PNNL-24673

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle Since 1965

Framework for Modeling High-Impact, Low-Frequency Power Grid Events to Support Risk-Informed Decisions

December 2015

A Veeramany
SD Unwin
GA Coles
JE Dagle
WD Millard
J Yao
CS Glantz
SNG Gourisetti

U.S. DEPARTMENT OF ENERGY

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
email: orders@ntis.gov <http://www.ntis.gov/about/form.aspx>
Online ordering: http://www.ntis.gov

This document was printed on recycled paper.
(8/2010)

PNNL-24673

Framework for Modeling High-Impact, Low-Frequency Power Grid Events to Support Risk-Informed Decisions

A Veeramany
SD Unwin
GA Coles
JE Dagle
WD Millard
J Yao
CS Glantz
SNG Gourisetti

December 2015

Prepared for
the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99352

Executive Summary

Natural and man-made hazardous events resulting in the simultaneous loss of multiple grid infrastructure assets challenge the electric power grid's security and resilience. However, the planning and allocation of appropriate contingency resources for such events requires an understanding of their likelihood and the extent of their potential impact. Where these events are of low likelihood, a risk-informed perspective on planning can be problematic as there exists an insufficient statistical basis to directly estimate the probabilities and consequences of their occurrence. Since risk-informed decisions rely on such knowledge, a basis for modeling the risk associated with high-impact low frequency events (HILFs) is essential. Insights from such a model can inform where resources are most rationally and effectively expended. The present effort is focused on development of a HILF risk assessment framework. Such a framework is intended to provide the conceptual and overarching technical basis for the development of HILF risk models that can inform decision makers across numerous stakeholder sectors.

The North American Electric Reliability Corporation (NERC) Standard TPL-001-4 considers severe events for transmission reliability planning, but does not address events of such severity that they have the potential to fail a substantial fraction of grid assets over a region, such as geomagnetic disturbances, extreme seismic events, and coordinated cyber-physical attacks. These are beyond current planning guidelines. As noted, the risks associated with such events cannot be statistically estimated based on historic experience; however, there does exist a stable of risk modeling techniques for rare events that has proven of value across a wide range of engineering application domains.

The value of a risk model is reflected in the degree to which it can be exercised to provide insight to stakeholders and decision-makers, and in the process by which it is maintained as an evergreen and continually improving model of the domain it represents. Figure E.1 depicts the broader paradigm of risk management and the integral role of risk analysis and risk modeling. Elements of risk management include the modeling, evaluation of management options based on interrogation of the model, implementation of the selected options, communication of strategy and actions to stakeholders, and monitoring new data and insights to update the model as appropriate. The framework defined here is focused on the means of developing the underlying risk model.

There is an active and growing interest in evaluating the value of risk-management techniques in the State transmission planning and emergency response communities, some of this interest in the context of grid modernization activities. The availability of a grid HILF risk model, integrated across multi-hazard domains which, when interrogated, can support transparent, defensible and effective decisions, is an attractive prospect among these communities.

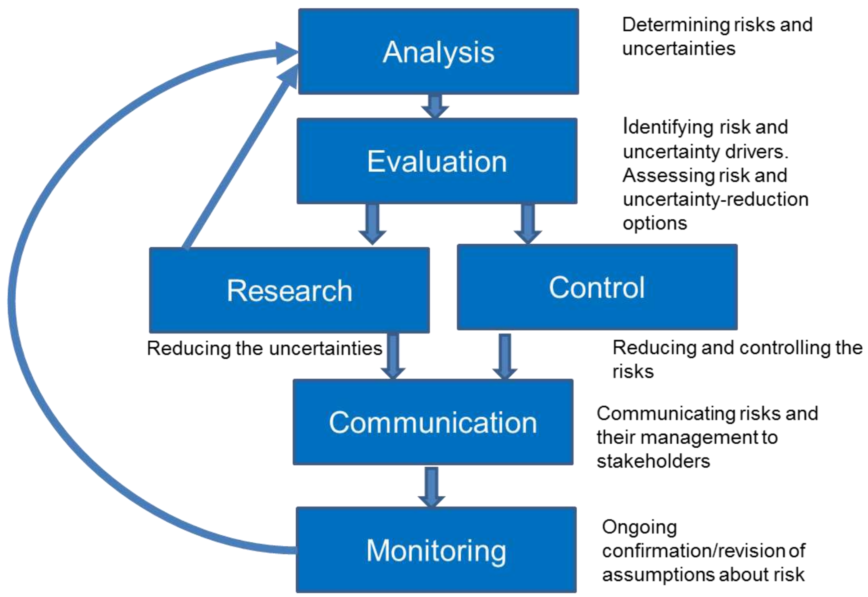

Figure E1. Risk Management Paradigm

In this report, we document an integrated HILF risk framework intended to inform the development of risk models. These models would be based on the systematic and comprehensive (to within scope) characterization of hazards to the level of detail required for modeling risk, identification of the stressors associated with the hazards (i.e., the means of impacting grid and supporting infrastructure), characterization of the vulnerability of assets to these stressors and the probabilities of asset compromise, the grid's dynamic response to the asset failures, and assessment of subsequent severities of consequence with respect to selected impact metrics, such as power outage duration and geographic reach. Specifically, the current framework is being developed to:

1. Provide the conceptual and overarching technical paradigms for the development of risk models.
2. Identify the classes of models required to implement the framework - providing examples of existing models, and also identifying where modeling gaps exist.
3. Identify the types of data required, addressing circumstances under which data are sparse and the formal elicitation of informed judgment might be required.
4. Identify means by which the resultant risk models might be interrogated to form the necessary basis for risk management.

As the framework was under development, anticipated challenges for implementation were identified. One key challenge is that there is substantial lack of uniformity in the extent to which domain models are available across hazard categories. For instance, while fully quantitative models of seismic hazard and stressors have been developed, the same is not true of geomagnetic disturbances. While risk models do not generally require the availability of detailed quantitative domain models, the expectation is that implementation of the framework will require the elicitation of informed opinion to augment areas in which models are less mature and data are sparser. Another key finding is that the large number of alternative impact scenarios associated with potential combinations of asset failures, will necessitate use of approximation techniques that can establish scenario samples that allow acceptably accurate estimates of risk to be produced. In this context, various Monte Carlo approaches are considered.

Acknowledgments

This work was funded by U.S. Department of Energy Office of Electricity Delivery and Energy Reliability performed under contract DE-AC05-76RL01830.

Acronyms and Abbreviations

DCS	Distributed Control Systems
DHS	Department of Homeland Security
DOE	U.S. Department of Energy
EF	Enhanced Fujita
EMP	electromagnetic pulse
EPRI	Electric Power Research Institute
FEMA	Federal Emergency Management Agency
GIC	geomagnetic-induced current
GMD	geomagnetic disturbances
HEMP	high-altitude electromagnetic pulse
HILF	High-Impact, Low-Frequency (Event)
LHS	Latin Hypercube Sampling
NERC	North American Electric Reliability Corporation
NHC	National Hurricane Center
NOAA	National Oceanic and Atmospheric Administration
NRC	U.S. Nuclear Regulatory Commission
PRA	Probabilistic Risk Assessment
SCADA	Supervisory Control and Data Acquisition

Contents

Figures

Tables

1.0 Introduction

1.1 High-Impact, Low-Frequency Event Risk

A high-impact, low-frequency event (HILF) is the realization of a specific hazard that has the potential to produce a high impact on grid operability. Such high-impact events are, by virtue of their rarity, considered low frequency. Table 1 lists examples of hazards that, when realized in severe degree, could produce HILFs.

Table 1. Examples of Hazards that could Produce HILFs

Hazard Category	Examples
Natural hazards	Meteorological (e.g., hurricane, tornado, snowstorm)
	Geological (e.g., seismic, volcanic)
	Hydrological (e.g., coastal flooding)
	Space Weather (e.g., geomagnetic storm)
Biological hazards	Biological (e.g., pandemic)
Human (non-intentional) hazards	Operational Error
Human (malicious) hazards	Physical attack, cyber-attack, coordinated cyber-physical attack, electromagnetic pulse

A specific realization of a HILF is referred to as an initiating event, or initiator. For instance, a realization of the seismic hazard might be an earthquake of specified magnitude at a specified epicenter. This initiator then begins a sequence of events resulting in an accident sequence. Such a sequence will involve damage to some combination of grid and supporting infrastructure assets that then results in a given level of consequence, such as loss of power over a given geographic area for a given duration. A risk model seeks to systematically and comprehensively (to within the scope of the model) identify the accident sequences, to estimate their probabilities of occurrence, and to quantify their degrees of impact. It is the concurrent quantitative consideration of event probabilities and event consequences that characterizes a risk model.

Blackouts for the past four decades have been extensively studied by the power engineering society (Kundur et al. 2007, Assante et al. 2010). The consequence of an initiating extreme event in most circumstances has been loss of a single grid asset quickly followed by cascading events such as heavy loading and further asset loss due to reduced ability to perform time-sensitive corrective actions. The impact is more catastrophically significant when the recovery time is more than a day.

North American Electric Reliability Corporation (NERC) Standard TPL-001-4 (NERC 2014) identifies event scales and a corresponding list of specific combination of critical asset failures that need to be taken in to consideration as thresholds for transmission system planning purposes. These include loss of at most two generating stations in a wide area or loss of any one asset locally. Single assets include substations that represent one voltage level and all transformers, a generating station having any number of generating units, and all transmission lines that share the same right-of-way. These extreme events were named as 'Category D' events in an earlier NERC standard (NERC 2005). However, such plans are not based on an understanding of the relative or absolute risks associated with the hazards. Furthermore, hypothetical scenarios may be conceived that are substantially more severe than those identified with Category D and the question arises of what resources are warranted to plan for them. Here a risk-perspective is crucial. In the framework defined here, events that potentially result in failure of asset combinations of greater magnitude than those identified in the NERC standard are considered for the purposes of assessing HILF risk to the grid. The current focus is on HILFs that might result in widespread asset failures.

There has been a history of power grid HILFs to which grid infrastructure has proven resilient or rapidly recoverable. But the set of hypothetical HILFs widely exceeds those that have been realized. A meaningful risk framework must therefore provide the basis for the systematic identification of such hypothetical scenarios, and their incorporation into an assessment of risk. That is the goal of the current framework, intended to provide the conceptual and high-level technical guidelines for development of HILF risk models that can provide insight to decision- and policy-makers. The intended users of the framework include transmission and system planners, and state planners that need risk tools to make mid-to-long-term planning decisions.

The maturities of methods for assessing risk are uneven across hazard categories. While this document is not intended as a review of existing methods, a broad characterization of the state of the art across hazard categories forms the basis for presaging the modeling challenges that will need to be addressed when developing the risk models. Where challenges revolve around data availability, we address methodologies available for the formalized use of informed opinion to supplement available data. The framework is intended to be sufficiently general to accommodate a range of hazards and asset types.

There are at least five principal components to the framework which guide the elements of risk modeling:

1. Characterization of HILF hazards and initiating events.
2. Knowledge of the geographic configuration of grid-supporting assets.
3. Assessment of the means by which an initiator can impact a grid or supporting asset in terms of relevant stressors and the level of vulnerability to such stressors.
4. Understanding of the operational logic dictating the reliance of grid assets on supporting infrastructure.
5. Power outage or other consequence implications of loss of various combinations of grid assets.

Finally, the number of assets associated with a power grid system is large, which means that the number of hypothetical scenarios involving various combinations of assets failures can be substantial. Therefore, an issue to be addressed is the tractability of analyzing all scenarios and the identification of simplifying analytical processes that do not compromise risk insights. Prospective means of addressing tractability are considered in the framework.

