: http://www.nerc.com/page.php?cid=5|252.

Figure 2

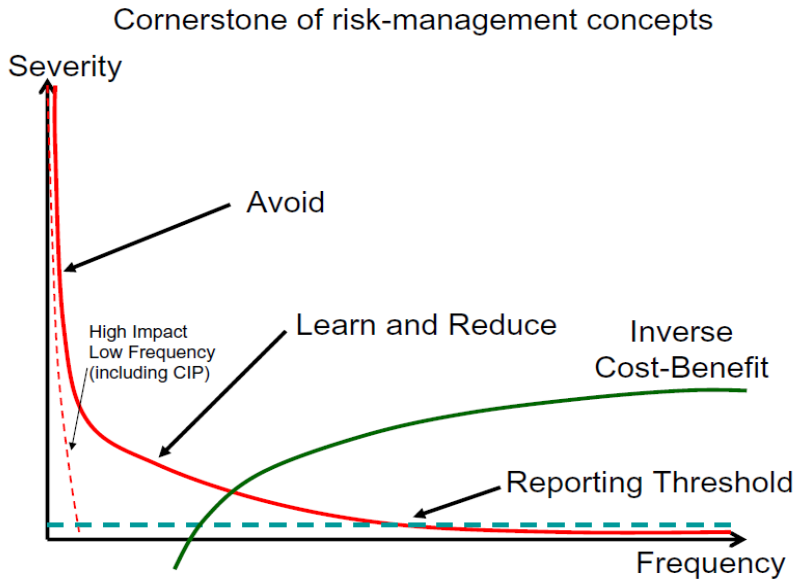
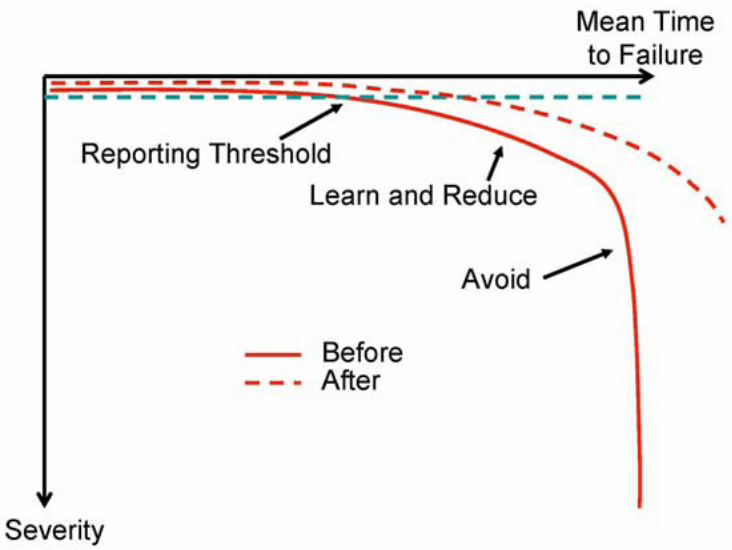


Figure 3 below changes the perspective. In addition to a reversal of the axis, the beneficial impact of reviewing events and applying knowledge is shown. By applying the risk assessment results to operations, there is the potential to extend the mean time to failure and reduce the event's severity. This concept is the fundamental premise of any risk management effort.

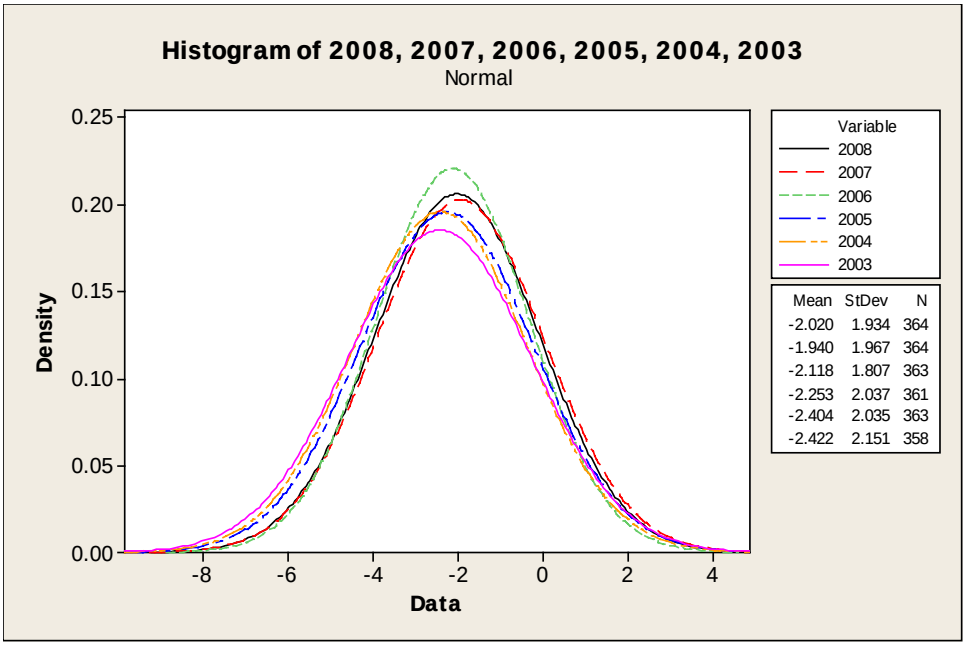
Figure 3 – Severity Reduction and Beneficial Impact



5. Severity Risk Curves Already in Use on Distribution Systems

Since the introduction of automated outage management systems and the development of the Institute of Electrical and Electronics Engineers (IEEE) Standard 1366-2003, IEEE Guide for Electric Power Distribution Reliability Indices, much greater access to reliability data within the electric distribution system has become available. This data is founded upon the calculation of customer minutes interrupted and customer interruptions within each day of the year for each system. During development, it was hypothesized that the performance of an electric distribution system could be approximated by a log-normal curve that captured daily customer minutes interrupted (translated into system SAIDI,[20] to be fungible across systems of varying sizes). If a sufficient period of time, or number of data points, were analyzed, a characteristic Gaussian curve would emerge, as shown in Figure 4.

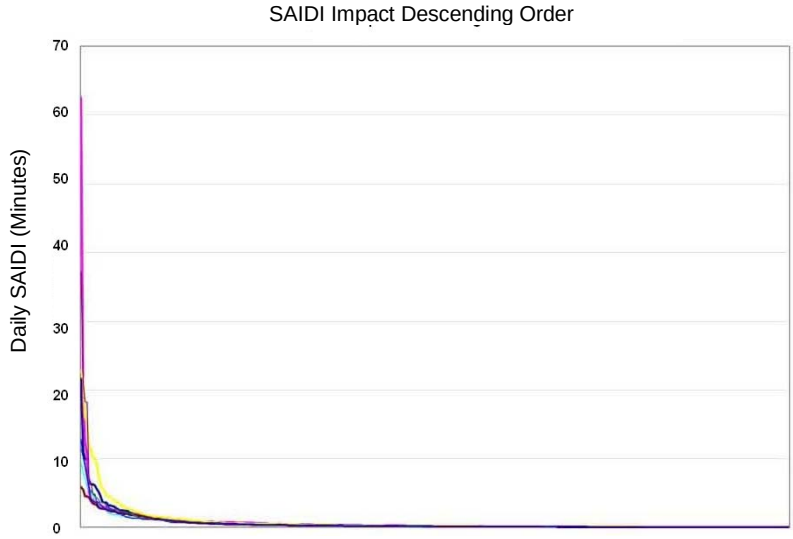
Figure 4 – Illustration of Natural Log Daily SAIDI Gaussian Distribution



If that same dataset were to be sorted in descending order, it results in a logarithmic curve as illustrated in Figure 5 below.

[20] Detailed SAIDI (System Average Interruption Duration Index) definitions are available at http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1300984.

Figure 5 – Logarithmic Curve Resulting from Descending Daily SAIDI



This curve, which also measures severity within the electric distribution system, bears great similarity to the curve shown previously for the electric transmission system. Upon further consideration, this similarity should not be surprising. Fundamentally daily SAIDI serves as an indicator of severity, while in the proposed electric transmission risk event model, load lost in addition to fractions of the transmission and generators out of service that directly contribute to an event acts as similar measures of impacts to the system's operations.

6. Data Required to Measure Risk and Severity

An integrated risk measurement process will be developed and evaluated for validity using historical event data. The identification of the system weaknesses and significant risk events is the first step to measure risk. Significant risk events are events that directly affect bulk power system performance and are a function of time horizon, voltage level, and system conditions. Further, these events, by definition, cover the majority of risks, demonstrate a consistent link to reliability, and do not overlap.

The occurrence rate of these events (events/year) will be derived primarily from existing databases such as the disturbance analysis, Transmission Availability Data System (TADS), ALR metrics, and the electricity supply & demand (ES&D) database. In order to determine statistical significant values, a 5-year period of these events will be examined. When no historical event data is available, reasonable assumptions will be included to estimate the occurrence rate of the event.

7. Severity Risk Index

Historically, to avoid events that present risk, the bulk power system has been designed using deterministic criteria to limit the magnitude of events. This deterministic criterion is based upon experienced engineering judgment. This "defense in depth" approach can benefit from risk-informed prioritization which accommodates the changing nature of the bulk power system, providing feedback on performance improvement activities.

This effort uses historical event data to develop a severity metric risk measurement tool to establish the bulk power system's characteristic performance curve. This curve would then be applied, prospectively to particular risk events, period performance assessments and provide groundwork for developing cost avoidance parameters. Further, a family of curves focused on structural (i.e. interconnection), components (i.e. generation, transmission, etc.) and trends evaluations (grouping events by causes) can be developed.

The severity of an event has a number of key characteristics, which are reflected in the ALR definition:

1) Duration of event (hours)
2) Amount of demand (MW) lost during the event
3) Number of bulk power system components forced out of service during the event
4) Unacceptable facility damage

Risk will be ranked by relative severity levels to quantify the impact of a particular event. Impact can be along multiple dimensions such as load (as a proxy for customers) or loss of facilities (such as generators, transmission lines, substations or communications facilities). These measures provide a numerical ranking to determine which events are more important to maintaining system reliability. In other words, the metrics are an integrated risk measurement system, which classifies an event's impact.