1.2 Precedents

Some precedent for modeling HILFs in a risk framework does exist. For instance, Scherb et al. (2015) developed a probabilistic risk assessment framework to study the risk impact of hurricanes on infrastructure networks with applications to the electrical power grid. In this approach, the hazard intensity given the occurrence of a hurricane is a probabilistic distribution informed by historic maximum wind speed data. The probability of failure of a network component is conditional on the damage state induced by the hurricane, which is itself a function of the wind speed informed by a fragility model. Consequence has been quantified using a physical power-flow model.

Francis et al. (2011) developed a natural disaster mitigation framework for electric power infrastructure that has the capability to account for hazard intensity, asset fragility, and expected utility cost. In this approach, the expected failure probability of an asset is an aggregation over hazard intensity distribution and the fragility function given the hazard intensity. The expected utility cost is attributable to service disruption and restoration. Revenue loss resulting from service disruption is dependent on restoration time, which is in itself a function of the hazard intensity and certain decision-making parameters specific to the hazard and the asset under study.

Garrick et al. (2004) developed a framework for quantitative risk assessment of terrorist-initiated high-consequence events with application to cyber-physical attacks on the electrical power grid. The grid was viewed as a system with four constituent elements: 1) substations, 2) transmission lines, 3) supervisory control and data acquisition systems, and 4) energy-management systems. Garrick et al. (2004) emphasized the notion of probability of frequency through Bayes inference to derive probability curves that characterize likelihood of a scenario.

Panteli and Mancarella (2015) furnished a conceptual framework that employs fragility curves to evaluate the impact of (HILF) on the power grid with an implementation for hurricane winds on a section of the United Kingdom's transmission network. A sequential Monte Carlo simulation was used to sample intensities from transmission tower and line fragility curves. The Loss-of-Load Expectation reliability index was used to measure the average number of hours of customer disconnection.

Current grid risk models and tools tend to focus either on detailed consequence modeling at the level of localized transmission and distribution systems, or on consideration of a single, specific hazard. Given the narrow focus of such models, this precludes broader risk insight across numerous hazard classes that could support planning and prioritization. Our current intent is to develop a framework for creating risk models that integrate across hazards and associated HILFs to aid planners in understanding decision tradeoffs across disparate hazards and asset types.

1.3 Models and Frameworks

We have been making distinction throughout between risk frameworks and risk models, and t. This subsection is intended to provide some clarification. Risk modeling in this current context involves:

1. Hazard identification and probabilistic characterization (frequencies of associated events)
2. Initiating event development (selection of representative events for analysis)
3. Grid and supporting infrastructure response characterization (probabilities of asset failures)
4. Consequence assessment (power outage or other metrics)
5. Model integration to develop risk profiles.

While a risk model generally produces a bottom-line quantitative risk estimate, this is seldom the principal value of the model. Rather, greater insights come from improved understanding of the distribution of risk: among hazards, among initiating events, among assets, and over geographic areas. Interrogation of the model generally involves asking the question, "If I make the following adjustment to system design, system operations, or contingency measures, how is the risk impacted?" When applied in combination with costing models, a risk model provides a basis for cost-benefit analysis that identifies where resources can be most effectively be expended. The primary objective is to evolve the model as a useful and practical decision-support tool that aids planners in risk-ranking of various HILFs and appropriately allocating resources in anticipation of such risks.

A risk framework in the present context is a conceptual structure intended to guide the development of risk models. It identifies the elements of a model and the means by which they are integrated. The framework is not intended to be prescriptive and so it leaves flexibility in the specifics of its implementation, but at the same time ensures that the essential components of the resultant risk model are present.

1.4 Risk-Management Paradigms

The HILF risk framework is intended to underlie risk models that have value to decision-makers in the context of conventional risk-management paradigms. Several paradigms have been described (Apostolakis et al. 2012), but they all coincide in essential features. Figure 1 represents typical concepts. It would allow risk to the electric power grid due to extreme events to be managed as part of a continuous improvement lifecycle.

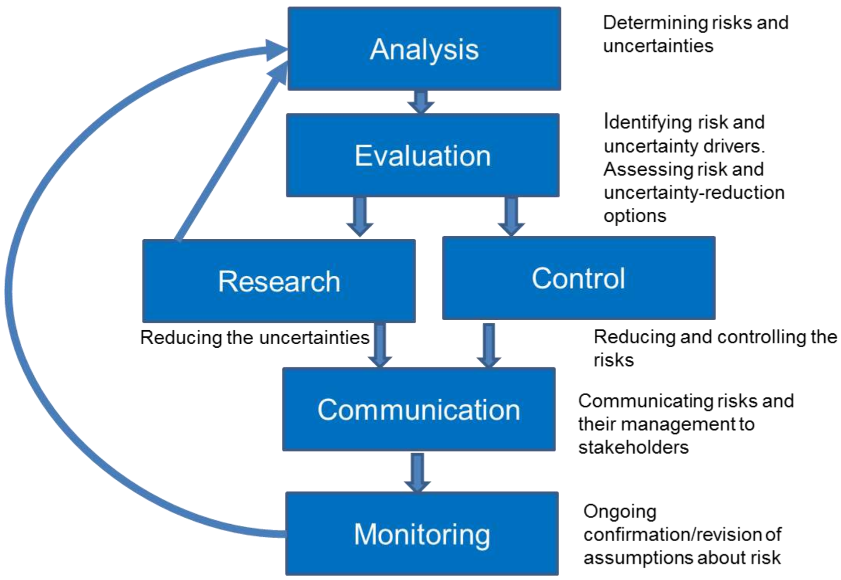

Figure 1. Elements of the Risk-Management Paradigm

Analysis, evaluation, and decision implementation are major elements of any risk-management paradigm. Methods for analysis are exemplified by PRA) methodology (see Garrick [2008] for PRA fundamentals), where most experience is in the nuclear power arena. In the analysis phase, the system under study is quantitatively characterized, supported by subject matter experts, to systematically identify adverse scenarios, their frequencies of occurrence, and their severities of outcome. A scenario is a set of events triggered by an initiating event and followed by the failure of mitigative systems, resulting ultimately in an end state associated with a given severity of consequences. For low-frequency events where direct statistical data are unavailable, frequency estimates generally derive from models, some of which extrapolate from available data, often augmented by informed judgment. Consequence estimates are generally derived from domain models of the systems under analysis.

The evaluation phase is the digestion of results of the analysis which are cast in forms that support decision-making. This may be ranking or importance analysis of factors such as hazards, events, assets, and conducting "*what-if?*" assessments in which the risk impact of engineered or operational changes are evaluated. Based on the evaluation, decisions are made on the best risk-management strategies. Elements of risk control tend to be either preventive or mitigative in nature, where the former prevents or reduces the likelihood of a scenario, and the latter reduces its impact. Cost-benefit analysis is often a factor in selecting between risk management options. A risk model may also identify the need for reducing uncertainties through either additional data collection or model enhancement. The efficacy of risk management decisions is generally dependent on strong communications to all stakeholders. Such stakeholders may include policymakers, operational decision-makers, regulators, and the public. Once implemented, the risk model and associated risk management strategy are maintained evergreen through monitoring and analysis of emerging hazard and operational data to validate the model or to update it where warranted.

2.0 HILF Risk Framework

2.1 Major Elements of the HILF Framework

This section provides the essential elements of the HILF framework, portrayed graphically in Figure 2. This figure represents the flow of analysis and information transfer associated with a risk model developed in conformance with the framework. In this section, each element of the framework is described. Appendix A lays out the framework in greater mathematical rigor, while the other appendices provide clarification of the framework elements.

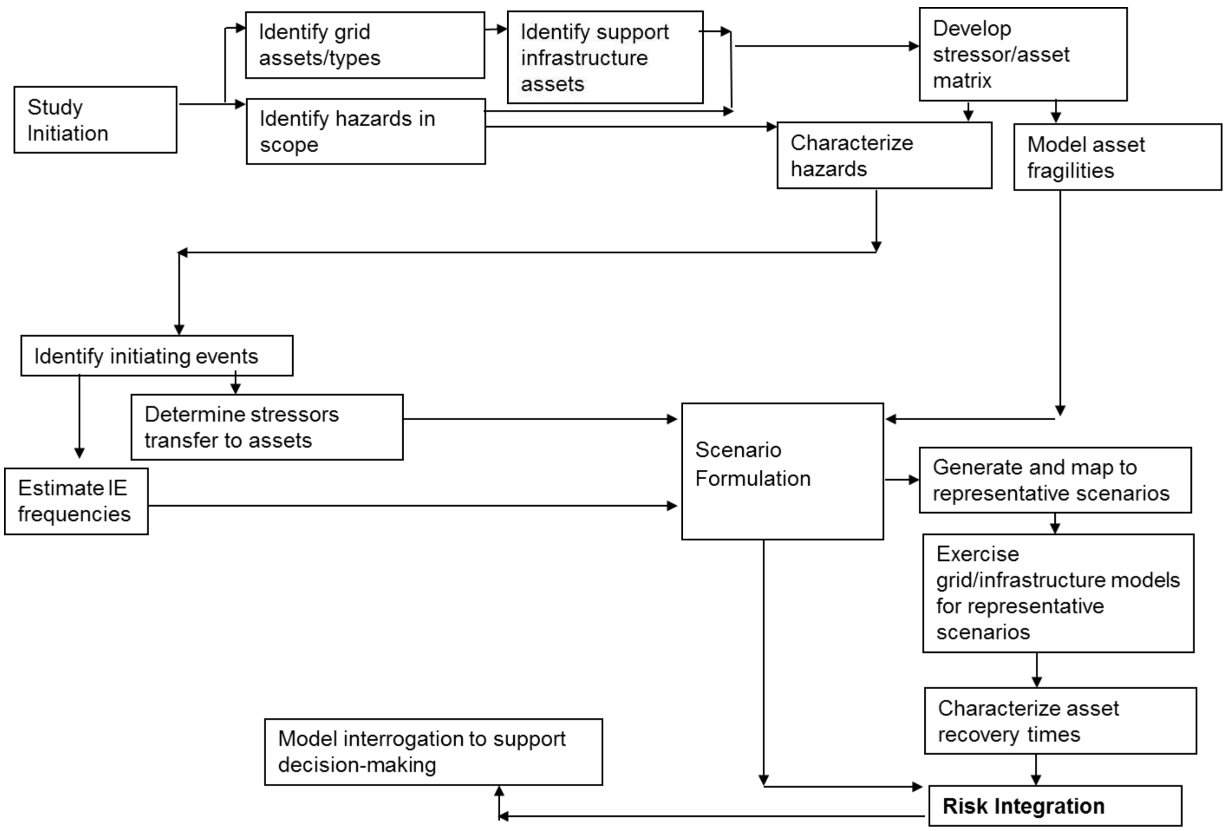

Figure 2. Elements of the HILF Framework

2.1.1 Study Initiation

Prior to implementation of the framework, the objective of the resulting risk model should be established. How will the model be used and by whom? This will dictate the model scope (such as hazards, assets, and geographic application), its level of resolution, and likely data requirements. These insights are then among the bases for implementing subsequent elements.

2.1.2 Identify Grid Assets/Types

In this element, critical grid infrastructure assets relevant to the application scope are identified. If the study is driven more by hazard scope than asset focus, then the subsequent element identifying assets vulnerable to specific hazards will be needed to define the asset classes of interest. The U.S. Department of Energy (DOE) Grid Technology Team, as part of its grid modernization strategic plan, categorizes electric grid in to these asset domains (Bose et al. 2013):

1. generation
2. transmission
3. distribution and end users.