One approach is to establish a Severity Risk Index (SRI), which could serve as an indicator of severity of the major impacts into one measure. The SRI measures the change to system reliability from each event, based on transmission, generation and load outage data. Relative weights, based on industry judgment, can be used to develop prioritized measures. The value of the severity is calculated based on impact of risk-significant events and the relative weightings. For example:

$$SRI_{event} = w_L*(MW_L) + w_T*(N_T) + w_G*(N_G)) + w_D*(H_D) + w_E*(N_E)$$

Where:

SRI_{event}	=	severity risk index for specified event,
w_L	=	weighting of load loss,
MW_L	=	normalized MW of Load Loss in percent,
w_T	=	weighting of transmission lines lost,
N_T	=	normalized number of transmission lines lost in percent,
w_G	=	weighting of generators lost,

N_G	=	normalized number of generators lost in percent
w_D	=	weighting of duration of event,
H_D	=	normalized duration of the event in percent,
w_E	=	weighting of equipment damage, and
N_E	=	normalized number of equipment damaged in percent

At this time, the RMWG believes some form of blended severity weighting may serve to start to populate characteristic curves at a high and generic level. Based upon feedback from stakeholders, this approach may change, or as discussed further below, weighting factors may vary based on periodic review and risk model update. The RMWG will continue refinement of the severity risk index calculation and consider other factors that impact severity of a particular event, including equipment operated as designed and loss of load from a reliability perspective (intentional and controlled load-shedding); further it will explore developing mechanisms for enabling ongoing refinement (which should be influenced by a wide set of stakeholders) of the historic and simulated events for future severity risk calculations.

While the total number of transmission line outages may not always be meaningful, there are times where this number would provide a good indication of an event's impact to the resilience of the system. For example, if Event A in which 10 transmission lines are impacted, and compare that to Event B where 30 transmission lines are impacted, the time for the system to be returned to normal operations would typically be expected to be less in Event A. Regarding generators, there could be some benefit derived by adding a factor for total capacity lost.

The loss of load due to transmission-related events is weighted the highest (50%) since it directly indicates the unacceptable reliability level per ALR.6. The transmission outages are ranked second (30%), which reveals inability to meet ALR.1, ALR.2 and ALR.3 requirements. Generation outages are placed third (10%) because the majority of generation outages have less impact to the grid since operating reserves are allocated to preserve load and generation balance. Duration of the event is a significant factor in assigning a severity to an incident and is included as a factor in the overall severity risk index (5%). Unacceptable damage to system equipment represents a failure to meet ALR.4 requirement and is included as a factor in the severity risk index score (5%). The formula, utilizing these values, is restated as follows:

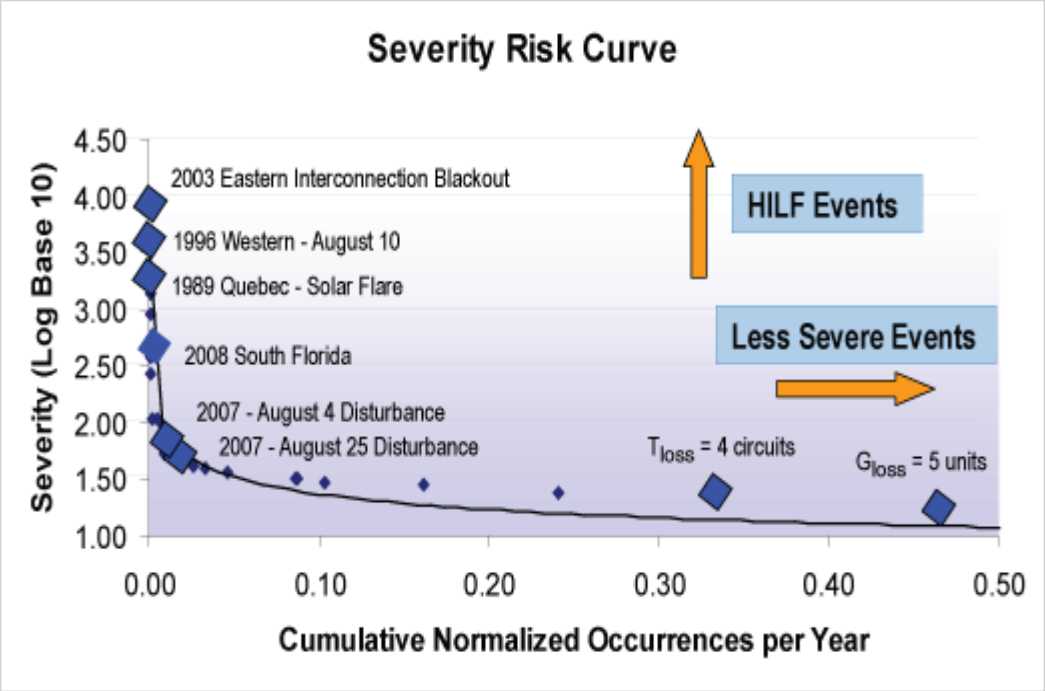
$$SRI_{event} = 50\%*(MW_L) + 30\%*(N_T) + 10\%*(N_G) + 5\% (H_D) + 5\% (N_E)$$