Within each of these categories, specific assets are identified as part of this element. Other facilities, systems and equipment that might be listed include control centers and special systems required to maintain reliability of the bulk power system (NERC 2009), such as generator plant control, transmission protection, and load shedding. In a subsequent element, each member of the list of assets will be characterized in terms of its vulnerability to HILF events. That will depend on factors such as its fragility to stressors associated with the hazard, its protective features, and its geographic location.

2.1.3 Identify Hazards in Scope

The hazards to be captured in the model scope are identified. If the study is driven more by asset scope than hazard focus, then the subsequent element identifying assets vulnerable to specific hazards will be needed to define the hazards of interest. In this element, the stressors associated with each hazard are identified. A stressor is the mechanism by which an event realized by the hazard can challenge the integrity of an asset. For instance, a seismic event is associated with the stressor of peak ground acceleration to which an asset may be vulnerable. An example list of candidate hazards and their associated stressors are listed in Appendix C.

Note that not all hazards are credibly associated with HILFs and some may be screened out on this basis. The current focus is to consider events that can potentially result in outages on a wide-area scale with asset failures occurring in disparate locations. The element therefore requires establishment of screening criteria by which hazard classes are included.

2.1.4 Identify Support Infrastructure Assets

Infrastructure dependence models are used to identify assets that service the grid assets of interest. The boundary between core grid assets and the assets on which the grid relies for reliable functionality are delineated. Grid assets that directly rely on support systems are identified. The risk model must ultimately model the vulnerabilities associated with those assets comprising the support systems.

The basis for support infrastructure identification and the associated support assets can be driven by interdependency modeling methodologies (Pederson et al. 2006, Rinaldi et al. 2001). These assets can be identified under the categories such as means of transport for essential supplies, crew logistics, professional services, and information infrastructure.

It is likely impractical to identify a comprehensive set of support infrastructure assets given the complexity of interoperability between infrastructure types, such as cyber, transportation, and electrical power, for example. The challenge is to establish a basis for model simplification. The practical basis for such simplification might be a focus on assets most vulnerable to the hazard types under review, supplemented by a screening assessment that demonstrates the major contributors to risk have been captured. This will likely require iteration between the current element and the asset/stressor development element to follow.

2.1.5 Develop Stressor/Asset Matrix

A matrix connecting hazard classes to asset classes is developed. This pairs assets to hazards via the stressor types to which the assets are potentially vulnerable. For instance, distribution lines may be linked to meteorological hazards via high winds and generated projectiles, while transmission lines may be coupled via generated projectiles only. This matrix forms the basis for developing scenarios in which the loads associated with certain stressors exceed the capacities of specified assets to withstand them. Appendix D provides an example of a stressor/asset matrix.

Depending on the asset/hazard combinations within scope, it is likely that this step will require the exploration of asset vulnerabilities to stressors that are beyond established, standard methodology. That is, some degree of methodology development, supported by use of informed opinion, will be necessary. For instance, hazards associated with pandemics require a characterization of stressors and vulnerabilities that appropriately reflect the potential impact of loss of human resources to control and maintain grid and infrastructure assets. In this sense, the current framework goes beyond establishment of the basis for developing risk models to identifying methodology development needs.

2.1.6 Characterize Hazards

In this element, a probabilistic characterization of hazard degree is developed. For example, a hazard characterization for the seismic hazard is a curve that specifies the annual frequencies of exceedance of a given earthquake magnitudes, specified by location. Of all hazards, seismicity is probably the most mature in terms of quantitative characterization in the United States. (e.g., USGS 2015, EPRI/DOE/NRC 2012). Characterizations of other hazards are also available, albeit generally in less quantitative form. This characterization ultimately forms the basis for scenario initiating event identification. A list of available hazard models, geographic information system-based tools and guidance resources are listed in Appendix B. Because of the substantial variability in maturity of methods for characterizing the various hazards, it is anticipated that elicitation of informed judgment will play a substantial role in this element, for which several systematic methodologies are available (e.g., Budnitz et al. 1997, Ortiz et al. 1991). Elicitation methods are discussed further in Section 3.3.

2.1.7 Model Asset Fragilities

The asset/stressor matrix developed in a previous element is the starting point for the current element. Each asset's capacity to withstand a stressor of given intensity is modeled probabilistically. A fragility curve defines the probability of functional failure of the asset conditional on specified stressor magnitudes. For practicality, assets could be grouped into equivalence classes for each stressor type (e.g., seismic ground excitation, wind speed, projectile impulse, etc.), and the fragility curves developed for each class/stressor combination. An equivalence class would include all assets with approximately equal fragility characteristics. Fragility models and guidance resources are listed in Appendix B. It is expected that some methodology development will be required for stressor types not conventionally modeled in a stressor/fragility (i.e., load/capacity) paradigm. Ultimately, the convolution of such fragility curves with probabilistic stressor curves at the asset location will produce asset failure probabilities.

2.1.8 Identify Initiating Events

The hazard curves provide the basis for identification of scenario initiating events (which we'll shorten to "initiators"). Discrete representative events must be chosen as initiators. Hazard curves generally define a continuum of hypothetical events, both in terms of magnitude and, if applicable, geographic location, and these continua need to be discretized to identify specific events that capture the range of possible event magnitudes and other discriminating hazard characteristics (e.g., earthquake location, hurricane path, etc.). An initiator is the first event in a sequence that ultimately results in an adverse impact. These event sequences, or "scenarios", provide the underlying structure of the risk model. It is the frequencies and consequences of these scenarios that are the fundamental components of the risk calculation.

2.1.9 Estimate Initiating Event Frequencies

Based on comparison of the hazard curves or other source hazard characterization with the discrete initiating events selected for analysis, annual frequencies of those events are estimated. At the completion of this step, we now have a set of probabilistically characterized initiating events from which the scenarios will be generated.

2.1.10 Determine Stressor Transfer to Assets

The stressor to which an asset is exposed as a consequence of a specified initiator requires an understanding of the way in which the energy associated with the initiator is transferred to the asset. For example, a seismic event results in an energy release and ground motion that is attenuated between the earthquake epicenter and the asset. The degree of attenuation is dependent of factors such rock and soil properties between the two locations. There exist several ground attenuation models to assess the seismic stressor transfer (e.g., Stewart et al. 2015). The transfer model is likely to be probabilistic in nature, reflecting uncertainties in the degree of stressor attenuation. Examples of stressor transfer models are presented in Appendix B.

Depending on the maturity of methods and availability of geographically relevant data, it is likely that this element will require informed judgment to play a significant role. For example, the process for conducting a probabilistic seismic hazard assessment substantially incorporates informed judgment elicited through formal methods (Budnitz et al. 1997).

2.1.11 Scenarios Formulation

At this point, the elements are in place to systematically identify scenarios. A scenario is a deterministic, hypothetical sequence of events that begins with an initiating event and results in the functional failure of some combination of assets. Combinatorially, there is an extremely large set of scenarios that could be generated from the information developed, and so means of representing that set, without compromising risk insights, are necessary. A Monte Carlo approach is likely the most practical. The expectation is that for each initiating event, the scenarios will be sampled from joint distributions over stressor magnitudes and asset fragilities. That is, a given scenario will include the occurrence of an initiator and the subsequent failure of a set of assets, where for each asset in that set, at least one associated stressor exceeds the corresponding capacity to withstand it. Therefore, for each initiator, the number of scenarios generated is equal to number of members in the Monte Carlo sample for which at least one asset fails. The methodology and sample size selected must be demonstrated to generate good estimates of the risk characteristics.

A brief summary of Monte Carlo simulation sampling methods is presented in Appendix G. The integrating mathematical structure for scenario definition is discussed in Appendix A.

2.1.12 Generate and Map to Representative Scenarios

The severity of consequence associated with each scenario must ultimately be estimated. The consequence metric of interest (e.g., power outage duration and geographic extent) is evaluated using existing grid simulation models such as PSS/E (Siemens 2015). Public, private and open-source grid models have been developed over the past several years which can characterize cascading grid failures in response to initiating events. A list of grid simulation models and tools is shown in Appendix E.

Because the run times render impractical execution of such a model for every sample member (i.e., for every scenario), this element involves the identification of representative scenarios for which the consequences will be calculated and to which the full Monte Carlo sample of scenarios will be mapped. The methodological basis for establishing representative scenarios will need to be established. One possibility is the clustering of the sample members such that each member of a cluster (i.e., each scenario) has attributes that would result in similar consequences. Then a single scenario can be used to represent each cluster in the consequence analysis.

Note that in this element, there is the opportunity to screen from further analysis those scenarios, or scenario clusters, that lack to potential to result in high-impact consequences per the criteria established. This notion is discussed more in Section 3.2.

2.1.13 Exercise Grid/Infrastructure Models for Representative Scenarios

Support infrastructure models that map loss of supporting assets to loss of grid assets, as well as grid operability models for the representative scenario set are exercised to assess the degrees of impact for the consequence metrics identified.

Identification of grid assets lost either due to HILF stressors or to service system failures will be primary inputs to the grid operability models (e.g., Siemens 2015). Implications of the relative immaturity of grid support infrastructure models were addressed in Section 2.1.4.

This element produces consequence estimates in terms of the selected impact metrics such as power outage by geographic extent and duration, for each representative scenario.

2.1.14 Characterize Asset Recovery Times

The recovery times associated with each representative scenario are estimated as the basis to adjust consequence estimates. Recovery models are discussed in Appendix F.

While reliability databases containing mean times to asset repair will be of value, the sheer extent of impact associated with a HILF will necessitate the elicitation of informed judgment to address the practicality of repairs in the wake of a major event (see Section 3.3). The task of quantifying repair times becomes challenging because of possible asset inaccessibility in emergency conditions, occupational hazards, loss of manpower, loss of service systems, and combinations thereof.

2.1.15 Risk Integration

The realized scenarios, their frequencies of occurrence, and the consequence estimates are integrated to characterize the risk to the electric power grid due to the multiple hazards addressed. The mathematical structure that brings together the elements of the framework is outlined Appendix A. The platform for implementation and integration of the model is not prescribed by the framework which allows flexibility in approach – from a simple Excel framework to a custom software platform.

2.1.16 Model Interrogation to Support Decision-Making

Once implemented, the risk model can be interrogated in numerous ways to provide insight to decision-makers. Some of the most common means of manipulating a model to provide insight are:

1. Identification of principal risk drivers: hazards, initiators, asset classes, specific assets, geographic regions. This points to where there is the greatest potential for risk reduction.
2. Sensitivity/*what-if?* analysis to understand the risk impact of hypothetical engineered or operational risk-management measures.
3. In conjunction with use of costing models, cost-benefit analysis undertaken to determine where risk reduction can be most cost efficiently achieved.

3.0 Implementation

3.1 Constituent Models

Based on the framework as described in Section 2, implementation will require the availability or development of a mix of underlying model types. These types are depicted in Figure 3. Hazard models provide a characterization of initiating event magnitude versus frequencies of occurrence. Induced stressor models allow estimation of the stressors to the assets given the magnitude of the initiator and accounting for the relative locations of the initiators and assets. For example, in hurricane hazard models, decay rate of wind speed between hurricane path and asset is modeled (Vickery et al. 2009) while ground-motion attenuation models (Stewart et al. 2015) are employed for seismic hazard analysis. Other hazard domains are less mature and will likely demand some degree of approximation methods development.