All system risks are being considered, including cyber security risks. First, if a cyber event occurs then the entity must ask if a "critical cyber asset" is involved. If the answer is yes then the parties must handle the assessment and mitigation according to its original plan of mitigating risks or threats that involve "critical cyber assets". Second, the entity must determine if the cyber security risk adversely impacts the BPS. One way to determine if the risk adversely impacts the BPS is to test the

risk against the Adequate Level of Reliability (ALR) attributes.[21] If the risk violates any of the ALRs then the risk will have adversely impacted the BPS. Another way to evaluate the impact of the cyber risk on the BPS is to use computer models (e.g. PSS/E, stability models) to confirm how the BPS should react to the risk against how the system actually responded. We solicited information from risk managers. The integrated risk models reflect how various stakeholder groups are trying to recognize the different risks and threats to the grid.

Other aspects impacting weighting factors include differences between electrically remote facilities which are out of service and those in close proximity which either initiate or propagate the effects of the event. In the load pocket areas where local voltage support is essential to maintain system stability, the generation loss in these areas will be weighted more. The final severity and impact scores/percentages will be determined over time by industry experts and stakeholders as appropriate. The values presented here represent an example for discussion and concept development. Figure 6 provides a risk assessment graphic representation using the aforementioned SRI.

Figure 6 – Example of BPS Risk Assessment for Risk-Significant Events



As outlined previously a theoretical logarithmic curve has been advanced where risk event severity is measured on the vertical axis and historic occurrence rate of the risk event is measured on the horizontal axis. This curve is created by taking all recorded risk events and using a proposed risk event severity scale, determining the risk event's severity. Then the risk events are sorted in descending order and what has emerged is a somewhat sparse, but power distribution curve. While the curve is sparse, this sparseness appears to be a by-product of reporting history being somewhat

[21] The draft ALR Impact Test Template is available at http://www.nerc.com/docs/eawg/ALR_Tests_Aug_10_2010_DRAFT.pdf.

short in addition to reporting thresholds the industry has traditionally operated under. As additional low impact/high frequency data is defined and greater reporting history occurs, it is expected that the ambiguity will diminish and the right end of the curve will become better defined.

8. Linkage of Severity and Rate of Occurrence

Based upon the limited data analyzed to this point, there is a linkage between risk event severity and its occurrence, leading to the further development of the curves discussed in Figures 2, 3, 5 and 6. This hypothesis will continually be tested, and if found to inaccurately portray industry experience, assessment parameters will be modified to incorporate new data points and validate an advanced approach. The equations outlined below begin the mathematical basis.

Risk, is calculated by multiplying the severity (impact of the event) and the rate of occurrence:

Risk (associated w. an event) = Severity (of the event) * (Rate of Occurrence)

The "rate of occurrence" is analogous to "frequency of the event". Postulating the rate of occurrence will be based on historical data set and statistical model, which links the severity and risk. Conceptually the risk is the area covered under the rate of occurrence and the severity curve. It is expected the detailed industry-wide risk model, including the time period used for rate of occurrence, will be established when more data is available and further analysis are completed.

9. Event Analysis: Historical Perspectives and How They May Be Quantified

9.1 Low Impact/High Frequency

Historically the majority of data collected on the transmission system pertained to fairly significant events that met specific reporting thresholds. Data below those thresholds was not centrally collected and may not have been heavily investigated for learning opportunities. NERC's GADS (generator availability data system) and newly developed TADS (transmission availability data system) provides a day-to-day operational dataset of generator and line outage data collected in a consistent way across the industry. Thus, while the historical dataset available for evaluating historic performance is sparse for high impact/low frequency (HILF), a much richer dataset is becoming available with the low impact/high frequency (LIHF) events the system has experienced. This is somewhat analogous to safety investigations and their focus on off-normal events. In other words, in order to assess the day-to-day effectiveness of the electric transmission system it is critical to logically recognize the relationship between low impact/high frequency risk events and high impact/low frequency risk events.

9.2 High Impact/Low Frequency

Measuring and monitoring high impact/low frequency (HILF) risk is another important element of the risk assessment process. Ensuring that the processes and metrics exist to provide visibility into the changing nature of these risks will be critical to risk management efforts. Identifying and monitoring reliability indicators, where they exist, will allow the industry to enact a strategic plan to detect early signs of HILF events and take preventative measures as warranted.

HILF events have recently become a renewed focus for risk managers. These risks have the potential to cause catastrophic impacts on the electric power system, but either rarely occur, or, in some cases, have never occurred. Examples of HILF risks include coordinated cyber, physical, and blended attacks, the high-altitude detonation of a nuclear weapon, and major natural disasters like earthquakes, tsunamis, large hurricanes, pandemics, and geomagnetic disturbances caused by solar weather. HILF events truly transcend other risks due to their magnitude of impact and the scope of the impact (in many cases) reaching beyond the limits of the industry sector, and the relatively limited operational experience in addressing them. Deliberate attacks (including acts of war, terrorism, and coordinated criminal activity) pose especially unique scenarios due to their inherent unpredictability and significant national security implications.