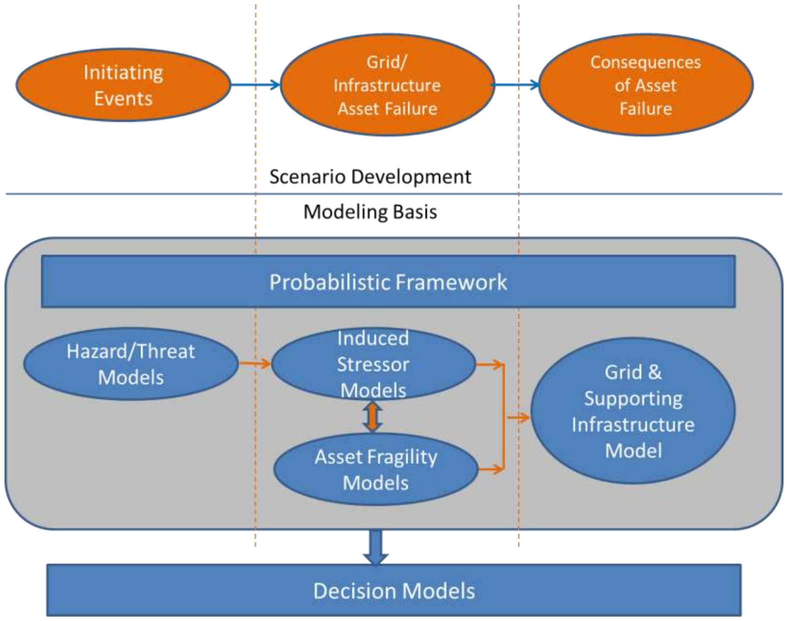

Figure 3. Constituent Models to Implement the Risk Framework

Asset fragility models characterize, in probabilistic terms, the vulnerability or performance of an asset subject to stressors associated with a hazard (Straub and Der Kiureghian, 2008). An example vulnerability model addresses loss-of-load probability, which is described as a function of the number of cyber-attack attempts (Xiang et al. 2014). Quantitative seismic fragility models (Pitilakis 2014) couched in terms of the stressor of peak ground acceleration represent the most mature of the methodologies among natural hazards. Fragility models for other types of stressors are sometime qualitative in nature, such as those that characterize the extent of structural damage associated with specified wind speeds.

Grid behavior models consist of combinations of simulation, physics-based or probabilistic models that analyze cascading failures due to overloads, voltage deviations, loss of protection systems, and operator actions (Morgan, 2011) given a set of initial degraded conditions. There are a number of research and commercial software packages that perform contingency analysis either conservatively based on steady-state solutions or in more detail involving dynamic interaction of events. Some of these readily available packages are shown in Appendix E.

Grid support models would provide two key functionalities: 1) fragility models that identify supporting assets likely to fail in response to the initiating event and critical to the operation of the grid and 2) identification of grid assets that are impacted due to loss of supporting assets. The availability of such models may be a key constraint on the comprehensiveness of the integrated risk model. An important element of risk modeling is determination of what depth of domain modeling is essential to support usable risk insights. Implementation of the current framework will shed light on such questions.

Finally, risk and decision models then aggregate the component model analyses into information and insights that are of value to decision-makers.

3.2 Steps in Implementation

In modeling a system as large and complex as the power grid, it is inevitable that there will be issues of model tractability due to the sheer number of hypothetical scenarios that can be generated. In Section 2.1, some observations have already been made on how some tractability issues can be addressed, such as the Monte Carlo generation of a scenario sample and the subsequent identification of representative scenarios for consequence estimation.

Tractability can also be enhanced by consideration of the constraints associated with the scope of the HILF model; that is, our interest is in the subset of scenarios that give rise to high impact. Screening of scenarios against the HILF criteria will further reduce the scenario set to be explicitly modeled. For example, some scenarios are likely to fall within the extreme event criteria defined by the NERC performance requirements standard (NERC 2014) and so are considered outside the scope of the current HILF framework.

Given the availability of high-performance computing and parallelization, run time challenges for grid models may be significantly reduced. There are three classes of grid operability models that perform contingency analysis following the initial loss of a set of assets: 1) power-flow models, 2) dynamic-transient models, and 3) hybrid modeled that combine elements of the first two. Power-flow models evaluate post-contingency, grid equilibrium conditions and run faster than other models, yielding conservative consequence estimates. However, certain conditions that cause significant asset losses may result in convergence issues during the runtime. Such numerical instabilities are likely to happen given the extreme nature of HILFs under study. This occurs when dynamic models search for stable steady-state solutions through tracking power flow over smaller time steps. However, these models are known to be resource intensive, time consuming, and possibly demand the use of supercomputers. For this reason, hybrid models that default to conservative analysis in the event of convergence challenges would likely be preferred for the purposes of implementing the framework.

Grid operability models do not typically consider support infrastructure assets (e.g. communications) in the network topology. As noted before, the immaturity of available infrastructure models may demand approximate approaches to addressing infrastructure failures. For example, a conservative approach might be to associate grid assets with supporting infrastructure assets and assume that loss of the supporting asset leads deterministically to loss of the associated grid assets.

3.3 Use of Informed Opinion

Where historical data or statistical information is deemed incomplete or insufficient to represent uncertainty in a classical, statistical sense, the formal and structured elicitation of informed judgment has substantial precedent as a basis for augmenting sparse or ambiguous data (Meyer and Booker. 2001; Boring et al. 2005). The risk framework requires modeling of an inhomogeneous set of phenomena with regard to data and model availability. It is therefore inevitable that model development will demand the use of informed opinion in some areas. To maximize the transparency and defensibility of informed judgment, the methodology for its elicitation must itself be defensible and widely accepted. There are several such methods available.

Expert elicitation methods were first developed in conjunction with the development of decision-analysis techniques in the late 1960s and early 1970s (Spetzler and von Holstein [1975] is recognized as the seminal work). Since then, they have become standard—and in some domains, proceduralized—tools for uncertainty characterization (e.g., Wheeler et al. 1989, Budnitz et al. 1997). The methods have drawn extensively from research in cognitive psychology (Tversky and Kahneman 1974, Kahneman et al. 1982) showing that, when unaided, individuals tend to use various heuristics when making judgments about uncertainty, resulting in systematic biases in their assessment, such as overconfidence. If these biases are not identified and managed by the interviewer in the elicitation process, then the resulting probability assessment will suffer accordingly.

For example, the Delphi method of elicitation was initially developed by RAND Corporation. In a study for the U.S. Nuclear Regulatory Commission, Ortiz et al. (1991) adopted another example of an elicitation methodology during their assessment of severe accident risks for several nuclear power plants. One of the most widely applied methods for elicitation is described in the Senior Seismic Hazard Analysis Committee report (Budnitz et al. 1997), which has been used in the context of hazard characterization for seismicity and volcanism. Budnitz et al. describe multiple, optional levels of elicitation, depending on the study objectives and the resources available to achieve them. Factors that distinguish methodologies include whether experts are elicited individually or in groups, whether individual experts provide point estimates of parameters from which distributions are generated or they provide probability distributions over the parameter space, whether there is an opportunity for discourse between/among experts allowing adjustment of individual opinions, etc. The appropriate methodology is driven by objectives and resources (Cooke and Goossens 2004).

In the context of the current framework, the anticipation is that elicitation will be of greatest value in hazard characterization and asset fragility analysis.

4.0 Conclusions

The framework established here provides a systematic structure in which disparate hazards and their risk to the grid can be modeled. As the framework was under development, anticipated challenges for implementation were identified. A key challenge is that there is substantial lack of uniformity in the extent to which domain models are available, or in the maturities of those models, across hazard categories. For instance, while there is substantial literature on fully quantitative models of seismic hazards and ground-motion stressors, the same is not true of geomagnetic disturbances. However, risk models generally accommodate some level of approximation in analysis of the underlying domain, and detailed domain models are not always required. The expectation is that implementation of the framework will require some reliance on the elicitation of informed opinion to augment areas in which models are less mature and data more sparse. Nevertheless, the framework should be viewed not only as a template for the development of risk models, but also as a means of systematically identifying methodological and data development needs.

Another key finding is that given the large number of alternative impact scenarios associated with potential combinations of asset failures, approximation techniques will need to be established to generate samples of scenarios that allow acceptably accurate estimates of risk. In this context, Monte Carlo approaches are discussed, but the nonprescriptive nature of the framework allows alternative approaches to be considered.

The anticipation is that early implementation of the framework will not necessarily capture the full range of hazards and assets that the framework is developed to accommodate but, rather, will be used to address a more limited objective focused on specific hazard and/or asset types. Depending on the selected applications, the expectation is that some risk methodology development will be necessary for implementation of the framework. This framework should then provide the structure and risk context in which those development needs can be identified and their relative importance assessed.

5.0 References

Anagnos T. 1999. *Development of an Electrical Substation Equipment Performance Database for Evaluation of Equipment Fragilities*. Pacific Earthquake Engineering Research Center, University of California-Berkley, Berkley, California.

Anghel M, K Werley, and AE Motter. 2007. “Stochastic Model for Power Grid Dynamics.” In *System Sciences, 2007. HICSS 2007*, 40th Hawaii International Conference on System Sciences, January 3-6, 2007, Big Island, Hawaii.

Apostolakis G, M Cunningham, C Lui, G Pangburn, and W Reckle. 2012. *A Proposed Risk Management Regulatory Framework*. NUREG-2150, U.S. Nuclear Regulatory Commission, Washington D.C.

Assante M, W Bryan, S Moore, RB Stephan, S Brindley, T Bowe, T Burgess, J Dixon, M Franke, S Holeman, J Kappenman, R McClanahan, J Palin, and W Radasky. 2010. *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System*. North American Electric Reliability Corporation, Washington, D.C.

Bhuiyan MR and RN Allan. 1994. “Inclusion of Weather Effects in Composite System Reliability Evaluation using Sequential Simulation.” *IEE Proceedings-Generation, Transmission and Distribution* 141(6):575-584.

Billinton R and G Singh. 2006. “Application of Adverse and Extreme Adverse Weather: Modeling in Transmission and Distribution System Reliability Evaluation.” *IEE Proceedings-Generation, Transmission and Distribution* 153(1):115-120.

Boissonnade A, Q Hossain, J Kimball, R Mensing, and J Savy. 2000. *Development of a Probabilistic Tornado Wind Hazard Model for The Continental United States*. UCRL-ID-140922-VOL-1 Main Report, Lawrence Livermore National Laboratory, Livermore, California.

Boring R and D Gertman. 2005. *Simplified Expert Elicitation Guideline for Risk Assessments of Operating Events.*, INL/EXT-05-00433, Idaho National Laboratory, Idaho Falls, Idaho.

Bose A, W Parks, and K Cheung. 2013. *DOE’s Strategic Plan for Grid Modernization*. Available at http://smartgrid.ieee.org/january-2013/738-doe-s-strategic-plan-for-grid-modernization.

Budnitz RJ, G Apostolakis, DM Boore, LS Cluff, KJ Coppersmith, CA Cornell, and PA Morris. 1997. *Recommendations for Probabilistic Seismic Hazard Analysis: Guidance on Uncertainty and Use of Experts*. NUREG/CR-6372, Vol. 1 (Main Report), U.S. Nuclear Regulatory Commission Washington, D.C.

Chee Chien A. 2006. *Optimized Recovery of Damaged Electrical Power Grids*. Master’s Thesis, Naval Postgraduate School, Monterey, California.

Center for Disease Control and Prevention (CDC). 2012. *Pandemic Preparedness Tools - CommunityFlu 2.0*. Atlanta, Georgia. Available at http://www.cdc.gov/flu/pandemic-resources/tools/communityflu.htm.

Cooke RM and LH Goossens. 2004. "Expert Judgment Elicitation for Risk Assessments of Critical Infrastructures." *Journal of Risk Research* 7(6):643-656.

Duggan P and T Michalski. 2007. *Threat Analysis Framework.* SAND2007-5792, Sandia National Laboratories, Albuquerque, New Mexico.

Electric Power Research Institute (EPRI). 1981. *Tornado Missile Simulation and Design Methodology, Volume 1: Simulation Methodology, Design Applications and TORMIS Computer Code*. EPRI Topical Report NP-2005-V1, Palo Alto, California.

Electric Power Research Institute (EPRI). 2002. *Seismic Fragility Application Guide*. TR-1002988, Palo Alto, California.

Electric Power Research Institute (EPRI)/U.S. Department of Energy (DOE)/U.S. Nuclear Regulatory Commission (NRC). 2012. *Central and Eastern United States Seismic Source Characterization for Nuclear Facilities*. NUREG-2115, Electric Power Research Institute, Palo Alto, California.

Federal Emergency Management Agency (FEMA). 2003. *HAZUS-MH Multi-Hazard Loss Estimation Methodology – Earthquake Model. Technical Manual*. Washington, D.C.

Francis RA, SM Falconi, R Nateghi, and SD Guikema. 2011. "Probabilistic Life Cycle Analysis Model for Evaluating Electric Power Infrastructure Risk Mitigation Investments." *Climatic Change* 106(1):31-55.

Garrick BJ. 2008. *Quantifying and Controlling Catastrophic Risks*. Academic Press. London, United Kingdom.

Garrick BJ, JE Hall, M Kilger, JC McDonald, T O'Toole, PS Probst, ER Parker, R Rosenthal, AW Trivelpiece, LA Van Arsdale, and EL Zebroski. 2004. "Confronting the Risks of Terrorism: Making the Right Decisions." *Reliability Engineering & System Safety* 86(2):129-176.

Gelfand AE and AFM Smith. 1990. "Sampling-Based Approaches to Calculating Marginal Densities." *Journal of the American Statistical Association* 85:398-409.

Helton JC and FJ Davis. 2003. "Latin Hypercube Sampling and the Propagation of Uncertainty in Analyses of Complex Systems." *Reliability Engineering and System Safety* 81(1):23-69.

Herbranson WT and J Schroeder. 2010. "Are Birds Smarter Than Mathematicians? Pigeons (*Columba livia*) Perform Optimally on a Version of the Monty Hall Dilemma." *Journal of Comparative Psychology* 124:1-13.

Iman RL and WJ Conover. 1980. "Small Sample Sensitivity Analysis Techniques for Computer Models, with an Application to Risk Assessment." *Communications in Statistics: Theory and Methods 1980* A9(17):1749-1842.

Iman RL and JM Davenport. 1982. "Rank Correlation Plots for Use with Correlated Input Variables." *Communications in Statistics: Simulation and Computation* 11(3):335-360.

Jones D, CE Davis, M Turnquist, and LK Nozick. 2006. *Physical Security and Vulnerability Modeling for Infrastructure Facilities*. SAND2006-4155, Sandia National Laboratories, Albuquerque, New Mexico.

Kahneman D, P Slovic, and A Tversky (editors). 1982. *Judgment under Uncertainty: Heuristics and Biases*. Cambridge University Press, Cambridge, United Kingdom.

Kappenman J. 2010. *Geomagnetic Storms and Their Impacts on the U.S. Power Grid.* Meta-R-319, Metatech Corporation, Goleta, California. Available at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.227.2009&rep=rep1&type=pdf.

Kundur P, C Taylor, and P Pourbeik (Chairmen). 2007. *Blackout Experiences and Lessons, Best Practices for System Dynamic Performance, and the Role of New Technologies*. IEEE Special Publication 07TP190, IEEE Task Force Report. Available at http://www.researchgate.net/publication/272482692_Blackout_Experiences_and_Lessons_Best_Practices_for_System_Dynamic_Performance_and_the_Role_of_New_Technologies.

Lanzano G, E Salzano, FS de Magistris, and G Fabbrocino. 2013. "Seismic Vulnerability of Natural Gas Pipelines." *Reliability Engineering & System Safety* 117:73-80.

Mateski M, CM Trevino, CK Veitch, J Michalski, JM Harris, S Maruoka, and J Frye. 2012. *Cyber Threat Metrics*. SAND2012-2427, Sandia National Laboratories, Albuquerque, New Mexico.

McQueen MA, WF Boyer, MA Flynn, and GA Beitel. 2005. *Time-to-Compromise Model for Cyber Risk Reduction Estimation*. INL/CON-05-00649, Idaho National Laboratories, Idaho Falls, Idaho.

Meyer MA and J Booker. 2001. *Eliciting and Analyzing Expert Judgment: A Practical Guide*. Book. 7, SIAM. ISBN: 9780898714746, Society for Industrial and Applied Mathematics, Philadelphia, Pennsylvania.

Morgan MG and H Henrion. 1990. *Uncertainty: A Guide to Dealing with Uncertainty in Quantitative Risk and Policy Analysis*. Cambridge University Press, Cambridge, United Kingdom.

National Hurricane Center (NHC). 2009. *Tropical Cyclone Wind Speed Probabilities Products*. Miami, Florida. Available at http://www.nhc.noaa.gov/aboutnhcprobs2.shtml.

National Oceanic and Atmospheric Administration (NOAA). 2013. "Saffir-Simpson Hurricane Wind Scale." Available at http://www.nhc.noaa.gov/aboutsshws.php.

North American Electric Reliability Corporation (NERC). 2005. "Standard TPL-004-4a, System Performance Following Extreme BES Events." Available at http://www.nercipedia.com/active-standards/tpl-004-0a/.

North American Electric Reliability Corporation (NERC). 2009. *Security Guideline for the Electricity Sector: Identifying Critical Assets*. Available at http://www.nerc.com/fileUploads/File/Standards/Critcal_Asset_Identification_2009Nov19.pdf.

North American Electric Reliability Corporation (NERC). 2014. "Standard TPL-001-4, Transmission System Planning Performance Requirement." Available at http://www.nerc.com/pa/Stand/Reliability%20Standards/TPL-001-4.pdf.

Oakridge National Laboratory (ORNL). 2010. *The Late-Time (E3) High-Altitude Electromagnetic Pulse (HEMP) and Its Impact on the U.S. Power Grid.* Meta-R-321, Metatech Corporation Report, Oak Ridge, Tennessee.

Ortiz NR, TA Wheeler, RJ Breeding, S Hora, MA Meyer, and RL Keeney. 1991. "Use of Expert Judgment in NUREG-1150." *Nuclear Engineering and Design* 126(3):313-331.

Panteli M and P Mancarella. 2015. "Modeling and Evaluating the Resilience of Critical Electrical Power Infrastructure to Extreme Weather Events" *IEEE Systems Journal* PP(99):1-10.

Pederson P, D Dudenhoeffer, S Hartley, and M Permann..2006. Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research. INL/EXT-06-11464, Idaho National Laboratory, Idaho Falls, Idaho.

Pitilakis K, H Crowley, and A Kaynia (editors). 2014. *SYNER-G: Typology Definition and Fragility Functions for Physical Elements AT Seismic Risk*. Springer, New York.

Portante EC, JA Kavicky, SF Folga, BA Craig, LE Talaber, and GR Wulfkuhle. 2010. "Simulating the Seismic Performance of a Large-Scale Electric Network in the U.S. Midwest." In *Proceedings of the 2010 Winter Simulation Conference*, pp.3482-3493, December 5-8, 2010, Baltimore, Maryland.

Rinaldi SM, JP Peerenboom, and TK Kelly. 2001. "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies." *IEEE Control Systems* 21(6):11-25.

Salman AM. 2014. "Age-Dependent Fragility and Life-Cycle Cost Analysis of Timber and Steel Distribution Poles Subjected to Hurricanes." Master's Thesis, Michigan Technological University, Houghton, Michigan.

Scherb A, L Garrè, and D Straub. 2015. "Probabilistic Risk Assessment of Infrastructure Networks Subjected to Hurricanes." Presented at 12th International Conference on Applications of Statistics and Probability in Civil Engineering, ICASP12, July 12-15, 2015, Vancouver, Canada.

Schultz MT, BP Gouldby, JD Simm, and JL Wibowo. 2010. *Beyond the Factor of Safety: Developing Fragility Curves to Characterize System Reliability*. ERDC-SR-10-1, Engineer Research and Development Center, U.S. Army Corps of Engineers, Washington, D.C.

Shinozuka M, M Feng, X Dong, SE Chang, TC Cheng, X Jin, and MA Saadeghvaziri. 2003. "Advances in Seismic Performance Evaluation Of Power Systems." *Research Progress and Accomplishments 2001-2003* 1-16.

Simm JD, BP Gouldby, PB Sayers, J Flikweert, S Wersching, and ME Bramley. 2008. "Representing Fragility of Flood and Coastal Defenses: Getting Into the Detail." FLOODrisk 2008, September 30-October 2, 2008, Keble College, Oxford, United Kingdom.

Siemens. 2015. "PSS/E Power System Simulator for Engineering." Version 34.0, Siemens Power Transmission and Distribution, Inc., Schenectady, New York.

Spetzler CS and CA Stael von Holstein. 1975. "Probability Encoding in Decision Analysis." *Management Science* 22:340-358.

Stewart MG, MD Netherton, and DV Rosowsky. 2006. "Terrorism Risks and Blast Damage to Built Infrastructure." *Natural Hazards Review* 7(3):114-122.

Stewart JP, J Douglas, M Javanbarg, Y Bozorgnia, NA Abrahamson, DM Boore, KW Campbell, E Delavaud, M Erdik, and PJ Stafford. 2015. "Selection of Ground Motion Prediction Equations for the Global Earthquake Model." *Earthquake Spectra* 31(1):19-45.

Straub D and A Der Kiureghian. 2008. "Improved Seismic Fragility Modeling from Empirical Data." *Structural Safety* 30(4):320-336.

Suppasri A, S Koshimura, and F Imamura. 2011. "Developing Tsunami Fragility Curves Based on the Satellite Remote Sensing and the Numerical Modeling of the 2004 Indian Ocean Tsunami in Thailand." *Natural Hazards and Earth System Science* 11(1):173-189.

Swiler LP and NJ West. 2010. "Importance Sampling: Promises and Limitations." In *Proceedings of the 51st AIAA/ASME/ASCE/AHS/ASC Structures*, Structural Dynamics, and Materials Conference, April 12-15, 2010, Orlando, Florida.

Torta JM, S Marsal, and M Quintana. 2014. "Assessing the Hazard from Geomagnetically Induced Currents to the Entire High-Voltage Power Network in Spain." *Earth, Planets and Space* 66:87.

Tversky A and D Kahneman. 1974. "Judgment under Uncertainty: Heuristics and Biases." *Science* 185:1124-1131.

U.S. Department of Energy (DOE). 2002. *Natural Phenomena Hazards Assessment Criteria*. DOE-STD-1023-95, Washington D.C.

U.S. Department of Homeland Security (DHS). 2007. *National Population, Economic, and Infrastructure Impacts of Pandemic Influenza with Strategic Recommendations*. Washington D.C.

U.S. Department of Homeland Security (DHS). 2010. *DHS Risk Lexicon 2010 Edition*. Security Risk Steering Committee, Washington, D.C. Available at http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf.

U.S. Department of Homeland Security – Office of Risk Management and Analysis (DHS-RMA). 2011. *Geomagnetic Storms: An Evaluation of Risks and Risk Assessments* in Risk Management Issue. Brief retrieved from http://www.dhs.gov/xlibrary/assets/rma-geomagnetic-storms.pdf.

U.S. Geological Survey (USGS). 2015. "Hazards: Seismic Hazard Maps and Data." Earthquake Hazards Program. Available at http://earthquake.usgs.gov/hazards/products.