It is impossible to fully protect the system from every threat. Sound management of these and all risks to the sector must focus on determining the appropriate balance of resilience, protection, and restoration. Further, HILF risks present unique challenges to risk managers. They fall into a category of "macro-prudential" risk, which behaves differently than most forms of business risk. Macro-prudential risk is non-transferrable and cannot be fully insured against, diversified, or hedged at the individual firm level. The strength of the individual firm also does not dilute the risk to the firm from these events, as risks still exist from other players in the same sector. Therefore, this form of risk must be considered on a sector-wide basis, particularly in sectors (like the electric sector) formed of entities that are highly interconnected and interdependent.

The risks associated with the electric sector have a number of characteristics in common:

- HILF risks have the potential to cause widespread or catastrophic impact to the sector—whether through impact to the workforce in the case of a pandemic, or through widespread physical damage to key system components in the case of a high-altitude electromagnetic pulse event.
- HILF risks generally originate through external forces outside the control of the sector. For example, actions can be taken to avoid vegetation contact with a transmission line. However, no amount of preemptive action will reduce the likelihood of a geomagnetic storm or pandemic.
- HILF events can occur very quickly and reach maximum impact with little warning or prior indication of an imminent risk. Effective response and restoration from HILF events require fast initiation and mobilization exercised through thorough planning.
- Little real-world operational experience generally exists with respect to responding to HILF risks, for the simple reason that they do not regularly occur.
- Probability of HILF risks' occurrence and impact is difficult to quantify. Historical occurrence and severity do not provide a strong indicator of potential future frequency or impacts.

Understanding and effectively managing HILF risks therefore require a different approach to viewing risk. A complete risk landscape includes three primary categories of threats and hazards:

natural, human caused (both intentional and unintentional), and technological[22]. A technological event is not typically thought to be a HILF event since traditionally it had the most controls applied, in the form of standards, quality controls, protections etc. which would limit the likelihood or the impact of a failure. The risks for the other two HILF type events (natural disasters and deliberate attacks) differ remarkably and require different approaches and considerations to appropriately address them. Each risk presents unique, though sometimes overlapping, concerns and a different profile of existing preparedness across the electric sector. It may be useful to consider categorizing these risks into these two categories as further work on other HILF risks proceeds.

The impact of HILF risks may be measured by several factors, including, but not limited to, population affected (number of customers without power), geographic area affected (region with no electricity in terms of square miles), time taken to restore power, potential for repeat incidents, intangibles (loss of perception of secure image), and various cost quantifiers (cost of repairing damage; cost of re-fortifying systems to ensure no repeat incidents; cost to consumers; cost to industry due to lost productivity, products, or services; cost to government and taxpayers; cost of increased insurance).

Once a risk has been identified and assessed, effort turns to its management and mitigation. Risk management builds on the risk assessment process by seeking answers to several questions: What can be done and what options are available? What are the associated tradeoffs in terms of all costs, benefits, and risks? And what are the impacts of current management decisions on future options?

As mitigating options are further considered, it is impossible to fully protect the system from every threat or threat actor. Sound management of these and all risks must focus on determining the appropriate balance of resilience, protection, and restoration. A successful risk management approach will begin by identifying the threat environment and protection goals for the system, balancing expected outcomes against the costs associated with proposed mitigations.

9.3 Identifying Risk

The process of identifying risk and mitigating it is an iterative process. This process should be continuous due to the need to identify evolving new risks and the limitations of equipment installed on the system. Some of the common methods of identifying risk on the system are:

- Indentifying meaningful metrics and using them to perform risk analysis (e.g. commercial aircraft fatalities per passenger-mile flown);
- Evaluating performance based on requirements in standards which presumably capture some sense from the industry as to what is important;[23]
- Through trend analysis, identifying emerging potential performance issues before they become actual performance issues;

[22] NERC's Electricity Sub-sector Coordinating Council (ESCC) has recently developed a Critical Infrastructure Strategic Roadmap, which discusses the risk landscape in more detail, available at http://www.nerc.com/docs/bot/agenda_items/10-DRAFT_ESCC_Strat_Roadmap_14Jul2010_clean.pdf.

[23] Over 75% of the requirements in standards however are documentation oriented and do not provide useful information as to the risks being taken. Reference Results Based performance – presented to the NERC Board of Trustees, November 4, 2009.

- Using expert judgment to identify risk by recognizing reliability performance gaps or needs, and considering all aspects of the system;
- Use subject-matter-specific committees in NERC to define concepts to identify risk on the system by examining key performance metrics to judge the performance of the bulk power system.