Vickery PJ, FJ Masters, MD Powell, and D Wadhera. 2009. "Hurricane Hazard Modeling: The Past, Present, and Future." *Journal of Wind Engineering and Industrial Aerodynamics* 97(7):392-405.

Wheeler TA, SC Hora, WR Cramond, and SD Unwin. 1989. *Analysis of Core Damage Frequency from Internal Events: Expert Judgment Elicitation*. NUREG/CR-4550, Vol. 2, U.S. Nuclear Regulatory Commission, Washington, D.C.

Winkler J, L Duenas-Osorio, R Stein, and D Subramanian. 2010. "Performance Assessment of Topologically Diverse Power Systems Subjected to Hurricane Events." *Reliability Engineering & System Safety 95*(4):323-336.

Xiang Y, L Wang, and Y Zhang. 2014. "Power System Adequacy Assessment with Probabilistic Cyber Attacks Against Breakers." In *Proceedings of the IEEE Power and Energy Systems General Meeting Conference & Exposition*, July 27-31, 2014, National Harbor, Maryland.

Xie L, J Tang, H Tang, Q Xie, and S Xue. 2012. "Seismic fragility assessment of transmission towers via performance-based analysis." In *Proceedings of the 15th World Conference on Earthquake Engineering*, September 24-28, 2008, Lisbon, Portugal.

Appendix A

HILF Risk Mathematical Formulation

Appendix A

HILF Risk Mathematical Formulation

This appendix outlines the underlying mathematical structure specified by the HILF risk framework.

A.1 HILF Risk Framework: Building Blocks

Object	Definition	Example
A_i	i'th asset associated with geographic/functional scope of interest: could belong to grid or support system	The substation located at x^0N y^0W
H_j	j'th hazard category	Seismic hazard
$E_{k(j)}$	k'th initiating event in hazard category H_j	Magnitude M=3 earthquake occurs at epicenter x^0N y^0W, depth 100 m
$F_{k(j)}$	Annual rate of occurrence of initiating event $E_{k(j)}$	Annual occurrence rate of magnitude M=3 earthquake at epicenter x^0N y^0W, depth 100 m
$S_{r(j,i)}$	r'th stressor type associated with hazard category H_j to which asset type A_i is vulnerable	Distribution line segment x vulnerability to impact from projectiles associated with hurricane hazard
$P_{ik(j)}$	The probability that asset A_i functionally fails given the occurrence of initiating event $E_{k(j)}$	Probability that Substation located at x^0N y^0W fails given the occurrence of a magnitude M=3 earthquake at epicenter w^0N z^0W, depth 100 m
$Q_{ik(j)r(i,j)}(L_r)$	Probability (density) that the stressor load at asset A_i associated with stressor type $S_{r(j,i)}$ given occurrence of initiator $E_{k(j)}$ is at magnitude L_r	Probability density that peak ground acceleration at Substation located at x^0N y^0W is 0.5g given magnitude M=3 earthquake occurs at epicenter u^0N v^0W, depth 100 m
$C_{ir(i,j)}(L_r)$	Probability (density) that the threshold failure load (i.e., capacity) for asset A_i associated with stressor type $S_{r(j,i)}$ is L_r	Probability density that failure threshold for Substation located at x^0N y^0W is at a gust wind speed of 100 mph
$\underline{B}$	Vector describing a scenario (defined by a combination of asset failures) such that B_i=1 if A_i fails, B_i=0 otherwise	Five specified transmission lines functionally fail, all other assets intact
$D_{k(j)}(\underline{B})$	Consequence associated with scenario $\underline{B}$ for k'th initiating event of hazard category H_j	20% load loss due to a scenario involving loss of five specified transmission lines with other assets remaining intact due to Magnitude M=3 earthquake occurs at epicenter x^0N y^0W, depth 100 m

Let the stressors associated with a hazard category *j* and an asset type *i* be enumerated by *r(j, i).* If there is only one stressor, *r*(*j*,*i*)=1, associated with a given hazard class-asset combination, then the probability that asset A_i functionally fails given the occurrence of initiating event $E_{k(j)}$ is:

(1) $P_{ik(j)} = {}_0\int^{\infty} C_{ir}(L_r)\, dL_r\ {}_{Lr}\int^{\infty} Q_{ik(j)r}(L_r')\, dL_r'$

If there are multiple stressors that connect a hazard class with an asset then:

(2) $P_{ik(j)} = \Sigma_{r(i,j)}\ {}_0\int^{\infty} C_{ir}(L_r)\, dL_r\ {}_{Lr}\int^{\infty} Q_{ik(j)r}(L_r')\, dL_r'$ + Cross Terms

We are now interested in identifying scenarios that involve some combination of asset failures. Consider occurrence of initiator $E_{k(j)}$. A subset of A_i fail and some survive with a given probability. Say B_i is an indicator such that

B_i = 1 if asset A_i fails
B_i = 0 if A_i survives.

So vector $\underline{B}$ defines a single asset failure/survival scenario.

Conditional on the initiator $E_{k(j)}$ occurring, the probability of *N* specific assets failing and the remainder (*M* assets) surviving is:

(3) $T_{k(j)}(\underline{B}) = {}_{i=1}\Pi^{N} P_{ik(j).}\ {}_{i=N+1}\Pi^{N+M} (1-P_{ik(j)}).$

Therefore, the frequency with which initiator $E_{k(j)}$ occurs resulting in the failure vector $\underline{B}$ is:

(4) $F(\underline{B})_{k(j)} = F_{k(j).}\ T_{k(j)}(\underline{B}).$

Assume the consequence of this scenario is $D_{k(j)}(\underline{B})$. Note that this *D* factor accounts for recovery times associated with the scenario, accounting for challenges associated with the recovery environment that the scenario has created. Therefore, the risk contribution from this scenario is now:

(5) $R_{k(j)}(\underline{B}) = F(\underline{B})_{k(j).}\, D_{k(j)}(\underline{B})$

and the total risk contribution from initiator $E_{k(j)}$ is:

(6) $R_{k(j)} = \Sigma_{\underline{B}}\ R_{k(j)}(\underline{B}).$

where the summation is effected over all asset failure combinations. Therefore, the total risk associated with hazard category H_j is:

(7) $R_j = \Sigma_{k(j)}\ R_{k(j)}$

and the grand total risk over all hazard categories is given by

(8) $R = \Sigma_j\ R_j$

or, partially expanding this out:

(9) $R = \Sigma_j\, \Sigma_{k(j)}\, F_{k(j).}\, \Sigma_{\underline{B}}\ T_{k(j)}(\underline{B}).\ D_{k(j)}(\underline{B}).$

Note that the calculational tractability issue addressed in the main report is associated principally the large size of the set of possible $\underline{B}$ vectors; i.e. asset failure combinations. It is assumed that Monte Carlo methods will prove the most practical means of implementing Equation 9 and the challenge is to demonstrate good risk approximations associated with practical sample sizes (see Appendix G).

Appendix B

State of the Art in Hazard and Fragility Modeling

Appendix B

State of the Art in Hazard and Fragility Modeling

Quantitative characterization of hazards and asset fragilities are key elements of the high-impact, low-frequency risk framework. There is a broad range of maturities and availabilities of methods and data across the spectrum of hazard types. For this reason, implementation of the framework is likely to demand some degree of methodology development depending on the scope of application. In this appendix, we tabulate an overview of the state of methods maturity in hazard and fragility analysis.

Table B.1. State of Availability of Supporting Hazards and Fragility Models and Data

Hazard	Frequency Characterization	Associated Fragility
Seismic	– Full quantitative hazard models for several geographic regions (USGS 2015, EPRI/DOE/NRC 2012) – Quantitative ground-motion attenuation models for selected geographic regions (Stewart et al. 2015)	– Quantitative fragility models for limited asset types (FEMA-HAZUS 2015, EPRI 2002)
Pandemic	– Quantitative pandemic outbreak probability models – Quantitative spread rate and transmission probability models (CDC 2012; DHS 2007, 2010)	– Exploratory impact models available across some aspects of national infrastructure (DHS 2007)
Hurricane	– Quantitative near-term forecast of wind speed and storm surge probabilities for coastal and inland locations (NHC 2009) – Quantitative hurricane wind field models for inland wind decay (NHC 2009)	– Quantitative fragility models for structures (FEMA 2003, DOE 2002)
Tornado	– Site-specific probabilistic wind hazard assessment for key locations (LLNL 2000, DOE 2002) – Site-specific wind velocity intensity distributions for high-risk sites (Boissonnade 2000)	– Projectile probabilistic risk evaluation methodology for nuclear power plant structures (EPRI 1981)
Geomagnetic storm	– Estimated frequency of geomagnetic storms of different magnitudes (DHS-RMA 2011) – Latitude-specific probability of a North American event for a given disturbance intensity (DHS-RMA 2011)	– Power grid failure probability analysis from geomagnetic-induced current threat scenario (Kappenman 2010)
High-altitude electromagnetic Pulse	– Propagation characteristics of high-altitude pulse waves to electric fields in the Earth (ORNL 2010)	– Probabilistic loss of critical assets
Cyber-attack[(a)]	– Cyber-attack frequency metric (Mateski et al. 2012) – Probabilistic threat characterization (Duggan et al. 2007)	– Probabilistic characterization of cyber-asset loss due to cyber-attack (McQueen et al. 2005)
Physical Attack[(a)]	– Probabilistic threat detection (Jones et al. 2006) – Probabilistic threat intensity characterization (Jones et al. 2006)	– Probabilistic breach of physical security (Jones et al. 2006)

(a) Possibility of a coordinated cyber-physical attack.

Appendix C

Hazards and Associated Stressors

Appendix C

Hazards and Associated Stressors

Implementation of the framework requires understanding of the range of event severities associated with specific hazards and the mechanisms by which the events can impact the integrity of grid and support infrastructure assets. This appendix lists some hazards potentially associated with high-impact, low-frequency events examples of the scales by which they're measured, and the associated stressors to grid/infrastructure assets. Some historic events are also identified.

Hazard	Example Severity Scales	Stressor(s)	Example Historic Event(s) and Scale
Seismic	– Moment Magnitude (M_w), or the Modified Mercalli Intensity Scale (I to XII)	– Peak ground acceleration – Tsunami inundation	1964 Great Alaska Earthquake, magnitude M_w 9.2
Pandemic	– Pandemic Severity Index Category 1 to 5 – (Mild, Moderate and Severe)	– Reduction in workforce / expertise	1918 Influenza Pandemic (Category 5)
Hurricane	– Saffir-Simpson Hurricane Wind Scale – Category 1 to 5	– Peak gust wind – Storm surge – Inundation – Hurricane-induced projectile – Hydrostatic loading	Hurricane Katrina, 2005 (Category 3); Hurricane Sandy, 2012 (Category 1)
Tornado	– Enhanced Fujita Scale EF0 to EF5	– Peak gust wind – Tornado-induced projectile – Lightning	Joplin, 2011 (EF-5)
Geomagnetic Storm	– G1 to G5 – Minor to Extreme	– Geomagnetic Induced Current (GIC)	March 13, 1989. Canada and the United States. (Extreme)
High-Altitude Electromagnetic Pulse	– To be identified	– Blast – Shock – Thermal Pulse – Geomagnetic Induced Current (GIC)	Starfish, 1962 (high-altitude nuclear test in Hawaii)
Cyber-attack[a]	– To be identified	– Degradation of cyber functionality – Data breach	Stuxnet, 2010. Computer worm attack in Iran
Physical[a] Attack	– To be identified	– Chemical attack – Radiological attack – Kinetic attack	Metcalf substation breach, 2013

a Possibility of a coordinated cyber-physical attack

Appendix D

Stressor/Asset Interaction

Appendix D

Stressor/Asset Interaction

Assessment of the fragility of grid and infrastructure assets to HILF-generated stressors is an element of the risk framework. In this appendix, some resources to support assessment of the impact of stressors on assets and associated fragilities are identified.

Asset	Hazard/ Stressor	Asset-Stressor Interaction	Sources Characterizing the interaction
Substation	Hurricane	Storm surge causing damage to building and equipment	Winkler et al. 2010
	Seismic	Loss of integrity and structural damage. Structural loss due to tsunami hydrodynamic force and inundation	Pitilakis et al. 2014, Schultz et al. 2010, Portante et al. 2010, Suppasri et al. 2011
	Physical Attack	Loss of integrity and structural damage due to sabotage	Stewart et al. 2006
	Cyber-Attack	Compromise of remote field devices and control systems potentially causing cascading events	Xiang et al. 2014
Transmission Line Support System	Hurricane Wind	Intense gusts of downburst winds cause loss of structural integrity of the transmission line tower	Panteli and Mancarella 2015, Salman 2014 for distribution steel poles
	Hurricane Flooding	Very strong currents erode the land and undercut the transmission line tower foundation	Simm et al. 2008 for embankments
	Seismic	Loss of structural integrity and reliability of transmission tower	Xie et al. 2012
	Hurricane Wind	Live wires touch each other causing short circuit and power flash	Winkler et al. 2010
	Hurricane Flooding	Buried transmission lines fail due to salt water intrusion	
Road	Hurricane	Debris/storm water/landslide/sinkhole/erosion/land subsidence. Fallen branches or severed lines	Pitilakis et al. 2014
Rail	Geomagnetic storm	Failure of SCADA equipment causes disruption in signaling	
	Hurricane – Wind	Train tankers carrying fuel overturn causing disruption in power generation	
	Hurricane Flooding	Disruption in fuel transportation for generation	
	Seismic	Deformation of rail roads and bridges leading to disruption in fuel transportation for generation	Pitilakis et al. 2014

Error! Reference source not found.. (contd)

Asset	Hazard/ Stressor	Asset-Stressor Interaction	Sources Characterizing the interaction
Pipelines	Geomagnetic storm	Failure of SCADA equipment causes disruption in load forecasting and hence supply of natural gas to generation facilities	
	Hurricane – Wind	Rupture or leakage is likely due to wind-borne projectile causing disruption in supply of natural gas to generation facility	
	Hurricane Flooding	Stress aftermath a mudslide/erosion causes disruption in oil and gas supply for electricity generation	
	Seismic	Structural damage and loss containment causing disruption in supplying fuel to generation facility	Pitilakis et al. 2014
Telecom	Geomagnetic storm	Satellite and radio communications are disrupted leading to failure of GPS and time sync	
Transformer	Geomagnetic storm	Geomagnetic induced current, overheat, saturate and fail multiple transformer cores (severe if line is long)	
	Hurricane Flooding	Damage to wires prevent transformers to detect spikes in electricity leading to overheating and melting	
	Seismic	Transformer malfunction due to leaks and internal failure	Pitilakis et al. 2014, Shinozuka et al. 2003, Anagnos 1999
Generating Station	Seismic	Structural damage due to ground motion and/or tsunami	Pitilakis et al. 2014, EPRI 2002, Portante et al. 2010

Appendix E

Grid Operability Models

Appendix E

Grid Operability Models

The risk framework requires use of existing grid models to assess how the grid responds to an initiating event and to estimate consequences. There is a variety of tools for transmission and distribution modeling which are publicly or commercially available. These models perform conservative, steady-state analysis or comprehensive time-step varying dynamic simulations. Some available tools are tabulated here.

Grid Operability Models

Grid Operability Model	Scope	Maturity Level and Availability
PSS/E	Transmission	Tool, Commercial
GE-PSLF	Transmission	Tool, Commercial
PowerVolt	Transmission	Open source/free to use
MatPower	Transmission	Open source
GridLAB-D	Distribution	PNNL owned – Open source
DSA Toolbox	Transmission	Tool, Commercial
Power System Analysis toolbox	Transmission	Free to use
Power system toolbox	Transmission	Free to use
TRELS	Transmission	Free to use
HAZUS	Transmission; Distribution	Free to use
HURRTRAK	Transmission; Distribution	Tool, Commercial
ESRI ArcGIS	Transmission; Distribution	Tool, Commercial
SELFE	Transmission; distribution	Open source
MATCASC	Transmission	Open source Matlab-based
OMNeT++, INET, ReaSE	Smart Grid	Free to use
ASKxELP	Power Networks	Open source
BROKE	Transmission line systems	Open source
Metatech Tools	Transmission	Commercial

Appendix F

Grid Recovery Models

Appendix F

Grid Recovery Models

The risk framework requires a characterization of asset recovery times to produce realistic estimates of scenario consequences. There is some precedent for modeling recovery times and this appendix identifies available resources.

Table F.1. Grid Recovery Models

Recovery Model Characteristics	HILF Context	Reference
The restoration time is assumed to be double that of normal weather conditions. Restoration delay is attributed to situational awareness and information sharing.	Hurricane winds	Panteli and Mancarella 2015
The restoration time is the sum of a minimum fixed required time to assemble and dispatch crew, and a random repair time that follows exponential distribution.	General blackout	Anghel et al. 2007
It is assumed that repair cannot be performed during major adverse weather periods. Random failure rates for transmission lines are associated with an error factor to reflect increase in failure rate during adverse weather conditions.	Severe weather	Billinton and Singh 2006
Repair duration of a line is not length-dependent and not more than that of normal conditions since extra manpower and resources are made available.	Adverse weather	Bhuiyan and Allan 1994
A network recovery-planning model is implemented to produce repair schedule that minimizes cost of power loss. Test-cases involved placing 4% to 20% of network assets out of service. Transportation time for spare large-sized transformers is also accounted.	Hurricane and terrorist attacks	Chee Chien 2006
The causal factors associated with restoration time are assumed to be hazard intensity and decision-making factors related to system repairs. The cost attributable to service disruptions is a function of restoration time.	Hurricane winds and storm floods	Francis et al. 2011

Appendix G

Monte Carlo Sampling

Appendix G

Monte Carlo Sampling

Monte Carlo methods involve multiple implementations of underlying deterministic models, sampled in accordance with assigned parameter probability distributions. Generally, a Monte Carlo approach that involves random sampling of input distributions can be problematic when the run time of the underlying model is substantial. In these cases, multiple implementations of the model may be impractical, particularly if the sample size required to achieve unbiased output distribution estimates is in the thousands, or tens of thousands. Therefore, much attention has been focused across numerous domains on the development of statistical methods that reduce the required sample size for a given model. Latin Hypercube Sampling (LHS; Helton and Davis 2003) is one of the more established methods for improved Monte Carlo analysis. It is a so-called stratified sampling approach that ensures the full breadths of the input distributions are sampled and that the output distributions are sufficiently unbiased for a sample size much smaller than would be required for the same output properties using conventional random sampling. LHS-based methodologies also exist to allow required correlations to be imposed on the input marginal distributions (Iman and Davenport 1982).

Importance sampling (Swiler and West 2010) is another alternative to random sampling in which the more influential portions of the input parameter space can be preferentially sampled to produce a more accurate uncertainty characterization for the output ranges of interest. For instance, the analyst's interest may be focused on extreme output wind speed predictions, in which case importance sampling provides a means of focusing on the regions of the input space that most influence these extreme predictions. Again, this approach allows an economy of sample size, in this case by focusing on the parameter space region of most interest.

Another class of sampling methodologies is Markov Chain Monte Carlo (Gelfand and Smith 1990). Unlike the methods previously identified, a given sample member in Markov Chain Monte Carlo is randomly selected based on the value of the previous sample member. That is, the entire input sample is not drawn a priori, but is generated sequentially throughout the analysis process with the objective of reaching an equilibrium distribution that closely estimates the actual output distribution. The sampling process is continued until the stable output distribution is produced.

An alternative to sampling economy as a means of addressing long model run times is to create surrogate models that emulate the behaviors of the detailed models while having substantially shorter run times. There are numerous approaches available for the development of surrogate models, the most conventional being the development of so-called response surfaces, which are generally constructed from statistical regression fits between model inputs and outputs based on a limited number of model runs (Iman and Conover 1980). These response surfaces, which have minimal run times, are then used as the basis for conducting the full uncertainty analysis in lieu of the original model. Note, however, that, depending on the goodness of fit of the surrogate, uncertainty can be introduced around the accuracy with which the source model is being emulated.

Appendix H

Peer Review Comments and Response

Appendix H

Peer Review Comments and Response

This appendix presents comments on the report from three peer reviewers: two senior risk practitioners/educators and an electrical power industry professional. While some editorial changes were made in light of the comments, the reviewers' insights largely provide focus for future development of the framework and highlight potential technical challenges of which the authors should be wary. Overall, the feedback is extremely helpful. In what follows, the three sets of review comments are presented along with the authors' interpretations of how they will help guide the path forward.

H.1 Comments from Professor Ali Mosleh, Director of the UCLA B. John Garrick Institute for the Risk Sciences

The report offers a framework for risk analysis of the electric power grid, which is vulnerable to natural and man-made hazards resulting in the simultaneous loss of multiple grid infrastructure assets. Within the risk modeling framework, the report provides a description of the process, needed elements and steps, and possible methods that could be used to implement them. The report also identifies some of the methodological gaps and complexities that need to be addressed further research and development efforts. The following offers a few comments and observations on the proposed framework and its elements.

1. Overall Framework

The report proposes a model-based approach to risk assessment of high-impact, low-frequency power grid events. I agree with this choice and the report's statement that a model-based approach is justified on the grounds that a direct data-based assessment of the risk of the events of concern is problematic due to insufficiency of the statistical basis to estimate their probabilities and consequences.

The structure of proposed framework is quite reasonable as it leverages the well-established "scenario-based" explicit modeling approach to risk assessment of complex technological systems, and maps it into the characteristics of electric power networks. The scope is broad and involves events of diverse nature (natural hazards, system failure, and international and unintentional acts of human), and includes all major elements of the power grid (generation, transmission, and distribution). While this may pose challenges in the choice and integration of appropriate models, the overarching framework and its underlying principles are all on solid grounds. With respect to risk metrics, a quantitative perspective is adopted while correctly indicating that estimation of some of the needed parameters such as event probabilities would have to rely on expert judgment. This, however, is a situation encountered by virtually all risk and reliability assessments involving rare events and complex phenomena.

2. Elements of the Framework

The proposed framework identifies areas where models are needed and the sequence or process that should to be followed in applying them. Accordingly, models are needed for:

- Hazard identification and probabilistic characterization (frequencies of associated events)
- Initiating event development (selection of representative events for analysis)
- Grid and supporting infrastructure response characterization (probabilities of asset failures)
- Consequence assessment (power outage or other metrics)
- Model integration to develop risk profiles

These steps follow typical model-based, scenario-driven, risk analyses and cover all core activities of engineered systems risk methodologies, although in most cases Uncertainty Characterization and Quantification is also included as a separate step, highlighting the importance of measuring and communicating uncertainties in risk assessment and risk management.