10. Managing Risk

10.1 Methods of Measuring

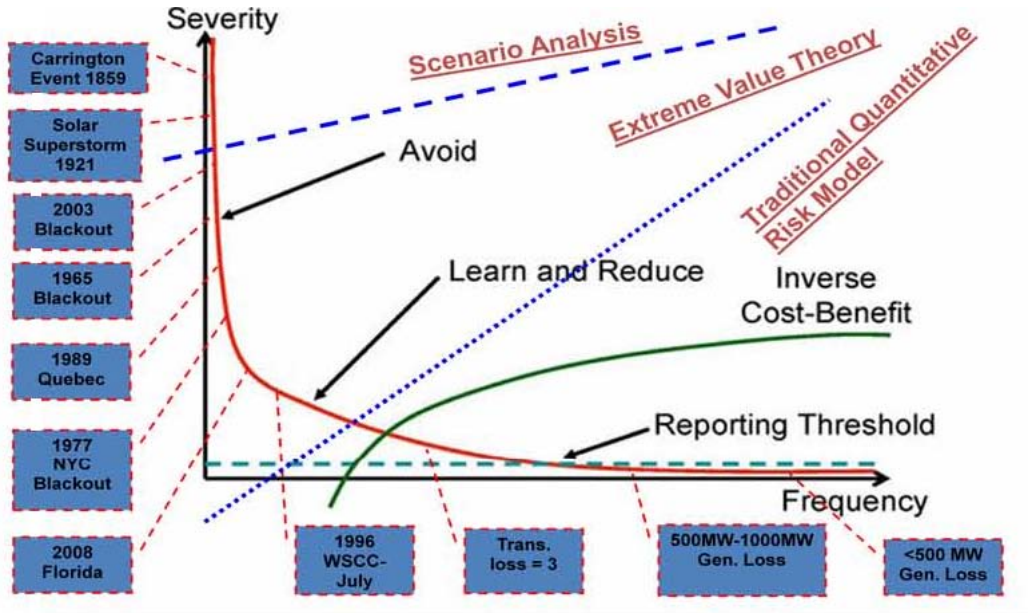
As shown in Figure 7, risk curves can map to different risk measurement approaches:

1) The far right of the curve would employ a standard quantitative risk model
2) The middle (or early rise) would employ extreme value theory (EVT)
3) The HILF events (or late rise) can rely upon scenario analysis

A traditional risk model strives to produce a good fit along the curves where most of the data falls, potentially at the expense of a good fit on the curve where few observations fall (such as HILF events or other lower frequency events). However, the model of operational risk must account well for the outer tail of the risk curve to capture low-frequency, high severity losses.

Traditional quantitative methods therefore are supported by NERC's GADS/TADS systems and can be mapped using standard quantitative risk models. Where there is increasingly limited data, Extreme Value Theory may be more appropriate to achieve a reliable estimate of extreme probabilities, where sparse data may be available from NERC's Events Analysis database. A generalized extreme value estimate, for example, uses the largest loss observed in each of the preceding years to obtain the distribution parameters best fitted by the years.

Figure 7 – Different Methods to Measure Risk/Severity

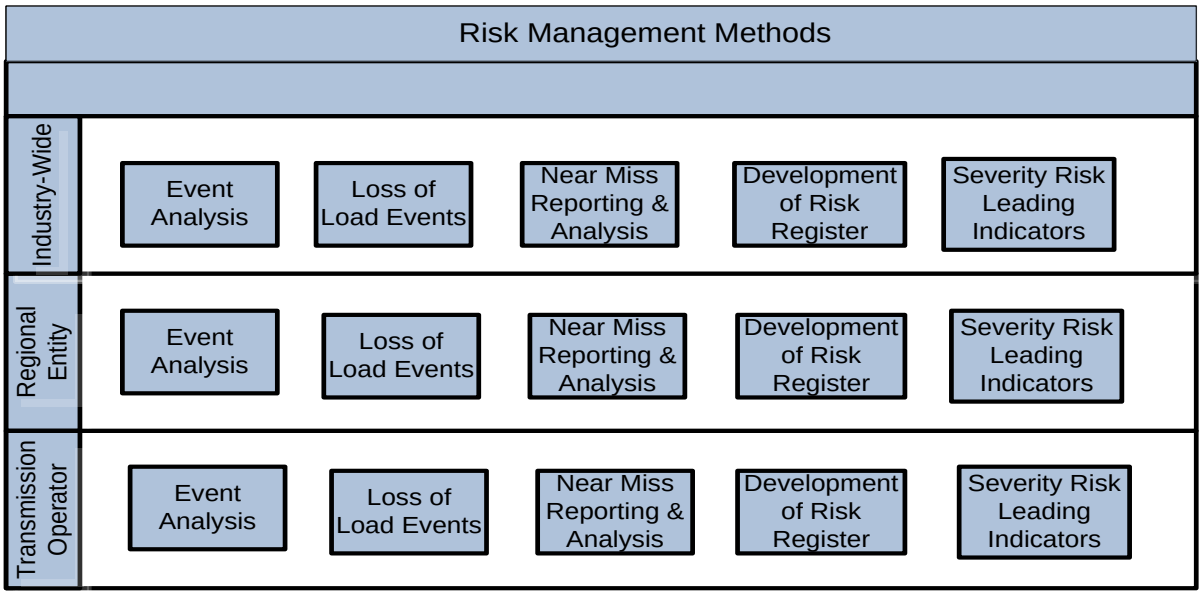


Where there is a sparse supply of operational loss data (e.g. HILF), for example, major solar storms (NERC or NOAA can set up a process to obtain data so one can start using EVT[24]), scenario analysis[25] can be used. Scenario analysis, while more subjective, does offer several benefits that are not captured by a quantitative approach. A scenario analysis is used to capture diverse opinions, concerns, and experience/expertise of key persons and represents them in a business model for measuring risk. Scenario analysis is a useful tool in capturing the qualitative and quantitative dimension of operational risk. Risk translates to where operational risk exposures exists, the severity of associated risks, identifies controls that are in place, and the type of control: damage, preventive, or detective. Cause and effect relationships can be captured with this method as well. The shortcoming of scenario analysis, however, is its subjectivity, which creates a potential for recording data inconsistently. Despite the shortcomings, the application of several divergent models can help develop a more confident convergent view of how much of an issue/response you need to prepare for in this event.