The report then offers a process and constituent activities that cover various aspects of the above core steps (Fig. 2 of the report), suggests possible starting points or example outputs (e.g., list of hazards), and provides a brief assessment of methods and tools that could be used, as well as potential methodological and implementation challenges. At the conceptual level the proposed process and modeling choices are quite reasonable. The following comments are offered on the few modeling aspects that could pose methodological challenges:

a. <u>Modeling of the Relation between Support Infrastructure and Power Network</u>

The report highlights some of challenges including the selection of a subset of support infrastructure to keep the model complexity and size to a manageable level, and challenges involving modeling the interdependencies. While model simplification is a practical necessity and a meaningful strategy, the risk scenario identification may still be quite complex, and may have to relay more on simulation methods or dynamic network models, rather than the typical event sequence diagramming and discrete logic modeling. Perhaps a hybrid of all three approaches would be needed. All this may be much simpler if a detailed model of the network system is not required to identify failure/impact categories, which is likely to be the case for large-scale natural hazards. The case of cyber-attack or other international human acts may be more challenging.

b. <u>Modeling Asset Fragilities</u>

This step as described in the report generalizes the concept of fragility to all assets. As stated in the report a fragility curve defines the probability of functional failure of the asset conditional on specified stressor magnitude. The generalization is fine conceptually and at high level of abstraction, but perhaps not very useful at practical levels for human or software initiated events. The report recognizes this point by stating "It is expected that some methodology development will be required for stressor types not conventionally modeled in a stressor/fragility (i.e., load/capacity) paradigm." But the question is whether there is real benefit in fitting everything in that paradigm.

Another area that needs careful examination is the idea of "grouping assets into equivalence classes for each stressor type (e.g., seismic ground excitation, wind speed, projectile impulse, etc.), and developing the fragility curves for each class/stressor combination". Then according to the report "an equivalence class would include all assets with approximately equal fragility characteristics". This however may complicate the development and tracing scenarios from initiators to consequences.

c. <u>Scenario Formulation</u>

For risk scenario generation, the report anticipates that there may be a combinatorial complexity due to extremely large set of scenarios that could be generated. Monte Carlo approach is mentioned as a possible solution strategy, adding that "The expectation is that for each initiating event, the scenarios will be sampled from joint distributions over stressor magnitudes and asset fragilities. That is, a given scenario will include the occurrence of an initiator and the subsequent failure of a set of assets, where for each asset in that set, at least one associated stressor exceeds the corresponding capacity to withstand it. Therefore, for each initiator, the number of scenarios generated is equal to number of members in the Monte Carlo sample for which at least one asset fails. The methodology and sample size selected must be demonstrated to generate good estimates of the risk characteristics".

This is an attractive idea but its effect on ability to gain qualitative insights from the scenarios needs to be carefully considered.

d. <u>Risk Integration</u>

For calculating aggregated risk across different hazards, Appendix A provides a high level mathematical formalism that brings together the elements of the framework. In practice the various terms and parameter of the mathematical model need to be developed based on possibly complex models and/or computational procedures. Therefore the simplicity of the abstracted mathematical formalism in the report should not be taken as an indication of the level of computational complexity of implementing the methodology. In other words "a simple Excel framework" is not a likely option.

Authors' Response

The authors appreciate Prof. Mosleh's insightful review of the HILF risk framework. His perspectives complement our own with regard to implementation challenges we will likely need to address going forward, and we take exception to none of his comments. A theme highlighted by Prof. Mosleh is wariness of certain aspects of the methodology that may potentially obscure qualitative insights; for example, the notion of grouping assets for fragility characterization, and the Monte Carlo approach to selecting from the combinatorially large number of potential scenarios for the purposes of risk estimation. We fully agree that gaining qualitative insights from a risk model is a crucial outcome, and through test implementation of the framework, we will identify methodological issues and shortcomings that need to be addressed. We do note that in the grouping of assets for fragility analysis, the intent was not to leave specific assets undistinguished from one another in the risk model, but more to provide a means of defining a population of equivalent assets for data analysis supporting fragility characterization.

Prompted by Prof. Mosleh's mention of uncertainty quantification, a few observations are appropriate. The current framework does not make explicit distinction between epistemic (state of knowledge) and aleatory (randomness inherent in the system) uncertainty, and consequently does not advocate the overlay of an explicit epistemic uncertainty analysis over an underlying aleatory model. The decision was made that implementation of the framework would produce an analysis based on point estimates of risk, and there are two principal reasons for this. One is the practical consideration that there is a substantial jump in the resources required to implement a full, probabilistic uncertainty analysis that distinguishes epistemic and aleatory uncertainties. Second, while uncertainty analysis is crucial if the study is being conducted to obtain absolute measures of risk, as noted in the report, this is seldom the prime application of a risk model and greater insights always derive from an understanding of relative risks. Examples include the risk-informed prioritization of issues or assessment of the risk-reduction impact associated with a risk-management measure. While for such applications there may remain an argument for conducting an explicit uncertainty analysis, adequate insights can generally be gained from sensitivity studies which are substantially less resource-intensive. We believe the test implementation phase of the framework will provide insight on this question.

H.2 Comments from Dr. Robert Youngblood, Senior Risk Consultant, Idaho National Laboratory

The writing style is good and the report says that it is about a "framework" rather than model, this framework being defined at a high level.

For some purposes, the grid can be seen as a colony of mutually reinforcing elements (sources and sinks), and it can tolerate some hits here and there because it all works together. But when the grid comes crashing down, you don't just flip a switch to turn it back on. The report appropriately mentions recovery time as a consideration, but for the class of events being discussed, modeling black-start capability would also be something to mention. And beyond black-start: in a really widespread event with losses of assets, getting new assets where they need to go arguably needs also to be modeled. (Think "FLEX.") The report is relatively silent about that. Actually the report's scope may overlap that of post-9/11 work on events causing widespread disruption. This work would be worth mentioning somewhere as a resource. Some of it probably touches on loss of grid as a consequence.

The US has already had some pretty widespread blackouts, occasioned not by catastrophic and widespread initiating events but by instability. The report says somewhere that risk models frequently don't bother with detailed phenomenological modeling. Well, electrical engineering is one of the few areas where people actually can predict what will happen (unlike, for example, materials behavior), and for important classes of blackout events, such models are arguably warranted. The report mentions models that apparently do this, but the reader cannot easily tell what use is contemplated for them, unless it's analogous to success criteria in classical logic modeling. Models of some events don't really need to go too deeply into analysis of rapid voltage transients, but they do need to go into analysis of stability. Suppose a fairly widespread instability develops, maybe involving grid mismanagement, and then something ordinarily minor happens; down goes a region. The report uses the term "cascading" and that's a good term, but the idea isn't developed much in the report.

This may be a misimpression, but it seems that the report's authors contemplate a classical event-tree / fault-tree development, with most of the "failures" being asset failures induced directly by severe external events (e.g., seismic fragility of assets). Example: Section 2.1.8: "Discrete representative events must be chosen as initiators." Well, yes, in a classical event-tree model, but not in a simulation. Arguably, there are reasons to doubt the viability of classical logic models for this sort of situation; many workers would argue for a simulation-based approach. One would construct a simulation model and then hit it with a simulated external event, model asset failures, and let the system evolve. If it were near a stability limit anyway, the event might push it over the edge even with few direct asset failures. And then turning it on might be difficult, and getting new assets where they are needed might be difficult if roads and bridges were out. Some argue that this sort of modeling is infeasible. The present writer disagrees, and has disagreed for a generation.

Figure 1. WHO is managing the risks here? The regulator or the regulated entity? The figure has an appropriate risk management spin, and in general the report has an appropriate emphasis on decision-making, but it could go a bit farther in this region than it does.

Figure 2. Things not mentioned: Stability, Voltage transients, black-start, FLEX, …. The figure does not flatly state that all "failures" would be due to asset fragility to external events, but the reader could easily get this impression.

Authors' Response

The authors very much appreciate Dr. Youngblood's insightful comments, and they will provide substantial value in helping set the path forward for test implementation of the framework. The key theme we take away from his observations is that the route to using simulation methods as the basis for risk assessment is by no means a well-established one, and there exists a range of perspectives on the feasibility and optimal methodology for such an integration. While we do not consider the framework to be one that is purely simulation-based, we do expect it to rely on the use of simulations in its implementation, such as in the comparison of asset fragilities and loads across a broad space of asset types. That is, while the simulation of scenario elements will be a useful and necessary tool, risk evaluation based on a full system/event simulation would likely be highly resource intensive and probably lack a clear prospect of incremental benefits. We do realize that this viewpoint may elicit contrasting perspectives. With regard to the role of event/fault trees, while the framework does not necessarily prescribe their use, the anticipation is that the rudimentary Boolean logic they represent will inevitably be useful tools in the structuring of the impact scenarios underlying the risk models.

Dr. Youngblood reaches conclusions about the possible use of power grid models that do correctly reflect the authors' intent. We see the specific means of integrating the system dynamics predicted by grid models into an underlying risk model as a key area for evaluation during the framework test implementation. That means of integration will determine the effectiveness with which the risk model captures compounding factors associated with grid dynamics.

H.3 Comments from Scott Mix, Senior Critical Infrastructure Protection (CIP) Technical Manager, North American Reliability Corporation (NERC)

1. There should be some method for determining individual stressor components to individual power system asset classes, for example seismic events to specific lines. This would allow refined physical-to-power flow analysis of the various non-power system events.
2. Wild fires should be categorized and evaluated as natural or man-made. Naturally occurring and accidental man-made wild fires could be predicted using stochastic methods. Targeted man-made wild fires require assessment of a malevolent threat.
3. I suggest including electromagnetic pulse (EMP) as a separate class from Geomagnetic Disturbances (GMD), since it has some different characteristics.
4. When you refer to "loss of two generating station" are you really referring loss of two generating "units"?
5. I suggest that that there are two kinds of supervisory control and data acquisition (SCADA) systems, those associated with control centers and those associated with Distributed Control Systems (DCSs). If you intend to include generator DCSs, transmission protection, and generation plant control systems as part of your asset mix then it would be better to identify them as a separate asset group referred to as DCSs.

Authors' Response

The authors appreciate Mr. Scott Mix's comments and believe that they will provide practical guidance in developing test implementation of the framework. In regards to the specific comments:

1. The authors agree that specific stressors for asset groups according to different hazards should be determined. Application of the risk framework is designed to identify asset-specific stressors that would result from initiating events associated with a given hazard. The authors intend that assets be grouped by vulnerability and location, and then consequences of specific asset failures should be modeled.
2. Application of the risk framework is intended to identify hazards that could produce HILF events. Wild fires can potentially produce HILF events and it is our intention that they should be considered. As pointed out, two different classes of initiating events (caused naturally or deliberately targeted) should be considered.
3. The authors agree that addressing EMP could be considered a separate hazard class from GMD because it has some different characteristics. Table 1 was adjusted to include an EMP as an example of human-induced hazard.
4. The authors mean to refer to "two generating stations" as referred to on page 11 of the NERC Standard TPL-001-4 (Transmission System Planning Performance Requirements).
5. The authors intend that all major asset groups represented by the bulk power system should be addressed, including Controls Centers and their supervisory control of bulk power system assets and special system that perform supervisory control of DCS such as protection systems, generation plant control systems, and load shedding. Related text was adjusted per the comment.

Distribution

No. of
Copies

1 Eric Rollison, General Engineer
Department of Energy, Office of Electricity and Energy Reliability (OE-40)
Washington, DC 20585

1 David Ortiz, PhD
Deputy Assistant Secretary
Department of Energy, Office of Electricity and Energy Reliability (OE-40)
Washington, DC 20585

1 Alice Lippert
Senior Technical Advisor
Department of Energy, Office of Electricity and Energy Reliability (OE-40)
Washington, DC 20585

No. of
Copies

Local Distribution
Pacific Northwest National Laboratory

Jud Virden	K9-53
Carl Imhoff	K9-69
Diana Shankle	K7-76
Paul Skare	J4-90

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by **Battelle** *Since 1965*

U.S. DEPARTMENT OF
ENERGY

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99352
1-888-375-PNNL (7665)

www.pnnl.gov