Outlined in Figure 8, is a conceptual framework for managing risk which recognizes that at a Transmission Operator (TOP), Regional Entity (RE) and NERC level there are companion processes to measure risk. However the thresholds for each of these processes differ.

Based upon many other industries' methods for managing risk, as the electric industry moves from a deterministic to a more probabilistic method it will be important to create new tools and processes.

Figure 8 – Conceptual Framework for Managing Risk in Bulk Power System



[24] The detailed EVT (Extreme Value Theory) can be found in "The Extreme Value Theory, An Introduction", by Laurens de Haan and Ana Ferreira, Springer, 2000.

[25] An example of the Scenario Analysis can be viewed at http://www.nerc.com/files/2009_Scenario_Assessment.pdf.

10.2 Event Analysis

As part of NERC's mission to ensure the reliability of the bulk power system in North America, NERC and Regional Entities conduct detailed event analysis[26] of system disturbances to determine root causes, uncover lessons learned, and issue relevant findings as advisories, recommendations, and essential actions to the industry.

Responding to major blackouts and other system disturbances or emergencies is addressed in detail in the NERC RoP Section 807; NERC Blackout and Disturbance Response Procedures can be divided into four phases: (1) situation tracking and communications (Situational Awareness); (2) situational assessment and communications (Event Triage); (3) data collection, investigation, analysis, and reporting (Event Analysis and Investigation); and (4) follow-up on recommendations (Lessons Learned, Action Plans, and Industry Alerts). Major events are classified and categorized by use of the "Event Category and Level of Analysis" document.[27] These events will be analyzed and investigated in accordance with the NERC RoP Section 807 and Appendix 8.[28]

Review of major blackouts and other system disturbances or emergencies can provide identification of significant causes including among other things, control and protection system mis-operations, equipment failures, vegetation contact with transmission lines, and human error.

Once the learning phase of the process has identified risks, further analysis can prioritize risk in the context of all the other risks faced by utilities based on the probability of their occurrence and impact to the system. Generally, individual organizations can improve performance by focusing on high-priority risks to the bulk power system under their control. However, systemic risk is only observable on a broader industry or regional basis. Risks with low probabilities and impacts can be listed on a watch list for future monitoring. Using the industry process to influence standard developments can aid in the process of prioritizing risk and can help define and establish levels of probability of risk occurrence after they have been identified.

10.3 Off-normal Event Fact Finding

Responding to off-normal and other small events of value for analysis is called for in the NERC RoP Section 808. The need for addressing off-normal or other small events is to identify the root causes of events that may be precursors of potentially more serious events or that have the potential to cause more serious events; to assess past reliability performance for lessons learned, and to develop reliability performance benchmarks and trends. Off-normal and other small events of value for analysis are classified by the Event Analysis and Investigation Process Manual as Non-consequential but Noteworthy and defined as "The event did not result in notable consequences but had the potential to cause an event that would be more consequential under slightly different circumstances (e.g. near miss)." The event may produce a NERC alert or lessons learned for dissemination to the electric industry.

---

[26] Draft Event Analysis and Investigation Process Manual (Item 5.d.1.) is available at http://www.nerc.com/filez/pcmin.html.

[27] "Draft Event Categories and Level of Analysis" (Item 6.l.) can be viewed at http://www.nerc.com/filez/pcmin.html.

[28] NERC's Rules of Procedure are available at http://www.nerc.com/files/NERC_Rules_of_Procedure_EFFECTIVE_20100205.pdf

The risk assessment approach of off-normal and other events can continuously use the information provided by minor incidents and other reliability indicators to guide risk proactive prevention scheme. The finding can also help identify resolution of potential problems and treat each input as an opportunity to improve the system.

10.4 Root Cause Analysis & Human Performance

Root Cause Analysis (RCA)[29] determines the basic reason(s) (causal factors) for an undesirable condition or problem which, if eliminated or corrected, would have prevented the problem from existing or occurring. RCA seeks to find and correct not only the cause of a particular problem, but to determine the associated systems, processes, etc., that contributed to or allowed the event to occur. RCA corrective actions fix the problem, and also find and correct the contributing issues. When the facts identify that the causes of the problem include process/procedure or people type causes (human performance or human factors), care should be taken to use the appropriate human performance/factor guidelines that address the underlying causes.

Many historical events were triggered by human error. No matter how well we try to fix problems through training, supervision, process, procedures, and communications human beings make mistakes for many reasons. Errors in human performance are not only caused by human beings but also by management and leadership practices (or lack of). Weaknesses in work processes, cultural values and poor leadership can also lead to human error. Therefore people cannot perform better than the organization supporting them.

When conducting a Root Cause Analysis (RCA) we must investigate the organization's policies, and procedures; system operations and equipment; and the human performance factors at the same time.[30]

From the Top-Down perspective, shown in Figure 9, the industry through corporate policies and procedures should instill a "Risk Management" culture. This culture should be seen at the management level all the way to the front line. When viewed from the other direction, the Bottom-Up Approach is similar. The management team should provide a "foundation" for a "Risk Management" culture through its corporate policies and procedures. This foundation will provide the support for the staff to become a Risk Management organization.

The critical work products should be:

- Clear corporate strategies, goals and tactics;
- Clear written documentation;
- Concise verbal and written communications;
- Risk management tools;
- Human performance factors considered.

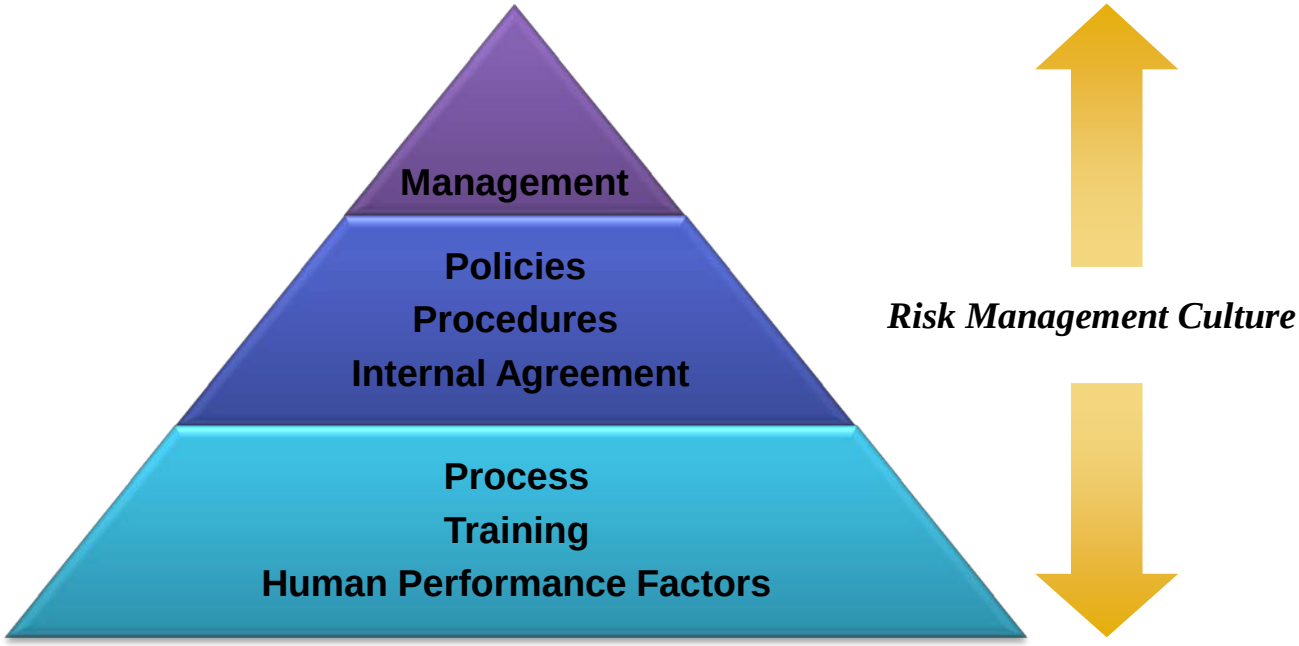
[29] Draft Cause Analysis Methods for NERC, Regional Entities and Registered Entities" (Item 5.d.2.) is available at http://www.nerc.com/filez/pcmin.html.

[30] The draft RCA Template is available at http://www.nerc.com/docs/eawg/RCA_Template_July_12_2010.pdf.

Ultimately everyone should be asking these questions:

- What can go wrong?
- What can we do to prevent this from happening?
- If the risk event happens then what can we do to minimize the impact?

Figure 9 – Top-Down or Bottom-Up Approach



11. Acknowledgements

The RMWG would like to express our sincere appreciation to the many people who participated in the development of the framework and this document, including reviewing concepts and providing the valuable comments that have helped improve the clarity and robustness of this paper. We are especially grateful to the staff at the US Department of Energy (DOE), who offered invaluable technical insight of the risk models used in other industry sectors, including Joseph Eto of Ernest Orlando Lawrence Berkeley National Laboratory, Kevin Stamber and Randy Gauntt of Sandia National Laboratories. We also acknowledge contributions made by George Wilson, Kenn Miller and Donnie Harrison of the US Nuclear Regulatory Commission, who shared risk management knowledge and experience during the early development stage. Finally, we acknowledge Angeli Tompkins from DOE's Argonne National Laboratory (ANL) for her collaboration in the development of ANL's infrastructure risk modeling.

12. Bibliography

"The Reliability Concepts Document", available at http://www.nerc.com/files/concepts_v1.0.2.pdf.

"Flirting with Disaster", Marc Gerstein, Union Square Press, 2008.

"Hostages of Each Other", Joseph V. Rees, the University of Chicago Press, 1994.

"Against the Gods – The Remarkable Story of Risk", Peter L. Bernstein, John Wiley & Sons, Inc., 1996.

IEEE 1366-2003 etc.